Kibana access from ELK VM : ‘ssh [sysadmin@10.1.0.4](mailto:sysadmin@10.1.0.4)’

Make sure that Kibana is working from Web and Localhost

sysadmin@ACME-VM1:~$ curl <http://localhost:5601/app/kibana>

Type in google : [http:// [52.138.103.192](https://portal.azure.com/#blade/HubsExtension/ResourceMenuBlade/id/%2Fsubscriptions%2F860bde32-c4fb-4a4f-9c48-26065e0b7281%2FresourceGroups%2FRed-Team%2Fproviders%2FMicrosoft.Network%2FpublicIPAddresses%2FACME-VM1-ip/menuid/configuration):5601/app/kibana](http://40.84.55.28:5601/app/kibana)

root@c1e0a059c0b0:/etc/ansible ‘mkdir files’

root@c1e0a059c0b0:/etc/ansible/files

curl https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat > /etc/ansible/files/filebeat-config.yml

root@c1e0a059c0b0:/etc/ansible/files# nano filebeat-config.yml

hosts: ["10.1.0.4:9200"]

username: "elastic"

password: "changeme” # TODO: Change this to the password you set

setup.kibana:

host: "10.1.0.4:5601"

Get the filebeat link installer here :

Kibana > Logs : Add log data > System logs > DEB > Getting started

curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb

root@c1e0a059c0b0:/etc/ansible/roles# nano filebeat-playbook.yml

filebeat-playbook.yml

---

- name: installing filebeat

hosts: webservers

become: yes

tasks:

- name: download filebeat deb

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb

- name: install filebeat deb

command: dpkg -i filebeat-7.6.1-amd64.deb

- name: drop in filebeat config

copy:

src: /etc/ansible/files/filebeat-config.yml

dest: /etc/filebeat/filebeat.yml

- name: enable and configure systems module

command: filebeat modules enable system

- name: setup filebeat

command: filebeat setup

- name: start filebeat

command: service filebeat start

Verify installation of playbook (Should have no errors)

root@c1e0a059c0b0:/etc/ansible/roles# ansible-playbook filebeat-playbook.yml

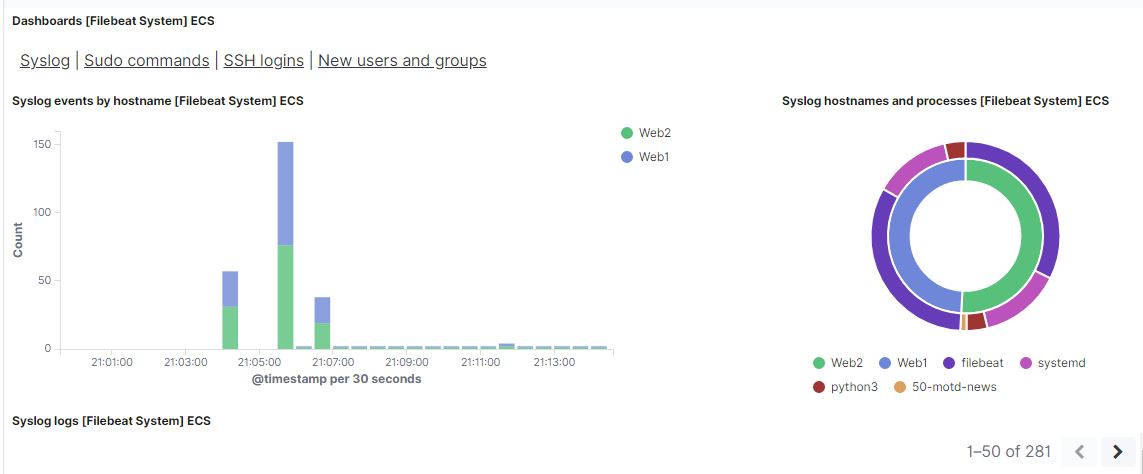
Make sure that ELK server is receiving filebeat logs from Kibana

Kibana > Logs : Add log data > System logs > 5:Module Status > Check data

“Data successfully received from this module”

Go to System logs dashboard

* It should show hostnames (Web1, Web2 Servers and Hostname Process)



Bonus : Metric Beat Installation and Configuration

Create the metricbeat data :

root@c1e0a059c0b0:/etc/ansible/files# curl -L -O https://gist.githubusercontent.com/slape/58541585cc1886d2e26cd8be557ce04c/raw/0ce2c7e744c54513616966affb5e9d96f5e12f73/metricbeat > /etc/ansible/files/metricbeat-config.yml

root@c1e0a059c0b0:/etc/ansible/files# nano metricbeat

output.elasticsearch:

# Array of hosts to connect to.

hosts: ["10.1.0.4:9200"]

username: "elastic"

password: "changeme"

setup.kibana:

host: "10.1.0.4:5601"

Get the metricbeat installer link here

Kibana > Add Metric Data > Docker Metrics > DEB > Getting Started

curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-amd64.deb

---

- name: install metric beat

hosts: webservers

become: true

tasks:

- name: download metricbeat

command: curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-amd64.deb

- name: install metricbeat

command: dpkg -i metricbeat-7.6.1-amd64.deb

- name: drop in metricbeat config

copy:

src: /etc/ansible/files/metricbeat

dest: /etc/metricbeat/metricbeat.yml

- name: enable and configure docker module for metric beat

command: metricbeat modules enable docker

- name: setup metric beat

command: metricbeat setup

- name: start metric beat

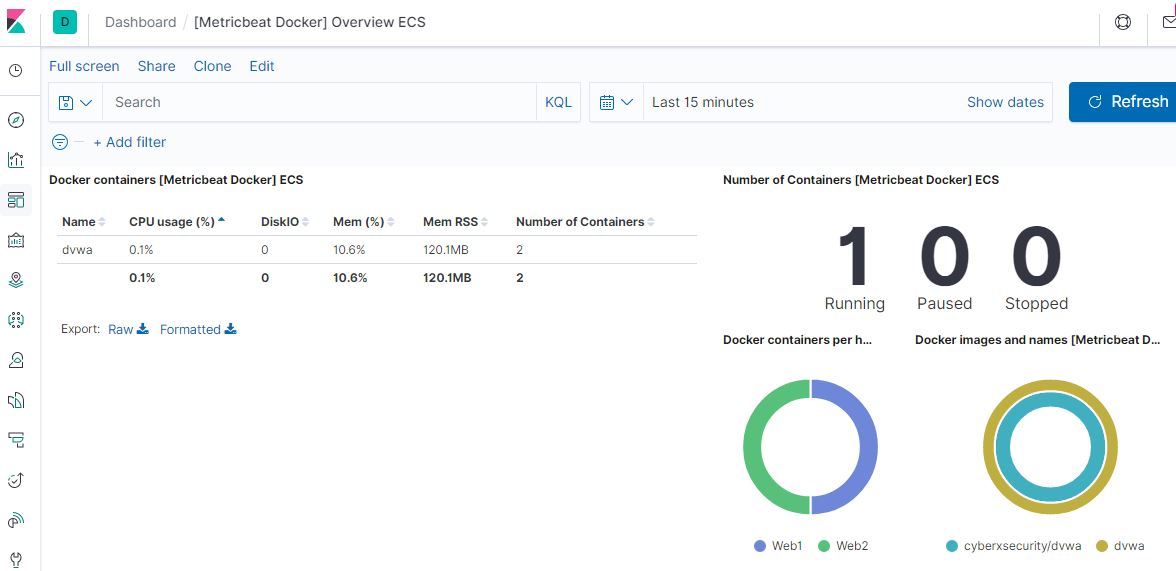
command: service metricbeat start

root@c1e0a059c0b0:/etc/ansible/files# ansible-playbook metricbeat-config.yml

Kibana > Add Metric Data > Docker Metrics > Module Status :

Data successfully received from this module

Then check the Metric Dashboard.



\*\* FOR the Metricbeat, docker container in Web1 and Web2 must be started first before starting the module and yml file otherwise it will not connect.

To start the filebeat :

sudo service filebeat restart

To start the metricbeat :

sudo service metricbeat restart

Summary :

Filebeat and Metricbeat Port Configuration in an ELK Container

hosts: ["10.1.0.4:9200"]

setup.kibana:

host: "10.1.0.4:5601"