**Azure Resource Group: (Red Team)**

1. Virtual Network (Red Team Net): 10.1.0.0/16 Subnet: 10.0.0.0/24
2. Network Security Group:

Incoming rule: My Public IP\_Access 22 107.190.0.0/16(Source) Virtual Network (Destination)

SSH\_JumpBox 22 10.1.0.4 (Source) Virtual Network (Destination)

Http 80 107.190.0.0/16 (Source) Virtual Network (Destination)

Outbound rule: Any Any Virtual network (Source) Internet (Destination)

1. Jump Box-VM 10.1.0.4 (Private IP) 13.90.94.255 (Public IP)
2. Web-1 101.0.5 (Private IP) 137.135.127.119 (Public IP)
3. Web-3 10.1.0.7 (Private IP) 137.135.127.119 (Public IP)
4. #ssh-keygen (Generate SSH key on Local PC and Copy public key and paste inside the Jump Box ssh password)
5. #ssh [AzureUser@13.90.94.255](mailto:AzureUser@13.90.94.255) (Access Jump Box and Log in)
6. azureuser@jump-box: $ sudo apt update

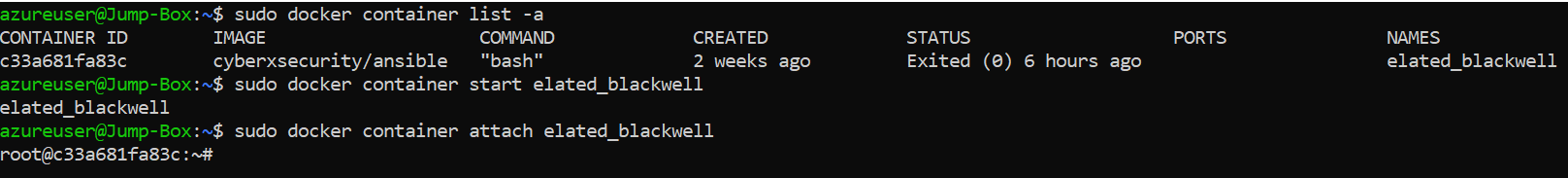
$ sudo apt install docker.io (Docker install on Jump Box)

$ sudo systemctl status docker (Docker services)

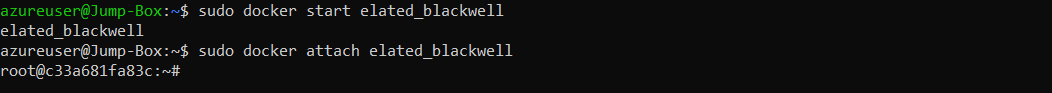
$ sudo systemctl start docker

1. $ sudo docker pull cyberxsecurity/ansible (Pull the cyberxsecurity/ansible container inside docker)
2. $ sudo docker run -ti cyberxsecurity/ansible:latest bash (Launch the ansible container with docker)
3. $ sudo docker container list -a or sudo docker ps

$ sudo docker start elated\_blackwell (Particular container start inside the docker)



1. $ sudo docker attach elated\_blackwell (Attached container with docker) After Prompt will change



1. Now prompt (root@......) changed and inside the container (Elated\_blackwell)
2. $ ssh-keygen (it will generate key inside the: /root/.ssh/id\_rsa.pub - - Copy key and paste inside the Web-1/2)
3. $ ssh [sysadmin@10.1.0.5](mailto:sysadmin@10.1.0.5) / 7 (Conform connection with Web-1/3)

Web-1





Web -3





1. Root# sudo nano /etc/ansible/ansible.cfg (Change ansible configure file)

Remote\_user = sysadmin

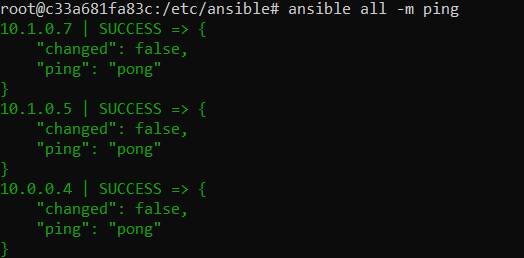
1. Root# sudo nano /etc/ansible/hosts (Change Hosts file)

10.1.0.5 ansible\_python\_interpreter = /usr/bin/python3

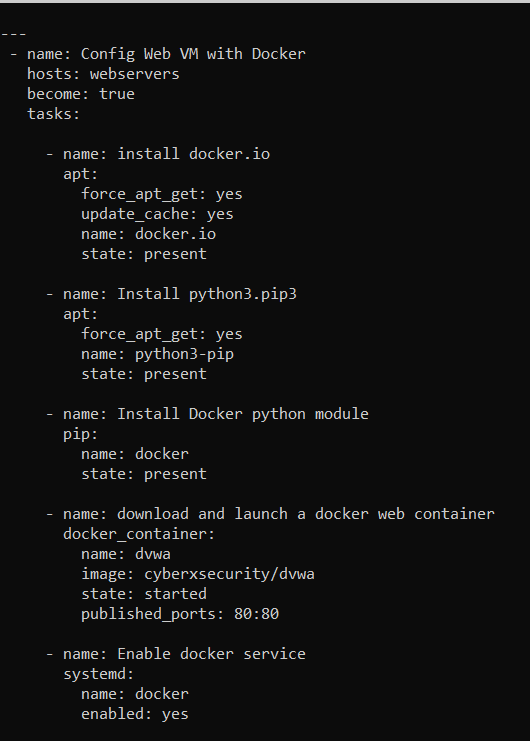
10.1.0.7 ansible\_python\_interpreter= /usr/bin/python3

13. root#........: cd /etc/ansible/

14. root#.... :/etc/ansible# ansible all -m ping (Verify the ansible configuration file)



15. root#......:/etc/ansible# nano pentest.yml (Run playbook to install docker, python and DVWA on web 1/3)



16. root#....: /etc/ansible# ansible-playbook pentest.yml

17. root#.... ssh [sysadmin@10.1.0.5/7](mailto:sysadmin@10.1.0.5/7) (connect the web1 and web3 to conform DVWA installation)

18. sysadmin@wen-3: $ curl localhost/setup.php

19. Create Load balancer (On Azure portal)

20. Name: Red-Team-LB

Add Health probe: RedTeamProbe – TCP – 80, Interval-5, Unhealthy threshold – 2

Add Backendpool: RedTeamPool – VirtualNetwork (RedTeamNet) – ipv4 – Associate to Virtual machine –

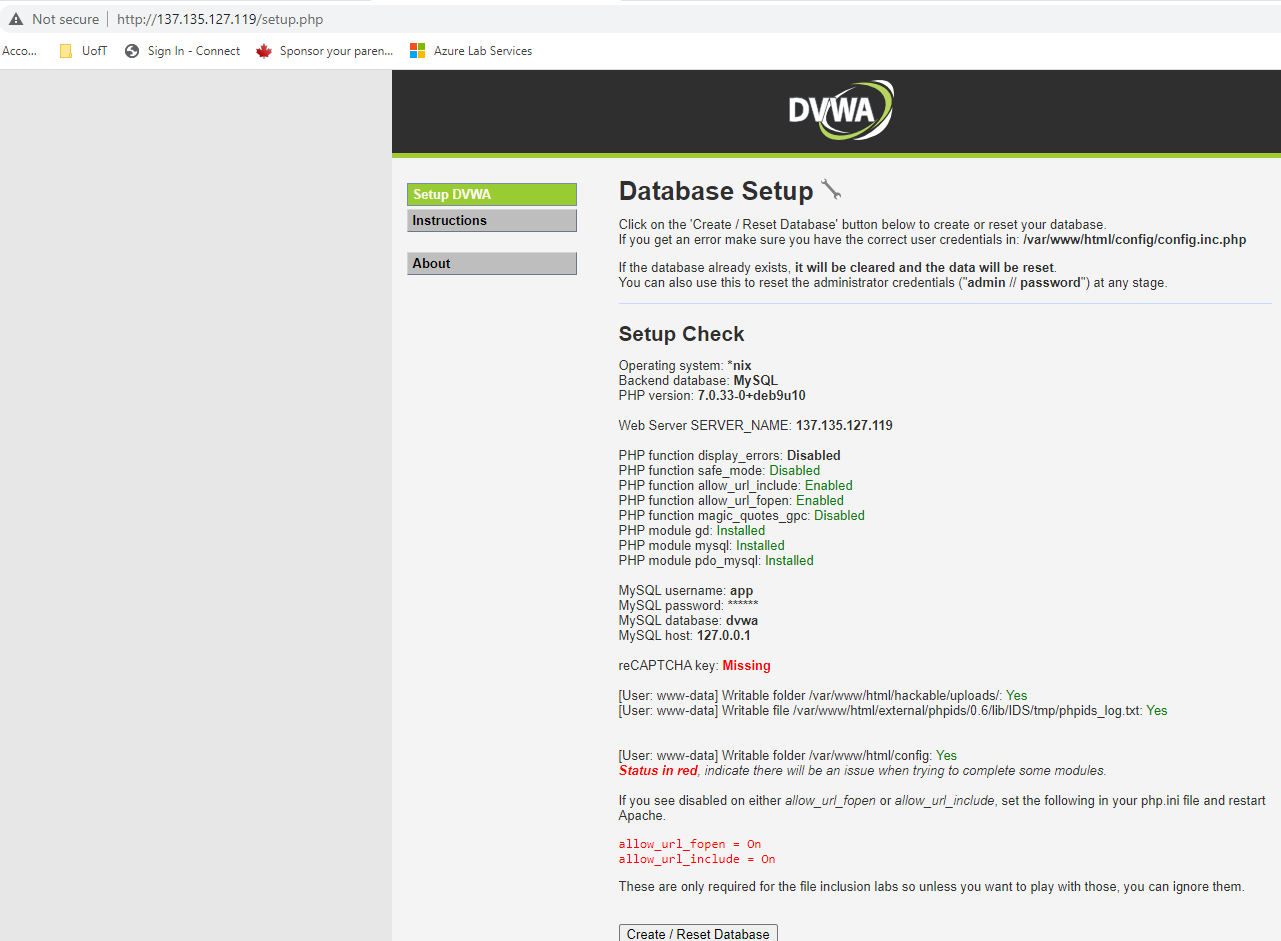
Virtual Machine (Web-1/ Web -3) and IP address (10.1.0.5 / 10.1.0.7)

I have already made network security rule before, but configuration will be:

SSH-LBR – Ipv4 – Frontend Address (137.135.127.119) – TCP – 80 – Backend port-80 – backend pool (2 virtual machine) – health Probe (TCP-80) – Session Persistence (Client IP and Protocol)

21. Homework would be done, if this DVWA application is working inside any browser: I check it and it is working fine.

<http://137.135.127.119/setup.php>



**Dhawal Pandya**

**Project:**

At last homework, I created 3 Virtual machines (1- Jump box, 2 – web server).

Installed docker and container(elated\_blackwell) on jump-box and DVWA on webserver to test vulnerability at web server.

1. For project, I built the one more virtual machine on different region (US West) for ELK

VM Name: ELK Server1 – IP: 10.0.0.4 and Public IP: 104.210.51.88 with default subnet under same resource group (Red-Team). Copy public key (jump box, elated\_backwell) to new vm computer.

1. Create Virtual network connection between both region (US-East and US-West)

Peering Network Connection:

(ELK) – End-to-Red - Address space 10.1.0.0/16,

(Red team) – Red-to-elk Address space 10.0.0.0/16,

1. Check the connection from elacted\_blackwell container to new ELK server.

ssh [sysadmin@10.0.0.4](mailto:sysadmin@10.0.0.4)

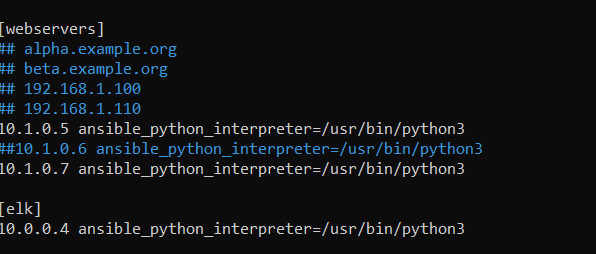


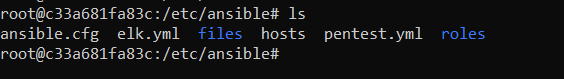


1. Edit the hosts file under jumpbox, elated\_blackwell container (/etc/ansible/hosts)

[ELKSERVER1}

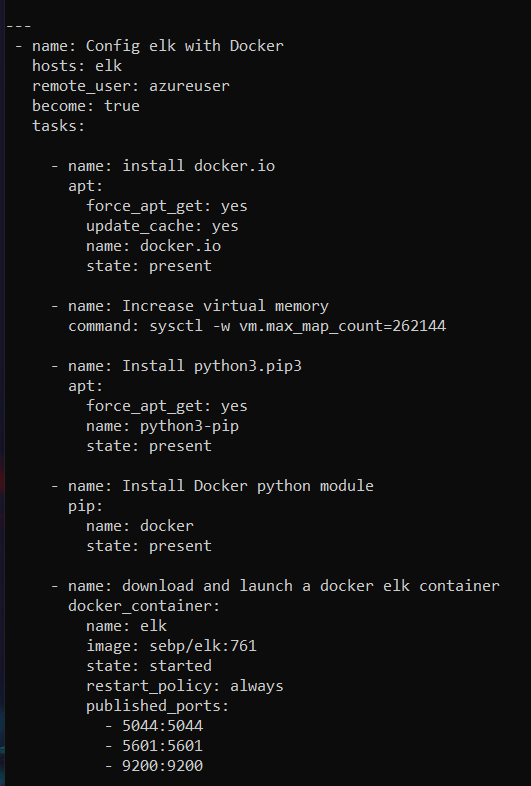
10.0.0.4 ansible\_python\_interpreter=/usr/bin/python3





1. After configured hosts file, I can run the play book and install packages

Build the play book to install packages for ELK server.



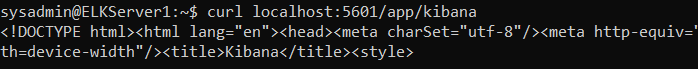
1. Add ssh access in network security group at ELKServer1NSG

SSH - 22 - Any – Any

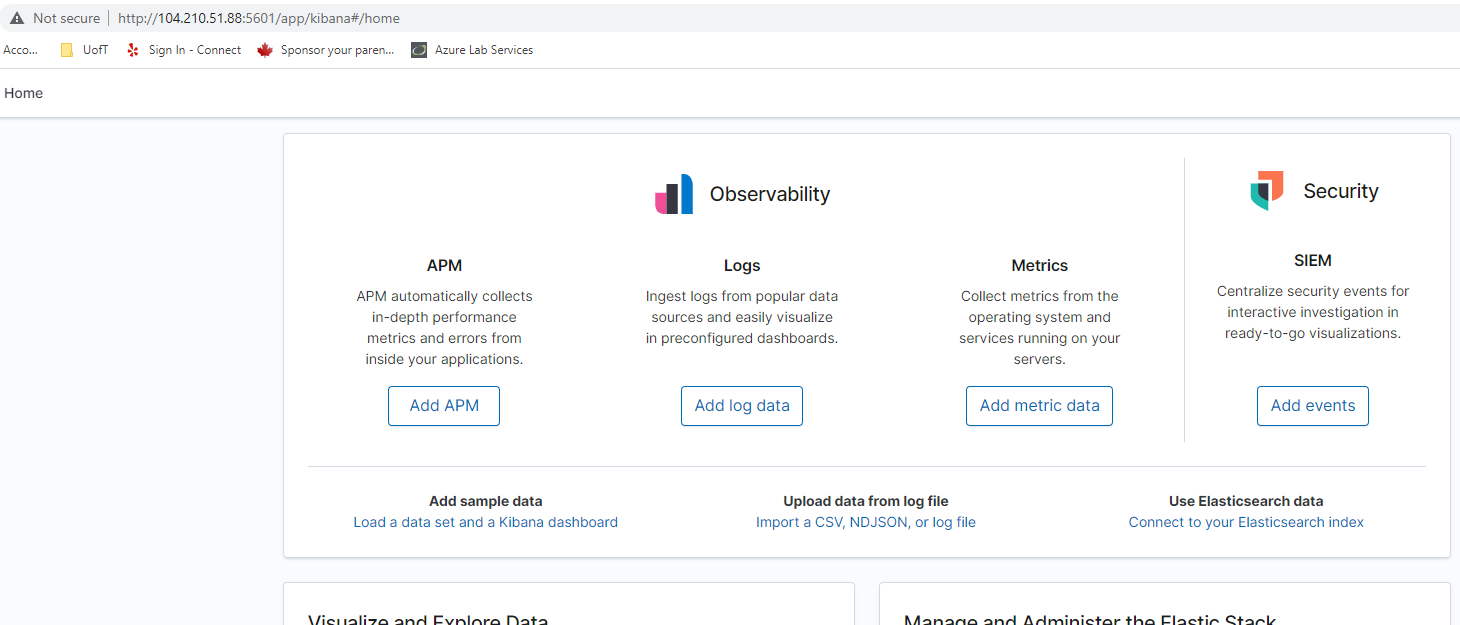
ELK-Http 5601 - any-any

1. Now check the Kibana is working form browser or not

Before browser, I can check it in elkserver:

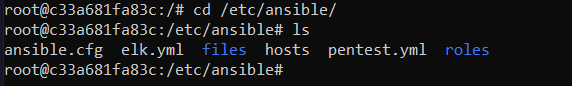


http://104.210.51.88:5601/app/kibana

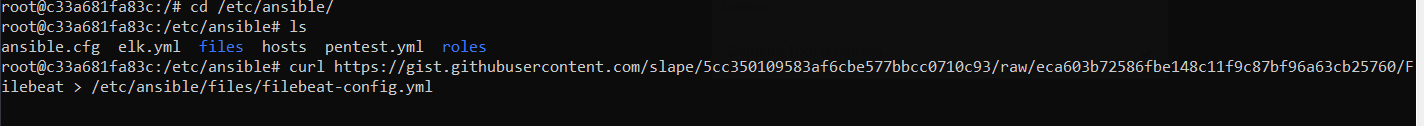


1. After run the kibana, I will install filebeat and metricbeat inside the files folder in ansible.

Fielbeat helps generate and organize log files to send to Logstash and Elasticsearch. It log information about the file system, including which files have changed and when.



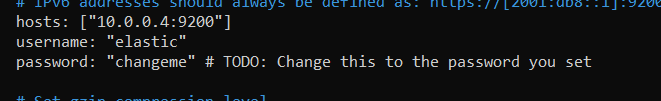
1. Run the Filebeat configuration file templete on ansible container.



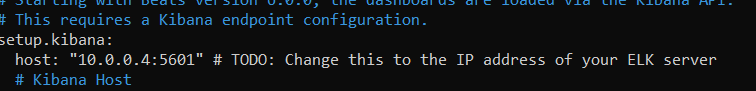
1. After install the filebeat configuration file inside the /etc/ansibe/files/filebeat-config.yml



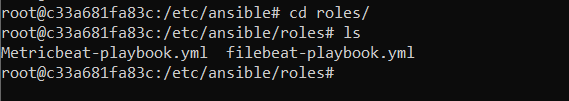
1. Edit the filebeat-config.yml for replace the ip address on elk machine(Ctrl+Shift+ -\_ 1106 and 1806)



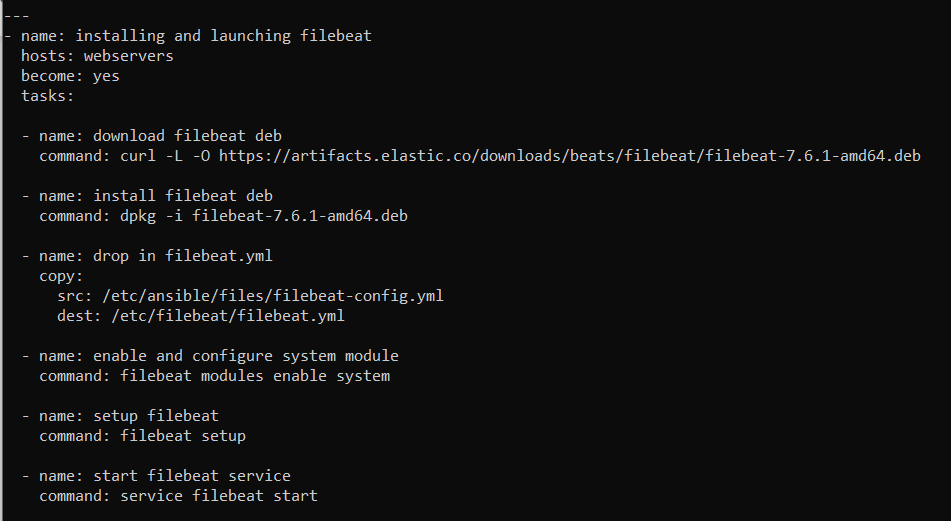
1. Line 1806 and replace the IP address at ELK Machine



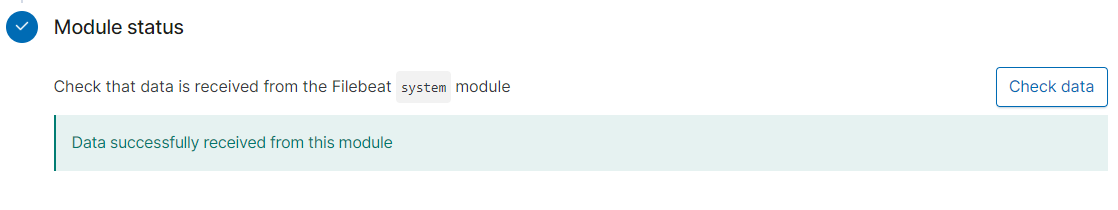
1. Now I create the filebeat installation playbook on /etc/ansible/roles/



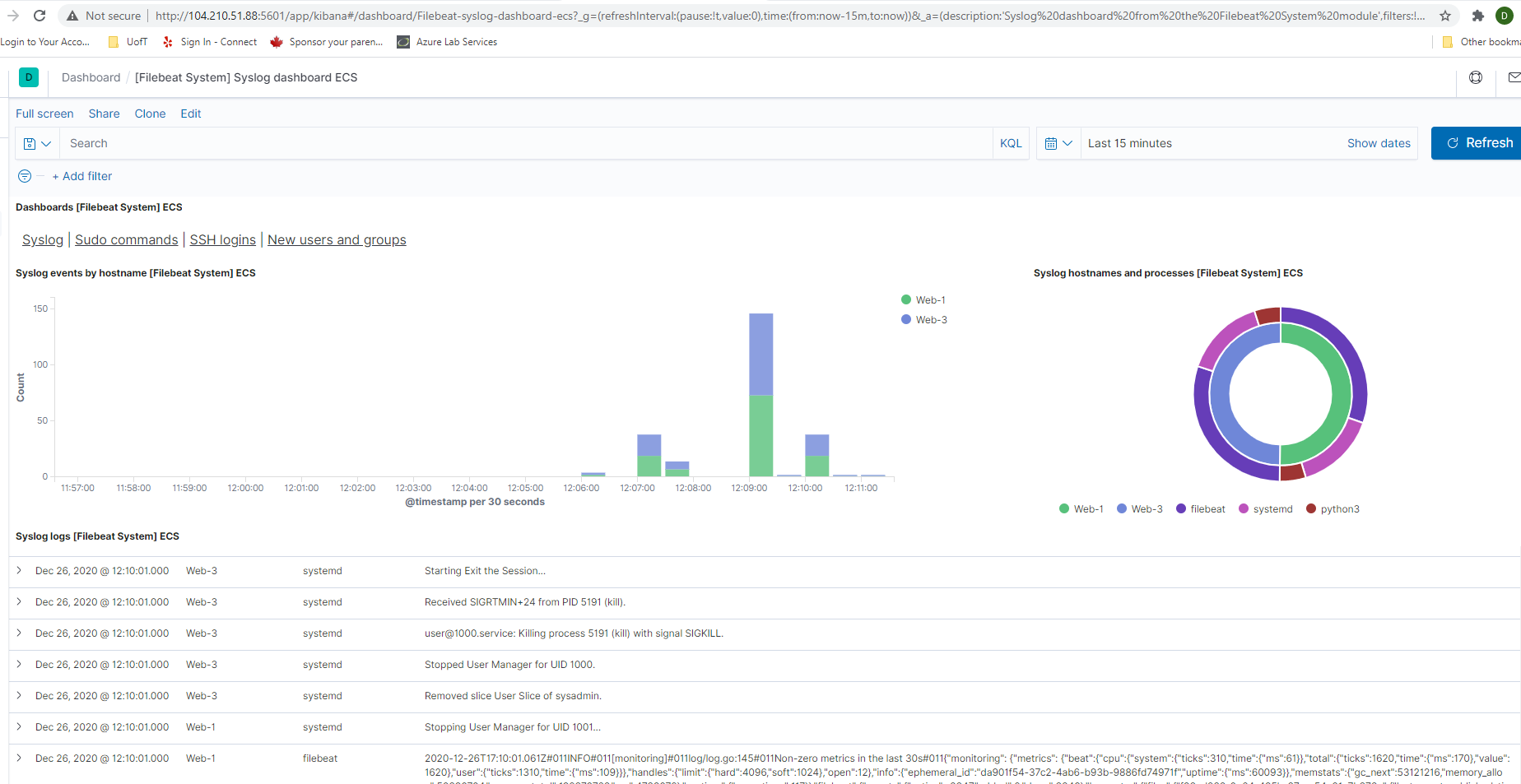
1. Create filebeat-playbook (filebeat-playbook.yml)



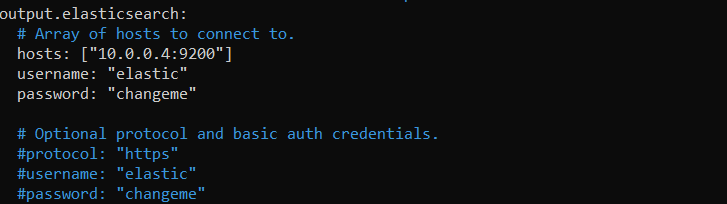
1. After run the playbook and check inside kibana browser, step-5 – Module status – Check data – verify incoming data.

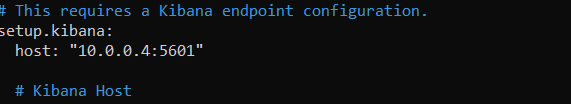


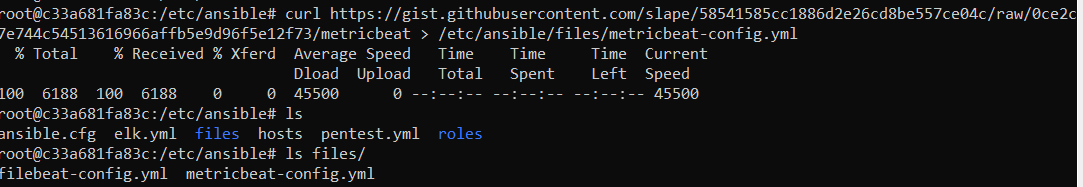
1. (Filebeat system) syslog dashboard ECS

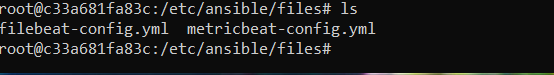


1. Now Create Meatricbeat inside the files (/etc/ansible/files/metricbeat)

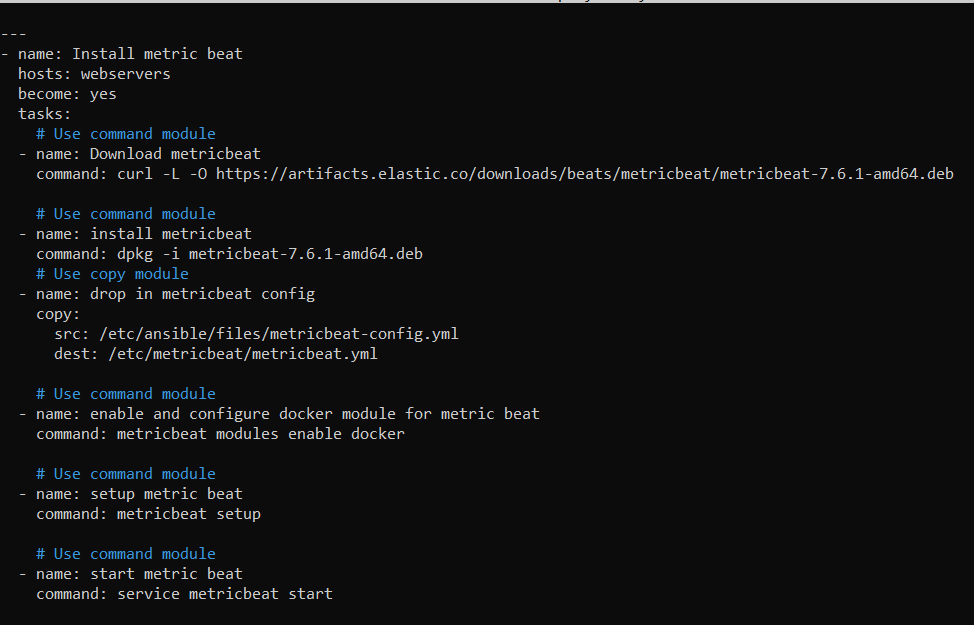


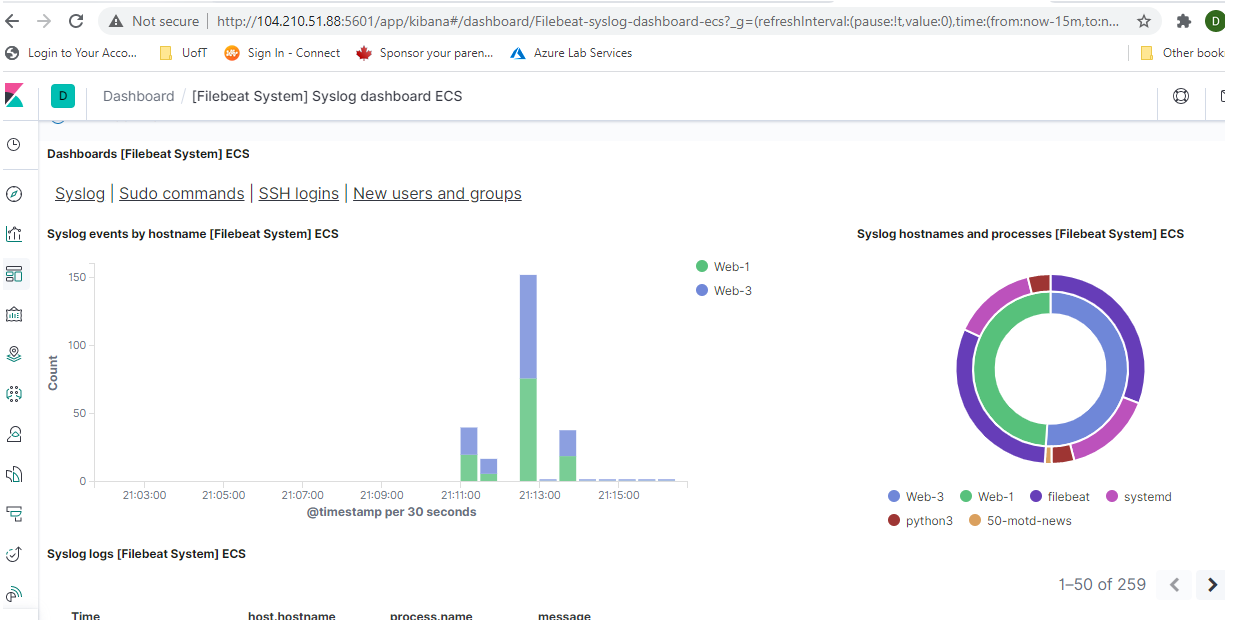




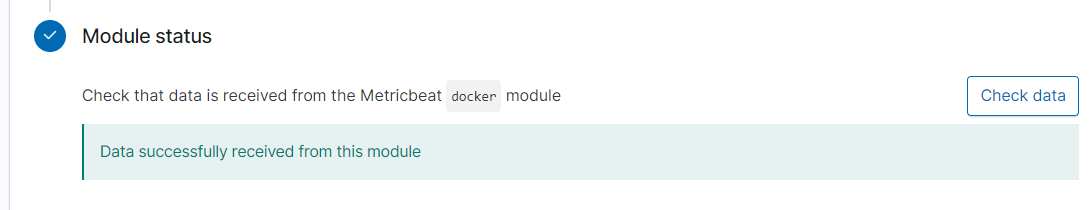


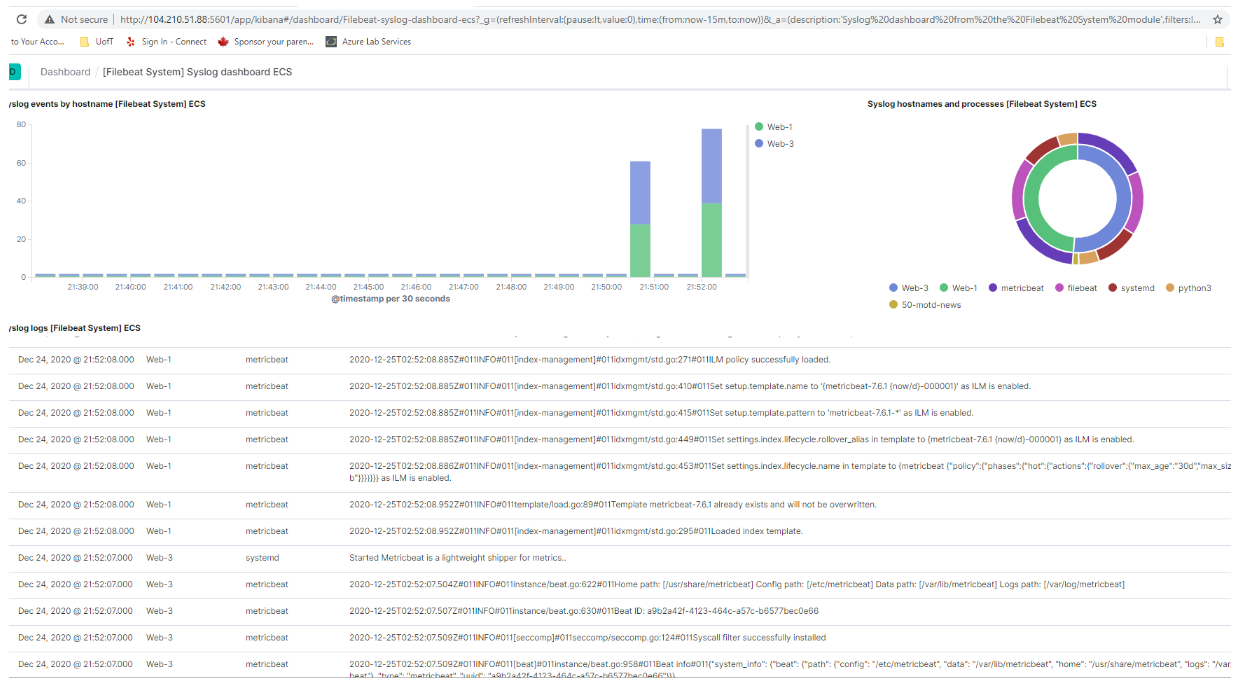
Metricbeat playbook :

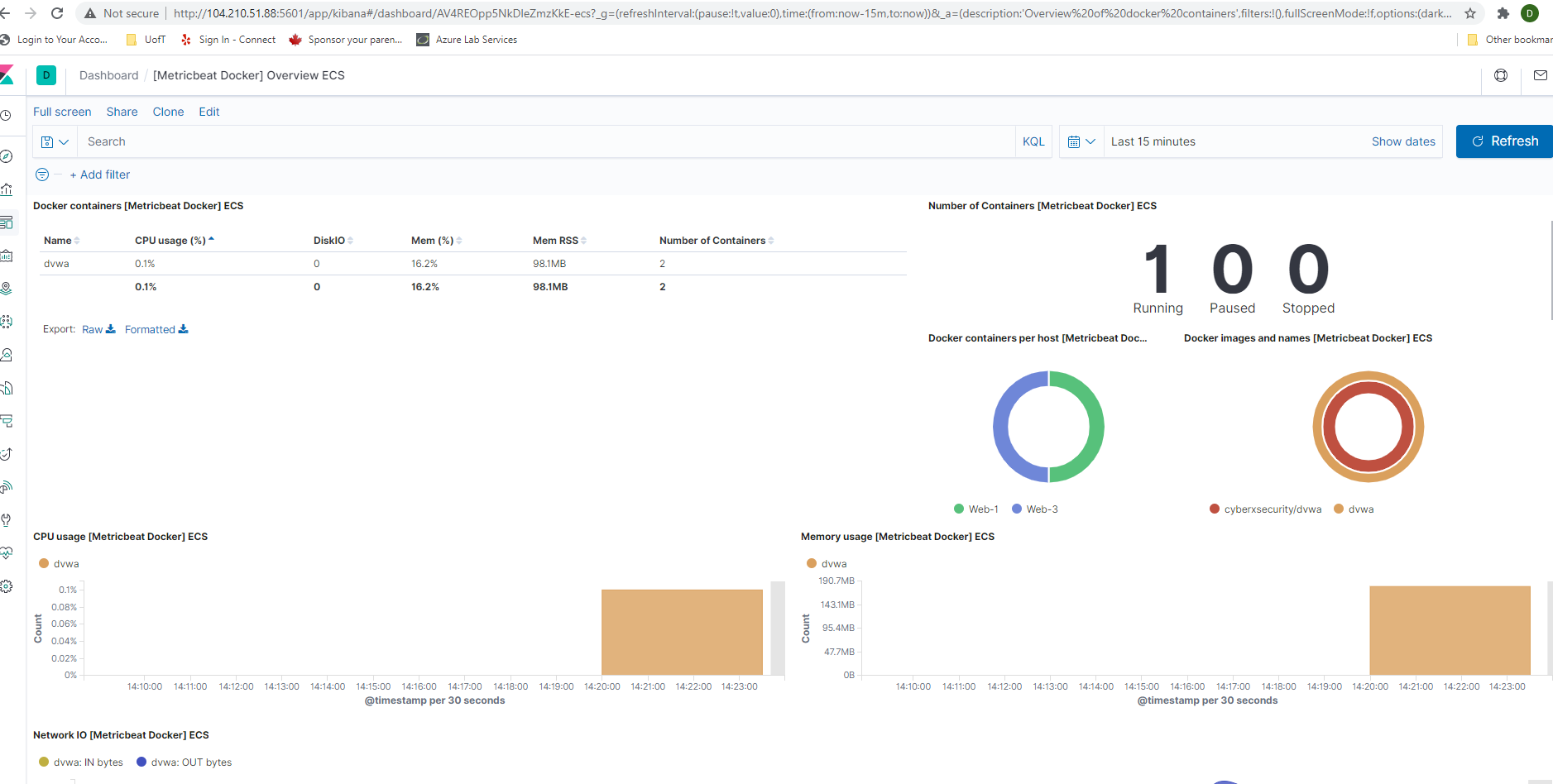




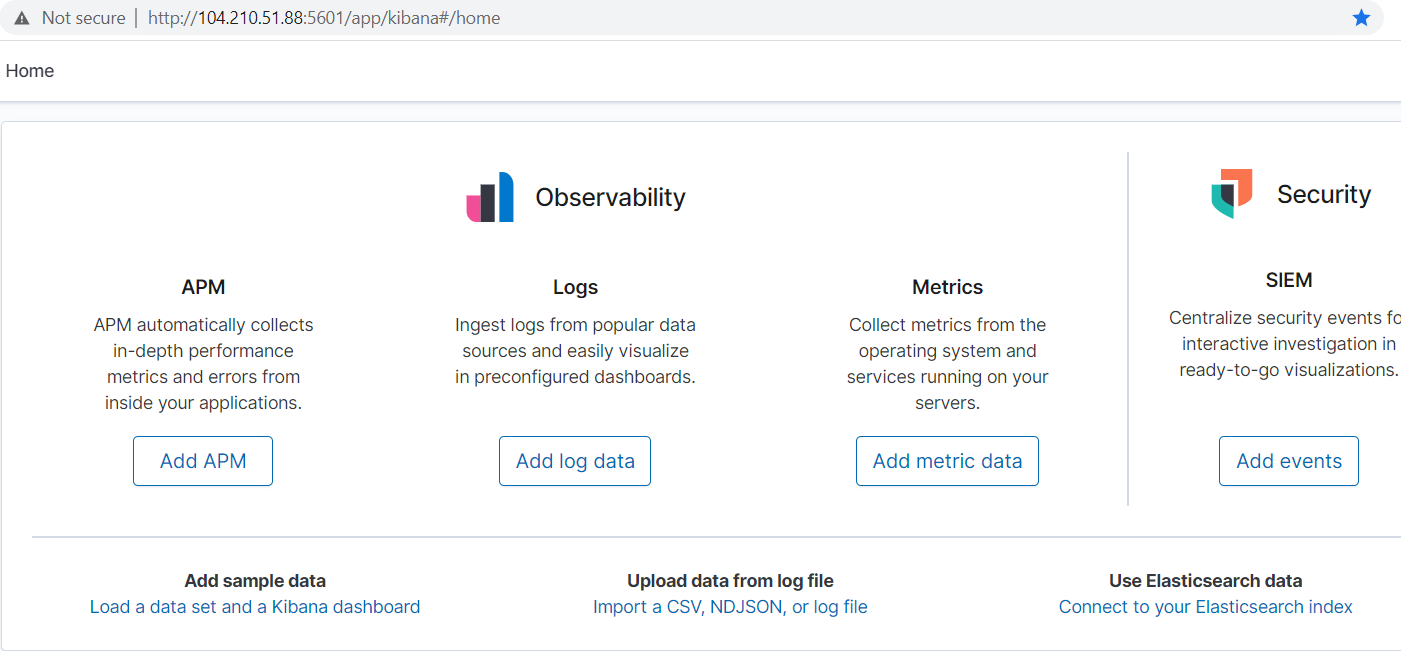
After run the metricbeat-playbook, went to bourse: Kibana-Metrics-Docker metric-DEB-Module Status- Check data



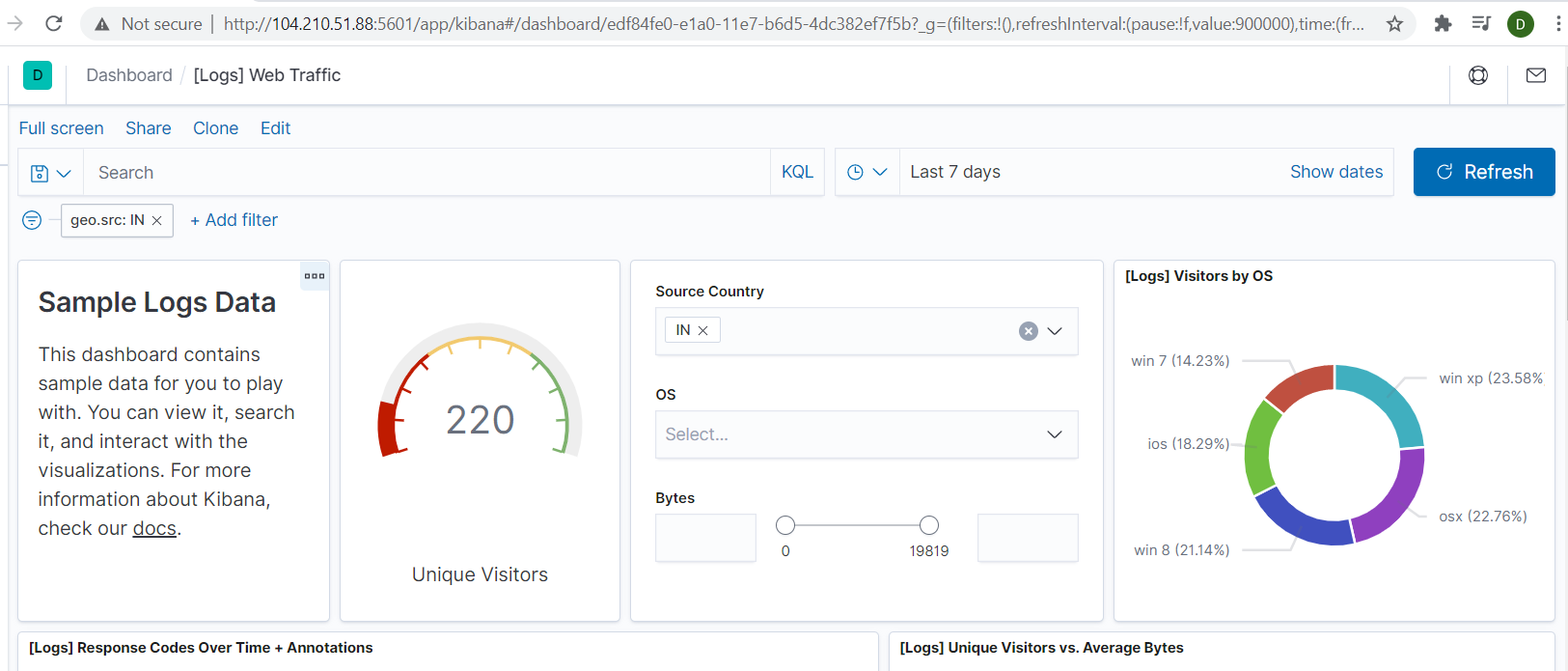




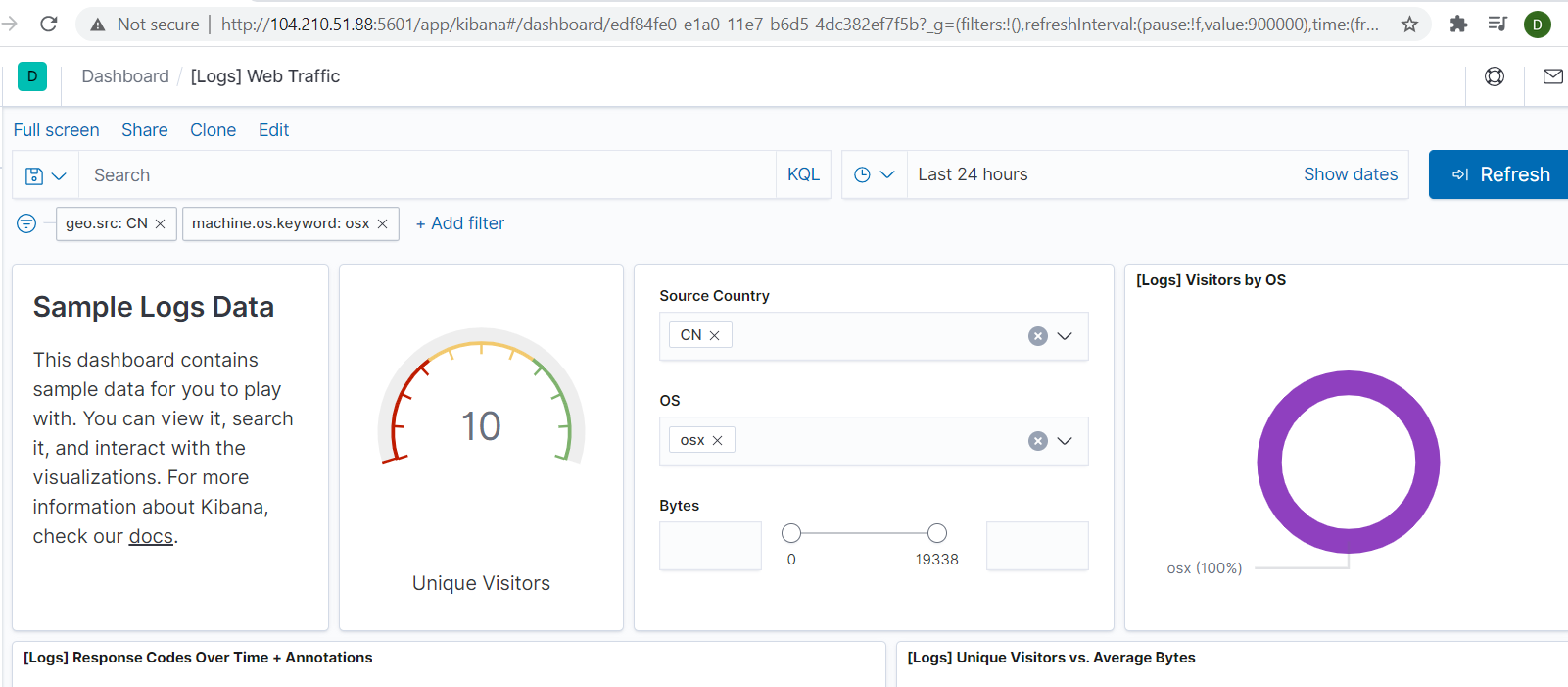
**Exploring Kibana -** Simple Web log data to kibana.



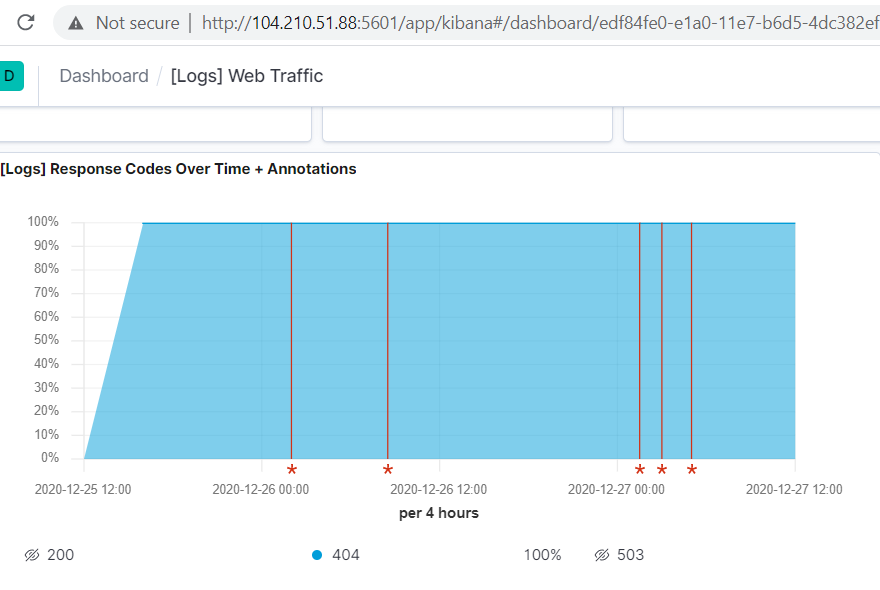
1. In the last 7 days, how many unique visitors were located in India?



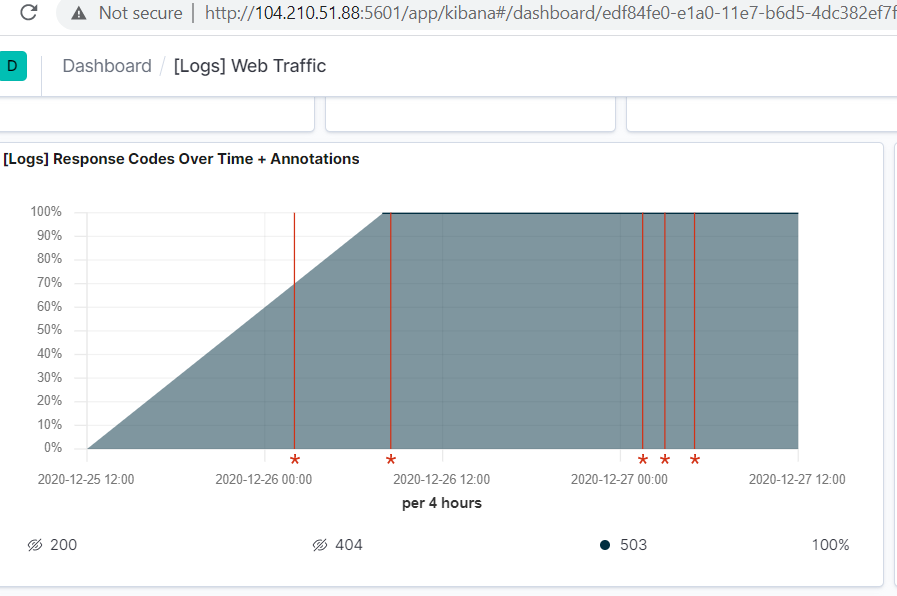
2. In the last 24 hours, of the visitors from china, how many were using Mac OSX?



1. In last 2 days, what percentage of visitors received 404 error? How about 503 errors?

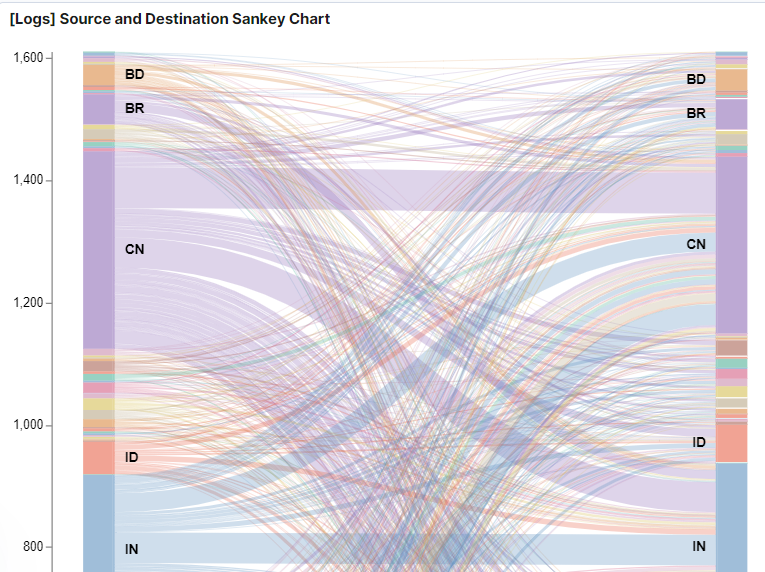


: 503 Err0r

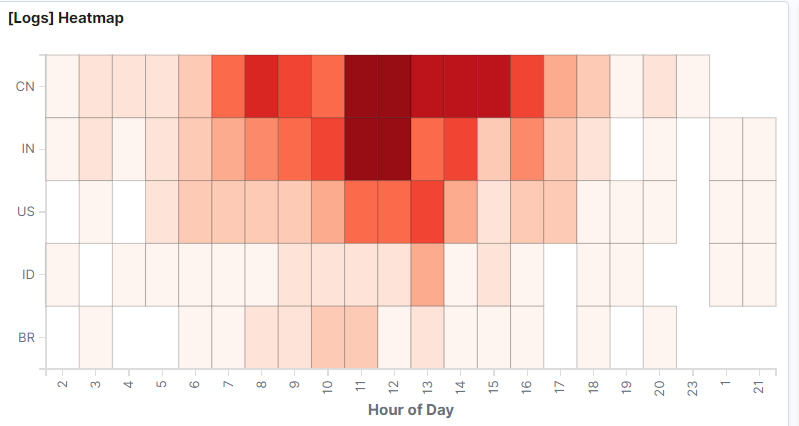


Last 7 days, what country produced the majority of the traffic on the website:

China(CN): 323- (20.1%) China to china (Internal traffic – 4.2%)

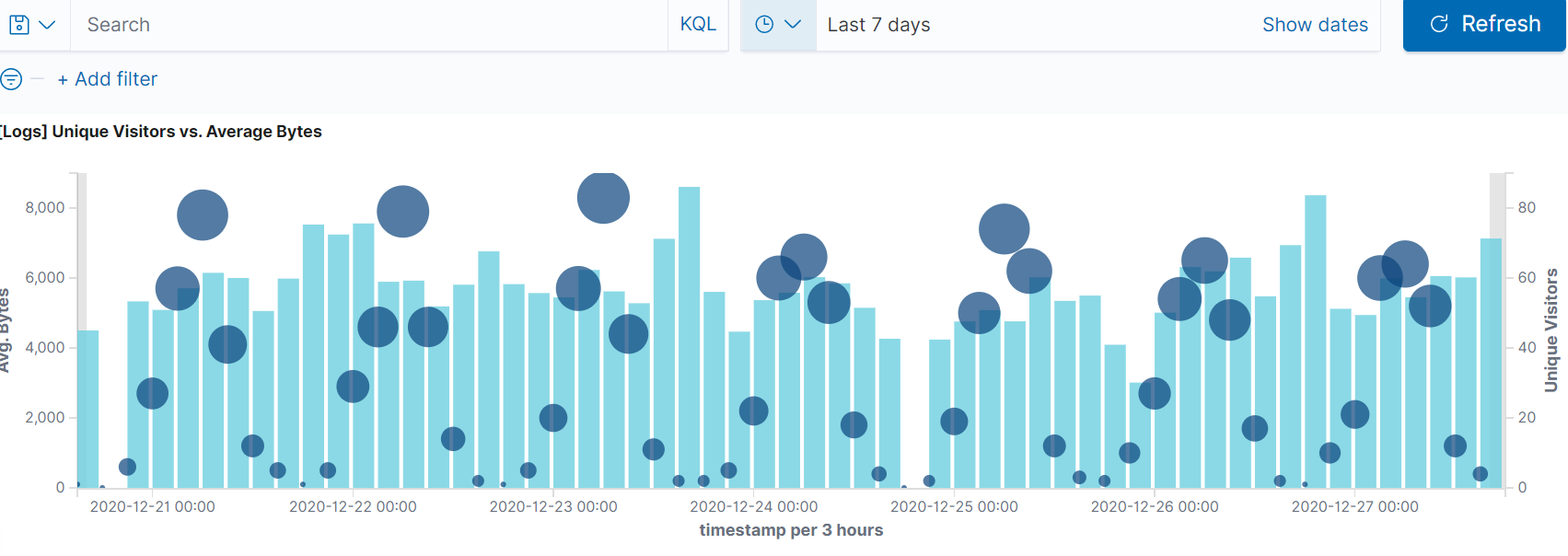


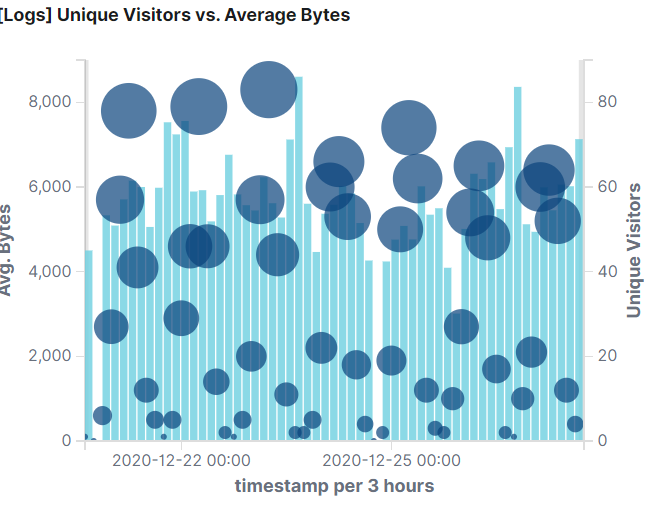
On the traffic that is coming from that country, what time of the day had the highest amount of activity. (Basis on 7 days)

China and India (10:30 am to 12:30 pm) 

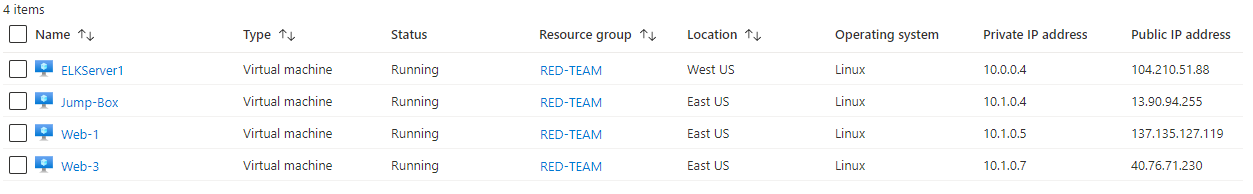
1. Unique visitors Vs average bytes:

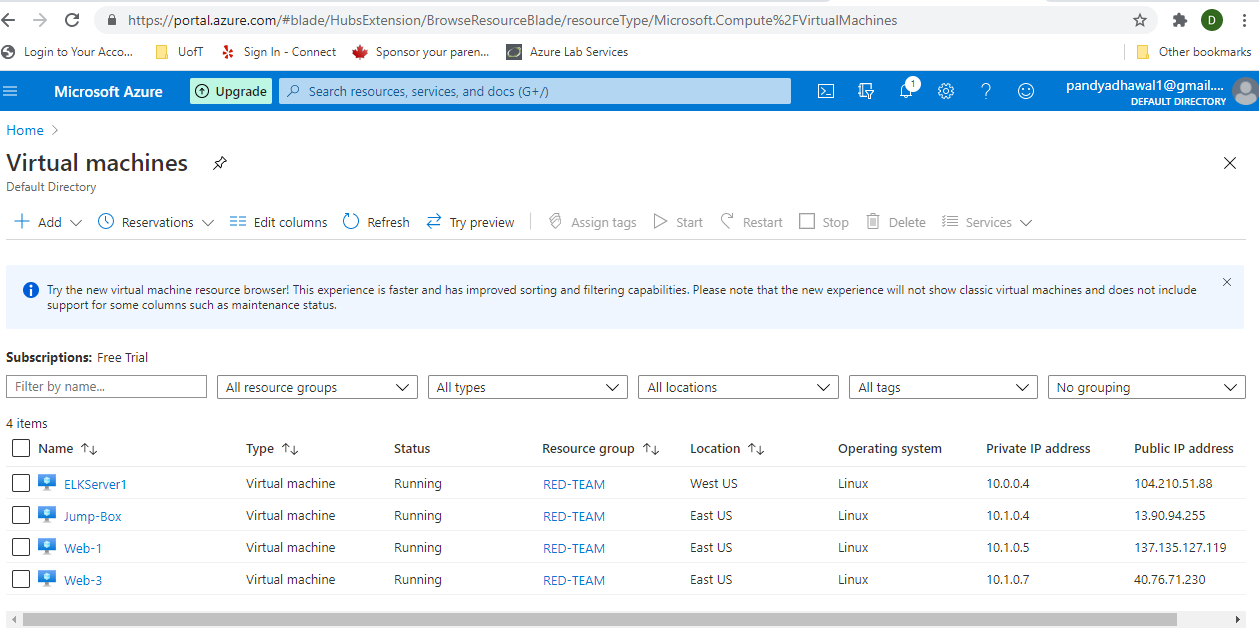
Unique visitors have accessed the more data on every 3 hours times (6-9-12-3-6—9-12) and particularly 6 o clock access more than others times periods.

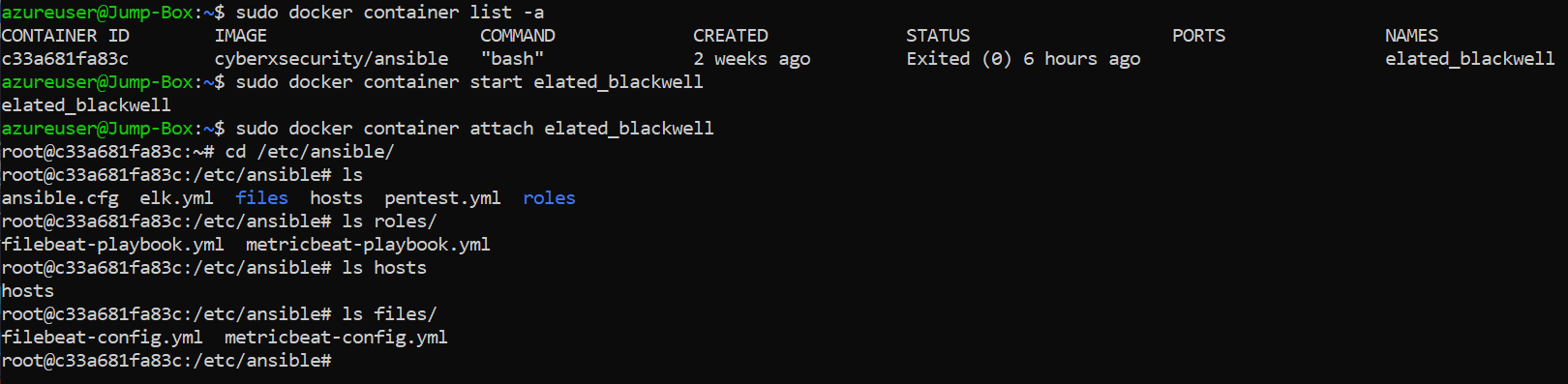




**Azure Cloud Virtual machine details:**







**Thank you for your time,**

**Dhawal Pandya**