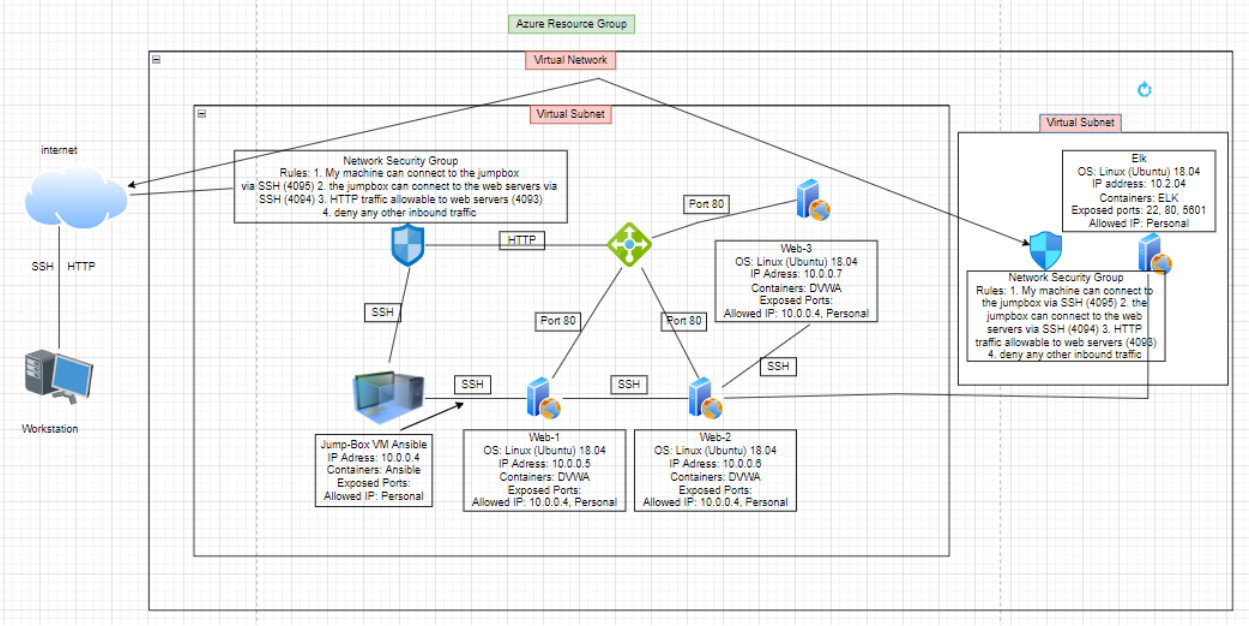
## Automated ELK Stack Deployment

The files in this repository were used to configure the network depicted below.

https://drive.google.com/file/d/1cE3zfSWrr9Dd24QOQv4tUjuhRtUN7era/view?usp=sharing




These files have been tested and used to generate a live ELK deployment on Azure. They can be used to either recreate the entire deployment pictured above. Alternatively, select portions of the .yml file may be used to install only certain pieces of it, such as Filebeat.

  - ELK Install
  - Metricbeat playbook
  - Filebeat playbook

This document contains the following details:
- Description of the Topology
- Access Policies
- ELK Configuration
  - Beats in Use
  - Machines Being Monitored
- How to Use the Ansible Build

### Description of the Topology

The main purpose of this network is to expose a load-balanced and monitored instance of DVWA, the D*mn Vulnerable Web Application.

Load balancing ensures that the application will be highly available, in addition to restricting access to the network.
**Load balancers ensure zero downtime in business-critical applications and can redirect traffic, distributing the incoming data.** Jumpbox allows you to manage multiple systems easily and provides extra layers of protection, allowing it to be an entry point, where you can ssh into vms.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the event logs and system metrics.

- Filbeats watch for specific log files.or directories
- Metricbeat helps gauge how servers are performing by collecting metrics from the system and services running on the server

The configuration details of each machine may be found below.
_Note: Use the [Markdown Table Generator](http://www.tablesgenerator.com/markdown_tables) to add/remove values from the table_.

| Name | Function | IP Address | Operating System |
|---|---|---|---|
| Jump Box | Gateway | 10.0.0.1 | Linux |
| Web 1 | Server | 10.0.0.5 | **Linux** |
| Web 2 | Server | 10.0.0.6 | **Linux** |
| Web 3 | Server | 10.0.0.7 | **Linux** |
| Elk | Log Server | 10.2.0.4 | **Linux** |

### Access Policies

The machines on the internal network are not exposed to the public Internet.

Only the jumpbox provisioner machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:
- Personal IP Address - 107.139.222.132

Machines within the network can only be accessed by the jumpbox provisioner.
- Elk machine had access through personal IP address through port 5601

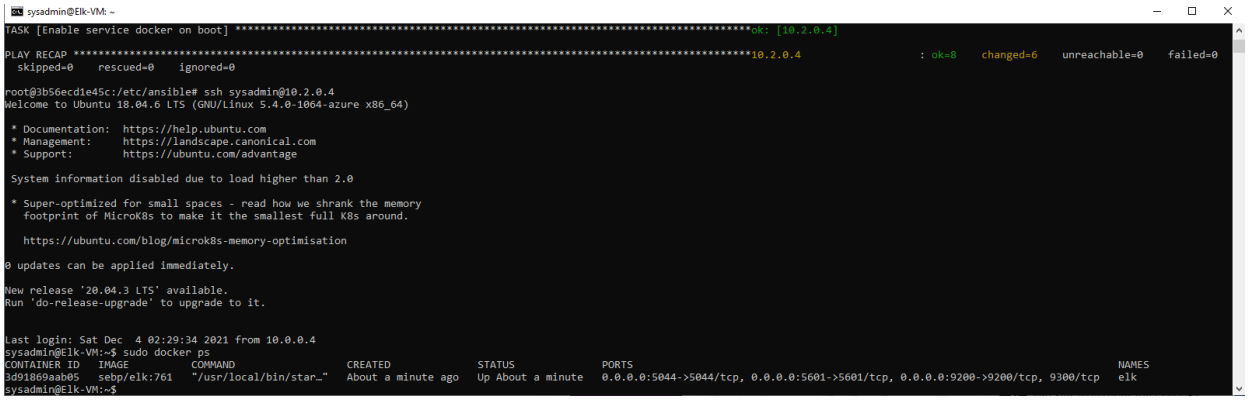
A summary of the access policies in place can be found in the table below.

| **Name** | **Publicly Accessible** | **Allowed IP Addresses** |
|---|---|---|
| Jump Box | Yes | Personal IP |
|Load Balancer| Yes | Open |
|Web 1 | No | 10.0.0.5 |
|Web 2 | No | 10.0.0.6 |
|Web 3 | No | 10.0.0.7 |
|Elk Server | Yes | **Personal IP** |

### Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because it saves time, reduces bug and errors, process was easy to streamline and replicate

The playbook implements the following tasks:
- installed docker.io, pip3 and the docker module
- increased virtual memory to count = 262144
- used sysctl module
- downloaded and launched docker container for elk server




### Target Machines & Beats

This ELK server is configured to monitor the following machines:

- Web 1 (10.0.0.5)
- Web 2 (10.0.0.6)
- Web 3 (10.0.0.7)

We have installed the following Beats on these machines:

- Filebeat and metricbeat

These Beats allow us to collect the following information from each machine:

- Filebeat monitors specific log files and directories, installed on the server through kibana. Shipper for forwarding and centralizing log data. Forwards them to either Elastisearch or Logstash for indexing.
- Metricbeat is also a lightweight shipper installed to collect statistics and metrics on servers. Takes those metrics and statistics and ships to elastisearch or logstash as well

### Using the Playbook

In order to use the playbook, you will need to have an Ansible control node already configured. Assuming you have such a control node provisioned:

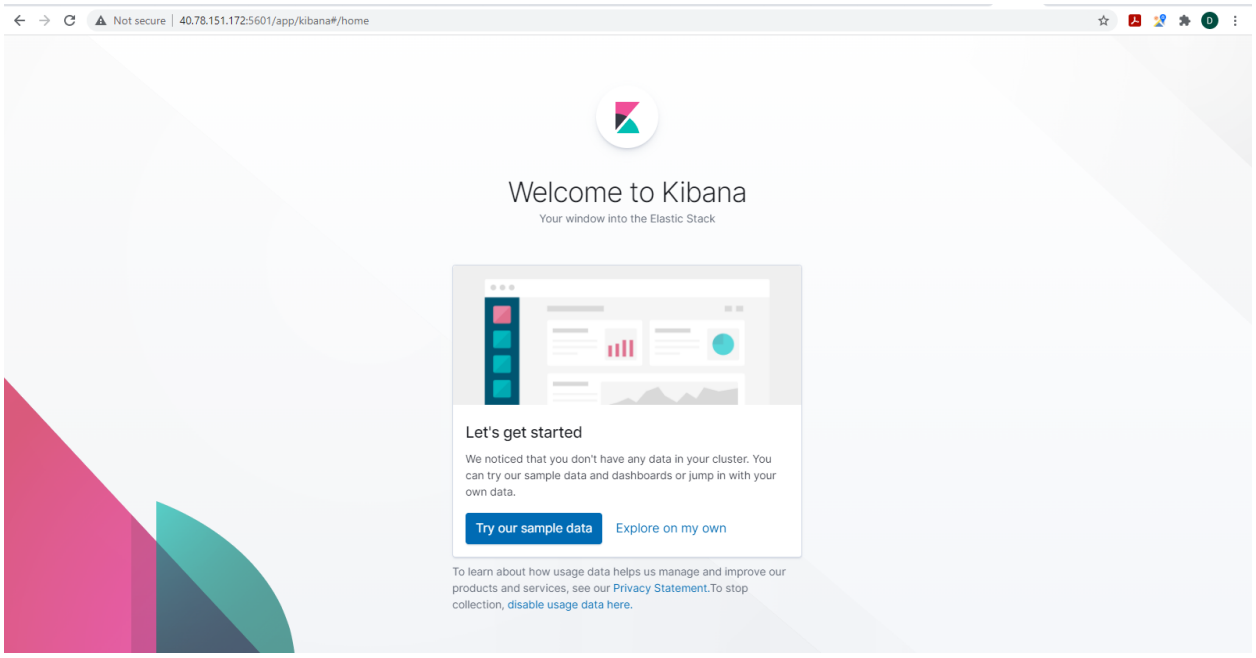
SSH into the control node and follow the steps below:

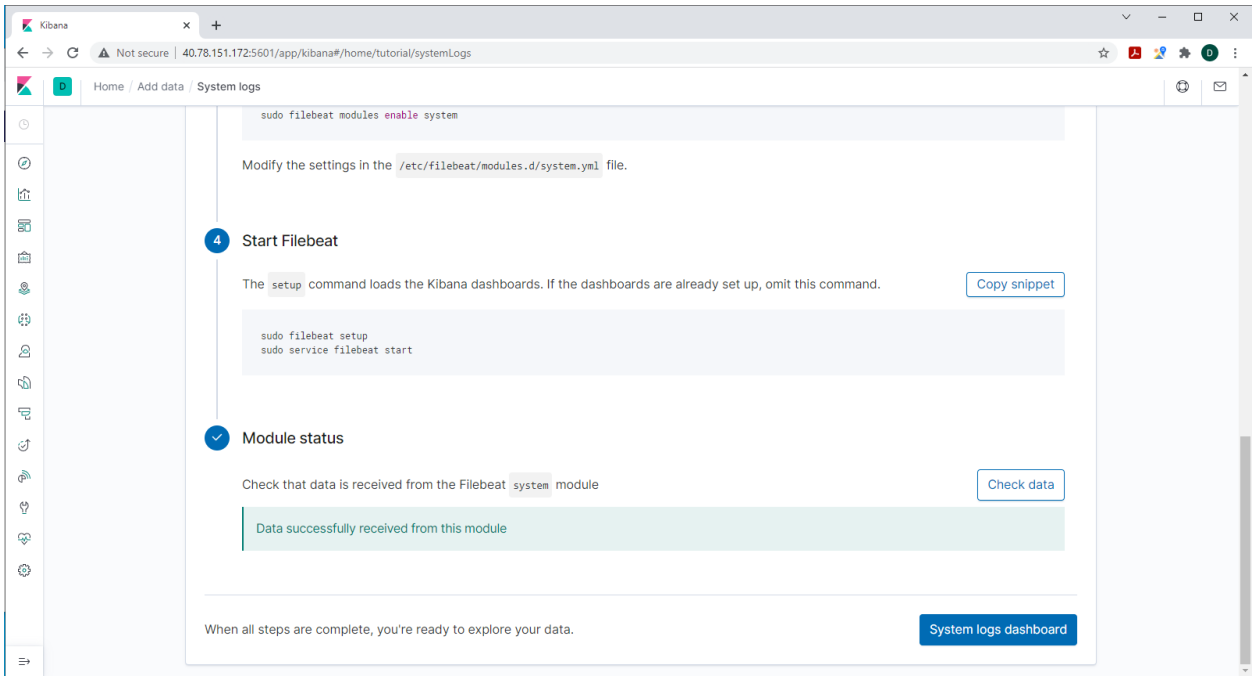
- Copy the configuration file from container to web vm.
- Update the /etc/ansible/hosts file to include IP addresses of elk server and webservers.

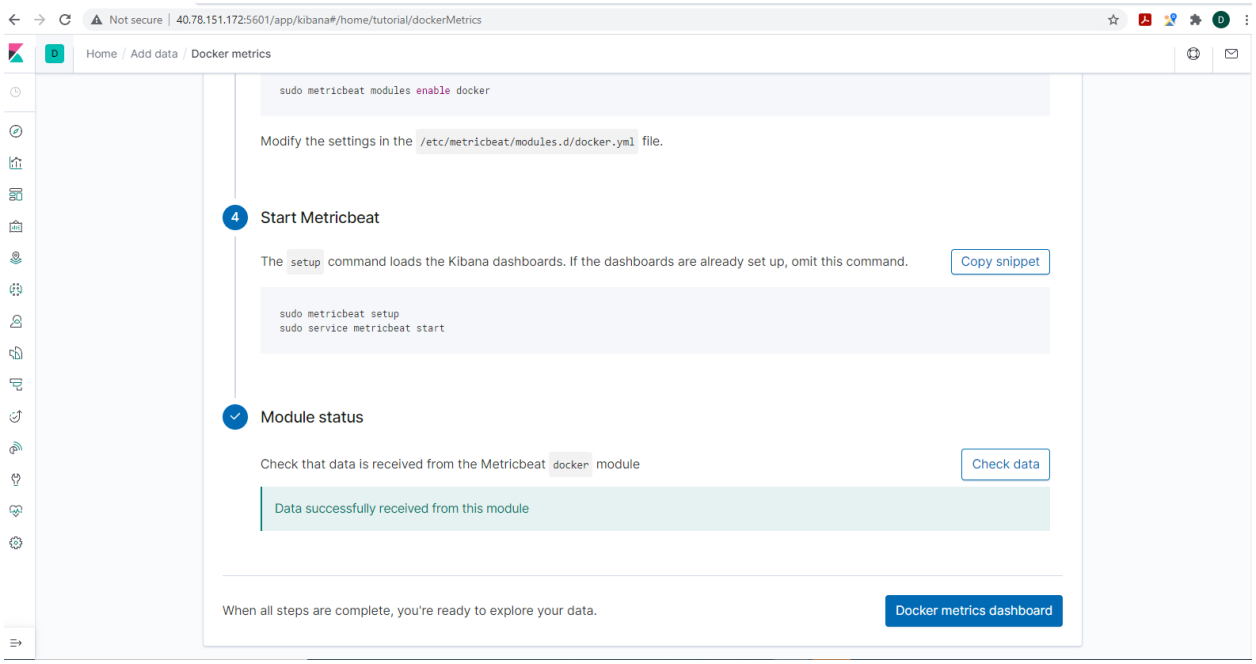
- Run the playbook, and navigate to http://40.78.151.172:5601/app/kibana to check that the installation worked as expected.

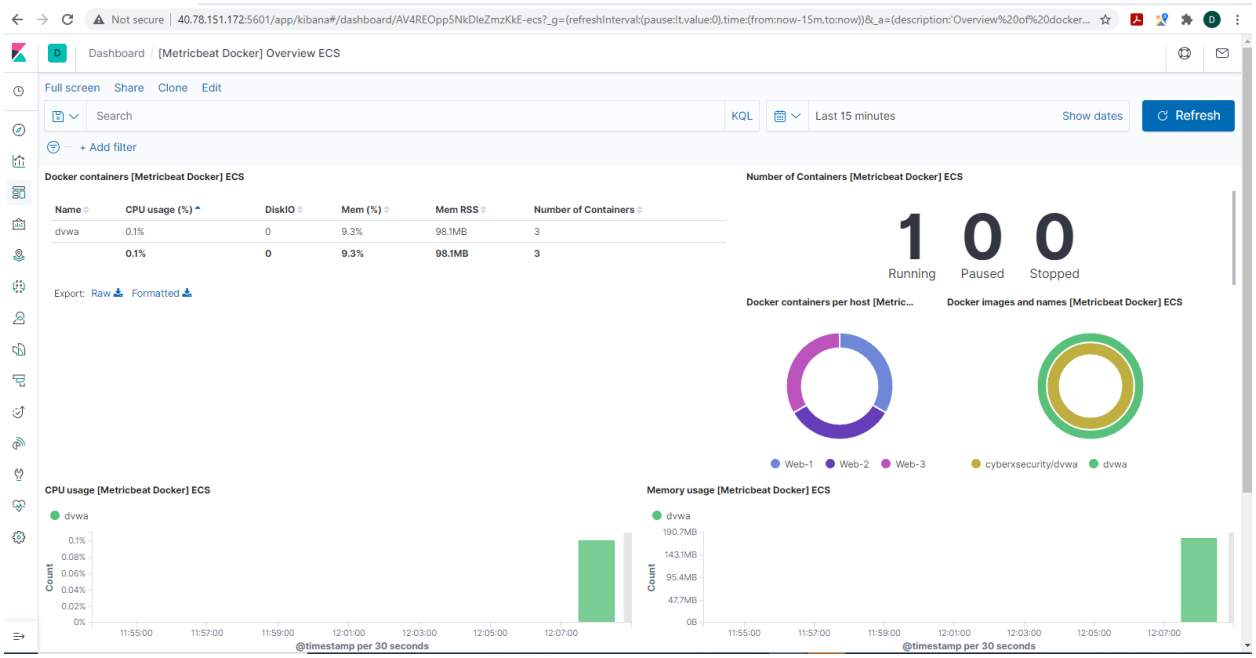
- _Which file is the playbook? Filebeat configuration
Where do you copy it? /etc/ansible/files/filebeat-config.yml to /etc/filebeat/filebeat.yml
- _Which file do you update to make Ansible run the playbook on a specific machine? Update filebeat-config.yml
How do I specify which machine to install the ELK server on versus which to install Filebeat on? By updating host files with ip addresses and letting know which group to run ansible on
- _Which URL do you navigate to in order to check that the ELK server is running? http://40.78.151.172:5601/app/kibana

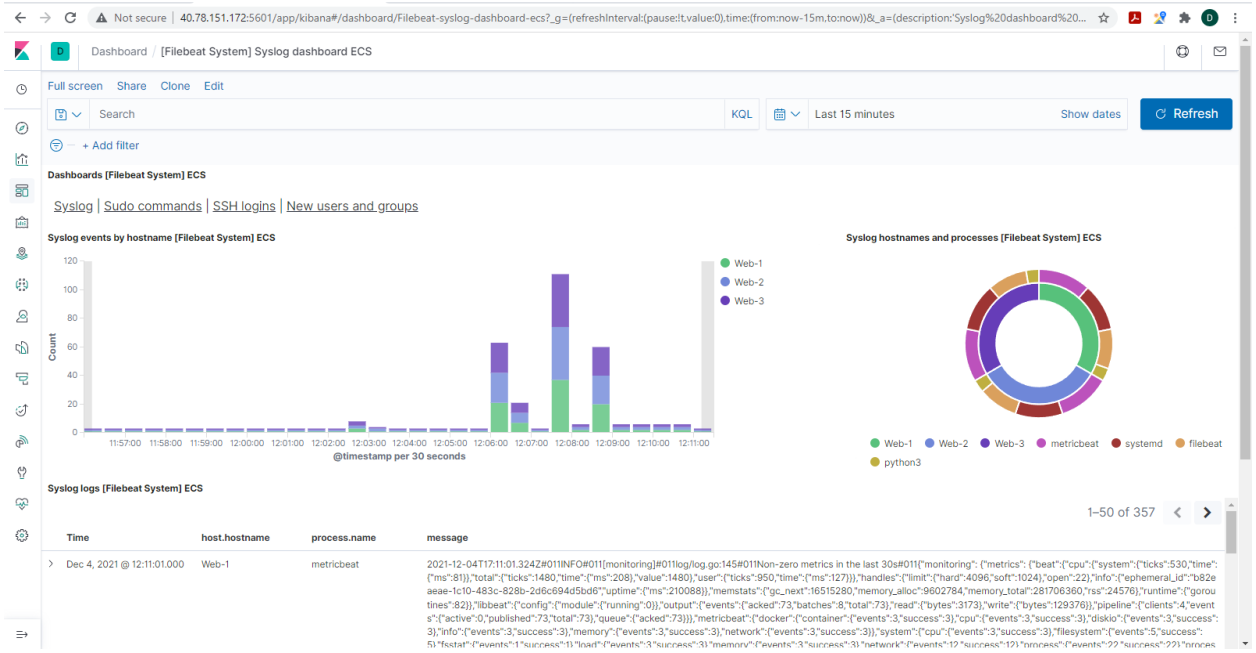
No bonus, bu twanted to add all the screenshots we were told to take while doing the project. See below.




Kibana
Not secure | 40.78.151.172:5601/app/kibana#/home/tutorial/systemLogs
Home / Add data / System logs
sudo filebeat modules enable system
Modify the settings in the /etc/filebeat/modules.d/system.yml file.
4 Start Filebeat
The setup command loads the Kibana dashboards. If the dashboards are already set up, omit this command.
Copy snippet
sudo filebeat setup
sudo service filebeat start
Module status
Check that data is received from the Filebeat system module
Check data
Data successfully received from this module
When all steps are complete, you're ready to explore your data.
System logs dashboard


Not secure | 40.78.151.172:5601/app/kibana#/home/tutorial/dockerMetrics
Home / Add data / Docker metrics
sudo metricbeat modules enable docker
Modify the settings in the /etc/metricbeat/modules.d/docker.yml file.
4 Start Metricbeat
The setup command loads the Kibana dashboards. If the dashboards are already set up, omit this command.
Copy snippet
sudo metricbeat setup
sudo service metricbeat start
Module status
Check that data is received from the Metricbeat docker module
Check data
Data successfully received from this module
When all steps are complete, you're ready to explore your data.
Docker metrics dashboard


Not secure | 40.78.151.172:5601/app/kibana#/dashboard/AV4REOpp5NkDleZmzKkE-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(description:'Overview%20of%20docker...
Dashboard / [Metricbeat Docker] Overview ECS
Full screen Share Clone Edit
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
Docker containers [Metricbeat Docker] ECS
Name
CPU usage (%)
DiskIO
Mem (%)
Mem RSS
Number of Containers
dvwa 0.1% 0 9.3% 98.1MB 3
0.1% 0 9.3% 98.1MB 3
Export: Raw Formatted
Number of Containers [Metricbeat Docker] ECS
1 Running
0 Paused
0 Stopped
Docker containers per host [Metric...
Web-1 Web-2 Web-3
Docker images and names [Metricbeat Docker] ECS
cyberxsecurity/dvwa dvwa
CPU usage [Metricbeat Docker] ECS
dvwa
Count
@timestamp per 30 seconds
Memory usage [Metricbeat Docker] ECS
dvwa
190.7MB
143.1MB
95.4MB
47.7MB
0B
Count
@timestamp per 30 seconds


Not secure | 40.78.151.172:5601/app/kibana#/dashboard/Filebeat-syslog-dashboard-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(description:'Syslog%20dashboard%20...
Dashboard / [Filebeat System] Syslog dashboard ECS
Full screen Share Clone Edit
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
Dashboards [Filebeat System] ECS
Syslog | Sudo commands | SSH logins | New users and groups
Syslog events by hostname [Filebeat System] ECS
Web-1
Web-2
Web-3
Count
@timestamp per 30 seconds
Syslog hostnames and processes [Filebeat System] ECS
Web-1 Web-2 Web-3 metricbeat systemd filebeat python3
Syslog logs [Filebeat System] ECS
1–50 of 357
Time
host.hostname
process.name
message
Dec 4, 2021 @ 12:11:01.000
Web-1
metricbeat