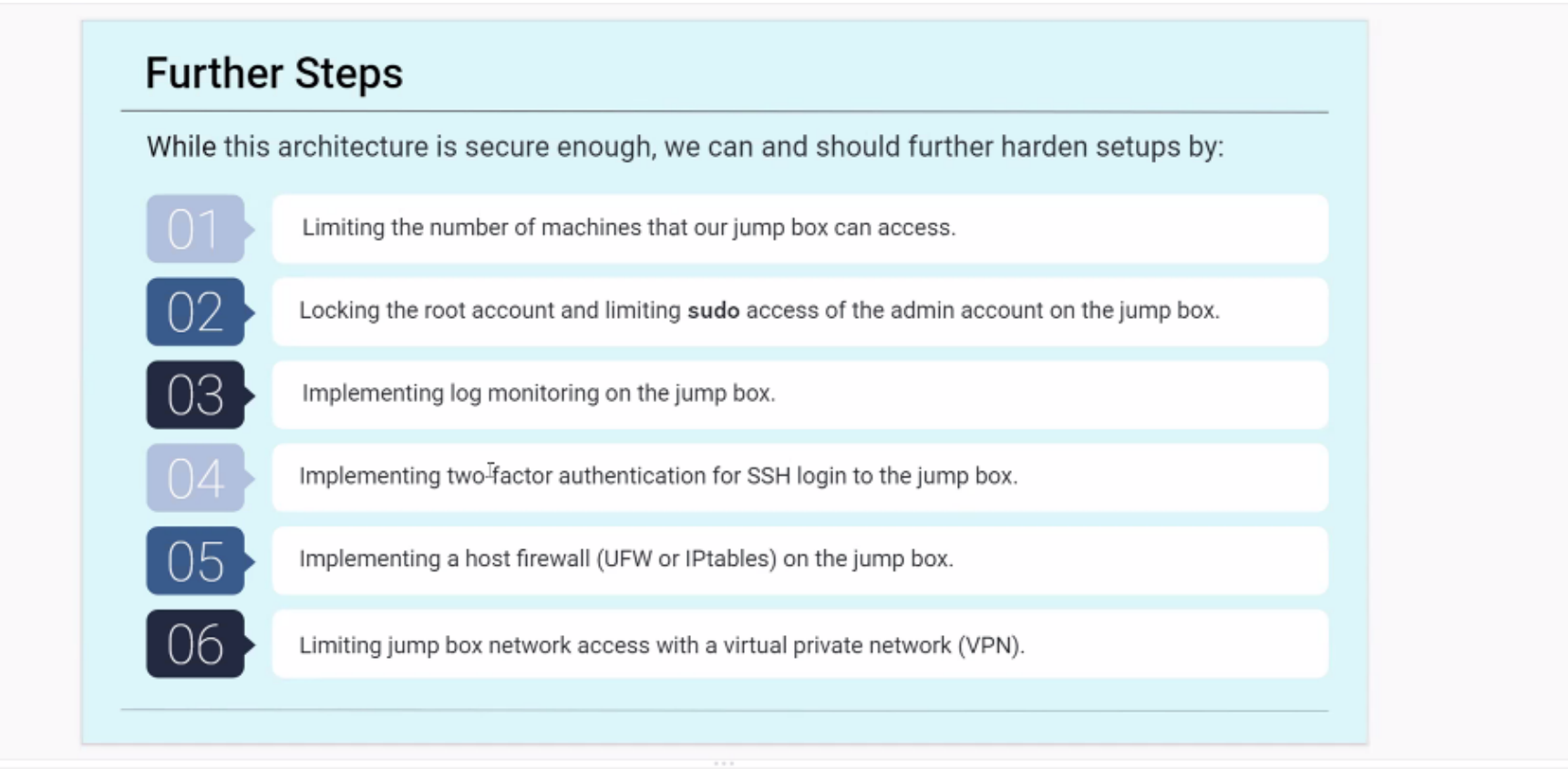
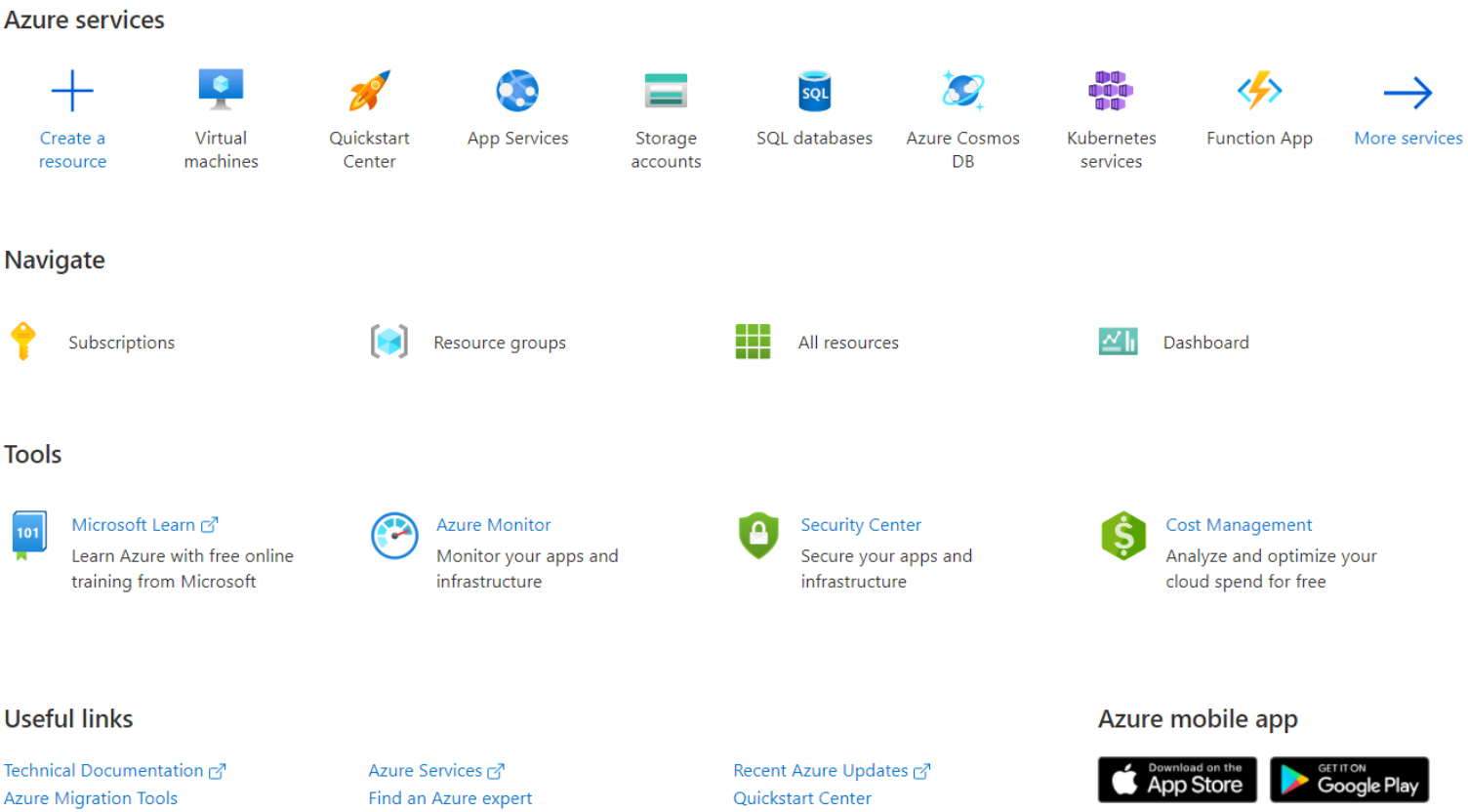
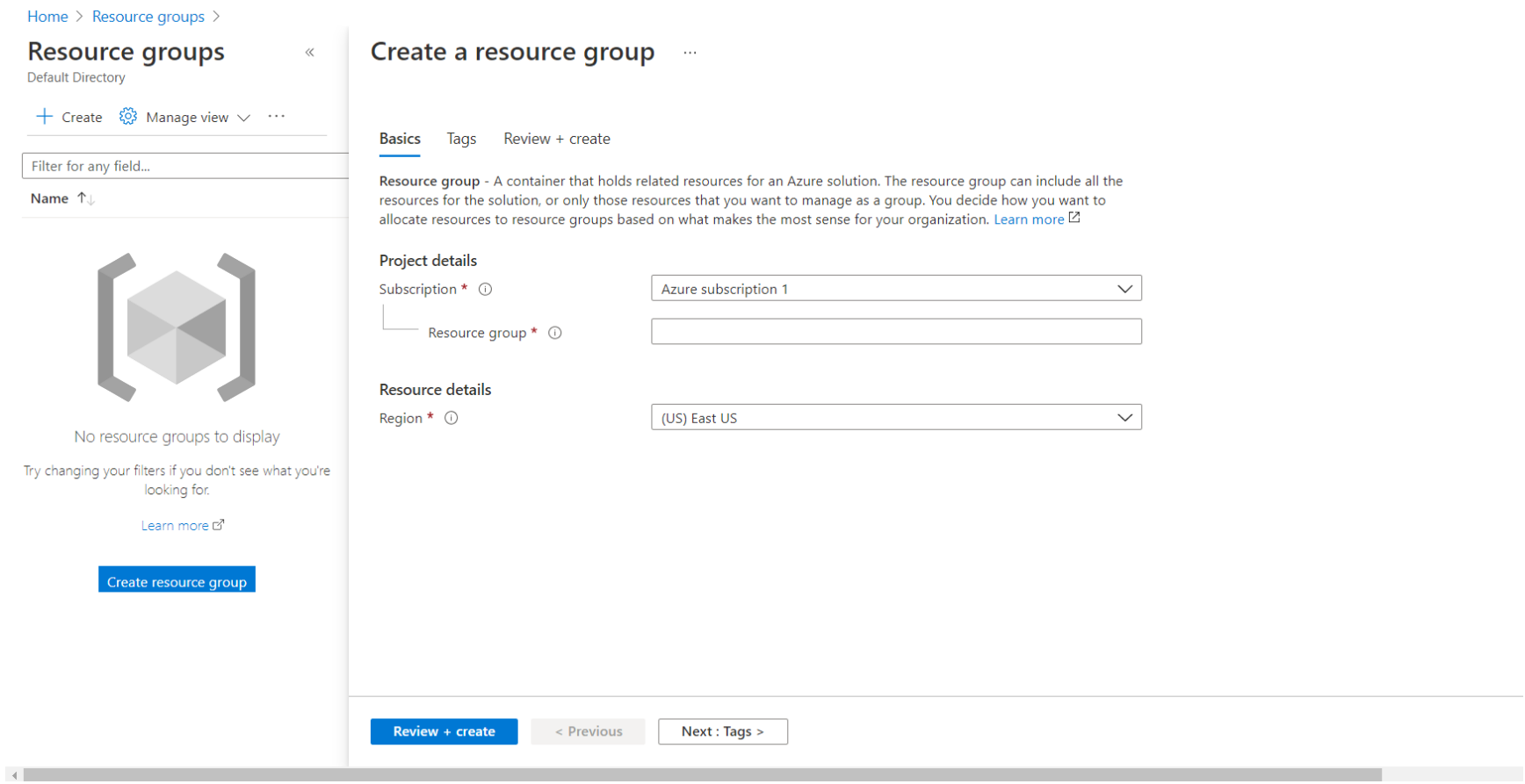
opt-



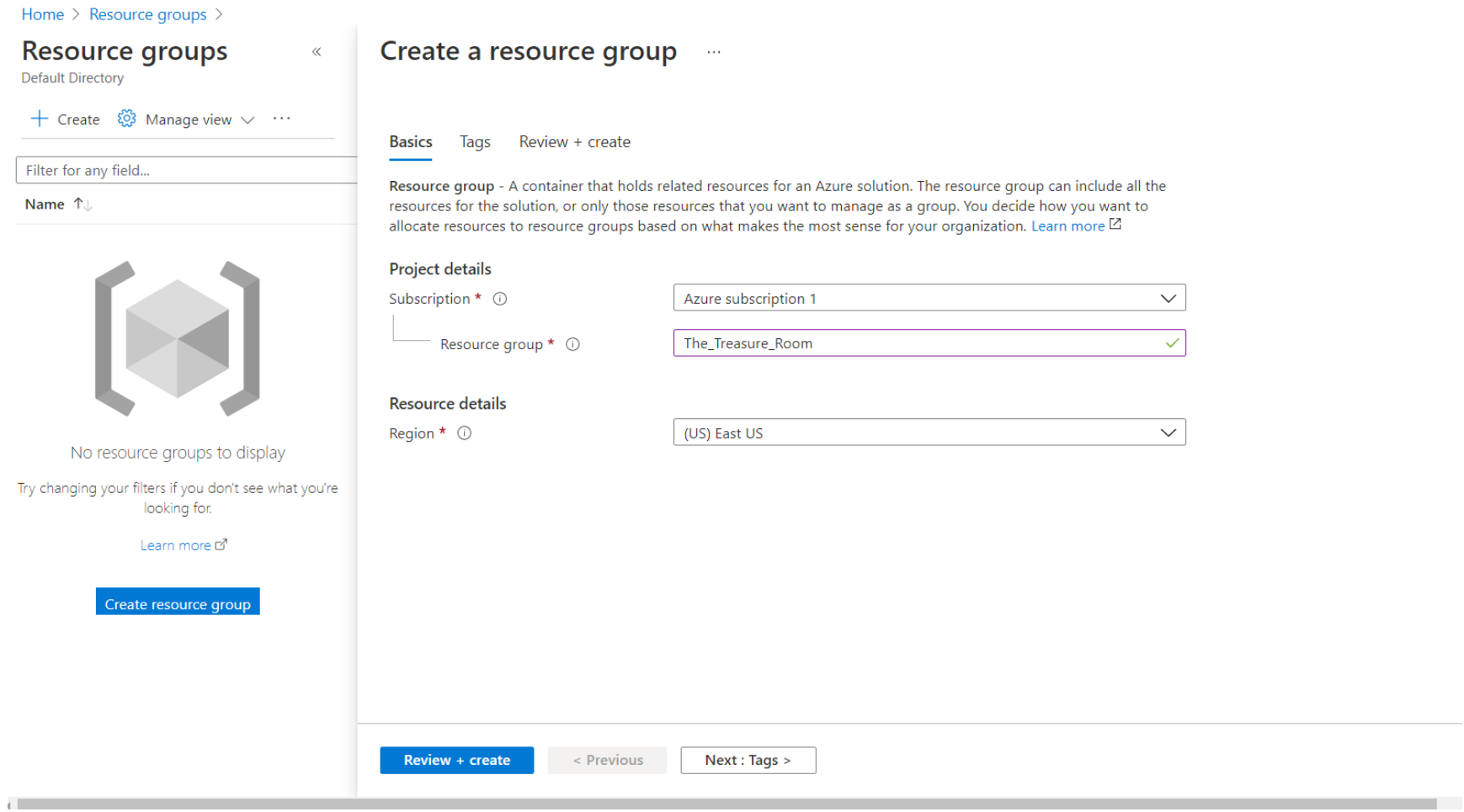
Step 1-Home



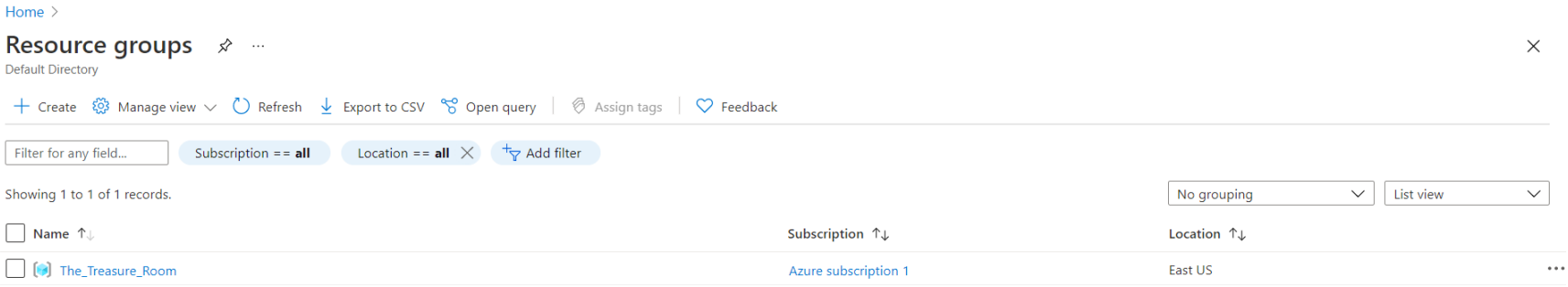
Step 2-Create a resource group-a container that holds all resources needed.


Home > Resource groups >
Resource groups
Default Directory
Create
Manage view
Filter for any field...
Name
No resource groups to display
Try changing your filters if you don't see what you're looking for.
Learn more
Create resource group
Create a resource group
Basics
Tags
Review + create
Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more
Project details
Subscription *
Azure subscription 1
Resource group *
Resource details
Region *
(US) East US
Review + create
< Previous
Next : Tags >

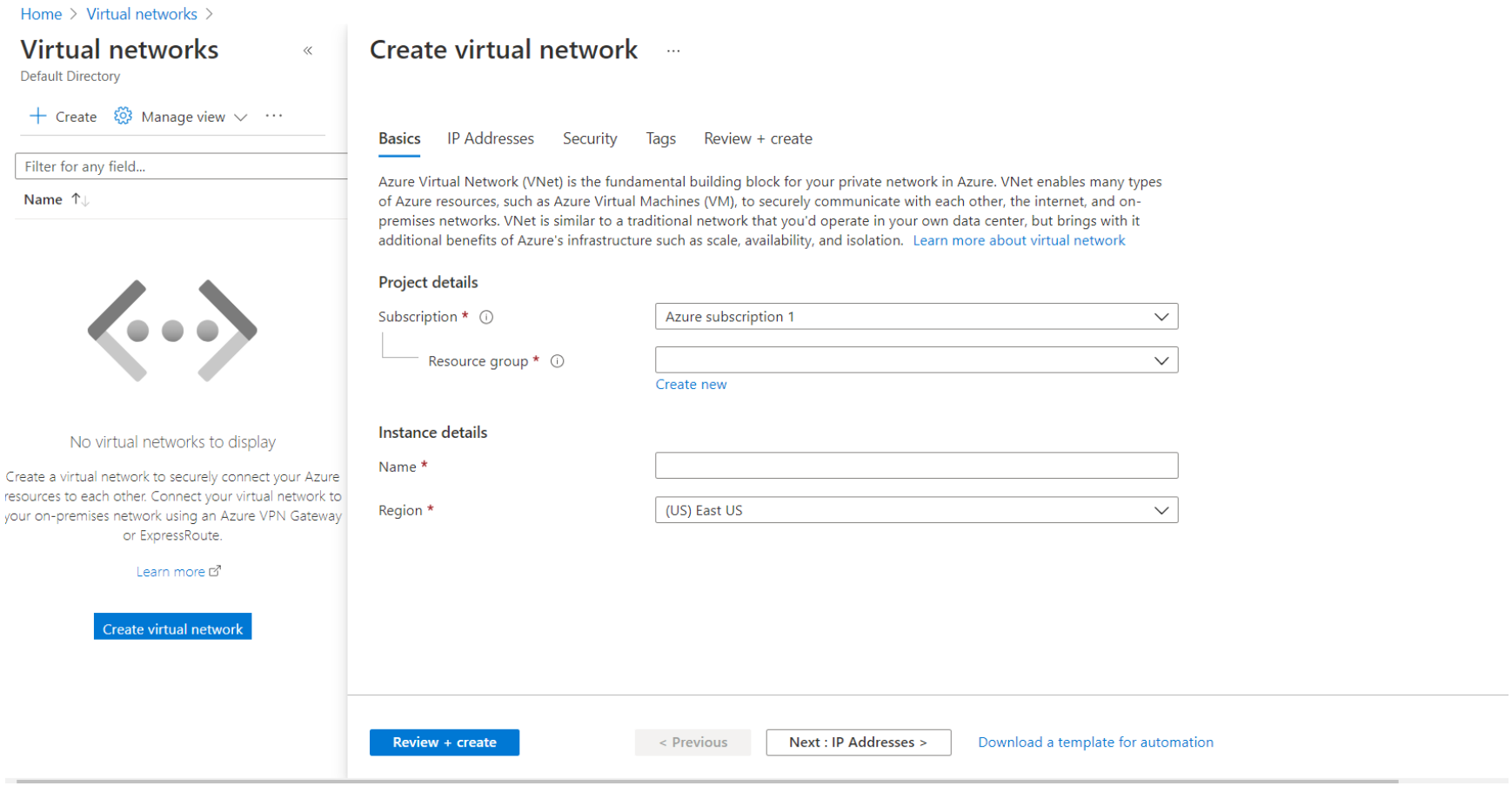
2.a


Home > Resource groups >
Resource groups
Default Directory
Create
Manage view
Filter for any field...
Name
No resource groups to display
Try changing your filters if you don't see what you're looking for.
Learn more
Create resource group
Create a resource group
Basics
Tags
Review + create
Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more
Project details
Subscription *
Azure subscription 1
Resource group *
The_Treasure_Room
Resource details
Region *
(US) East US
Review + create
< Previous
Next : Tags >

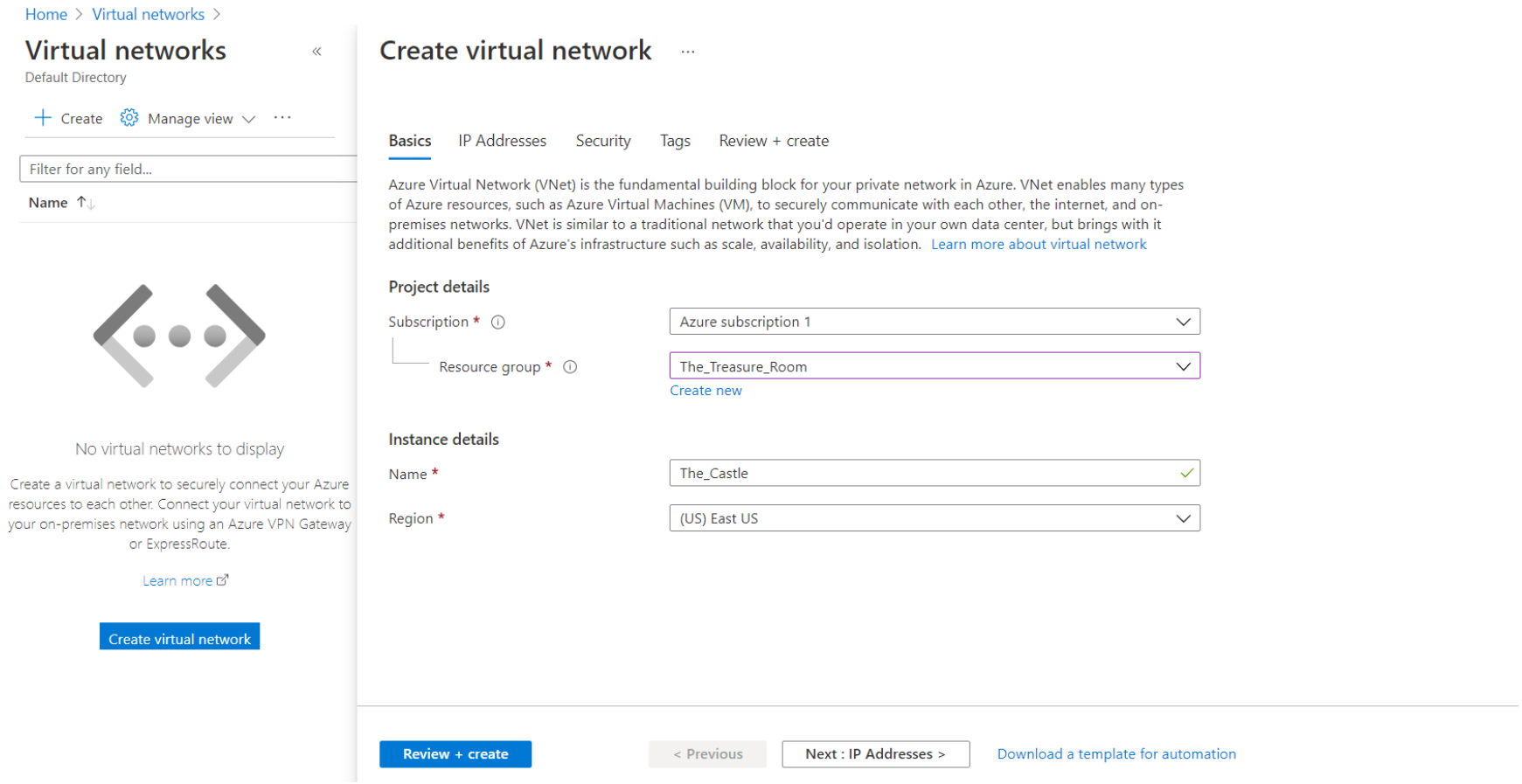
2.b



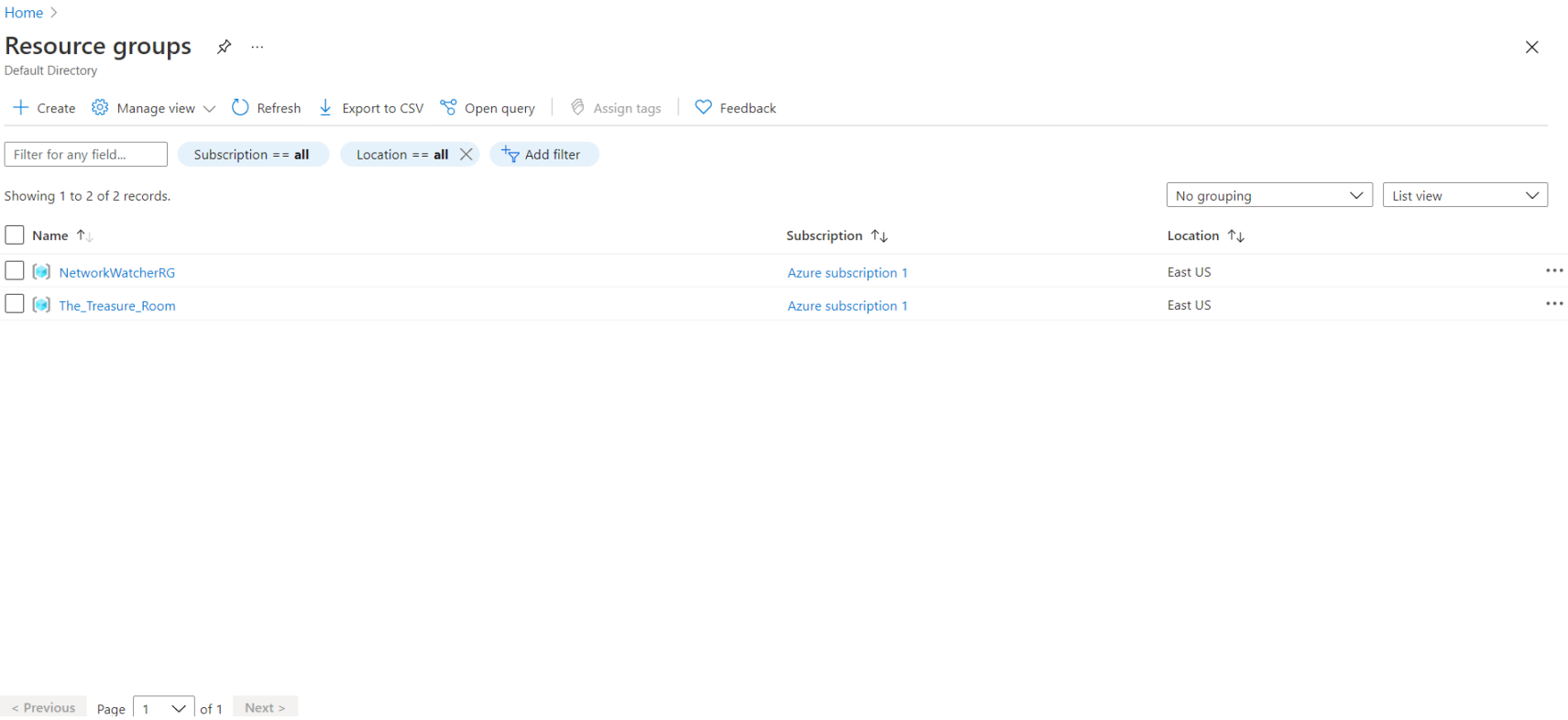
3.-Set up a virtual Network so resources can be accessed.


Home > Virtual networks >
Virtual networks
Default Directory
Create
Manage view
Filter for any field...
Name
No virtual networks to display
Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute.
Learn more
Create virtual network
Create virtual network
Basics
IP Addresses
Security
Tags
Review + create
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 *
Create new
Instance details
Name *
Region *
(US) East US
Review + create
< Previous
Next : IP Addresses >
Download a template for automation

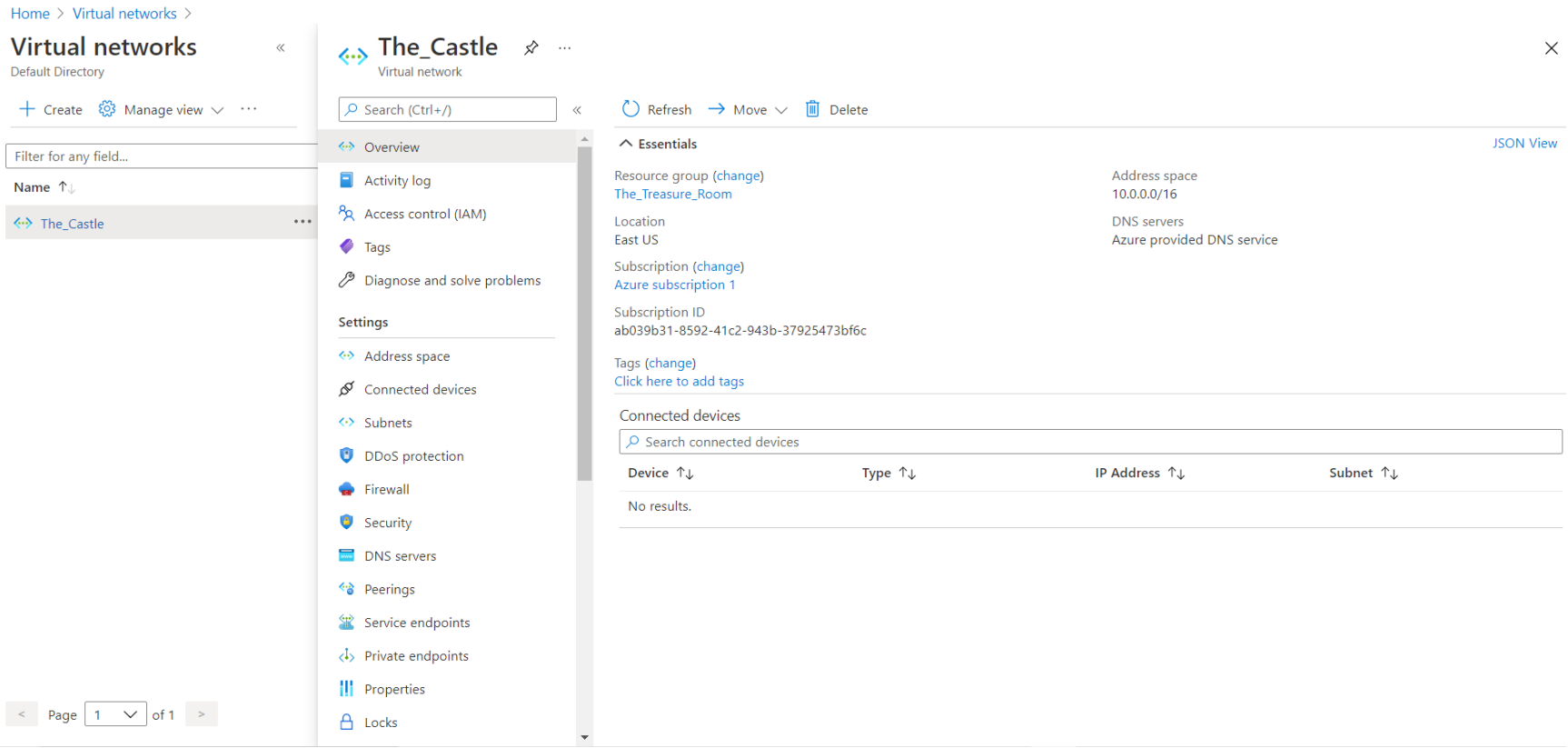
3.a


Home > Virtual networks >
Virtual networks
Default Directory
Create
Manage view
Filter for any field...
Name
No virtual networks to display
Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute.
Learn more
Create virtual network
Create virtual network
Basics
IP Addresses
Security
Tags
Review + create
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 *
The_Treasure_Room
Create new
Instance details
Name *
The_Castle
Region *
(US) East US
Review + create
< Previous
Next : IP Addresses >
Download a template for automation

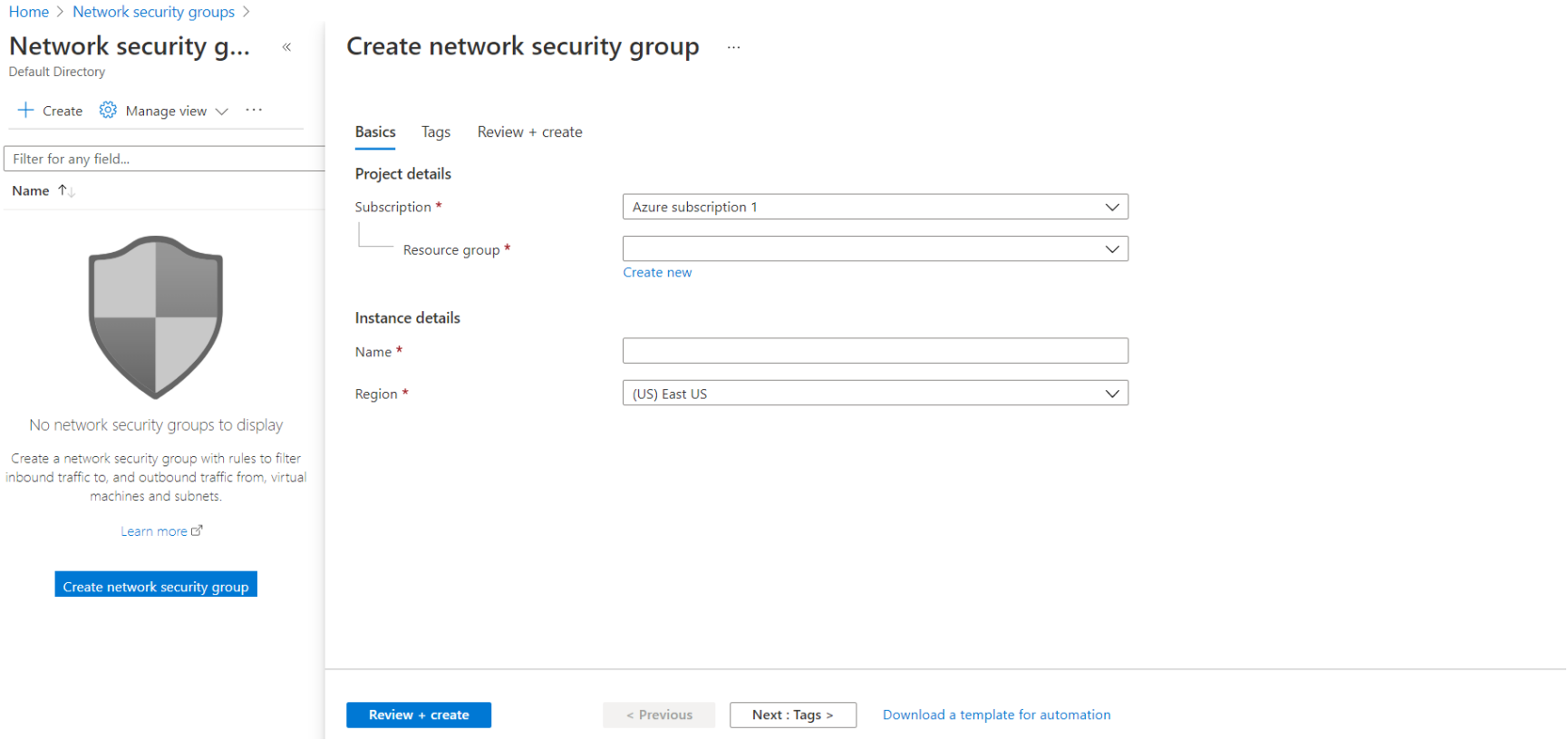
3.b-


Home
Resource groups
Default Directory
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Feedback
Filter for any field...
Subscription == all
Location == all
Add filter
Showing 1 to 2 of 2 records.
No grouping
List view
Name
Subscription
Location
NetworkWatcherRG
Azure subscription 1
East US
The_Treasure_Room
Azure subscription 1
East US
< Previous
Page 1 of 1
Next >

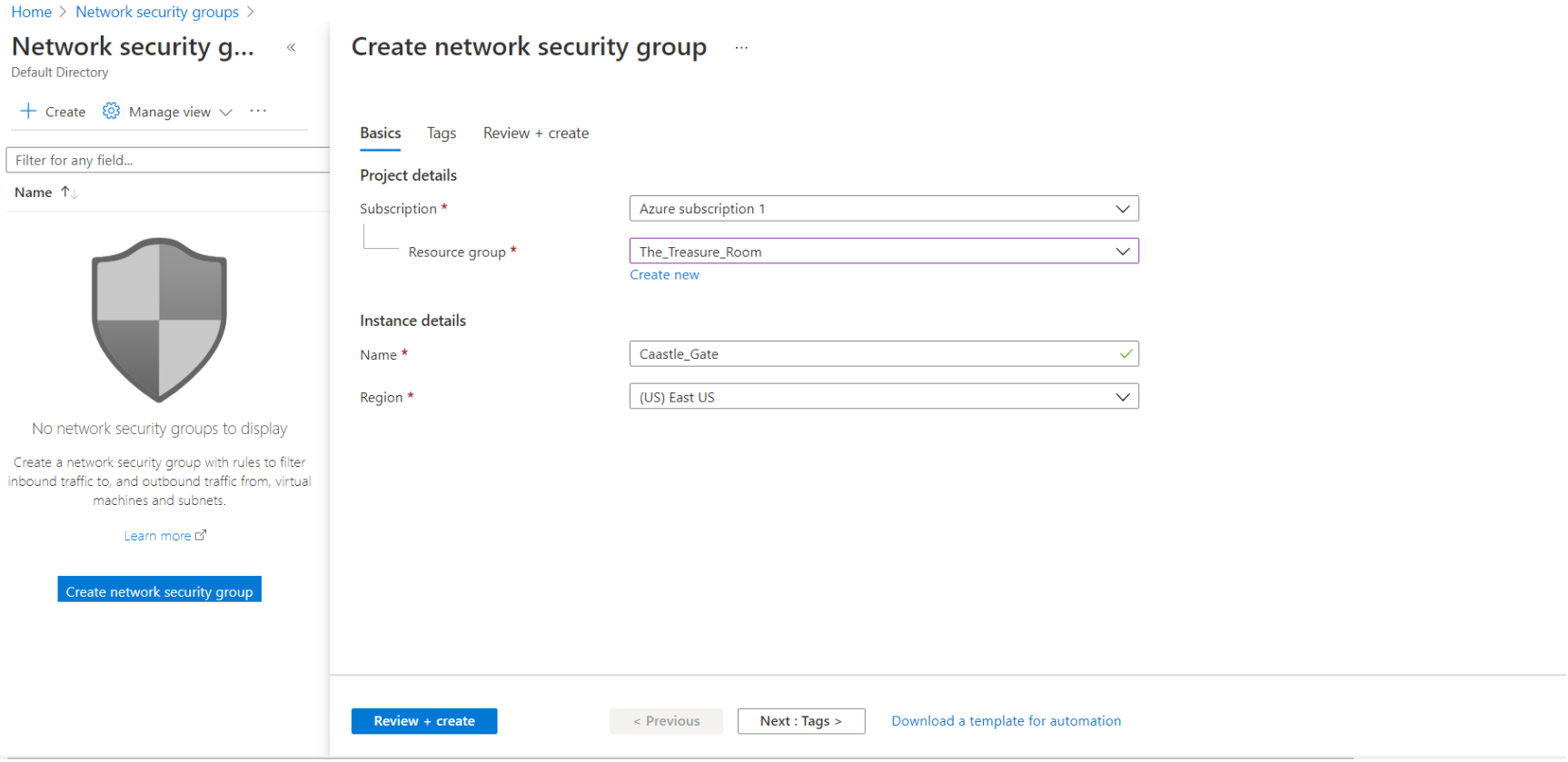
3.c-



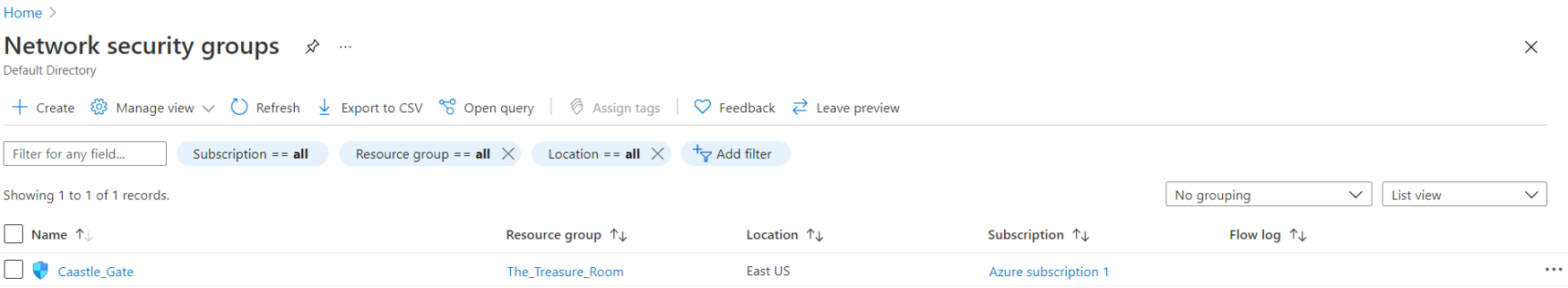
4.-Network Security Group


Home > Network security groups >
Network security g...
Default Directory
Create
Manage view
Filter for any field...
Name
No network security groups to display
Create a network security group with rules to filter inbound traffic to, and outbound traffic from, virtual machines and subnets.
Learn more
Create network security group
Create network security group
Basics
Tags
Review + create
Project details
Subscription *
Azure subscription 1
Resource group *
Create new
Instance details
Name *
Region *
(US) East US
Review + create
< Previous
Next : Tags >
Download a template for automation

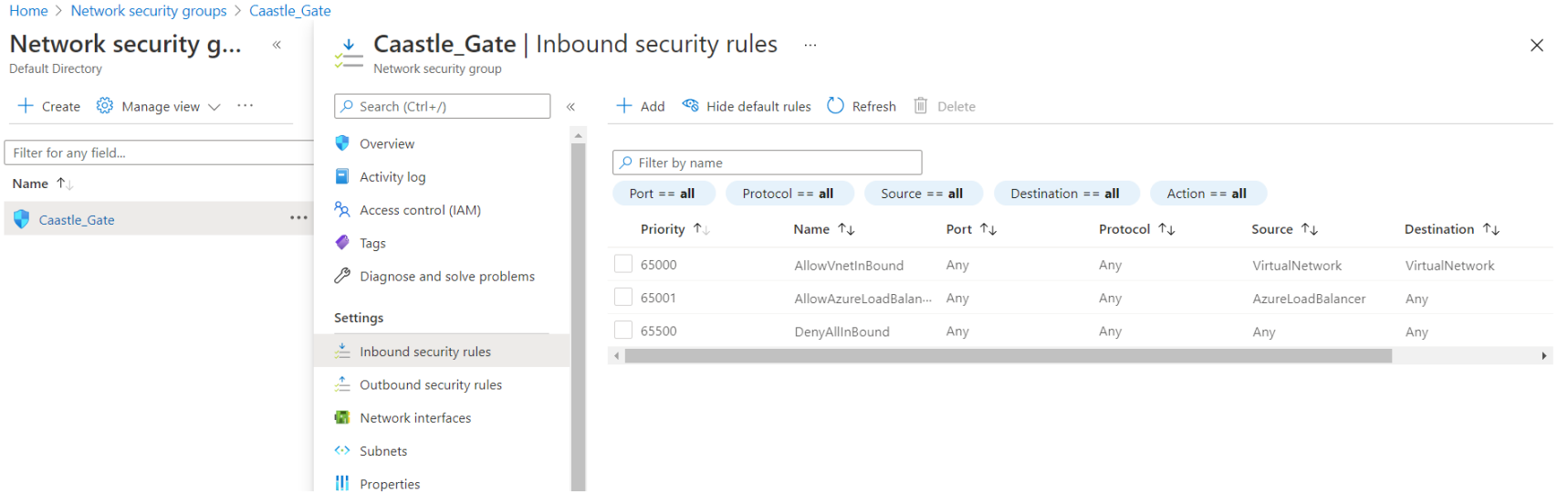
4.a


Home > Network security groups >
Network security g...
Default Directory
Create
Manage view
Filter for any field...
Name
No network security groups to display
Create a network security group with rules to filter inbound traffic to, and outbound traffic from, virtual machines and subnets.
Learn more
Create network security group
Create network security group
Basics
Tags
Review + create
Project details
Subscription *
Azure subscription 1
Resource group *
The_Treasure_Room
Create new
Instance details
Name *
Caastle_Gate
Region *
(US) East US
Review + create
< Previous
Next : Tags >
Download a template for automation

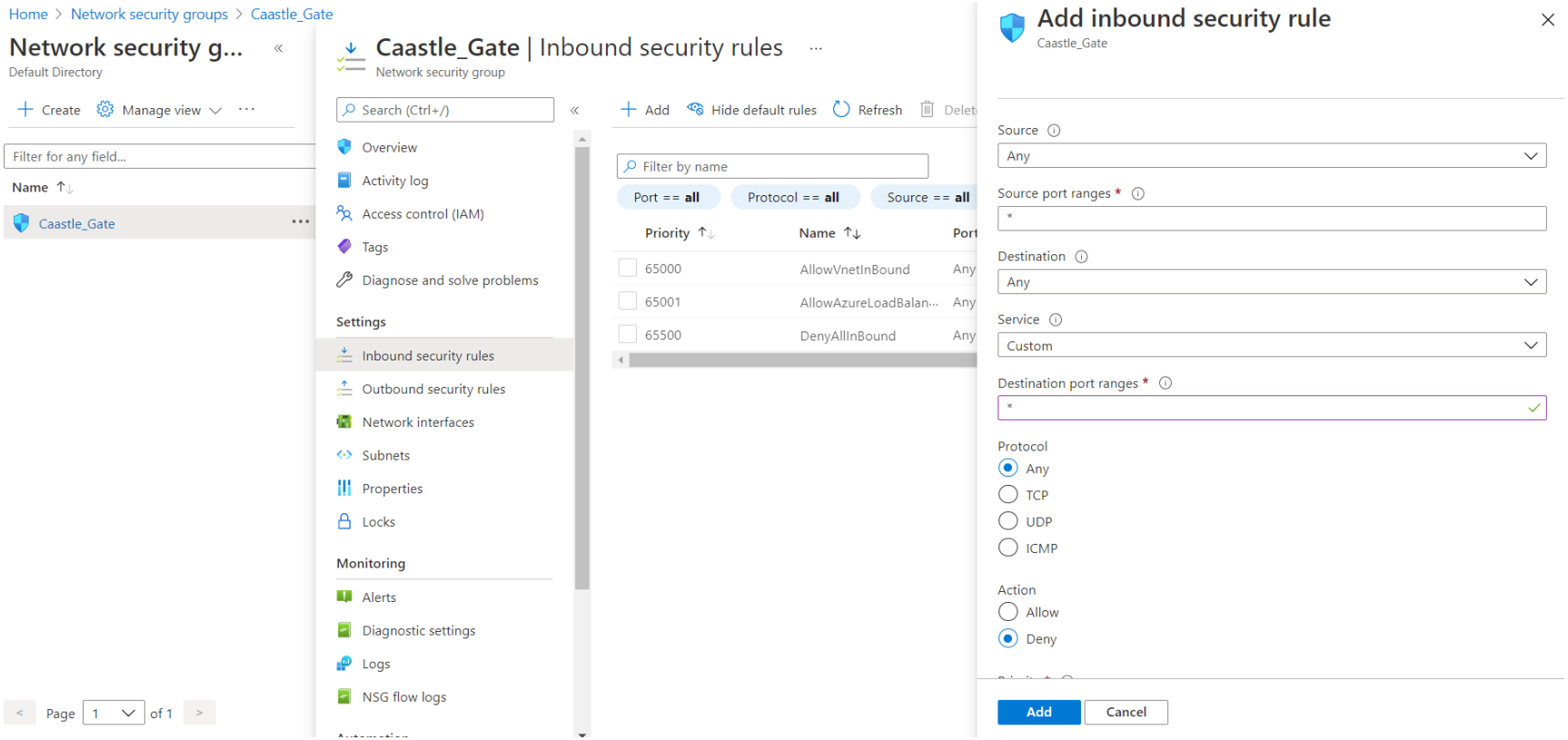
4.b



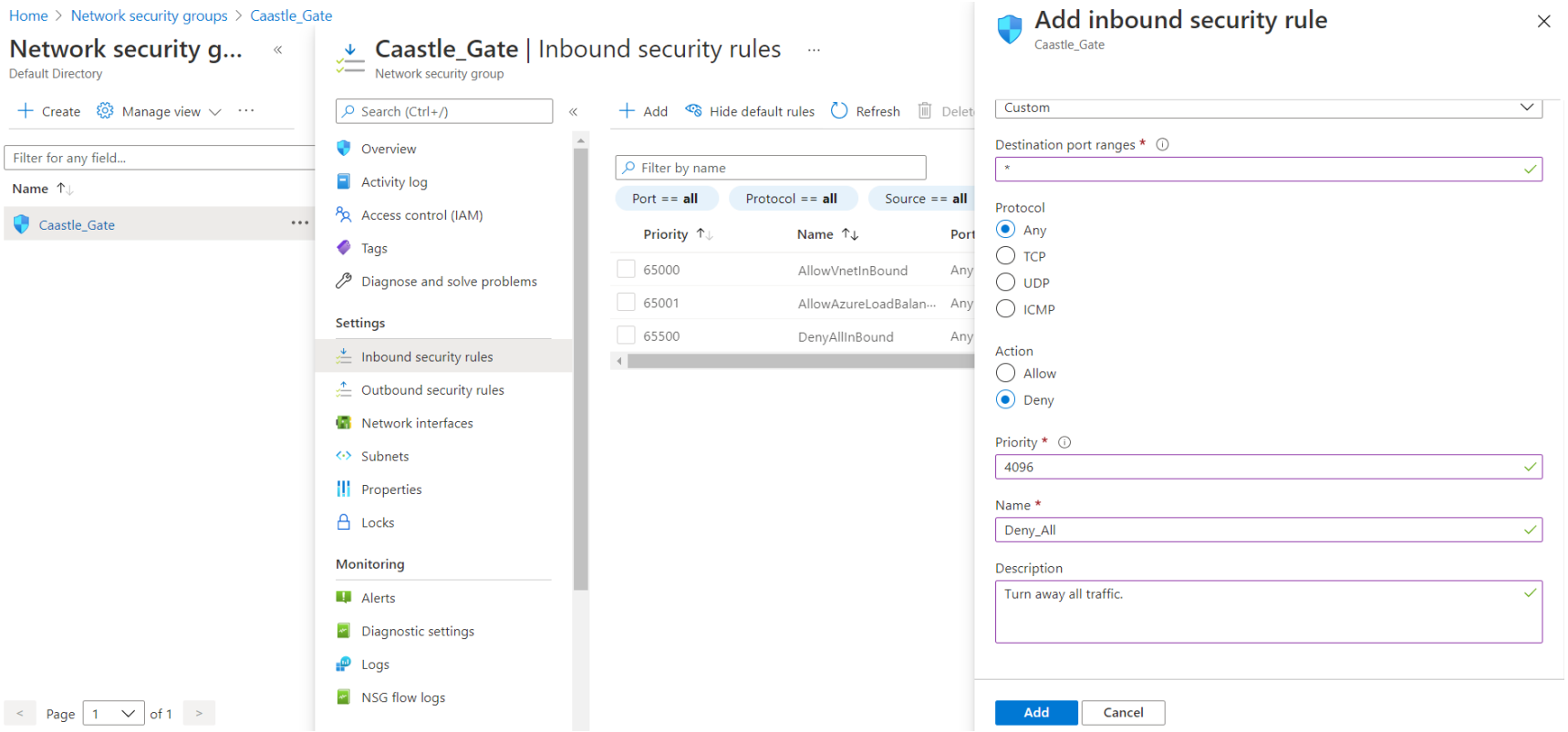
5.-Create an inbound rule



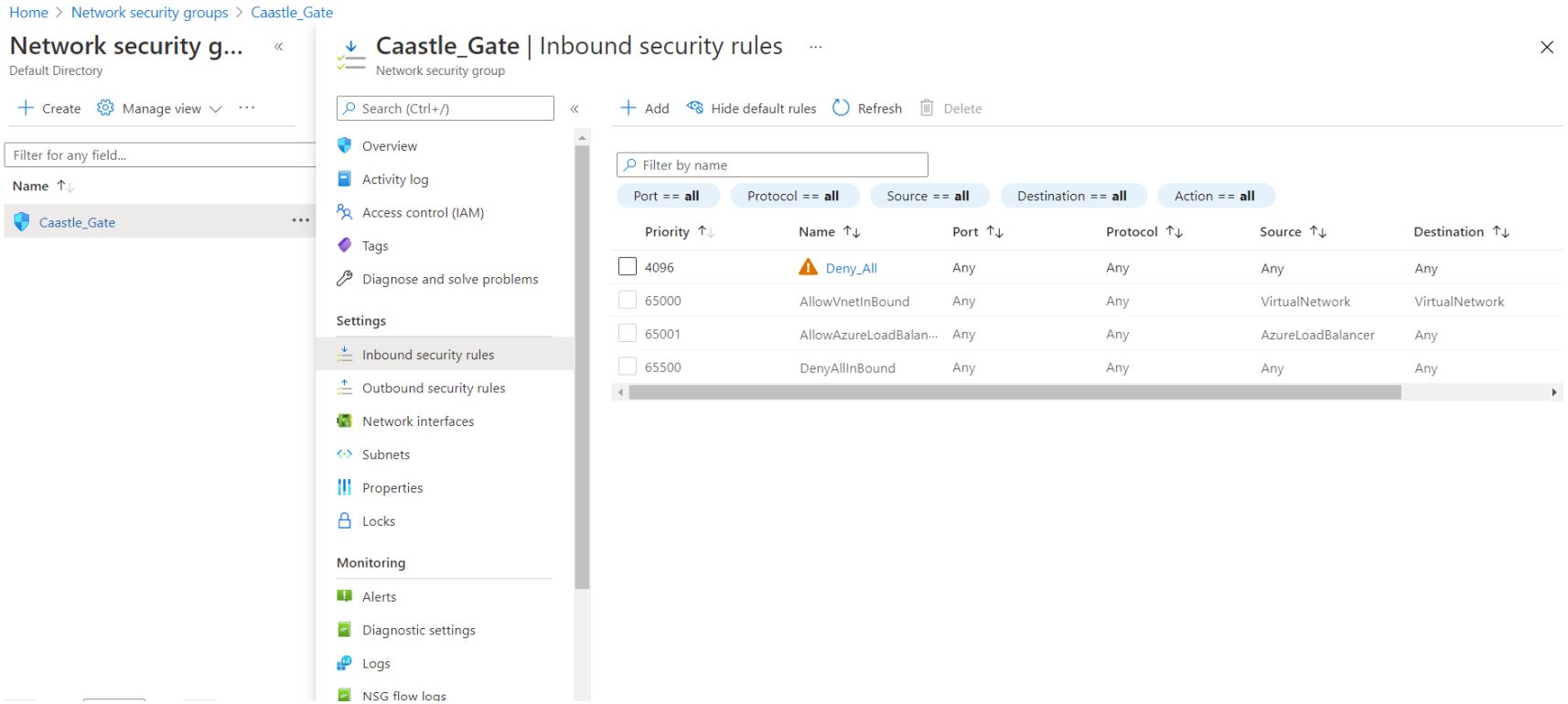
5.a



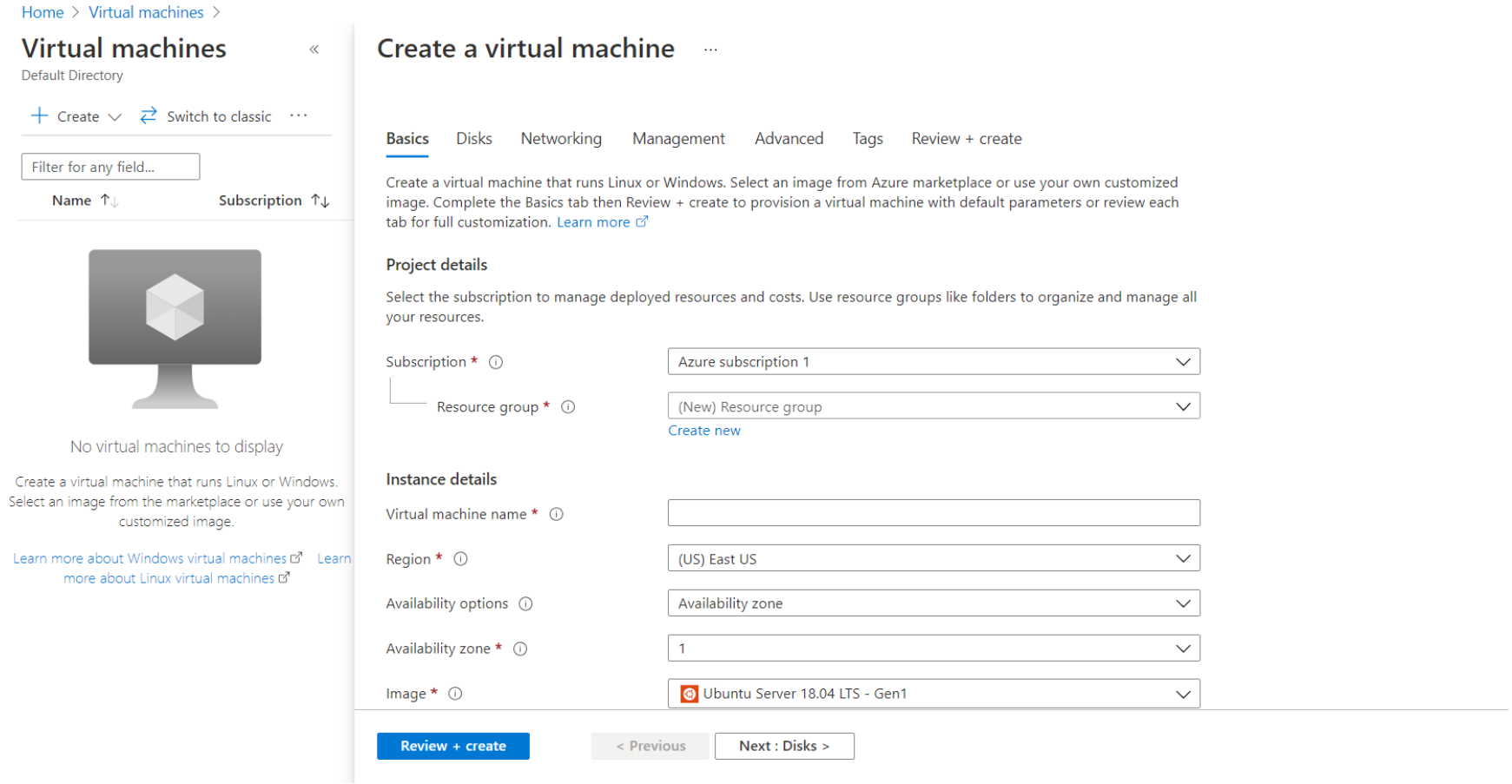
5.b-use ipv4 for source ip


Home > Network security groups > Caastle_Gate
Network security g...
Default Directory
Create
Manage view
Filter for any field...
Name
Caastle_Gate
Page 1 of 1
Caastle_Gate | Inbound security rules
Network security group
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Alerts
Diagnostic settings
Logs
NSG flow logs
Add
Hide default rules
Refresh
Filter by name
Port == all
Protocol == all
Source == all
Priority
Name
65000 AllowVnetInBound Any
65001 AllowAzureLoadBalan... Any
65500 DenyAllInBound Any
Add inbound security rule
Caastle_Gate
Custom
Destination port ranges *
*
Protocol
Any
TCP
UDP
ICMP
Action
Allow
Deny
Priority *
4096
Name *
Deny_All
Description
Turn away all traffic.
Add
Cancel

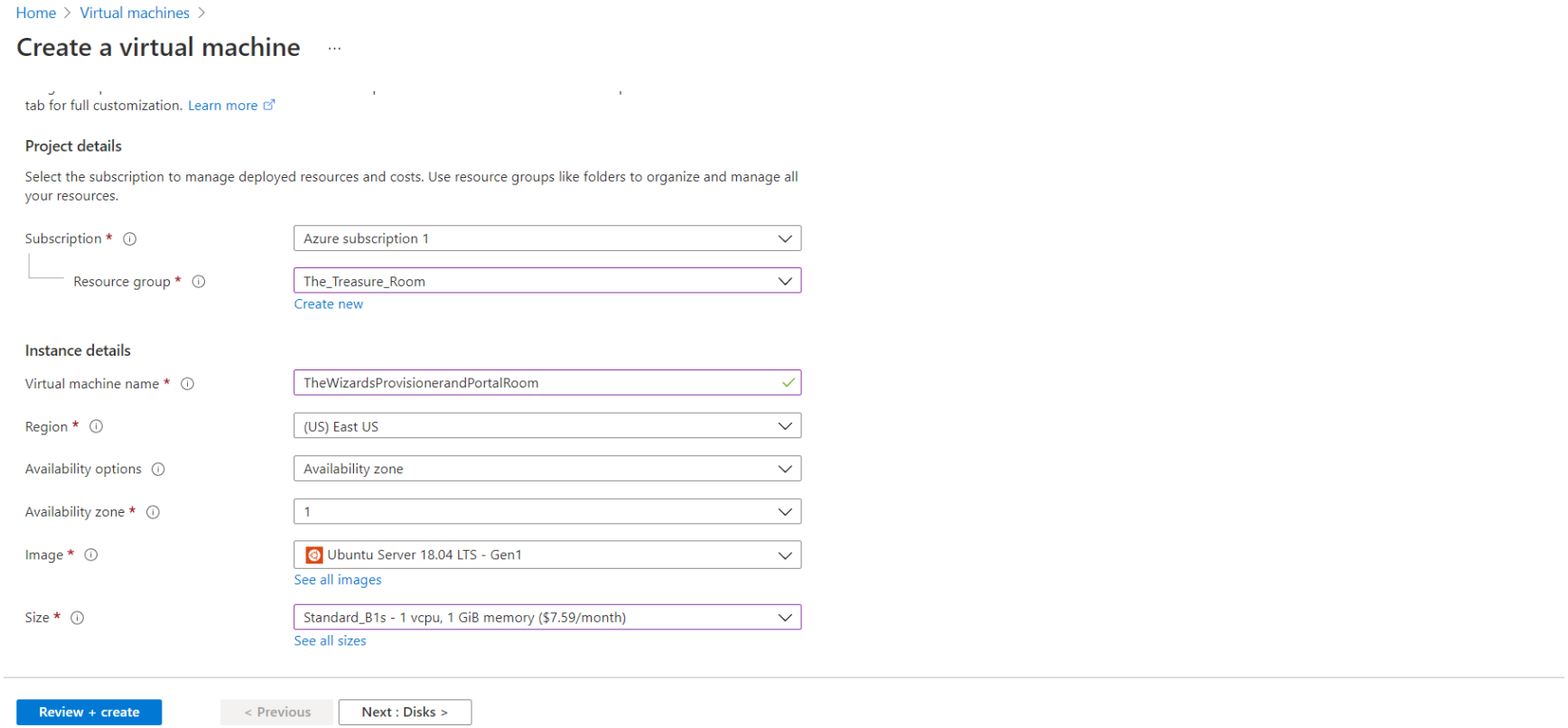
5.c



6.-Creating a virtual machine


Home > Virtual machines >
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
Subscription
No virtual machines to display
Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.
Learn more about Windows virtual machines
Learn more about Linux virtual machines
Create a virtual machine
Basics
Disks
Networking
Management
Advanced
Tags
Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each 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 *
(New) Resource group
Create new
Instance details
Virtual machine name *
Region *
(US) East US
Availability options
Availability zone
Availability zone *
1
Image *
Ubuntu Server 18.04 LTS - Gen1
Review + create
< Previous
Next : Disks >

6.a


Home > Virtual machines >
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 * The_Treasure_Room
Create new
Instance details
Virtual machine name * TheWizardsProvisionerandPortalRoom
Region * (US) East US
Availability options Availability zone
Availability zone * 1
Image * Ubuntu Server 18.04 LTS - Gen1
See all images
Size * Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/month)
See all sizes
Review + create
< Previous
Next : Disks >

6.b

Home > Virtual machines >

Create a virtual machine ...

Size * ⓘ: Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/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 * ⓘ: kingadmin

SSH public key source: Use existing public key

SSH public key * ⓘ:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDLW4tpIqxY2ZP3veVG2vA1zu22
VBaI2CvE3epqoBrSptBnpdnHyZKG1Kn1oOW8Yz3KStzOGU5ViGhRuW+1lY
```

ⓘ Learn more about creating and using SSH keys in Azure

Inbound port rules

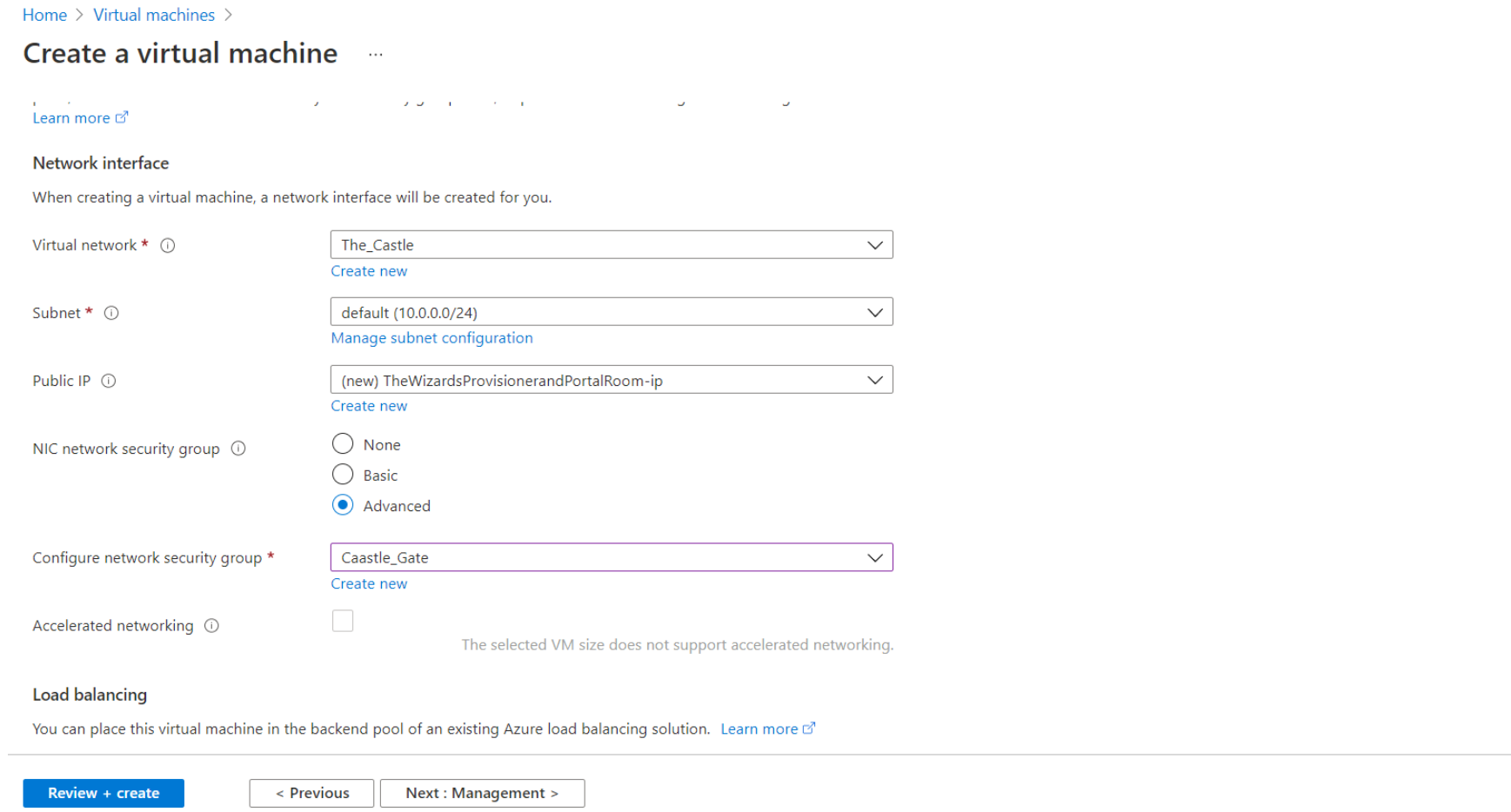
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

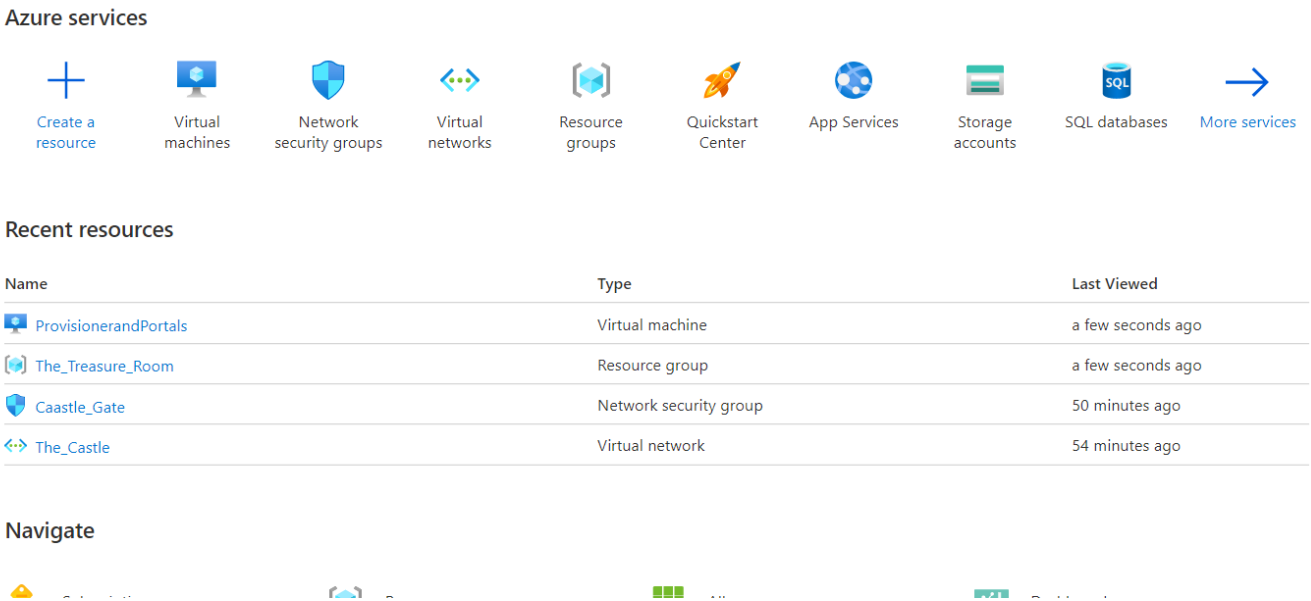
- ( ) None
- (•) Allow selected ports

Review + create | < Previous | Next : Disks >

6.c


Home > Virtual machines >
Create a virtual machine ...
Learn more
Network interface
When creating a virtual machine, a network interface will be created for you.
Virtual network *
The_Castle
Create new
Subnet *
default (10.0.0.0/24)
Manage subnet configuration
Public IP
(new) TheWizardsProvisionerandPortalRoom-ip
Create new
NIC network security group
None
Basic
Advanced
Configure network security group *
Caastle_Gate
Create new
Accelerated networking
The selected VM size does not support accelerated networking.
Load balancing
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more
Review + create
< Previous
Next : Management >

6.d



7.-Create a second VM

Home > Virtual machines >

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 * : The_Treasure_Room

Create new

Instance details

Virtual machine name * : EastTower

Region * : (US) East US

Availability options : Availability set

Availability set * : No existing availability sets in current resource group and location.

Create new

Image * : Ubuntu Server 18.04 LTS - Gen1

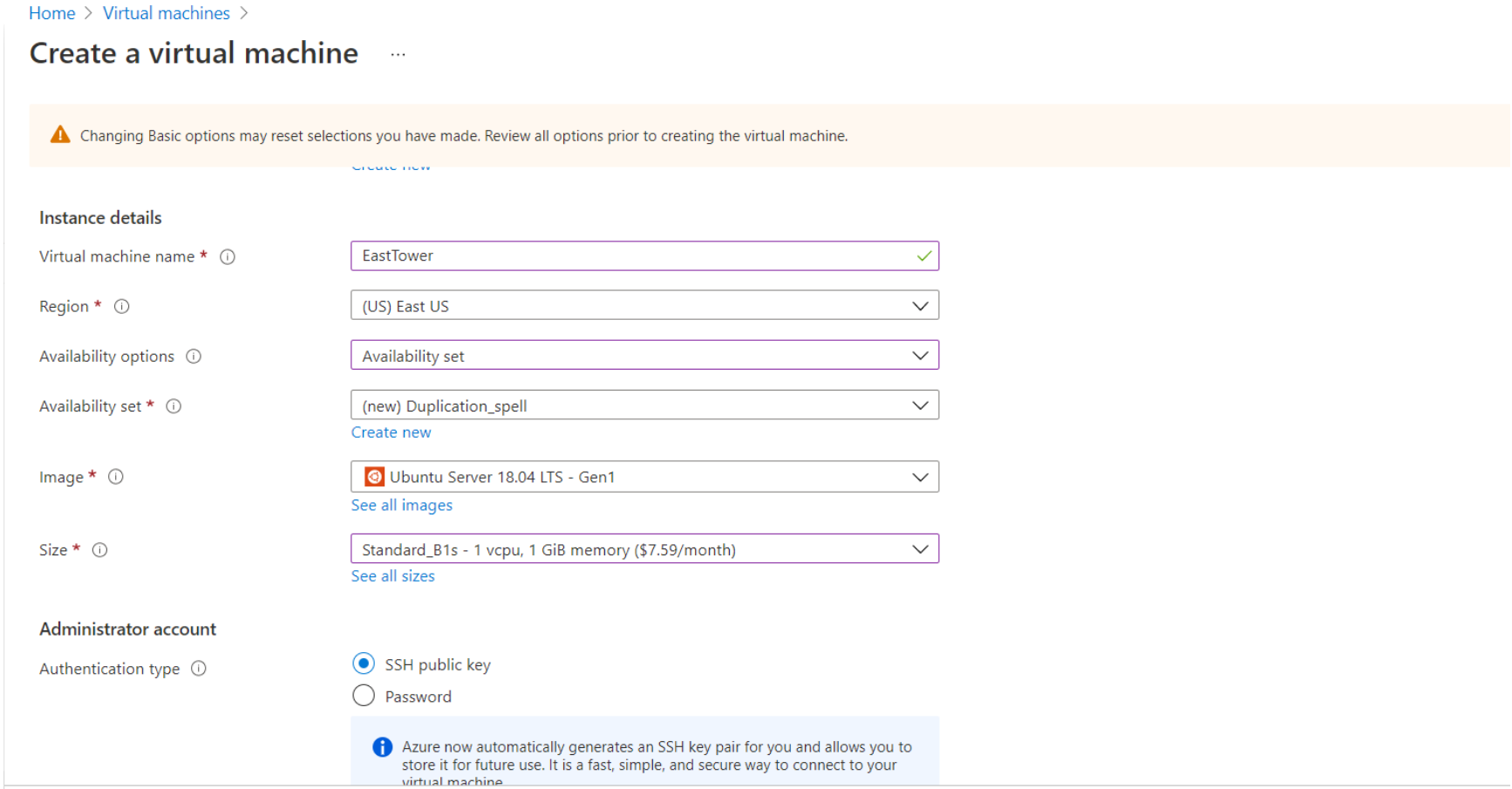
See all images

Size * : Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/month)

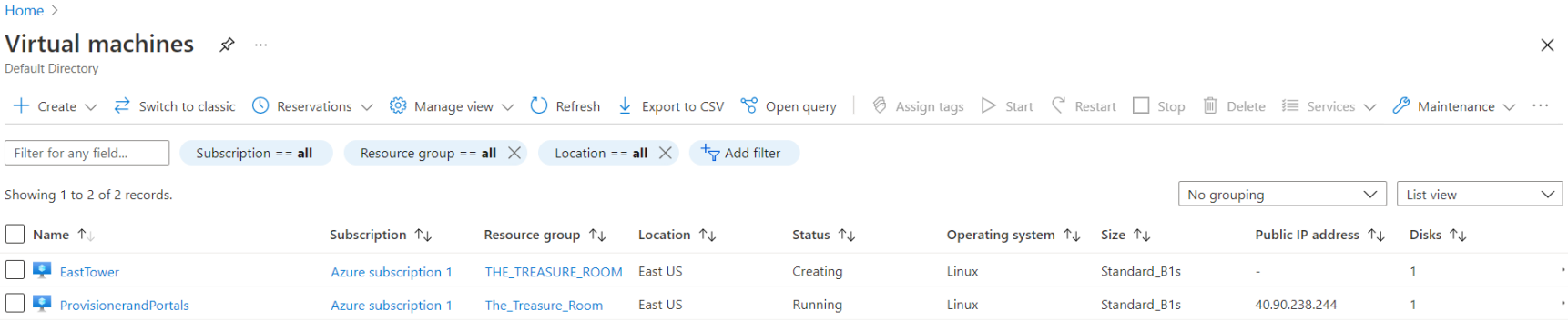
See all sizes

Review + create | < Previous | Next : Disks >

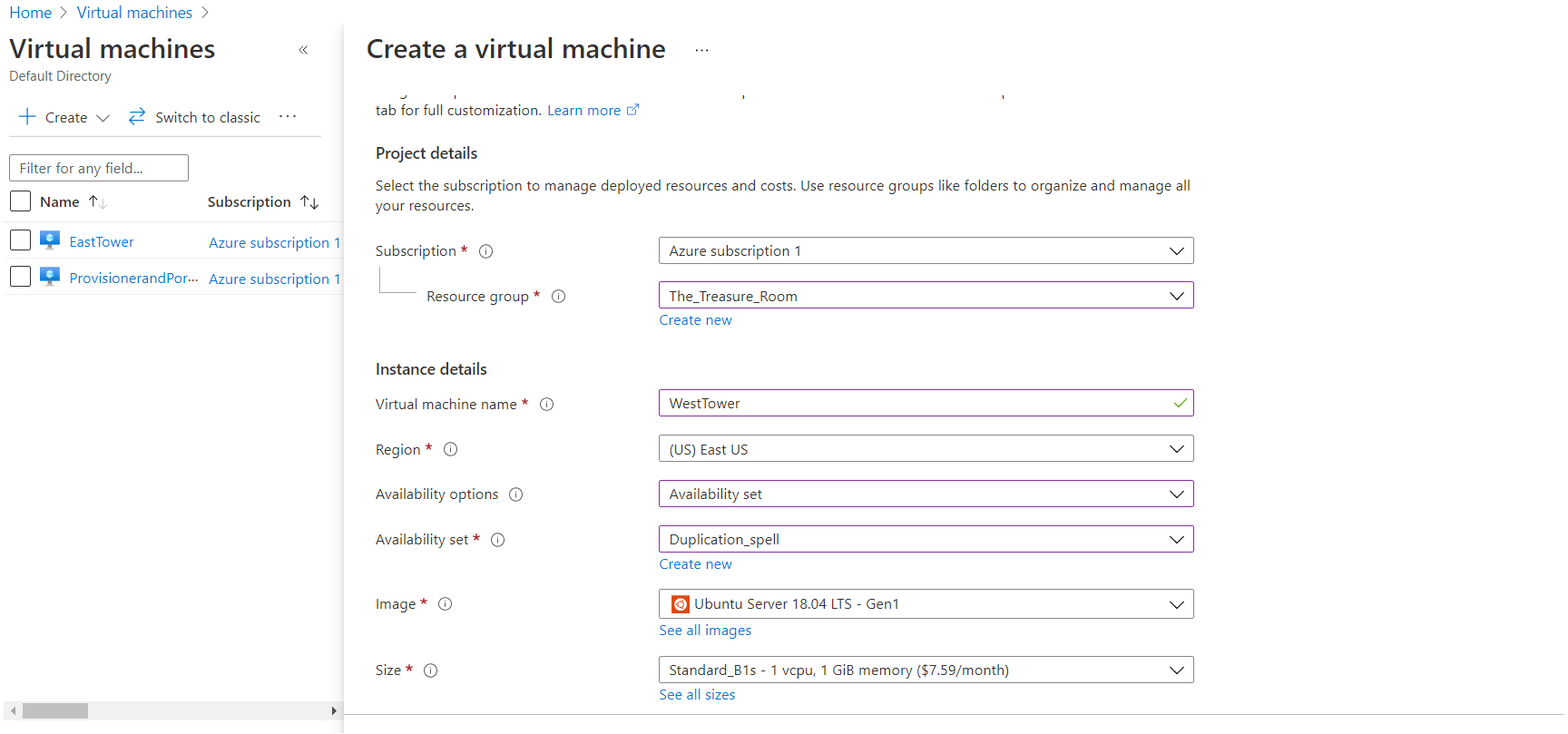
7.a


Home > Virtual machines >
Create a virtual machine ...
Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.
Instance details
Virtual machine name *
EastTower
Region *
(US) East US
Availability options
Availability set
Availability set *
(new) Duplication_spell
Create new
Image *
Ubuntu Server 18.04 LTS - Gen1
See all images
Size *
Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/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.

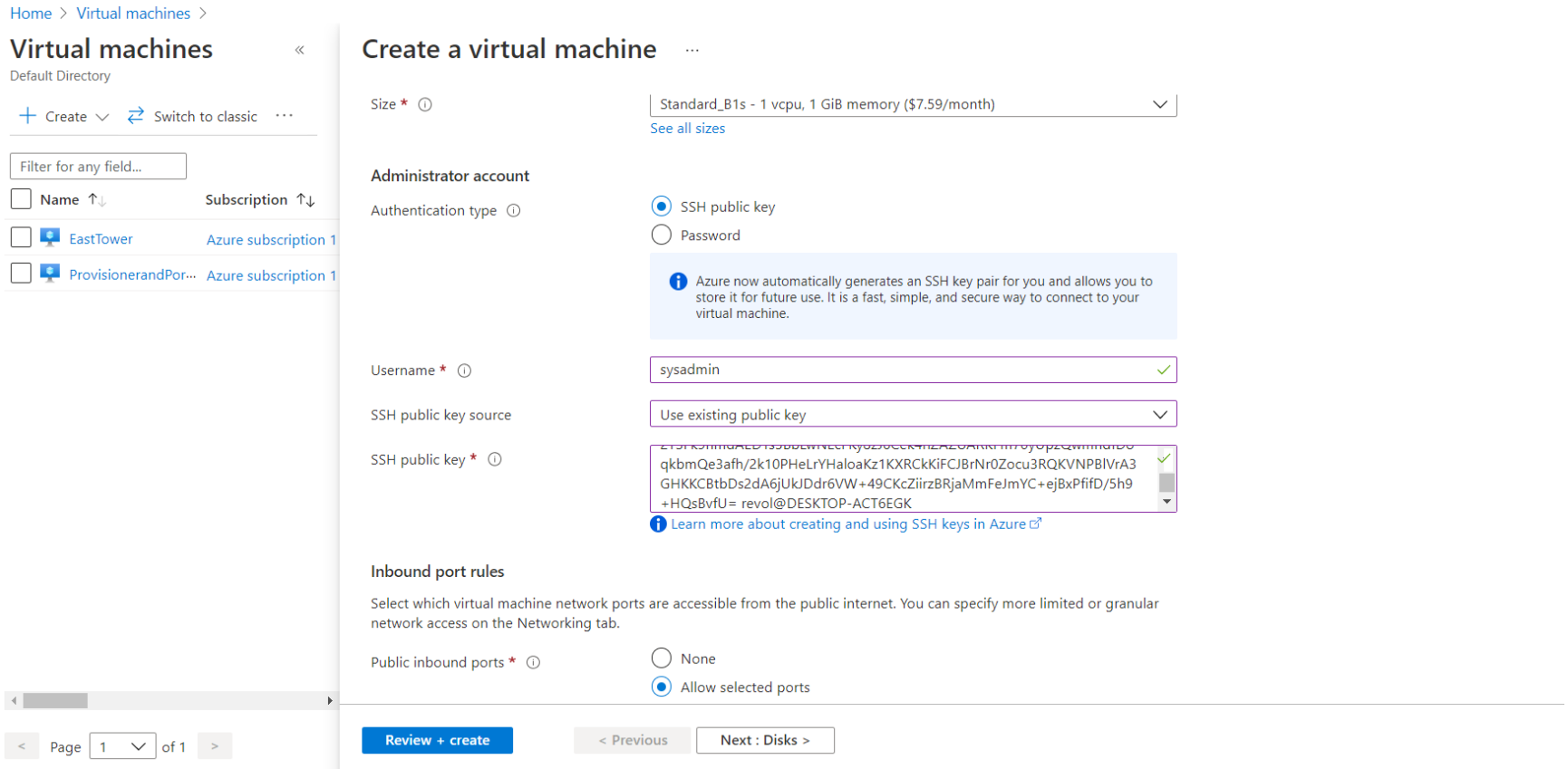
7.b



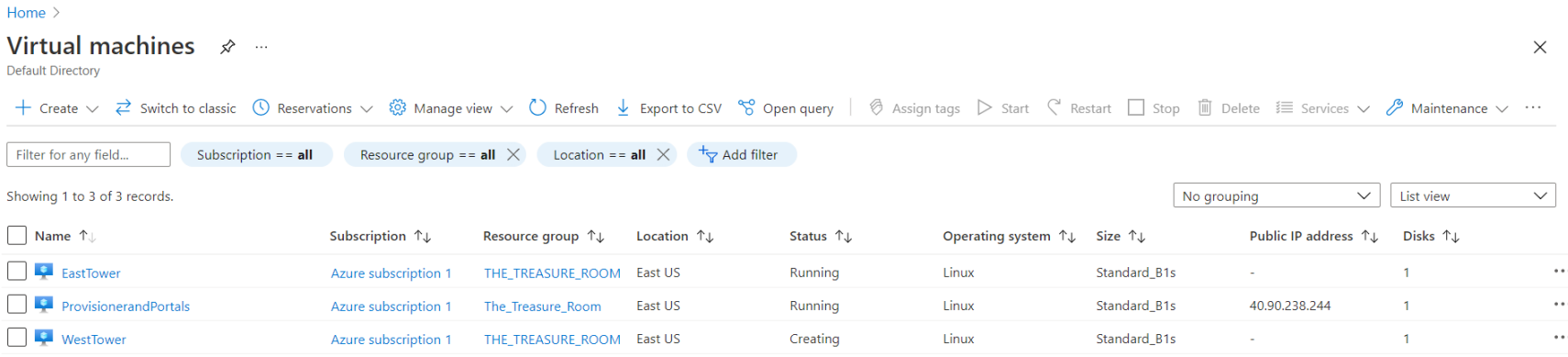
8.-Create another VM


Home > Virtual machines >
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
Subscription
EastTower
Azure subscription 1
ProvisionerandPor...
Azure subscription 1
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 *
The_Treasure_Room
Create new
Instance details
Virtual machine name *
WestTower
Region *
(US) East US
Availability options
Availability set
Availability set *
Duplication_spell
Create new
Image *
Ubuntu Server 18.04 LTS - Gen1
See all images
Size *
Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/month)
See all sizes

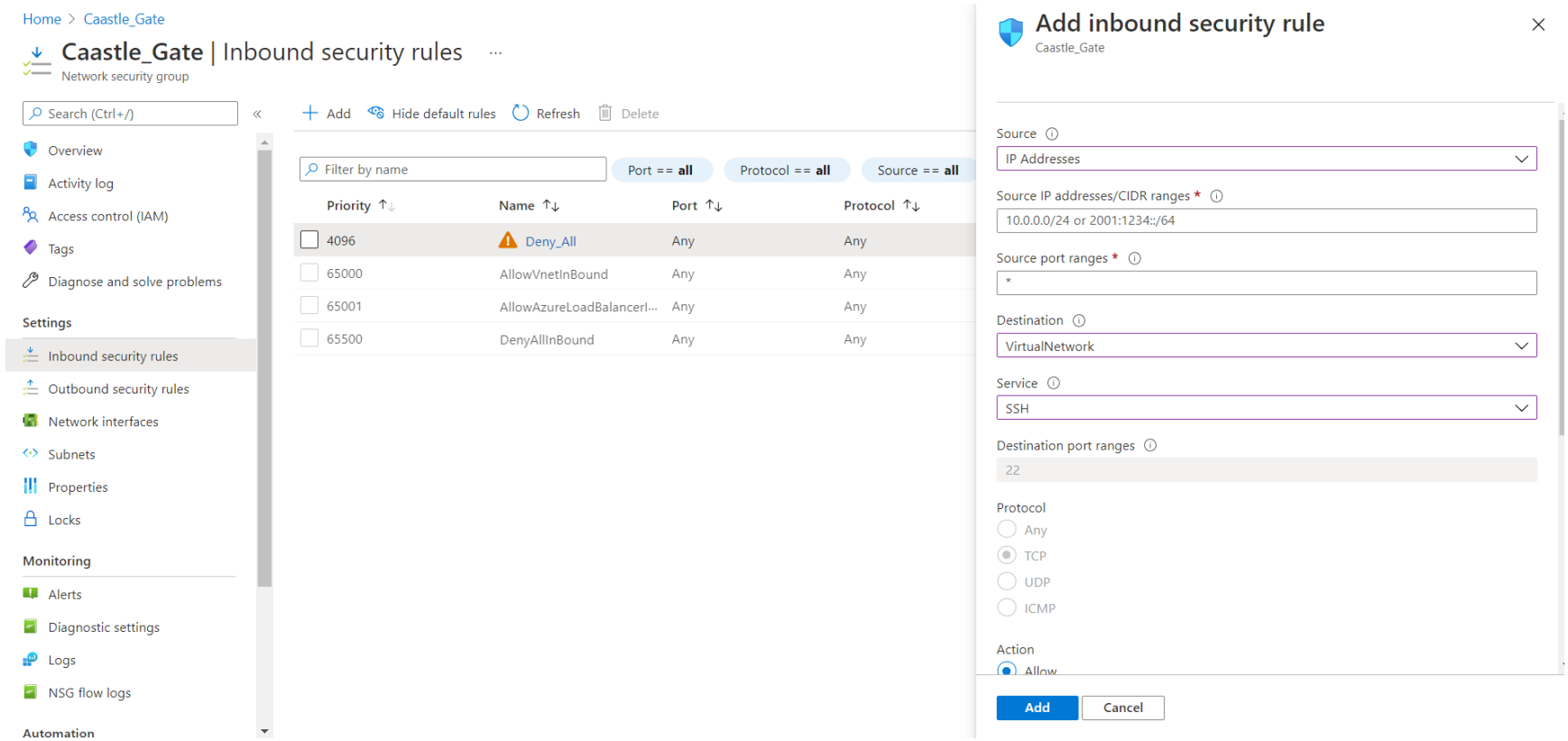
8.a


Home > Virtual machines >
Virtual machines
Default Directory
Create
Switch to classic
Filter for any field...
Name
Subscription
EastTower
Azure subscription 1
ProvisionerandPor...
Azure subscription 1
Page 1 of 1
Create a virtual machine
Size *
Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/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 *
sysadmin
SSH public key source
Use existing public key
SSH public key *
qkbmQe3afh/2k10PHeLrYHaloaKz1KXRCkKiFCJBrNr0Zocu3RQKVNPBlVrA3
GHKKCBtbDs2dA6jUkJDdr6VW+49CKcZiirzBRjaMmFeJmYC+ejBxPfifD/5h9
+HQsBvfU= revol@DESKTOP-ACT6EGK
Learn more about creating and using SSH keys in Azure
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports *
None
Allow selected ports
Review + create
< Previous
Next : Disks >

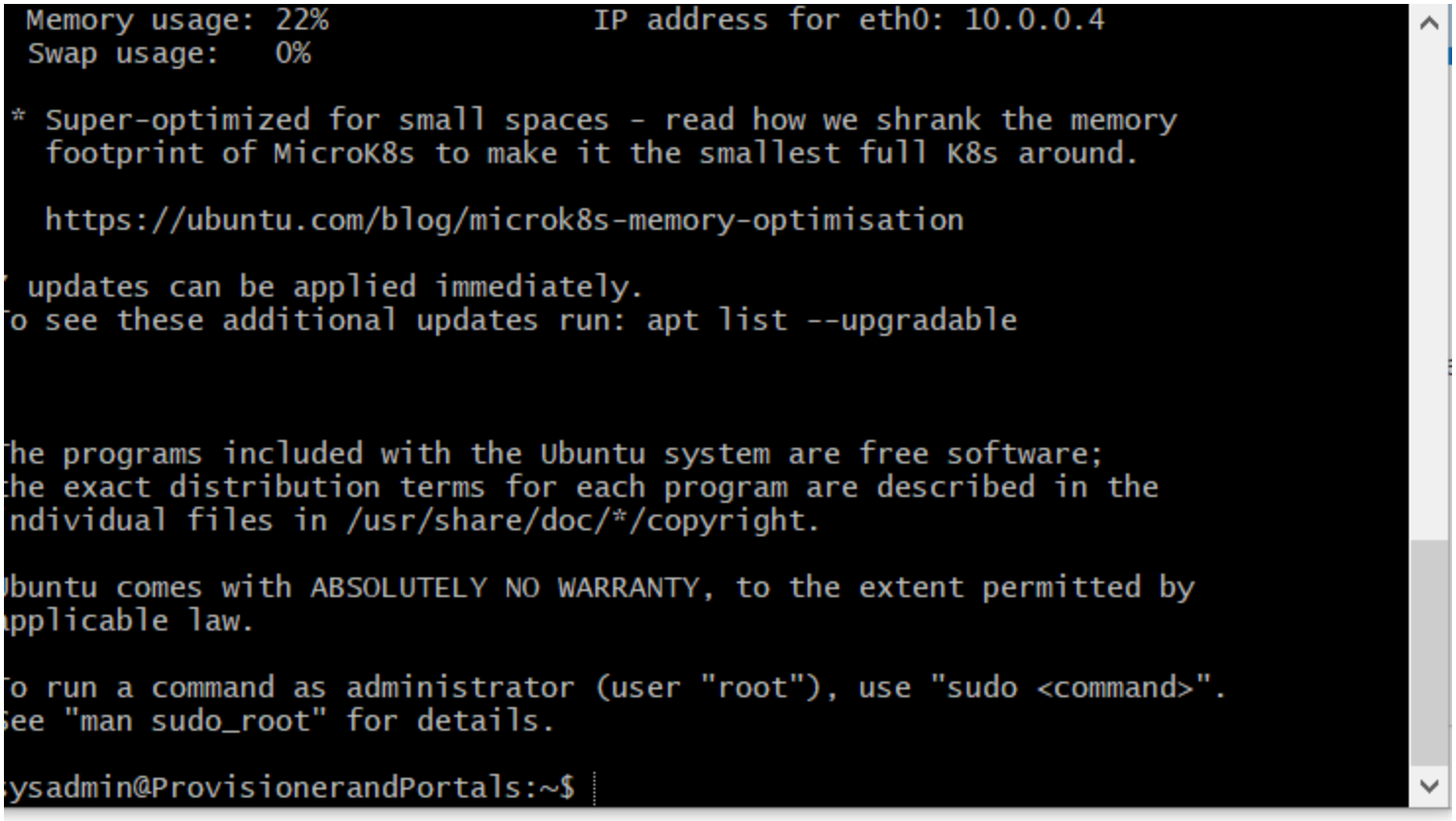
8.2



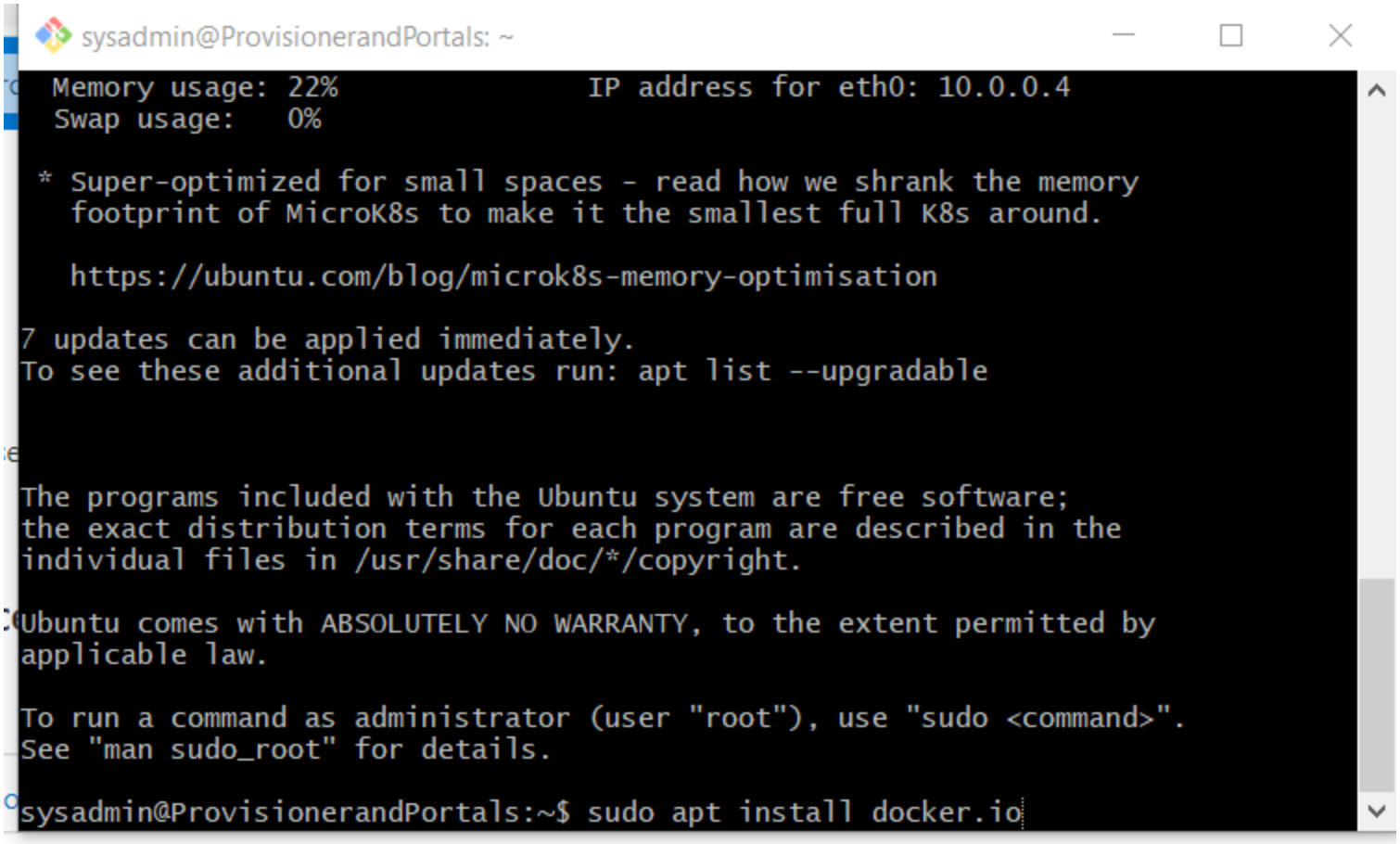
9.-Create an inbound rule for Jumpbox



10.-SSH into the Jump box



11.-install docker



12.-Verify Docker service is running

```
sysadmin@ProvisionerandPortals:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: e
   Active: active (running) since Fri 2021-07-16 20:06:58 UTC; 6min ago
     Docs: https://docs.docker.com
 Main PID: 3367 (dockerd)
    Tasks: 8
   CGroup: /system.slice/docker.service
           └─3367 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/contain

Jul 16 20:06:57 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:57.9
Jul 16 20:06:57 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:57.9
Jul 16 20:06:57 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:57.9
Jul 16 20:06:58 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:58.1
Jul 16 20:06:58 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:58.2
Jul 16 20:06:58 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:58.4
Jul 16 20:06:58 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:58.4
Jul 16 20:06:58 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:58.4
Jul 16 20:06:58 ProvisionerandPortals systemd[1]: Started Docker Application Con
Jul 16 20:06:58 ProvisionerandPortals dockerd[3367]: time="2021-07-16T20:06:58.4
lines 1-19/19 (END)
```

13.- Pull the ansible container

```
sysadmin@ProvisionerandPortals:~$ sudo docker pull cyberxsecurity/ansible
Using default tag: latest
latest: Pulling from cyberxsecurity/ansible
345e3491a907: Pull complete
57671312ef6f: Pull complete
5e9250ddb7d0: Pull complete
06c2579b8983: Pull complete
Digest: sha256:1e59530cfc0fb86b8fefdc2c7b0666e053c9f53a339639fb34e99ffee9812730
Status: Downloaded newer image for cyberxsecurity/ansible:latest
docker.io/cyberxsecurity/ansible:latest
sysadmin@ProvisionerandPortals:~$
```

14.-switch to the root user

```
sysadmin@ProvisionerandPortals:~$ sudo su
root@ProvisionerandPortals:/home/sysadmin#
```

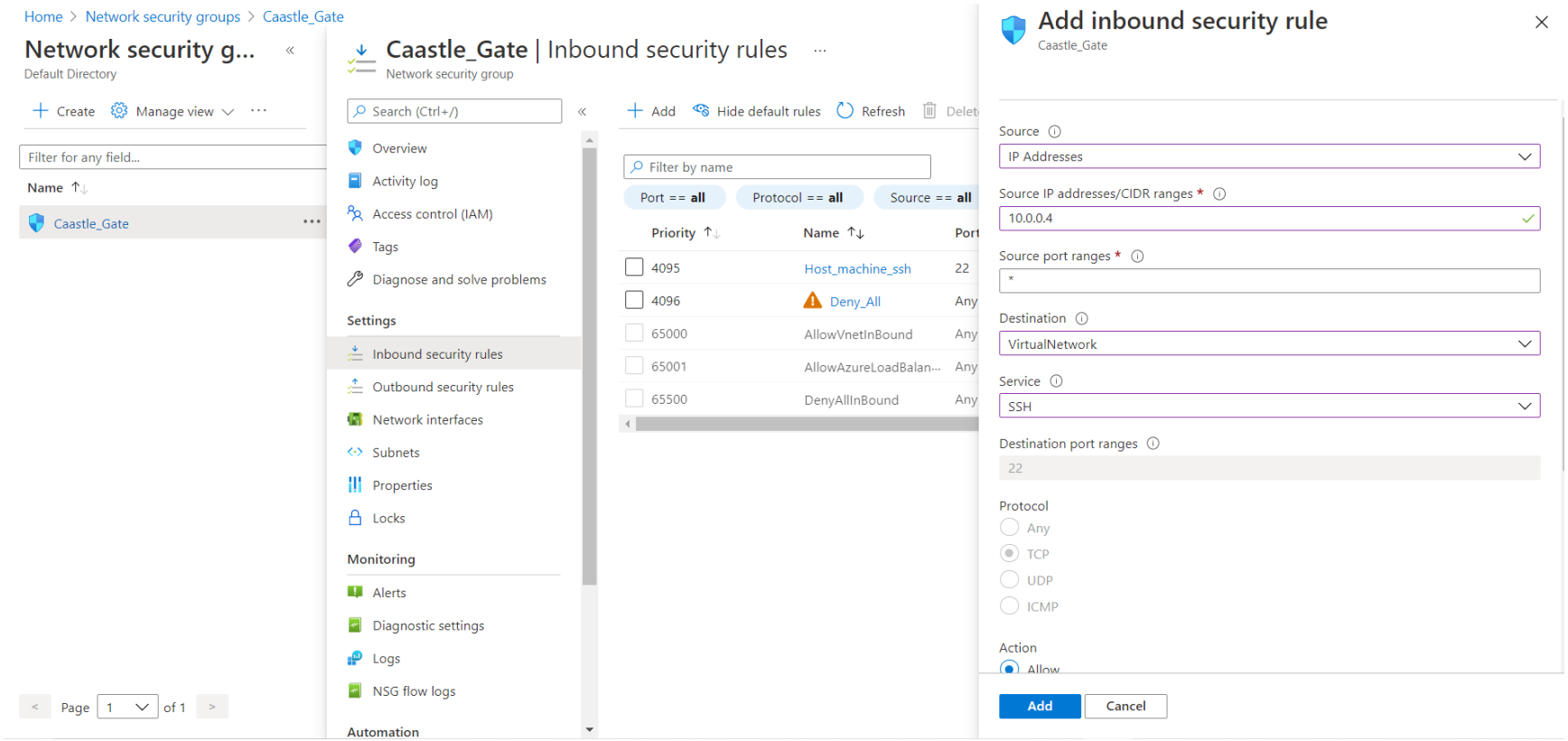
15.Launch ansible and connect to it

```
root@ProvisionerandPortals:/home/sysadmin# docker run -ti cyberxsecurity/ansible
:latest bash
root@4334b593fcd4:~#
```

15.a-exit

```
root@4334b593fcd4:~# exit
root@ProvisionerandPortals:/home/sysadmin#
```

16.-add a rule that allows jump box full access to vnet



17. Connect to ansible container and create a new SSH key

```
root@ProvisionerandPortals:/home/sysadmin# docker container list -a
CONTAINER ID   IMAGE                                COMMAND                  CREATED
    STATUS                      PORTS     NAMES
4334b593fcd4   cyberxsecurity/ansible:latest   "/bin/sh -c /bin/bas…"   11 minutes ag
o   Exited (0) 9 minutes ago                 confident_hopper
root@ProvisionerandPortals:/home/sysadmin#
```

17.a

```
root@ProvisionerandPortals:/home/sysadmin# docker run -it cyberxsecurity/ansible /bin
/bash
root@0ff8035613fc:~#
```

17.b

```
root@0ff8035613fc:~# ssh-keygen
```

17.c

```
root@0ff8035613fc:~# ls .ssh/
id_rsa  id_rsa.pub
root@0ff8035613fc:~# cat .ssh/id-rsa.pub
```

18.-reset the password of the first vm (non-jump box)

Home >

EastTower

Virtual machine

Search (Ctrl+/)

Diagnostic settings

Logs

Connection monitor (classic)

Workbooks

Automation

Tasks (preview)

Export template

Support + troubleshooting

Resource health

Boot diagnostics

Performance diagnostics

Reset password

Redeploy + reapply

Connect

Essentials

Resource group (ch

Status

Location

Subscription (chan

Subscription ID

Tags (change)

Properties

Mc

Virtual mac

Computer na

Operating sy

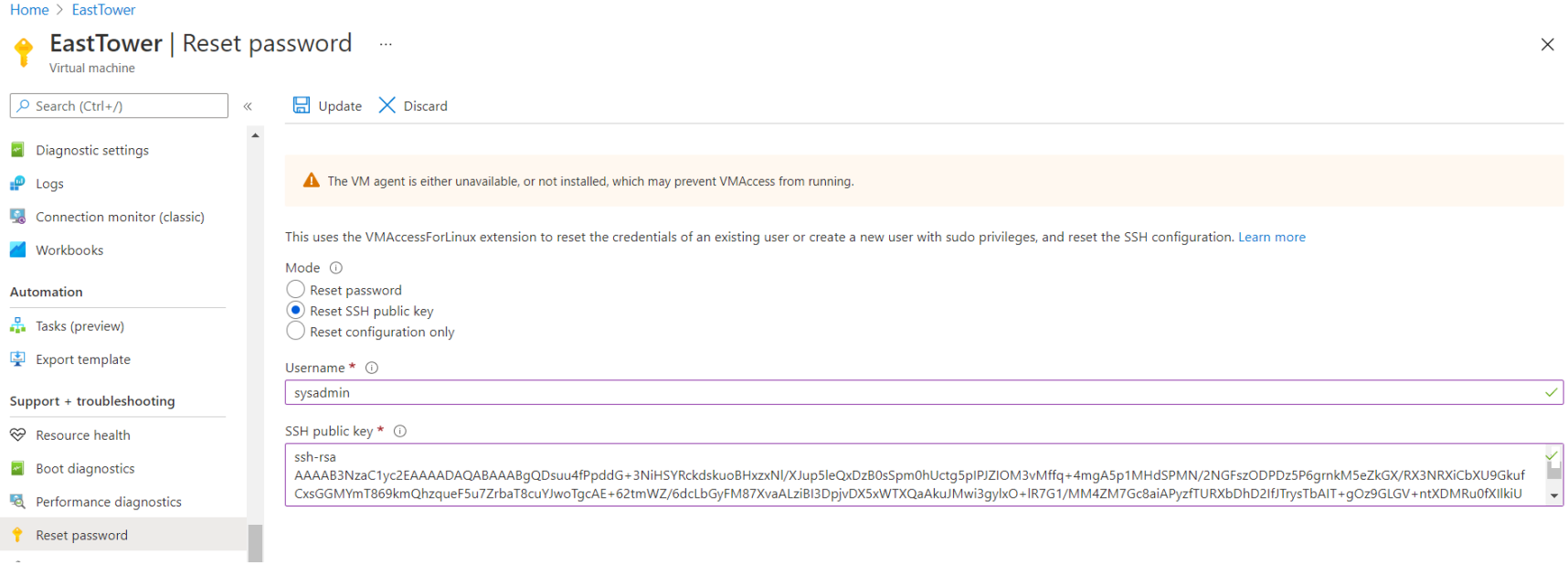
Publisher

Offer

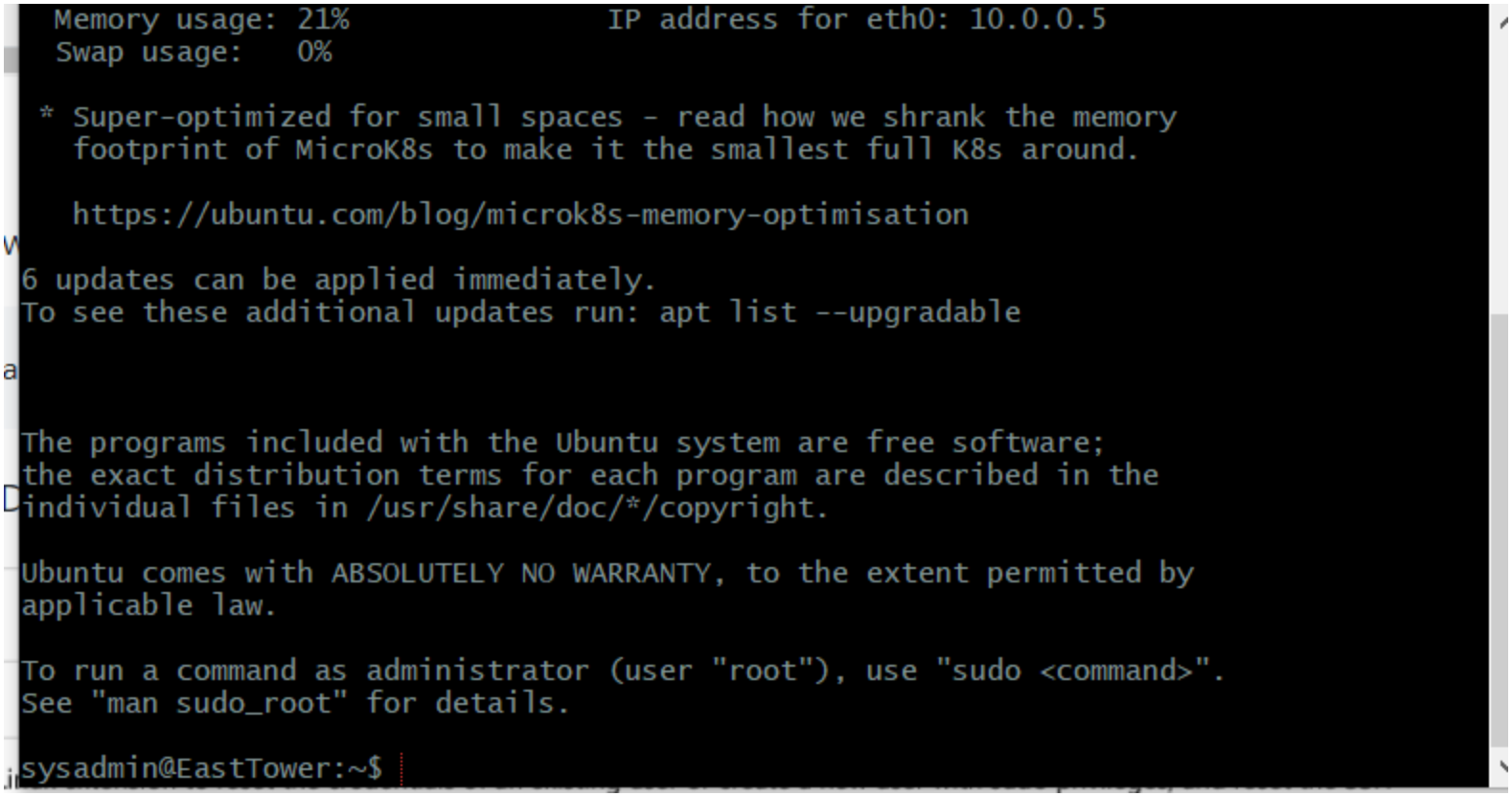
Plan

VM generati

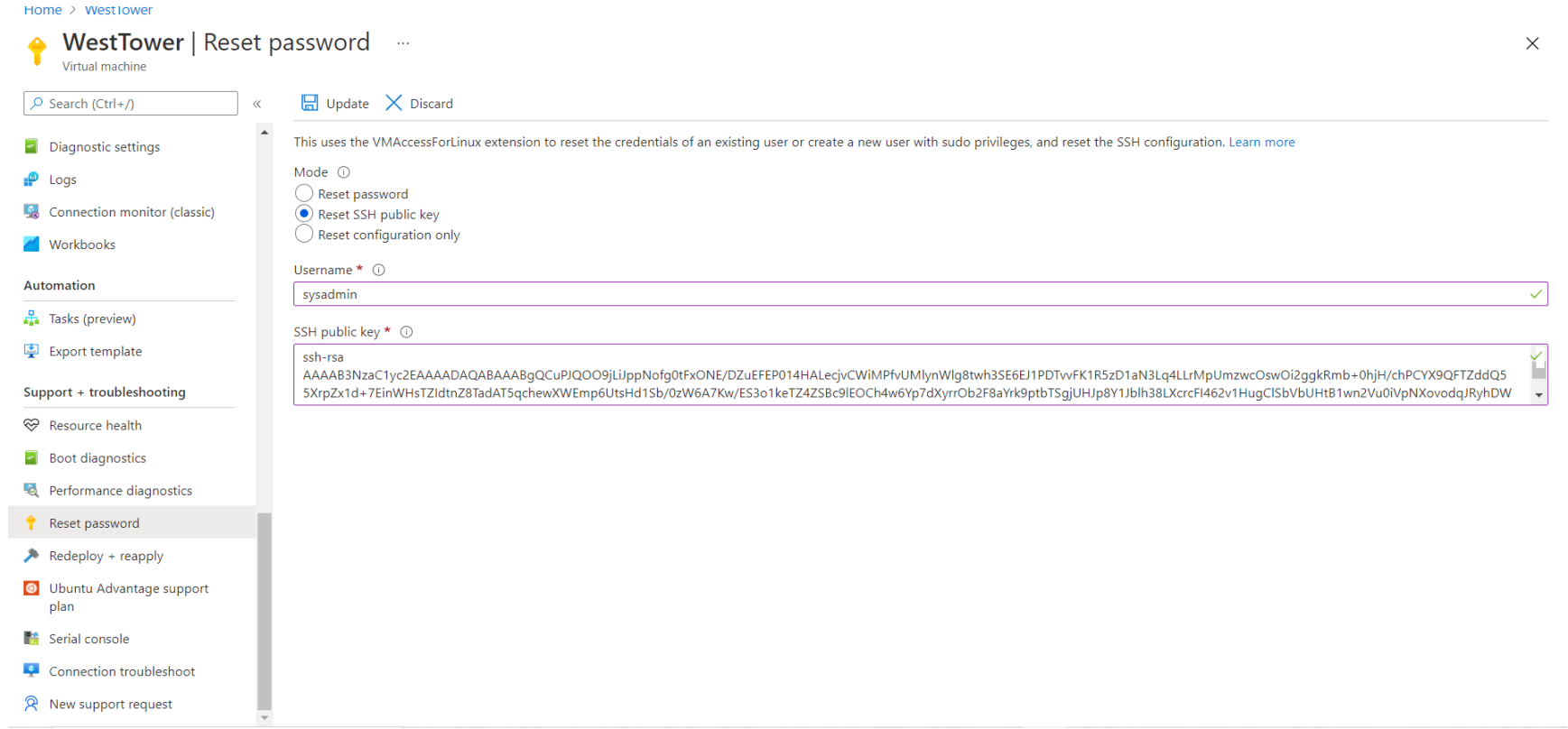
18.a- remove the name in key



19. From the jump box ansible container, SSH into the first vm



20- Save the key in the second vm--show list- sudo docker container list -a ,start docker command- sudo docker start [name of container],docker attach- sudo docker attach [name]


Home > WestTower
WestTower | Reset password
Virtual machine
Search (Ctrl+/)
Update
Discard
Diagnostic settings
Logs
Connection monitor (classic)
Workbooks
Automation
Tasks (preview)
Export template
Support + troubleshooting
Resource health
Boot diagnostics
Performance diagnostics
Reset password
Redeploy + reapply
Ubuntu Advantage support plan
Serial console
Connection troubleshoot
New support request
This uses the VMAccessForLinux extension to reset the credentials of an existing user or create a new user with sudo privileges, and reset the SSH configuration. Learn more
Mode
Reset password
Reset SSH public key
Reset configuration only
Username *
sysadmin
SSH public key *
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCuPJQOO9jLiJppNofg0tFxONE/DZuEFEP014HALecjvCWiMPfvUMlynWlg8twh3SE6EJ1PDTvvFK1R5zD1aN3Lq4LLrMpUmzwcOswOi2ggkRmb+0hjH/chPCYX9QFTZddQ5
5XrpZx1d+7EinWHsTZIdtnZ8TadAT5qchewXWEmp6UtsHd1Sb/0zW6A7Kw/ES3o1keTZ4ZSBc9lEOCh4w6Yp7dXyrrOb2F8aYrk9ptbTSgjUHJp8Y1Jblh38LXcrcFI462v1HugClSbVbUHtB1wn2Vu0iVpNXovodqJRyhDW

20.a

```
  System information as of Tue Jul 20 00:19:15 UTC 2021

  System load:  0.0               Processes:           107
  Usage of /:   4.8% of 28.90GB   Users logged in:     0
  Memory usage: 21%               IP address for eth0: 10.0.0.6
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

7 updates can be applied immediately.
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: Tue Jul 20 00:16:28 2021 from 10.0.0.4
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysadmin@WestTower:~$
```

21-Locate ansible config and host file

```
root@4334b593fcd4:~# ls /etc/ansible
ansible.cfg  hosts
root@4334b593fcd4:~#
```

21.a- open the hosts file

```
root@4334b593fcd4:~# vim /etc/ansible/hosts
```

21.b-uncomment web servers and add the internal ip of vm 1&2 and `ansible_python_interpreter=/usr/bin/python3 next to them` [not jumpbox]

```
[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
```

21.c-open,uncomment, and change the remote user name in the ansible config file

```
# default user to use for playbooks if user is not specified
# (/usr/bin/ansible will use current user as default)
remote_user = sysadmin

# logging is off by default unless this path is defined
# if so defined, consider logrotate
#log_path = /var/log/ansible.log
```

22-test ansible connection

```
root@4334b593fcd4:~# ansible all -m ping
[DEPRECATION WARNING]: Distribution Ubuntu 18.04 on host 10.0.0.6 should use
/usr/bin/python3, but is using /usr/bin/python for backward compatibility with
prior Ansible releases. A future Ansible release will default to using the
discovered platform python for this host. See https://docs.ansible.com/ansible/
2.11/reference_appendices/interpreter_discovery.html for more information. This
 feature will be removed in version 2.12. Deprecation warnings can be disabled
by setting deprecation_warnings=False in ansible.cfg.
10.0.0.6 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python"
    },
    "changed": false,
    "ping": "pong"
}
10.0.0.5 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

23.-Create a YAML playbook

```
root@4334b593fcd4:~# vim /etc/ansible/pentest.yml
```

23.a-

```yaml
---
- name: Config Web VMs with Docker
  hosts: webservers
  become: true
  tasks:
  - name: docker.io
    apt:
      force_apt_get: yes
      update_cache: yes
      name: docker.io
      state: present

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

  - name: Install Docker pyhton module
    pip:
      name: docker
      state: present

  - name: download and launch docker web container
    docker_container:
      name: dvwa
      image: cyberxsecurity/dvwa
      state: started
      published_ports: 80:80

  - name: Enable docker service
    systemd:
      name: docker
      enabled: yes
```

24. Run the playbook

```
root@4334b593fcd4:~# ansible-playbook /etc/ansible/pentest.yml
```

24.a-

```
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly calculated text widths that can cause Display to print incorrect line lengths

PLAY [Config Web VMs with Docker] ***********************************************************************************************************************************************************************************

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

TASK [docker.io] ****************************************************************************************************************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Install pip3] *************************************************************************************************************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Install Docker pyhton module] *********************************************************************************************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [download and launch docker web container] *********************************************************************************************************************************************************************
[DEPRECATION WARNING]: The container_default_behavior option will change its default value from "compatibility" to "no_defaults" in community.docker 2.0.0. To remove this warning, please specify an explicit
value for it now. This feature will be removed from community.docker in version 2.0.0. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Enable docker service] ****************************************************************************************************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

PLAY RECAP **********************************************************************************************************************************************************************************************************
10.0.0.5                   : ok=6    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.6                   : ok=6    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

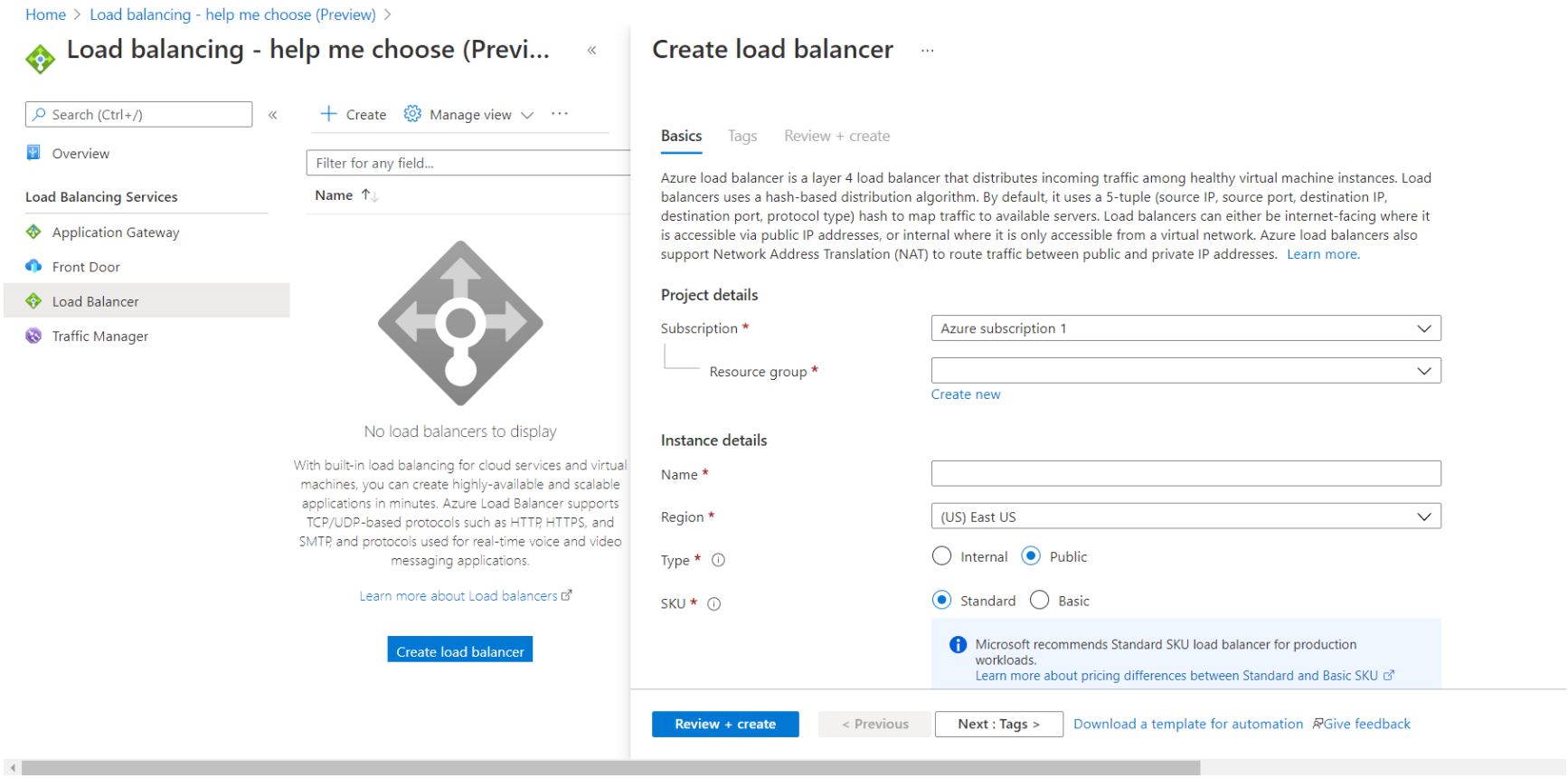
25.-Test dvwa by ssh into web 1 and run `curl localhost/setup.php`

```
sysadmin@EastTower:~$ curl localhost/setup.php
<!DOCTYPE html>

<html lang="en-GB">

        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

                <title>Setup :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>

                <link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

                <link rel="icon" type="\image/ico" href="favicon.ico" />

                <script type="text/javascript" src="dvwa/js/dvwaPage.js"></script>

        </head>

        <body class="home">
                <div id="container">

                        <div id="header">

                                <img src="dvwa/images/logo.png" alt="Damn Vulnerable Web Application" />

                        </div>

                        <div id="main_menu">

                                <div id="main_menu_padded">
                                <ul class="menuBlocks"><li class="selected"><a href="setup.php">Setup DVWA</a></li>
<li class=""><a href="instructions.php">Instructions</a></li>
</ul><ul class="menuBlocks"><li class=""><a href="about.php">About</a></li>
</ul>
                                </div>
```

25.a

```
sysadmin@WestTower:~$ curl localhost/setup.php
<!DOCTYPE html>

<html lang="en-GB">

        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

                <title>Setup :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>

                <link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

                <link rel="icon" type="\image/ico" href="favicon.ico" />

                <script type="text/javascript" src="dvwa/js/dvwaPage.js"></script>

        </head>

        <body class="home">
                <div id="container">

                        <div id="header">

                                <img src="dvwa/images/logo.png" alt="Damn Vulnerable Web Application" />

                        </div>

                        <div id="main_menu">

                                <div id="main_menu_padded">
                                <ul class="menuBlocks"><li class="selected"><a href="setup.php">Setup DVWA</a></li>
<li class=""><a href="instructions.php">Instructions</a></li>
</ul><ul class="menuBlocks"><li class=""><a href="about.php">About</a></li>
</ul>
                                </div>

                        </div>

                        <div id="main_body">
```

26-create a load balancer and give a static ip


Home > Load balancing - help me choose (Preview) >
Load balancing - help me choose (Previ...
Search (Ctrl+/)
Overview
Load Balancing Services
Application Gateway
Front Door
Load Balancer
Traffic Manager
Create
Manage view
Filter for any field...
Name
No load balancers to display
With built-in load balancing for cloud services and virtual machines, you can create highly-available and scalable applications in minutes. Azure Load Balancer supports TCP/UDP-based protocols such as HTTP, HTTPS, and SMTP, and protocols used for real-time voice and video messaging applications.
Learn more about Load balancers
Create load balancer
Create load balancer
Basics
Tags
Review + create
Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. Learn more.
Project details
Subscription *
Azure subscription 1
Resource group *
Create new
Instance details
Name *
Region *
(US) East US
Type *
Internal
Public
SKU *
Standard
Basic
Microsoft recommends Standard SKU load balancer for production workloads.
Learn more about pricing differences between Standard and Basic SKU
Review + create
< Previous
Next : Tags >
Download a template for automation
Give feedback

26.a

Create load balancer ...

Basics Tags Review + create

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. Learn more.

Project details

Subscription * Azure subscription 1

Resource group * The_Treasure_Room

Create new

Instance details

Name * The_Towers_load_balancer

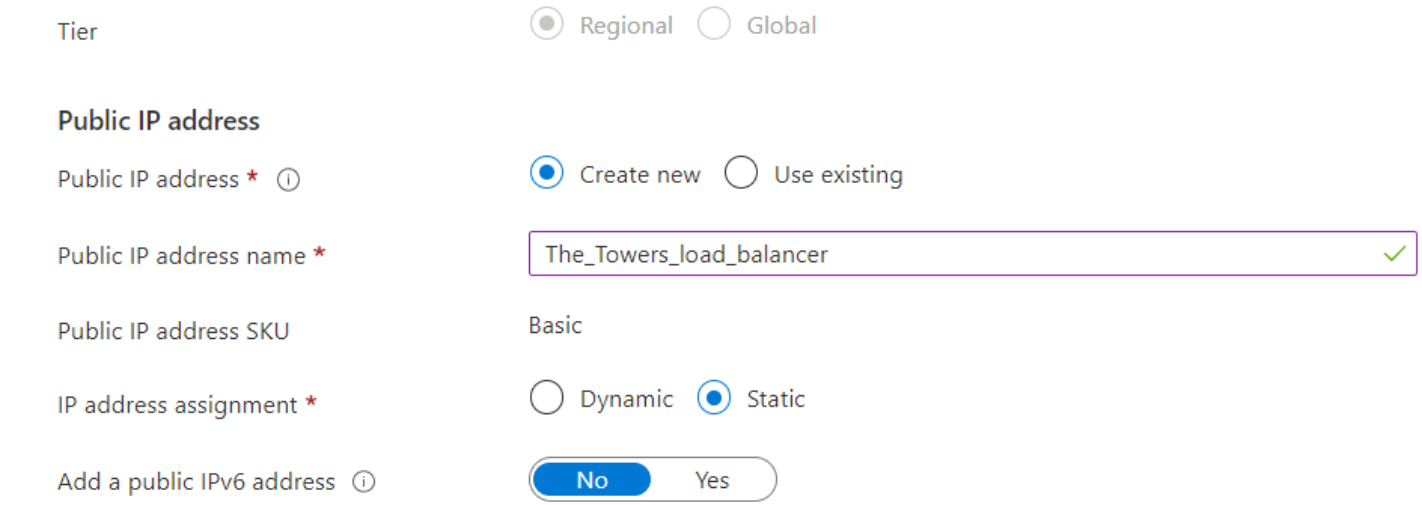
Region * (US) East US

Type * ⓘ ○ Internal ◉ Public

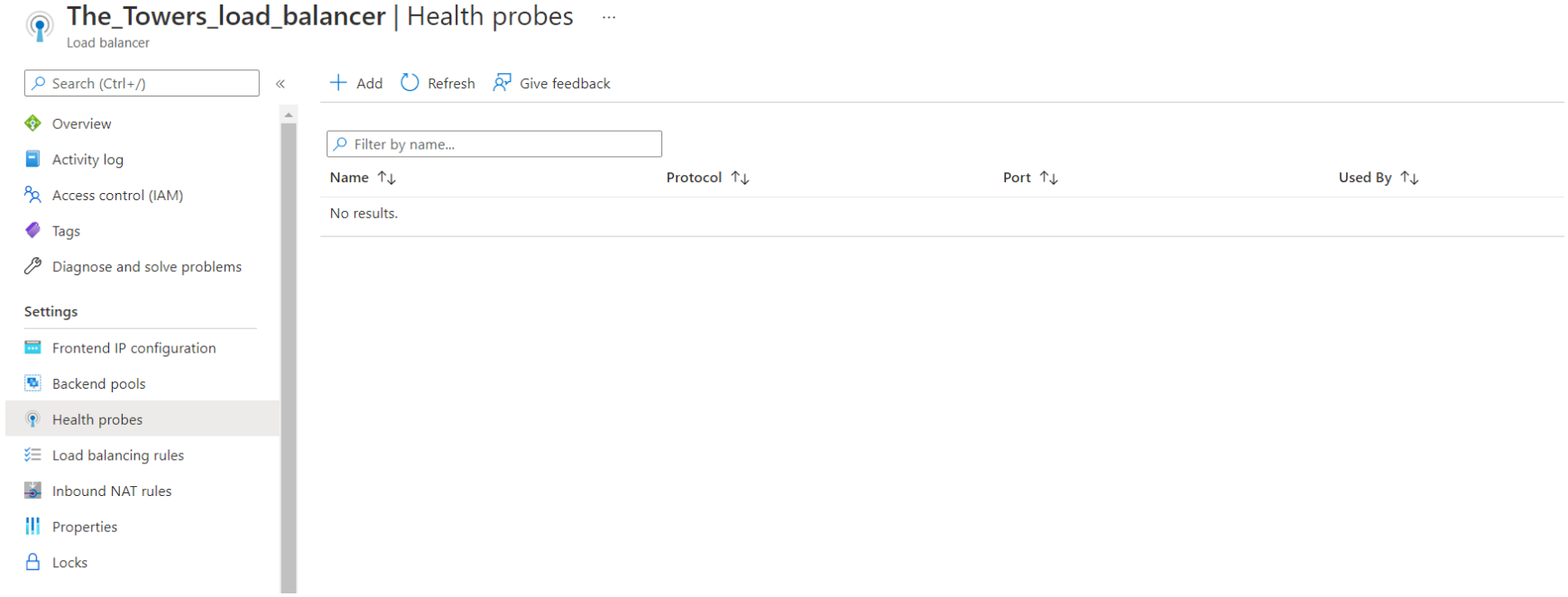
SKU * ⓘ ○ Standard ◉ Basic

ⓘ Microsoft recommends Standard SKU load balancer for production workloads.
Learn more about pricing differences between Standard and Basic SKU

26.b



27-add a health probe


The_Towers_load_balancer | Health probes
Load balancer
Search (Ctrl+/)
Add
Refresh
Give feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Frontend IP configuration
Backend pools
Health probes
Load balancing rules
Inbound NAT rules
Properties
Locks
Filter by name...
Name
Protocol
Port
Used By
No results.

27.a-

Add health probe

The_Towers_load_balancer

Name *: Towers_Sentry_Probe

Protocol *: TCP

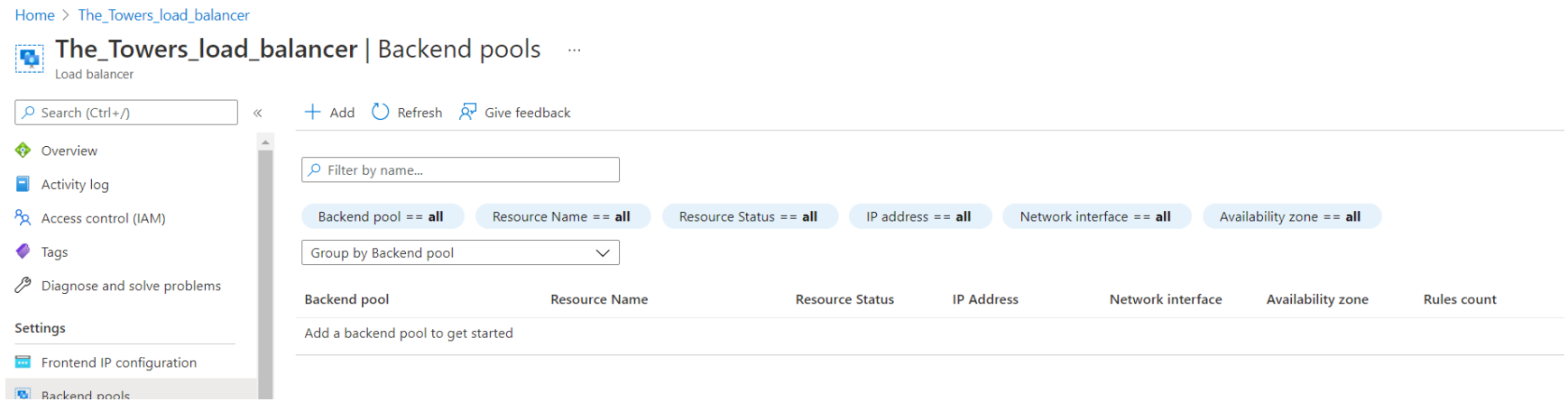
Port *: 80

Interval *: 5 seconds

Unhealthy threshold *: 2 consecutive failures

Used by: Not used

27.b-create backend pool


Home > The_Towers_load_balancer
The_Towers_load_balancer | Backend pools
Load balancer
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Frontend IP configuration
Backend pools
Add
Refresh
Give feedback
Filter by name...
Backend pool == all
Resource Name == all
Resource Status == all
IP address == all
Network interface == all
Availability zone == all
Group by Backend pool
Backend pool
Resource Name
Resource Status
IP Address
Network interface
Availability zone
Rules count
Add a backend pool to get started

27.c

Home > The_Towers_load_balancer >

Add backend pool ...

Name *

The_Towers_load_balancer_treasurer

Virtual network * ⓘ

The_Castle (The_Treasure_Room)

Associated to ⓘ

Virtual machines

IP Version

- (•) IPv4
- ( ) IPv6

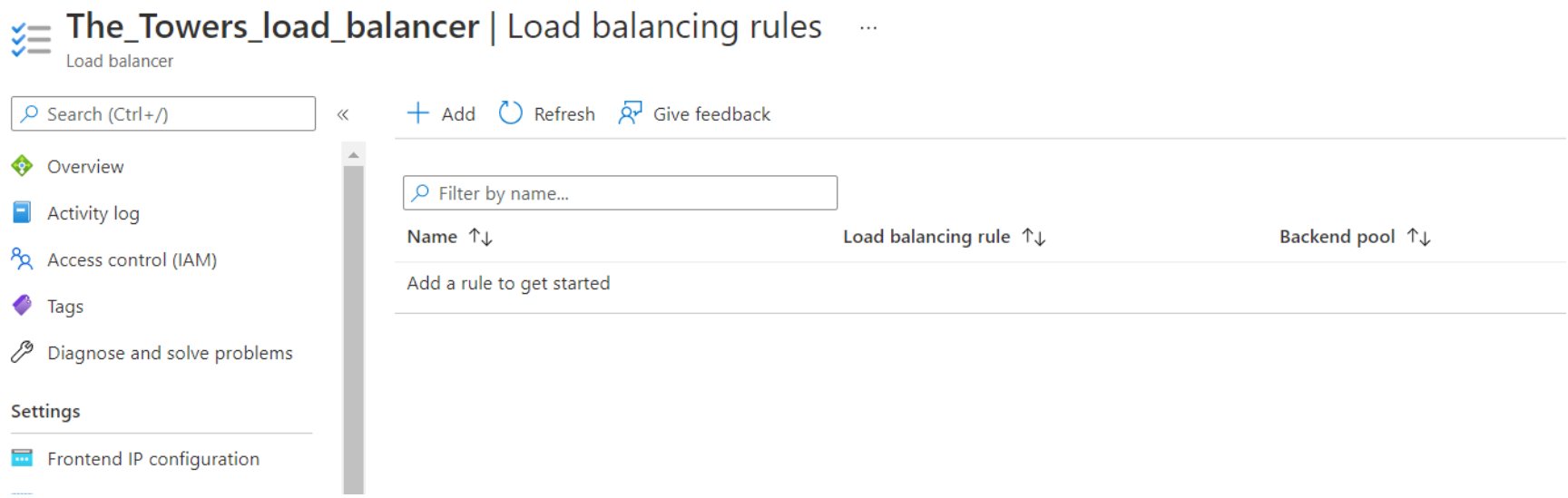
Virtual machines

You can only attach virtual machines in eastus that have a basic SKU public IP configuration or no public IP configuration. All virtual machines must be in the same availability set and all IP configurations must be on the same virtual network.

+ Add Remove

Virtual machine ↑↓	IP Configuration ↑↓	Availability set ↑↓
westtower	ipconfig1 (10.0.0.6)	duplication_spell
easttower	ipconfig1 (10.0.0.5)	duplication_spell

28-create a load balancer rule to forward port 80 to virtual network



28.a

Add load balancing rule

The_Towers_load_balancer

Name * Dividing_Towers_resources

IP Version * IPv4 / IPv6

Frontend IP address * LoadBalancerFrontEnd (40.88.131.235)

Protocol TCP / UDP

Port * 80

Backend port * 80

Backend pool * The_Towers_load_balancer_treasurer

Health probe * Towers_Sentry_Probe (TCP:80)

Create new

Session persistence Client IP and protocol

Idle timeout (minutes) * 4

Floating IP Disabled / Enabled

29-create a security group rule to allow port 80 traffic from internet to virtual network

Add inbound security rule

Caastle_Gate

Source

IP Addresses

Source IP addresses/CIDR ranges *

10.0.0.0/24 or 2001:1234::/64

Source port ranges *

*

Destination

VirtualNetwork

Service

Custom

Destination port ranges *

80

Protocol

- (•) Any
- ( ) TCP
- ( ) UDP

29.a

Add inbound security rule

Caastle_Gate

Custom

Destination port ranges *

80

Protocol

- (•) Any
- ( ) TCP
- ( ) UDP
- ( ) ICMP

Action

- (•) Allow
- ( ) Deny

Priority *

104

Name *

Port_80_traffic_to_The_Castle

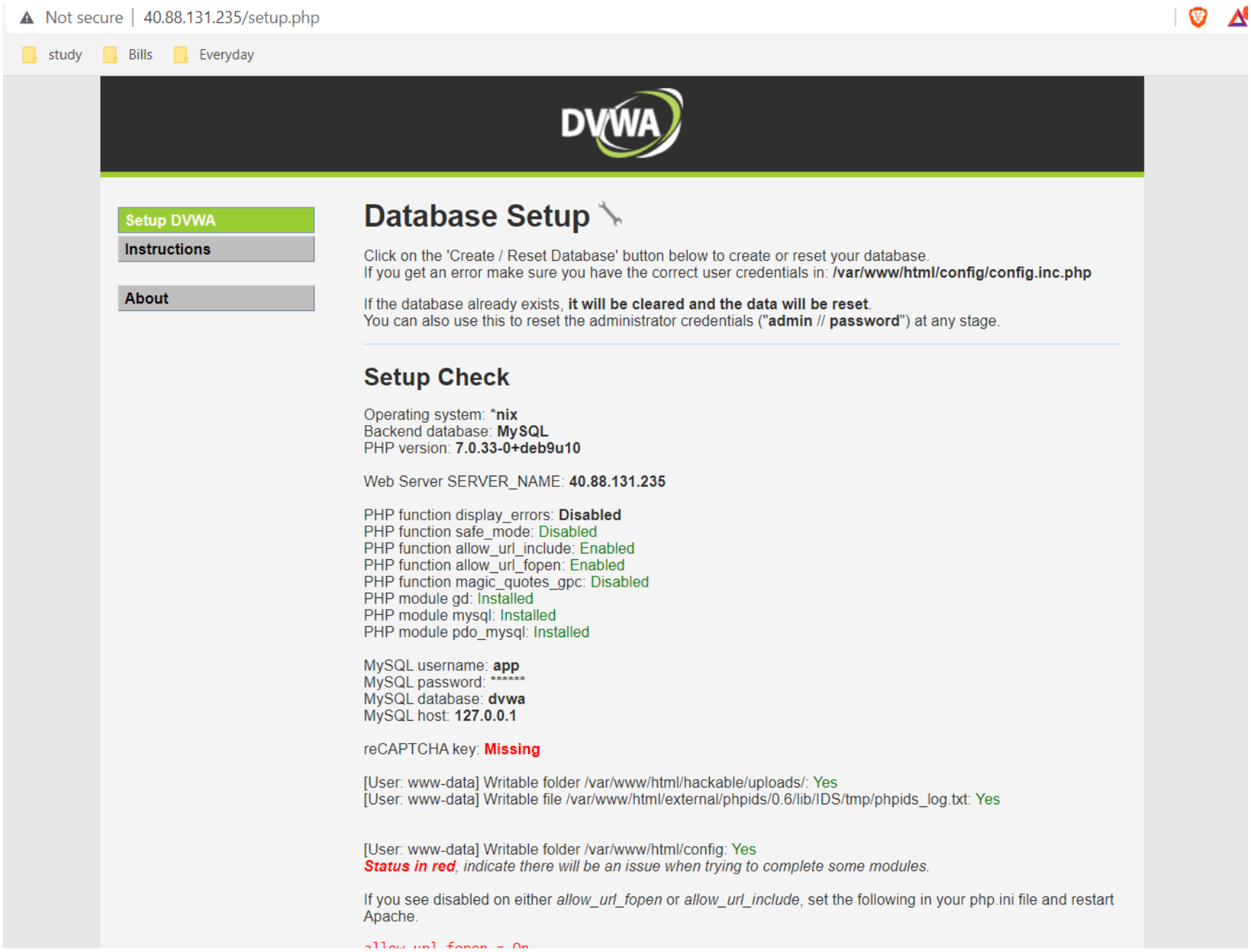
Description

Allow port 80 internet traffic to Virtual Network

30-remove deny all traffic rule

	Priority	Name	Port	Protocol	Source	Destination	Action	
☐	102	Host_machine_ssh	22	TCP	23.121.225.191	VirtualNetwork	Allow	🗑
☐	103	SSH_from_Provisionerand...	22	TCP	10.0.0.4	VirtualNetwork	Allow	🗑
☐	104	Port_80_traffic_to_The_Cas...	80	Any	23.121.225.191	VirtualNetwork	Allow	🗑
☐	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	🗑
☐	65001	AllowAzureLoadBalancerI...	Any	Any	AzureLoadBalancer	Any	Allow	🗑
☐	65500	DenyAllInBound	Any	Any	Any	Any	Deny	🗑

31-verify dvwa is running http://40.88.131.235/setup.php


Not secure | 40.88.131.235/setup.php
study
Bills
Everyday
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/config/config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.
Setup Check
Operating system: *nix
Backend database: MySQL
PHP version: 7.0.33-0+deb9u10
Web Server SERVER_NAME: 40.88.131.235
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed
MySQL username: app
MySQL password: ******
MySQL database: dvwa
MySQL host: 127.0.0.1
reCAPTCHA key: Missing
[User: www-data] Writable folder /var/www/html/hackable/uploads/: Yes
[User: www-data] Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes
[User: www-data] Writable folder /var/www/html/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

32.-Make a third vm for redundancy

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 * ⓘ — The_Treasure_Room

Create new

Instance details

Virtual machine name * ⓘ — WizardsTower ✓

Region * ⓘ — (US) East US

Availability options ⓘ — Availability set

Availability set * ⓘ — Duplication_spell

Create new

Image * ⓘ — Ubuntu Server 18.04 LTS - Gen1

See all images

Size * ⓘ — Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/month)

See all sizes

32.a

Create a virtual machine ···

Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : The_Castle
Create new

Subnet * : default (10.0.0.0/24)
Manage subnet configuration

Public IP : None
Create new

NIC network security group :
- ○ None
- ○ Basic
- ◉ Advanced

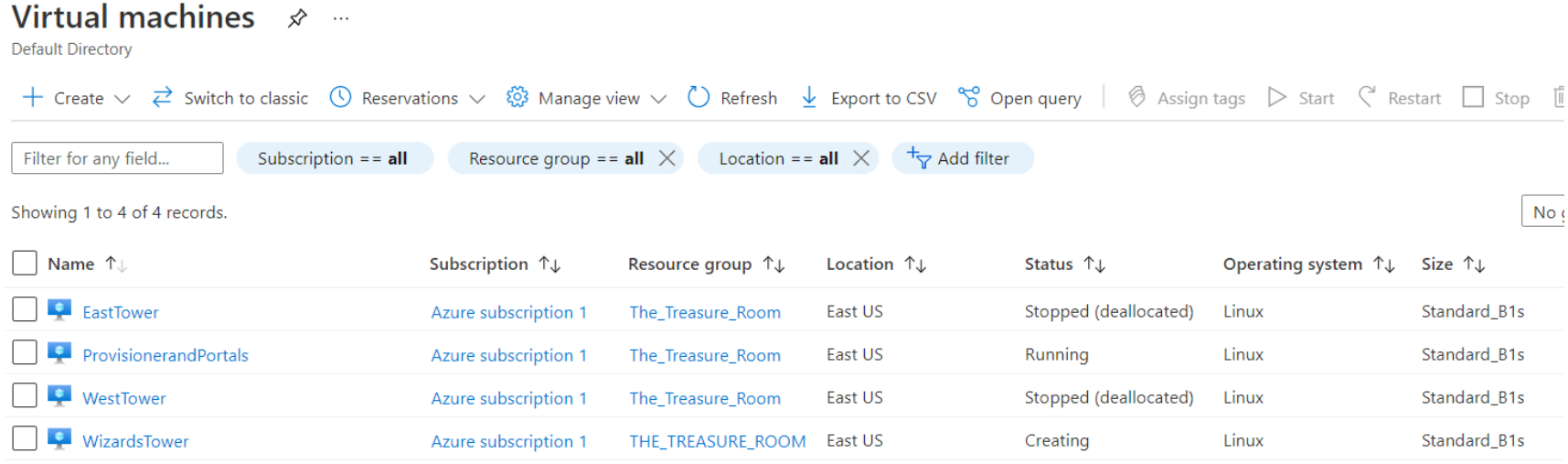
Configure network security group * : Caastle_Gate
Create new

Accelerated networking : ☐
The selected VM size does not support accelerated networking.

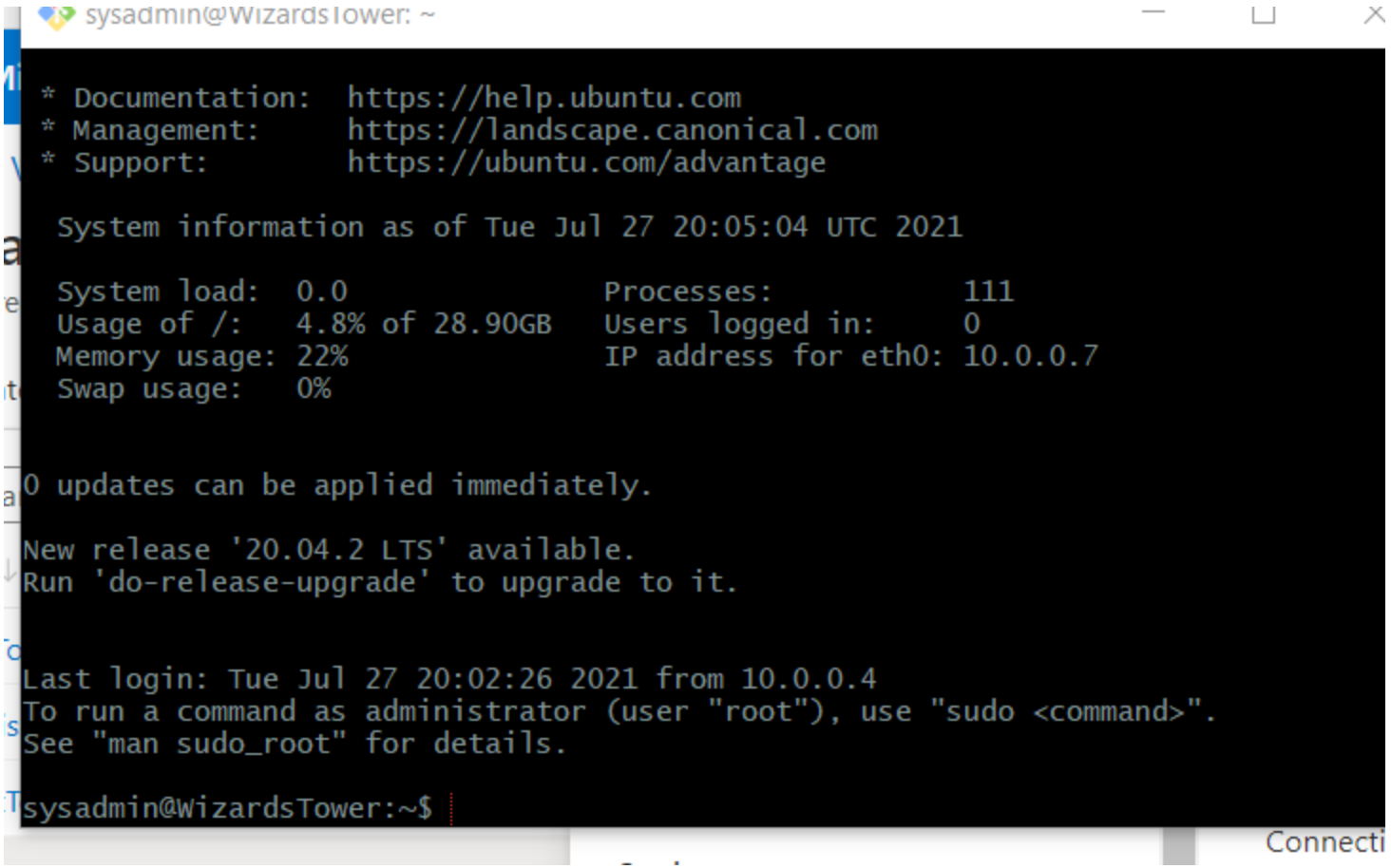
Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more

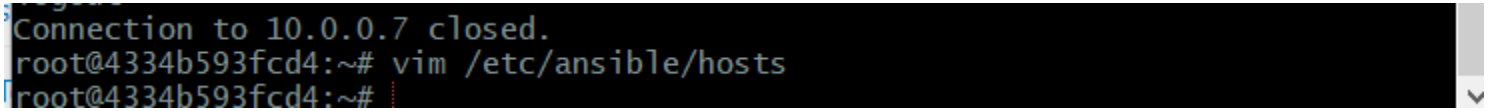
32.b- no public ip



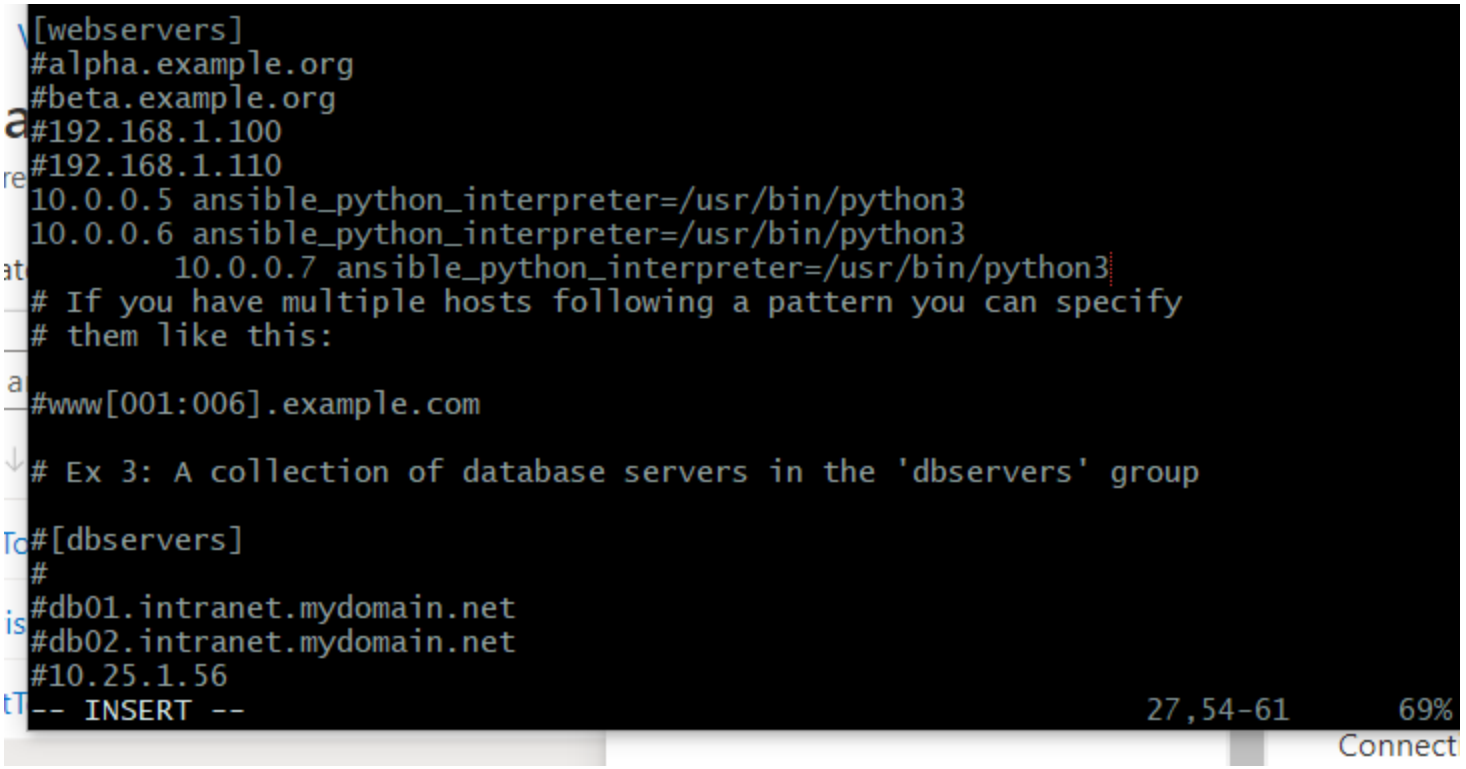
33. Test ssh



34-add new vm to host file



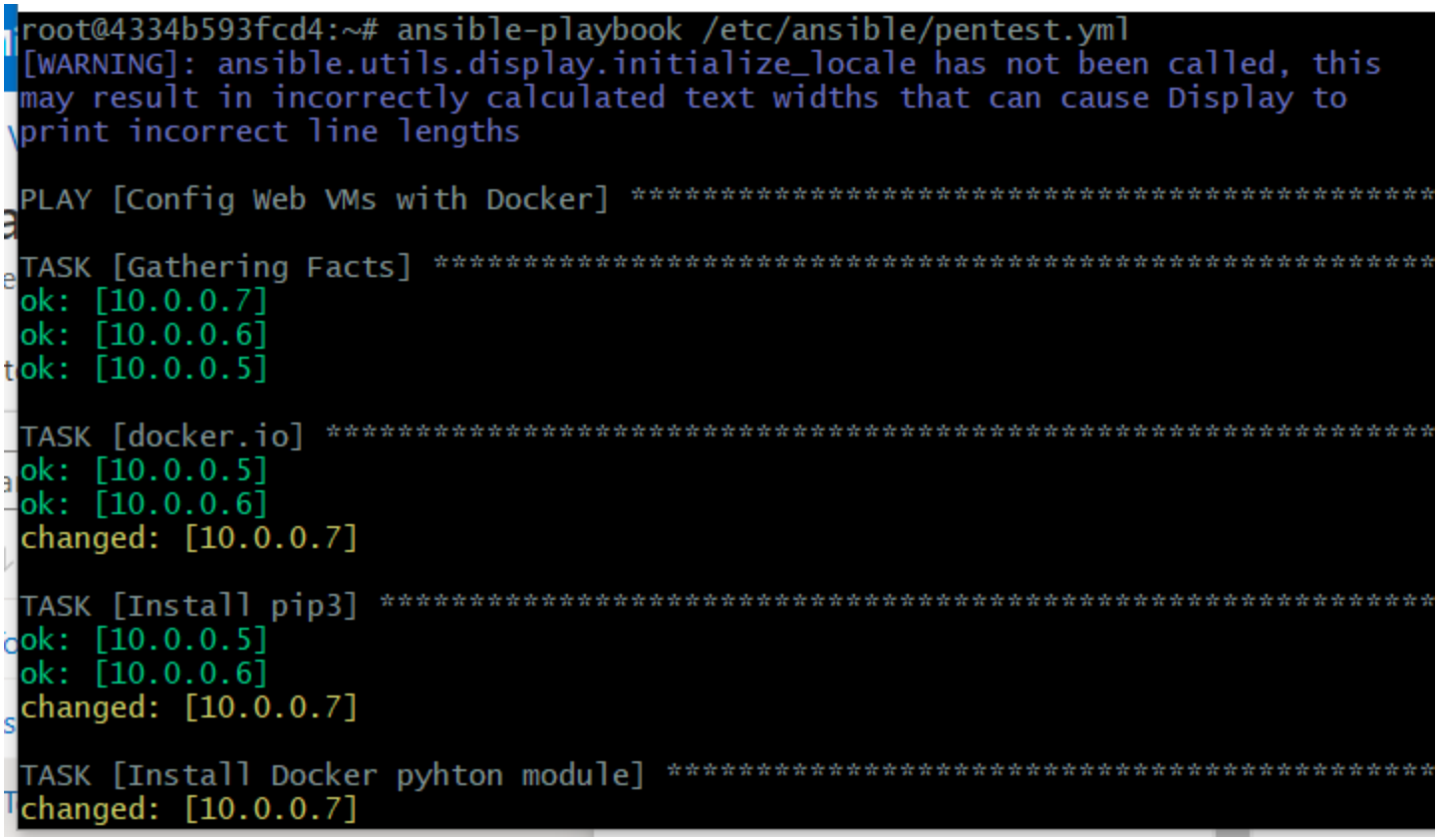
34.a



35- test ansible

```
root@4334b593fcd4:~# vim /etc/ansible/hosts
root@4334b593fcd4:~# ansible all -m ping
10.0.0.7 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

36-run ansible playbook


root@4334b593fcd4:~# ansible-playbook /etc/ansible/pentest.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this
may result in incorrectly calculated text widths that can cause Display to
print incorrect line lengths
PLAY [Config Web VMs with Docker] **********
TASK [Gathering Facts] **********
ok: [10.0.0.7]
ok: [10.0.0.6]
ok: [10.0.0.5]
TASK [docker.io] **********
ok: [10.0.0.5]
ok: [10.0.0.6]
changed: [10.0.0.7]
TASK [Install pip3] **********
ok: [10.0.0.5]
ok: [10.0.0.6]
changed: [10.0.0.7]
TASK [Install Docker pyhton module] **********
changed: [10.0.0.7]

36.a

```
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [download and launch docker web container] *********************************
[DEPRECATION WARNING]: The container_default_behavior option will change its
default value from "compatibility" to "no_defaults" in community.docker 2.0.0.
To remove this warning, please specify an explicit value for it now. This
feature will be removed from community.docker in version 2.0.0. Deprecation
warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
changed: [10.0.0.5]
changed: [10.0.0.6]
changed: [10.0.0.7]

TASK [Enable docker service] ****************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]
ok: [10.0.0.7]

PLAY RECAP **********************************************************************
10.0.0.5                   : ok=6    changed=1    unreachable=0    failed=0    s
kipped=0    rescued=0    ignored=0
10.0.0.6                   : ok=6    changed=1    unreachable=0    failed=0    s
kipped=0    rescued=0    ignored=0
10.0.0.7                   : ok=6    changed=4    unreachable=0    failed=0    s
```

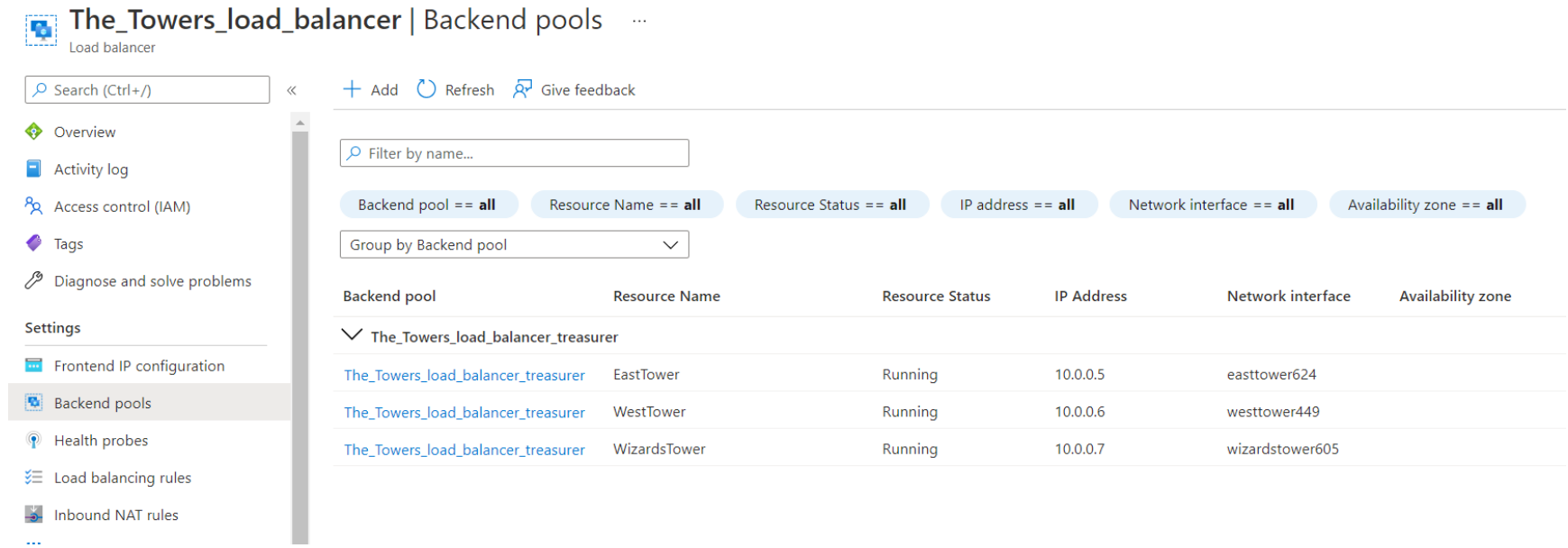
37-ssh into the new vm and curl localhost/setup.php

```
Last login: Tue Jul 27 20:20:21 2021 from 10.0.0.4
sysadmin@WizardsTower:~$ curl localhost/setup.php
```

37.a

```
Last login: Tue Jul 27 20:20:21 2021 from 10.0.0.4
sysadmin@WizardsTower:~$ curl localhost/setup.php
<!DOCTYPE html>

<html lang="en-GB">

        <head>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-
8" />

                <title>Setup :: Damn Vulnerable Web Application (DVWA) v1.10 *De
velopment*</title>

                <link rel="stylesheet" type="text/css" href="dvwa/css/main.css"
/>

                <link rel="icon" type="\image/ico" href="favicon.ico" />

                <script type="text/javascript" src="dvwa/js/dvwaPage.js"></scrip
t>

        </head>
```

38-add the new dvwa to the load balancer backend pool



39- go to dvwa site and test

Penetration testing | For class | study | Bills | Everyday

DVWA

Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your datab
If you get an error make sure you have the correct user credentials in: **/var/www**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**

Setup Check

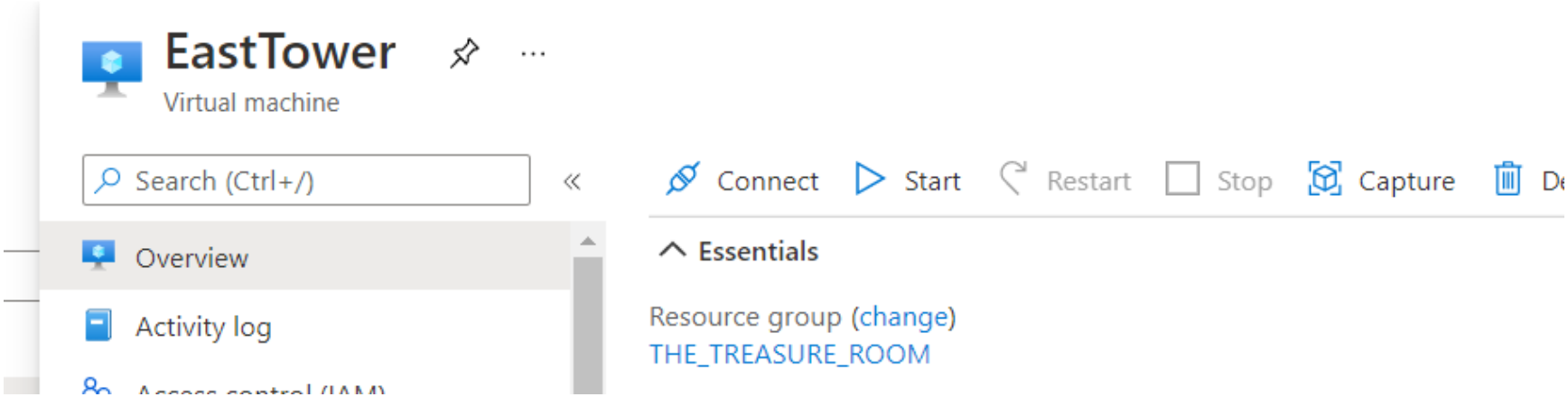
Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.0.33-0+deb9u10**

Web Server SERVER_NAME: **40.88.131.235**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **app**
MySQL password: ******
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

39.a-turn off 1 vm



39.b- verify dvwa site is still up

Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset yo
If you get an error make sure you have the correct user credentials in: /v

If the database already exists, **it will be cleared and the data will be re**
You can also use this to reset the administrator credentials ("**admin** // **pa**

Setup Check

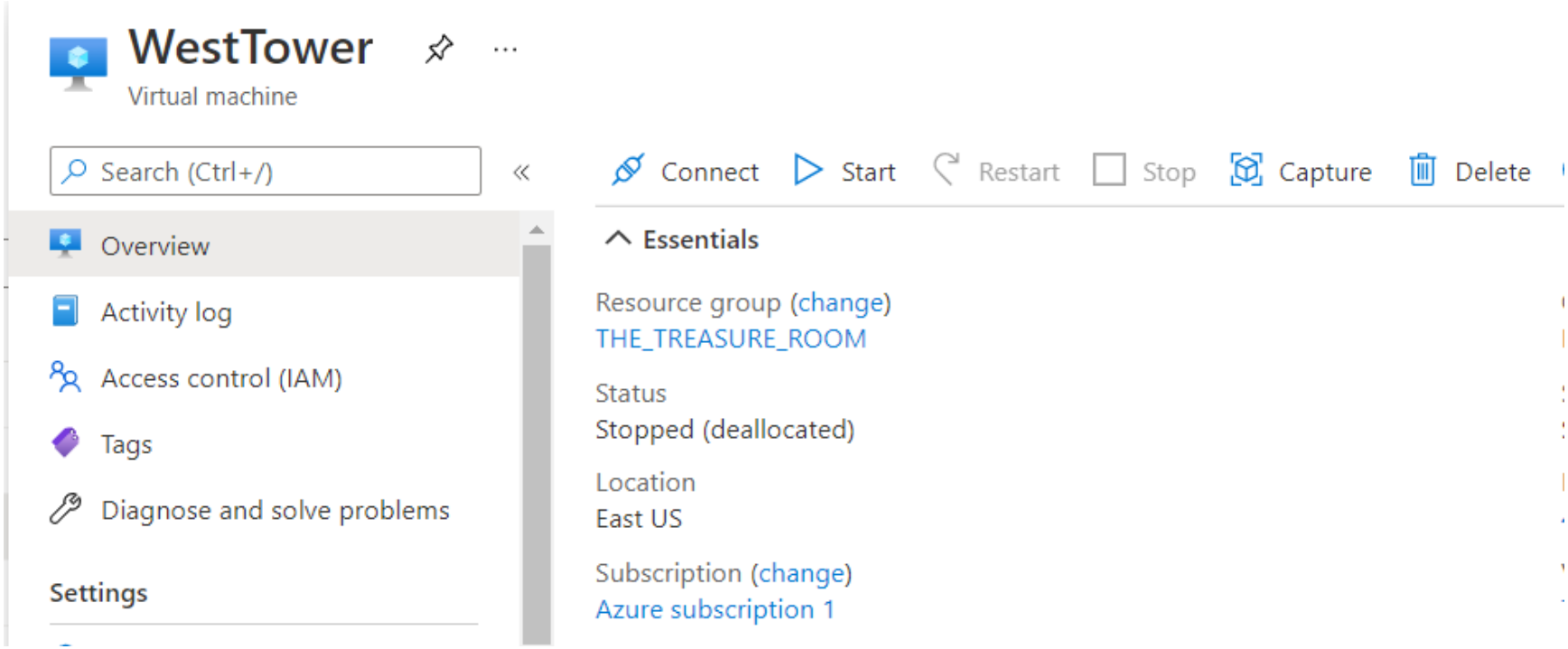
Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.0.33-0+deb9u10**

Web Server SERVER_NAME: **40.88.131.235**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **app**
MySQL password: ******
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

39.c- turn off another vm and see if dvwa site goes down



39.d

This site can’t be reached

40.88.131.235 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

39.e- start 1st vm run playbook, site should return. Continue with all three to verify all are running

Name	Subscription	Resource group	Location	Status	Operating system
EastTower	Azure subscription 1	THE_TREASURE_ROOM	East US	Running	Linux
ProvisionerandPortals	Azure subscription 1	The_Treasure_Room	East US	Running	Linux
WestTower	Azure subscription 1	THE_TREASURE_ROOM	East US	Running	Linux
WizardsTower	Azure subscription 1	THE_TREASURE_ROOM	East US	Running	Linux

39.f

Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to cre
If you get an error make sure you have the correct user cr

If the database already exists, **it will be cleared and the**
You can also use this to reset the administrator credentials

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.0.33-0+deb9u10**

Web Server SERVER_NAME: **40.88.131.235**

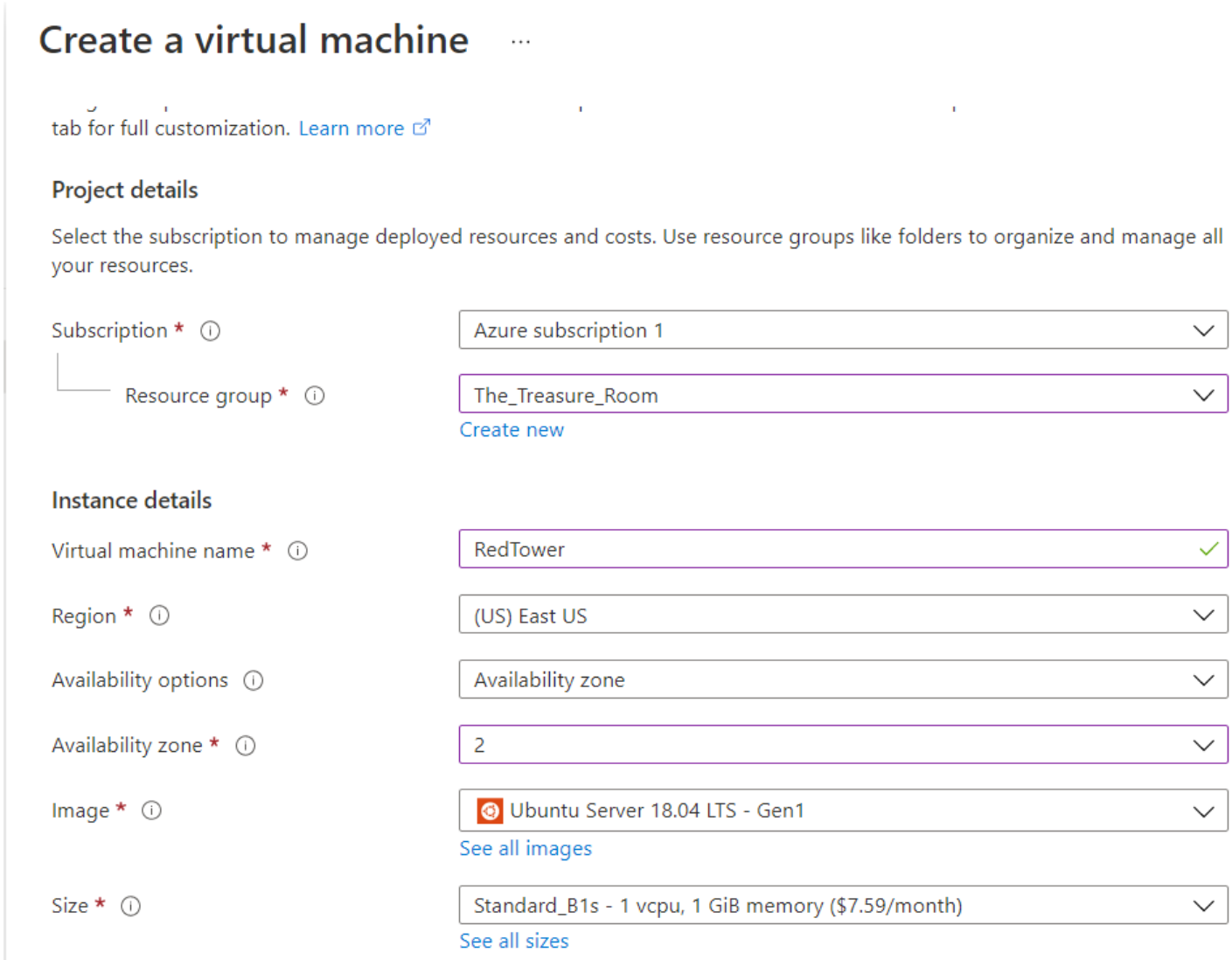
PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **app**
MySQL password: ******
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

40.-Make 2 new vms behind the same load balancer but in a different availability zone. Had to delete two since i only had 4 cpus to work with.

Name	Subscription	Resource group	Location	Status	Opera
EastTower	Azure subscription 1	The_Treasure_Room	East US	Stopped (deallocated)	Linux
ProvisionerandPortals	Azure subscription 1	The_Treasure_Room	East US	Running	Linux

40.a-new vm, new availability zone



40.b-new vm, different availability zone

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 * : The_Treasure_Room

Create new

Instance details

Virtual machine name * : BlueTower

Region * : (US) East US

Availability options : Availability zone

Availability zone * : 3

Image * : Ubuntu Server 18.04 LTS - Gen1

See all images

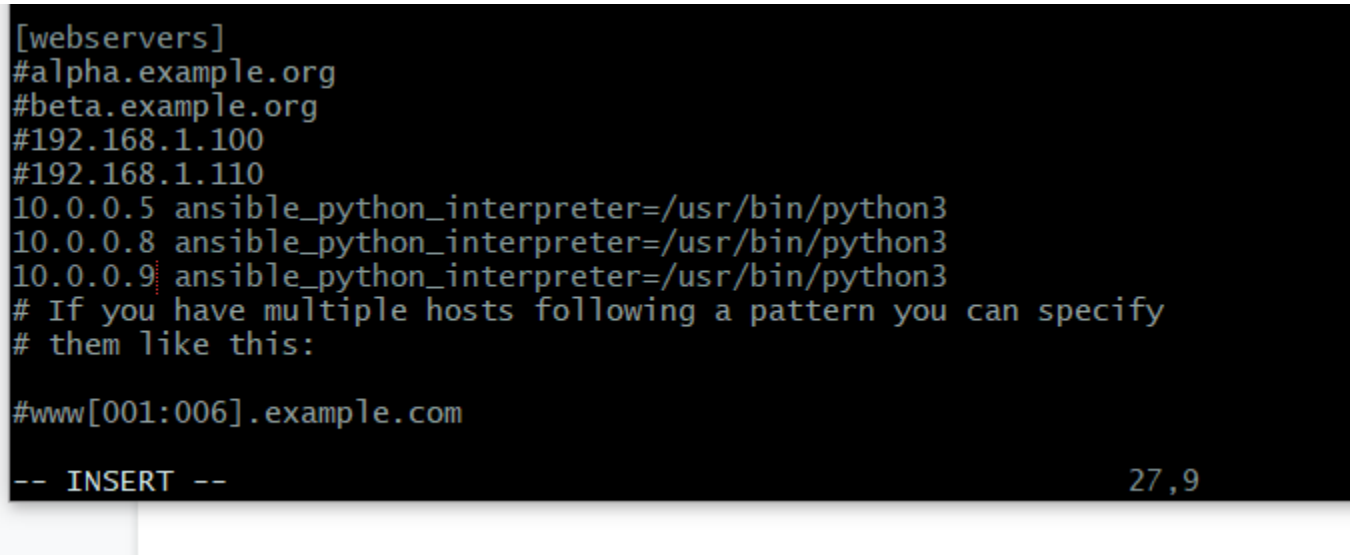
Size * : Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/month)

See all sizes

40.c

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
BlueTower	Azure subscription 1	The_Treasure_Room	East US	Running	Linux	Standard_B1s	-	1
EastTower	Azure subscription 1	The_Treasure_Room	East US	Stopped (deallocated)	Linux	Standard_B1s	40.88.131.235	1
ProvisionerandPortals	Azure subscription 1	The_Treasure_Room	East US	Running	Linux	Standard_B1s	40.90.238.244	1
RedTower	Azure subscription 1	The_Treasure_Room	East US	Running	Linux	Standard_B1s	-	1

41.-update the ansible hosts file



42.-run the playbook and check that you can ssh into them

```
root@4334b593fcd4:~# ansible-playbook /etc/ansible/pentest.yml
[WARNING]: ansible.utils.display.initialize_locale has not been called, this
may result in incorrectly calculated text widths that can cause Display to
print incorrect line lengths

PLAY [Config Web VMs with Docker] **********************************************

TASK [Gathering Facts] *********************************************************
ok: [10.0.0.9]
ok: [10.0.0.8]
ok: [10.0.0.5]

TASK [docker.io] ***************************************************************
ok: [10.0.0.5]
ok: [10.0.0.9]
ok: [10.0.0.8]

TASK [Install pip3] ************************************************************
ok: [10.0.0.9]
ok: [10.0.0.5]
ok: [10.0.0.8]
```

42.a-curl localhost/setup.php

```
Last login: Wed Jul 28 18:42:21 2021 from 10.0.0.4
sysadmin@RedTower:~$
```

42.b curl localhost/setup.php

```
Last login: Wed Jul 28 18:42:21 2021 from 10.0.0.4
sysadmin@BlueTower:~$
```

43-create a new load balancer, remove vms from other one, add them to this one with standard sku settings

Create load balancer ...

Instance details

Name * The_Towers_reinforced_load_balancer

Region * (US) East US

Type * ⓘ ○ Internal ◉ Public

SKU * ⓘ ◉ Standard ○ Basic

ⓘ Microsoft recommends Standard SKU load balancer for production workloads.
Learn more about pricing differences between Standard and Basic SKU

Tier * ◉ Regional ○ Global

Public IP address

Public IP address * ⓘ ◉ Create new ○ Use existing

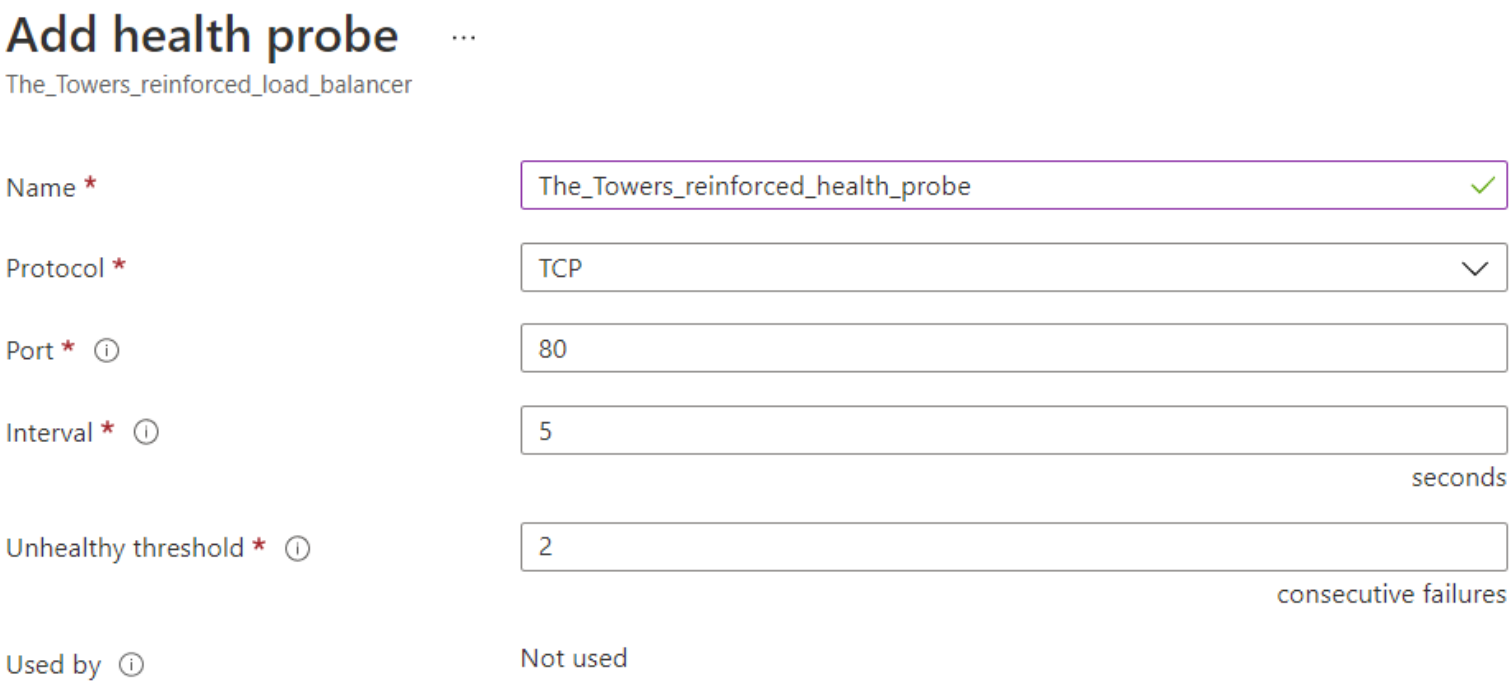
Public IP address name * The_Towers_reinforced_load_balancer

Public IP address SKU Standard

IP address assignment ○ Dynamic ◉ Static

Availability zone * Zone-redundant

43.a


Add health probe
...
The_Towers_reinforced_load_balancer
Name *
The_Towers_reinforced_health_probe
Protocol *
TCP
Port *
80
Interval *
5
seconds
Unhealthy threshold *
2
consecutive failures
Used by
Not used

43.b

Add backend pool ...

- (•) IPv4
- ( ) IPv6

Virtual machines

You can only attach virtual machines in eastus that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.

+ Add Remove

Virtual machine	IP Configuration	Availability set
easttower	ipconfig1 (10.0.0.5)	duplication_spell
RedTower	ipconfig1 (10.0.0.8)	-
BlueTower	ipconfig1 (10.0.0.9)	-

Virtual machine scale sets

43.c

Add load balancing rule

The_Towers_reinforced_load_balancer

Name *: Dividing_Towers_resources

IP Version *: (•) IPv4 ( ) IPv6

Frontend IP address *: LoadBalancerFrontEnd (20.85.184.40)

Protocol: (•) TCP ( ) UDP

Port *: 80

Backend port *: 80

Backend pool *: The_Towers_reinforced_load_balancer_backend_pool

Health probe *: The_Towers_reinforced_health_probe (TCP:80)

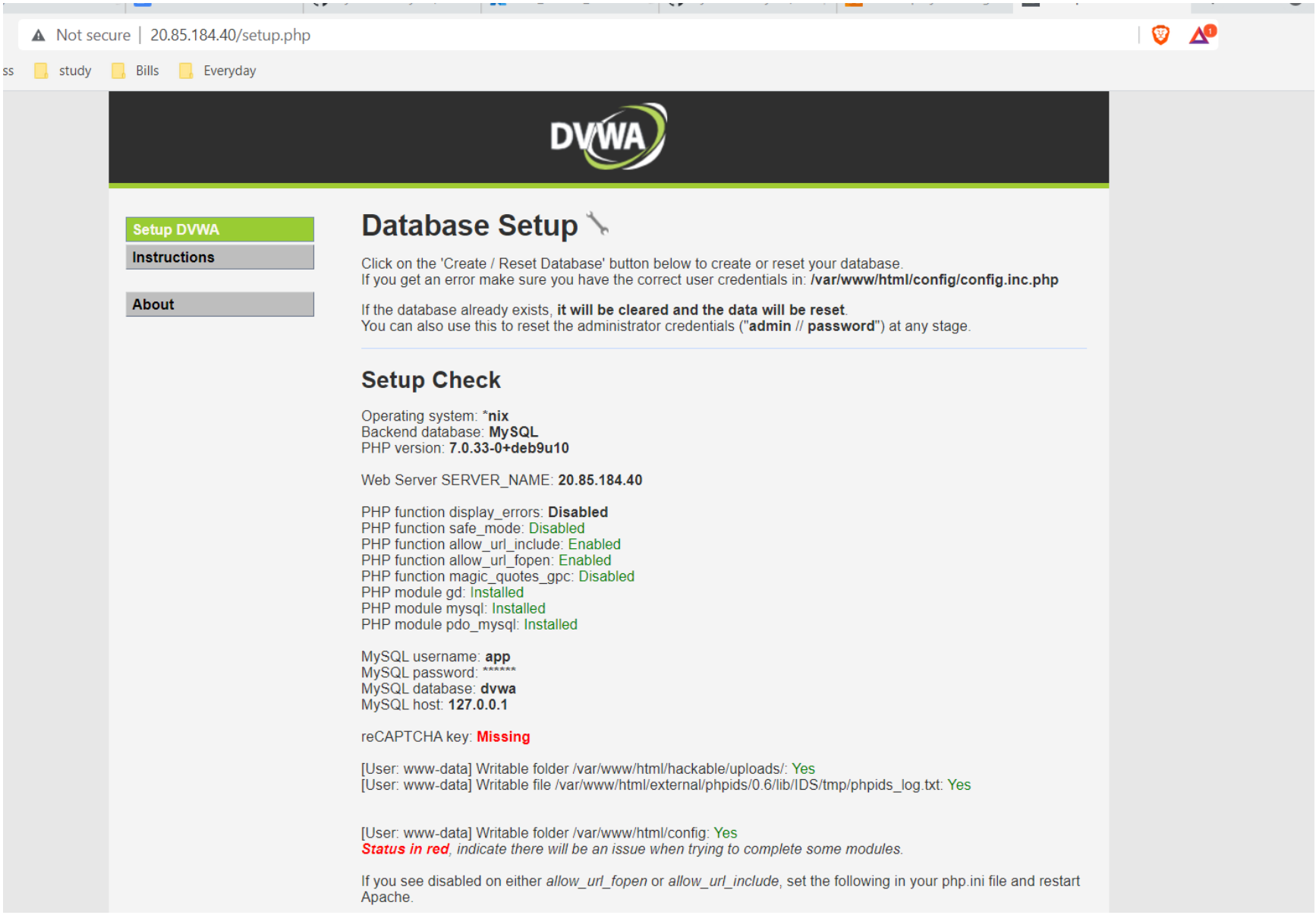
Create new

Session persistence: Client IP and protocol

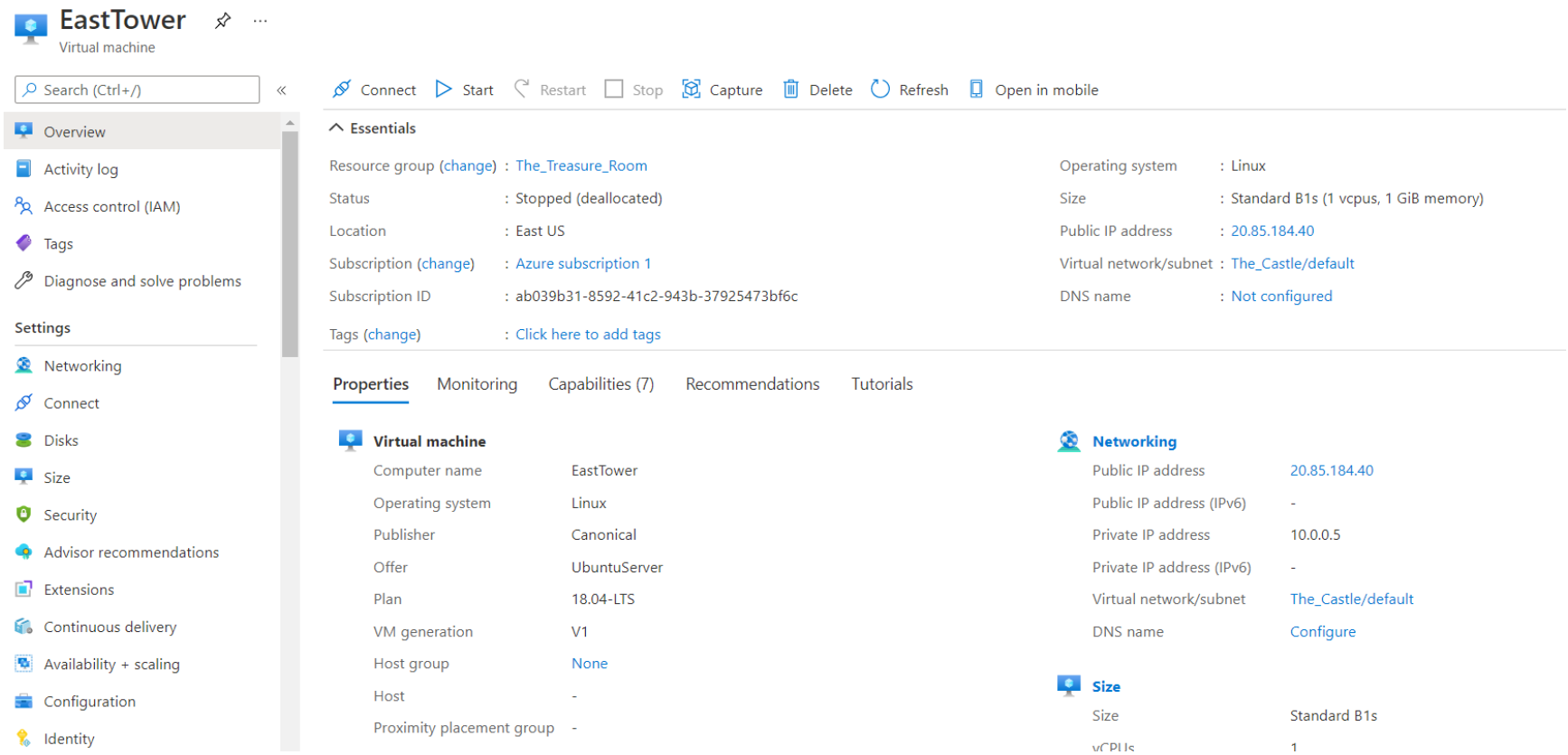
Idle timeout (minutes) *: 4

TCP reset: (•) Disabled ( ) Enabled

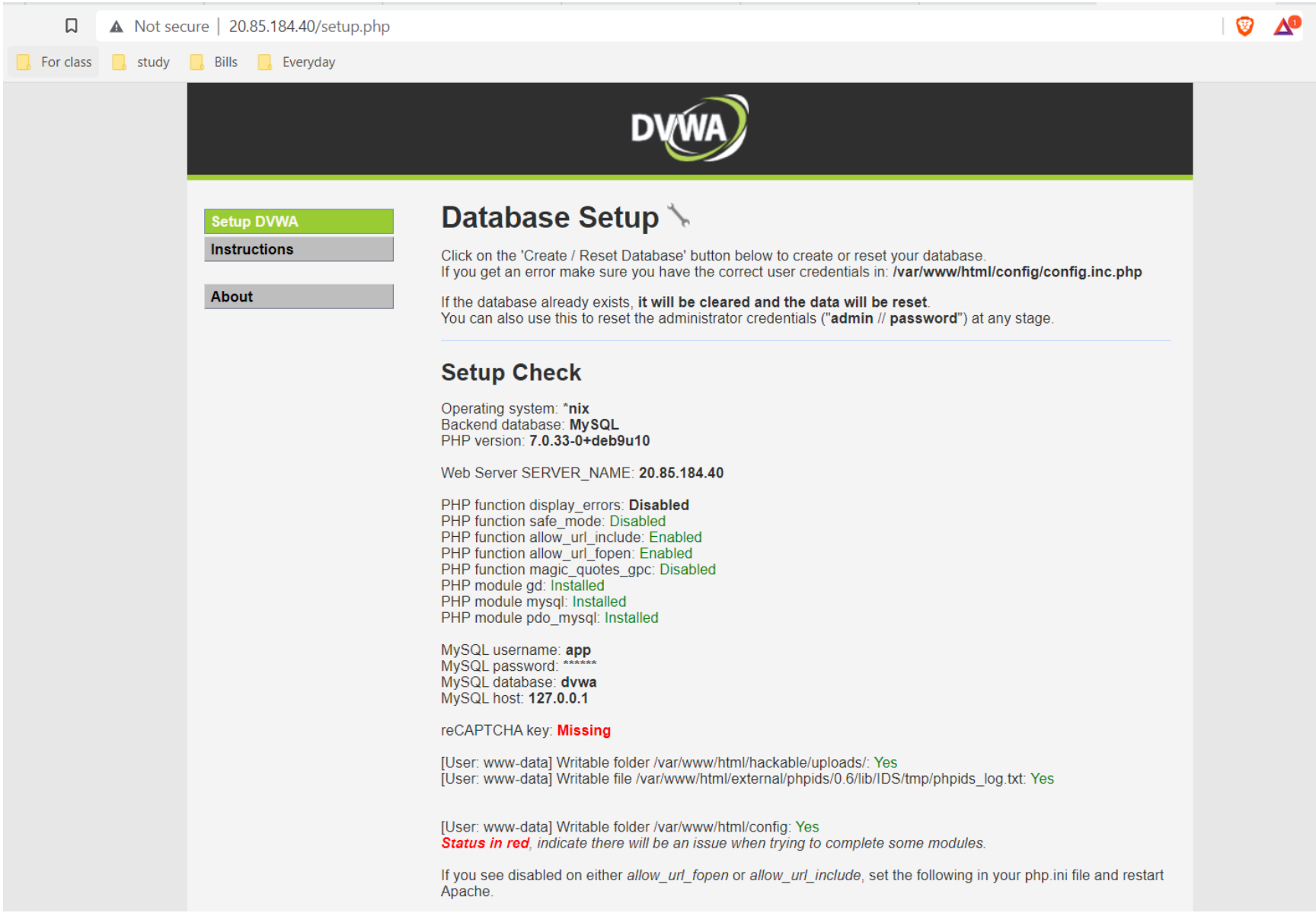
44-enter front end ip of load balancer/setup.php in browser to check dvwa


Not secure | 20.85.184.40/setup.php
ss
study
Bills
Everyday
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/config/config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.
Setup Check
Operating system: *nix
Backend database: MySQL
PHP version: 7.0.33-0+deb9u10
Web Server SERVER_NAME: 20.85.184.40
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed
MySQL username: app
MySQL password: ******
MySQL database: dvwa
MySQL host: 127.0.0.1
reCAPTCHA key: Missing
[User: www-data] Writable folder /var/www/html/hackable/uploads/: Yes
[User: www-data] Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes
[User: www-data] Writable folder /var/www/html/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

45-turn off vm from availability zone 1 and check that dvwa site is still up

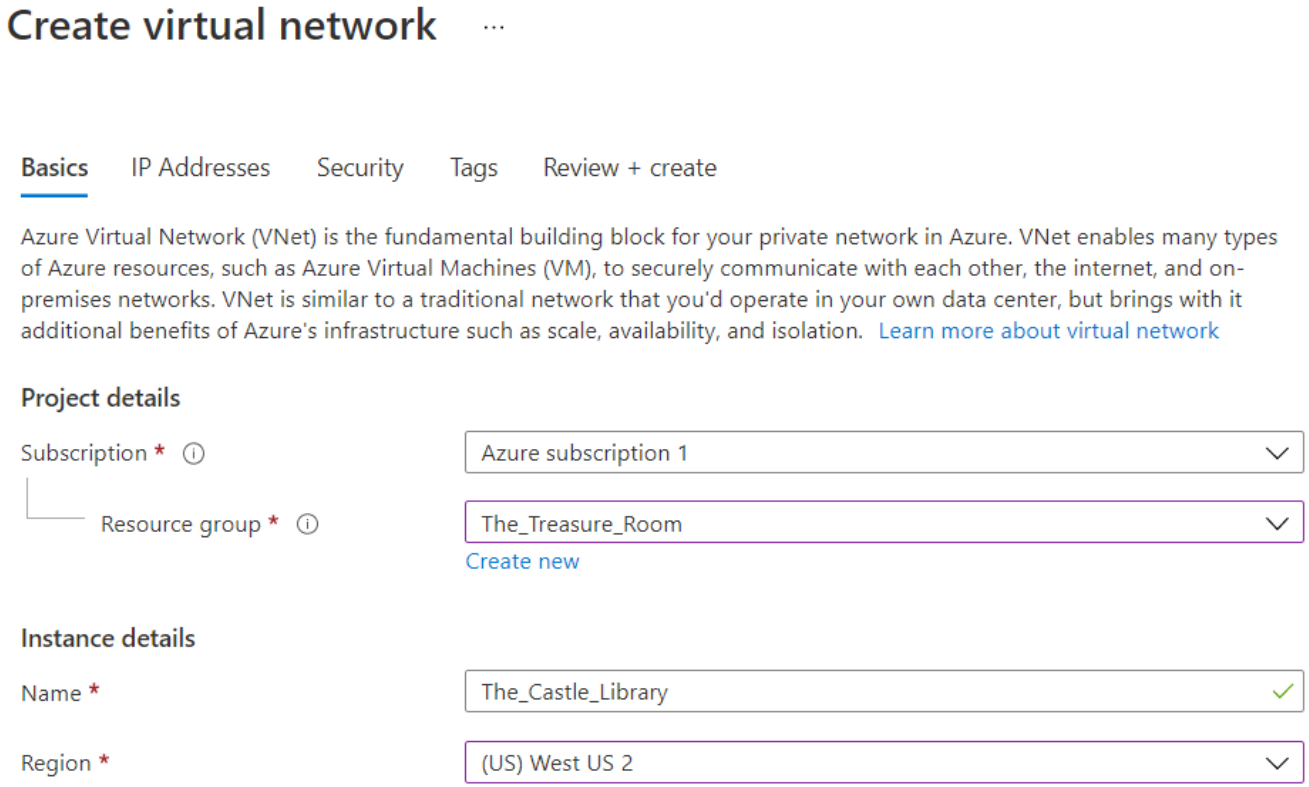


45.a

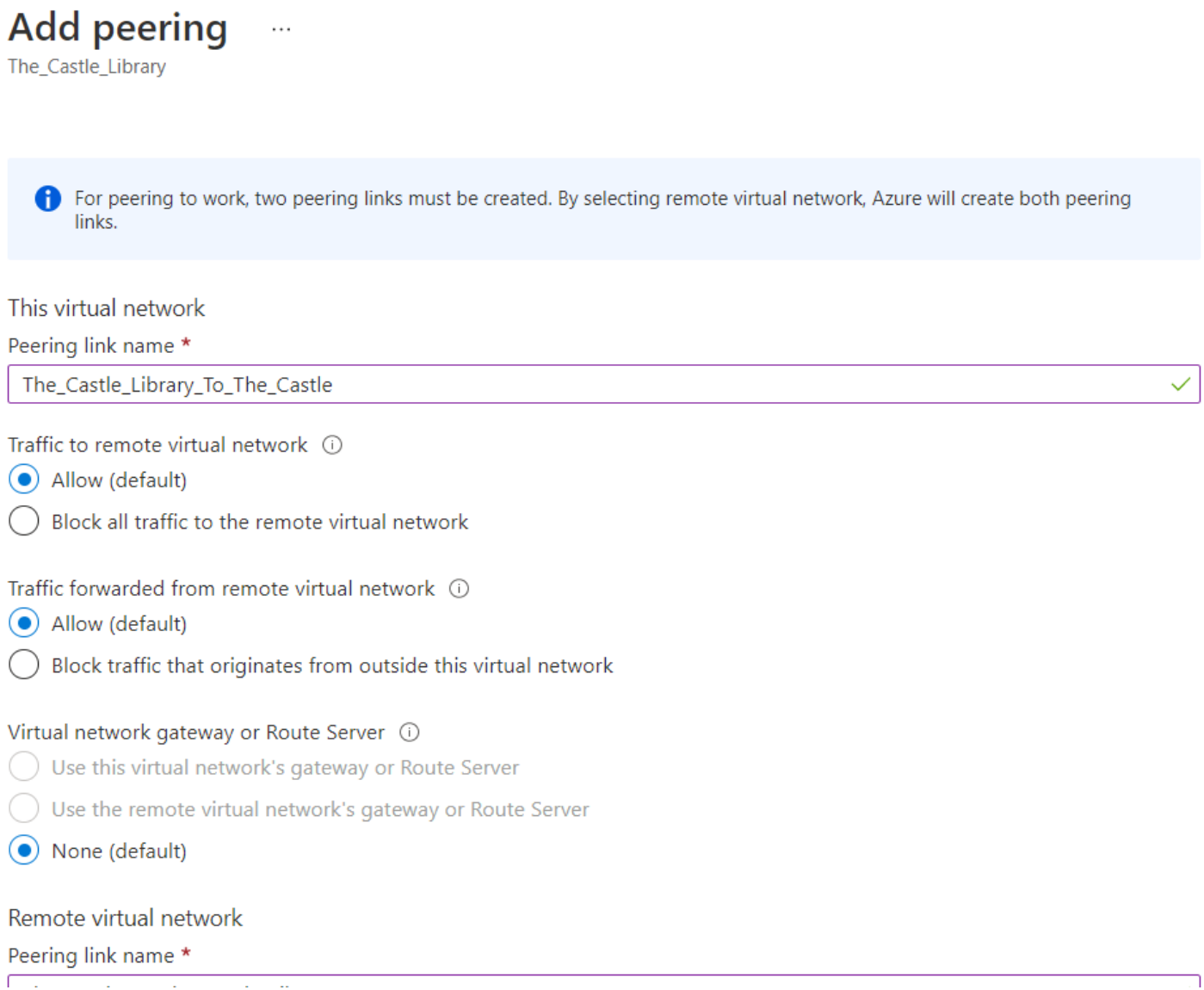

Not secure | 20.85.184.40/setup.php
For class
study
Bills
Everyday
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/config/config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.
Setup Check
Operating system: *nix
Backend database: MySQL
PHP version: 7.0.33-0+deb9u10
Web Server SERVER_NAME: 20.85.184.40
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed
MySQL username: app
MySQL password: ******
MySQL database: dvwa
MySQL host: 127.0.0.1
reCAPTCHA key: Missing
[User: www-data] Writable folder /var/www/html/hackable/uploads/: Yes
[User: www-data] Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes
[User: www-data] Writable folder /var/www/html/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

Elk Stack

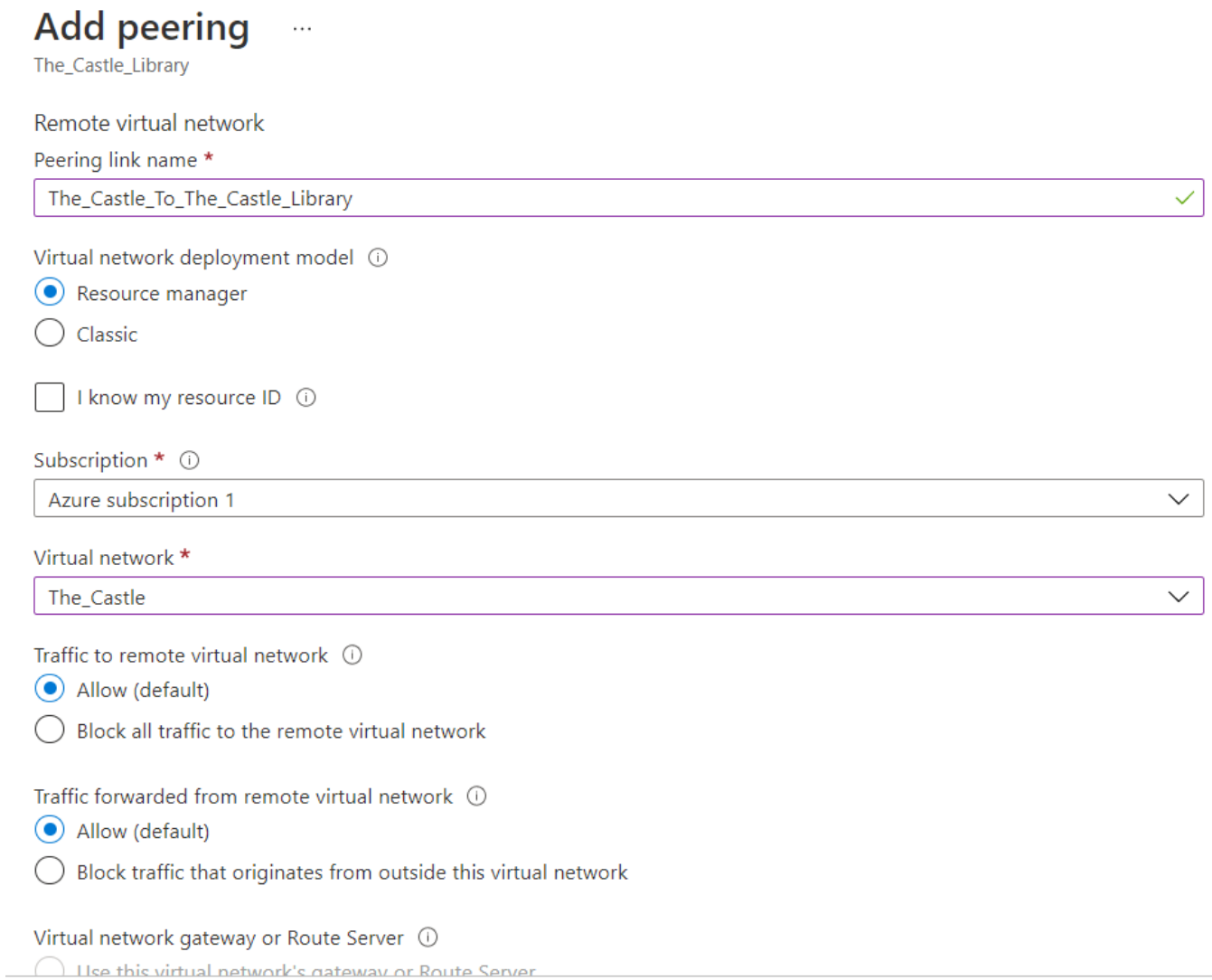
46.-Make a new virtual network in another region



47.a-create a peering from this vnet to your other vnet


Add peering
The_Castle_Library
For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.
This virtual network
Peering link name *
The_Castle_Library_To_The_Castle
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
Peering link name *

47.a



48.-create a new virtual machine to run elk, had to delete a vm-deleted from zone 3

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 * : The_Treasure_Room

Create new

Instance details

Virtual machine name * : ELKStudyRoom

Region * : (US) West US 2

Availability options : No infrastructure redundancy required

Image * : Ubuntu Server 18.04 LTS - Gen1

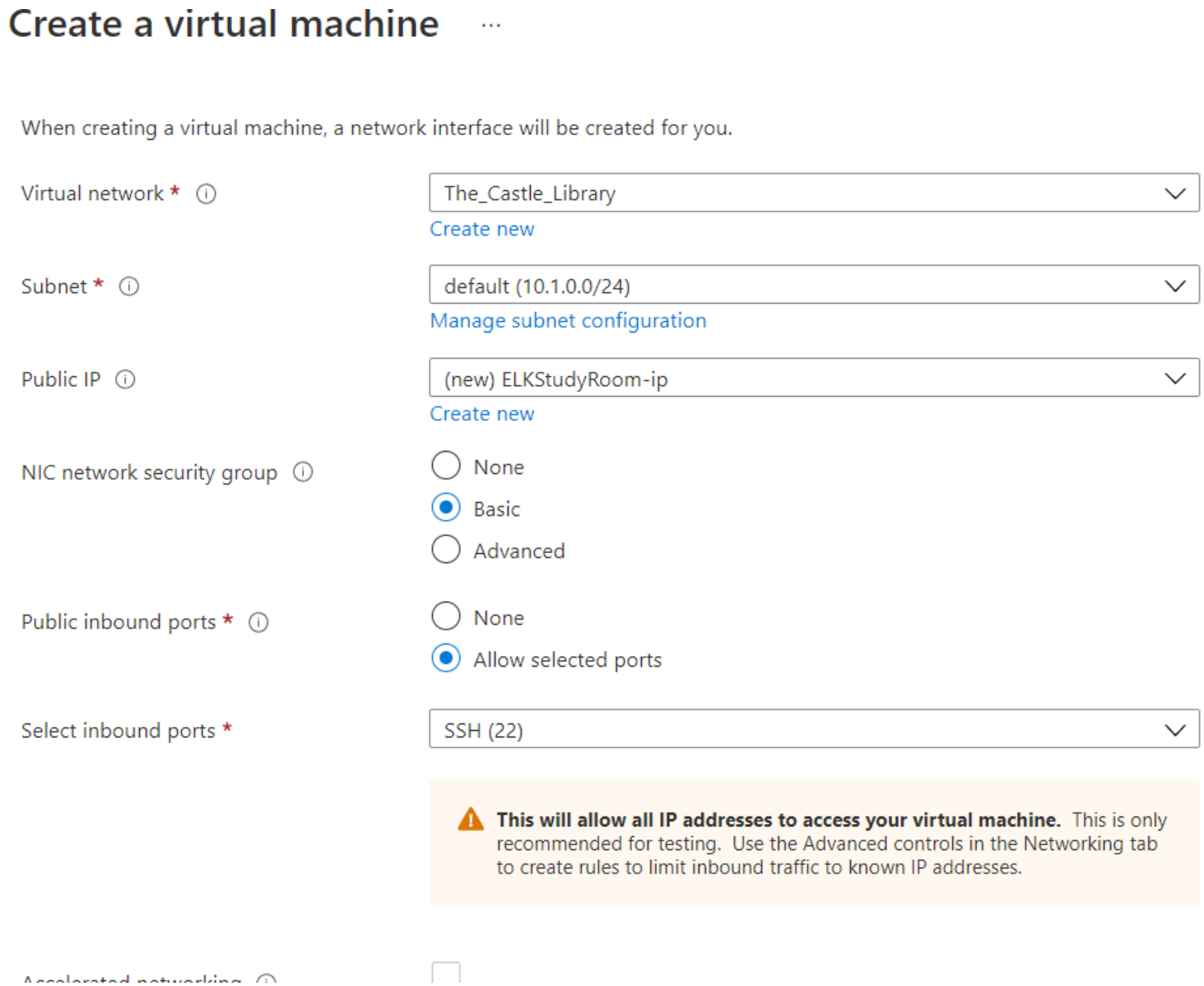
See all images

Size * : Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($70.08/month)

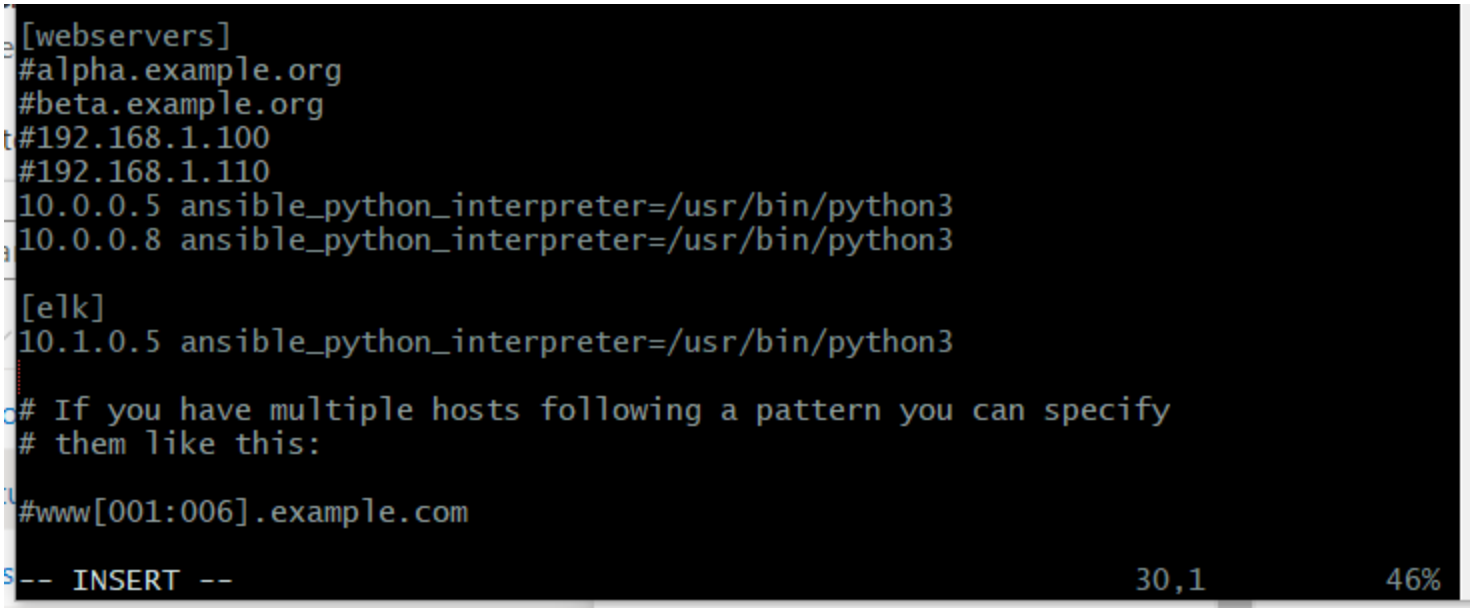
See all sizes

Administrator account

48.a



49.-create a new ansible playbook for the elk vm and add elk to the hosts file


[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
10.0.0.8 ansible_python_interpreter=/usr/bin/python3
[elk]
10.1.0.5 ansible_python_interpreter=/usr/bin/python3
If you have multiple hosts following a pattern you can specify
them like this:
#www[001:006].example.com
-- INSERT --
30,1
46%

49.a

```yaml
---
- 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 container
            docker_container:
                    name: elk
                    image: sebp/elk:761
                    state: started
                    restart_policy: always
                    published_ports:
```

49.b

```
root@4334b593fcd4:~# vim /etc/ansible/elk.yml
root@4334b593fcd4:~#
```

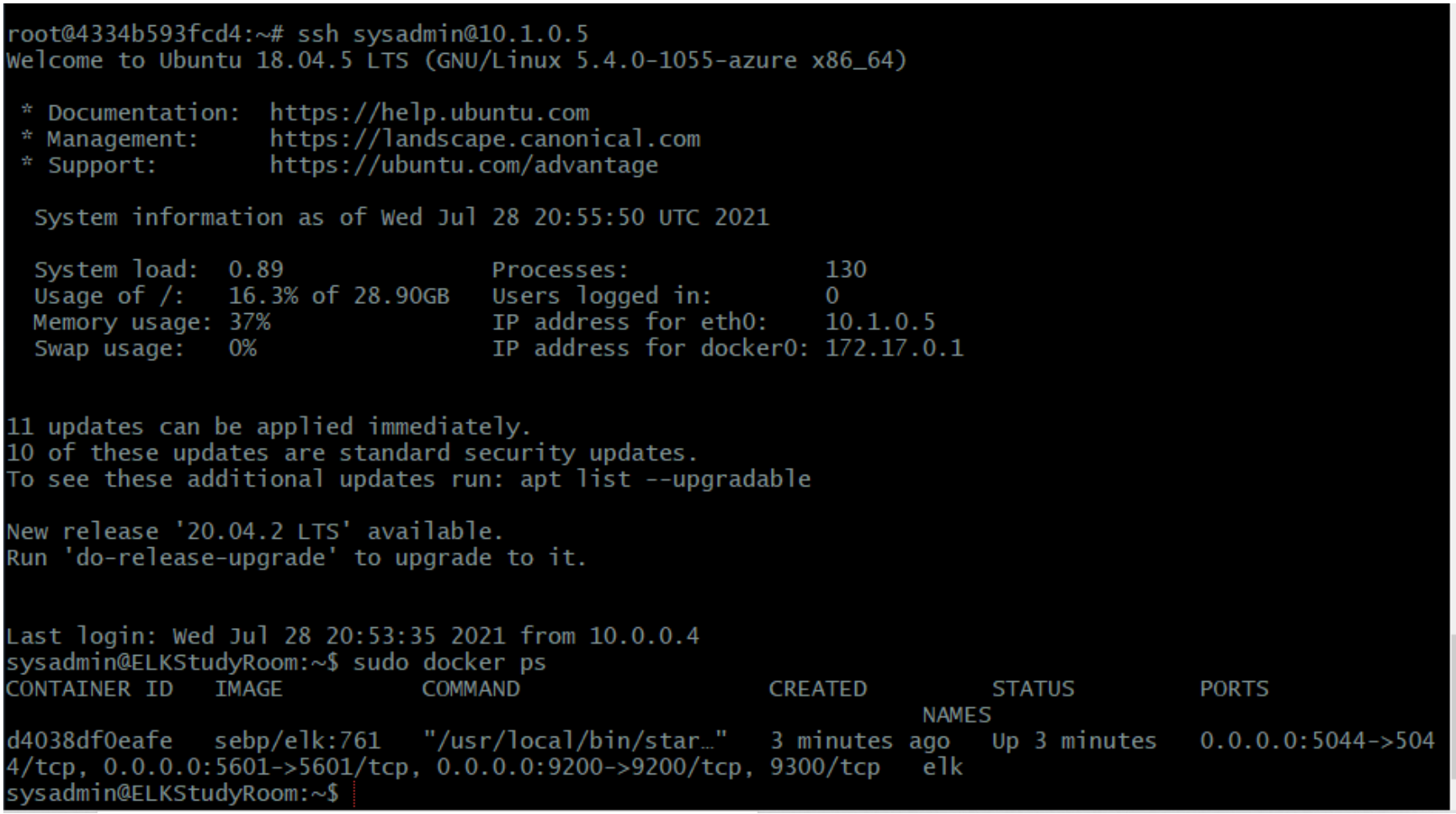
50.-run the playbook

```
root@4334b593fcd4:~# ansible-playbook /etc/ansible/elk.yml
```

50.a

```
[WARNING]: ansible.utils.display.initialize_locale has not been called, this may result in incorrectly
calculated text widths that can cause Display to print incorrect line lengths

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

TASK [Gathering Facts] *********************************************************************************
ok: [10.1.0.5]

TASK [Install docker.io] *******************************************************************************
ok: [10.1.0.5]

TASK [Install pip3] ************************************************************************************
ok: [10.1.0.5]

TASK [Install Docker python module] ********************************************************************
ok: [10.1.0.5]

TASK [Use more memory] *********************************************************************************
ok: [10.1.0.5]

TASK [Download and launch a docker elk container] ******************************************************
[DEPRECATION WARNING]: The container_default_behavior option will change its default value from
"compatibility" to "no_defaults" in community.docker 2.0.0. To remove this warning, please specify an
explicit value for it now. This feature will be removed from community.docker in version 2.0.0.
Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
ok: [10.1.0.5]

TASK [Enable service docker on boot] *******************************************************************
ok: [10.1.0.5]

PLAY RECAP *********************************************************************************************
10.1.0.5                   : ok=7    changed=0    unreachable=0    failed=0    skipped=0    rescued=0
  ignored=0

root@4334b593fcd4:~#
```

51.-ssh into the elk vm and run sudo docker ps to verify a running elk container



52. **–his ELK web server runs on port `5601`. Create an incoming rule for your security group that allows TCP traffic over port `5601` from your IP address.**

Source

IP Addresses

Source IP addresses/CIDR ranges *

10.0.0.0/24 or 2001:1234::/64

The value must not be empty.

Source port ranges *

*

Destination

Any

Service

Custom

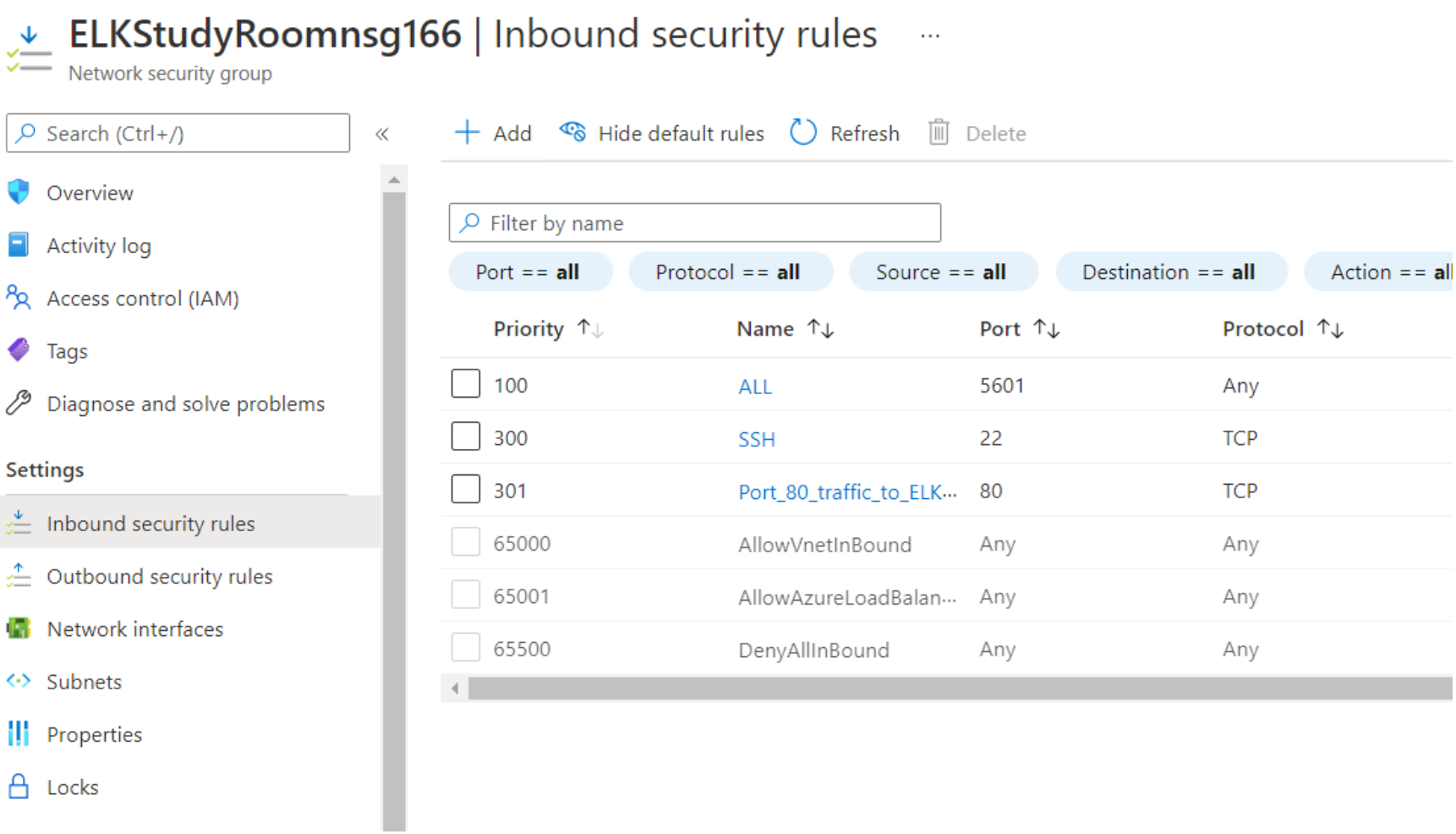
Destination port ranges *

5601

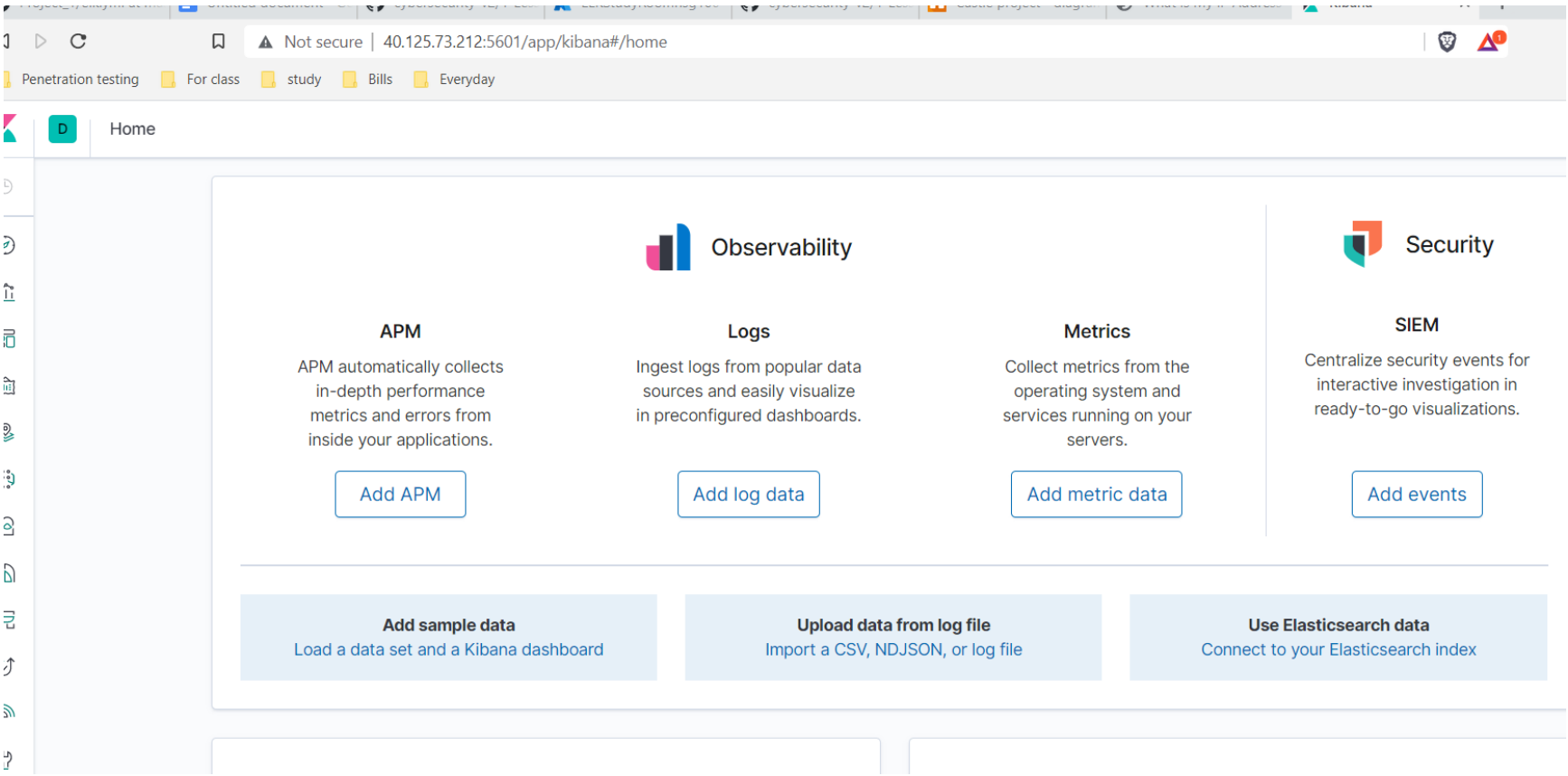
Protocol

- (•) Any
- ( ) TCP

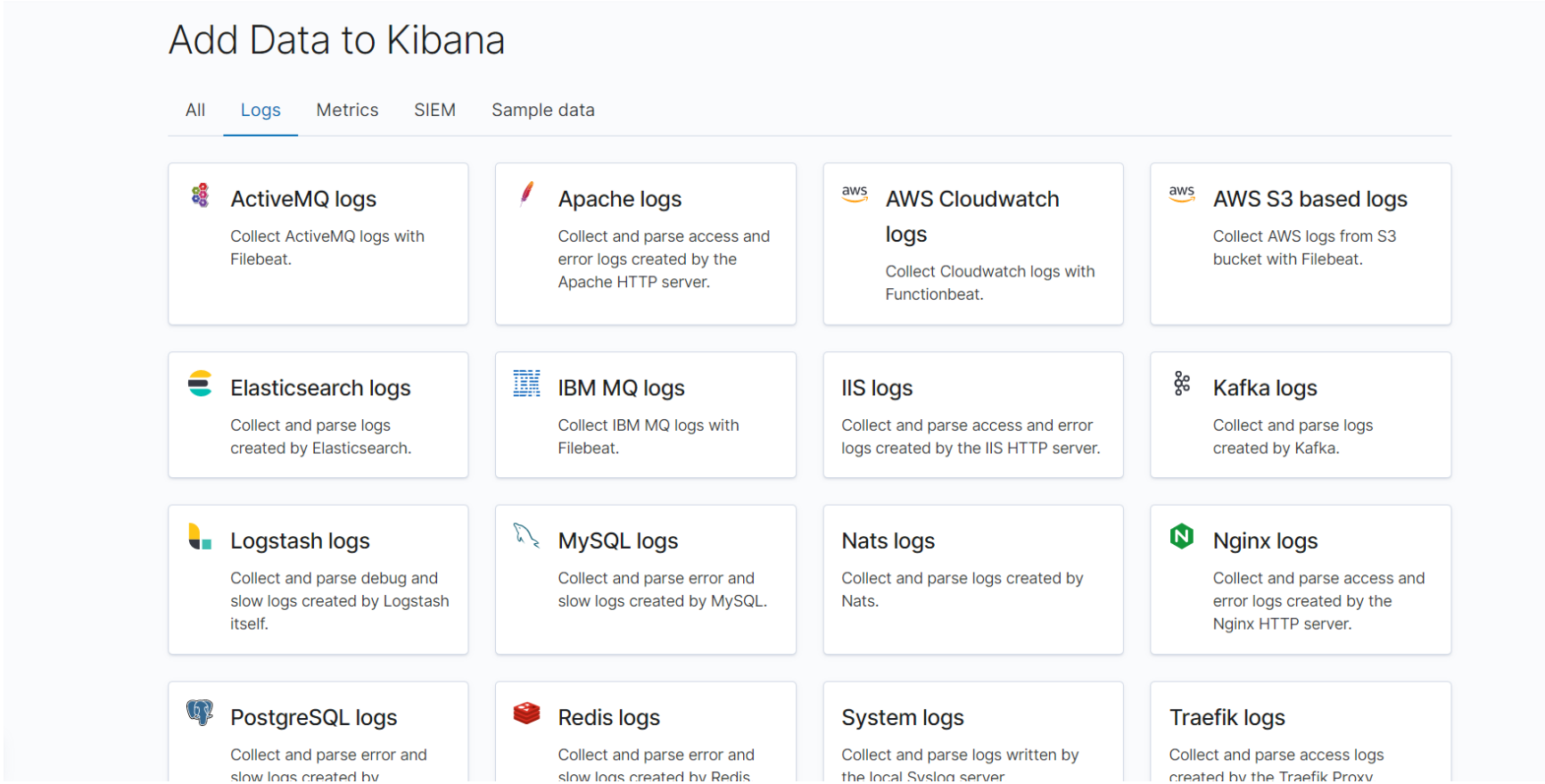
52.a-priority 100 all access to port 5601, port 80 traffic to vnet, ssh from host ip to elk



53.-Verify that you can load the ELK stack server from your browser at [http://[your.VM.IP]:5601/app/kibana](http://[your.VM.IP]:5601/app/kibana).



54-click on add log data, then system logs,finally, the Deb tab

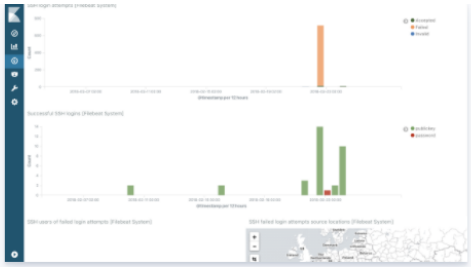

Add Data to Kibana
All
Logs
Metrics
SIEM
Sample data
ActiveMQ logs
Collect ActiveMQ logs with Filebeat.
Apache logs
Collect and parse access and error logs created by the Apache HTTP server.
AWS Cloudwatch logs
Collect Cloudwatch logs with Functionbeat.
AWS S3 based logs
Collect AWS logs from S3 bucket with Filebeat.
Elasticsearch logs
Collect and parse logs created by Elasticsearch.
IBM MQ logs
Collect IBM MQ logs with Filebeat.
IIS logs
Collect and parse access and error logs created by the IIS HTTP server.
Kafka logs
Collect and parse logs created by Kafka.
Logstash logs
Collect and parse debug and slow logs created by Logstash itself.
MySQL logs
Collect and parse error and slow logs created by MySQL.
Nats logs
Collect and parse logs created by Nats.
Nginx logs
Collect and parse access and error logs created by the Nginx HTTP server.
PostgreSQL logs
Collect and parse error and
Redis logs
Collect and parse error and
System logs
Collect and parse logs written by
Traefik logs
Collect and parse access logs

54.a

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.

View exported fields



Self managed | Elastic Cloud

Getting Started

macOS | DEB | RPM

1 Download and install Filebeat

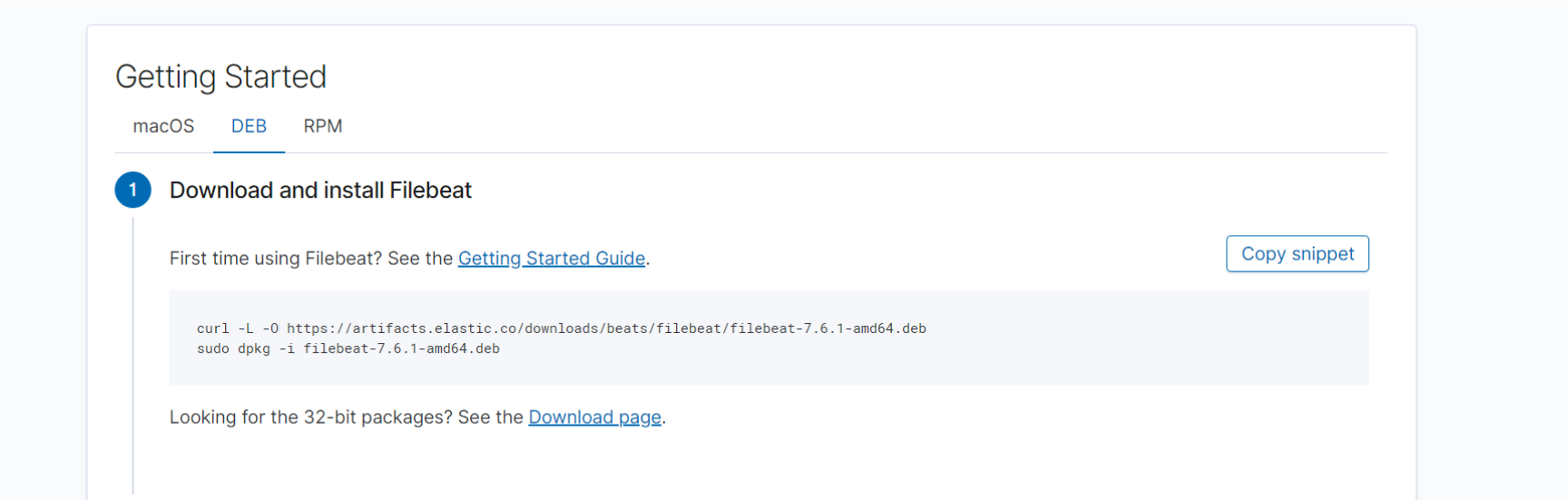
First time using Filebeat? See the Getting Started Guide.

Copy snippet

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-darwin-x86_64.tar.gz
tar xzvf filebeat-7.6.1-darwin-x86_64.tar.gz
cd filebeat-7.6.1-darwin-x86_64/
```

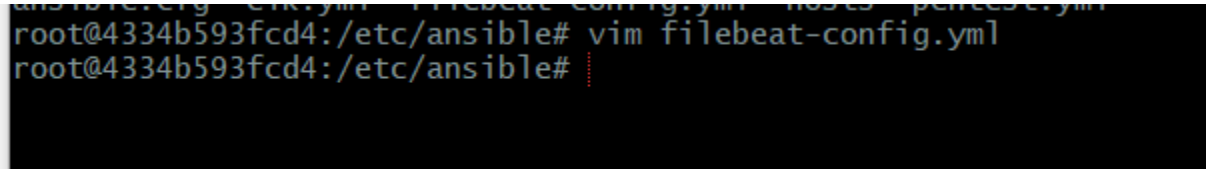
2 Edit the configuration

54.b

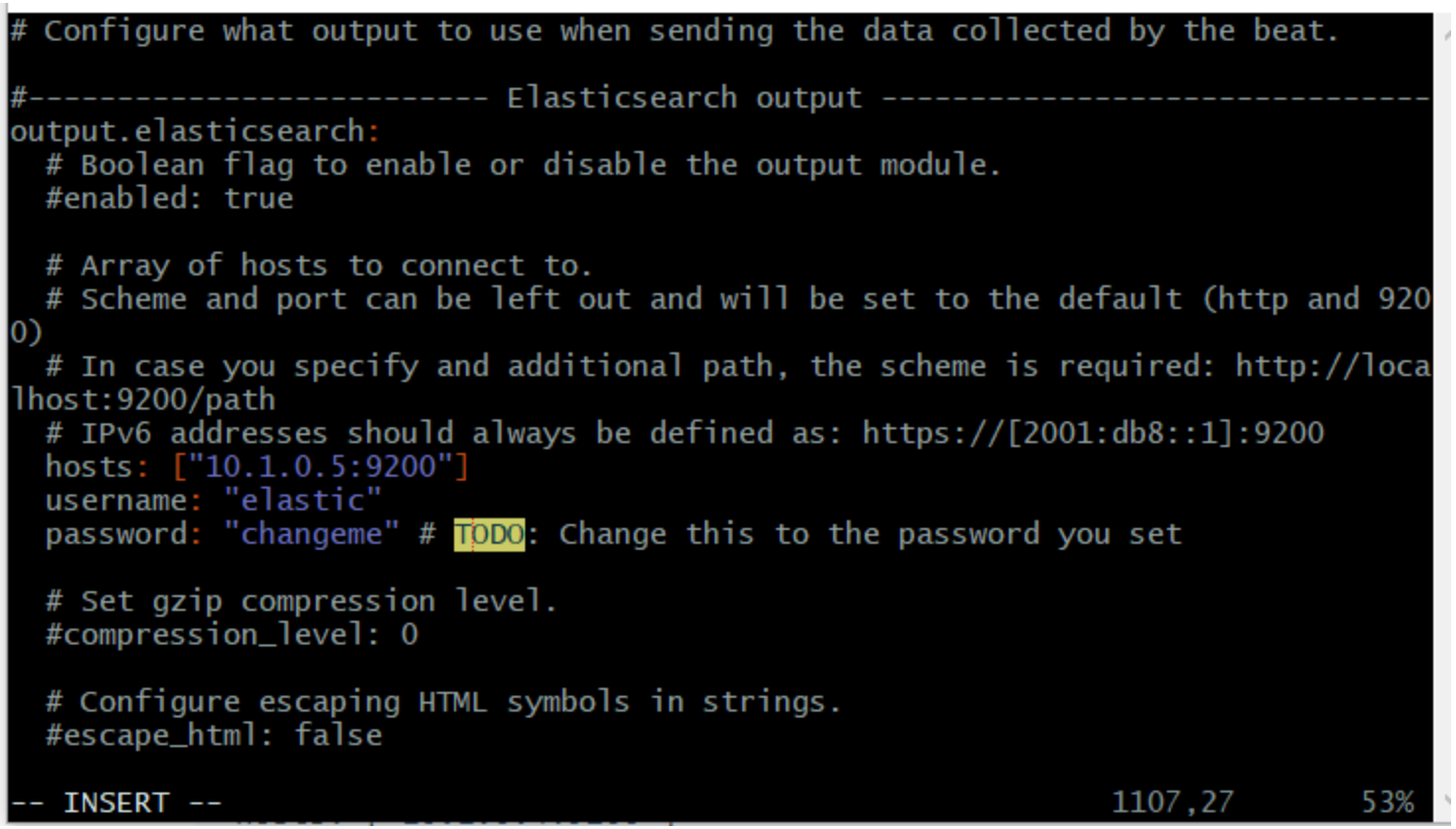


55-create a filebeat configuration file

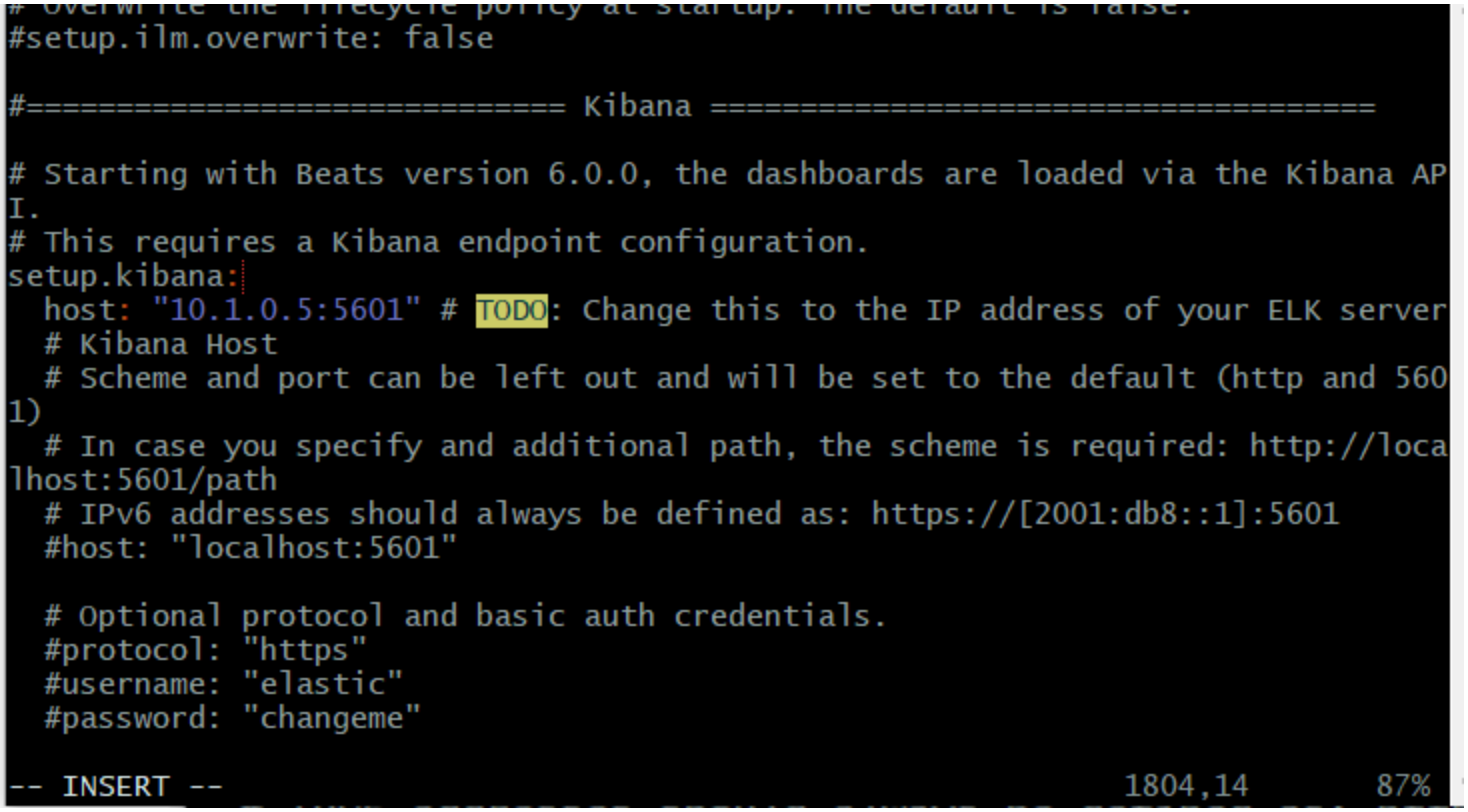
55.a



55.b-got to line 1106 and change ip address to elk vm ip



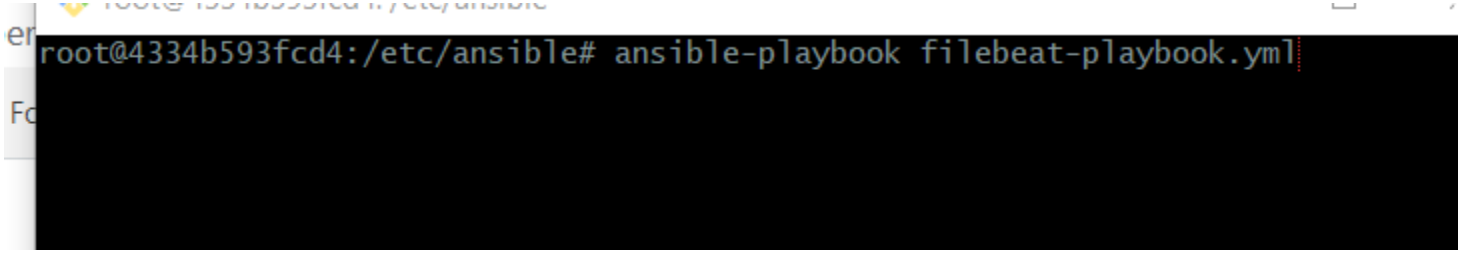
55.c-same thing for line 1806



56-install a filebeat installation playbook

```yaml
---
- name: Installing and Launch Filebeat
  hosts: webservers
  become: yes
  tasks:
    # Use command module
  - name: Download filebeat .deb file
    command: curl -L -O https://artifacts.elastic.co/downloads/beats/fileb

    # Use command module
  - name: Install filebeat .deb
    command: dpkg -i filebeat-7.6.1-amd64.deb

    # Use copy module
  - name: Drop in filebeat.yml
    copy:
      src: /etc/ansible/files/filebeat-config.yml
      dest: /etc/filebeat/filebeat.yml

    # Use command module
  - name: Enable and Configure System Module
    command: filebeat modules enable system

    # Use command module
  - name: Setup filebeat
    command: filebeat setup

    # Use command module
  - name: Start filebeat service
    command: service filebeat start

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

57-run the playbook



57.a