ELK Stack, Filebeat, and Metricbeat

Setup Walkthrough

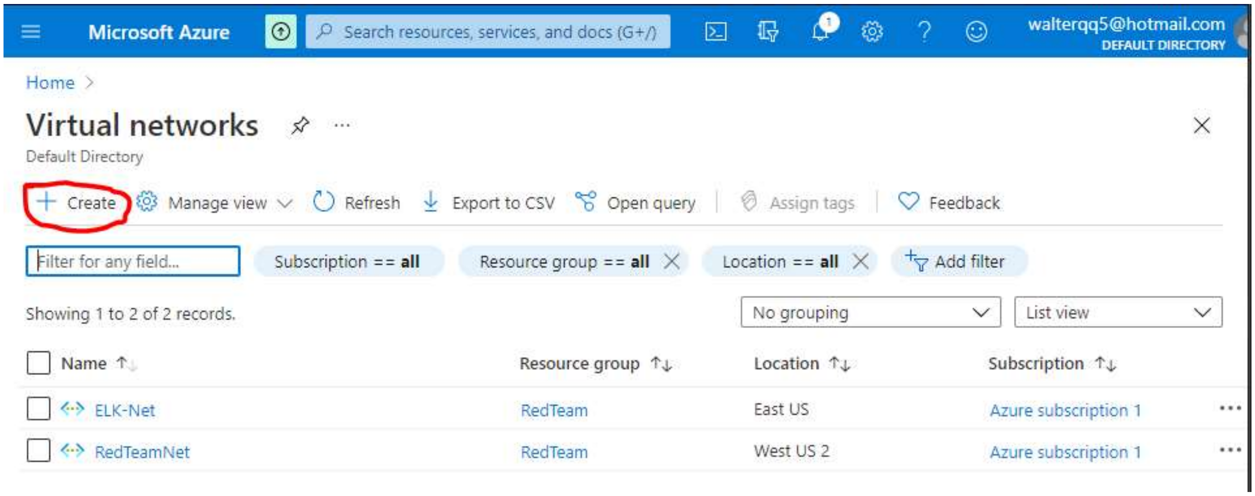
By: Walter T. Pan

Contents

Create a new virtual network for ELK Stack.

Navigate the Azure portal/Virtual Networks

Select create.



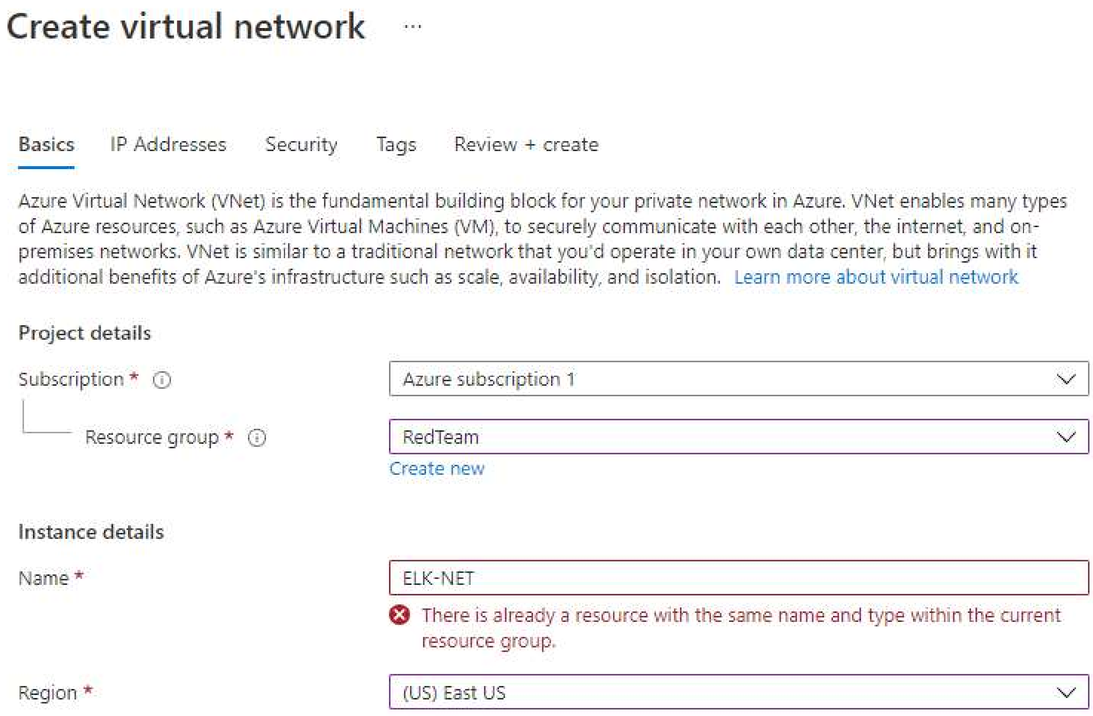
Virtual networks

Default Directory

Showing 1 to 2 of 2 records.

Name	Resource group	Location	Subscription
ELK-Net	RedTeam	East US	Azure subscription 1
RedTeamNet	RedTeam	West US 2	Azure subscription 1

Input the settings above and leave the rest of the settings at default.



Create virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network

Project details

Subscription * : Azure subscription 1

Resource group * : RedTeam

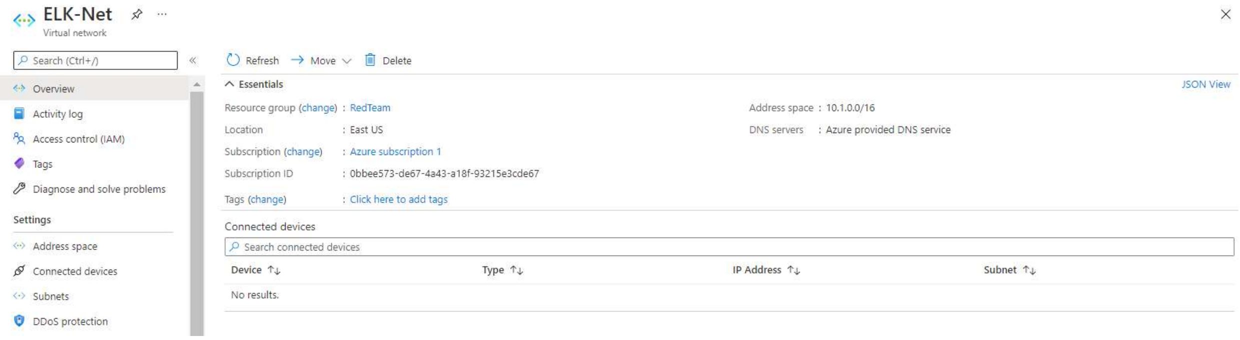
Create new

Instance details

Name * : ELK-NET

There is already a resource with the same name and type within the current resource group.

Region * : (US) East US



Essentials

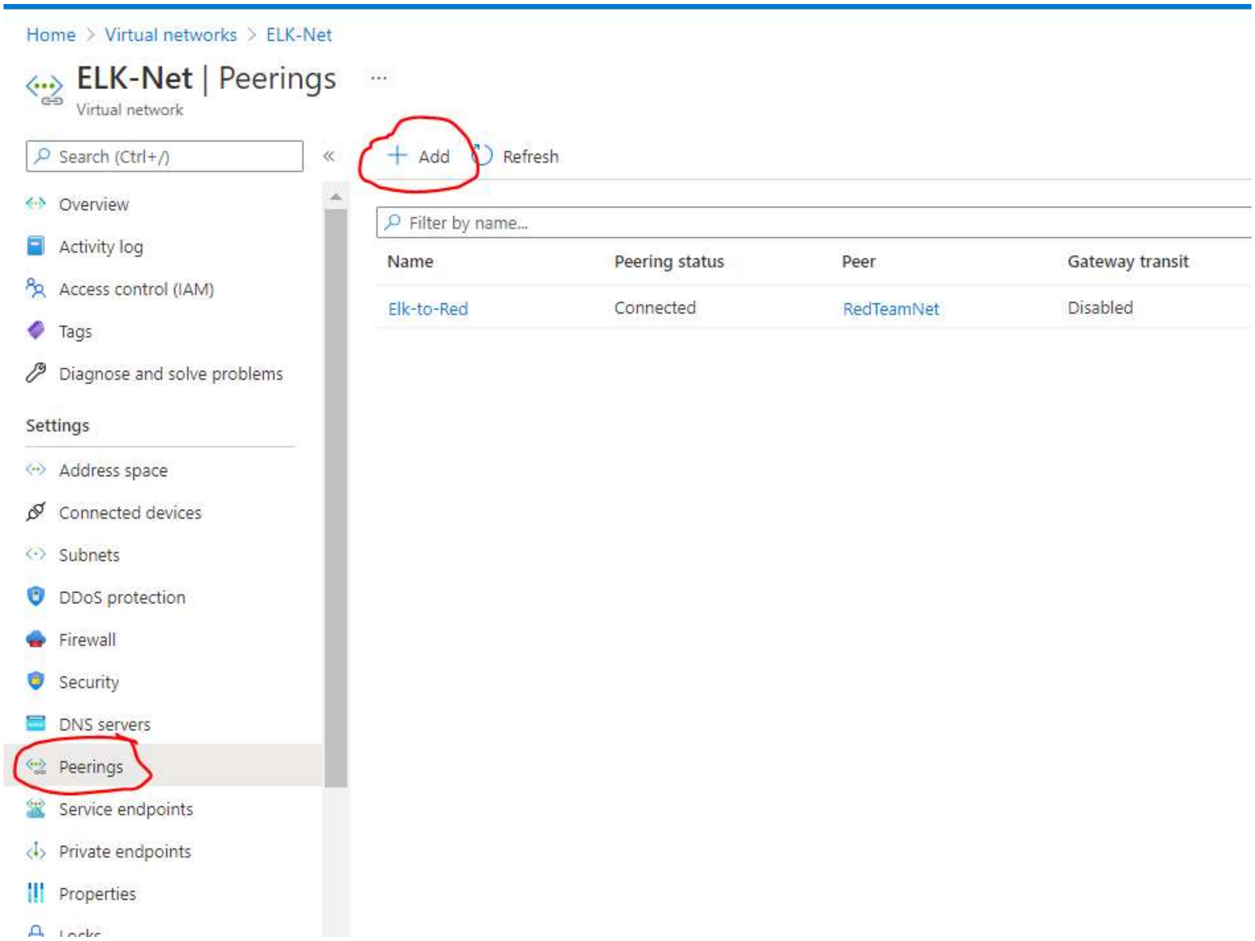
Resource group (change) : RedTeam
Location : East US
Subscription (change) : Azure subscription 1
Subscription ID : 0bbee573-de67-4a43-a18f-93215e3cde67
Tags (change) : Click here to add tags

Address space : 10.1.0.0/16
DNS servers : Azure provided DNS service

Connected devices

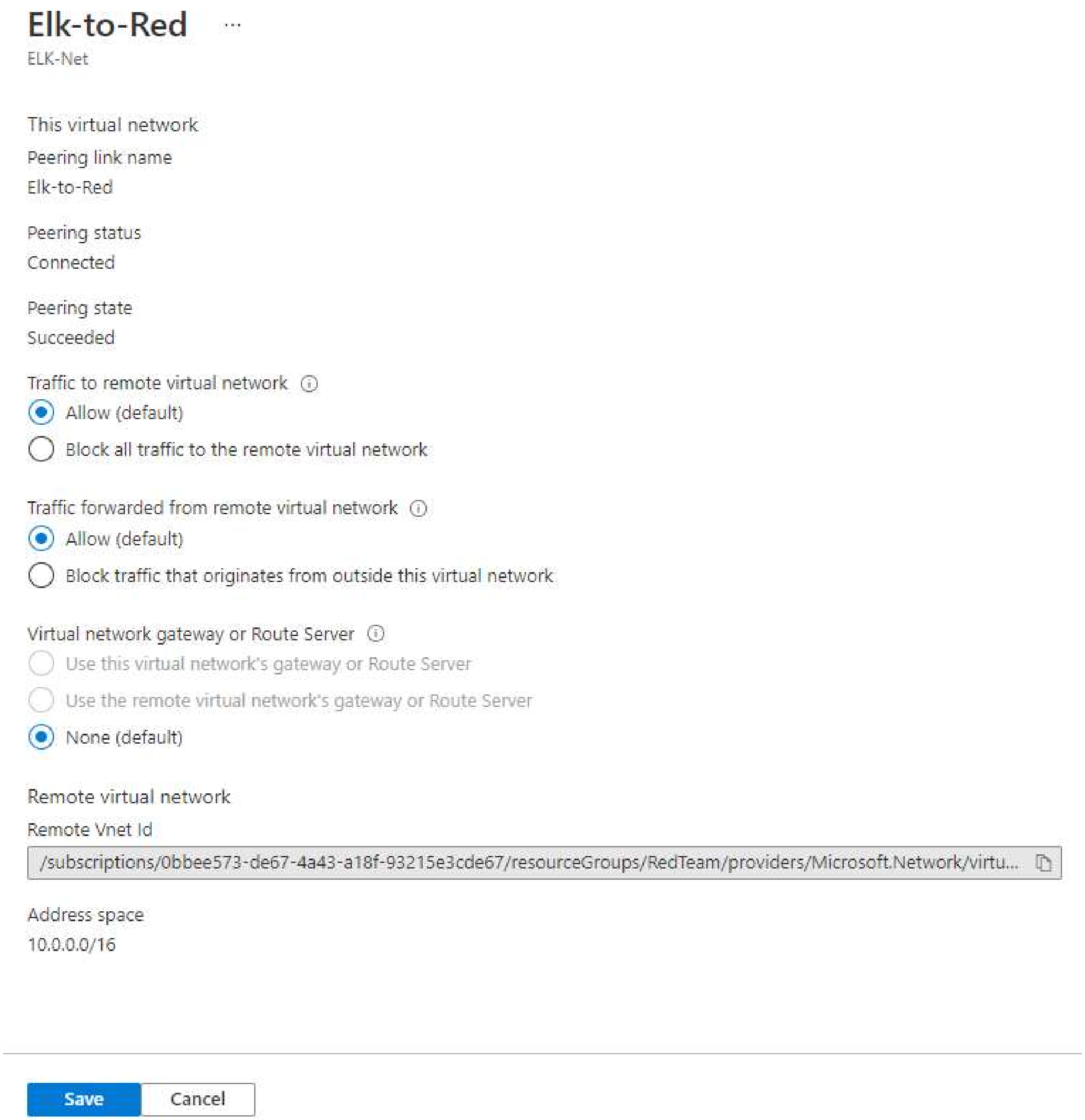
Device ↑↓	Type ↑↓	IP Address ↑↓	Subnet ↑↓
No results.			

Create a Peer connection between the virtual networks, by going to peering and adding a new peering.



Name	Peering status	Peer	Gateway transit
Elk-to-Red	Connected	RedTeamNet	Disabled

Select the following settings.



Elk-to-Red ···

ELK-Net

This virtual network

Peering link name

Elk-to-Red

Peering status

Connected

Peering state

Succeeded

Traffic to remote virtual network ⓘ

● Allow (default)

○ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

● Allow (default)

○ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

○ Use this virtual network's gateway or Route Server

○ Use the remote virtual network's gateway or Route Server

● None (default)

Remote virtual network

Remote Vnet Id

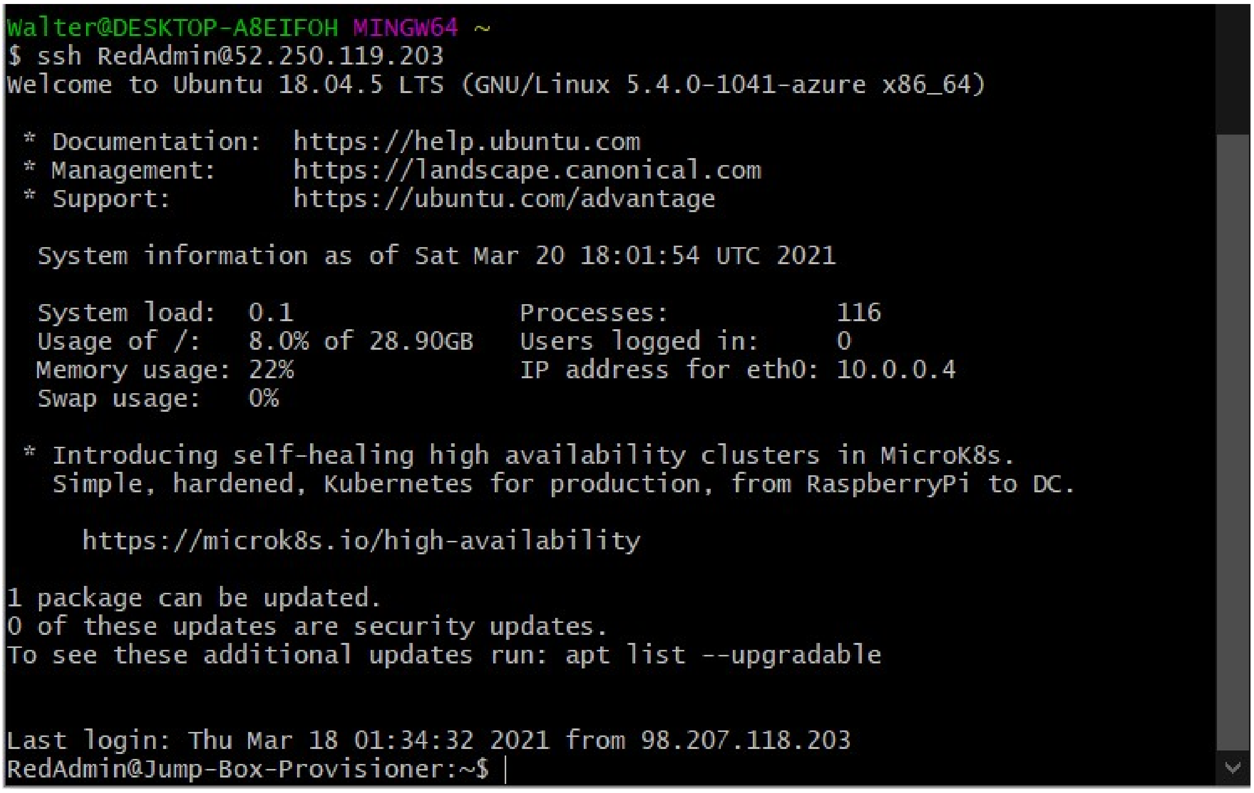
/subscriptions/0bbee573-de67-4a43-a18f-93215e3cde67/resourceGroups/RedTeam/providers/Microsoft.Network/virtu...

Address space

10.0.0.0/16

Set up ELK-Server VM

Navigate to GitBash and SSH into Jump Box.



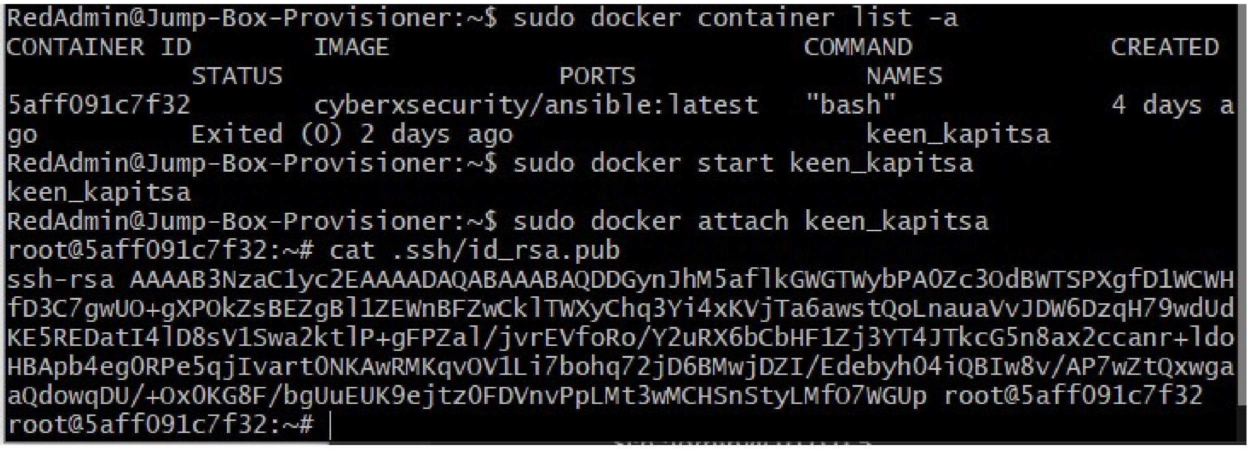
```
Walter@DESKTOP-A8EIFOH MINGW64 ~
$ ssh RedAdmin@52.250.119.203
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Mar 20 18:01:54 UTC 2021

  System load:  0.1               Processes:           116
  Usage of /:   8.0% of 28.90GB   Users logged in:     0
  Memory usage: 22%               IP address for eth0: 10.0.0.4
  Swap usage:   0%

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

1 package can be updated.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


Last login: Thu Mar 18 01:34:32 2021 from 98.207.118.203
RedAdmin@Jump-Box-Provisioner:~$ |
```

Check and locate an Ansible container.

Start the container.

Connect to the container.

Copy the SSH key from the Ansible container on your Jump Box.

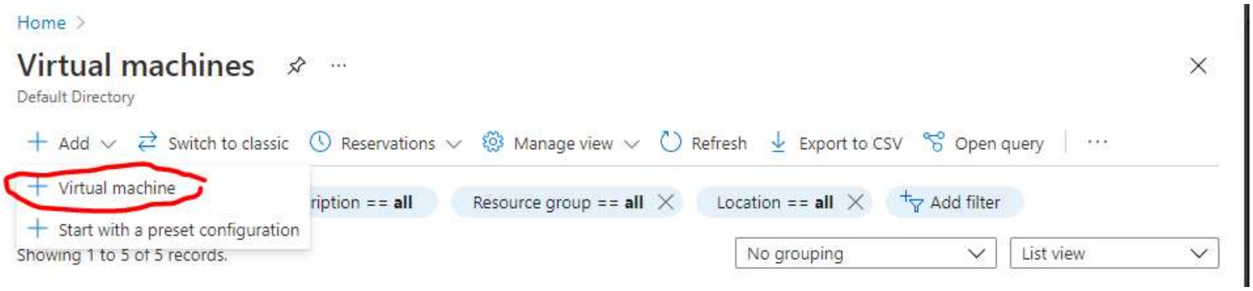


```
RedAdmin@Jump-Box-Provisioner:~$ sudo docker container list -a
CONTAINER ID        IMAGE                          COMMAND             CREATED
            STATUS                    PORTS               NAMES
5aff091c7f32        cyberxsecurity/ansible:latest   "bash"             4 days a
go          Exited (0) 2 days ago                         keen_kapitsa
RedAdmin@Jump-Box-Provisioner:~$ sudo docker start keen_kapitsa
keen_kapitsa
RedAdmin@Jump-Box-Provisioner:~$ sudo docker attach keen_kapitsa
root@5aff091c7f32:~# cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDGynJhM5aflkGWGTWybPA0Zc3OdBWTSPXgfD1WCWH
fD3C7gwUO+gXPOkZsBEZgBl1ZEWnBFZwCklTWXyChq3Yi4xKVjTa6awstQoLnauaVvJDW6DzqH79wdUd
KE5REDatI4lD8sV1Swa2ktlP+gFPZal/jvrEVfoRo/Y2uRX6bCbHF1Zj3YT4JTkcG5n8ax2ccanr+ldo
HBApb4eg0RPe5qjIvart0NKAwRMKqvOV1Li7bohq72jD6BMwjDZI/Edebyh04iQBIw8v/AP7wZtQxwga
aQdowqDU/+0x0KG8F/bgUuEUK9ejtz0FDVnvPpLMt3wMCHSnStyLMf07WGUp root@5aff091c7f32
root@5aff091c7f32:~# |
```

Create a new ELK-VM

Navigate to virtual machines.

Add new virtual machine.



ription == **all**

Resource group == **all**

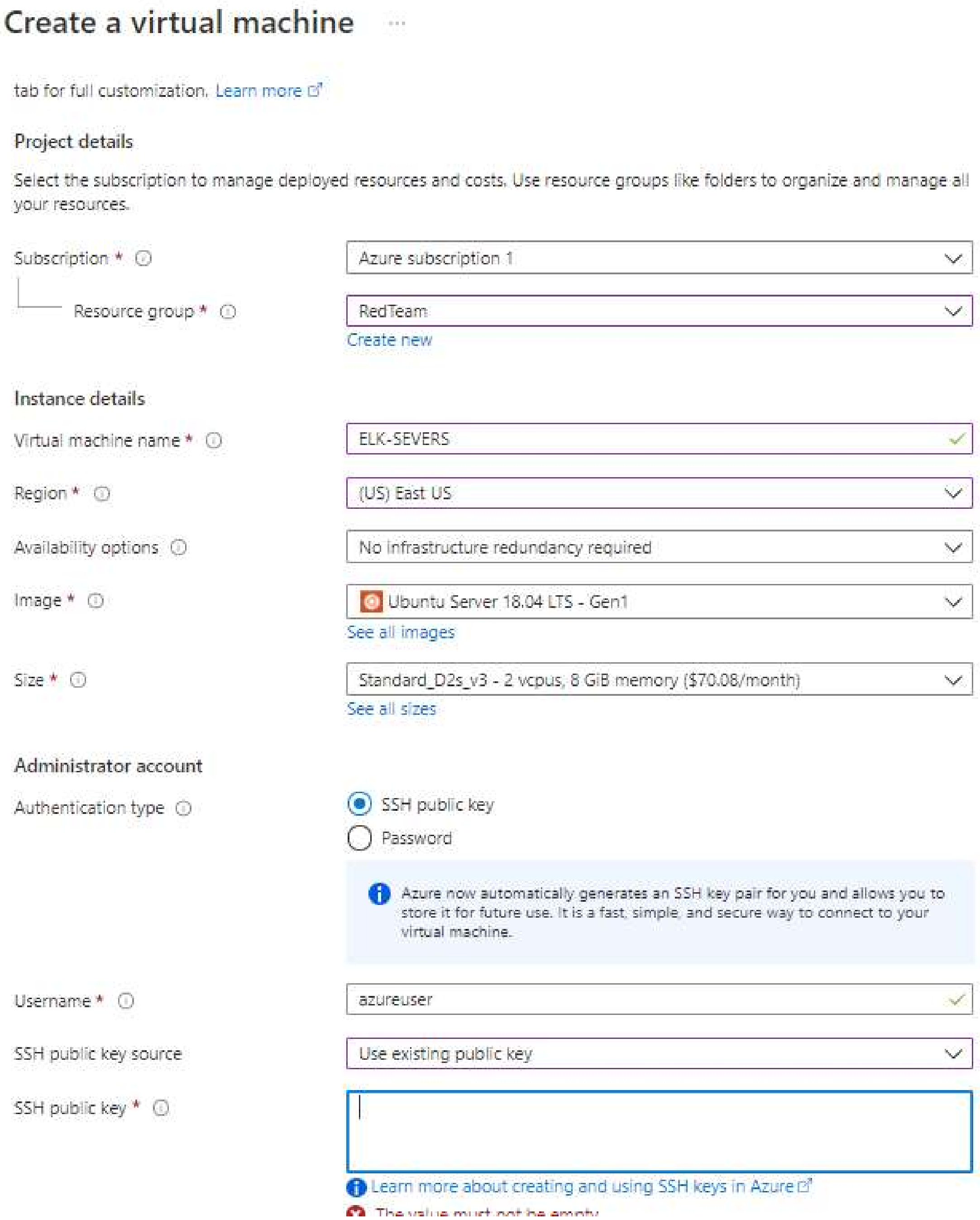
Location == **all**

Showing 1 to 5 of 5 records.

Memory: At least 4 GB of RAM

Public IP address

Add the ELK VM to a new security group.



Create a virtual machine

tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Azure subscription 1
Resource group *	RedTeam Create new

Instance details

Virtual machine name *	ELK-SEVERS ✓
Region *	(US) East US
Availability options	No infrastructure redundancy required
Image *	Ubuntu Server 18.04 LTS - Gen1 See all images
Size *	Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($70.08/month) See all sizes

Administrator account

Authentication type

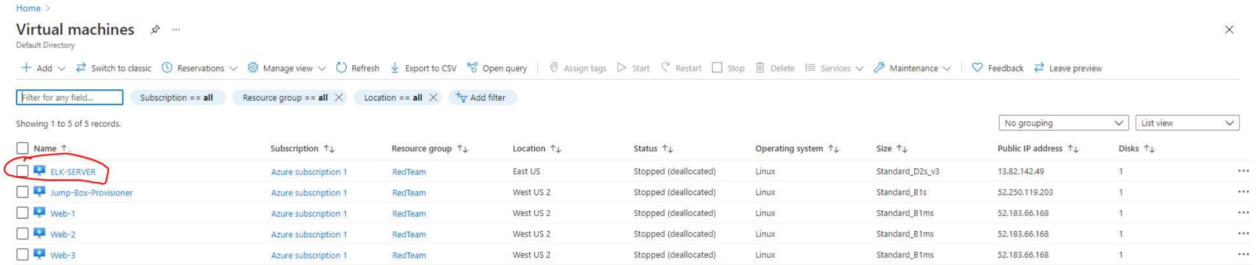
● SSH public key
○ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username *	azureuser ✓
SSH public key source	Use existing public key
SSH public key *	

Learn more about creating and using SSH keys in Azure

The value must not be empty



Home >

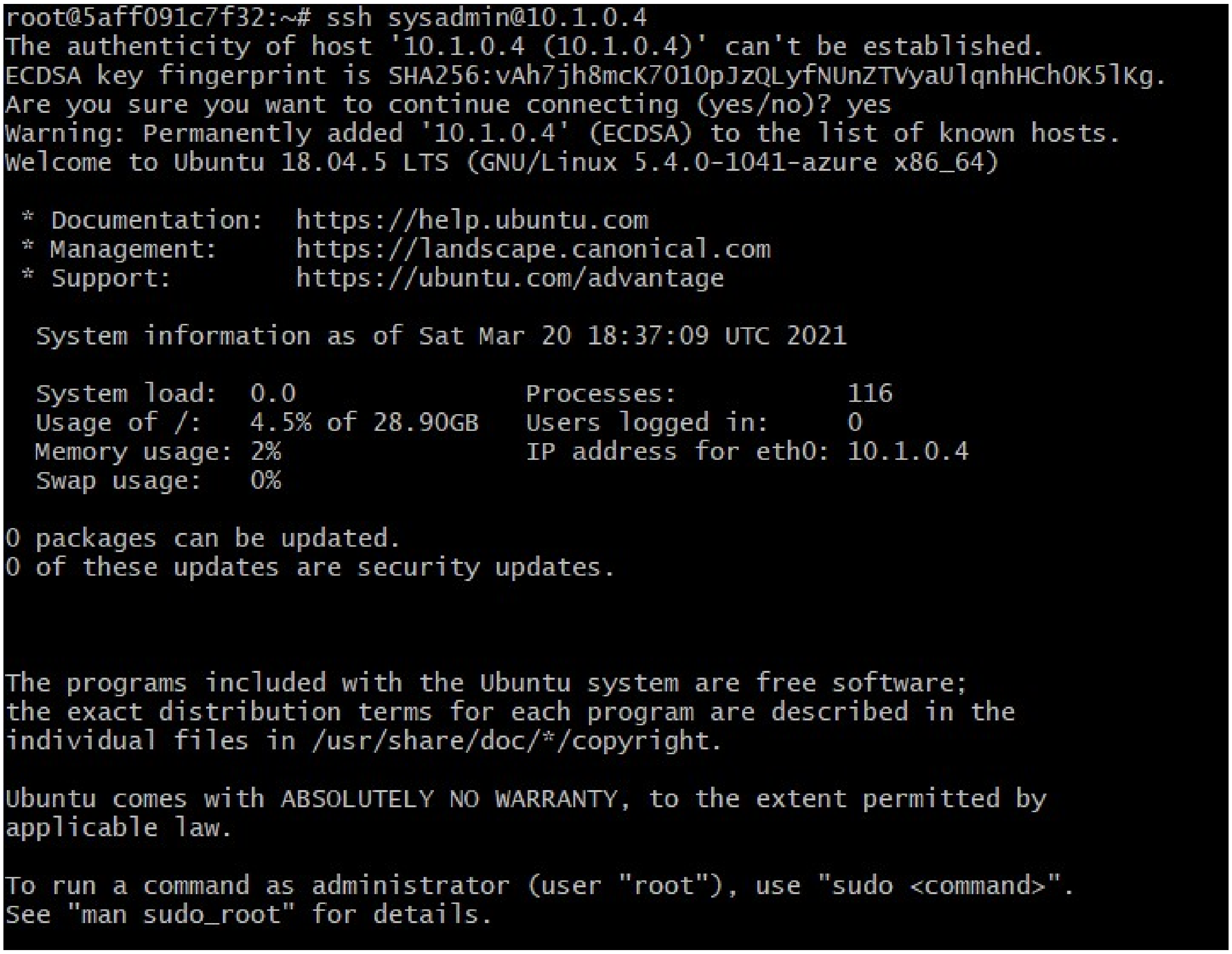
Virtual machines

Default Directory

Showing 1 to 5 of 5 records.

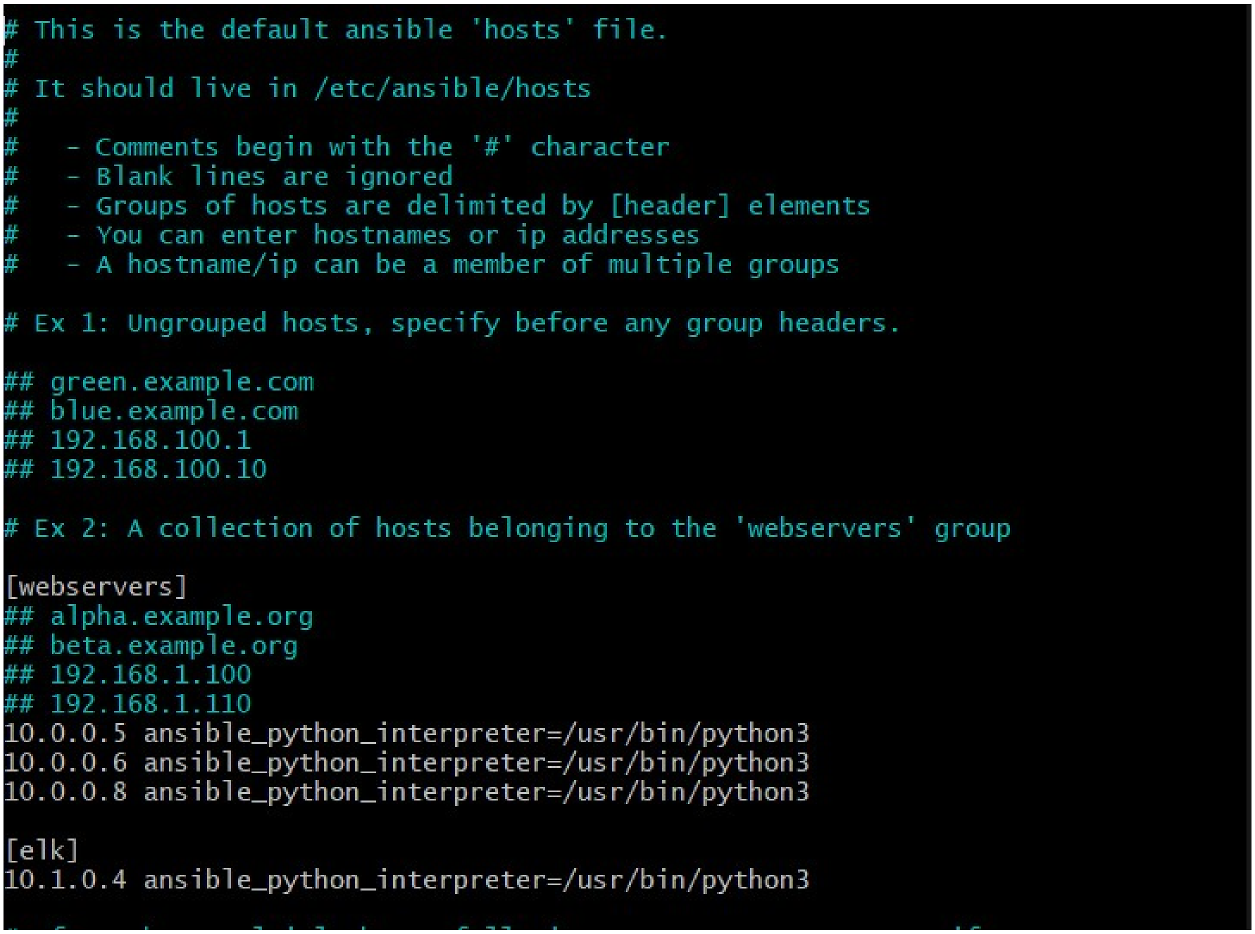
Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
ELK-SERVER	Azure subscription 1	RedTeam	East US	Stopped (deallocated)	Linux	Standard_D2s_v3	13.82.142.49	1
Jump-Box-Provisioner	Azure subscription 1	RedTeam	West US 2	Stopped (deallocated)	Linux	Standard_B1s	52.250.119.203	1
Web-1	Azure subscription 1	RedTeam	West US 2	Stopped (deallocated)	Linux	Standard_B1ms	52.183.66.168	1
Web-2	Azure subscription 1	RedTeam	West US 2	Stopped (deallocated)	Linux	Standard_B1ms	52.183.66.168	1
Web-3	Azure subscription 1	RedTeam	West US 2	Stopped (deallocated)	Linux	Standard_B1ms	52.183.66.168	1

Test the new virtual machine with SSH.



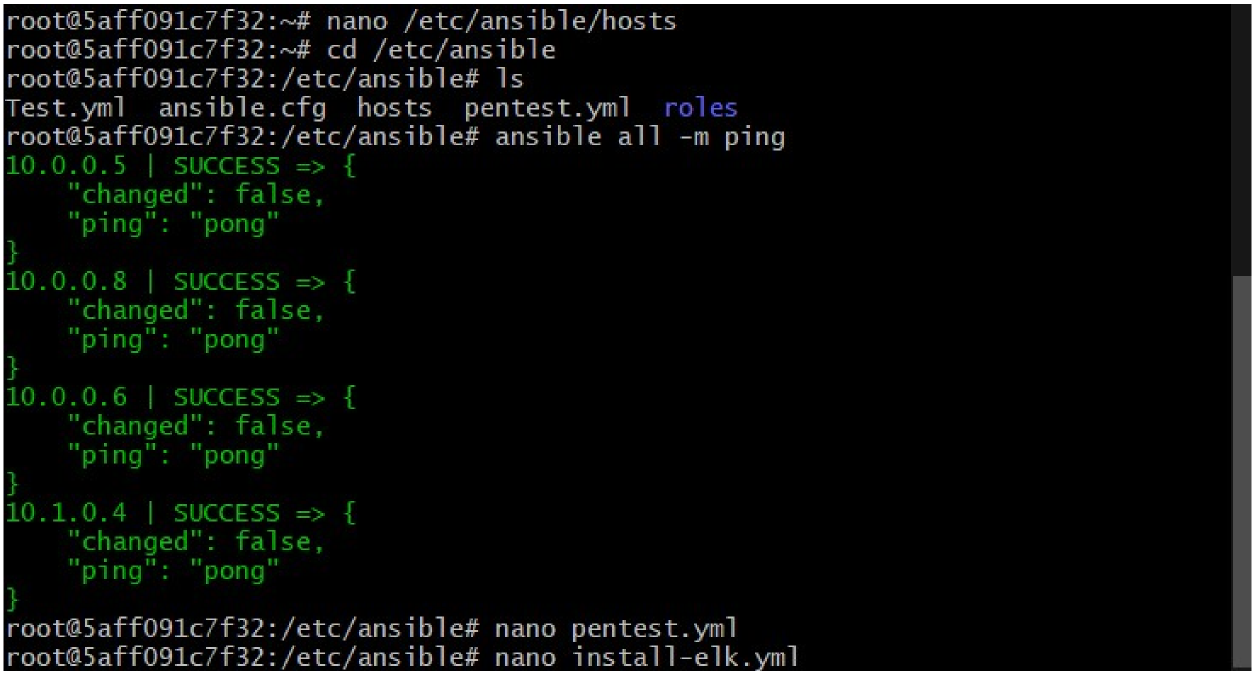
```
root@5aff091c7f32:~# ssh sysadmin@10.1.0.4
The authenticity of host '10.1.0.4 (10.1.0.4)' can't be established.
ECDSA key fingerprint is SHA256:vAh7jh8mcK7O1OpJzQLyfNUnZTVyaUlqnhHChOK5lKg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.0.4' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Mar 20 18:37:09 UTC 2021

  System load:  0.0               Processes:           116
  Usage of /:   4.5% of 28.90GB   Users logged in:     0
  Memory usage: 2%                IP address for eth0: 10.1.0.4
  Swap usage:   0%

0 packages can be updated.
0 of these updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Add the ELK VM to the ansible Host file at /etc/host.



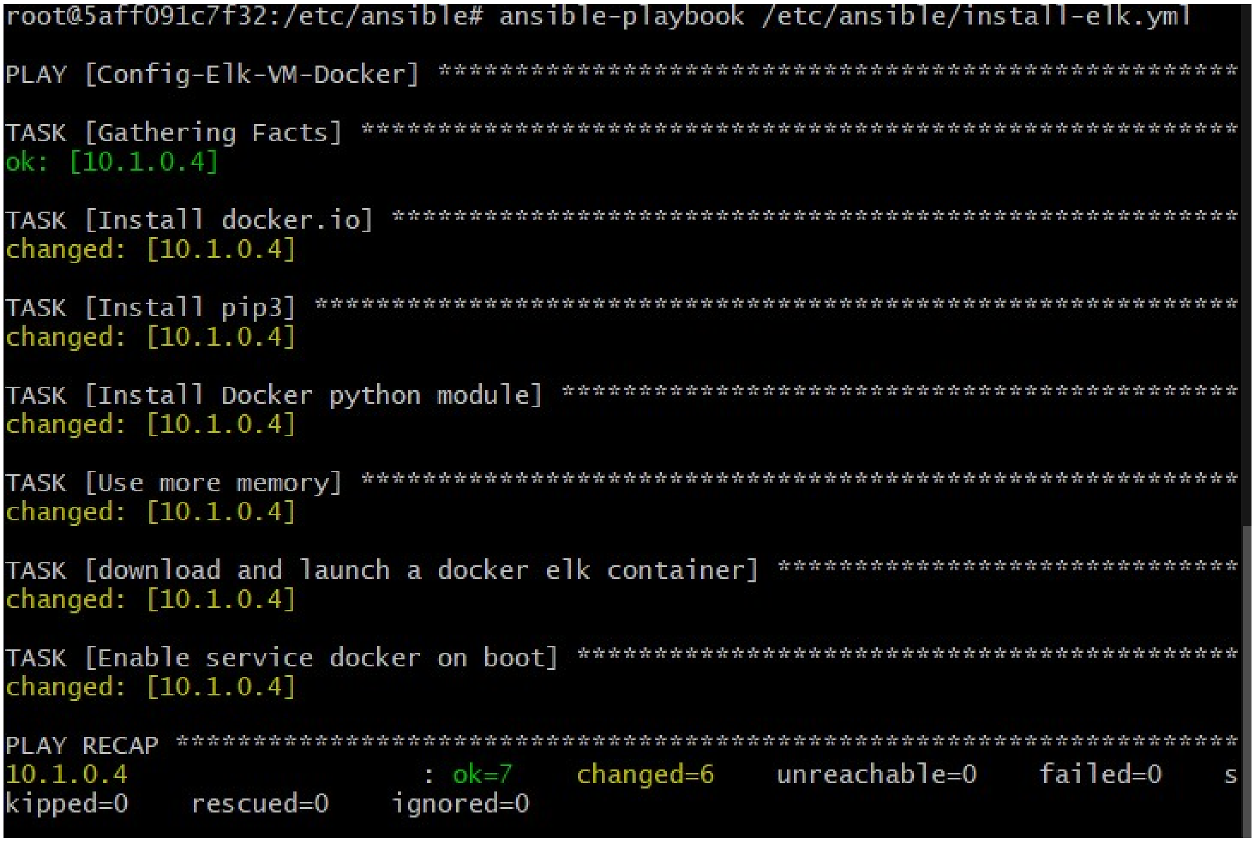
```
# This is the default ansible 'hosts' file.
#
# It should live in /etc/ansible/hosts
#
#   - Comments begin with the '#' character
#   - Blank lines are ignored
#   - Groups of hosts are delimited by [header] elements
#   - You can enter hostnames or ip addresses
#   - A hostname/ip can be a member of multiple groups

# Ex 1: Ungrouped hosts, specify before any group headers.

## green.example.com
## blue.example.com
## 192.168.100.1
## 192.168.100.10

# Ex 2: A collection of hosts belonging to the 'webservers' group

[webservers]
## alpha.example.org
## beta.example.org
## 192.168.1.100
## 192.168.1.110
10.0.0.5 ansible_python_interpreter=/usr/bin/python3
10.0.0.6 ansible_python_interpreter=/usr/bin/python3
10.0.0.8 ansible_python_interpreter=/usr/bin/python3

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

Test connection to the VMs.



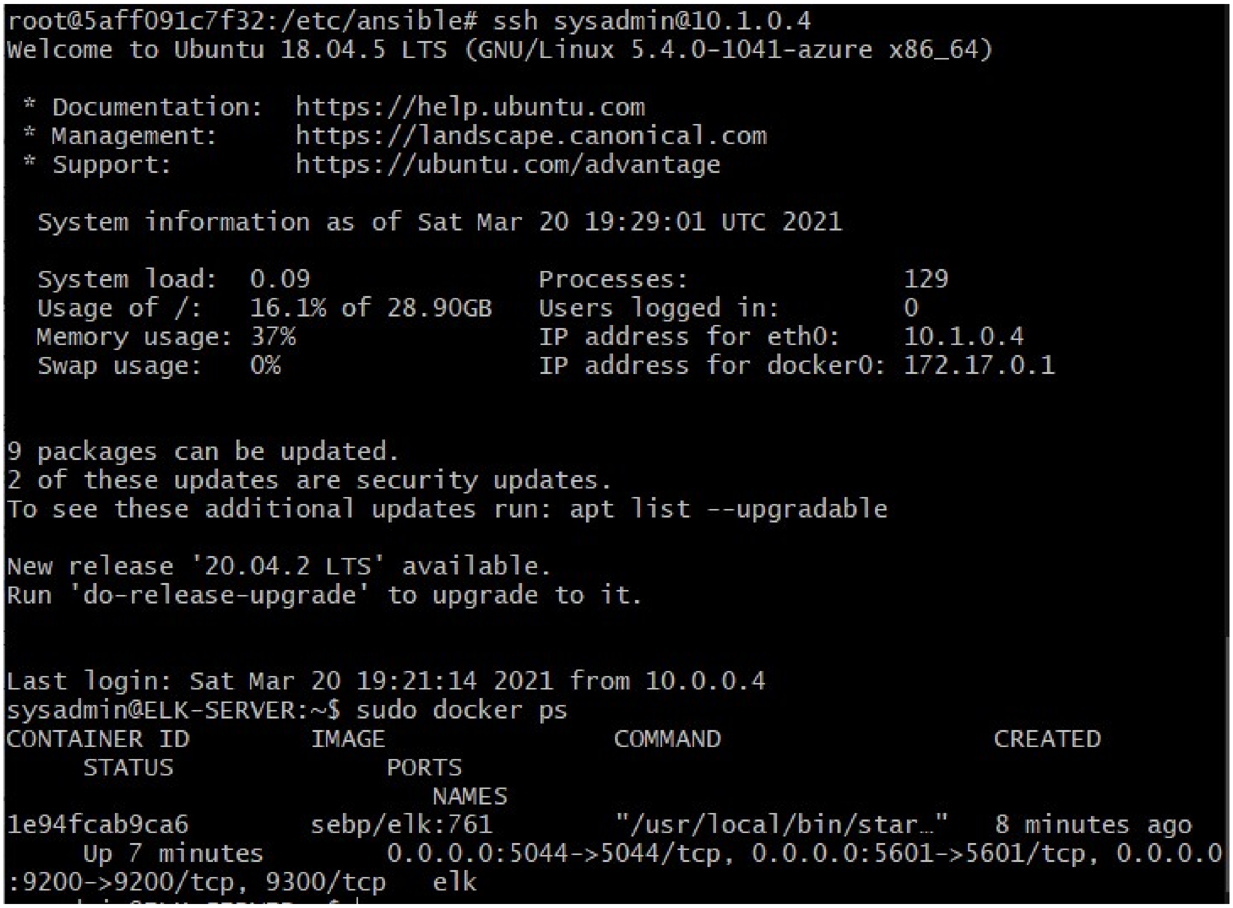
```
root@5aff091c7f32:~# nano /etc/ansible/hosts
root@5aff091c7f32:~# cd /etc/ansible
root@5aff091c7f32:/etc/ansible# ls
Test.yml  ansible.cfg  hosts  pentest.yml  roles
root@5aff091c7f32:/etc/ansible# ansible all -m ping
10.0.0.5 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.0.0.8 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.0.0.6 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.1.0.4 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
root@5aff091c7f32:/etc/ansible# nano pentest.yml
root@5aff091c7f32:/etc/ansible# nano install-elk.yml
```

Run ansible-playbook install-elk.yml



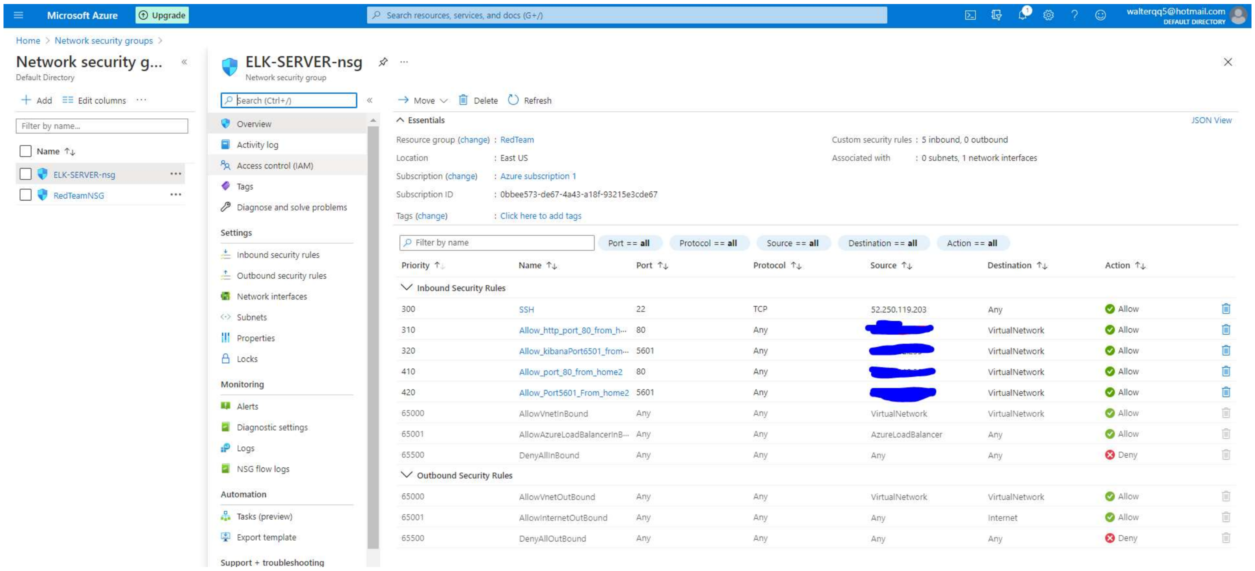
```
root@5aff091c7f32:/etc/ansible# ansible-playbook /etc/ansible/install-elk.yml

PLAY [Config-Elk-VM-Docker] ****************************************************

TASK [Gathering Facts] *********************************************************
ok: [10.1.0.4]

TASK [Install docker.io] *******************************************************
changed: [10.1.0.4]

TASK [Install pip3] ************************************************************
changed: [10.1.0.4]

TASK [Install Docker python module] ********************************************
changed: [10.1.0.4]

TASK [Use more memory] *********************************************************
changed: [10.1.0.4]

TASK [download and launch a docker elk container] ******************************
changed: [10.1.0.4]

TASK [Enable service docker on boot] *******************************************
changed: [10.1.0.4]

PLAY RECAP *********************************************************************
10.1.0.4                   : ok=7    changed=6    unreachable=0    failed=0    s
kipped=0    rescued=0    ignored=0
```

SSH into the ELK-Server VM and check ELK-Server VM sudo docker ps



```
root@5aff091c7f32:/etc/ansible# ssh sysadmin@10.1.0.4
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Mar 20 19:29:01 UTC 2021

  System load:  0.09               Processes:              129
  Usage of /:   16.1% of 28.90GB   Users logged in:        0
  Memory usage: 37%                IP address for eth0:    10.1.0.4
  Swap usage:   0%                 IP address for docker0: 172.17.0.1


9 packages can be updated.
2 of these updates are security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Mar 20 19:21:14 2021 from 10.0.0.4
sysadmin@ELK-SERVER:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED
     STATUS              PORTS
                            NAMES
1e94fcab9ca6        sebp/elk:761        "/usr/local/bin/star…"   8 minutes ago
     Up 7 minutes        0.0.0.0:5044->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0
:9200->9200/tcp, 9300/tcp   elk
```

Add security rules to allow connect to the ELK-Server VM



- ELK-SERVER-nsg
- RedTeamNSG

ELK-SERVER-nsg
Network security group

Essentials

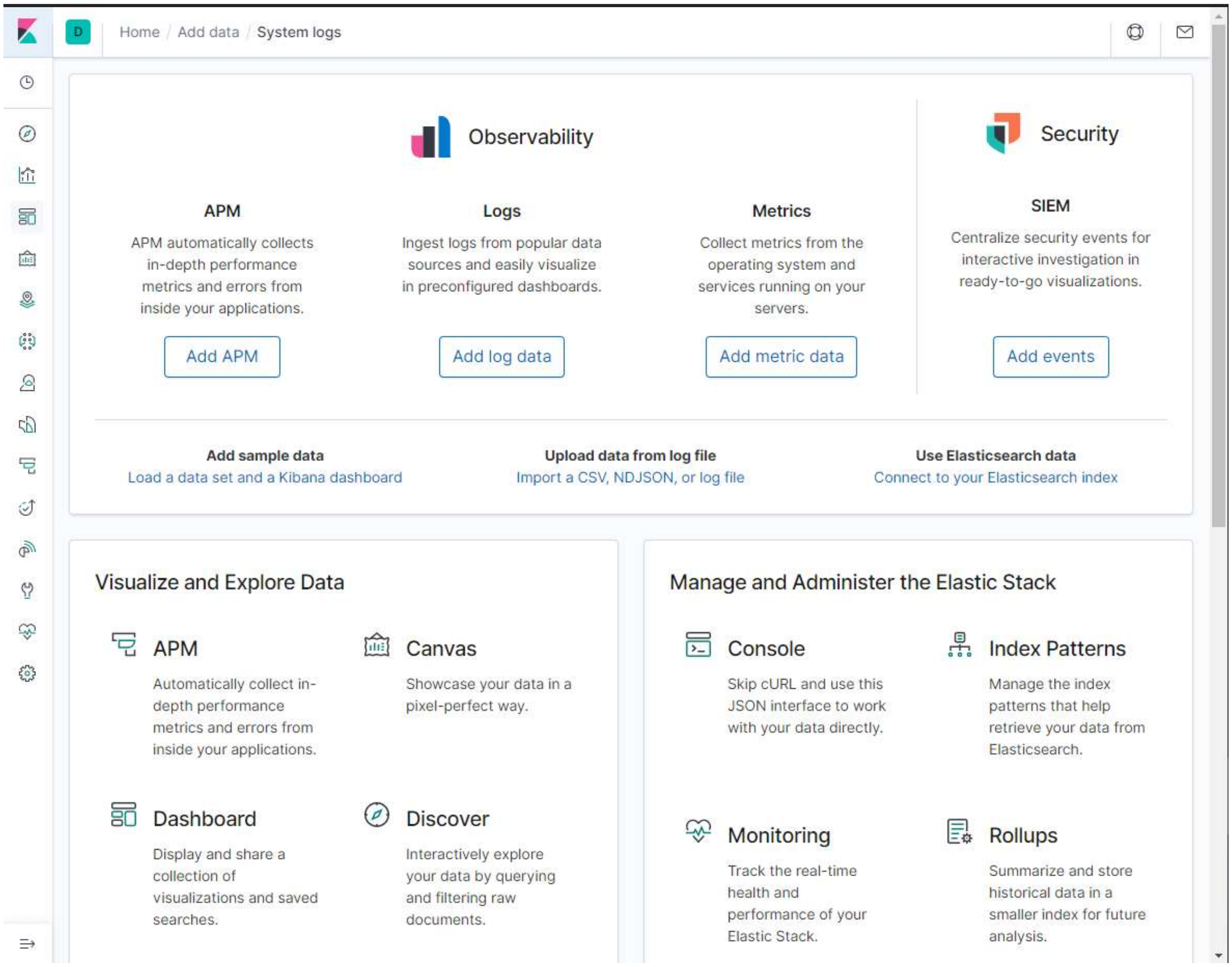
Resource group (change) : RedTeam
Location : East US
Subscription (change) : Azure subscription 1
Subscription ID : 0bbee573-de67-4a43-a18f-93215e3cde67
Tags (change) : Click here to add tags

Custom security rules : 5 inbound, 0 outbound
Associated with : 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
300	SSH	22	TCP	52.250.119.203	Any	Allow
310	Allow_http_port_80_from_h...	80	Any	[redacted]	VirtualNetwork	Allow
320	Allow_kibanaPort6501_from...	5601	Any	[redacted]	VirtualNetwork	Allow
410	Allow_port_80_from_home2	80	Any	[redacted]	VirtualNetwork	Allow
420	Allow_Port5601_From_home2	5601	Any	[redacted]	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Launch the Kibana webpage from the follow address:

http://13.82.142.49:5601/app/kibana



Observability

APM

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

Logs

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

Metrics

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

Security

SIEM

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

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

APM

Automatically collect in-depth performance metrics and errors from inside your applications.

Canvas

Showcase your data in a pixel-perfect way.

Dashboard

Display and share a collection of visualizations and saved searches.

Discover

Interactively explore your data by querying and filtering raw documents.

Manage and Administer the Elastic Stack

Console

Skip cURL and use this JSON interface to work with your data directly.

Index Patterns

Manage the index patterns that help retrieve your data from Elasticsearch.

Monitoring

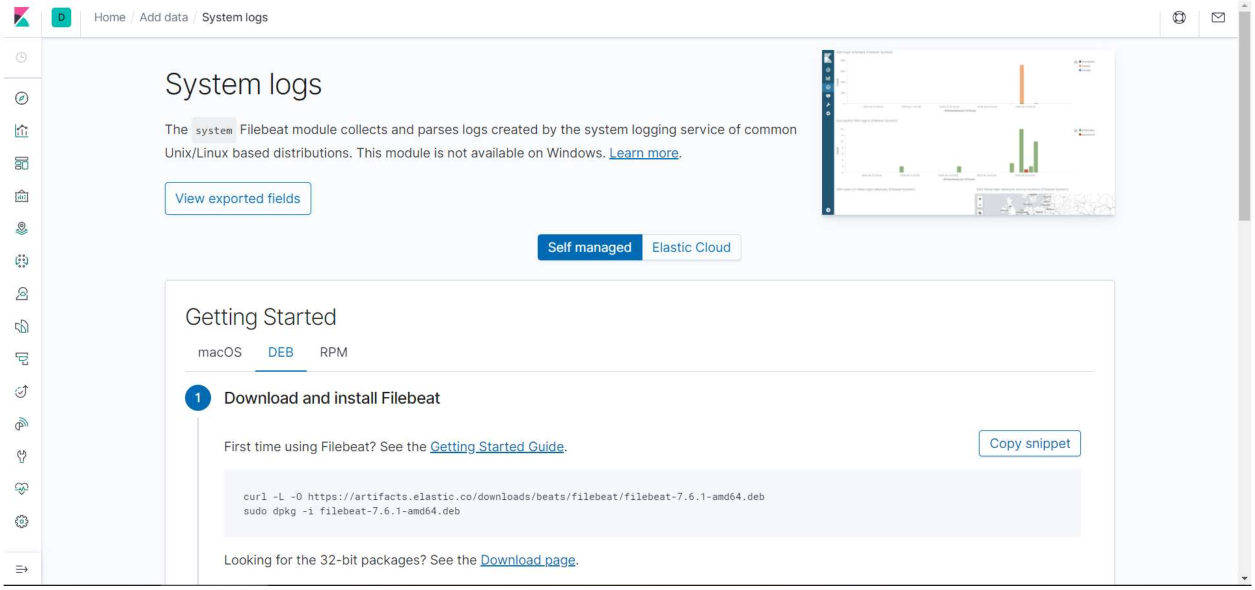
Track the real-time health and performance of your Elastic Stack.

Rollups

Summarize and store historical data in a smaller index for future analysis.

Setting up FileBeats

In the Kibana webpage, navigate to Home/Add data/ System Logs.



System logs

The `system` Filebeat module collects and parses logs created by the system logging service of common Unix/Linux based distributions. This module is not available on Windows. Learn more.

Getting Started

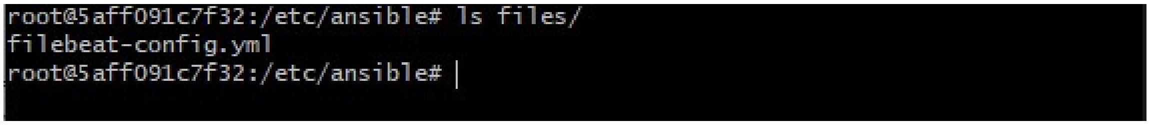
1 Download and install Filebeat

First time using Filebeat? See the Getting Started Guide.

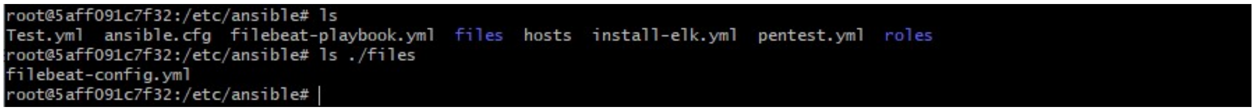
```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb
sudo dpkg -i filebeat-7.6.1-amd64.deb
```

Looking for the 32-bit packages? See the Download page.

Copy the file filebeat-config.yml to /etc/ansible/files.



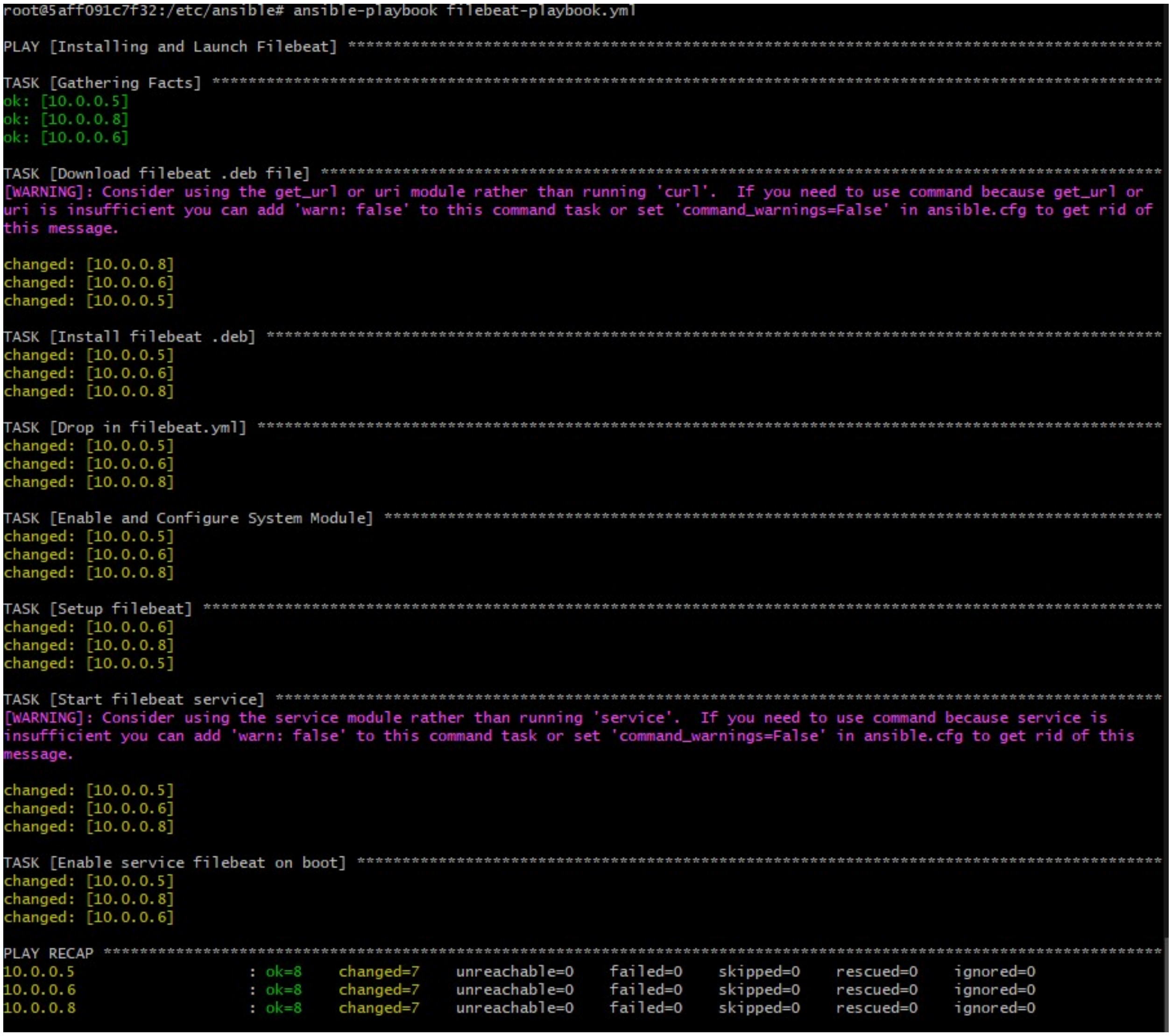
```
root@5aff091c7f32:/etc/ansible# ls files/
filebeat-config.yml
root@5aff091c7f32:/etc/ansible# |
```



```
root@5aff091c7f32:/etc/ansible# ls
Test.yml  ansible.cfg  filebeat-playbook.yml  files  hosts  install-elk.yml  pentest.yml  roles
root@5aff091c7f32:/etc/ansible# ls ./files
filebeat-config.yml
root@5aff091c7f32:/etc/ansible# |
```

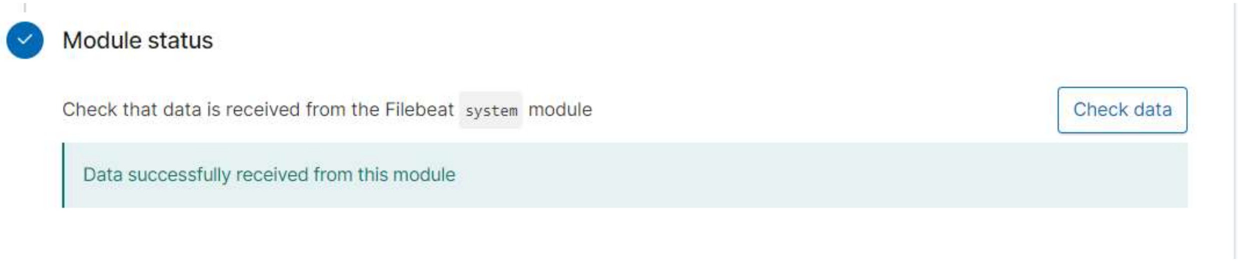
Copy the filebeat-playbook.yml file to /etc/ansible.

Run the filebeat-playbook.yml playbook.



```
root@5aff091c7f32:/etc/ansible# ansible-playbook filebeat-playbook.yml

PLAY [Installing and Launch Filebeat] *****************************************************************************************

TASK [Gathering Facts] ********************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.8]
ok: [10.0.0.6]

TASK [Download filebeat .deb file] ********************************************************************************************
[WARNING]: Consider using the get_url or uri module rather than running 'curl'.  If you need to use command because get_url or
uri is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get rid of
this message.

changed: [10.0.0.8]
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [Install filebeat .deb] **************************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [Drop in filebeat.yml] ***************************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [Enable and Configure System Module] *************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [Setup filebeat] *********************************************************************************************************
changed: [10.0.0.6]
changed: [10.0.0.8]
changed: [10.0.0.5]

TASK [Start filebeat service] *************************************************************************************************
[WARNING]: Consider using the service module rather than running 'service'.  If you need to use command because service is
insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get rid of this
message.

changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [Enable service filebeat on boot] ****************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.8]
changed: [10.0.0.6]

PLAY RECAP ********************************************************************************************************************
10.0.0.5                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.6                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.8                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

- Check on Kibana that logs are being received from module status.



Module status

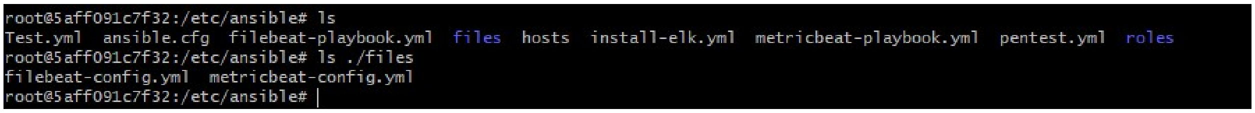
Check that data is received from the Filebeat `system` module

Data successfully received from this module

Setting up Metricbeats

In the Kibana webpage, navigate to Home/Add data/ System Logs.

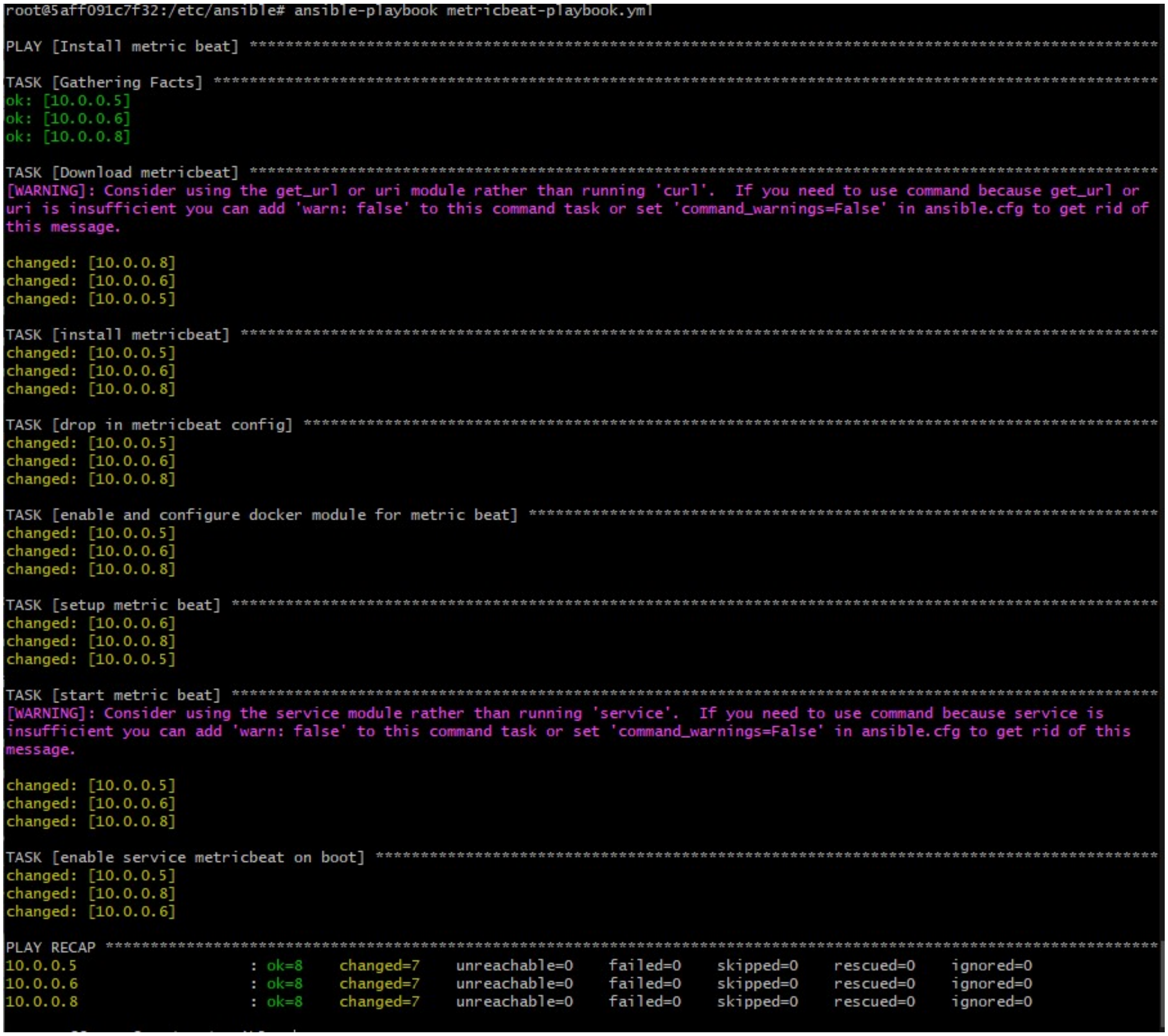
Copy the file metricbeat-config.yml to /etc/ansible/files.



```
root@5aff091c7f32:/etc/ansible# ls
Test.yml  ansible.cfg  filebeat-playbook.yml  files  hosts  install-elk.yml  metricbeat-playbook.yml  pentest.yml  roles
root@5aff091c7f32:/etc/ansible# ls ./files
filebeat-config.yml  metricbeat-config.yml
root@5aff091c7f32:/etc/ansible# |
```

Copy the metricbeat-playbook.yml file to /etc/ansible.

Run the metricbeat-playbook.yml playbook.



```
root@5aff091c7f32:/etc/ansible# ansible-playbook metricbeat-playbook.yml

PLAY [Install metric beat] ****************************************************************************************

TASK [Gathering Facts] ********************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]
ok: [10.0.0.8]

TASK [Download metricbeat] ****************************************************************************************
[WARNING]: Consider using the get_url or uri module rather than running 'curl'.  If you need to use command because get_url or
uri is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get rid of
this message.

changed: [10.0.0.8]
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [install metricbeat] *****************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [drop in metricbeat config] **********************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [enable and configure docker module for metric beat] *********************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [setup metric beat] ******************************************************************************************
changed: [10.0.0.6]
changed: [10.0.0.8]
changed: [10.0.0.5]

TASK [start metric beat] ******************************************************************************************
[WARNING]: Consider using the service module rather than running 'service'.  If you need to use command because service is
insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get rid of this
message.

changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.8]

TASK [enable service metricbeat on boot] **************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.8]
changed: [10.0.0.6]

PLAY RECAP ********************************************************************************************************
10.0.0.5                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.6                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.8                   : ok=8    changed=7    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Check on Kibana that logs are being received.