

# MS Azure Creation of ELK Server

Microsoft Azure

Search resources, services, and docs (G+ /)

Show portal menu

Home >

Microsoft.VirtualNetwork-20210227102321 | Overview

Deployment

Search (Cmd+ /)

Delete Cancel Redeploy Refresh

Overview

Inputs

Outputs

Template

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.VirtualNetwork-20210227102321 Start time: 2/27/2021, 10:27:12 AM

Subscription: Azure subscription 1 Correlation ID: 4684e2c3-c1f6-4f5e-a2e8-e7b4312fa7ac

Resource group: myresourcegroup

Deployment details (Download)

Next steps

Microsoft Azure

Search resources, services, and docs (G+ /)

sheapadilla2510@gmail...

STATE OF ARIZONA

Home > Virtual networks > ELK-NET-PRJ-1

Virtual networks

State of Arizona

Create Manage view

Filter for any field...

Name

ELK-NET-PRJ-1

resource\_group\_virtual\_network

ELK-NET-PRJ-1 | Peerings

Virtual network

Search (Cmd+ /)

Add Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Filter by name...

Name	Peering status	Peer	Gateway transit
East_to_West	Connected	resource_group_virtual_net...	Disabled

```
sheapadilla@Sheas-MacBook-Pro ~ % ssh azureuser@13.91.125.108
```

```
azureuser@Jump-Box-Provisioner:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS              NAMES
azureuser@Jump-Box-Provisioner:~$ sudo docker ps -a
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS              NAMES
886132173ab9        cyberxsecurity/ansible "bash"             6 days ago         Exited (0) 2 days ago                busy_elion
azureuser@Jump-Box-Provisioner:~$ sudo docker container start 886
886
azureuser@Jump-Box-Provisioner:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS              NAMES
886132173ab9        cyberxsecurity/ansible "bash"             6 days ago         Up 38 seconds                busy_elion
azureuser@Jump-Box-Provisioner:~$ sudo docker attach 886
root@886132173ab9:~# cat ~/.ssh/id_rsa.pub
```

[Home](#) >



## CreateVm-Canonical.UbuntuServer-18.04-LTS-20210227105042 | Overview

Deployment

Search (Cmd+/)

Delete Cancel Redeploy Refresh

Overview

Inputs

Outputs

Template

We'd love your feedback! →

### ✓ Your deployment is complete



Deployment name: CreateVm-Canonical.UbuntuServer-18.04-LTS-2... Start time: 2/27/2021, 11:01:26 AM  
Subscription: [Azure subscription 1](#) Correlation ID: ad4de8b2-98c4-4e48-b726-4bbab3aa6758  
Resource group: [myresourcegroup](#)

Deployment details [\(Download\)](#)

Next steps

[Setup auto-shutdown](#) Recommended

[Monitor VM health, performance and network dependencies](#) Recommended

[Run a script inside the virtual machine](#) Recommended

[Go to resource](#)

[Create another VM](#)



#### Security Center

Secure your apps and infrastructure

[Go to Azure security center >](#)

#### Free Microsoft tutorials

[Start learning today >](#)

#### Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

[Find an Azure expert >](#)

```
# Ex 2: A collection of hosts belonging to the 'webserver' group
[elk]
10.1.0.4
```



## Azure services

[Create a resource](#)

Virtual machines



Network security groups



Virtual networks



Load balancers



Resource groups



Subscriptions












Cost Management...



App Services

[More services](#)

## Recent resources

Name	Type	Last Viewed
 ELK	Virtual machine	10 minutes ago
 myresourcegroup	Resource group	11 minutes ago
 Jump-Box-Provisioner	Virtual machine	33 minutes ago
 my_nsg	Network security group	37 minutes ago
 ELK-NET-PRJ-1	Virtual network	45 minutes ago
 my_load_balancer	Load balancer	3 days ago
 Web-1	Virtual machine	3 days ago
 Web-2	Virtual machine	5 days ago
 resource_group_virtual_network	Virtual network	a week ago

install-elk.yml

```
1
2 - name: Configure Elk VM with Docker
3   hosts: elk
4   remote_user: sysadmin
5   become: true
6   tasks:
7     # Use apt module
8     - name: Install docker.io
9       apt:
10         update_cache: yes
11         name: docker.io
12         state: present
13
14     # Use apt module
15     - name: Install pip3
16       apt:
17         force_apt_get: yes
18         name: python3-pip
19         state: present
20
21     # Use pip module
22     - name: Install Docker python module
23       pip:
24         name: docker
25         state: present
26
27     # Use sysctl module
28     - name: Use more memory
29       sysctl:
30         name: vm.max_map_count
31         value: "262144"
32         state: present
33         reload: yes
34
35     # Use docker_container module
36     - name: download and launch a docker elk docker_container
37       docker_container:
38         name: elk
39         image: sebp/elk:761
40         state: started
41         restart_policy: always
42         published_ports:
43           - 5601:5601
44           - 9200:9200
45           - 5044:5044
46
47     # Use systemd module
48     - name: Enable service docker on boot
49       systemd:
50         name: docker
51         enabled: yes
```

```
--
- name: Configure Elk VM with Docker
  hosts: elk
  remote_user: sysadmin
  become: true
  tasks:
    # Use apt module
    - name: Install docker.io
      apt:
        update_cache: yes
        name: docker.io
        state: present

    # Use apt module
    - name: Install pip3
      apt:
        force_apt_get: yes
        name: python3-pip
        state: present

    # Use pip module
    - name: Install Docker python module
      pip:
        name: docker
        state: present

    # Use sysctl module
    - name: Use more memory
      sysctl:
        name: vm.max_map_count
        value: "262144"
        state: present
        reload: yes

    # Use docker_container module
    - name: download and launch a docker elk docker_container
      docker_container:
        name: elk
        image: sebp/elk:761
        state: started
        restart_policy: always
        published_ports:
          - 5601:5601
          - 9200:9200
          - 5044:5044

    # Use systemd module
    - name: Enable service docker on boot
      systemd:
        name: docker
        enabled: yes
```

```

root@886132173ab9:/etc/ansible# ansible-playbook elk.yml

PLAY [Configure Elk VM with Docker] *****

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

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

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

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

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

TASK [download and launch a docker elk docker_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=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

```

Microsoft Azure | Search resources, services, and docs (G+)

Home > Network security groups > ELK-nsg

### Network security g... <<

State of Arizona

+ Add Edit columns ...

Filter by name...

- ☐ Name ↑↓
- ☐ ELK-nsg ...
- ☐ my\_nsg ...

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces

### ELK-nsg | Inbound security rules ...

Network security group

Search (Cmd+)

+ Add Hide default rules Refresh Delete

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

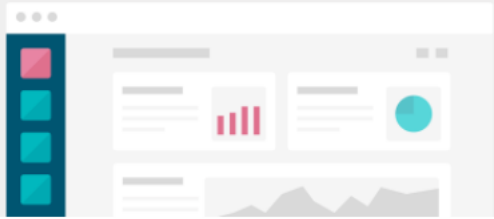
Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
<input type="checkbox"/> 300	SSH	22	TCP	174.17.174.239
<input type="checkbox"/> 310	5601_Port	5601	Any	174.17.174.239
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

20.55.105.58:5601/app/kibana#/home



# Welcome to Kibana

Your window into the Elastic Stack



### Let's get started

We noticed that you don't have any data in your cluster. You can try our sample data and dashboards or jump in with your own data.

[Try our sample data](#) [Explore on my own](#)

To learn about how usage data helps us manage and improve our products and services, see our [Privacy Statement](#). To stop collection, [disable usage data here](#).