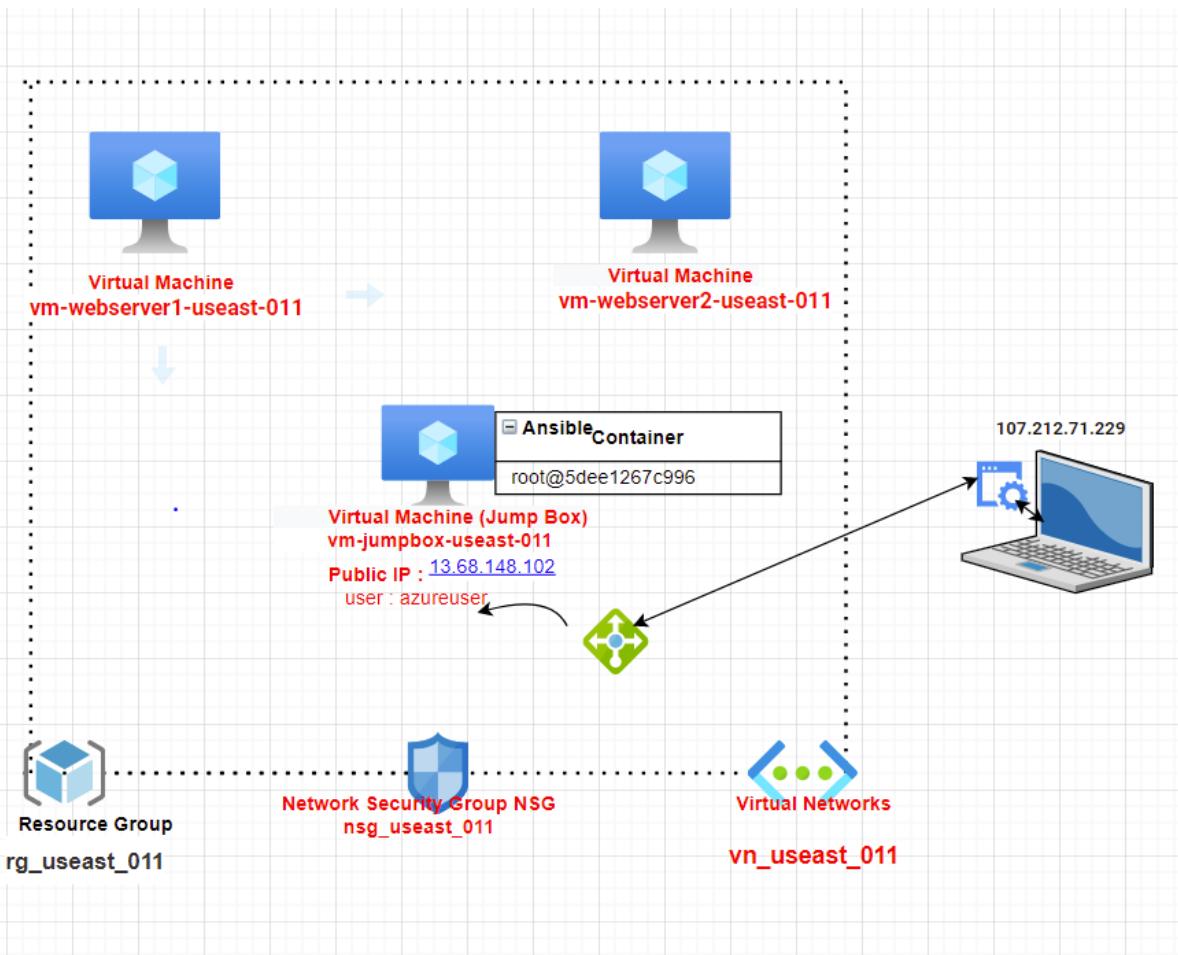


Deepa's Reference Diagram



1. Create free Azure account -

Go to <https://azure.microsoft.com/en-us/free/> and click on “Start Free”

Follow document(Individual Azure Setup Guide .pdf) for more details -

https://drive.google.com/file/d/1qQCBCO_PP6sBYr1CzWtvISGjKcfjVwnp/view?usp=sharing

2. The first step to creating an environment in Azure is to create a resource group.

My resource group : rg_useast_011

If you see this, click on this or search here -

The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the URL 'portal.azure.com/#home'. Below the navigation bar, there is a search bar containing the text 'resource' and a dropdown menu labeled 'Services' with 'Resource groups' selected. The main content area is titled 'Add new Resource Group' and shows a breadcrumb trail: 'Home > Resource groups'. The 'Resource groups' page has a header with buttons for '+ Add', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Feedback'. There is also a filter bar with fields for 'Subscription' (set to 'all') and 'Location' (set to 'all'). The message 'Showing 1 to 3 of 3 records.' is displayed below the filter bar.

Change highlighted values and click "Review + create"

Also created all the resources in the same “Region” (Like US East or US West)

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 * ⓘ rg_useast_011 ✓

Resource details

Region * ⓘ (US) East US

Review + create < Previous Next : Tags >

Create a resource group

...

Validation passed.

Basics Tags Review + create

Basics

Subscription Azure subscription 1
Resource group rg_useast_011
Region East US

Tags

None

Create

< Previous

Next >

Download a template for automation

Check name and region is correct.

Home >

Resource groups

...

Default Directory

+ Add Manage view Refresh Export to CSV Open query Assign tags Feedback

Filter for any field...

Subscription == all

Location == all

Add filter

No grouping

Showing 1 to 4 of 4 records.

Name ↑↓

Subscription ↑↓

Location ↑↓

deep-useast-rg

Azure subscription 1

East US

NetworkWatcherRG

Azure subscription 1

West US 2

rg_east_redteam

Azure subscription 1

West US 2

rg_useast_011

Azure subscription 1

East US

3. Create Virtual Network

Gives the ability to create a network to connect all different resources to connect together

My virtual networks : vn_useast_011

The screenshot shows the 'Virtual networks' blade in the Azure portal. On the left, there's a list of existing virtual networks: 'deep-useast-rg-vnet' and 'west_vn_1'. On the right, the 'Basics' tab is selected for creating a new VNet. The 'Project details' section shows 'Subscription' set to 'Azure subscription 1' and 'Resource group' set to 'rg_useast_011'. The 'Instance details' section shows 'Name' set to 'vn_useast_011' and 'Region' set to '(US) East US'. A yellow circle highlights the 'Review + create' button at the bottom of the form. Below the form, there are navigation links: '< Previous', 'Page 1 of 1', 'Next : IP Addresses >', and 'Download a template for automation'.

Leave the rest of the settings as it is.

4. Network security group(NSG)

Network security groups ⚡ ...

Default Directory



Filter for any field...

Subscription == all

Showing 1 to 7 of 7 records.

My network security group : nsg_useast_011

Network security g... <>

Default Directory

+ Add Manage view ...

Filter for any field...

Name ↑↓

- deep_useast_nsg
- deepJumpBoxEast-nsg
- deepWebServer1East-nsg
- deepWebServer2East-nsg
- Jump-Box-Provisioner-nsg
- nsg_west_redteam
- web-2-nsg

Create network security group <>

Basics Tags Review + create

Project details

Subscription * Azure subscription 1

Resource group * rg_useast_011 Create new

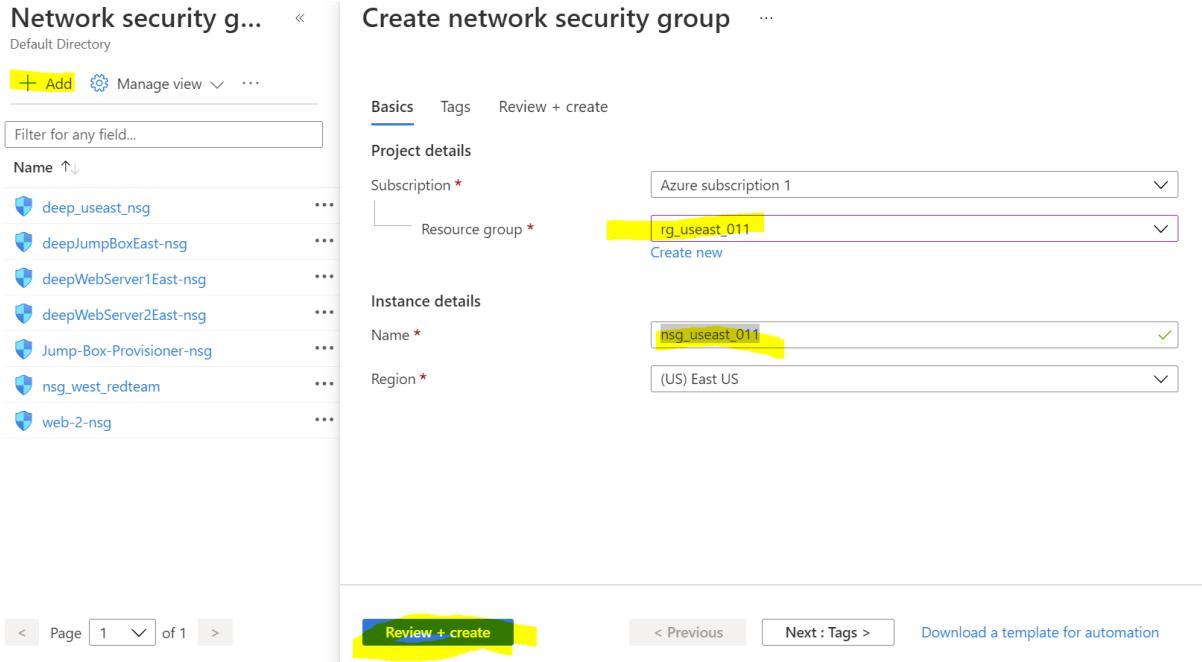
Instance details

Name * nsg_useast_011

Region * (US) East US

< Previous Next : Tags > Download a template for automation

Review + create



Create inbound security group - Below rule will deny all the traffic

nsg_useast_011 | Inbound security rules <>

Search (Ctrl+/)

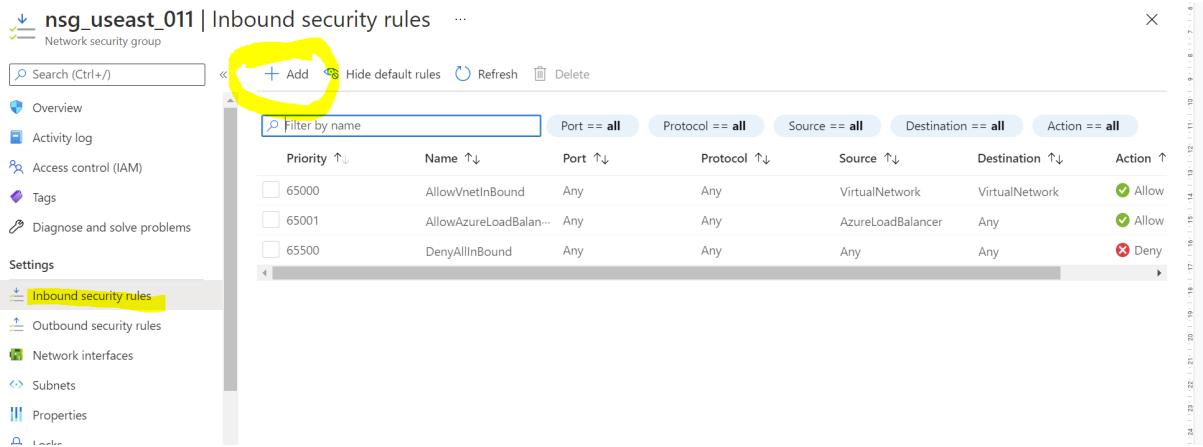
+ Add Hide default rules Refresh Delete

Filter by name

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Inbound security rules Outbound security rules Network interfaces Subnets Properties



Source ⓘ

Any



Source port ranges * ⓘ

*

Destination ⓘ

Any



Service ⓘ

Custom



Destination port ranges * ⓘ

*



Protocol

Any

TCP

UDP

ICMP

Action
 Allow
 Deny

Priority * ⓘ
 ✓

Name *
 ✓

Description
 ✓

Add
Cancel

5. Virtual machines :
- My jumpbox : vm-jumpbox-useast-011
 Jumpbox username : azureuser

Virtual machines

Default Directory

Filter for any field...

	Name	Subscription
<input type="checkbox"/>	deepJumpBoxEast	Azure subscription 1
<input type="checkbox"/>	deepWebServer1E...	Azure subscription 1
<input type="checkbox"/>	deepWebServer2E...	Azure subscription 1
<input type="checkbox"/>	Jump-Box-Provisi...	Azure subscription 1
<input type="checkbox"/>	web-1	Azure subscription 1
<input type="checkbox"/>	web-2	Azure subscription 1

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 * ⓘ

Resource group * ⓘ

Instance details

Virtual machine name * ⓘ ✓

Region * ⓘ ✓

Availability options ⓘ ✓

Availability options ⓘ

No infrastructure redundancy required

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

Info 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

Command to generate public keys

- Open gitbash
- Ssh-keygen(keyphrase(mykey) and path blank) (command to create public key)
- Cat ~/ssh/id_rsa.pub (command to view public key)

```
batra@DESKTOP-8G4KI38 MINGW64 ~
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/c/users/batra/.ssh/id_rsa):
/c/Users/batra/.ssh/id_rsa already exists.
overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /c/Users/batra/.ssh/id_rsa
Your public key has been saved in /c/Users/batra/.ssh/id_rsa.pub
The key's fingerprint is:
SHA256:i3o/I3kyeRqgJRxLx5npDZEzr203u5FkOHD0H3CU+0 batra@DESKTOP-8G4KI38
The key's randomart image is:
+---[RSA 3072]---+
| ..*+.o .o |
| =o++o* o |
| .o o*+= | |
| .o o==o E |
| S .=.o. |
| =.o.. |
| ...=.. |
| .++=oo |
| +Xo...o |
+---[SHA256]---+
batra@DESKTOP-8G4KI38 MINGW64 ~
$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQDFIVbCCUhkSgBm/f6Px2+VWOnN+eYABuWa2
5QqPhfsg1x4n/yNGZiPXPfpfXb7jEY0w622keFoUN0wTHqnIAGTdTYocstDygHVCjwuy/lrwTk
gOX7eG4oStvKcsZsdngL4/hulweog7C9YUhP9V+cLx6aD8iKO7W6qPU7x60bEO5OZzOlQr
zLDsFFF7vHwEoEE80A4frsKnMab/uYm6jDZ1d04iead/zHuCvIm0CP7pal0Zj0ipzNOozT9+a
K/ecp1lgEOYJcWAio7z87cl69LmQminGLHHOfZm76pOTjMxiflVZ+KX/AY2ir2zAHW67ZEpsf
L7sLPiNAvhVzc1ZqM9kSPUk9U/qYvNAQUhq0/tPc8324ZcPARbn92ovkwkzkoz9Bf6mh24xN
PP3ai5vvLCbftLPw0KmfNJad+ZU/Z77ZUGHjjJDpWJabvyeShgjBHahzWogMzn+8EJkMtTx
QyJaNXaNi4qwPwrP7OFaZ/fzEwQIneiEkHZDasNd7b171c=
```

(remove the last part batra@DESKTOP-8G4KI38)

ssh-rsa

AAAAB3NzaC1yc2EAAAQABAAABgQDFIVbCCUhkSgBm/f6Px2+VWOnN+eYABuWa2
5QqPhfsg1x4n/yNGZiPXPfpfXb7jEY0w622keFoUN0wTHqnIAGTdTYocstDygHVCjwuy/lrwTk
gOX7eG4oStvKcsZsdngL4/hulweog7C9YUhP9V+cLx6aD8iKO7W6qPU7x60bEO5OZzOlQr
zLDsFFF7vHwEoEE80A4frsKnMab/uYm6jDZ1d04iead/zHuCvIm0CP7pal0Zj0ipzNOozT9+a
K/ecp1lgEOYJcWAio7z87cl69LmQminGLHHOfZm76pOTjMxiflVZ+KX/AY2ir2zAHW67ZEpsf
L7sLPiNAvhVzc1ZqM9kSPUk9U/qYvNAQUhq0/tPc8324ZcPARbn92ovkwkzkoz9Bf6mh24xN
PP3ai5vvLCbftLPw0KmfNJad+ZU/Z77ZUGHjjJDpWJabvyeShgjBHahzWogMzn+8EJkMtTx
QyJaNXaNi4qwPwrP7OFaZ/fzEwQIneiEkHZDasNd7b171c=

SSH public key source

SSH public key *

[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

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab.

Review + create < Previous Next : Disks >

Select Networking tab and create new Public IP, select static

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings, ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancer. [Learn more](#)

Network interface

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

Virtual network *

Subnet *

Public IP

NIC network security group None Basic Advanced

Review + create < Previous Next : Management > **OK**

The screenshot shows the Azure portal interface for a virtual machine named 'vm-jumpbox-useast-011'. The 'Essentials' section displays basic information such as Resource group (rg_useast_011), Status (Running), Location (East US), Subscription (Azure subscription 1), and Tags. The Public IP address is listed as 13.68.148.102. The 'Virtual machine' properties show the computer name as vm-jumpbox-useast-011, operating system as Linux, publisher as Canonical, and offer as UbuntuServer. The 'Networking' section shows the public IP address as 13.68.148.102, private IP address as 10.2.0.4, and private IP address (IPv6) as -. The 'Properties' tab is selected.

Not able to access above Public IP 13.68.148.102, because of the network security group Step 4 (Priority 4090(Firewall Rule))

Webserver 1: vm-webserver1-useast-011

Availability set : as-useast-011 (Availability set: If one the server is down traffic will go to other)

Create a virtual machine

The screenshot shows the 'Create a virtual machine' wizard on the 'Basics' tab. The 'Subscription' dropdown is set to 'Azure subscription 1'. The 'Resource group' dropdown is set to 'rg_useast_011', with the 'Create new' option visible. The 'Virtual machine name' field contains 'vm-webserver1-useast-011'. The 'Region' dropdown is set to '(US) East US'. The 'Availability options' dropdown is set to 'Availability set'.

Create availability set

Group two or more VMs in an availability set to ensure that at least one is available during planned or unplanned maintenance events. [Learn more](#)

Name *

Fault domains 2

Update domains 5

Use managed disks No (Classic) Yes (Aligned)

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 *

OK

Create a virtual machine

Size *

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 *

SSH public key source

SSH public key *

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

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
[Learn more ↗](#)

Network interface

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

Virtual network * ⓘ ▼
[Create new](#)

Subnet * ⓘ ▼
[Manage subnet configuration](#)

Public IP ⓘ ▼
[Create new](#)

NIC network security group ⓘ None
 Basic
 Advanced

[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

Select inbound ports * ▼

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Review + create

< Previous

Next : Disks >

Webserver 2: vm-webserver2-useast-011

Create a virtual machine

Subscription * ⓘ ▼

Resource group * ⓘ ▼
[Create new](#)

Instance details

Virtual machine name * ⓘ ✓

Region * ⓘ ▼

Availability options ⓘ ▼

Availability set * ⓘ ▼
[Create new](#)

Image * ⓘ ▼
[See all images](#)

Size * ⓘ ▼
[See all sizes](#)

Create a virtual machine

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
[Learn more ↗](#)

Network interface

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

Virtual network * ⓘ ▼
[Create new](#)

Subnet * ⓘ ▼
[Manage subnet configuration](#)

Public IP ⓘ ▼
[Create new](#)

NIC network security group ⓘ None Basic Advanced

See all sizes

Administrator account

Authentication type SSH public key Password

Info 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 * ✓

SSH public key source ▾

SSH public key * ✓

Info Learn more about creating and using SSH keys in Azure ↗

Inbound port rules

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 * Allow selected ports None

Select inbound ports * ▾

Warning This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Review + create < Previous Next : Disks >

5. Create network security group to access from/to jumpbox

Check Your IP using -
<https://whatismyipaddress.com/>

107.212.71.229

Provide IP while creating inbound security rules as in image below:

Network security g... < Default Directory

+ Add Manage view ...

Filter for any field...

Name ↑

- deep_east_nsg
- deepJumpBoxEast-nsg
- deepWebServer1East-nsg
- deepWebServer2East-nsg
- Jump-Box-Provisioner-nsg
- nsg_useast_011
- nsg_west_redteam
- vm-jumpbox-useast-011-nsg
- vm-webserver1-useast-011-nsg
- vm-webserver2-useast-011-nsg
- web-2-nsg

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

nsg_useast_011 | Inbound security rules

+ Add

Search (Ctrl+ /)

Port == all

Priority ↑

Source IP Addresses

Source IP addresses/CIDR ranges *

107.212.71.229

Source port ranges *

*

Destination VirtualNetwork

Service SSH

Destination port ranges 22

Protocol Any

TCP

UDP

ICMP

Protocol

- Any
- TCP
- UDP
- ICMP

Action

- Allow
- Deny

Priority *

3900

Name *

sshIntoJumpBox

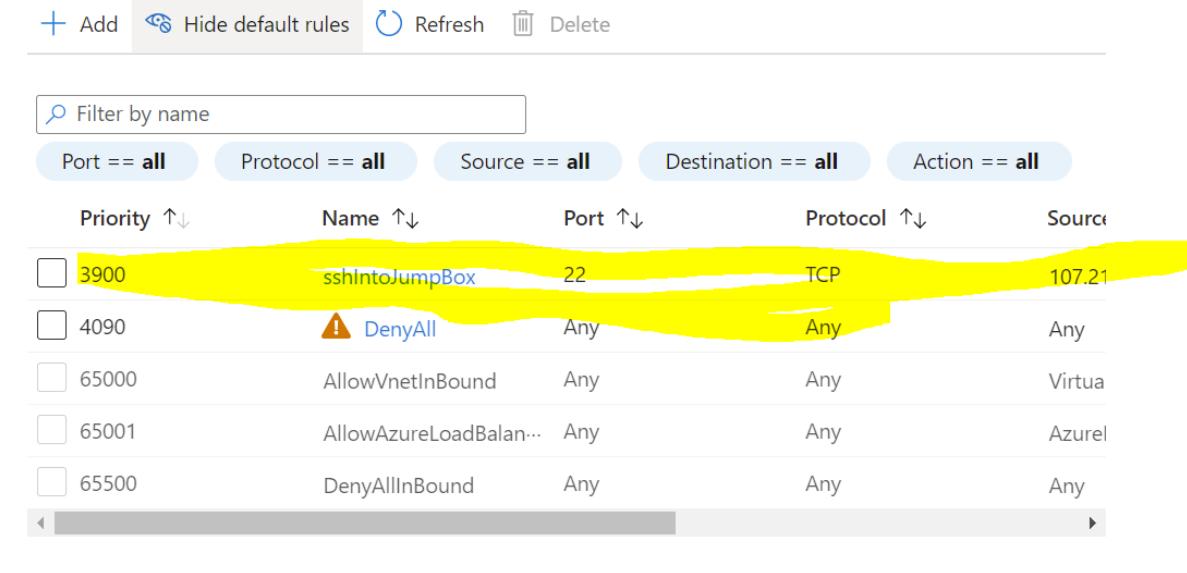
Description

Firewall Rule to ssh into Jumpbox

Add

Cancel

10:59 PM

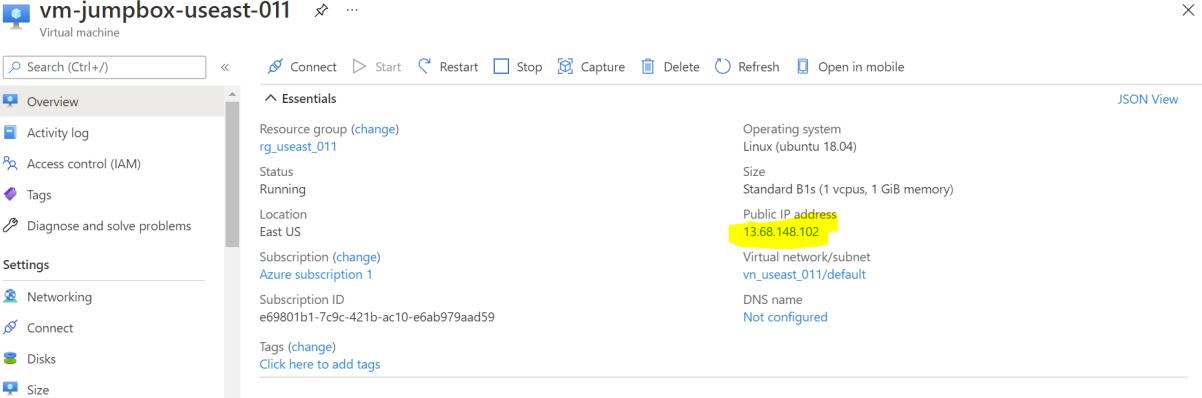


A screenshot of the Azure Firewall rules table. The table has columns for Priority, Name, Port, Protocol, and Source. A yellow highlight covers the first row, which contains the rule 'sshintoJumpBox' with port 22 and protocol TCP. Other rows include 'DenyAll' (port Any, protocol Any), 'AllowVnetInBound' (port Any, protocol Any), 'AllowAzureLoadBalanc...' (port Any, protocol Any), and 'DenyAllInBound' (port Any, protocol Any). The source for the highlighted rule is 107.21.

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source
<input type="checkbox"/> 3900	sshintoJumpBox	22	TCP	107.21
<input type="checkbox"/> 4090	⚠ DenyAll	Any	Any	Any
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	Virtua
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any	AzureI
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

Try to ssh into jumpbox

- Get IP and user of jumpbox



A screenshot of the Azure portal showing the details of a virtual machine named 'vm-jumpbox-useast-011'. The 'Overview' tab is selected. The public IP address '13.68.148.102' is highlighted with a yellow box. Other details shown include the resource group 'rg_useast_011', status 'Running', location 'East US', subscription 'Azure subscription 1', and tags.

IP : 13.68.148.102

User: azureuser

Open Gitbash

- Ssh user@ipAddress
- You have to enter your key that you added while creating public key

```
batra@DESKTOP-8G4KI38 MINGW64 ~
$ ssh azureuser@13.68.148.102
The authenticity of host '13.68.148.102 (13.68.148.102)' can't be established.
ECDSA key fingerprint is SHA256:rw8qwRsPNTkXWOTcSQ935p7HjPPcSUocplHbk\6hzAM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.68.148.102' (ECDSA) to the list of known hosts.
Enter passphrase for key '/c/Users/batra/.ssh/id_rsa': |
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1047-azure x86_64)

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

System information as of Thu May 13 03:04:17 UTC 2021

system load: 0.0          Processes:           110
Usage of /: 4.5% of 28.90GB   Users logged in:    0
Memory usage: 30%          IP address for eth0: 10.2.0.4
Swap usage:  0%          

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.

azureuser@vm-jumpbox-useast-011:~$ |
```

Check you have sudo permissions

Sudo echo "Hello"

Sudo apt update

```
azureuser@vm-jumpbox-useast-011:~$ sudo echo "Hello"
Hello
azureuser@vm-jumpbox-useast-011:~$ sudo apt update
Get:1 http://azure.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:4 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8570 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu bionic/universe Translation-en [4941 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [2068 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1735 kB]
Get:11 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [369 kB]
Get:12 http://azure.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [25.0 kB]
Get:13 http://azure.archive.ubuntu.com/ubuntu bionic-updates/multiverse Translation-en [6464 kB]
Get:14 http://azure.archive.ubuntu.com/ubuntu bionic-backports/main amd64 Packages [10.0 kB]
Get:15 http://azure.archive.ubuntu.com/ubuntu bionic-backports/main Translation-en [4764 B]
Get:16 http://azure.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 Packages [10.3 kB]
Get:17 http://azure.archive.ubuntu.com/ubuntu bionic-backports/universe Translation-en [4588 B]
Get:18 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [1725 kB]
Get:19 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [1125 kB]
Get:20 http://security.ubuntu.com/ubuntu bionic-security/universe Translation-en [253 kB]
Get:21 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [19.2 kB]
Get:22 http://security.ubuntu.com/ubuntu bionic-security/multiverse Translation-en [4412 B]
Fetched 21.4 MB in 5s (4211 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
azureuser@vm-jumpbox-useast-011:~$ |
```

sudo apt install docker.io

```
azureuser@vm-jumpbox-useast-011:~$ sudo apt install docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-headers-4.15.0-143
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  bridge-utils containerd pigz runc ubuntu-fan
Suggested packages:
  ifupdown aufs-tools cgroupfs-mount | cgroup-lite debootstrap docker-doc rinse zfs-fuse | zfsutils
The following NEW packages will be installed:
  bridge-utils containerd docker.io pigz runc ubuntu-fan
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 62.8 MB of archives.
After this operation, 320 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 pigz amd64 2.4-1 [57.4 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 bridge-utils amd64 1.5-15ubuntu1 [30.1 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 runc amd64 1.0.0~rc93~Ubuntu1~18.04.1 [4014 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 containerd amd64 1.3.3-0ubuntu1~18.04.4 [21.7 MB]
Get:5 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 docker.io amd64 20.10.2~0ubuntu1~18.04.2 [36.9 MB]
Get:6 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 ubuntu-fan all 0.12.10 [34.7 kB]
Fetched 62.8 MB in 1s (43.2 MB/s)
Preconfiguring packages ...
Selecting previously unselected package pigz.
(Reading database ... 76868 files and directories currently installed.)
Preparing to unpack .../0-pigz_2.4-1_amd64.deb ...
Unpacking pigz (2.4-1) ...
Selecting previously unselected package bridge-utils.
Preparing to unpack .../1-bridge-utils_1.5-15ubuntu1_amd64.deb ...
Unpacking bridge-utils (1.5-15ubuntu1) ...
Selecting previously unselected package runc.
Preparing to unpack .../2-runc_1.0.0~rc93~Ubuntu1~18.04.1_amd64.deb ...
Unpacking runc (1.0.0~rc93~Ubuntu1~18.04.1) ...
Selecting previously unselected package containerd.
Preparing to unpack .../3-containerd_1.3.3-0ubuntu1~18.04.4_amd64.deb ...
Unpacking containerd (1.3.3-0ubuntu1~18.04.4) ...
Selecting previously unselected package docker.io.
Preparing to unpack .../4-docker.io_20.10.2~0ubuntu1~18.04.2_amd64.deb ...
```

```
Preconfiguring packages ...
Selecting previously unselected package pigz.
(Reading database ... 76868 files and directories currently installed.)
Preparing to unpack .../0-pigz_2.4-1_amd64.deb ...
Unpacking pigz (2.4-1) ...
Selecting previously unselected package bridge-utils.
Preparing to unpack .../1-bridge-utils_1.5-15ubuntu1_amd64.deb ...
Unpacking bridge-utils (1.5-15ubuntu1) ...
Selecting previously unselected package runc.
Preparing to unpack .../2-runc_1.0.0~rc93-0ubuntu1~18.04.1_amd64.deb ...
Unpacking runc (1.0.0~rc93-0ubuntu1~18.04.1) ...
Selecting previously unselected package containerd.
Preparing to unpack .../3-containerd_1.3.3-0ubuntu1~18.04.4_amd64.deb ...
Unpacking containerd (1.3.3-0ubuntu1~18.04.4) ...
Selecting previously unselected package docker.io.
Preparing to unpack .../4-docker.io_20.10.2-0ubuntu1~18.04.2_amd64.deb ...
Unpacking docker.io (20.10.2-0ubuntu1~18.04.2) ...
Selecting previously unselected package ubuntu-fan.
Preparing to unpack .../5-ubuntu-fan_0.12.10_all.deb ...
Unpacking ubuntu-fan (0.12.10) ...
Setting up runc (1.0.0~rc93-0ubuntu1~18.04.1) ...
Setting up containerd (1.3.3-0ubuntu1~18.04.4) ...
Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service → /lib/systemd/system/containerd.service.
Setting up bridge-utils (1.5-15ubuntu1) ...
Setting up ubuntu-fan (0.12.10) ...
Created symlink /etc/systemd/system/multi-user.target.wants/ubuntu-fan.service → /lib/systemd/system/ubuntu-fan.service.
Setting up pigz (2.4-1) ...
Setting up docker.io (20.10.2-0ubuntu1~18.04.2) ...
Adding group 'docker' (GID 116) ...
Done.
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/systemd/system/docker.socket.
Processing triggers for systemd (237-3ubuntu10.47) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
azureuser@vm-jumpbox-useast-011:~$ |
```

sudo systemctl status docker

```
azureuser@vm-jumpbox-useast-011:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2021-05-13 03:25:17 UTC; 1min 24s ago
       Docs: https://docs.docker.com
 Main PID: 3104 (dockerd)
    Tasks: 8
   CGroup: /system.slice/docker.service
           └─3104 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.140791681Z" level=warning msg="Your kernel does not supp
May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.140955285Z" level=warning msg="Your kernel does not supp
May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.141347896Z" level=info msg="Loading containers: start."
May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.333967964Z" level=info msg="Default bridge (dockero0) is
May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.418462143Z" level=info msg="Loading containers: done."
May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.503657067Z" level=warning msg="Not using native diff for
May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.504238482Z" level=info msg="Docker daemon" commit="20.10
May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.504516589Z" level=info msg="daemon has completed initial
May 13 03:25:17 vm-jumpbox-useast-011 systemd[1]: Started Docker Application Container Engine.
May 13 03:25:17 vm-jumpbox-useast-011 dockerd[3104]: time="2021-05-13T03:25:17.570399917Z" level=info msg="API listen on /var/run/docke
lines 1-19/19 (END)
```

sudo docker pull cyberxsecurity/ansible

```
[lines 1-19/19 (END)]
[1]+  Stopped                  sudo systemctl status docker

azureuser@vm-jumpbox-useast-011:~$ sudo docker pull cyberxsecurity/ansible
Using default tag: latest
latest: Pulling from cyberxsecurity/ansible
7ddbc47eeb70: Pull complete
c1bbdc448b72: Pull complete
8c3b70e39044: Pull complete
45d437916d57: Pull complete
78440e84779a: Pull complete
b6f0115afe25: Pull complete
Digest: sha256:a245954c7eda5d15ec6bc8cca2ab129e12491e711de0db63344ebf40fa35d26b
Status: Downloaded newer image for cyberxsecurity/ansible:latest
docker.io/cyberxsecurity/ansible:latest
azureuser@vm-jumpbox-useast-011:~$ |
```

sudo docker run -ti cyberxsecurity/ansible:latest bash

```
docker: [1] CyberXSecurIty/Ansible:latest
azureuser@vm-jumpbox-useast-011:~$ sudo docker run -ti cyberxsecurity/ansible:latest bash
root@5dee1267c996:~# |
```

If you forgotten your password or user and need to reset - Regenerate key again in Gitbash

Ssh-keygen

Now in Virtual Machine

vm-jumpbox-useast-011 | Reset password

Virtual machine

Search (Ctrl+ /)

Update Discard

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 *

The value must not be empty.

The value must be between 1 and 64 characters long.

SSH public key *

Paste your SSH public key here...

Reset password

Redeploy + reapply

Ubuntu Advantage support pl...

Serial console

Connection troubleshoot

Add network security rule to access from jumpbox

nsg_useast_011 | Inbound security rules

+ Add Manage view ...

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

Source

IP Addresses

Source IP addresses/CIDR ranges *

13.68.148.102

Port == all

Priority

3900

4090

65000

65001

65500

Destination

VirtualNetwork

Service

SSH

Destination port ranges

22

Protocol

Any

TCP

UDP

Action
 Allow
 Deny

Priority * ⓘ
 ✓

Name *
 ✓

Description
 ✓

Add Cancel

nsg_useast_011 | Inbound security rules

Network security group

Subscription 'Azure subscription 1' has a remaining credit of \$192.94.
Click here to upgrade to a Pay-As-You-Go subscription.

Priority ↑	Name ↑	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑
3800	sshFromJumpbox	22	TCP	13.68.148.102	VirtualNetwork	Allow
3900	sshToJumpBox	22	TCP	107.212.71.229	VirtualNetwork	Allow
4090	DenyAll	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

6. Create key to access ansible

To create a key you have to be at root

```
azureuser@vm-jumpbox-useast-011:~$ sudo docker run -ti cyberxsecurity/ansible:latest bash
root@5dee1267c996:~#
```

```

root@5dee1267c996:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:t/asq/dhvYIGfdet4R2LFG/cppyCtoJu1D1pEGfAz08 root@5dee1267c996
The key's randomart image is:
+---[RSA 2048]---+
|   o = E   . |
| * o   . o   |
| . . . = =   |
| . o S.+ = =.*|
| . . B.=.*...=o|
| . . o +.+. . |
| o. . .+o..    |
+---[SHA256]----+
root@5dee1267c996:~# cat /root/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQADLE8xKjMVoVuljD0a/m7Mj6qywBDiws8Yxji8zBgESS4dyTELQkO0LkUVGyTix68UIY5AberusogEmUyS9ExqA0q+jRTDVTbF
2PLC9Njhf1uAGdhCIly807IF9ZkoJPrxt/lul//DA/hvV/yyfTLaHO9/cQOJribT3eo7PiDd
70ctsoEEJohH25yXDluuQhp3QH8V/mA5gDtQ/YJ6gF94Kyh684KHSYml7dY7uDEz
mMs/BAZSEHegJQYqJvC37oXuiMKr7aM4GwBLf0+YrkvnQFnCUR5Qql8/m8Ymqkii4nVwQXv54g9pyfvAq+B8baH7Rxh6sJOHACF8mBfkQLzR
root@5dee1267c996:~|

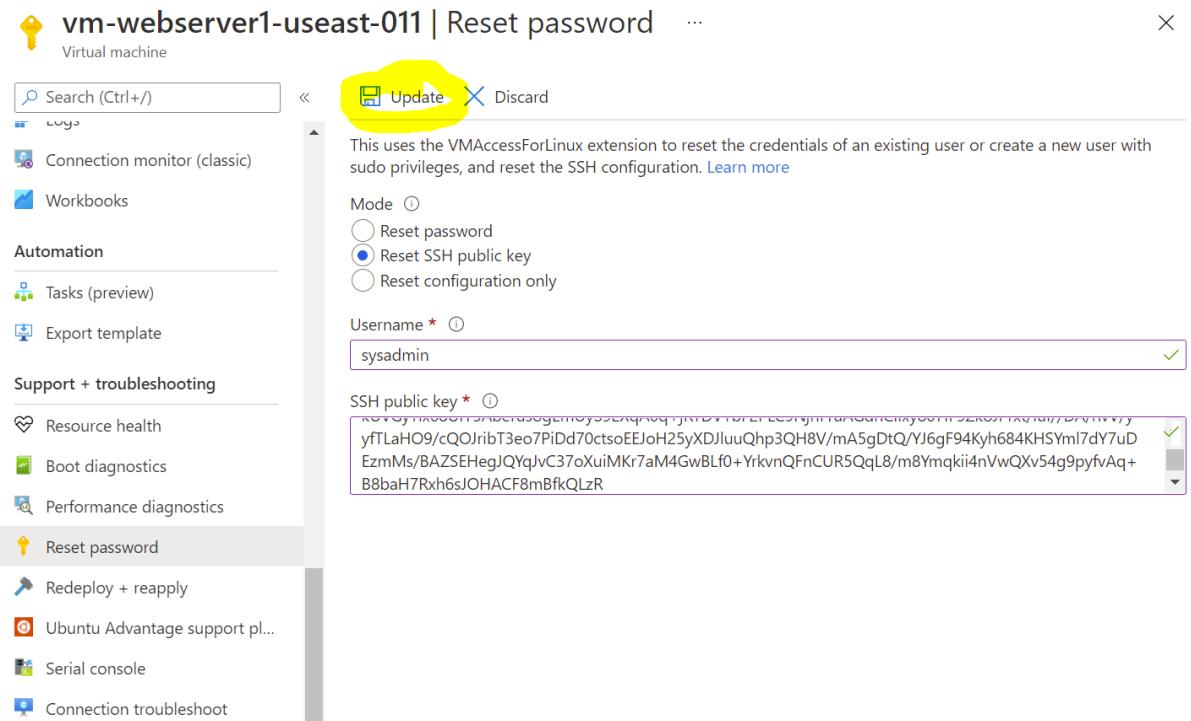
```

ssh-rsa

AAAAB3NzaC1yc2EAAAQABAAQADLE8xKjMVoVuljD0a/m7Mj6qywBDiws8Yxji8zBgEsS4dyTELQkO0LkUVGyTix68UIY5AberusogEmUyS9ExqA0q+jRTDVTbF
 2PLC9Njhf1uAGdhCIly807IF9ZkoJPrxt/lul//DA/hvV/yyfTLaHO9/cQOJribT3eo7PiDd
 70ctsoEEJohH25yXDluuQhp3QH8V/mA5gDtQ/YJ6gF94Kyh684KHSYml7dY7uDEz
 mMs/BAZSEHegJQYqJvC37oXuiMKr7aM4GwBLf0+YrkvnQFnCUR5Qql8/m8Ymqkii4nVwQXv54g9pyfvAq+B8baH7Rxh6sJOHACF8mBfkQLzR

Go to Azure and add public key to Webserver1 and Webserver2

The screenshot shows the Azure portal interface. On the left, the 'Virtual machines' blade is open, listing several VMs: 'Jump-Box-Provisioner', 'vm-jumpbox-useast-011', 'vm-webserver1-useast-011', and 'vm-webserver2-useast-011'. The 'vm-webserver1-useast-011' item is selected and highlighted with a yellow box. On the right, the details for this VM are shown. Under the 'Reset password' section, there is a 'Mode' dropdown with three options: 'Reset password' (radio button unselected), 'Reset SSH public key' (radio button selected), and 'Reset configuration only' (radio button unselected). Below the mode is a 'Username' field containing 'sysadmin' (also highlighted with a yellow box). Underneath the username is a 'SSH public key' field, which contains the previously copied RSA public key. A tooltip above the 'SSH public key' field explains: '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'.



Virtual machines

Default Directory

Add Switch to classic

Filter for any field...

Name ↑

Jump-Box-Provisioner

vm-jumpbox-useast-011

vm-webserver1-useast-011

vm-webserver2-useast-011

Connection monitor (classic)

Workbooks

Automation

Tasks (preview)

Export template

Support + troubleshooting

Resource health

Boot diagnostics

Performance diagnostics

Reset password

Redeploy + reapply

Ubuntu Advantage support pl...

Serial console

Connection troubleshoot

vm-webserver2-useast-011 | Reset password

Virtual machine

Update Discard

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 *

SSH public key *

Successfully reset SSH key 11:49 PM

Successfully reset SSH key for virtual machine 'vm-webserver2-useast-011'.

Get the private Ip of Webserver1 and webserver2

Private Ip webserver1 : 10.2.0.5

Private Ip webserver2: 10.2.0.6

vm-webserver1-useast-011

Computer name	vm-webserver1-useast-011	Public IP address	-
Operating system	Linux (ubuntu 18.04)	Public IP address (IPv6)	-
Publisher	Canonical	Private IP address	10.2.0.5
Offer	UbuntuServer	Private IP address (IPv6)	-
Plan	18.04-LTS	Virtual network/subnet	vn_useast_011/default
VM generation	V1	DNS name	-
Agent status	Ready	Size	
Agent version	2.2.54.2	Size	Standard B1s
Host group	None	vCPUs	1
Host	-	RAM	1 GiB
Proximity placement group	-	Disk	
Colocation status	N/A	OS disk	vm-webserver1-useast-011_OsDisk_1_a82946ea40744e43bb32c3c203371746
Availability + scaling		Azure disk encryption	Not enabled
Availability zone	-	Ephemeral OS disk	N/A
Scale Set	-	Data disks	0

vm-webserver2-useast-011

Computer name	vm-webserver2-useast-011	Public IP address	-
Operating system	Linux (ubuntu 18.04)	Public IP address (IPv6)	-
Publisher	Canonical	Private IP address	10.2.0.6
Offer	UbuntuServer	Private IP address (IPv6)	-
Plan	18.04-LTS	Virtual network/subnet	vn_useast_011/default
VM generation	V1	DNS name	-
Agent status	Ready	Size	
Agent version	2.2.54.2	Size	Standard B1s
Host group	None	vCPUs	1
Host	-	RAM	1 GiB
Proximity placement group	-	Disk	
Colocation status	N/A	OS disk	vm-webserver2-useast-011_OsDisk_1_b04fff562d6340fc9ad6c67361058d8
Availability + scaling		Azure disk encryption	Not enabled
Availability zone	-	Ephemeral OS disk	N/A
Scale Set	-	Data disks	0

In gitbash try to ssh into webserver1

```
root@5dee1267c996:~# ssh sysadmin@10.2.0.5
The authenticity of host '10.2.0.5 (10.2.0.5)' can't be established.
ECDSA key fingerprint is SHA256:hE92/QoLpWSZJ8bwRlueju5muLYUiBwncxVRN2o3YaA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.2.0.5' (ECDSA) to the list of known hosts.
Enter passphrase for key '/root/.ssh/id_rsa':
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1047-azure x86_64)

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

 System information as of Thu May 13 03:52:56 UTC 2021

 System load:  0.08           Processes:      108
 Usage of /:   4.5% of 28.90GB  Users logged in:  0
 Memory usage: 20%           IP address for eth0: 10.2.0.5
 Swap usage:   0%

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.
```

```
sysadmin@vm-webserver1-useast-011:~$ |
```

```

sysadmin@vm-webserver1-useast-011:~$ exit
logout
Connection to 10.2.0.5 closed.
root@5dee1267c996:~# ssh sysadmin@10.2.0.6
The authenticity of host '10.2.0.6 (10.2.0.6)' can't be established.
ECDSA key fingerprint is SHA256:ns6jIExonLrFdo4ocL1bv7fbyvexBc2zKBI8uPtph0I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.2.0.6' (ECDSA) to the list of known hosts.
Enter passphrase for key '/root/.ssh/id_rsa':
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1047-azure x86_64)

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

 System information as of Thu May 13 03:54:16 UTC 2021

 System load:  0.06           Processes:      108
 Usage of /:   4.5% of 28.90GB  Users logged in:  0
 Memory usage: 20%           IP address for eth0: 10.2.0.6
 Swap usage:   0%

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.

sysadmin@vm-webserver2-useast-011:~$ |

```

To list all the containers

sudo docker container list -a

```

sysadmin@vm-webserver2-useast-011:~$ exit
logout
Connection to 10.2.0.6 closed.
root@5dee1267c996:~# exit
exit
azureuser@vm-jumpbox-useast-011:~$ sudo docker container list -a
CONTAINER ID   IMAGE          COMMAND   CREATED        STATUS          PORTS     NAMES
5dee1267c996   cyberxsecurity/ansible:latest   "bash"   27 minutes ago   Exited (0)  15 seconds ago   nifty_merkle
azureuser@vm-jumpbox-useast-011:~$ |

```

To go back to your container

- sudo docker start nifty_merkle
- sudo docker attach nifty_merkle

```

azureuser@vm-jumpbox-useast-011:~$ sudo docker container list -a
CONTAINER ID   IMAGE          COMMAND   CREATED        STATUS          PORTS     NAMES
5dee1267c996   cyberxsecurity/ansible:latest   "bash"   29 minutes ago   Exited (0)  About a minute ago   nifty_merkle
azureuser@vm-jumpbox-useast-011:~$ sudo docker start nifty_merkle
nifty_merkle
azureuser@vm-jumpbox-useast-011:~$ sudo docker attach nifty_merkle
root@5dee1267c996:~# |

```

Configure ansible in container file

cd /etc/ansible

ls -ltr

```
root@5dee1267c996:~# cd /etc/ansible
root@5dee1267c996:/etc/ansible# ls -ltr
total 28
-rw-r--r-- 1 root root 1016 Dec  4 2019 hosts
-rw-r--r-- 1 root root 19985 Dec  4 2019 ansible.cfg
drwxr-xr-x 2 root root 4096 Dec  4 2019 roles
root@5dee1267c996:/etc/ansible# nano hosts|
```

In hosts file, weservers is commented(##[webservers]) remove ## to uncomment and add ip of webserver1 and webserver2

Webserver1 ip :10.2.0.5

Webserver2 Ip: 10.2.0.6

10.2.0.5 ansible_python_interpreter=/usr/bin/python3

10.2.0.6 ansible_python_interpreter=/usr/bin/python3

```
# 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
10.2.0.5 ansible_python_interpreter=/usr/bin/python3
10.2.0.6 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
```

Nano ansible.cfg

remote_user={username}

```
GNU nano 2.9.3                               ansible.cfg

#task_includes_static = False
#handler_includes_static = False

# Controls if a missing handler for a notification event is an error or a warning
#error_on_missing_handler = True

# change this for alternative sudo implementations
#sudo_exe = sudo

# What flags to pass to sudo
# WARNING: leaving out the defaults might create unexpected behaviours
#sudo_flags = -H -S -n

# SSH timeout
#timeout = 10

# 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

# default module name for /usr/bin/ansible
#module_name = command

# use this shell for commands executed under sudo
# you may need to change this to bin/bash in rare instances
# if sudo is constrained
#executable = /bin/sh

# if inventory variables overlap, does the higher precedence one win
```

Yml file

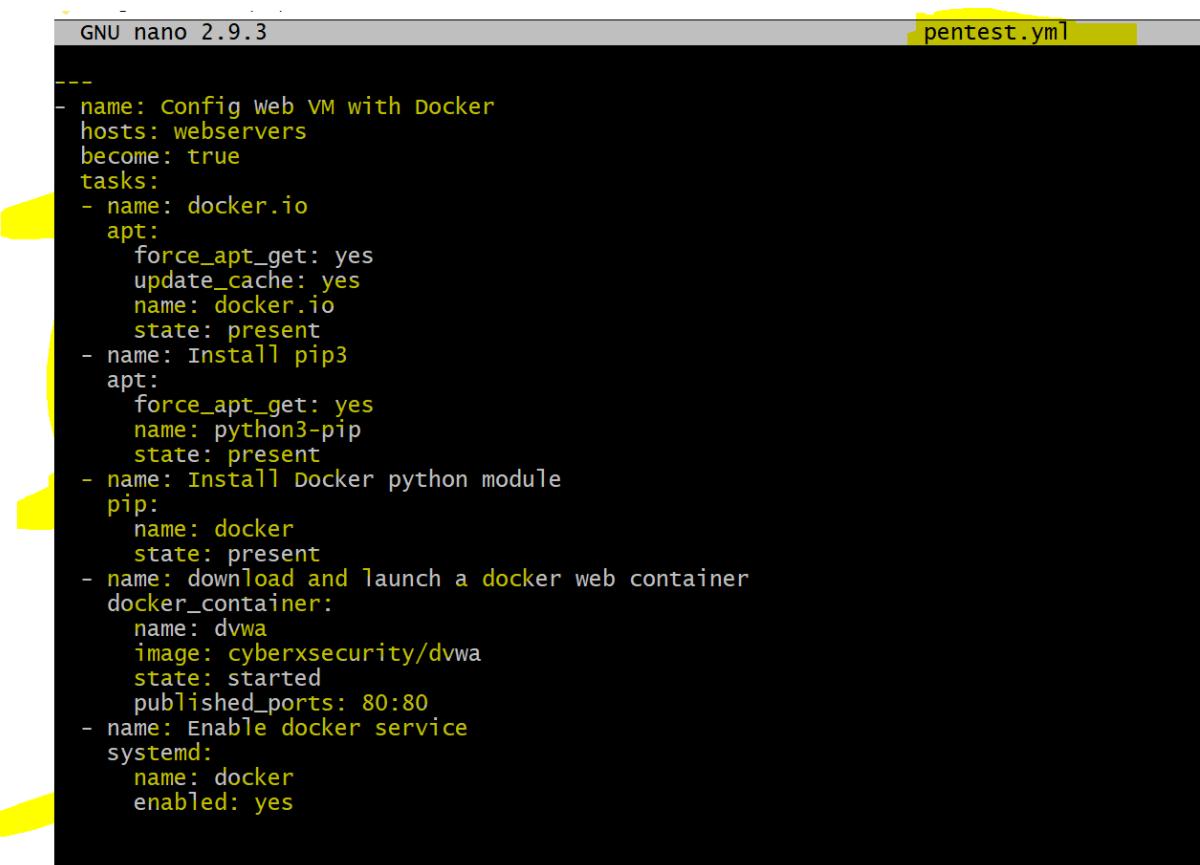
```
---

- name: Config Web VM 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 python module
      pip:
        name: docker
        state: present
    - name: download and launch a 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
```

Create yml file and paste above code
nano /etc/ansible/pentest.yml

```
root@5dee1267c996:/etc/ansible# nano ansible.cfg
root@5dee1267c996:/etc/ansible# nano pentest.yml
```



```
GNU nano 2.9.3
pentest.yml
---
- name: Config web VM 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 python module
pip:
  name: docker
  state: present
- name: download and launch a 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
```

Ansible-playbook pentest.yml

Ansible -m ping all

If you see this error regenerate key again from root

```

root@5dee1267c996:/etc/ansible# ansible -m ping all
Enter passphrase for key '/root/.ssh/id_rsa': Enter passphrase for key '/root/.ssh/id_rsa':
Enter passphrase for key '/root/.ssh/id_rsa':
Enter passphrase for key '/root/.ssh/id_rsa':
Enter passphrase for key '/root/.ssh/id_rsa':
Enter passphrase for key '/root/.ssh/id_rsa':
10.2.0.6 | UNREACHABLE! => {
    "changed": false,
    "msg": "Failed to connect to the host via ssh: sysadmin@10.2.0.6: Permission denied (publickey).",
    "unreachable": true
}

[3]+  Stopped                  ansible -m ping all

```

Don't provide any keyphrase when creating public key

```

root@5dee1267c996:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:7xukzDTqjys1k08zjhjyyI1dgubEVdG1jd57EQEqBfE root@5dee1267c996
The key's randomart image is:
+---[RSA 2048]---+
+=+.+=000.oo.
..o..o.+.= .
+ .+.o Eo ..
+ * o o= ...
. * o . S+.. .
+ .o. .
. * o: .
o o ...
+---[SHA256]---+
root@5dee1267c996:~# cat /root/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQADQDNJY+hH38iK9cu2/mKib7Q9fyipazhhP0/gEQ6x7lqpZDenIE+xAtzW7NrsOyRkiTP0a/d4iqypfTPrexyABifCNNYlyREHjbIghS4lveLFQYk413LK1u1sC/4uMb3OY16bNmWBQwyQwx2oDUYZZkMC604yPssmuB2f w40I10/F1a85vhBF4D6BxSaEa8I0agd6DUQ+u7Rx1Z1K1V59z6PHEjIV7/8lhcd24ZP uyUn0ellddq+ApiQ1Bbb6LKIqlM7CpJZxmvBla36B7MuQ+LC26ICeh9zmDlr0+7ygop MNxSsZGj+c+Tb13GUtmohHYf+TX9GOP5hnnZw5oRSoX
root@5dee1267c996:~#

```

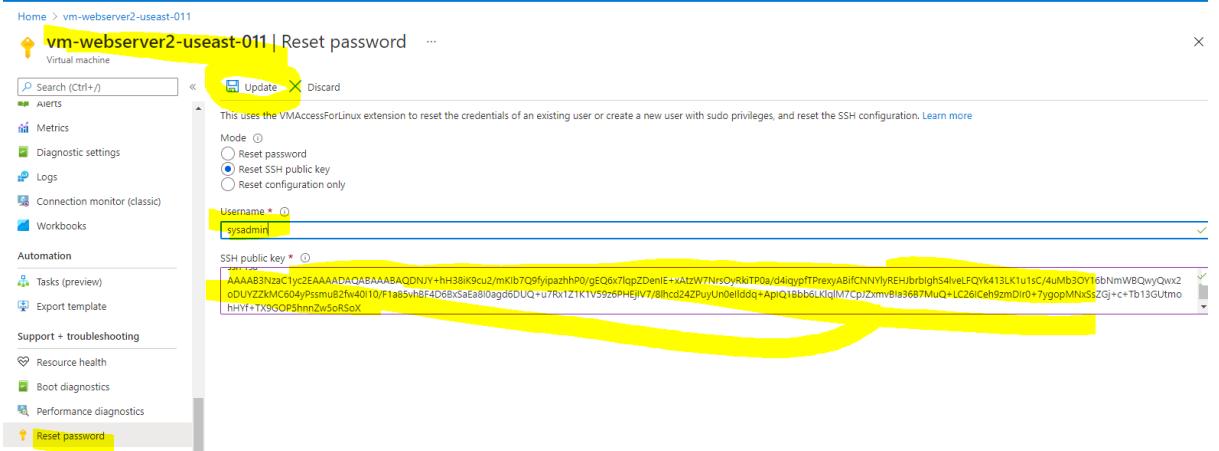
ssh-rsa

```

AAAAB3NzaC1yc2EAAAQABAAQADQDNJY+hH38iK9cu2/mKib7Q9fyipazhhP0
/gEQ6x7lqpZDenIE+xAtzW7NrsOyRkiTP0a/d4iqypfTPrexyABifCNNYlyREHjbIghS
4lveLFQYk413LK1u1sC/4uMb3OY16bNmWBQwyQwx2oDUYZZkMC604yPssmuB2f
w40I10/F1a85vhBF4D6BxSaEa8I0agd6DUQ+u7Rx1Z1K1V59z6PHEjIV7/8lhcd24ZP
uyUn0ellddq+ApiQ1Bbb6LKIqlM7CpJZxmvBla36B7MuQ+LC26ICeh9zmDlr0+7ygop
MNxSsZGj+c+Tb13GUtmohHYf+TX9GOP5hnnZw5oRSoX

```

Update key again on Webserver1 and webserver2



After updating key try to ping again

Ansible -m ping all

```
root@5dee1267c996:/# ansible -m ping all
10.2.0.6 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.2.0.5 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

After that ansible-playbook pentest.yml

```
root@5dee1267c996:/# cd /etc/ansible
root@5dee1267c996:/etc/ansible# ansible-playbook pentest.yml
PLAY [Config web VM with Docker] ****
TASK [Gathering Facts] ****
ok: [10.2.0.6]
ok: [10.2.0.5]

TASK [docker.io] ****
changed: [10.2.0.6]
changed: [10.2.0.5]

TASK [Install pip3] ****
changed: [10.2.0.6]
changed: [10.2.0.5]

TASK [Install Docker python module] ****
changed: [10.2.0.6]
changed: [10.2.0.5]

TASK [download and launch a docker web container] ****
changed: [10.2.0.6]
changed: [10.2.0.5]

TASK [Enable docker service] ****
ok: [10.2.0.6]
ok: [10.2.0.5]

PLAY RECAP ****
10.2.0.5 : ok=6    changed=4    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.2.0.6 : ok=6    changed=4    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@5dee1267c996:/etc/ansible# |
```

Ssh into one of the web server and run curl localhost/setup.php

```
root@5dee1267c996:/etc/ansible# ssh sysadmin@10.2.0.6
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1047-azure x86_64)

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

 System information as of Thu May 13 21:24:43 UTC 2021

 System load:  0.36           Processes:      124
 Usage of /:   10.3% of 28.90GB  Users logged in:    0
 Memory usage: 43%            IP address for eth0:  10.2.0.6
 Swap usage:   0%              IP address for docker0: 172.17.0.1

 * Pure upstream Kubernetes 1.21, smallest, simplest cluster ops!
   https://microk8s.io/

 * Canonical Livepatch is available for installation.
 - Reduce system reboots and improve kernel security. Activate at:
   https://ubuntu.com/livepatch

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

Last login: Thu May 13 21:23:16 2021 from 10.2.0.4
sysadmin@vm-webserver2-useast-011:~$ curl localhost/setup.php
<!DOCTYPE html>

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

```
</html>sysadmin@vm-webserver2-useast-011:~$ exit
logout
Connection to 10.2.0.6 closed.
root@5dee1267c996:/etc/ansible# ssh sysadmin@10.2.0.5
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1047-azure x86_64)

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

System information as of Thu May 13 21:26:37 UTC 2021

System load:  0.06          Processes:           124
Usage of /:   10.3% of 28.90GB  Users logged in:      0
Memory usage: 43%
Swap usage:   0%            IP address for eth0:   10.2.0.5
                           IP address for docker0: 172.17.0.1

* Pure upstream Kubernetes 1.21, smallest, simplest cluster ops!
  https://microk8s.io/

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch

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

Last login: Thu May 13 21:23:16 2021 from 10.2.0.4
sysadmin@vm-webserver1-useast-011:~$ curl localhost/setup.php
<!DOCTYPE html>
```

Create Load Balancer



Load balancers

Load balancing - help me choose (Previous)

Create load balancer

Basics Tags Review + create

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

Project details

Subscription * Azure subscription 1
Resource group * rg_useast_011 [Create new](#)

Instance details

Name * lb_useast_011
Region * (US) East US
Type * Public Internal
SKU * Basic Standard

[Review + create](#) < Previous Next : Tags > Download a template for automation

Create load balancer

Type * Public Internal

SKU * Basic Standard

Information

Microsoft recommends Standard SKU load balancer for workloads. [Learn more about pricing differences between Standard and Basic](#)

Tier Regional Global

Public IP address

Public IP address * Create new Use existing

Public IP address name * lb_useast_011

Public IP address SKU Basic

IP address assignment * Static Dynamic

Add a public IPv6 address No Yes

Review + create < Previous Next : Tags > Download a template for automation

✓ Your deployment is complete



Deployment name: Microsoft.LoadBalancer-20210513174014
Subscription: Azure subscription 1
Resource group: rg_useast_011

Start time: 5/13/2021, 5:44:43 PM
Correlation ID: b6a556c3-064a-4668-8b8a-94175d2

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

^ Next steps

[Go to resource](#)

[Home](#) > Microsoft.LoadBalancer-20210513174014 > lb_useast_011



lb_useast_011 | Backend pools

Load balancer

Search (Ctrl+ /)

«

+ Add Refresh

Filter by name...



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

Add Load Balancer health probe

+ Add Refresh

Filter by name...

Backend pool == all

Resource Name == a

Availability zone == all

Group by Backend pool

Backend pool

Resource Name

Add a backend pool to get started

Add health probe

lb_useast_011

Name *

healthprobe_useast_011



Protocol *

TCP



Port * ⓘ

80

Interval * ⓘ

5

seconds

Unhealthy threshold * ⓘ

2

consecutive failures

Used by ⓘ

Not used

Add backend pool

vn_useast_011 (rg_useast_011)

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 ↑↓

vm-webserver1-useast-011

ipconfig1 (10.2.0.5)

as-useast-011

vm-webserver2-useast-011

ipconfig1 (10.2.0.6)

as-useast-011

Add

Name *

backendpool_useast-011



Virtual network ⓘ

vn_useast_011 (rg_useast_011)



Settings

Frontend IP configuration

Backend pools

Health probes

Load balancing rules

Inbound NAT rules

Backend pool

Resource Name

Resource Status

IP Address

Network interface

Availability zone

backendpool_useast-011

vm-webserver2-useast-011

Running

10.2.0.6

vm-webserver2-useast...

..

backendpool_useast-011

vm-webserver1-useast-011

Running

10.2.0.5

vm-webserver1-useast...

..

Add Load Balancing rule

Add load balancing rule ...

lb_useast_011

Info A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *	loadbalancerule_useast_011	✓
IP Version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	
Frontend IP address * ⓘ	LoadBalancerFrontEnd (13.68.220.120)	✓
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	
Port *	80	✓
Backend port *	80	✓
Backend pool *	backendpool_useast-011	✓
Health probe *	healthprobe_useast_011 (TCP:80)	✓
Create new		
Session persistence ⓘ	Client IP and protocol	✓
Create new		
Session persistence ⓘ	Client IP and protocol	✓
Idle timeout (minutes) *	4	
Floating IP ⓘ	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
Validating...		

Home > Network security groups > nsg_useast_011

nsg_useast_011 | Inbound security rules

Search (Ctrl+)

Overview

Activity log

Tags

Diagnose and solve problems

Inbound security rules

Priority ↑ Name ↑ Port ↑ Protocol ↑ Source ↑

Priority	Name	Port	Protocol	Source
3700	sshFromElkVM	22	TCP	
3800	sshFromJumpbox	22	TCP	
3900	sshIntoJumpBox	22	TCP	
4090	DenyAll	Any	Any	
65000	AllowVnetInBound	Any	Any	
65001	AllowAzureLoadBalancerInB...	Any	Any	
65500	DenyAllInBound	Any	Any	

Add Hide default rules Refresh Delete

Add inbound security rule

Source (IP Addresses)

Source IP addresses/CIDR ranges *

Source port ranges *

Destination (Virtual Network)

Service (HTTP)

Destination port ranges: 80

Protocol: Any (TCP, UDP, ICMP)

Action: Allow (Allow, Deny)

Priority: 3750

Name: AllowInBound

Add Cancel