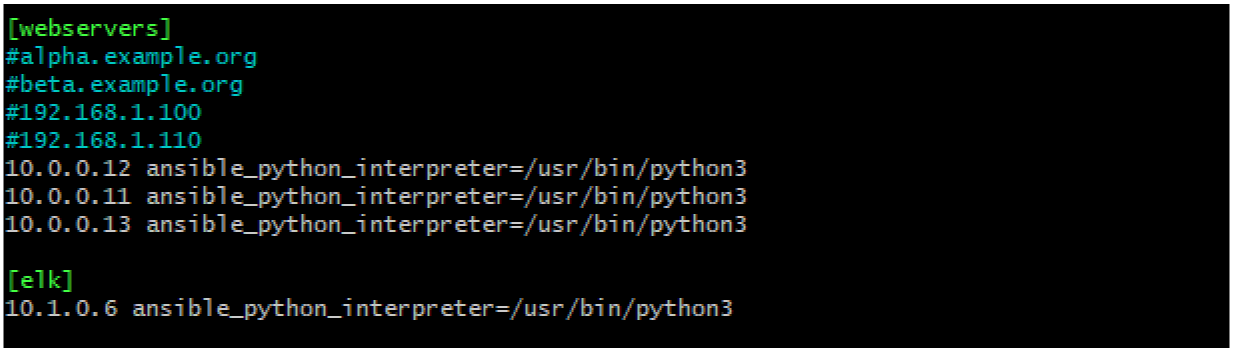
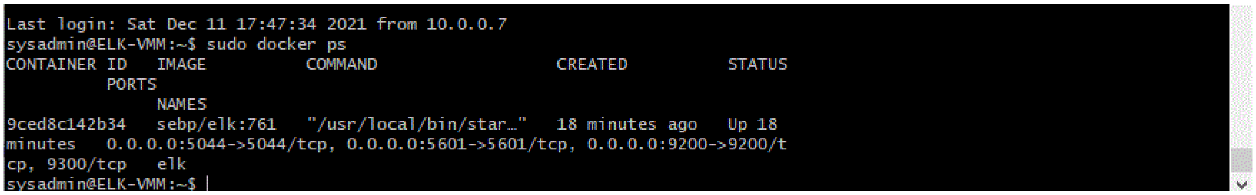
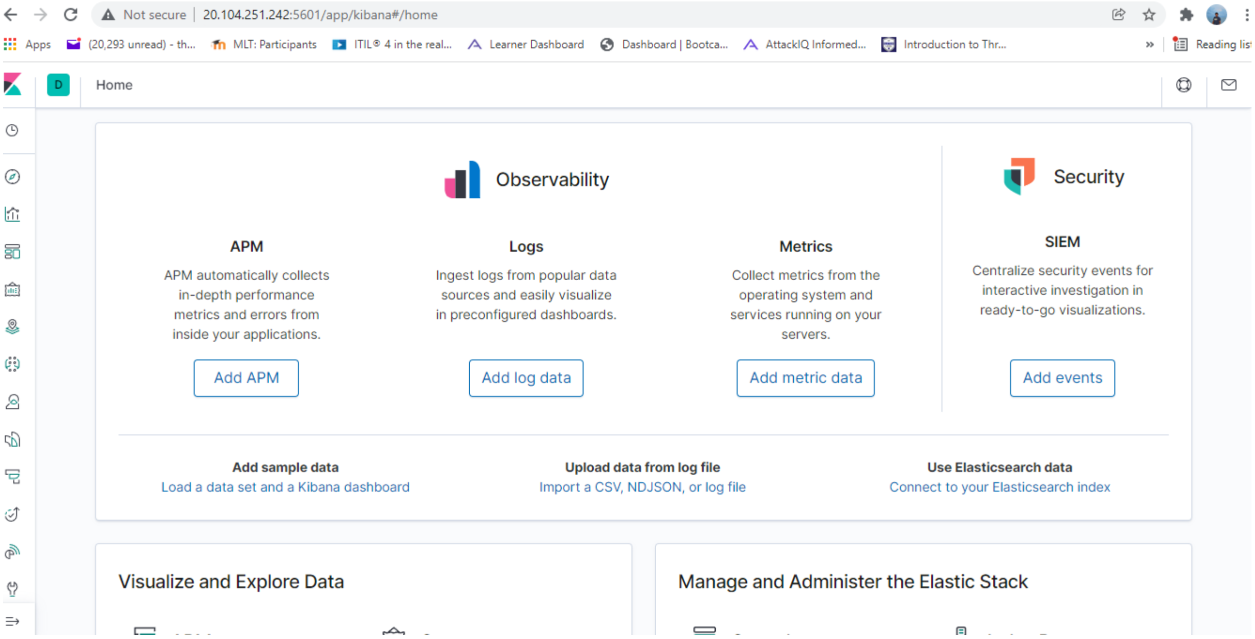


```
[webservers]
#alpha.example.org
#beta.example.org
#192.168.1.100
#192.168.1.110
10.0.0.12 ansible_python_interpreter=/usr/bin/python3
10.0.0.11 ansible_python_interpreter=/usr/bin/python3
10.0.0.13 ansible_python_interpreter=/usr/bin/python3

[elk]
10.1.0.6 ansible_python_interpreter=/usr/bin/python3
```



```
Last login: Sat Dec 11 17:47:34 2021 from 10.0.0.7
sysadmin@ELK-VMM:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED          STATUS
          PORTS
               NAMES
9ced8c142b34   sebp/elk:761   "/usr/local/bin/star…"   18 minutes ago   Up 18
minutes   0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/t
cp, 9300/tcp   elk
sysadmin@ELK-VMM:~$ 
```



Observability

Security

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

Add metric data

SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

Add events

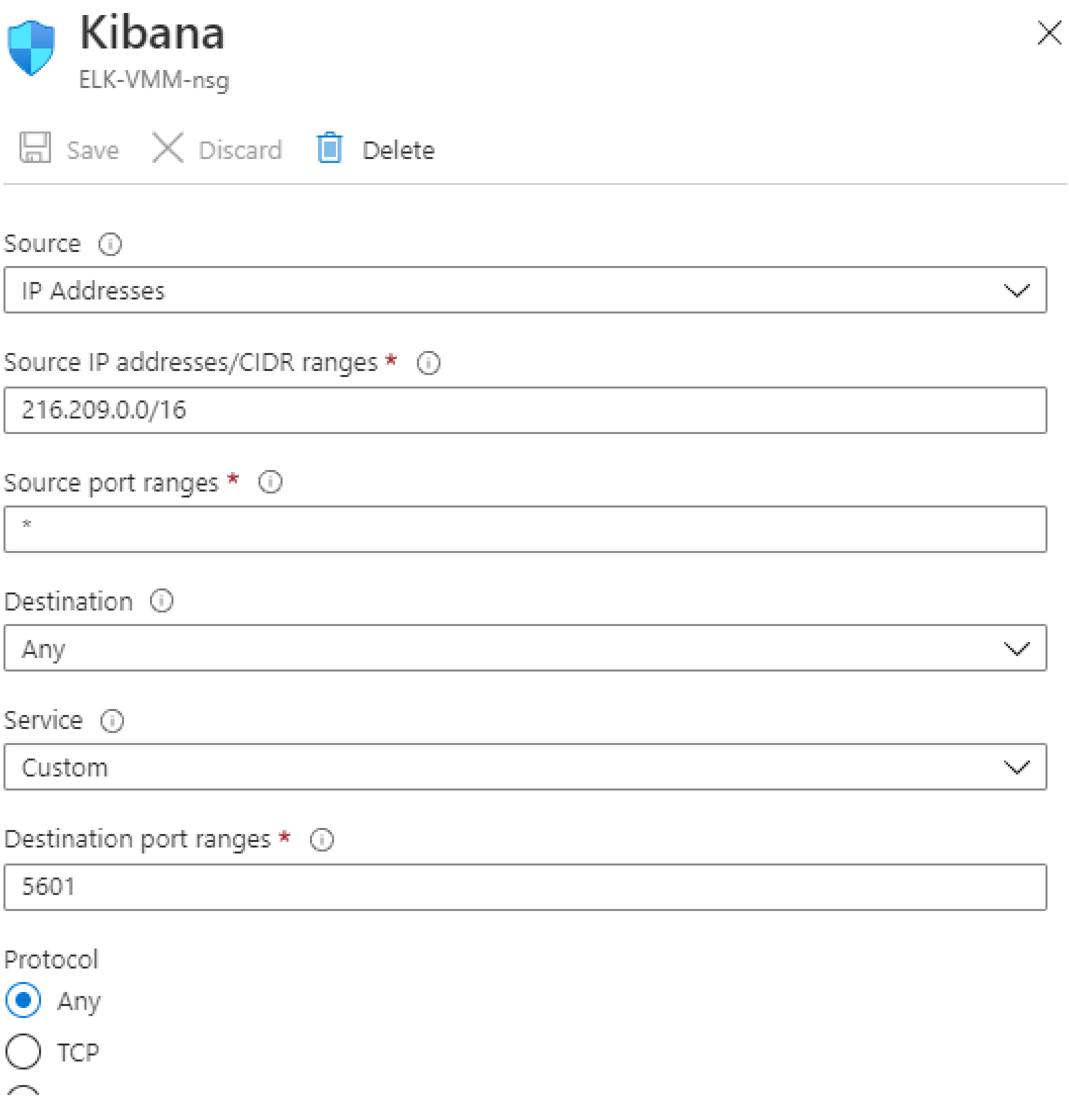
Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

Manage and Administer the Elastic Stack



Kibana

ELK-VMM-nsg

Source: IP Addresses

Source IP addresses/CIDR ranges *: 216.209.0.0/16

Source port ranges *: *

Destination: Any

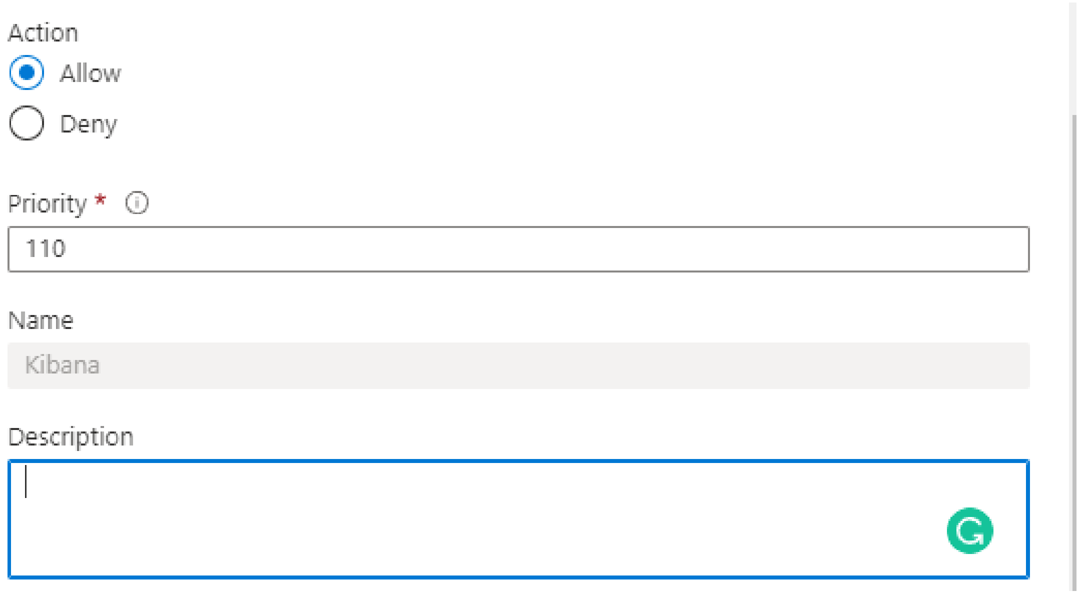
Service: Custom

Destination port ranges *: 5601

Protocol

● Any

○ TCP



Action

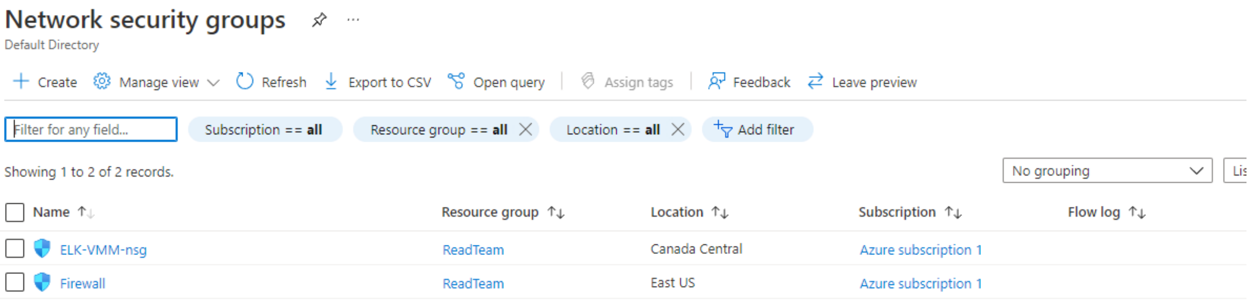
● Allow

○ Deny

Priority *: 110

Name: Kibana

Description:



Network security groups

Default Directory

Filter for any field...

Subscription == **all**

Resource group == **all**

Location == **all**

Showing 1 to 2 of 2 records.

No grouping

□	Name	Resource group	Location	Subscription	Flow log
□	ELK-VMM-nsg	ReadTeam	Canada Central	Azure subscription 1	
□	Firewall	ReadTeam	East US	Azure subscription 1	