Project:
Securing the Perimeter

By
Hazrat Umer

https://www.linkedin.com/in/hazrat-umer/

Hazrat Umer:
4/3/2024

Section 1

Designing a Secure Network Architecture

Section 1: Designing the Network

Time to tackle XYZ's perimeter challenges. You've identified that the first thing to do is design a secure network architecture for XYZ. XYZ has provided you a list of business requirements so you can get started on designing a secure layout. Your first task is to incorporate all the requirements securely in a network design.

Use https://app.diagrams.net/ to design a secure network architecture.

Include and label the following requirements in your design:

1) An on-premise network that has 3 workstations in it.

2) A Virtual Network with the following segments:

- Public DMZ with two web servers and a load balancer in it.
- Private DMZ with two database servers.
- Management LAN with one management server in it.
- Internal LAN with 5 workstations in it.
- Private Secure LAN with 3 database servers.

Additionally include the following:

1) A VPN gateway connecting the on-premise network to your Virtual Network.

2) Show placement of security devices in the architecture, including load balancer(s), firewall(s), IDS/IPS device(s).

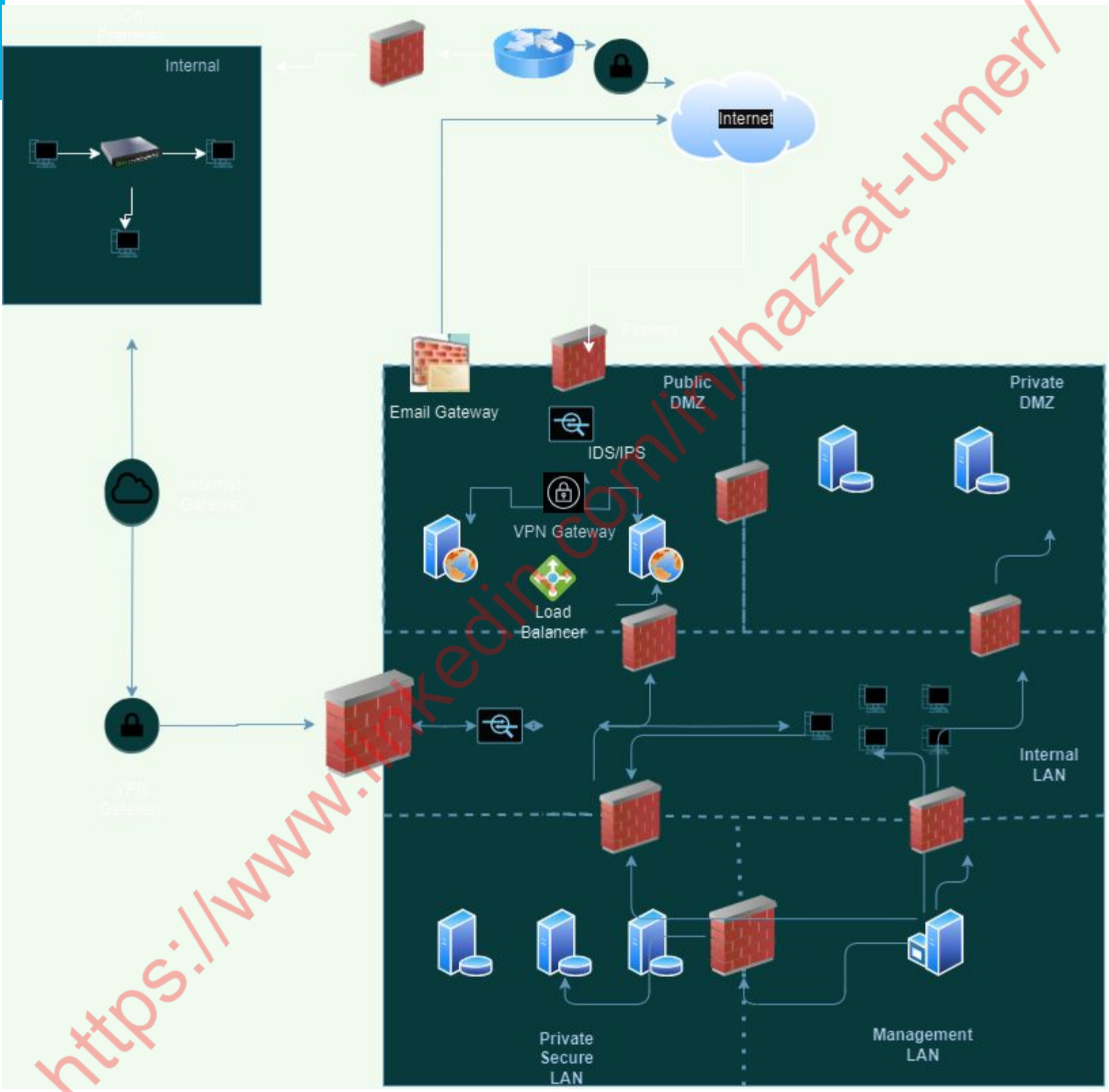
3) Show the flow of traffic, and remember to incorporate best security practices with the flow of traffic between the different subnets.

Designing the Network

Diagram Link:

https://drive.google.com/file/d/1k9uTyJYFp7Kkr1NZdSMGW_Bllf2az51W/view?usp=sharing

1.1 Designing the Network



Digram URL: https://drive.google.com/file/d/1k9uTyJYFp7Kkr1NZdSMGW_Bllf2az51W/view?usp=sharing

Section 2

Building a Secure Network Architecture in Azure

Section 2: Building the Network

After designing the network architecture, you now present your design to XYZ's stakeholders. They're all on board with your design, and have given you the green light to start building the architecture out in Azure.

So your next task is to go the Project Workspace in the classroom, and build out the enterprise network in Azure!

If you are accessing Azure with the Udacity classroom workspace, there will be a Resource Group in Azure called 'entp-project' that has already been created for you.

If you are accessing Azure using your own Azure account, first of all you should create a resource group called 'entp-project'.

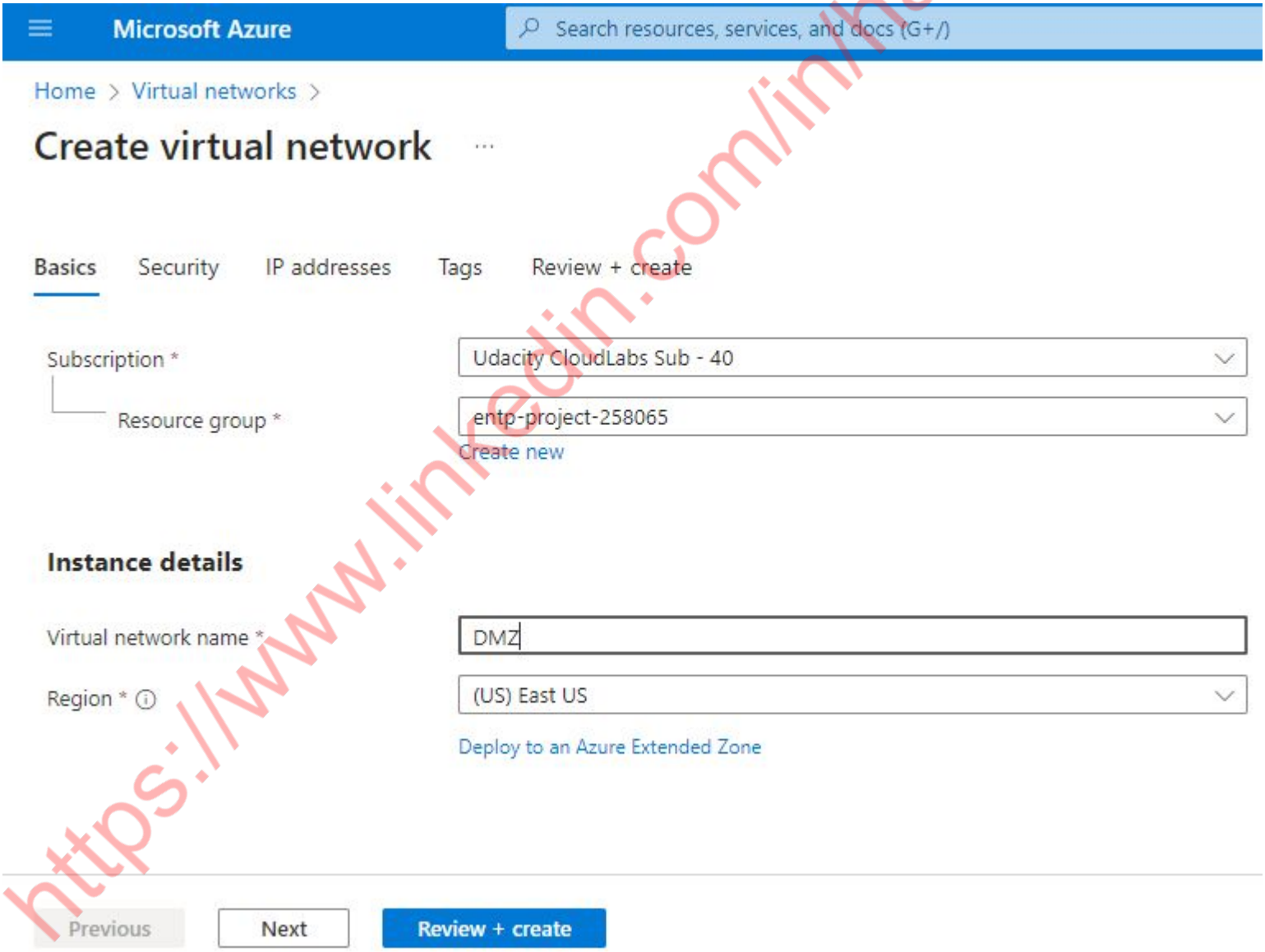
This 'entp-project' resource group is where you will create all the components that make up this project. When creating VMs in this section, please only use Standard_B1s for your VM size and the Linux Ubuntu 18.04 image.

Insert screenshots of your network on the following pages, showing completion of each of the specified tasks.

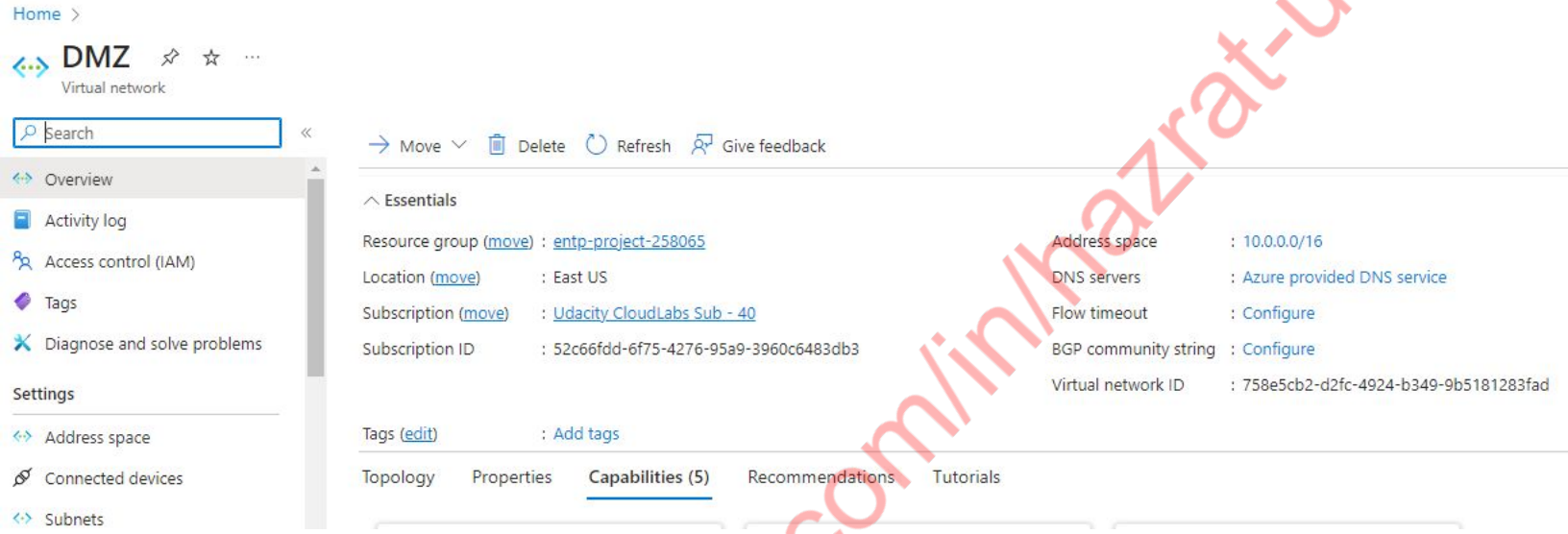
2.1.1 Screenshot

Create two Azure Virtual Networks in the resource group ‘entp-project’. Label one for your DMZ and one as your Internal.

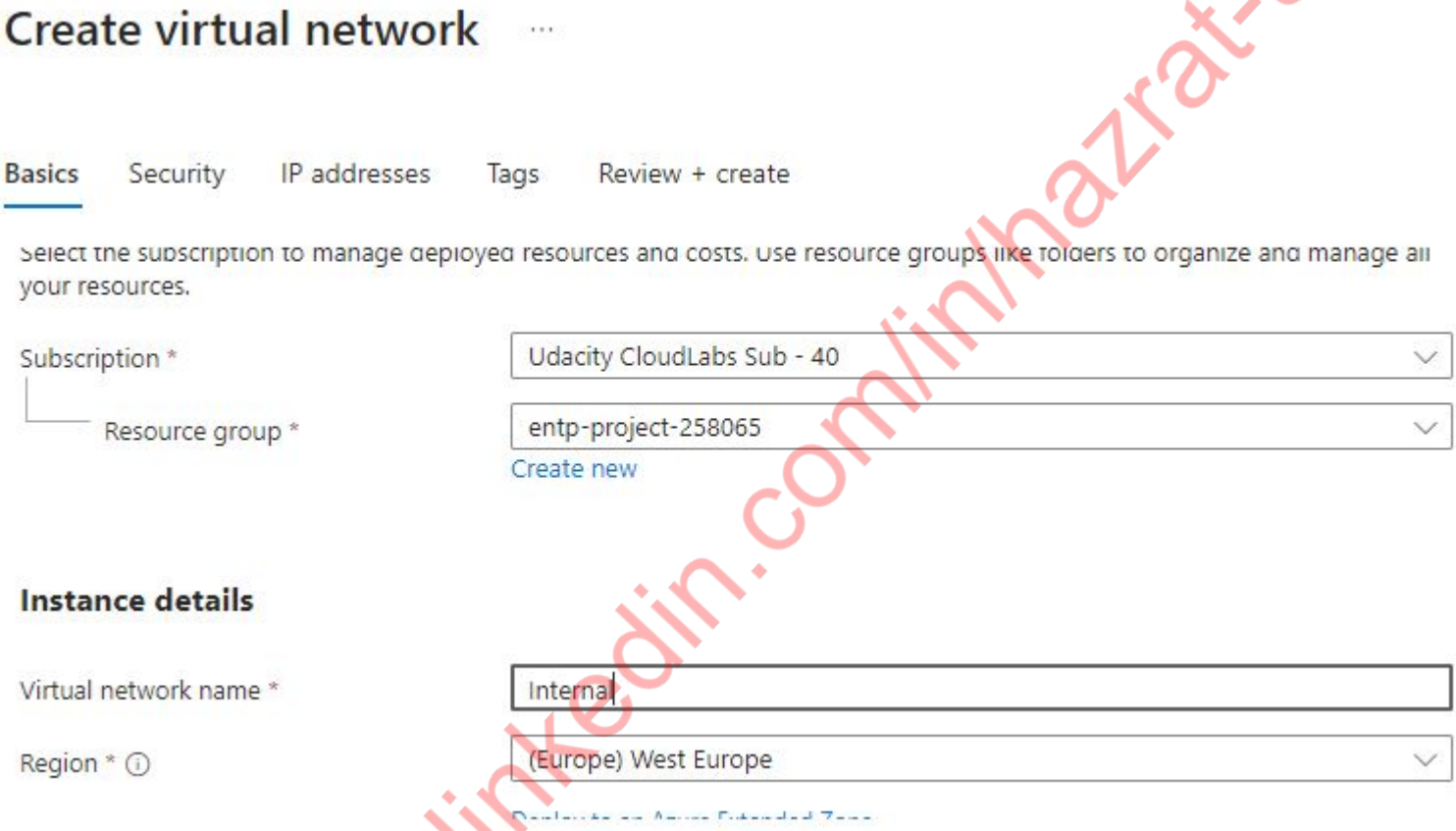
Creating Virtual Network DMZ



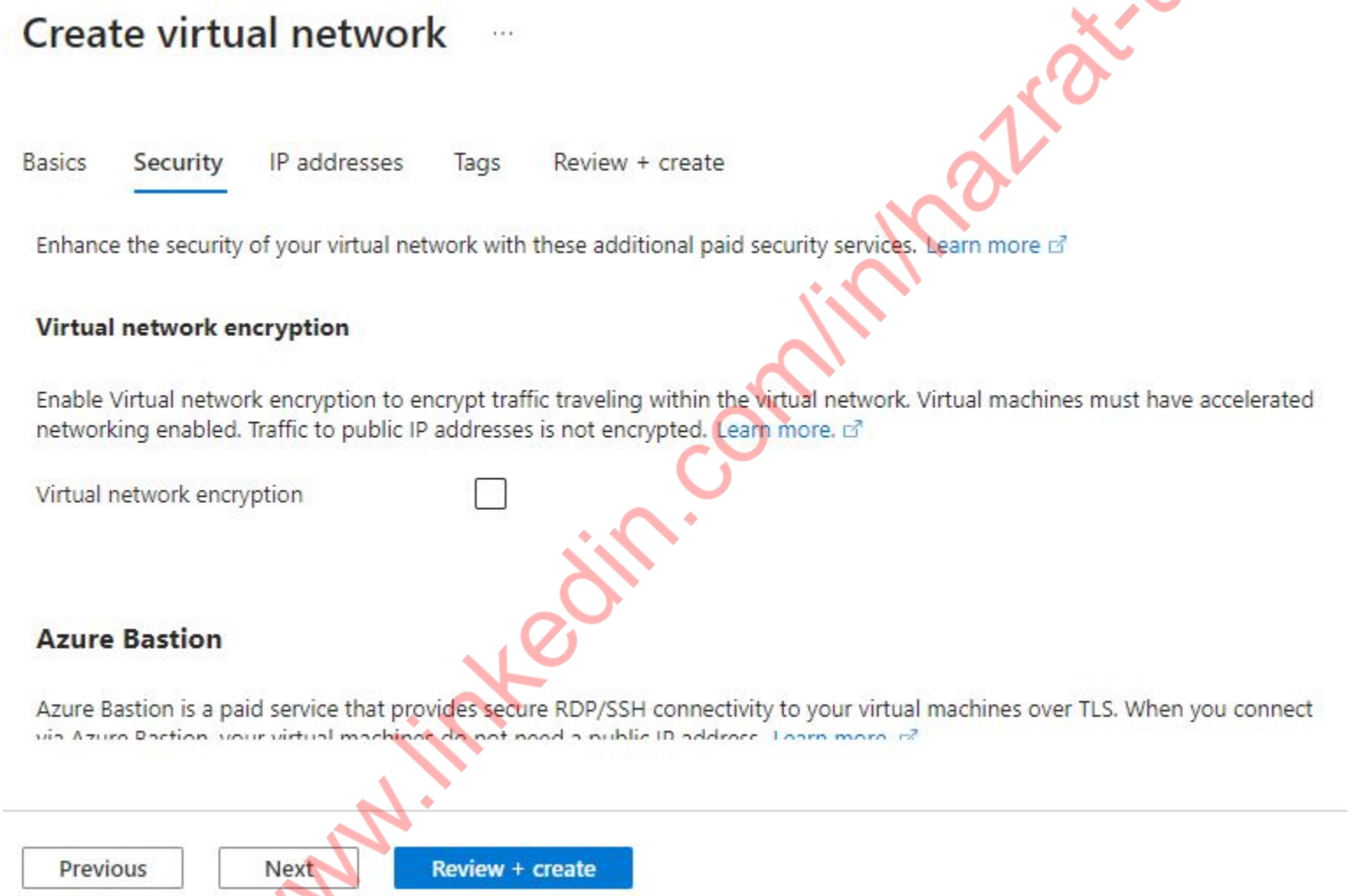
DMZ Virtual Network Created



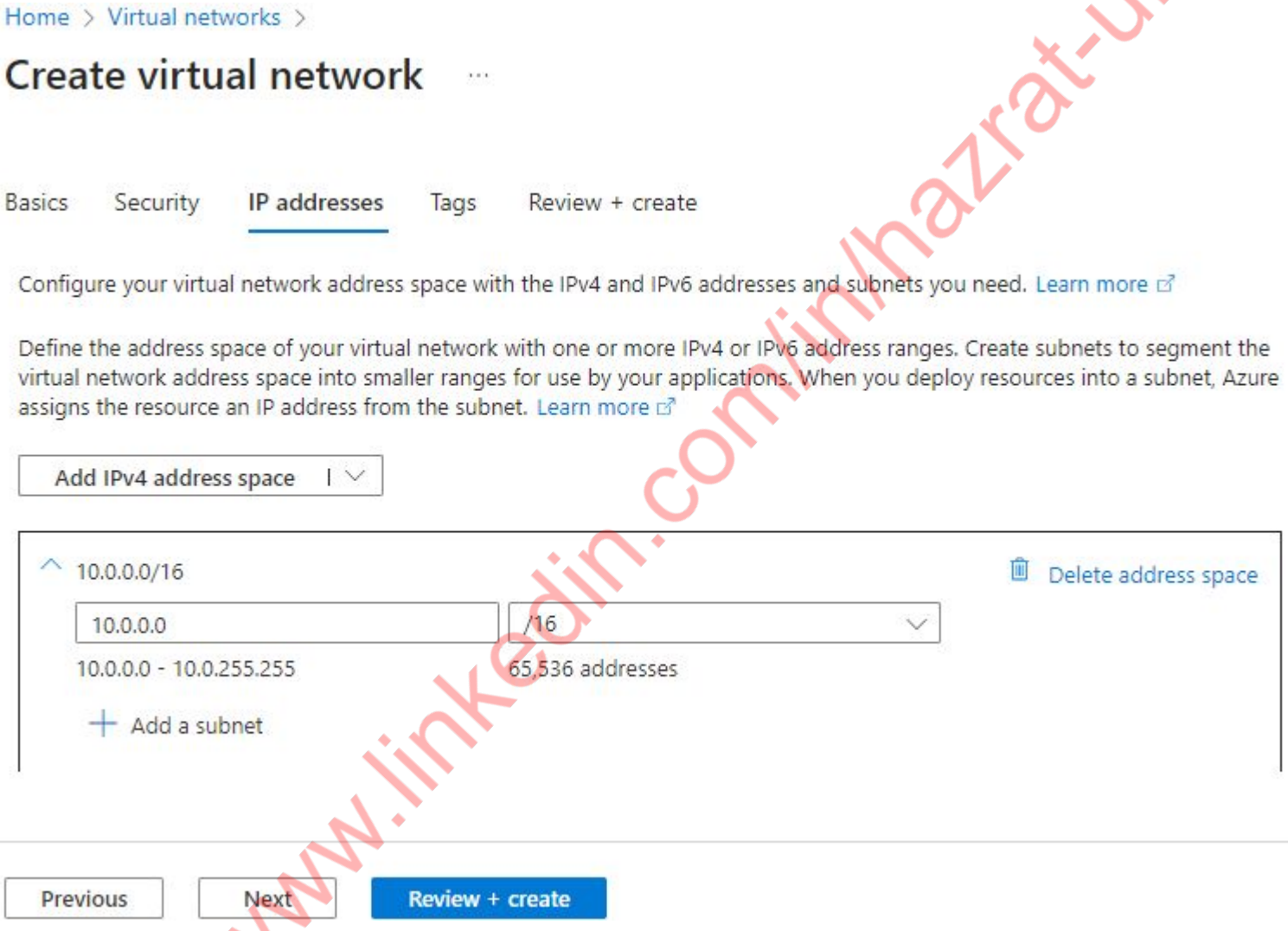
Creating Virtual Network named “Internal”



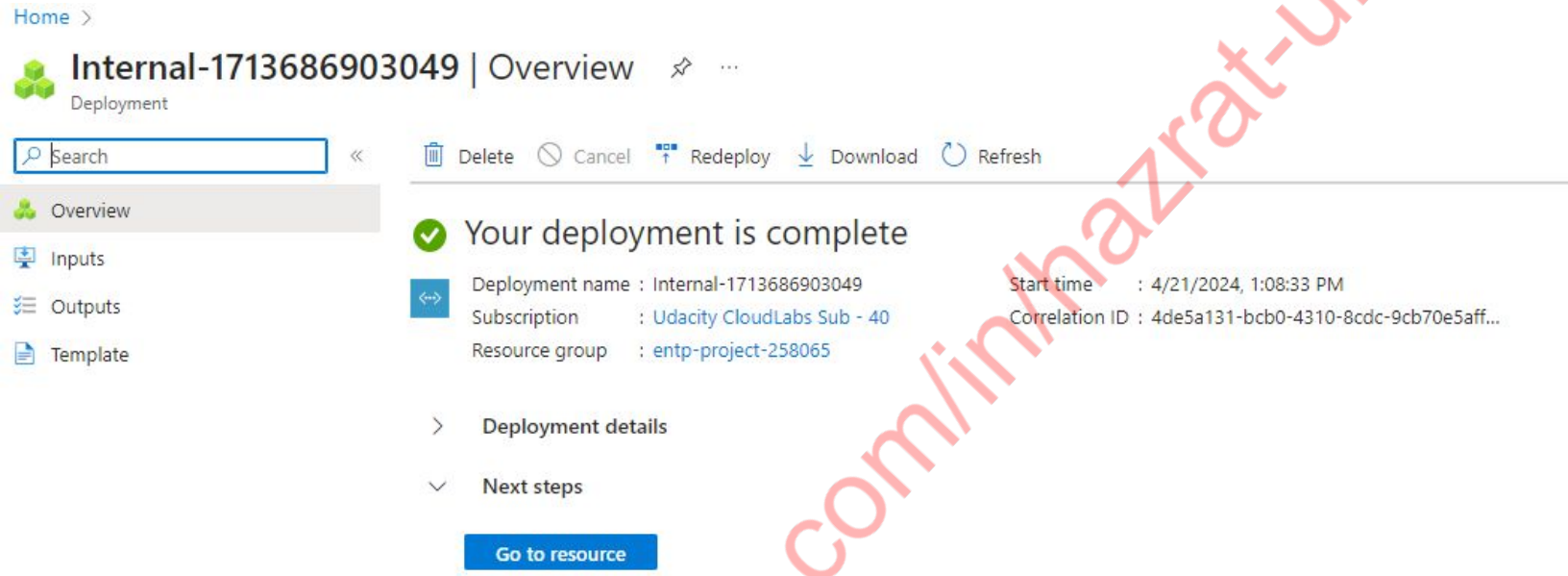
Leaving the security option as default

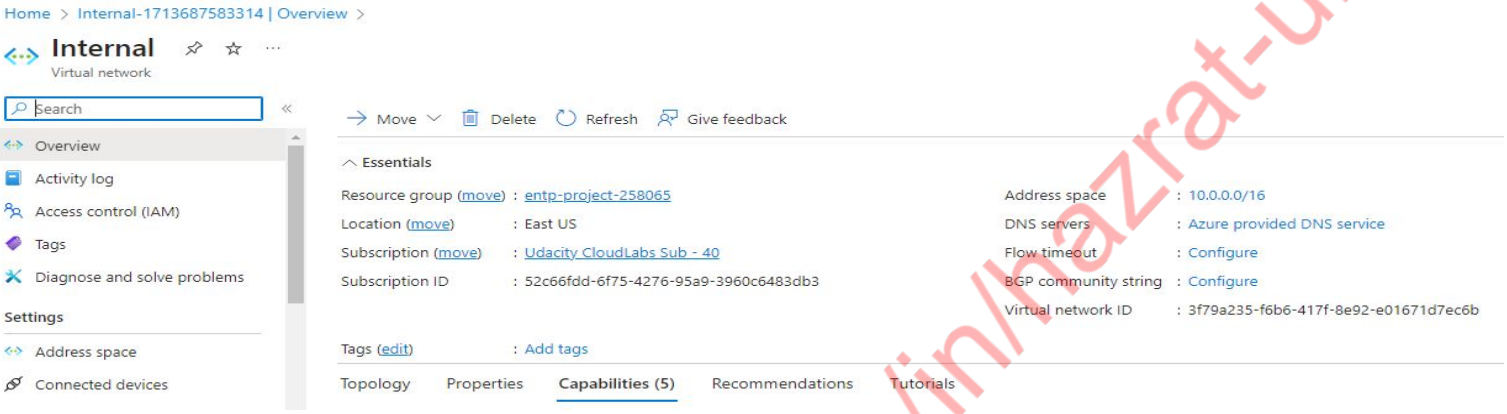


Leaving the IP addresses as default

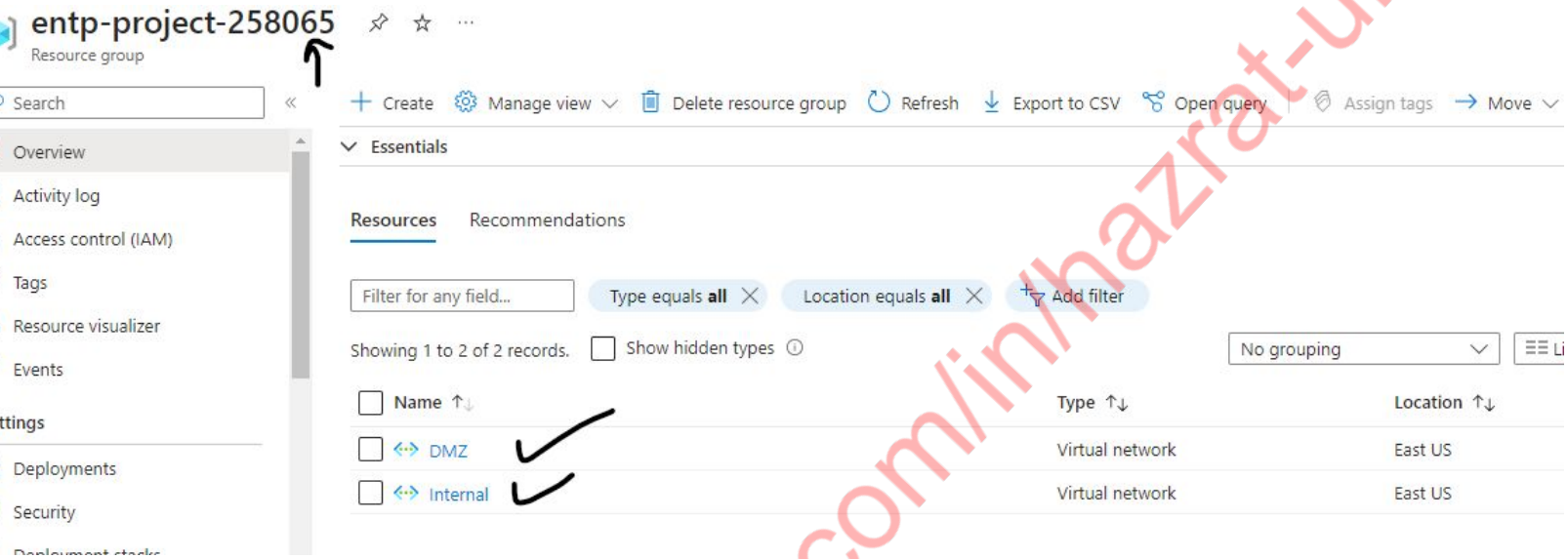


Internal Virtual Network is Created





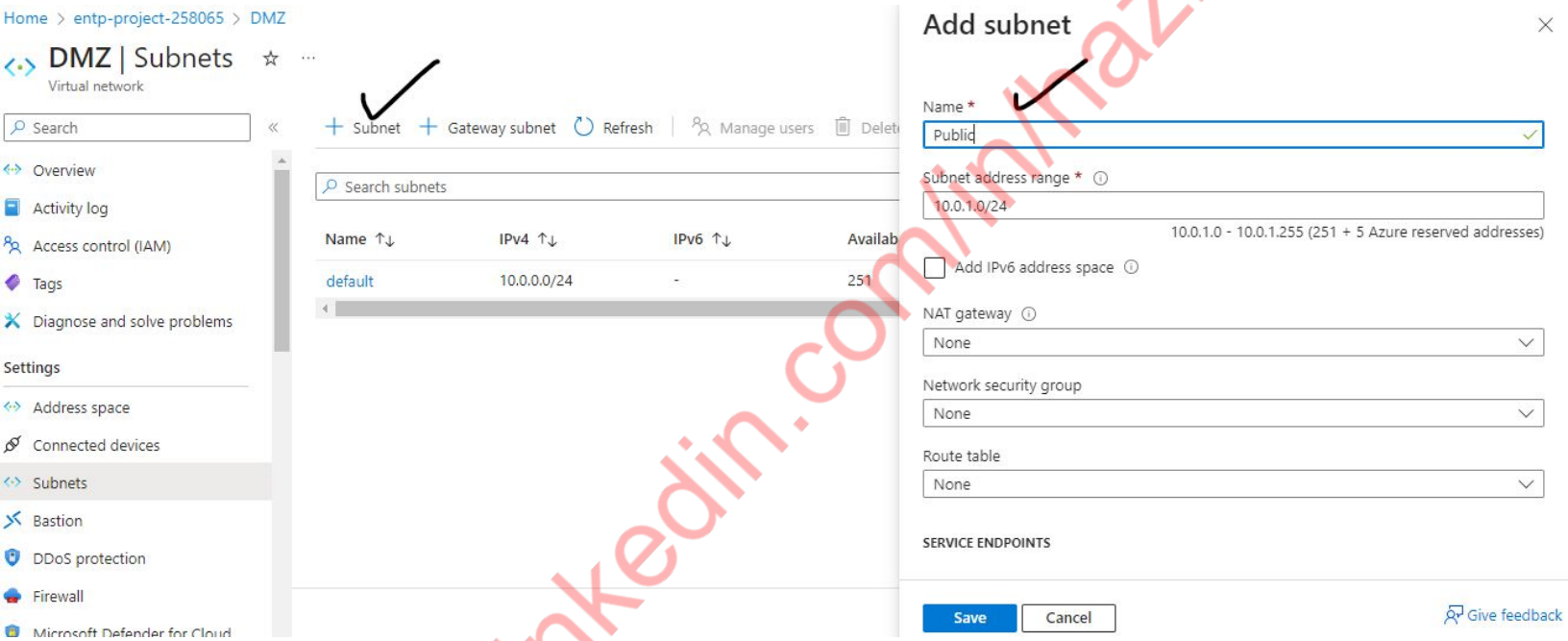
Both the Virtual Networks are present in Resource Group

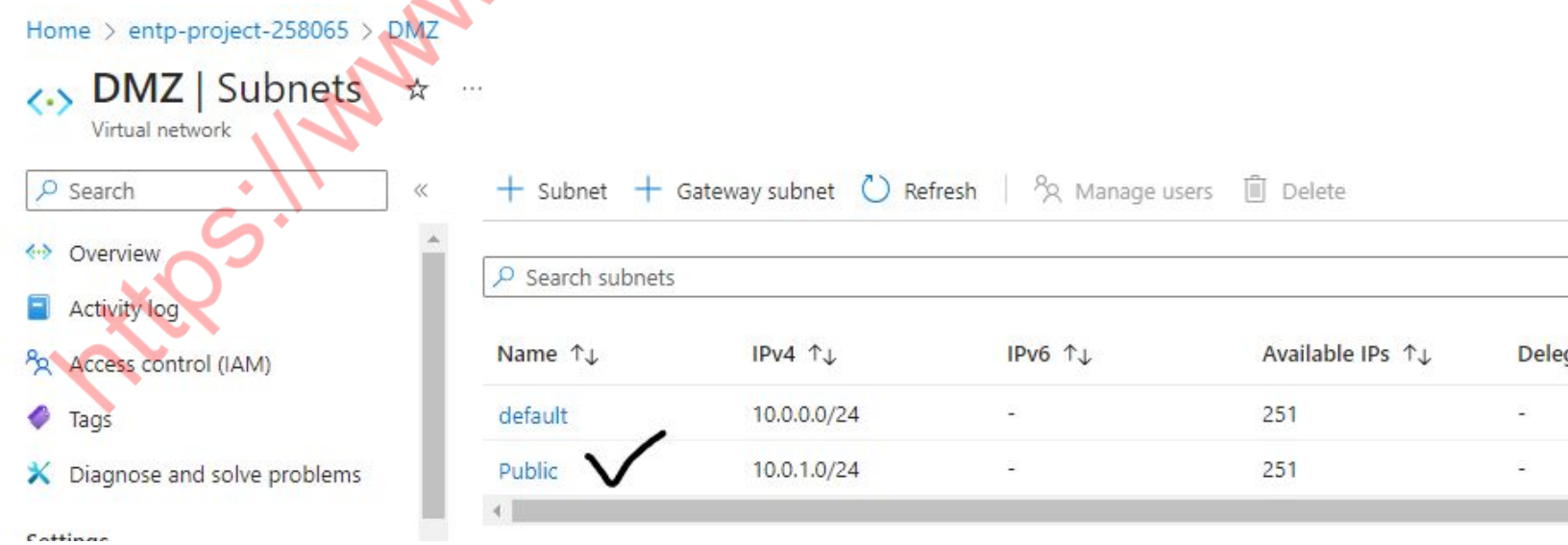


2.1.2 Screenshot

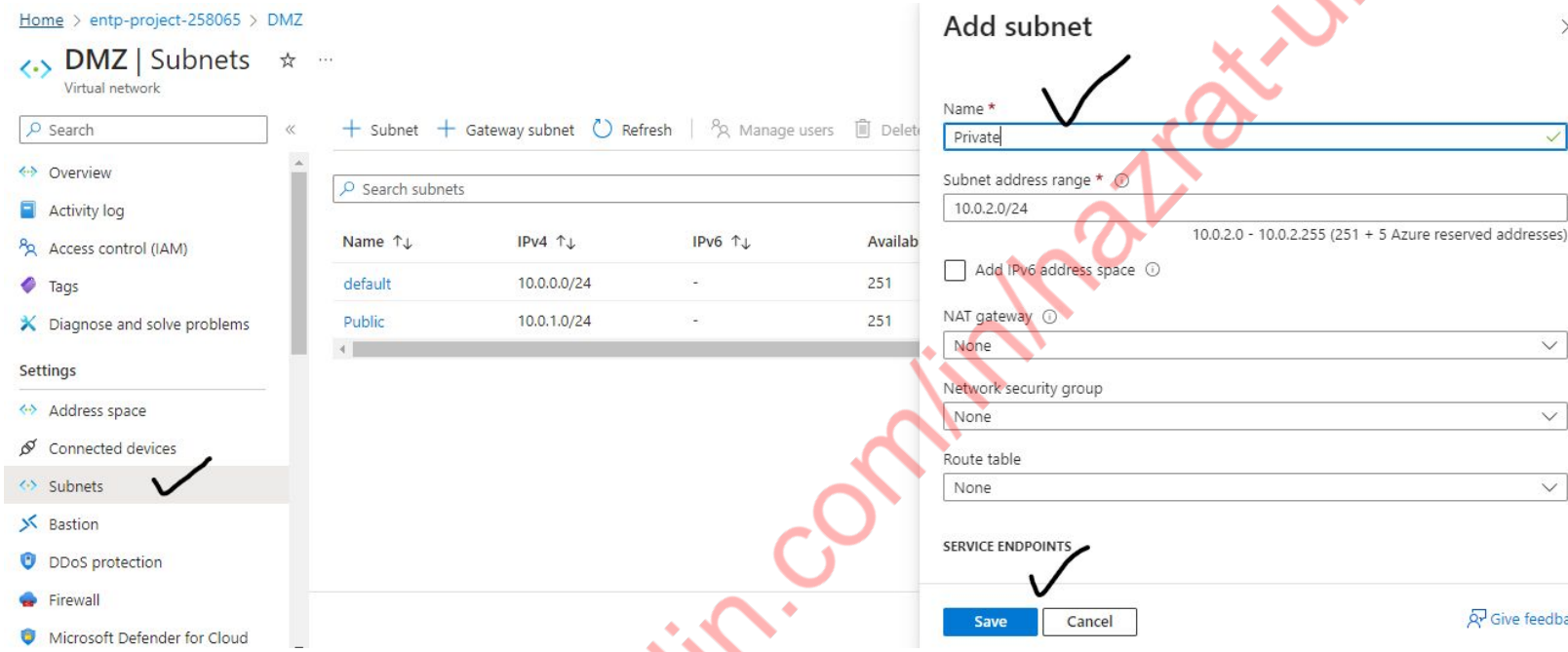
Create 2 subnets within your DMZ - subnets should be public and private.

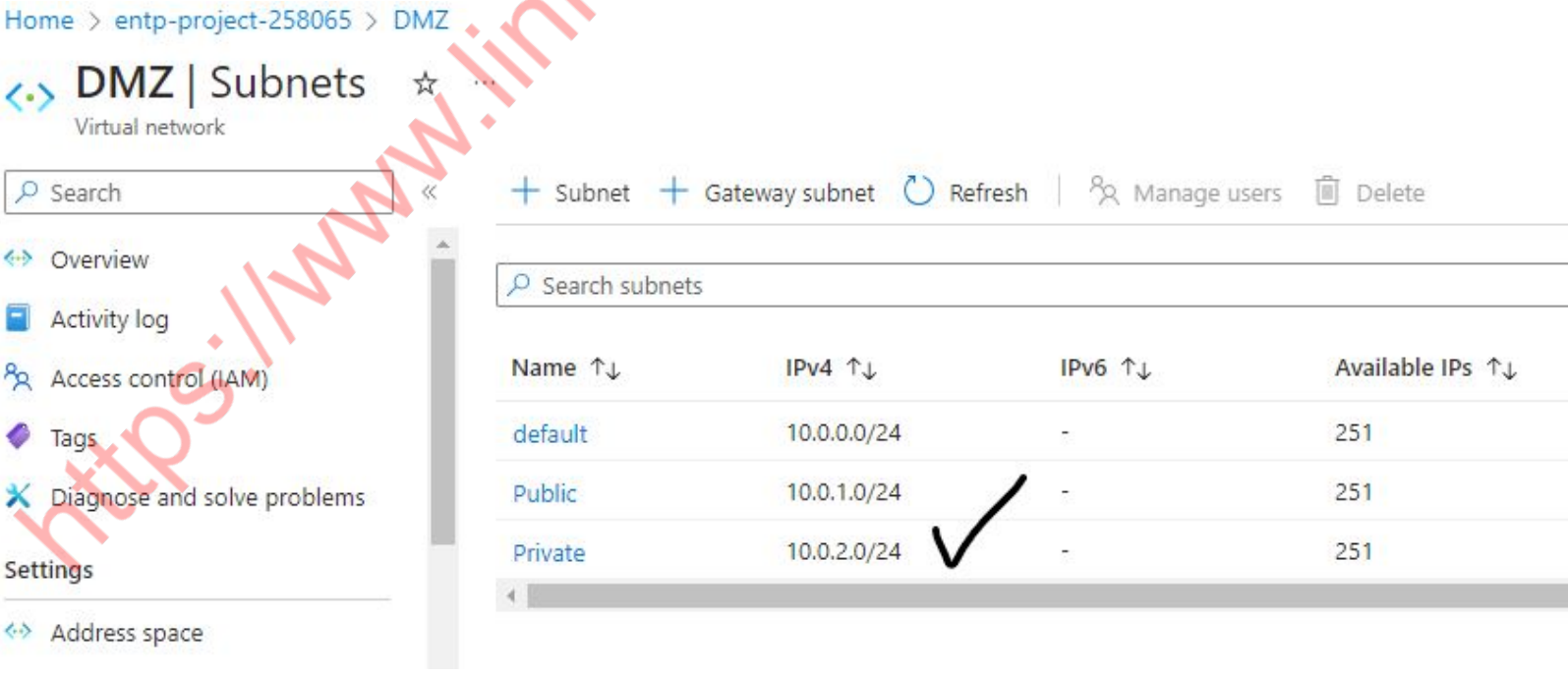
Creating public Subnet



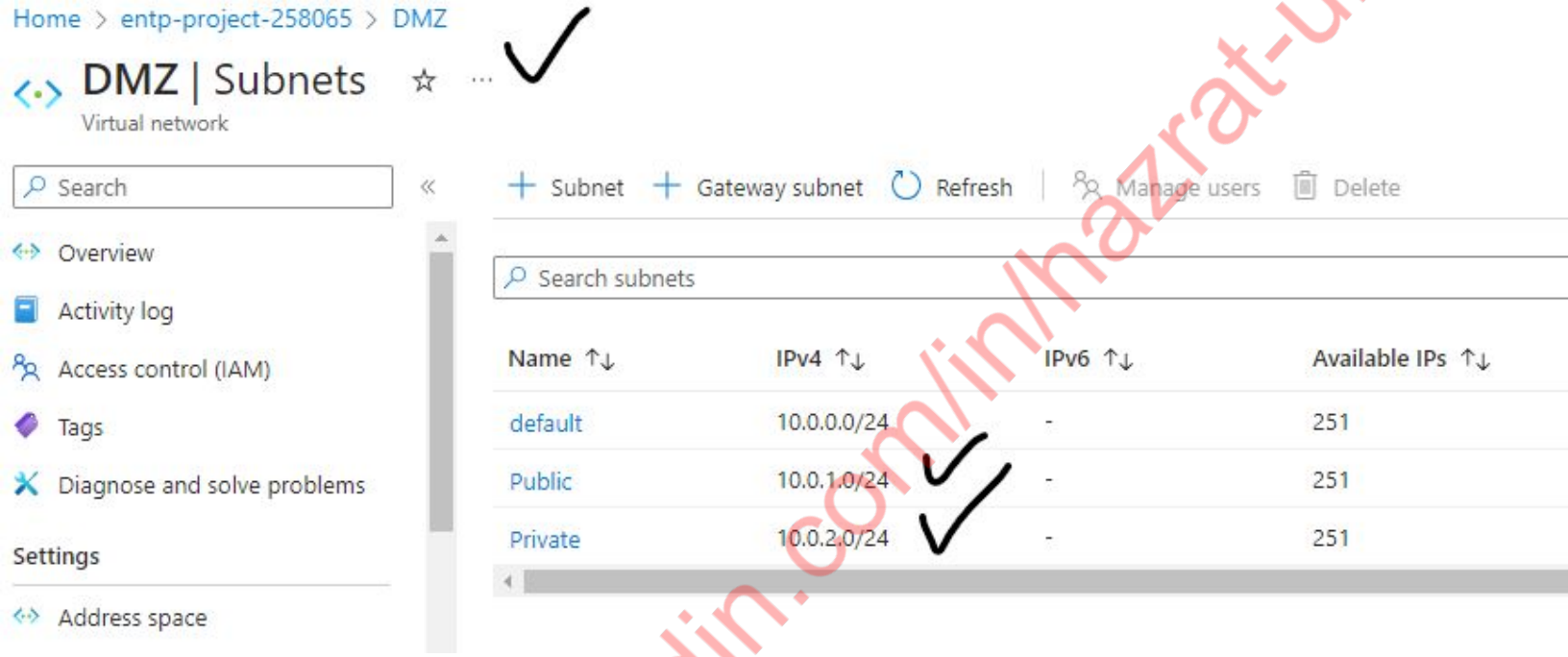


Creating Private Subnet in DMZ





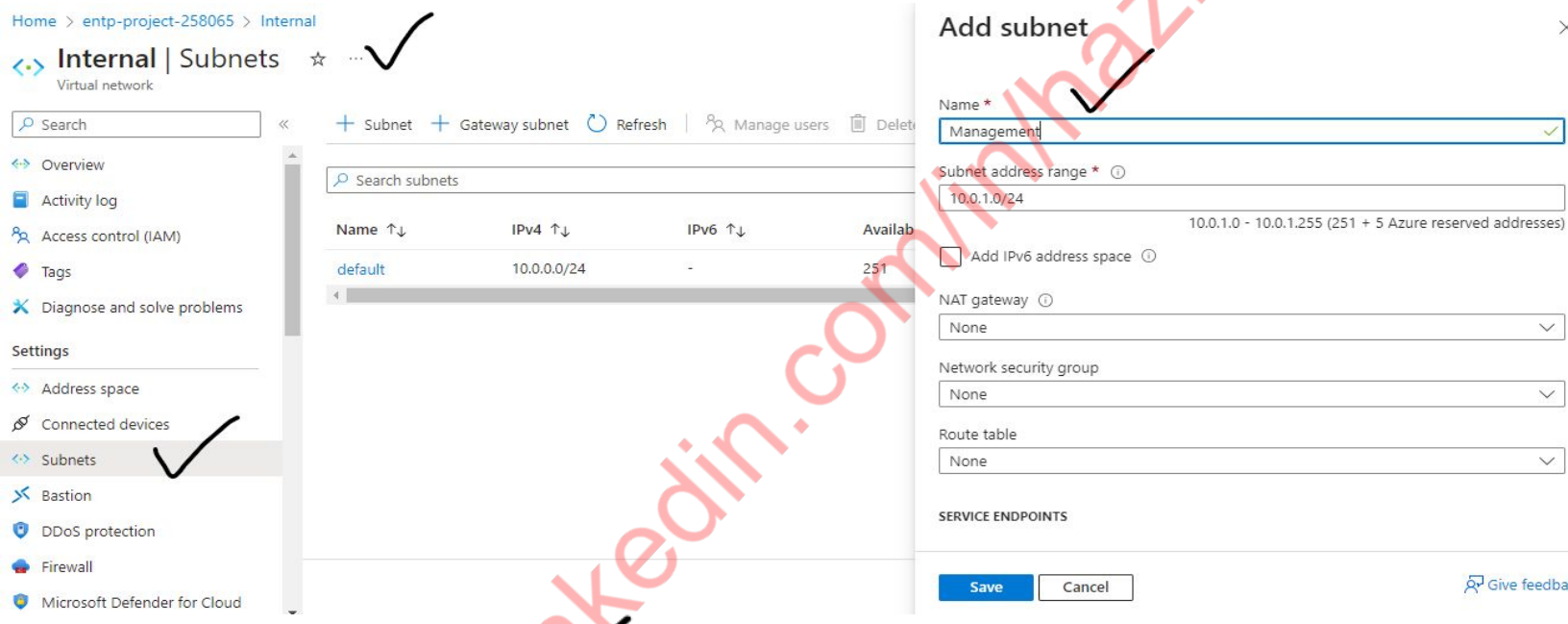
Both Private and Public Subnets created in DMZ

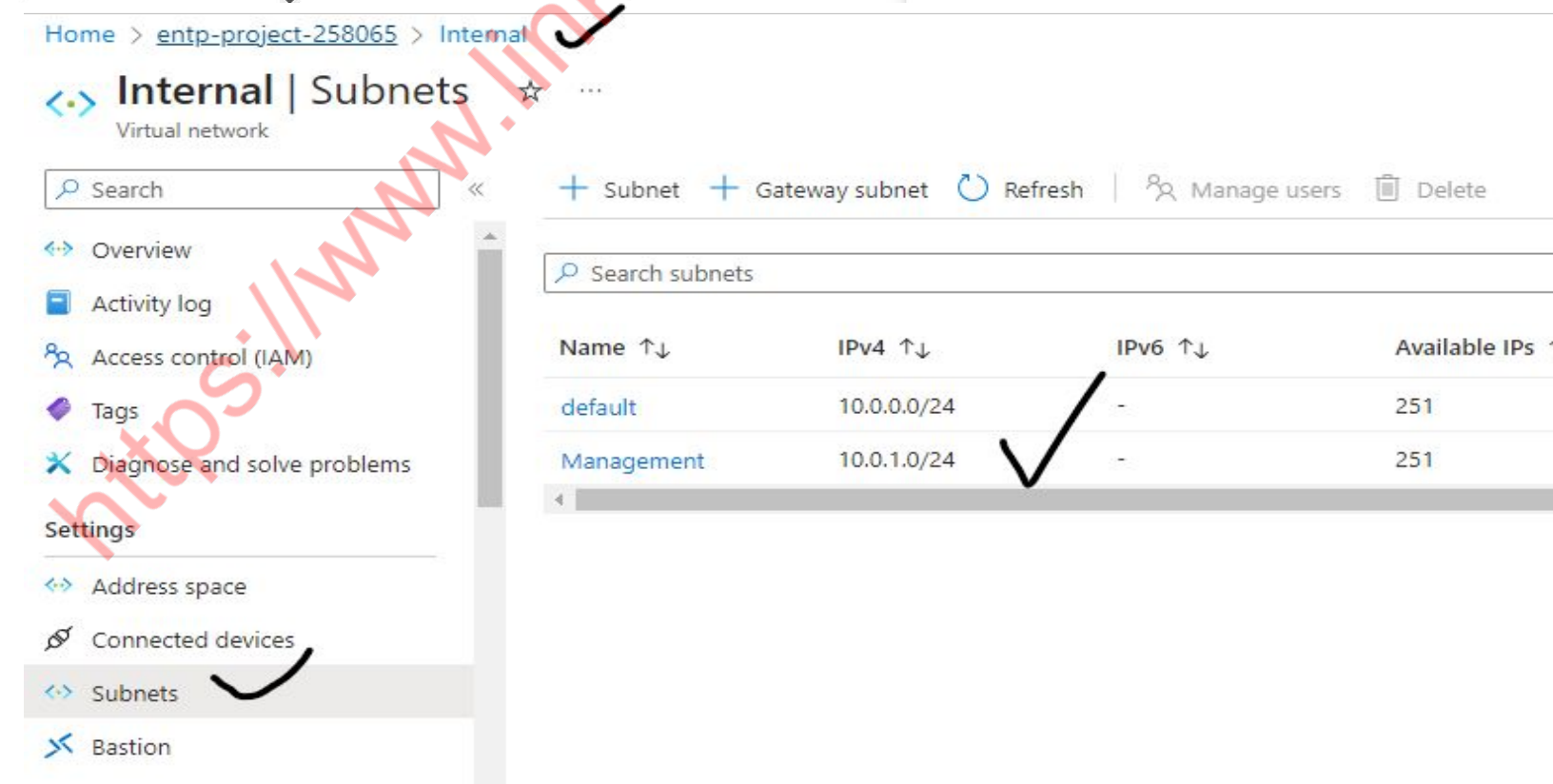


2.1.3 Screenshot

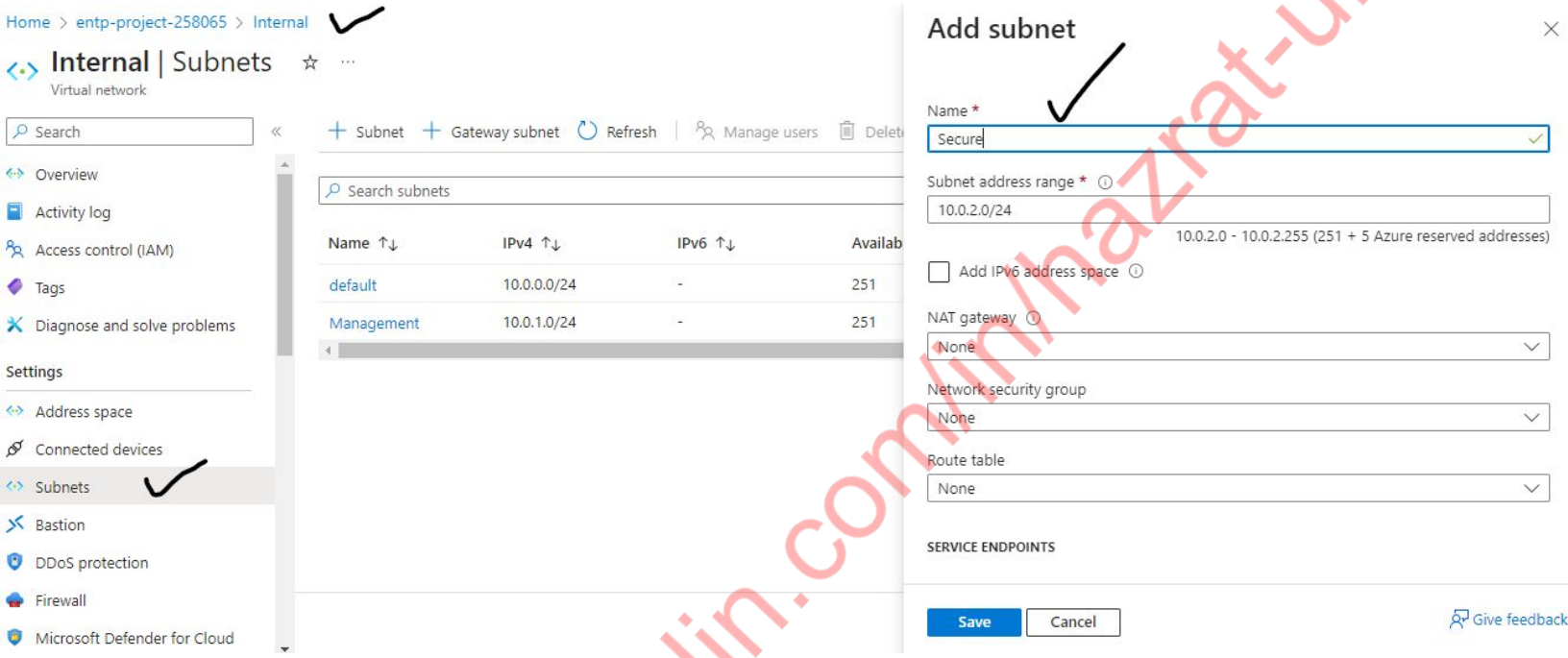
Create three subnets in your internal network and label them Management, Secure, and Enterprise.

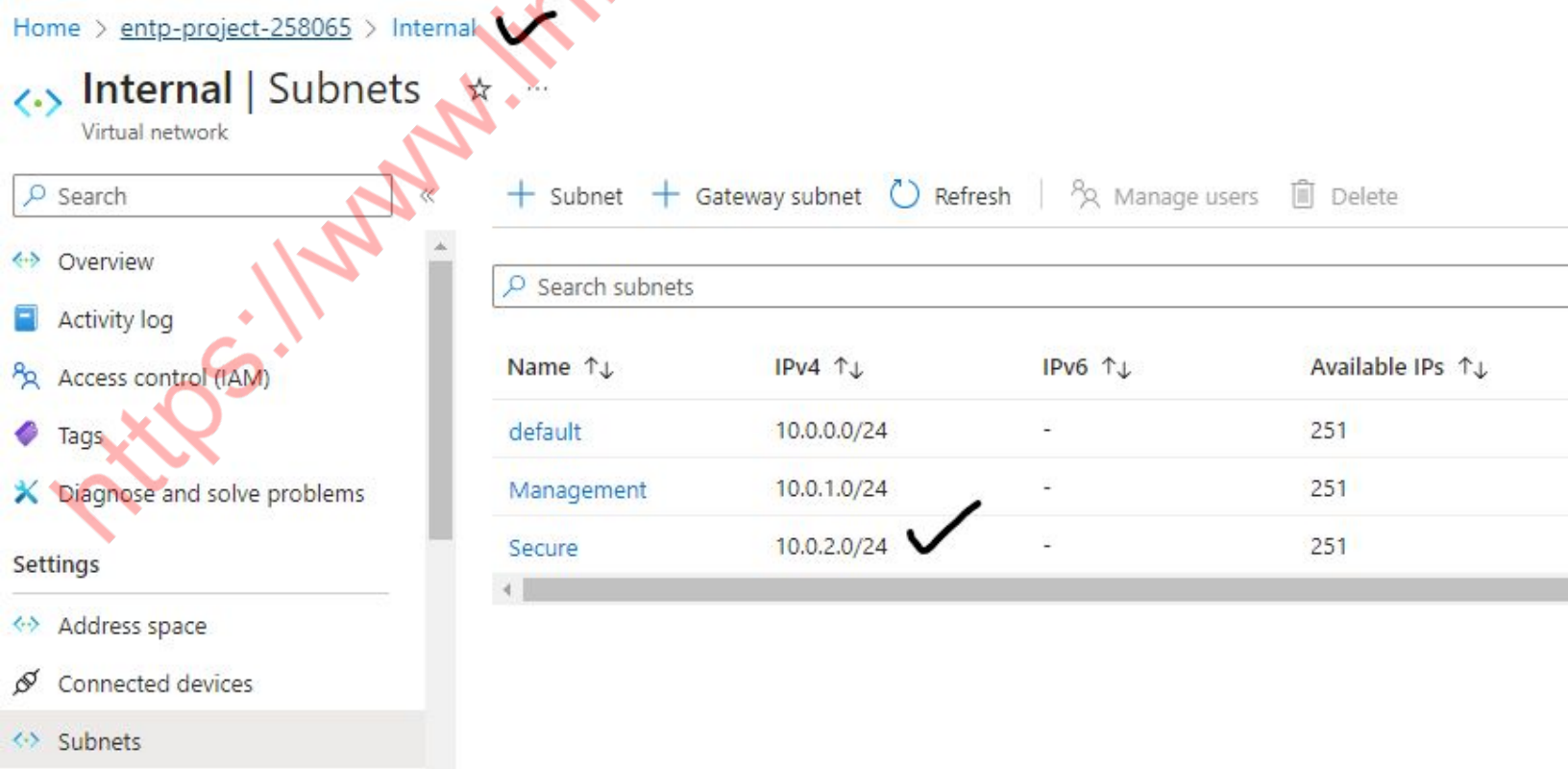
Creating Management Subnet in Internal Network



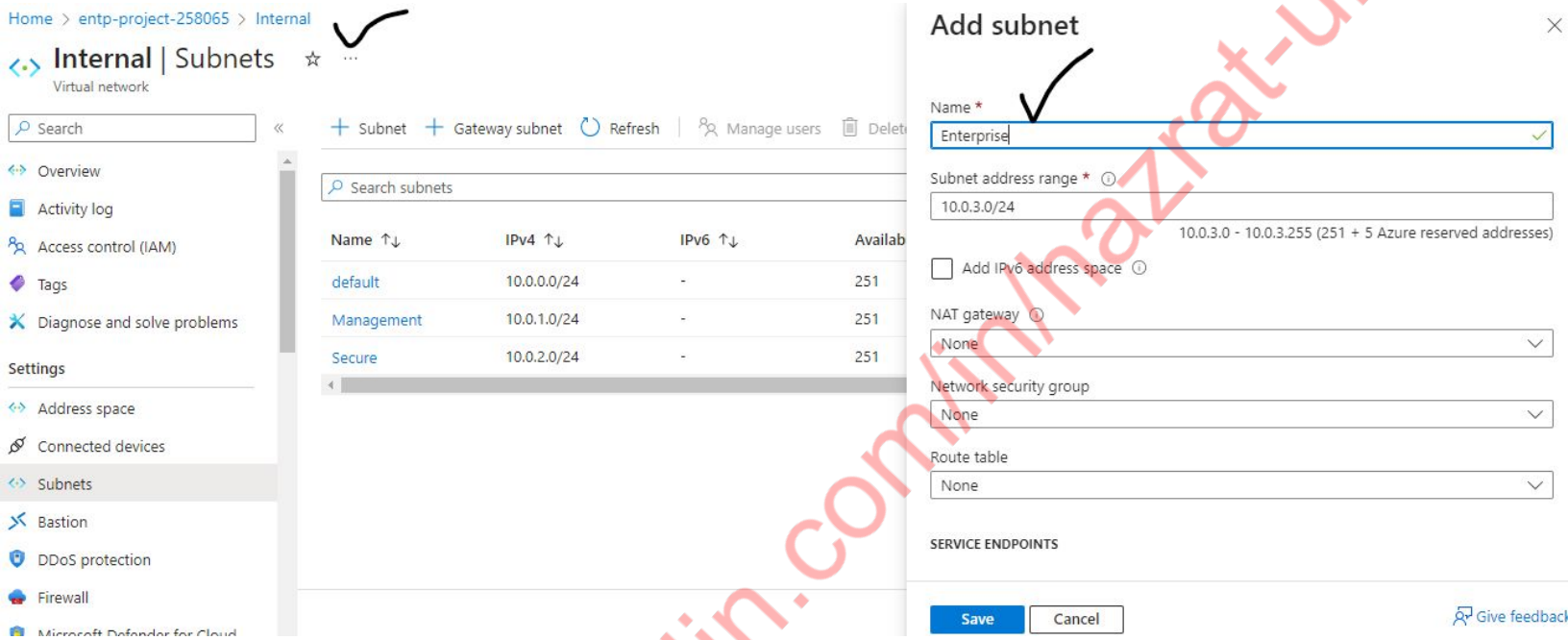


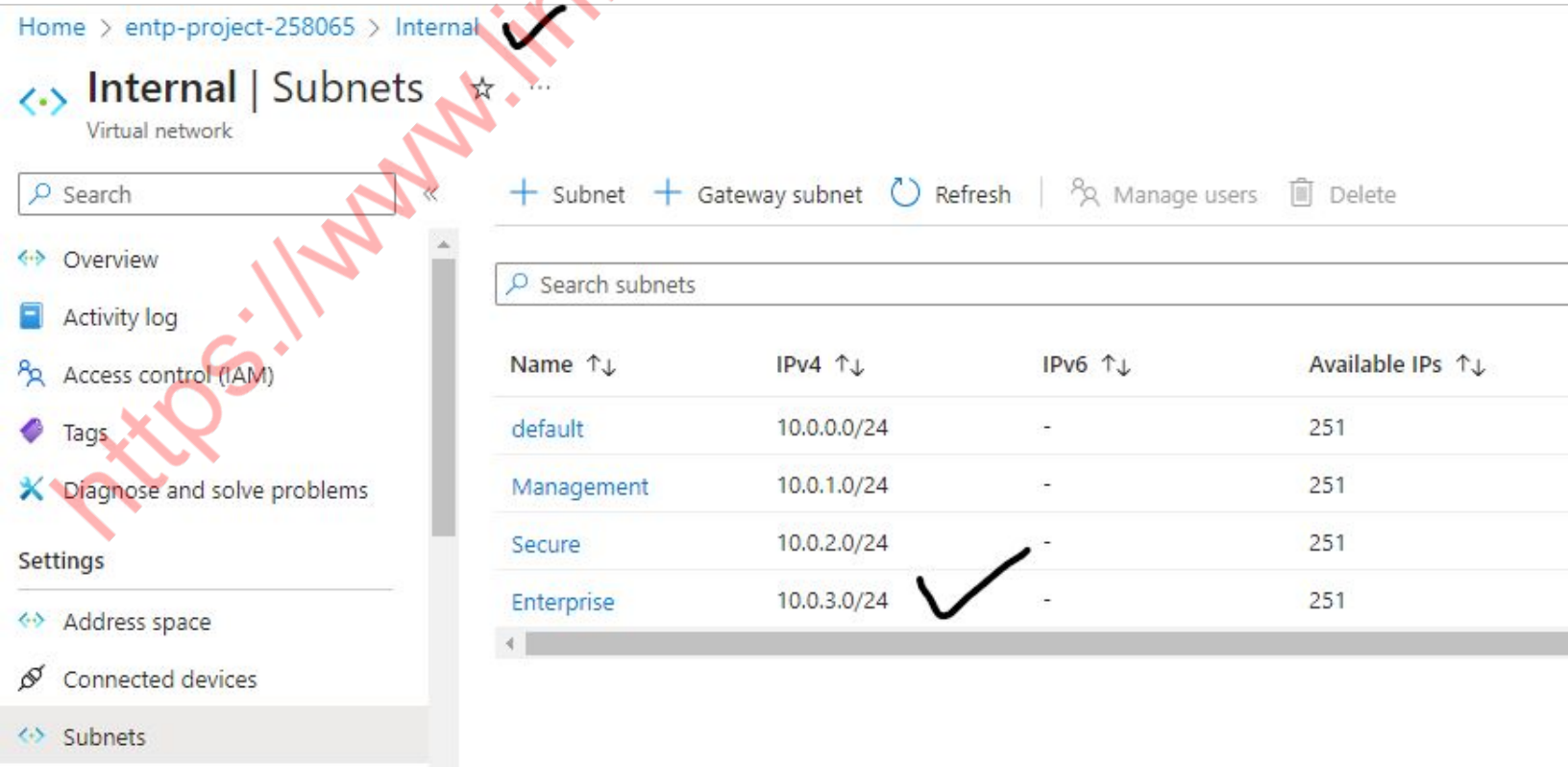
Creating a Secure Subnet in Internal Virtual Network



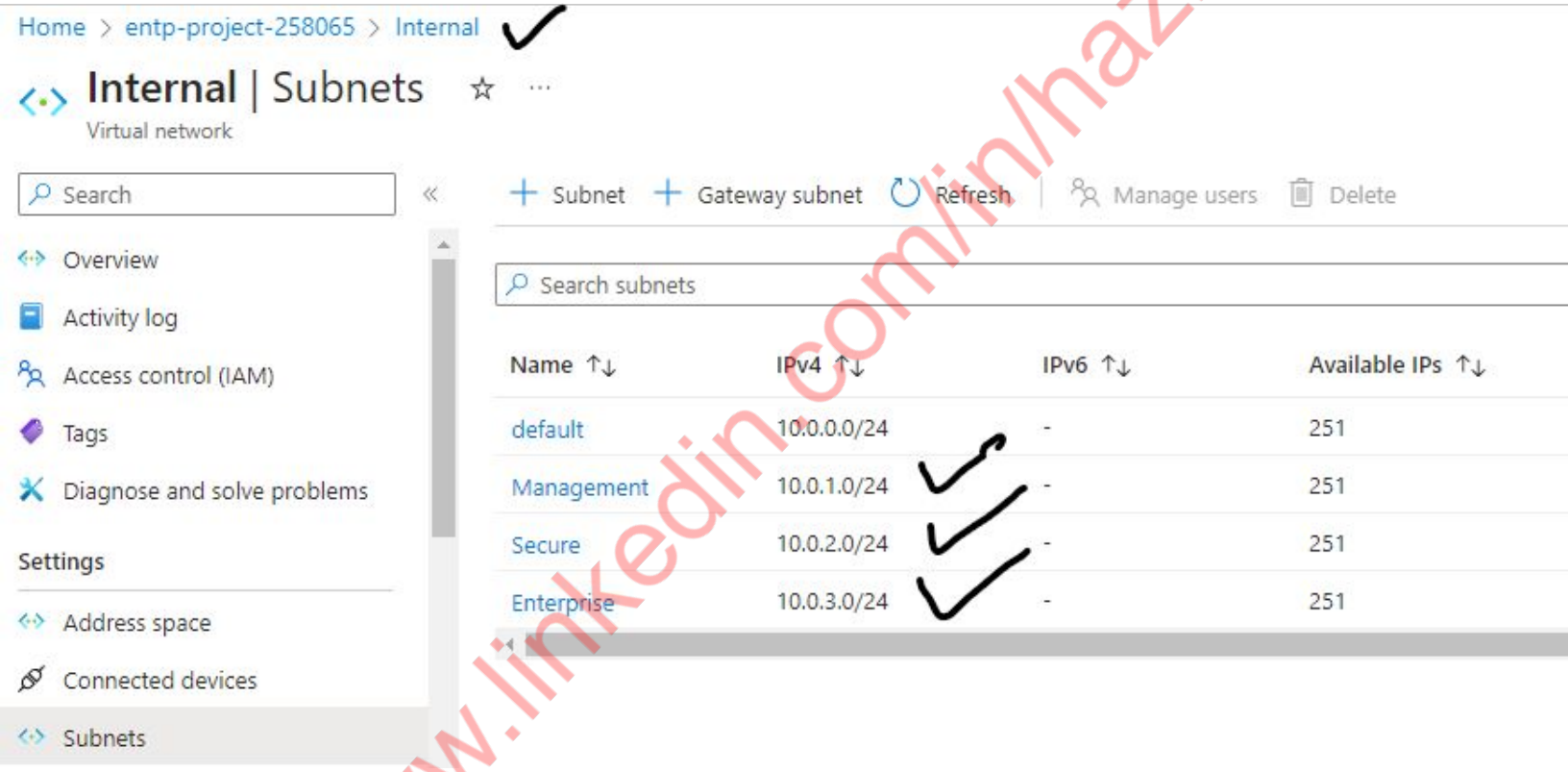


Creating Enterprise Subnet in Internal Virtual Network



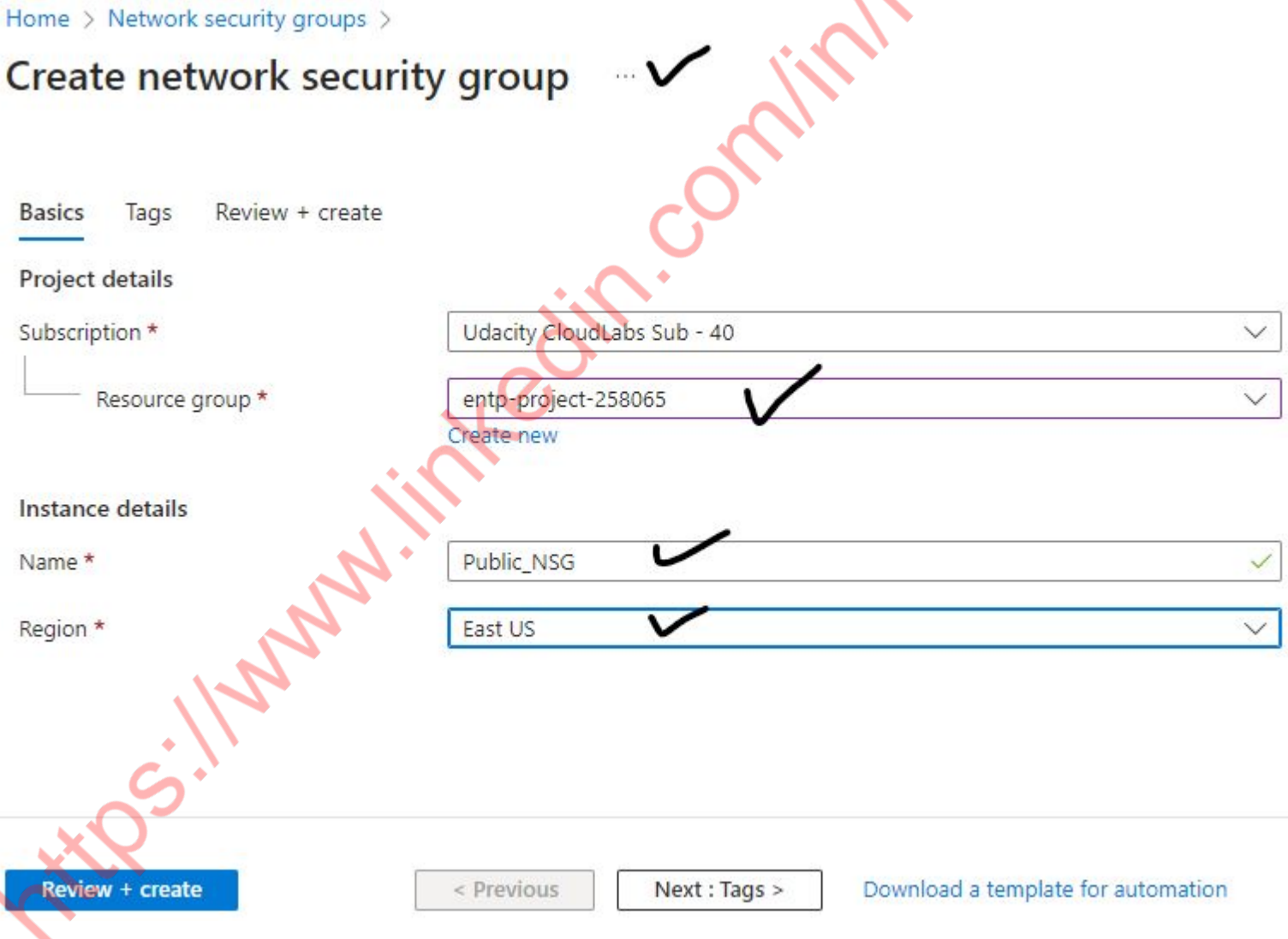


Management, Secure and Enterprise Subnets created in Internal Virtual Network

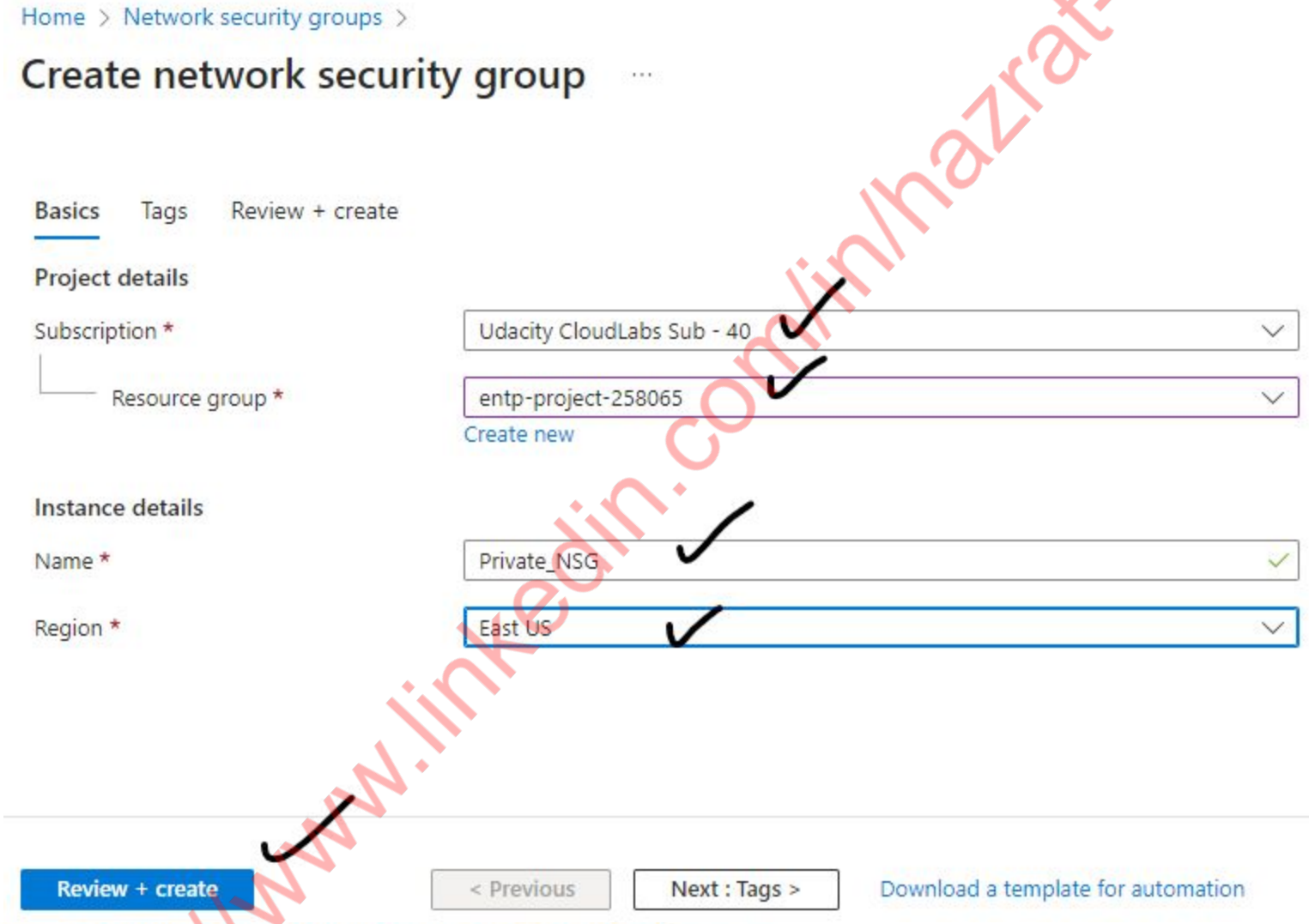


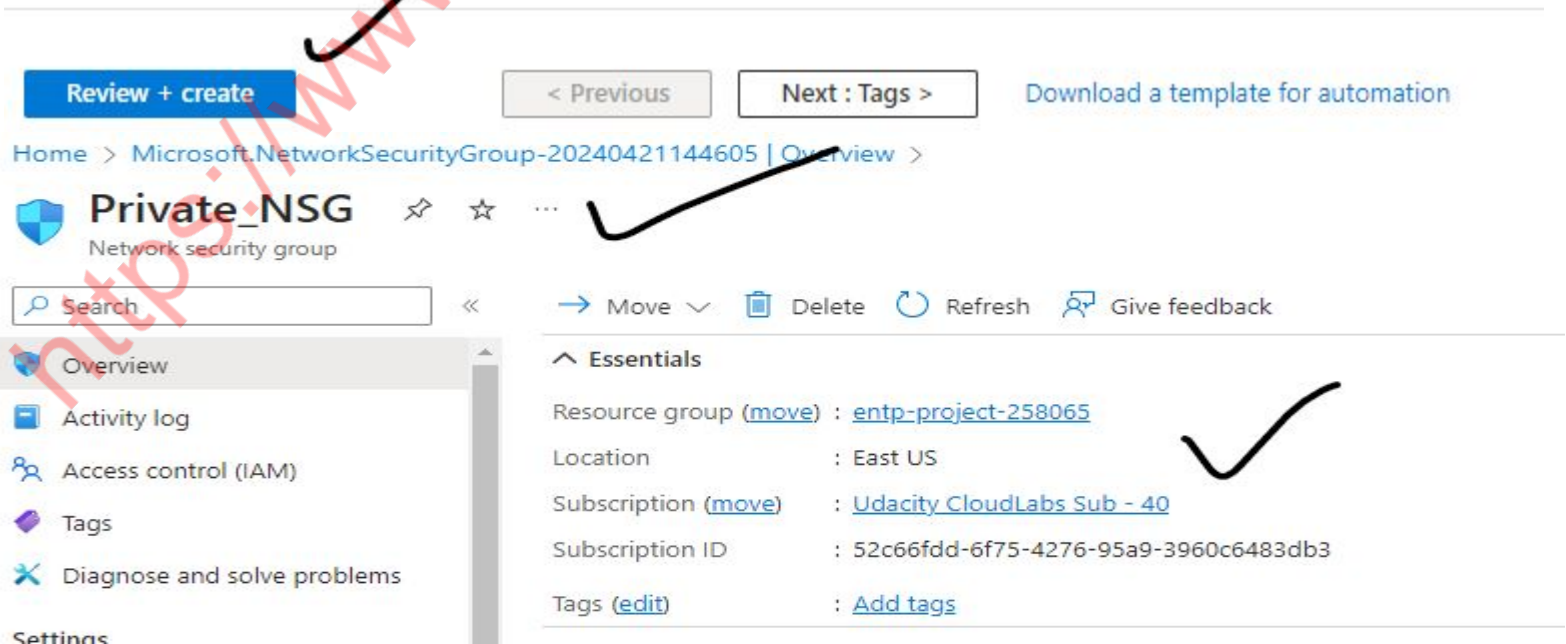
Creating Network Security Groups for the Subnets

Creating Public Network Security Group for public Subnet of DMZ



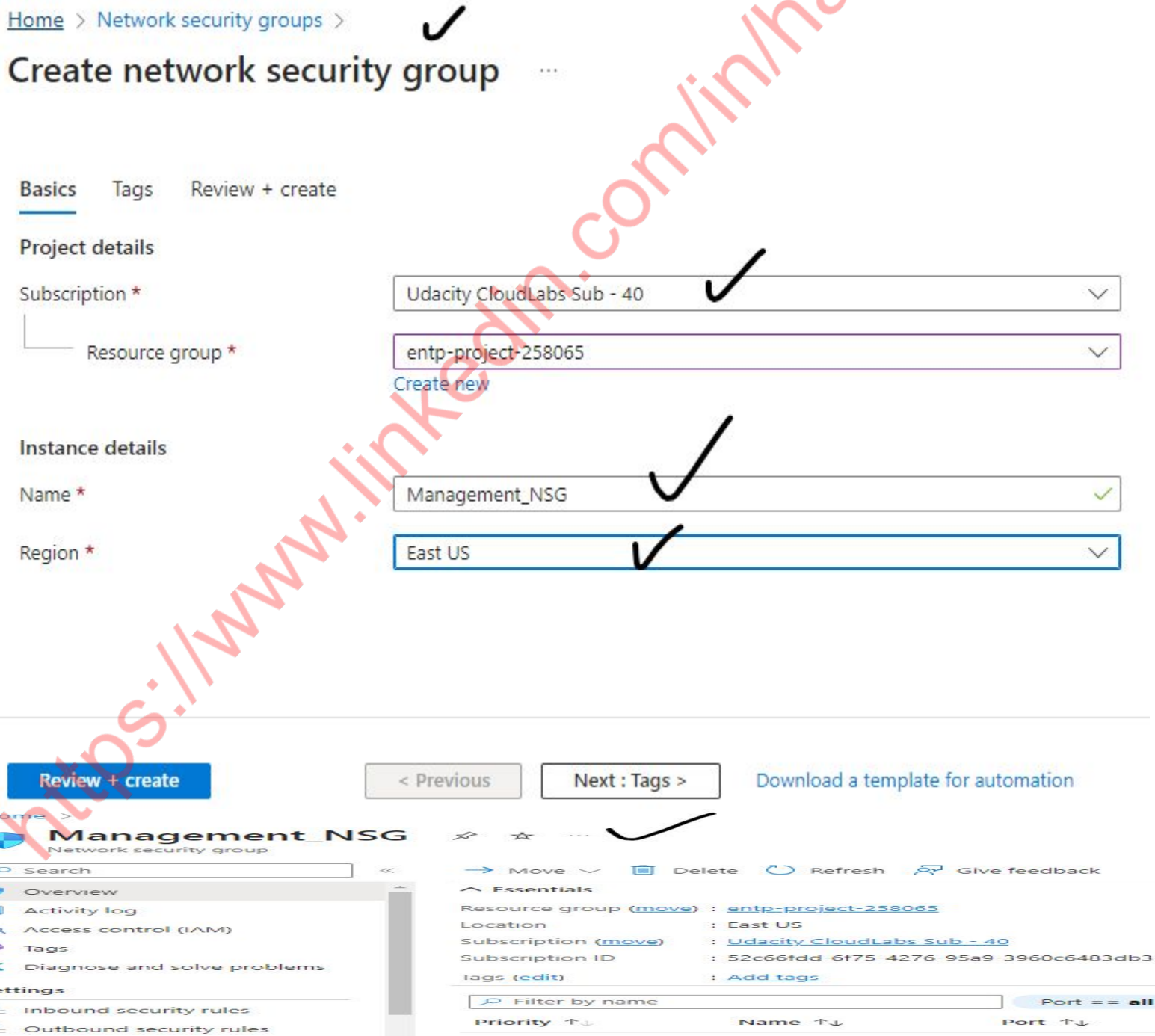
Creating Private Network Security group for Private subnet of DMZ



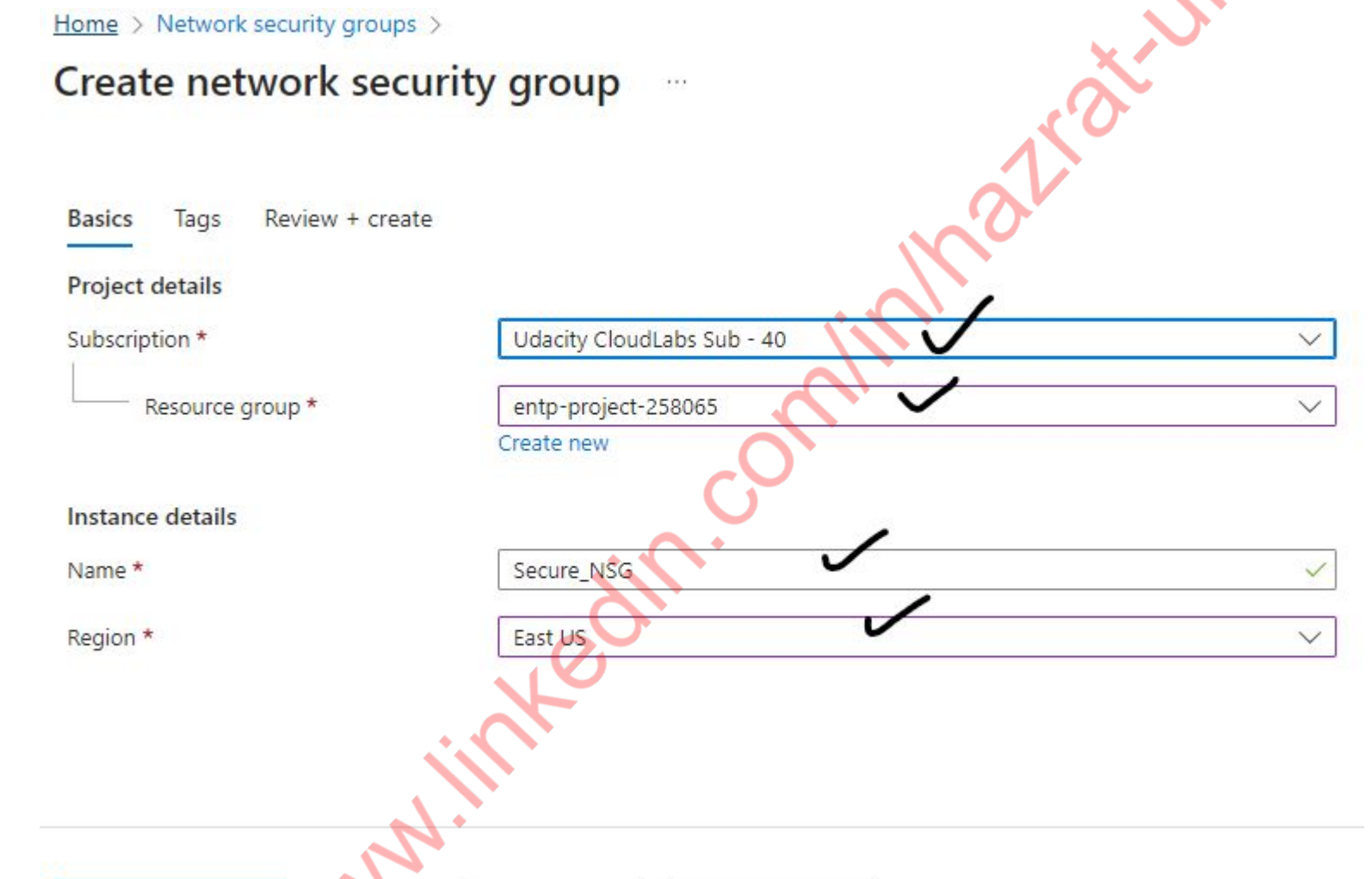


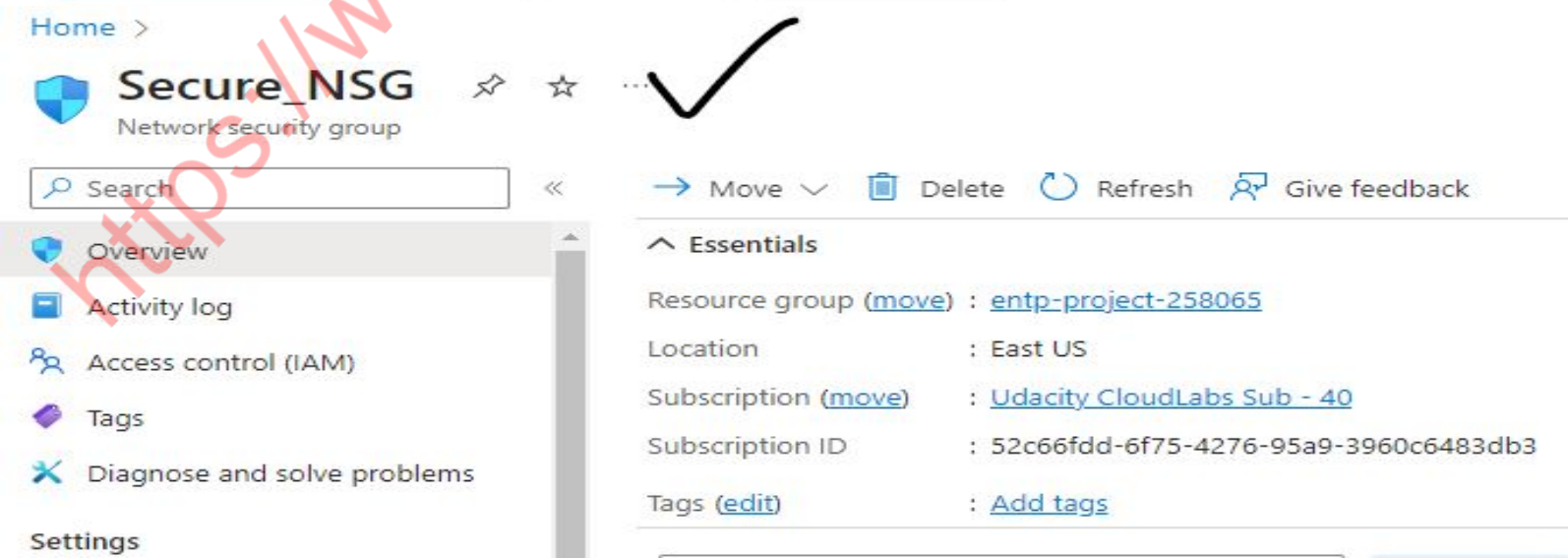
Creating Network Security Groups for Management, Secure and Enterprise

Creating NSG for Management Subnet

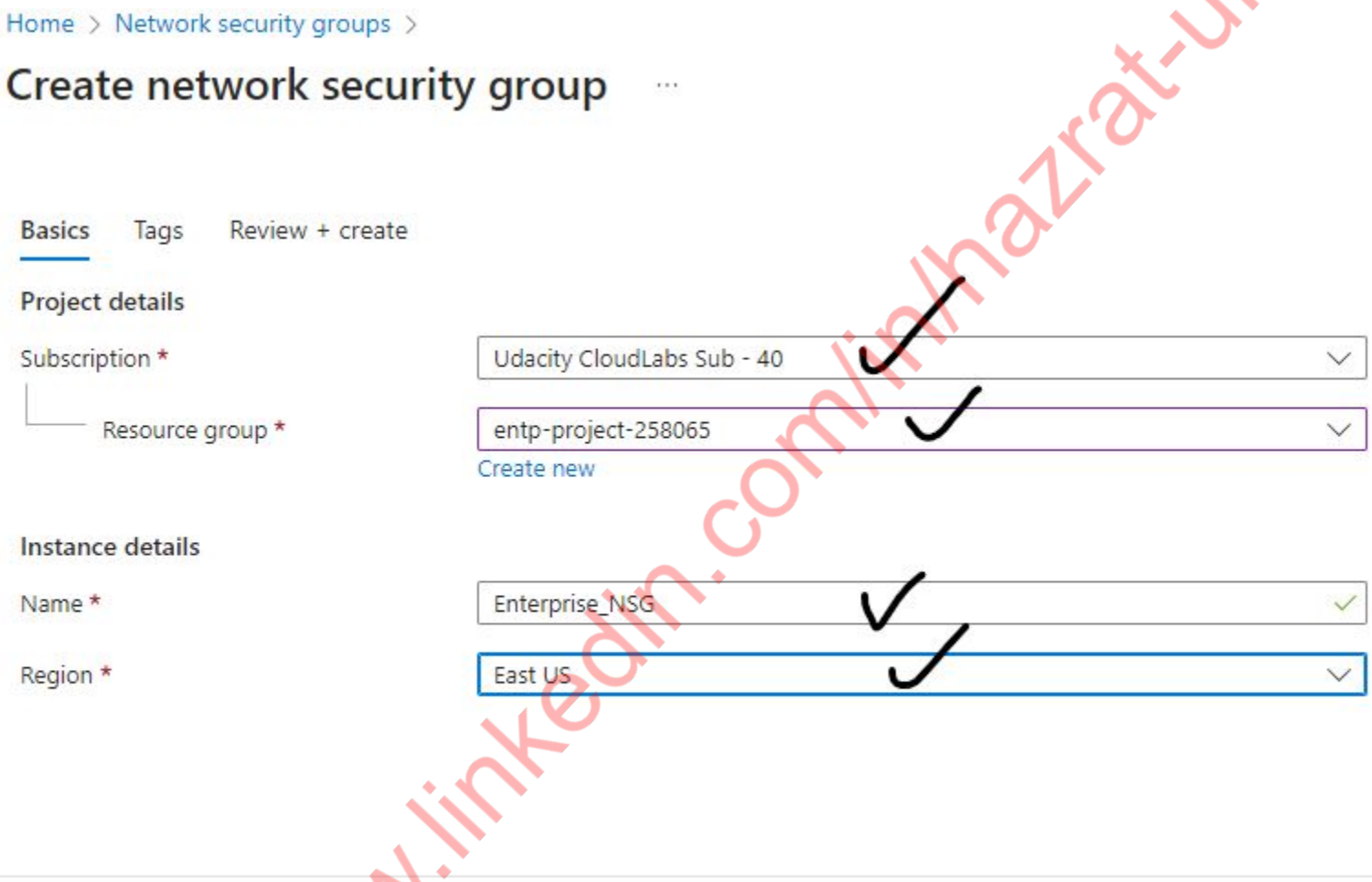


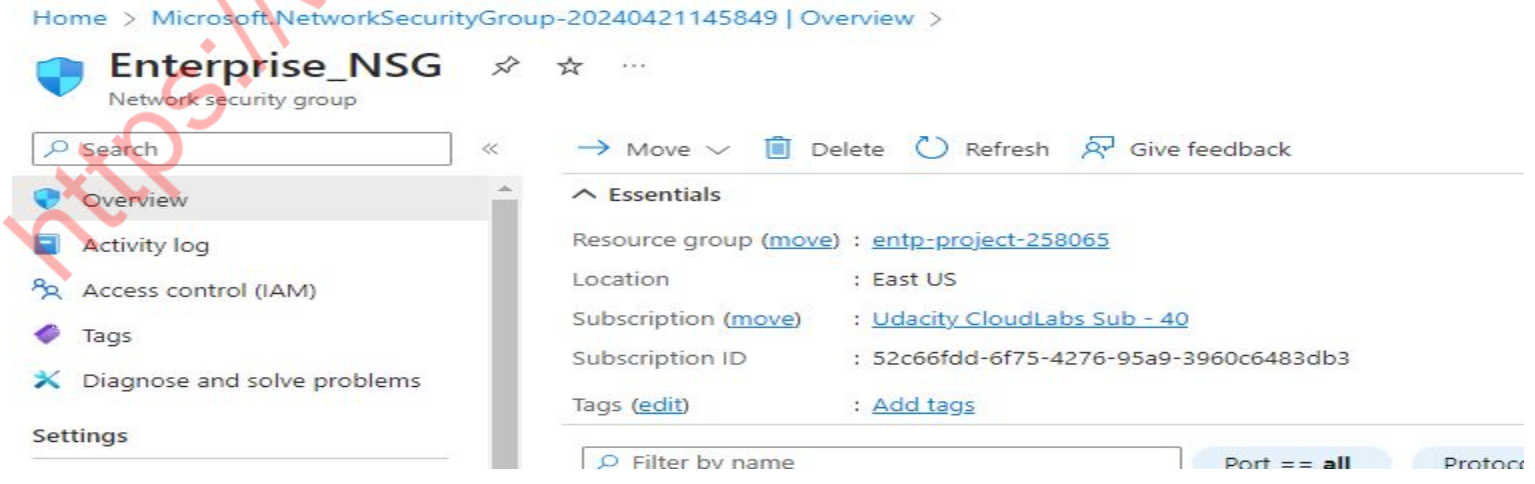
Creating NSG for Secure Subnet



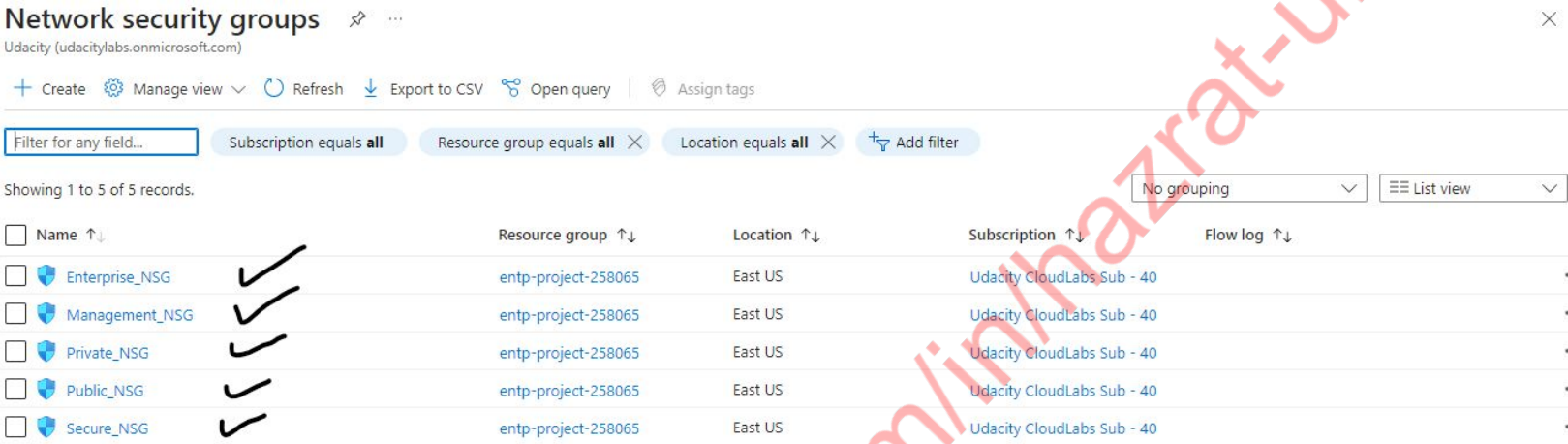


Creating NSG for Enterprise



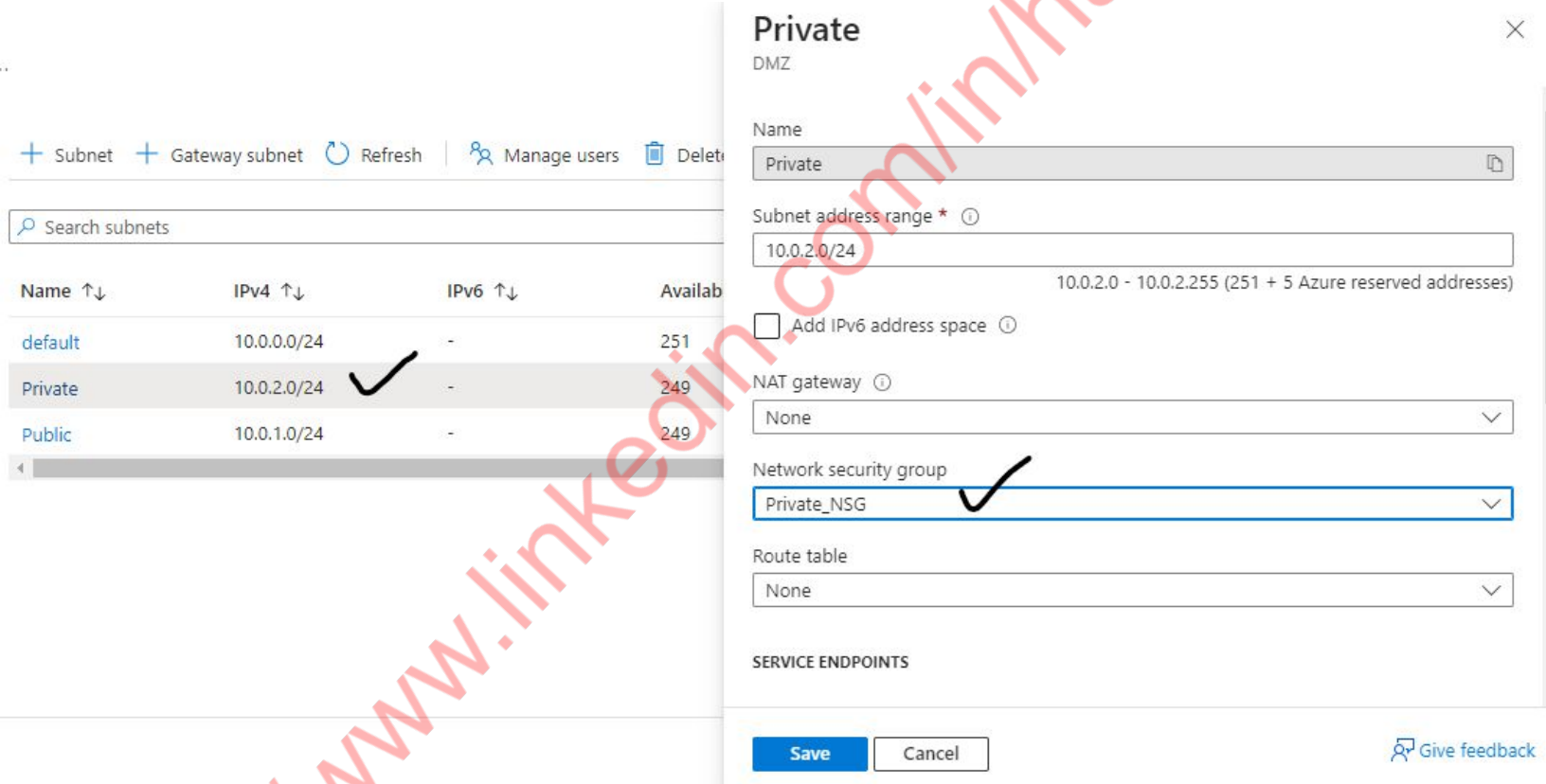


Network Security Groups created for all the subnets



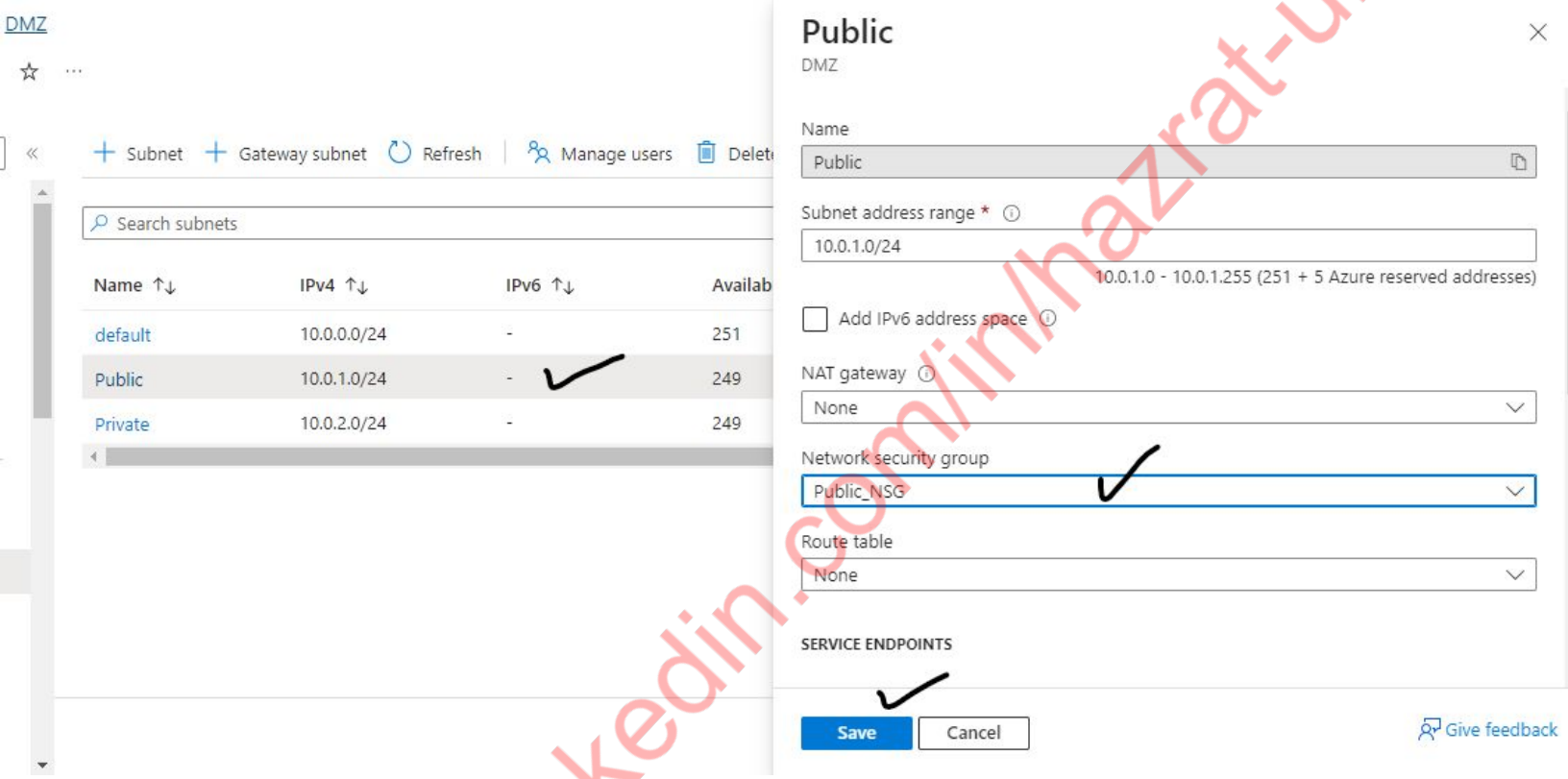
Associating subnets with Network Security Groups

Associating private DMZ Subnet with Private Network Security Group.



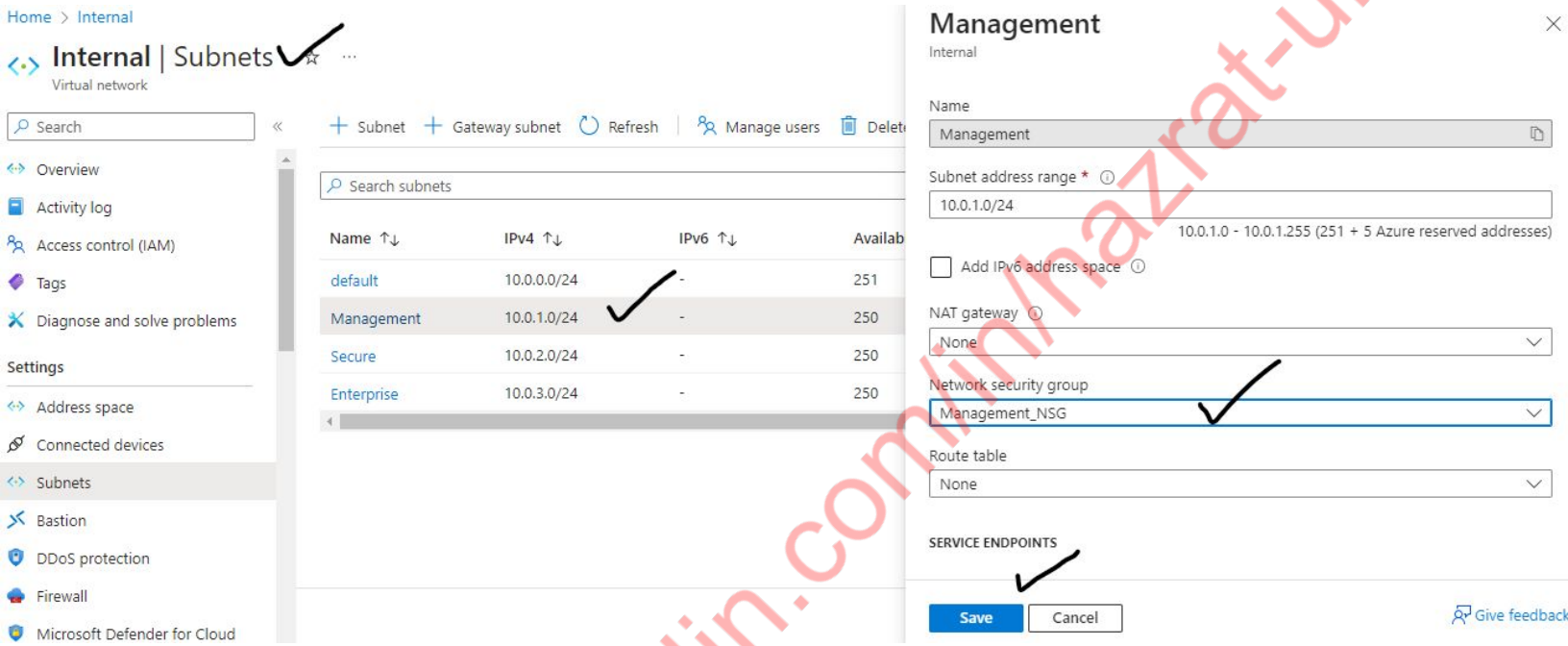
Name	IPv4	IPv6	Available IPs	Delegated to	Security group
default	10.0.0.0/24	-	251	-	-
Private	10.0.2.0/24	-	249	-	Private_NSG
Public	10.0.1.0/24	-	249	-	Public_NSG

Associating public DMZ subnet with public NSG



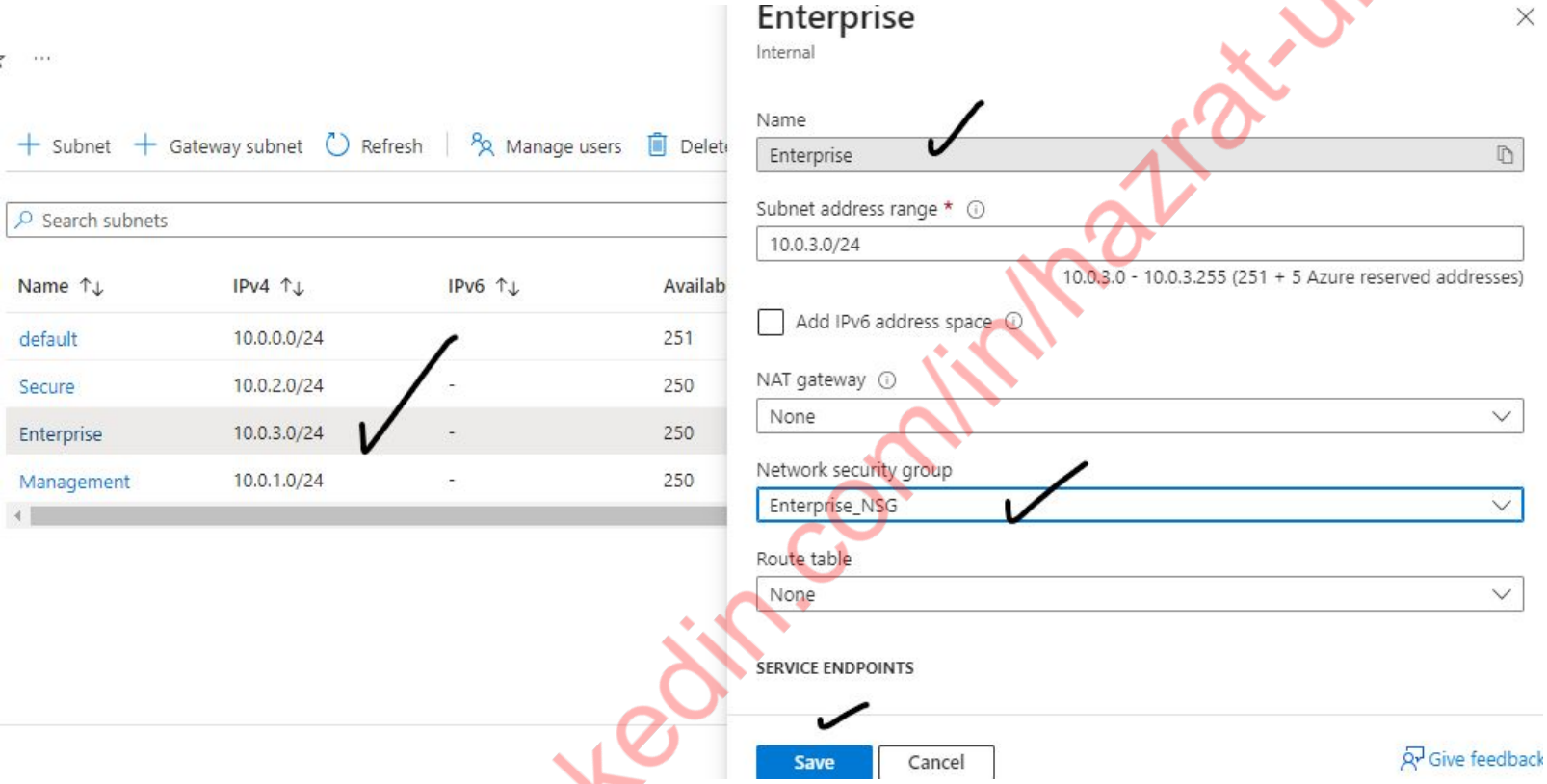
Name	IPv4	IPv6	Available IPs	Delegated to	Security group
default	10.0.0.0/24	-	251	-	-
Private	10.0.2.0/24	-	249	-	Private_NSG
Public	10.0.1.0/24	-	249	-	Public_NSG

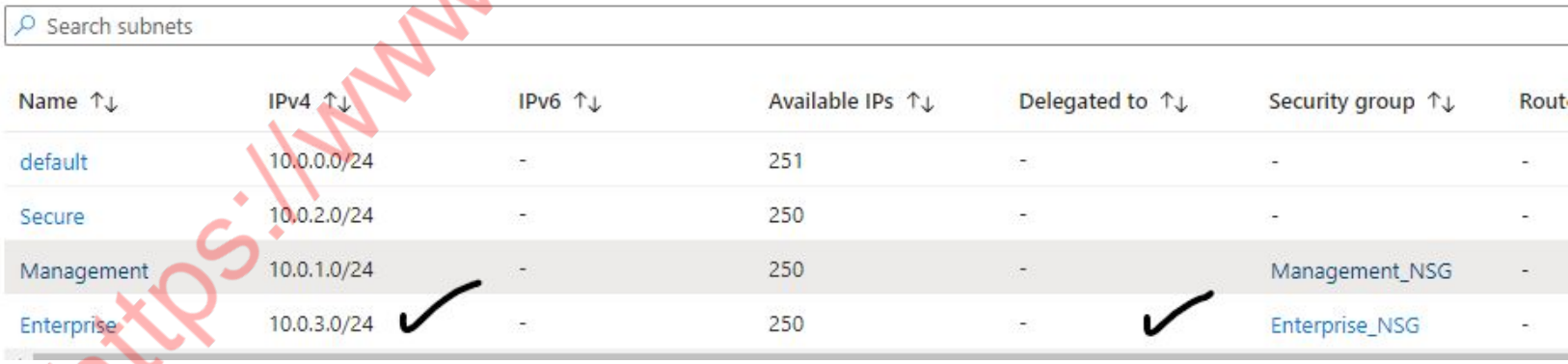
Associating Internal Management DMZ subnet with management NSG



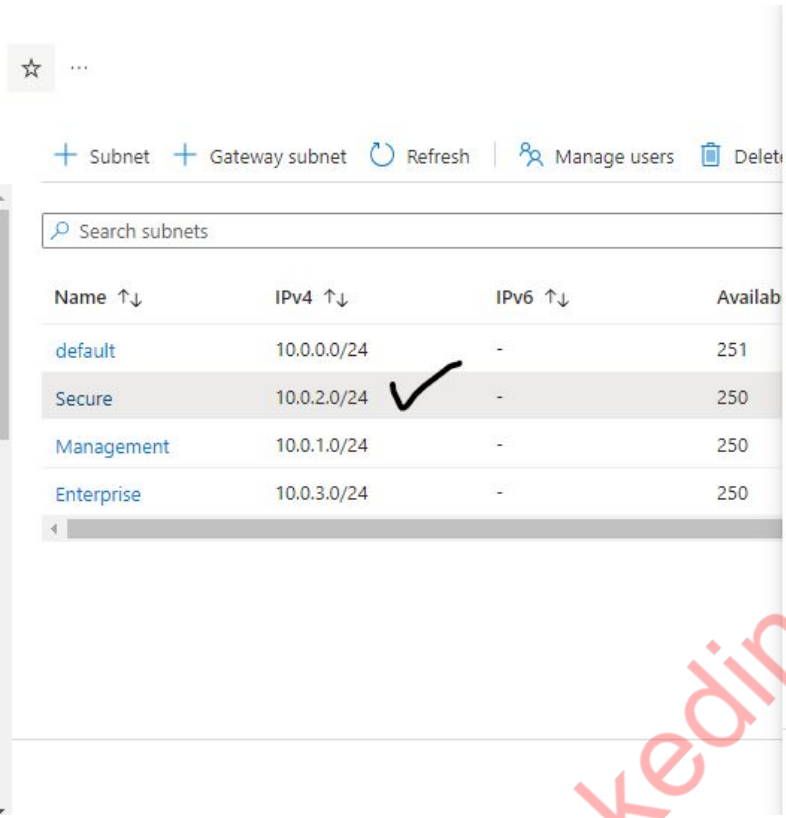
Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Ro
default	10.0.0.0/24	-	251	-	-	-
Secure	10.0.2.0/24	-	250	-	-	-
Enterprise	10.0.3.0/24	-	250	-	-	-
Management	10.0.1.0/24	-	250	-	Management_NSG	-

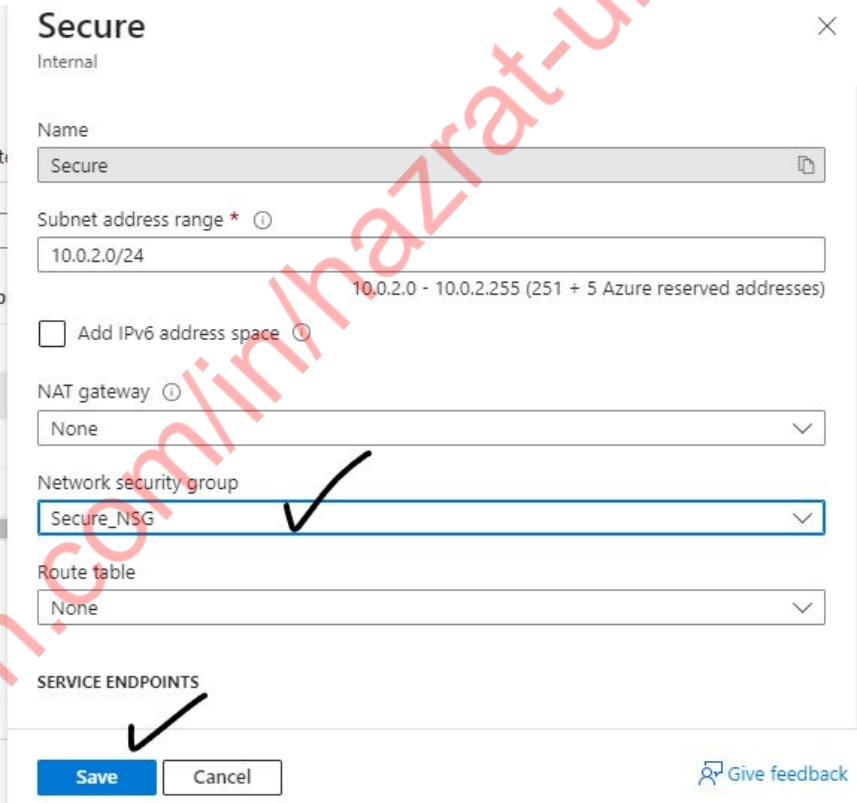
Associating Internal Enterprise DMZ subnet with Enterprise NSG





Associating Internal Secure DMZ subnet with Secure NSG





Associated all three Internal Subnets with NSGs

Search subnets

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
default	10.0.0.0/24	-	251	-	-	-
Management	10.0.1.0/24	-	250	-	Management_NSG	-
Enterprise	10.0.3.0/24	-	250	-	Enterprise_NSG	-
Secure	10.0.2.0/24	-	250	-	Secure_NSG	-

2.2 Creating Virtual Machines

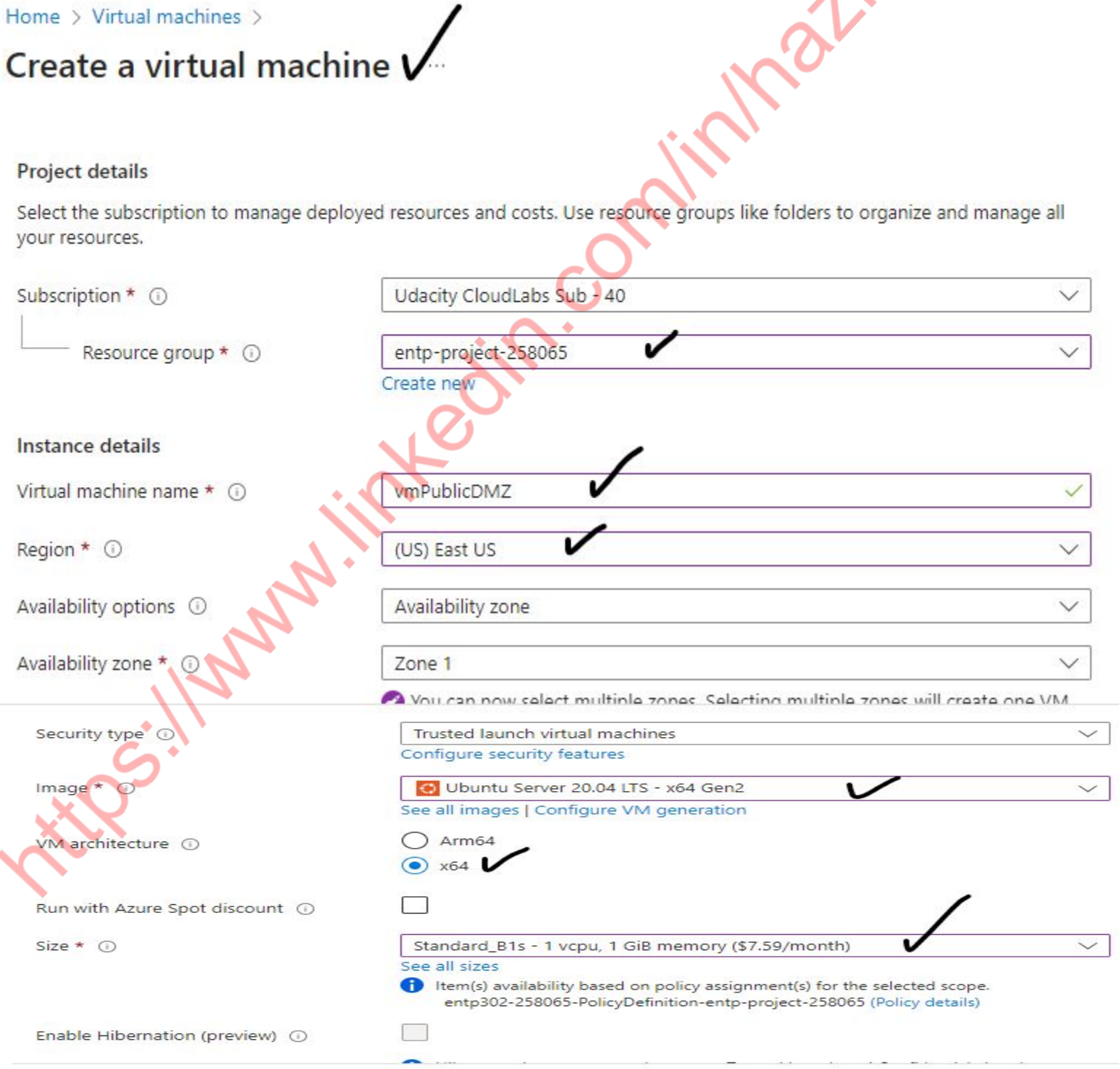
In this next section you will create Virtual Machines in your subnets. You will create 2 VMs in your DMZ and 3 VMs in your internal network. Please only use the Standard_B1s VM size and the Linux Ubuntu 18.04 image.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

2.2.1 Screenshot

Create one VM in each of your public and private DMZ subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.

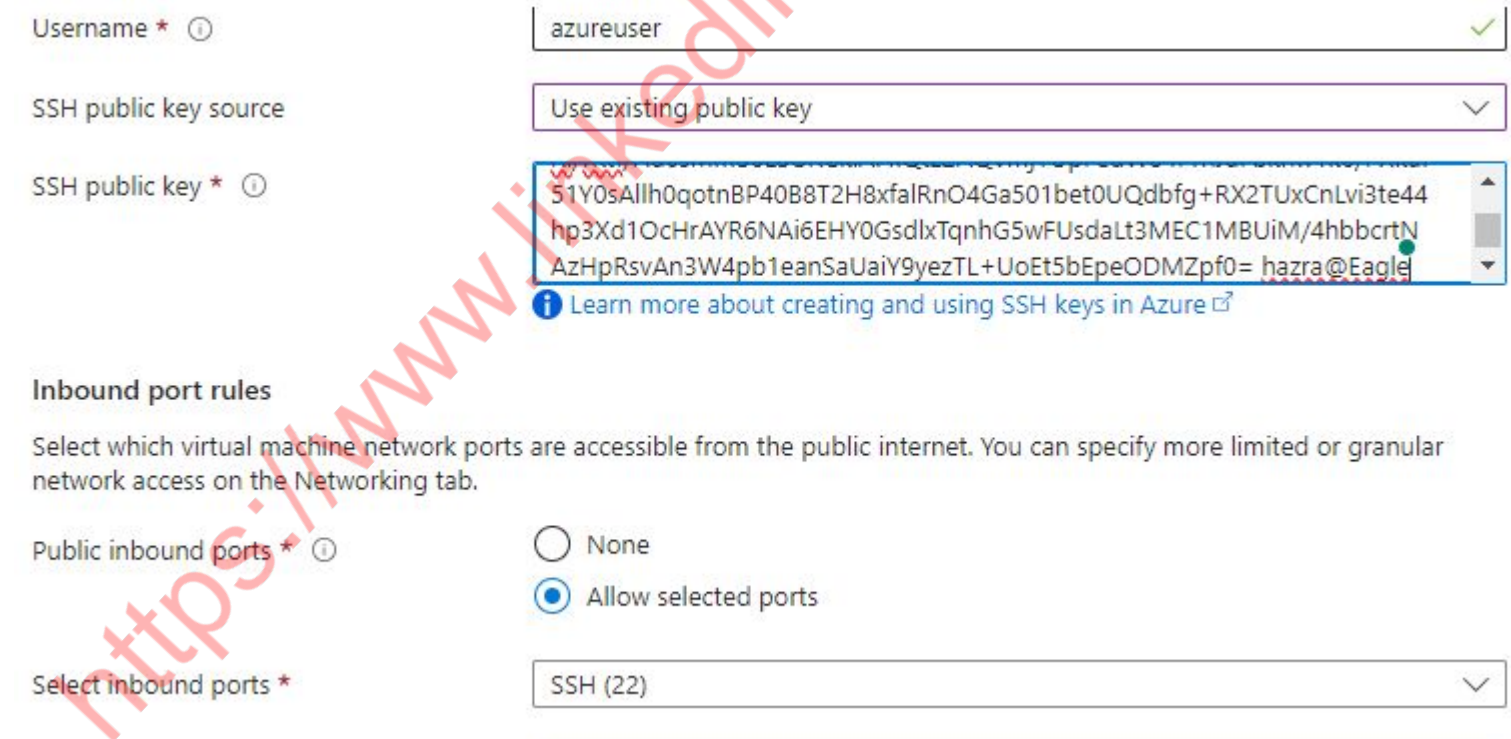
Creating VM in Public DMZ



Generating and pasting the ssh public key

```
PS C:\Users\hazra> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\hazra/.ssh/id_rsa):
C:\Users\hazra/.ssh/id_rsa already exists.
```

```
PS C:\Users\hazra> cat C:\Users\hazra/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDzIaMQaOFJrX2ArVo1WYeWd6gCferDf7iinEPeNgvJSJvQuZzbiNEE78EHV6xfl4UbzTV2GAyBApVQ+qW9
CVNHxGD9m0y5KrDHGVgMlwJuT4g6Y4Vg72RqdFPnPYtyXTfKEsaCJQkPsuhj8JdgxKcrQBzTzYO2EuDpVkb5/Ue9ArF2IdALH8simFpJxd6GZUlSOVFsC+EL
ltsIzi9tzhoNA3ilAux0l8c++WhqE0PHiVOSzsGRGI4uEye5FcI0z5FcDXHczRv6cQcVEnJ7u1z/Rl/rKtf/Ad6sMmS6LSURCkiAl4iQtz2AQVmjYUpFedW8
4PrhJuFbkhw1k6/PXkui51Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44hp3Xd1OcHrAYR6NAi6EHY0GsdlxTqnhG5wFU
sdaLt3MEC1MBUiM/4hbbcrtNAzHpRsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMZpf0= hazra@Eagle
```



Leaving the Disk portion as default

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ⓘ ☐

ⓘ Encryption at host is not registered for the selected subscription.
Learn more about enabling this feature

OS disk

OS disk size ⓘ — Image default (30 GiB)

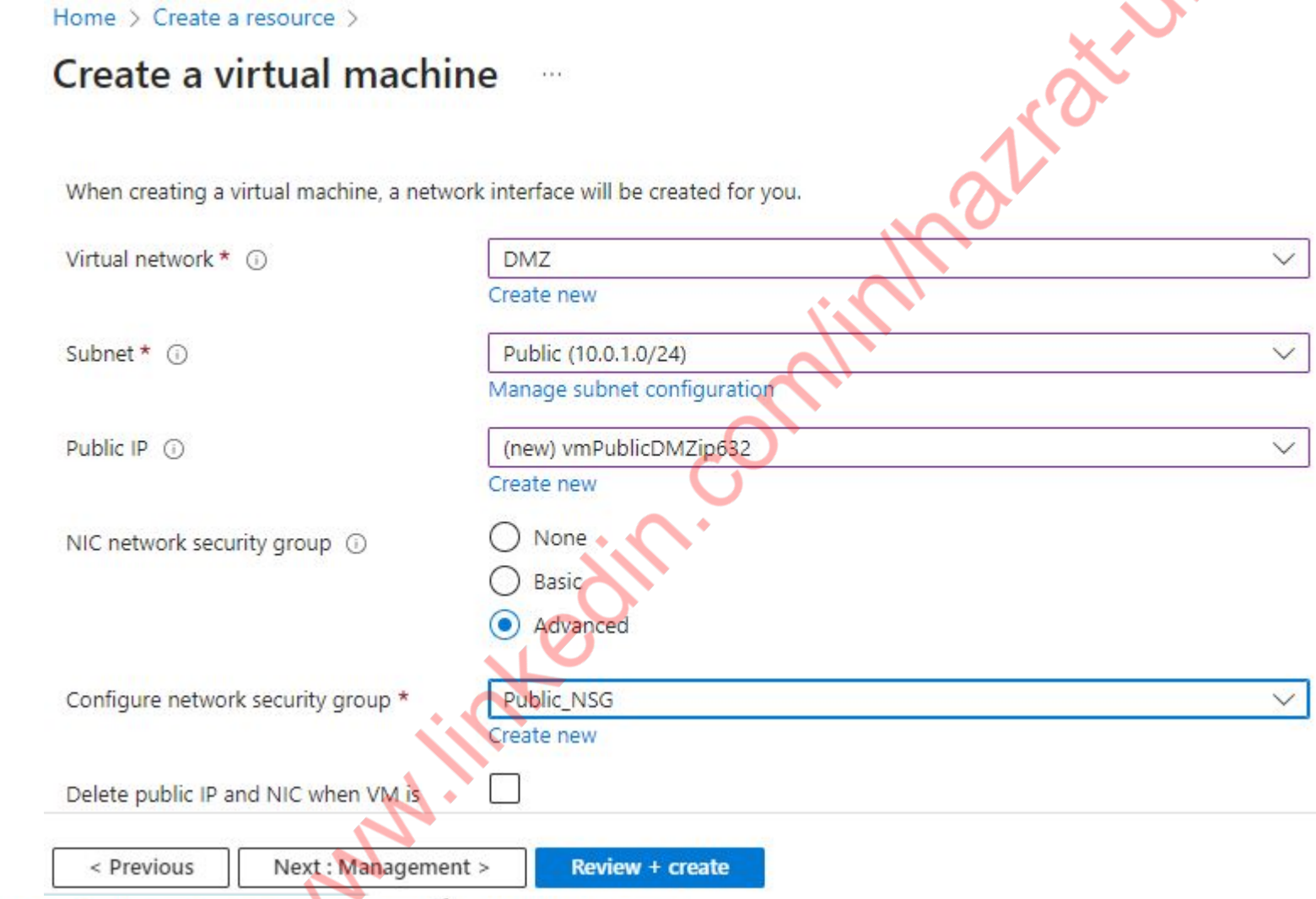
OS disk type * ⓘ — Premium SSD (locally-redundant storage)

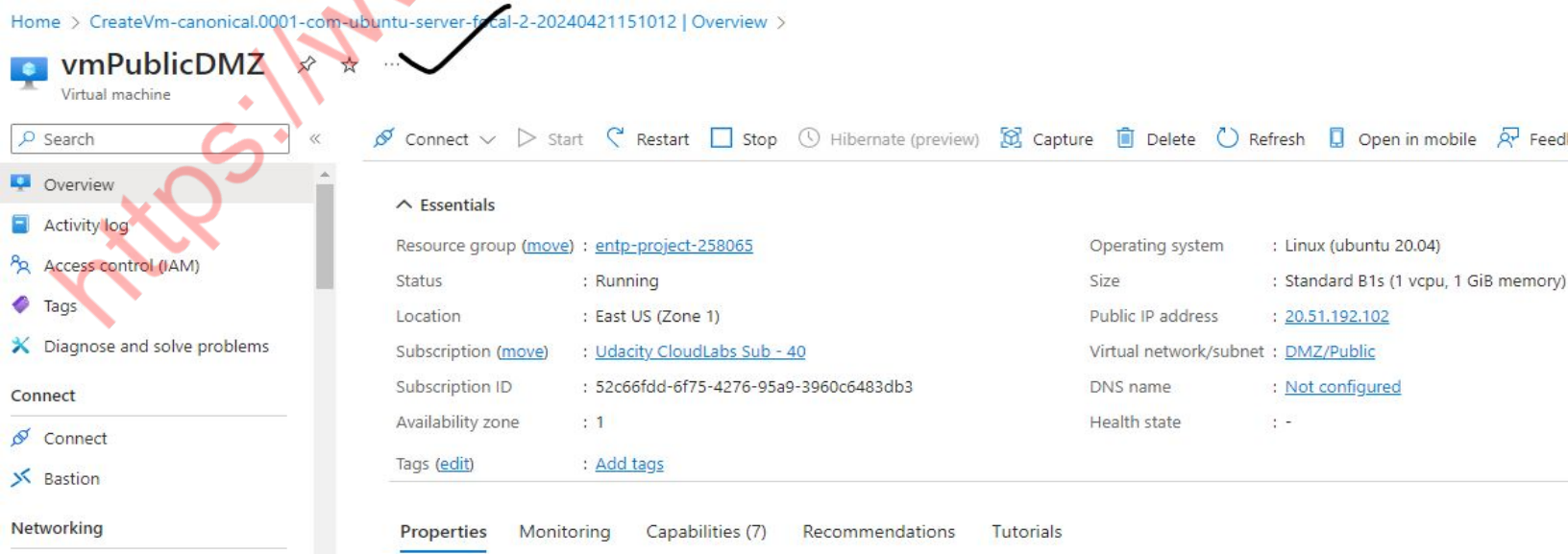
Delete with VM ⓘ ☑

Key management ⓘ — Platform-managed key

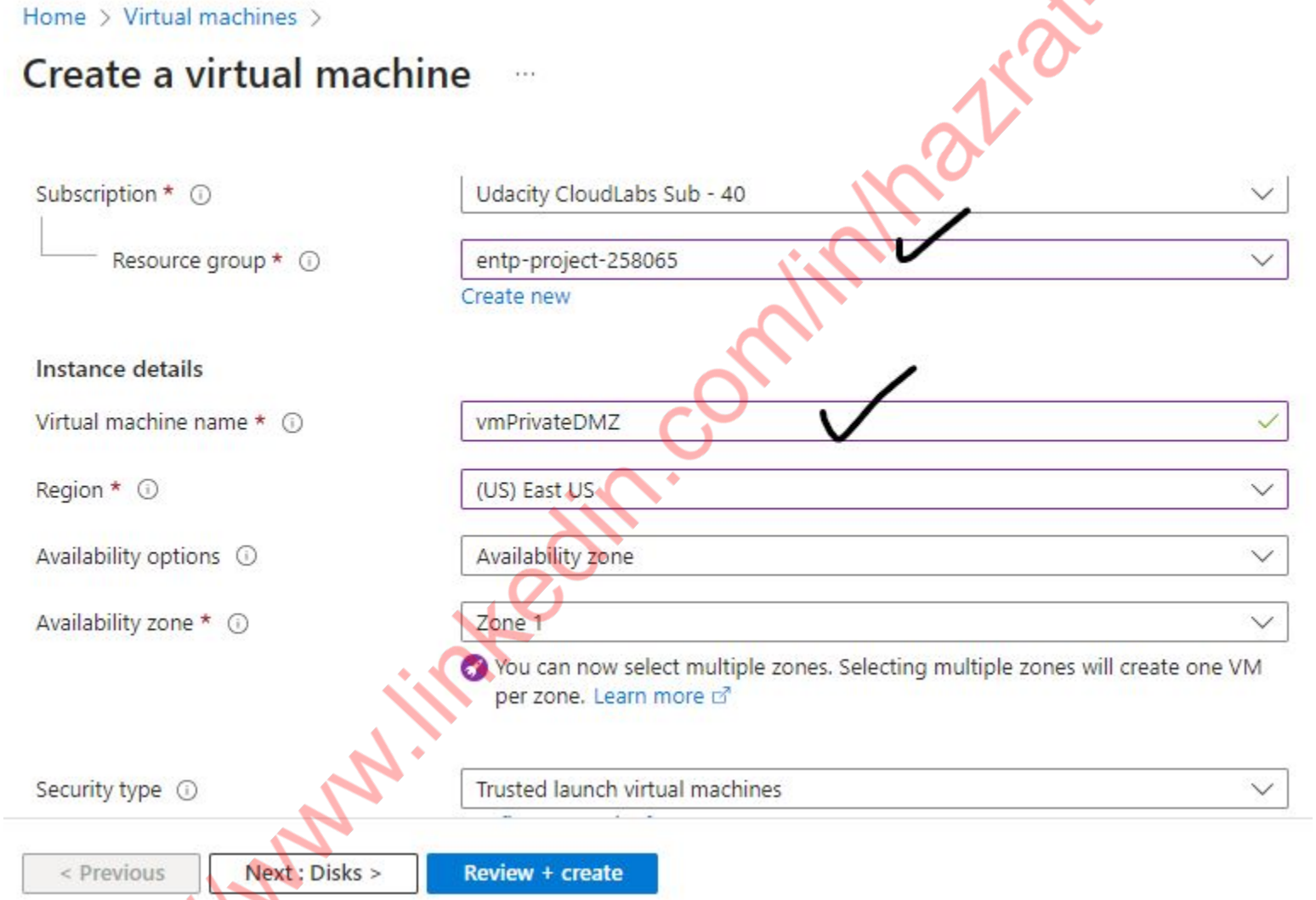
Enable Ultra Disk compatibility ⓘ ☐

Assigning it a virtual network and subnet





Creating VM in Private DMZ subnet



Home > Virtual machines >

Create a virtual machine ...

Basics | Disks | **Networking** | Management | Monitoring | 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 * : DMZ
Create new

Subnet * : Private (10.0.2.0/24)
Manage subnet configuration

Public IP : (new) vmPrivateDMZ-ip
Create new

NIC network security group : None

< Previous | Next : Management > | Review + create

vmPrivateDMZ created

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20240421151600 | Overview >

vmPrivateDMZ
Virtual machine

Search

Connect | Start | Restart | Stop | Hibernate (preview) | Capture | Delete | Refresh | Open in mobile | Feedback

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

Connect
- Connect
- Bastion

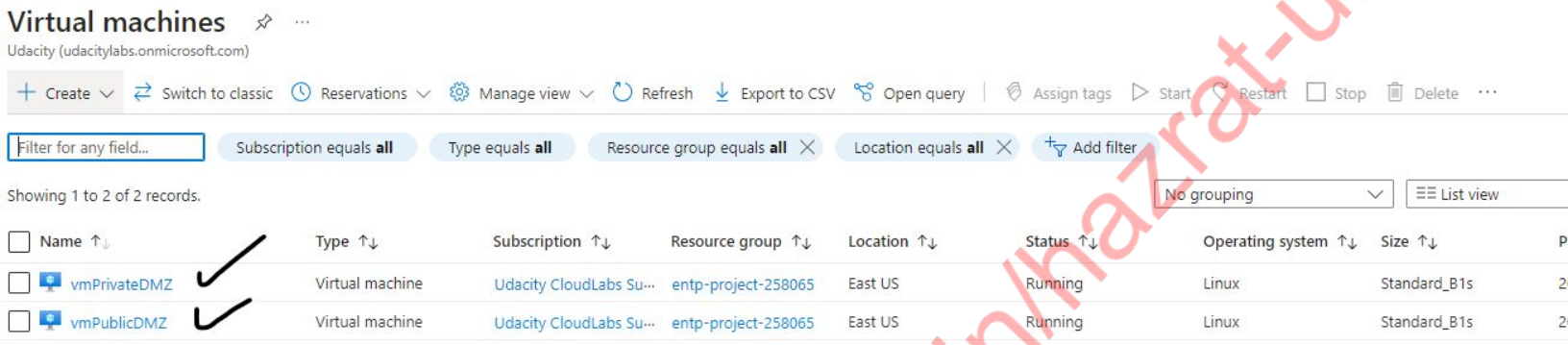
Networking

Essentials

Resource group (move)	: entp-project-258065	Operating system	: Linux (ubuntu 20.04)
Status	: Running	Size	: Standard B1s (1 vcpu, 1 GiB memory)
Location	: East US (Zone 1)	Public IP address	: 20.51.193.77
Subscription (move)	: Udacity CloudLabs Sub - 40	Virtual network/subnet	: DMZ/Private
Subscription ID	: 52c66fdd-6f75-4276-95a9-3960c6483db3	DNS name	: Not configured
Availability zone	: 1	Health state	: -
Tags (edit)	: Add tags		

Properties | Monitoring | Capabilities (7) | Recommendations | Tutorials

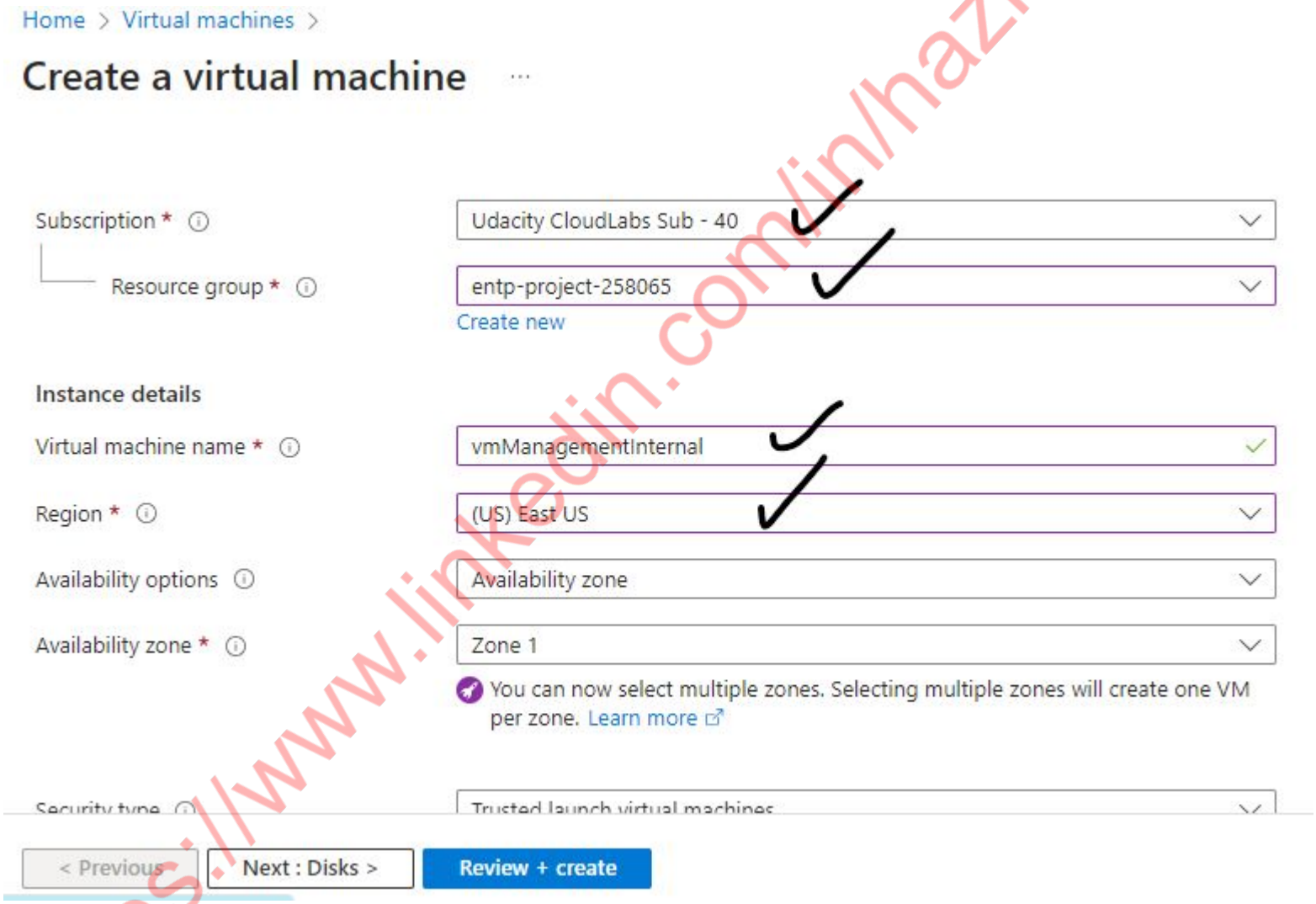
VMs Created in Public and Private DMZ subnets



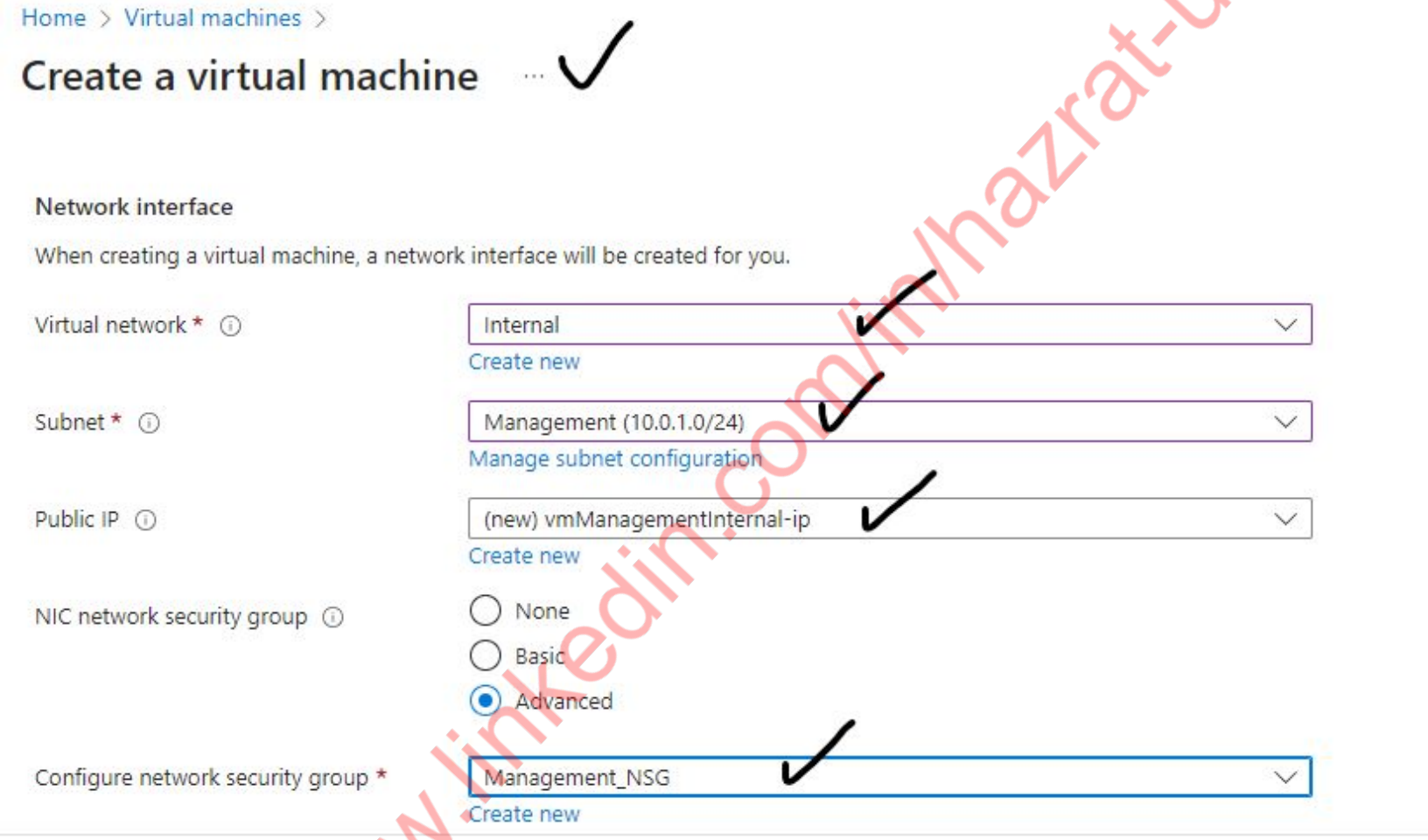
2.2.2 Screenshot

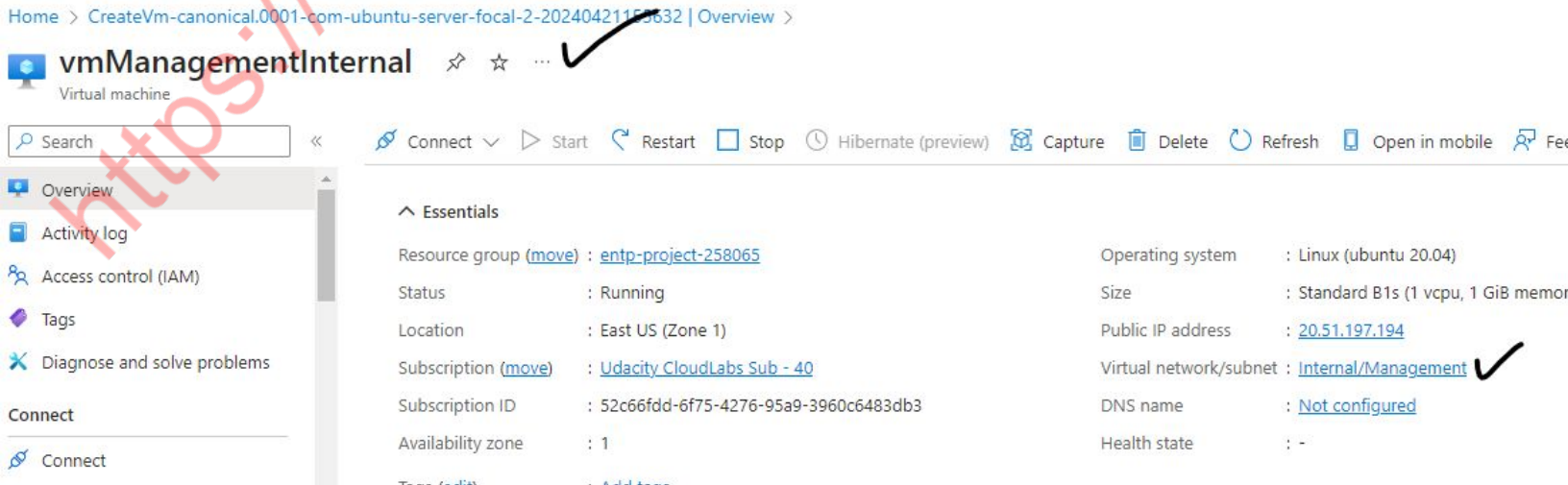
Create one VM in each of your Management, Secure, and Enterprise internal subnets. Please only use Standard_B1s for your VM size and select the Linux Ubuntu 18.04 image, otherwise you will encounter an error.

Creating VM in Management subnet

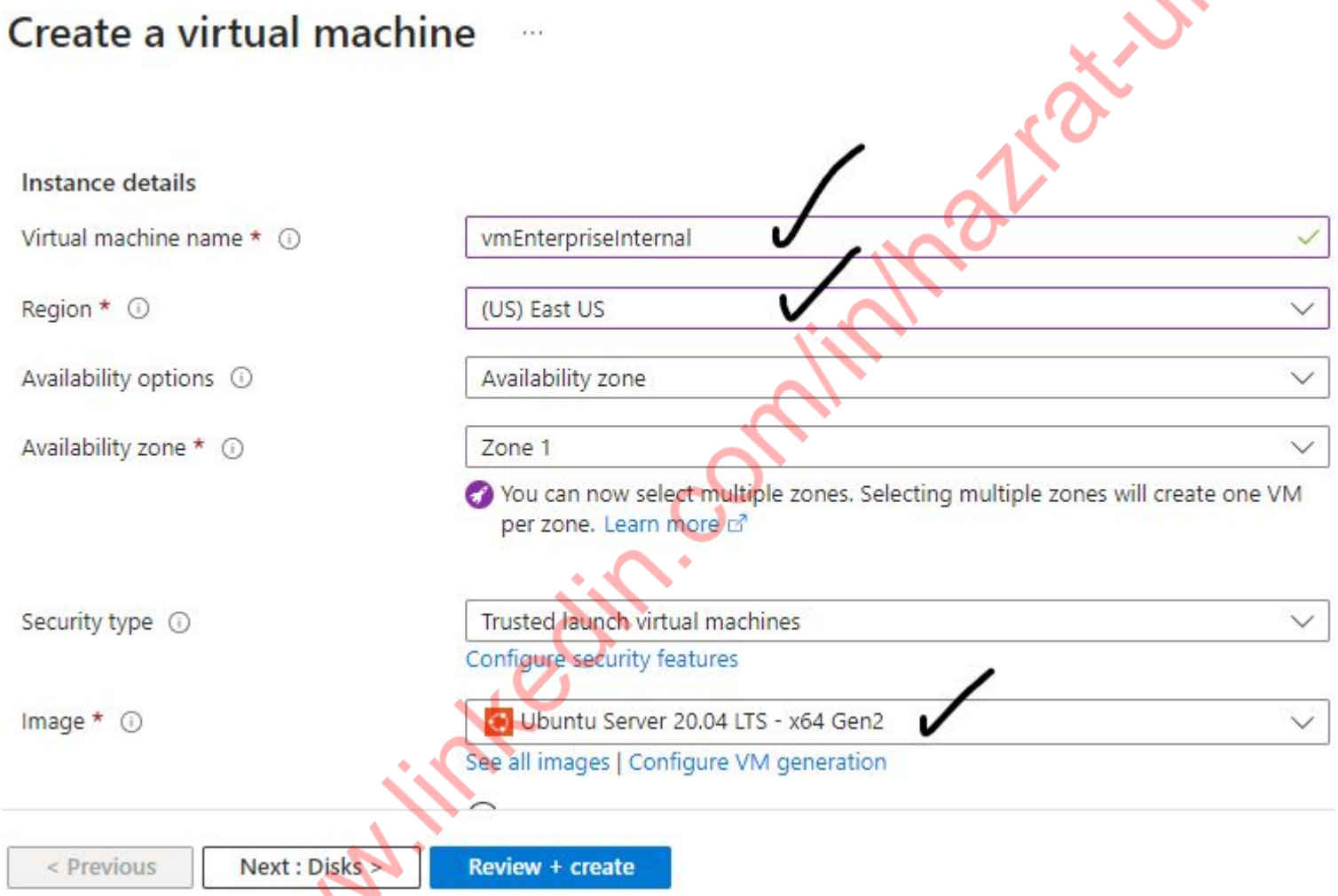


Assigning Virtual Network, Internal Subnet and NSG

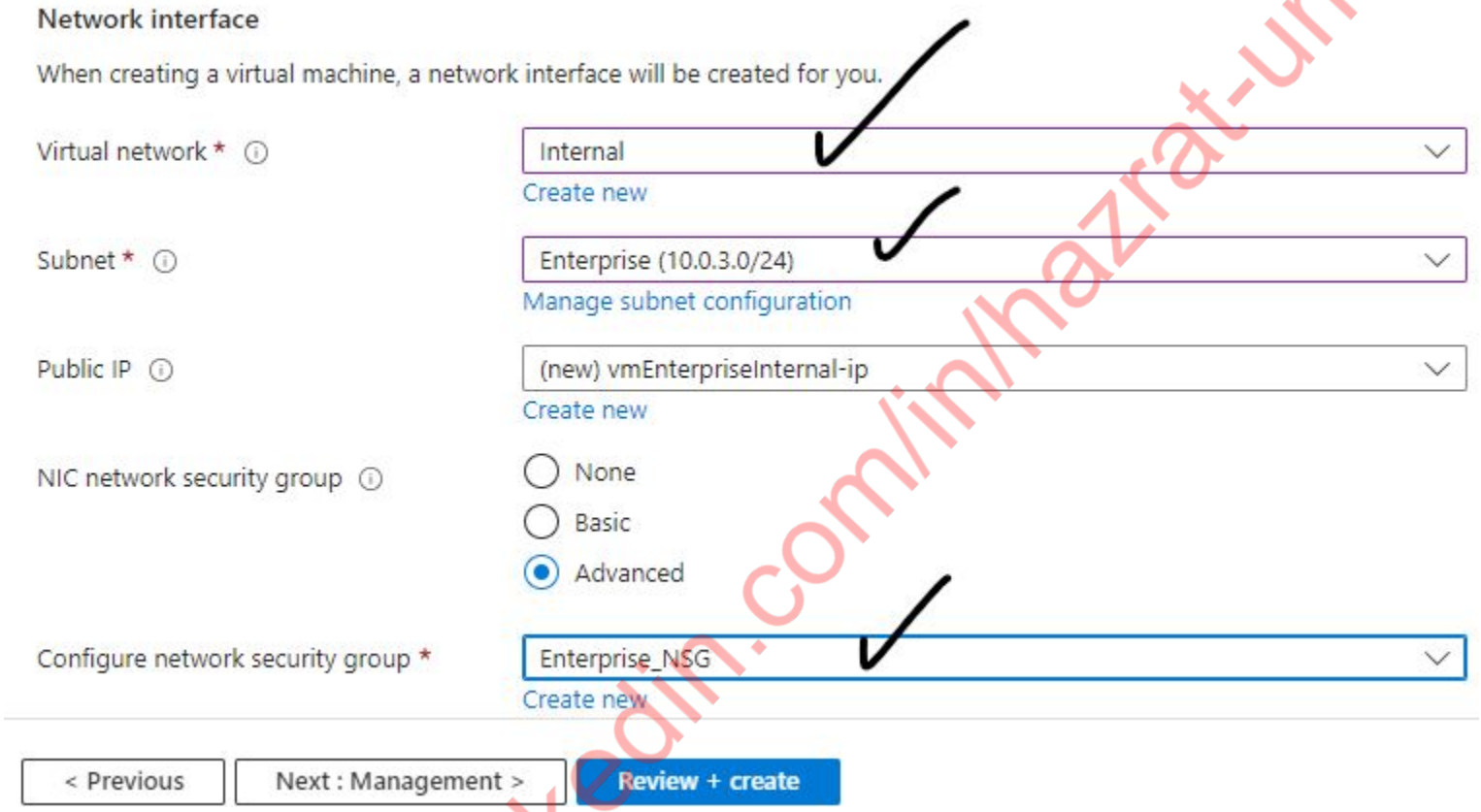


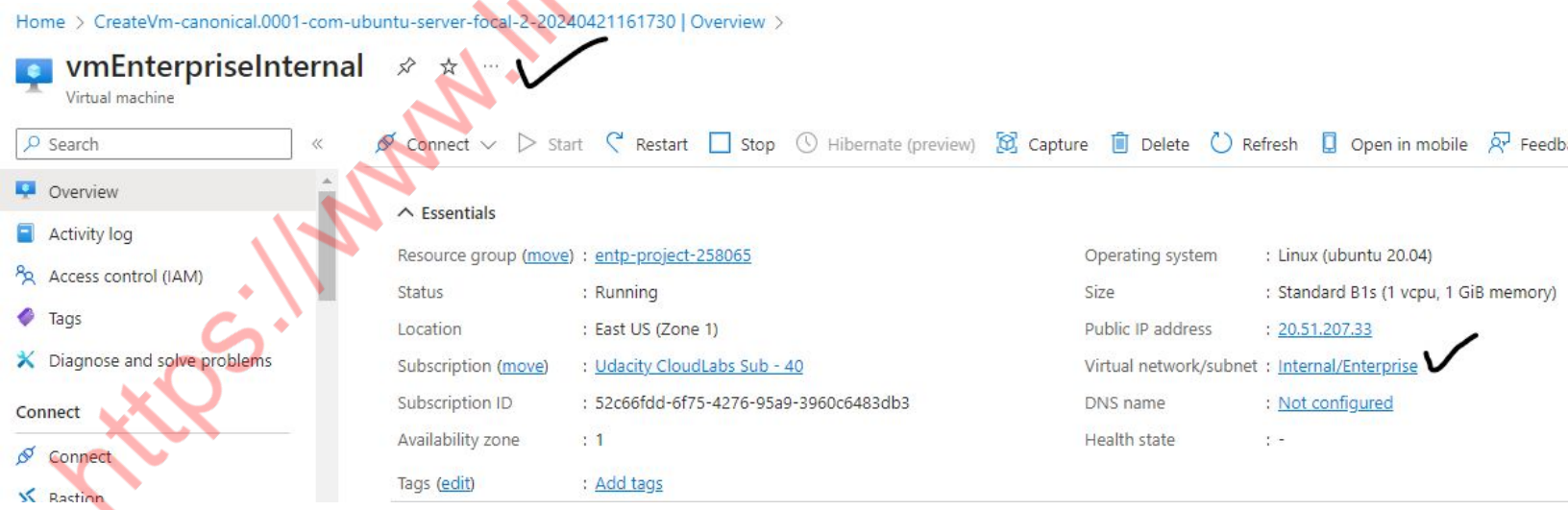


Creating VM in Enterprise Internal Subnet

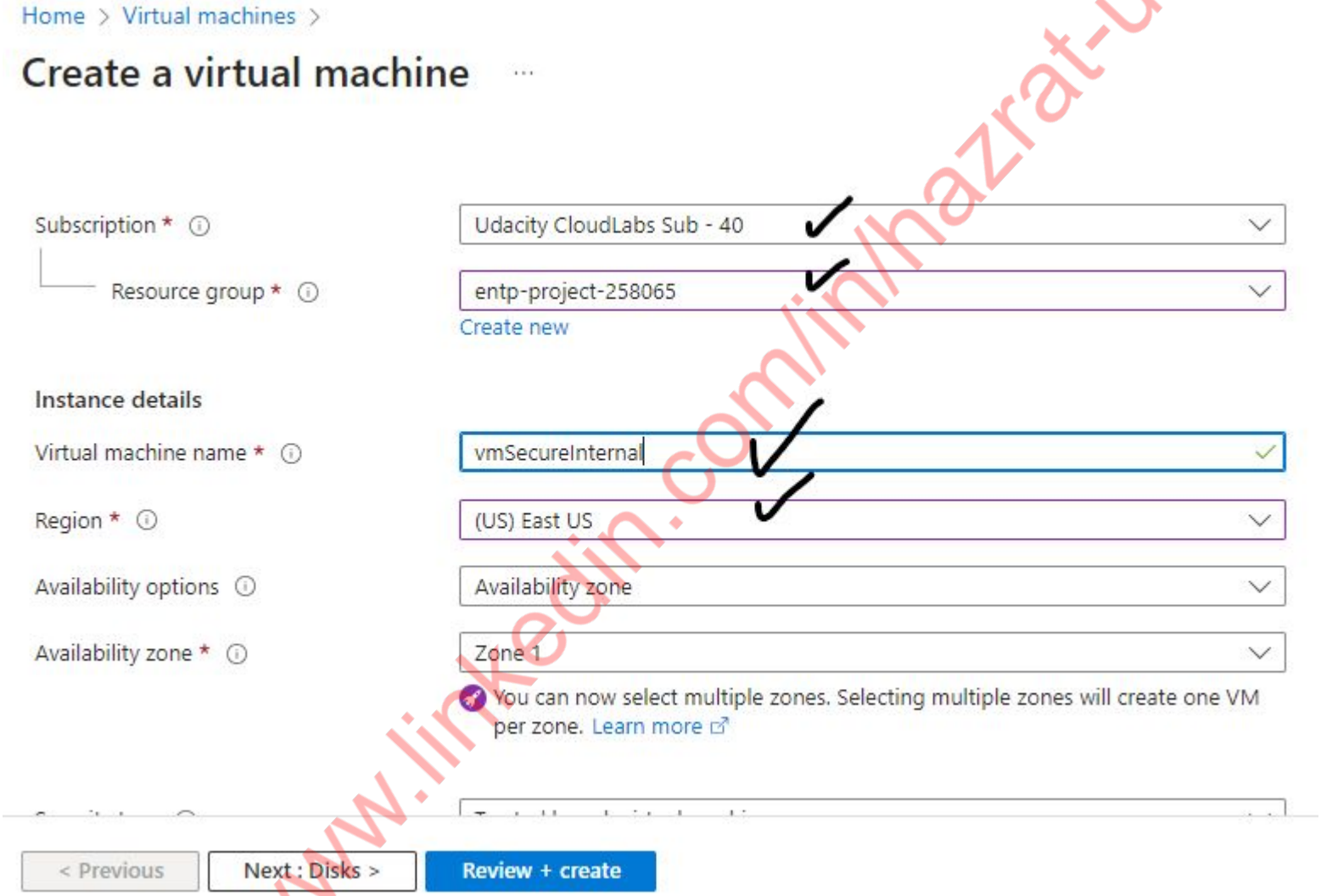


Assigning Virtual Network, Internal Subnet and NSG

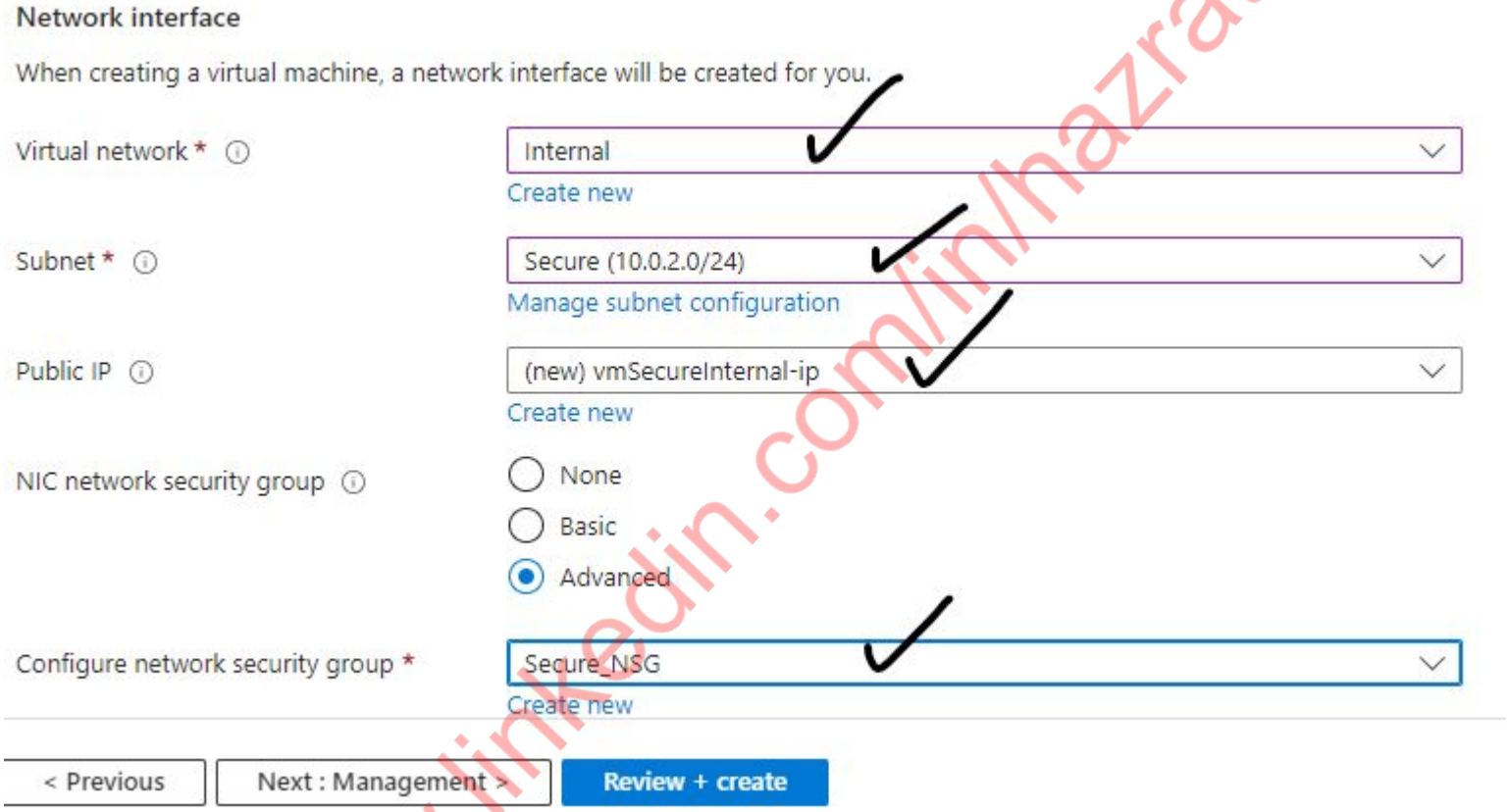


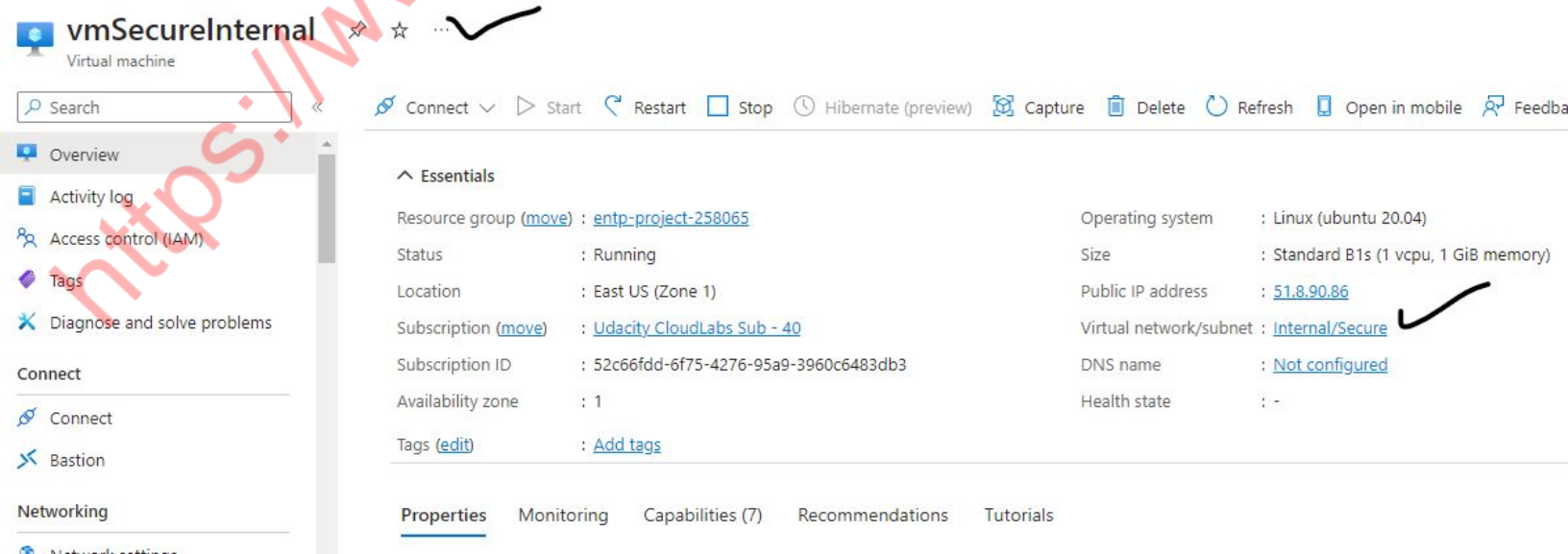


Creating VM in Secure Subnet

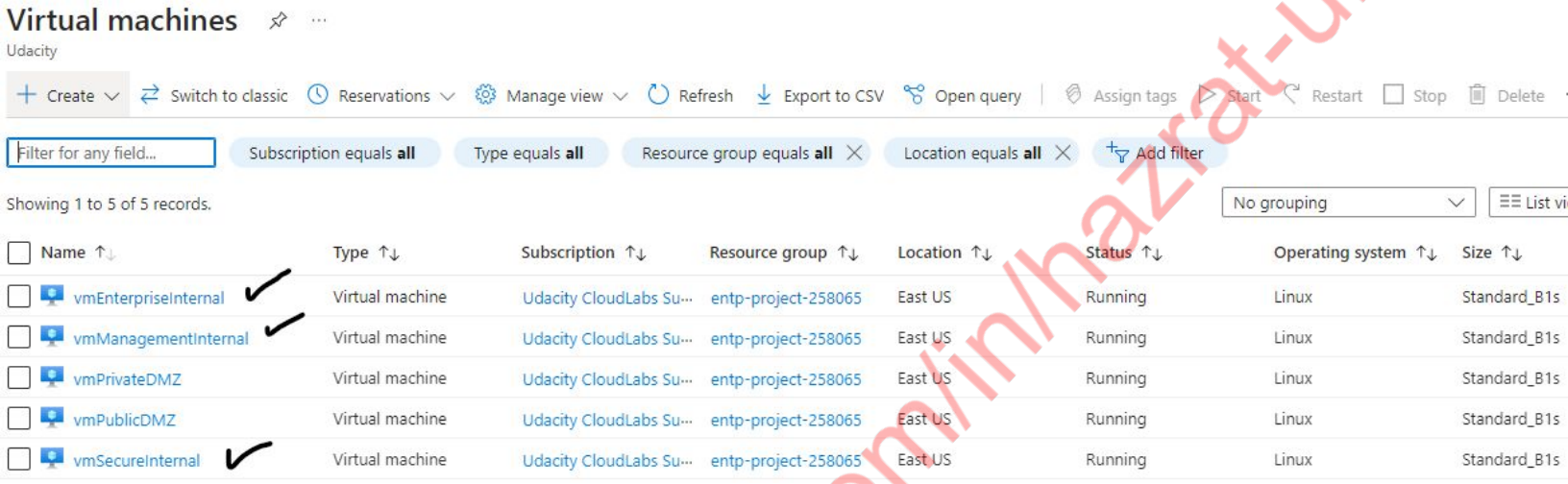


Assigning Virtual Network, Network Security Group and Subnet





Three VMs deployed in Internal



2.3 Secure Routing

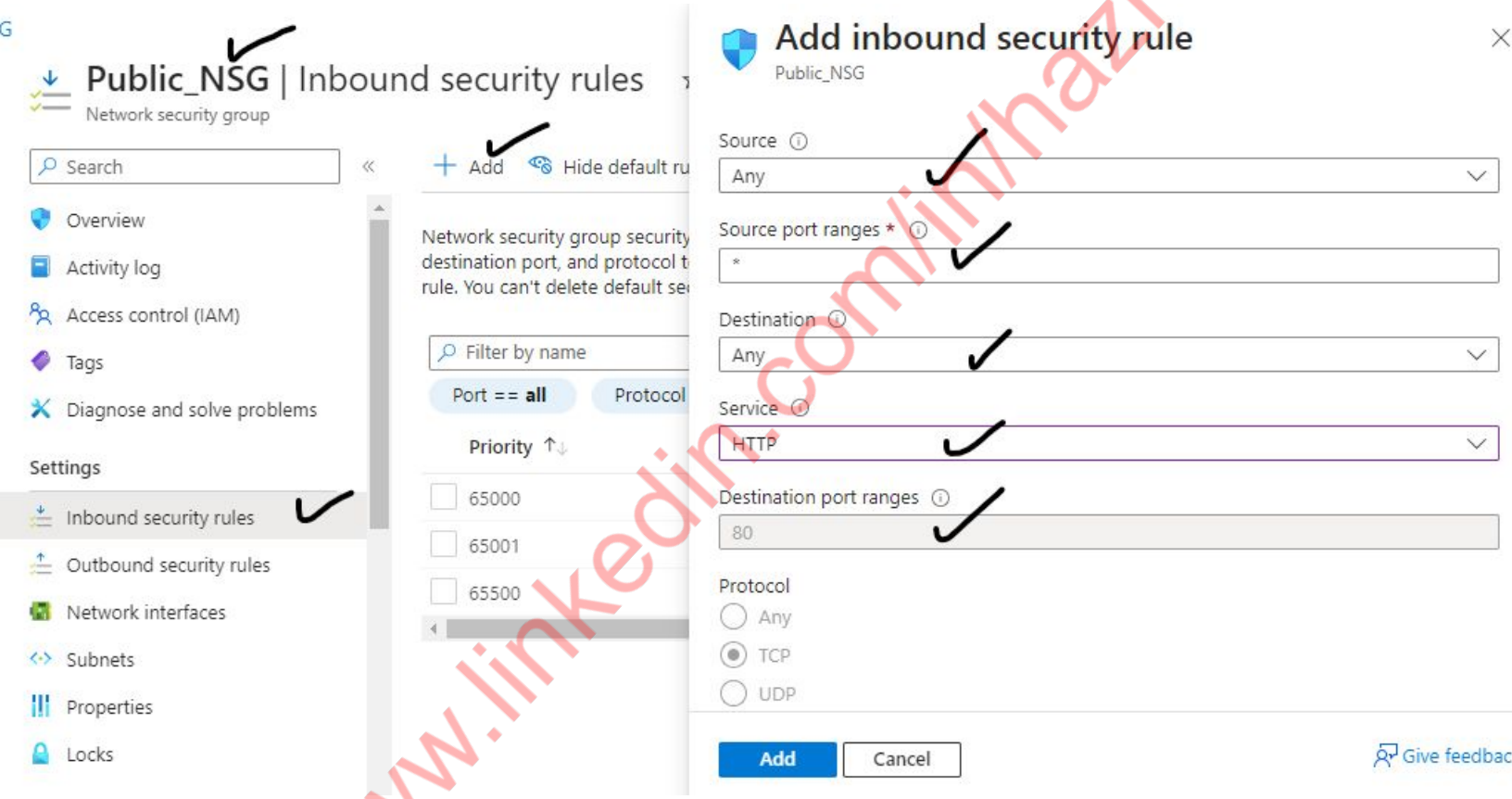
In this next section you will configure secure routing within your Virtual Network and subnets. Follow secure best practices when creating network traffic rules.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

2.3.1 Screenshot

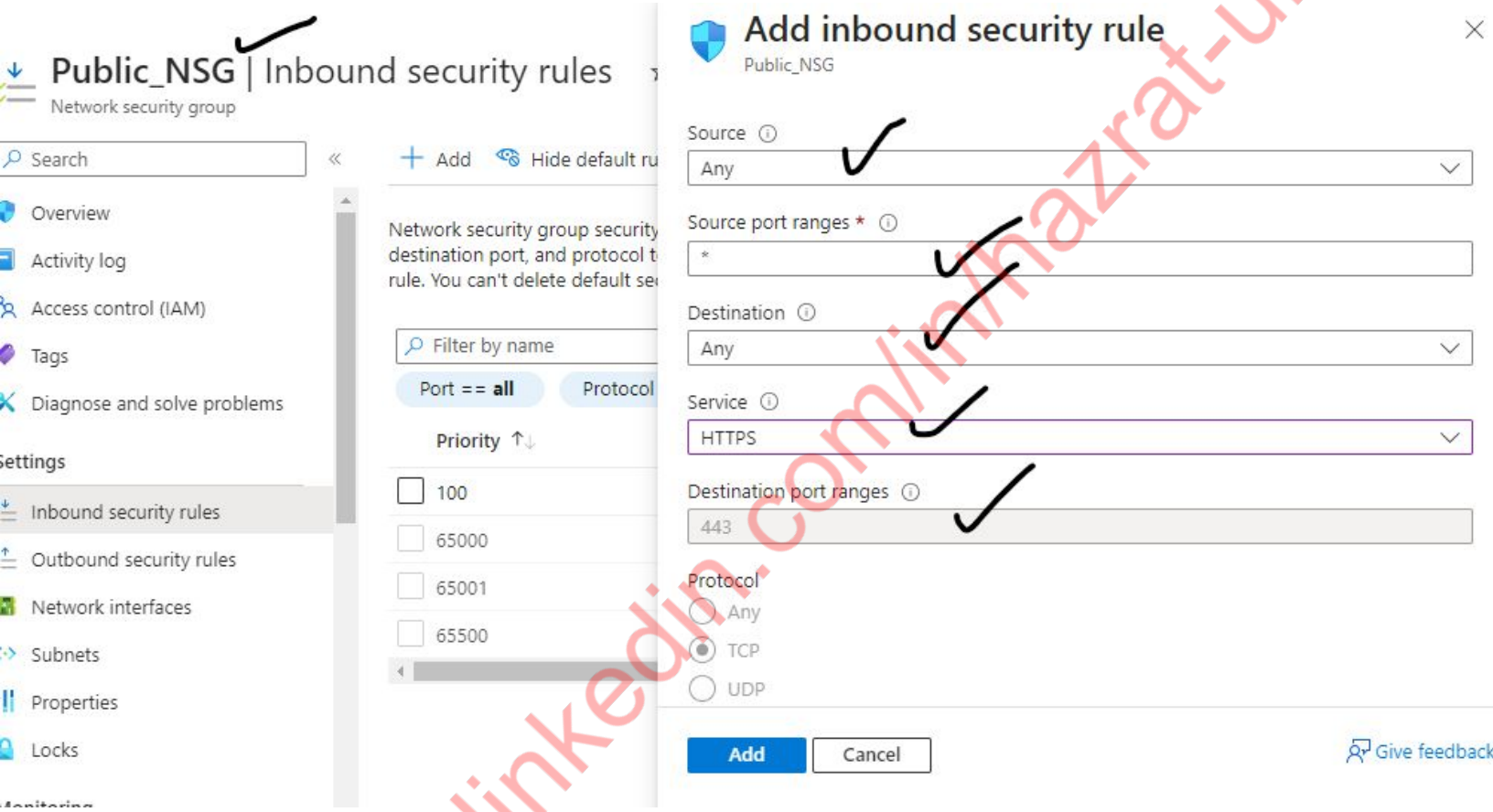
Traffic rules in your DMZ.

Allowing inbound HTTP for public DMZ



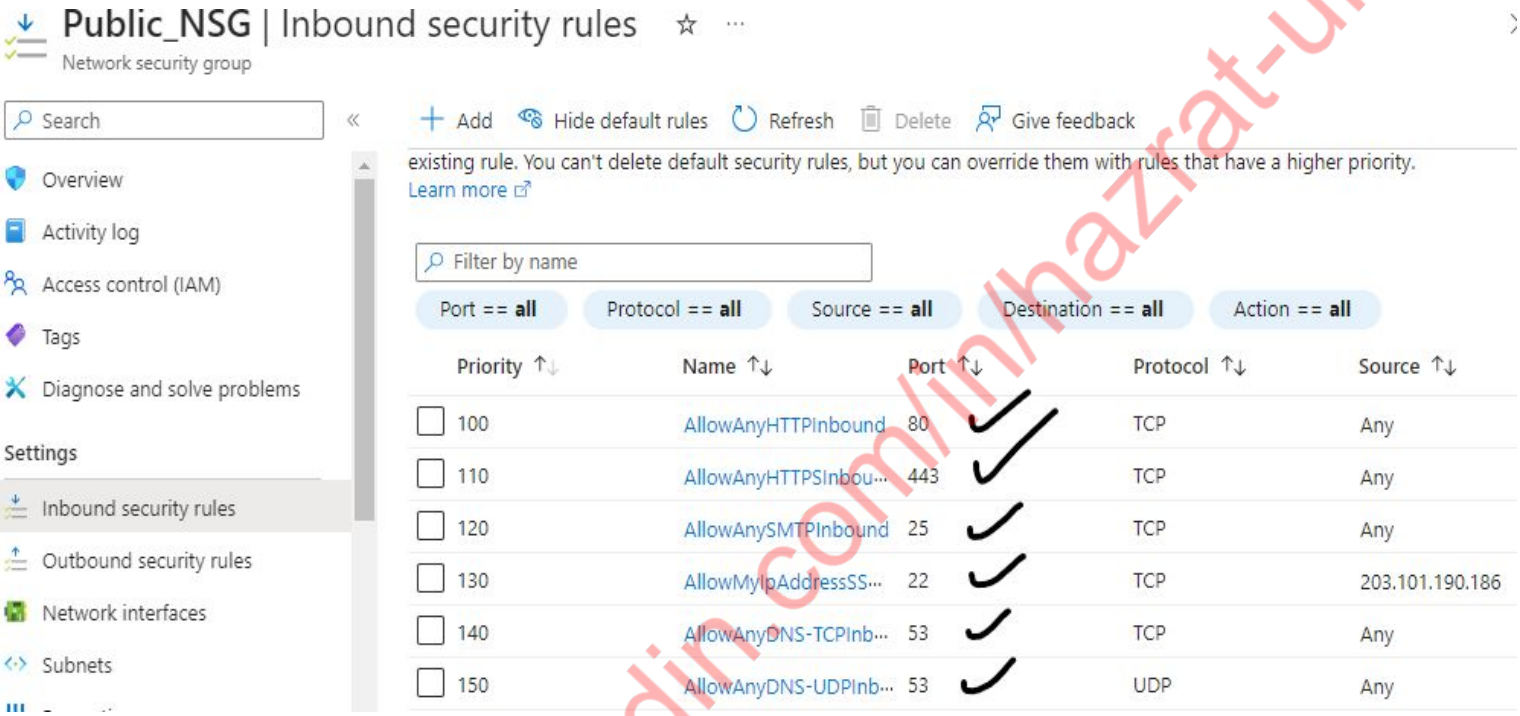
Priority	Name	Port	Protocol	Source
100	AllowAnyHTTPInbound	80	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any

Allowing inbound HTTPs Traffic for public DMZ



Priority	Name	Port	Protocol	Source
100	AllowAnyHTTPInbound	80	TCP	Any
110	AllowAnyHTTPSInbou...	443	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalan
65500	DenyAllInBound	Any	Any	Any

Created following inbound Rules for Public DMZ

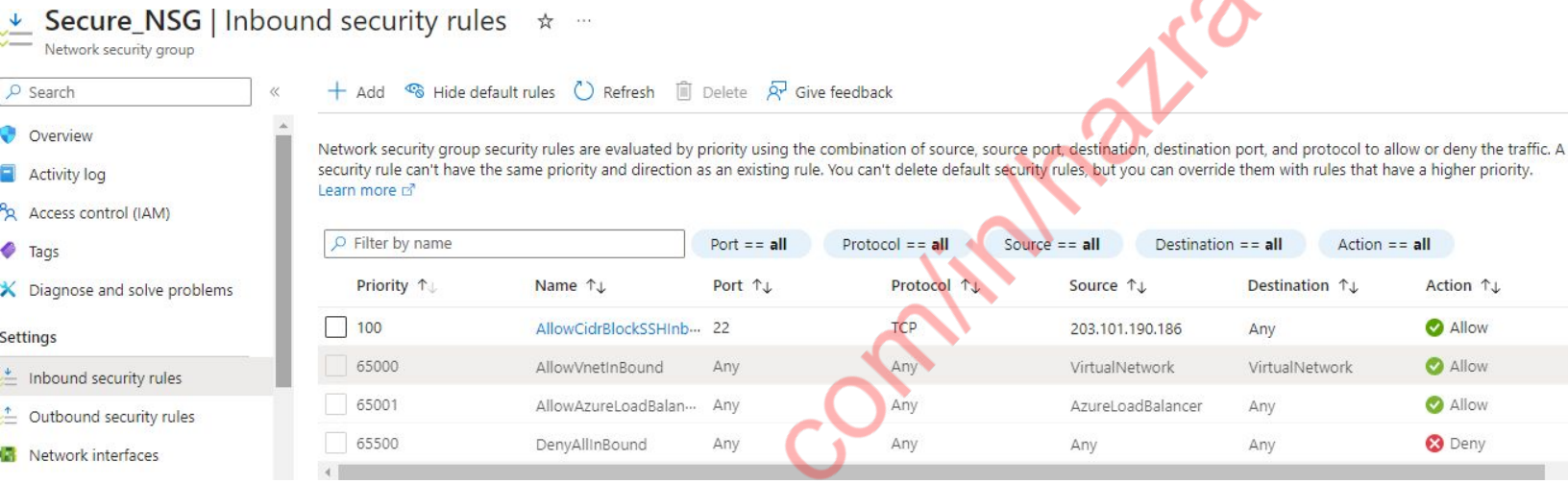


☐	100	AllowAnyHTTPInbound	80	TCP	Any
☐	110	AllowAnyHTTPSInbou...	443	TCP	Any
☐	120	AllowAnySMTPInbound	25	TCP	Any
☐	130	AllowMyIpAddressSS...	22	TCP	203.101.190.186
☐	140	AllowAnyDNS-TCPInb...	53	TCP	Any
☐	150	AllowAnyDNS-UDPInb...	53	UDP	Any
☐	65000	AllowVnetInBound	Any	Any	VirtualNetwork
☐	65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalance
☐	65500	DenyAllInBound	Any	Any	Any

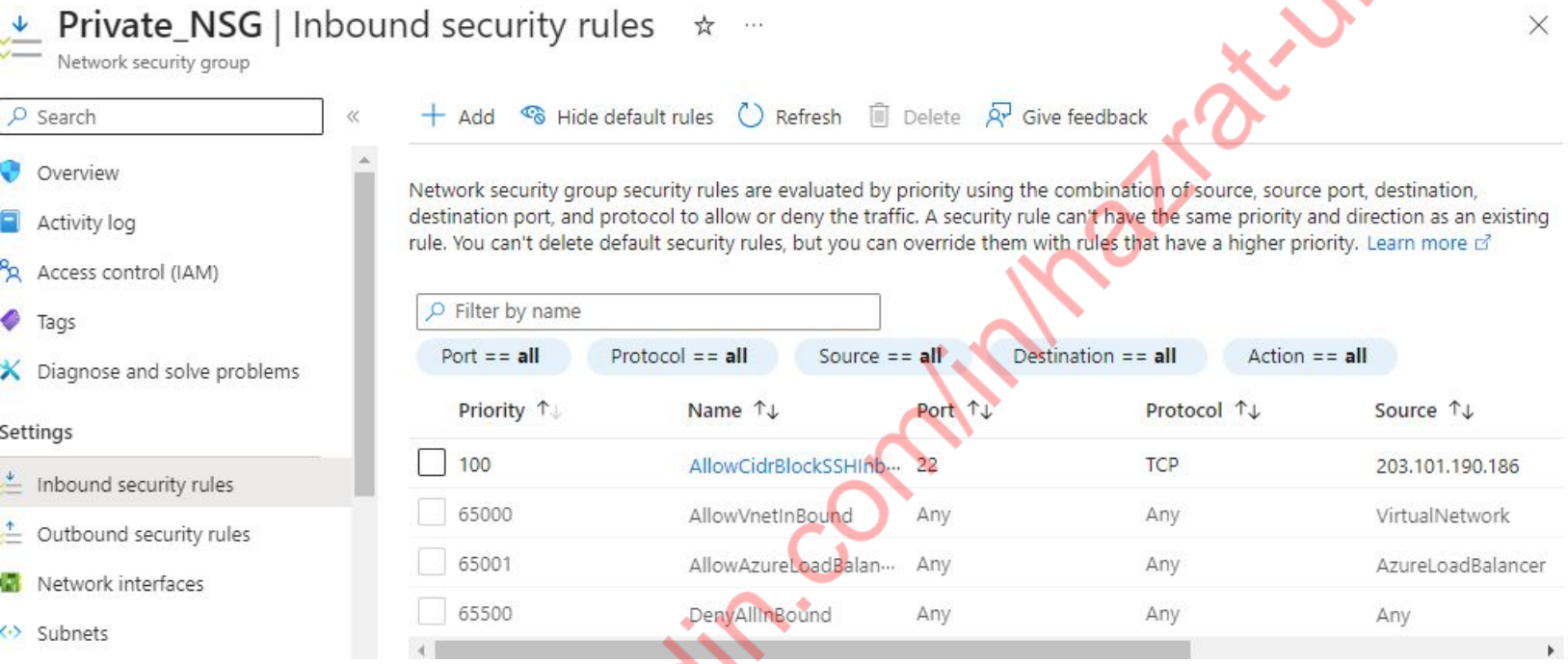
2.3.2 Screenshot

Traffic rules in your Internal network.

Secure NSG

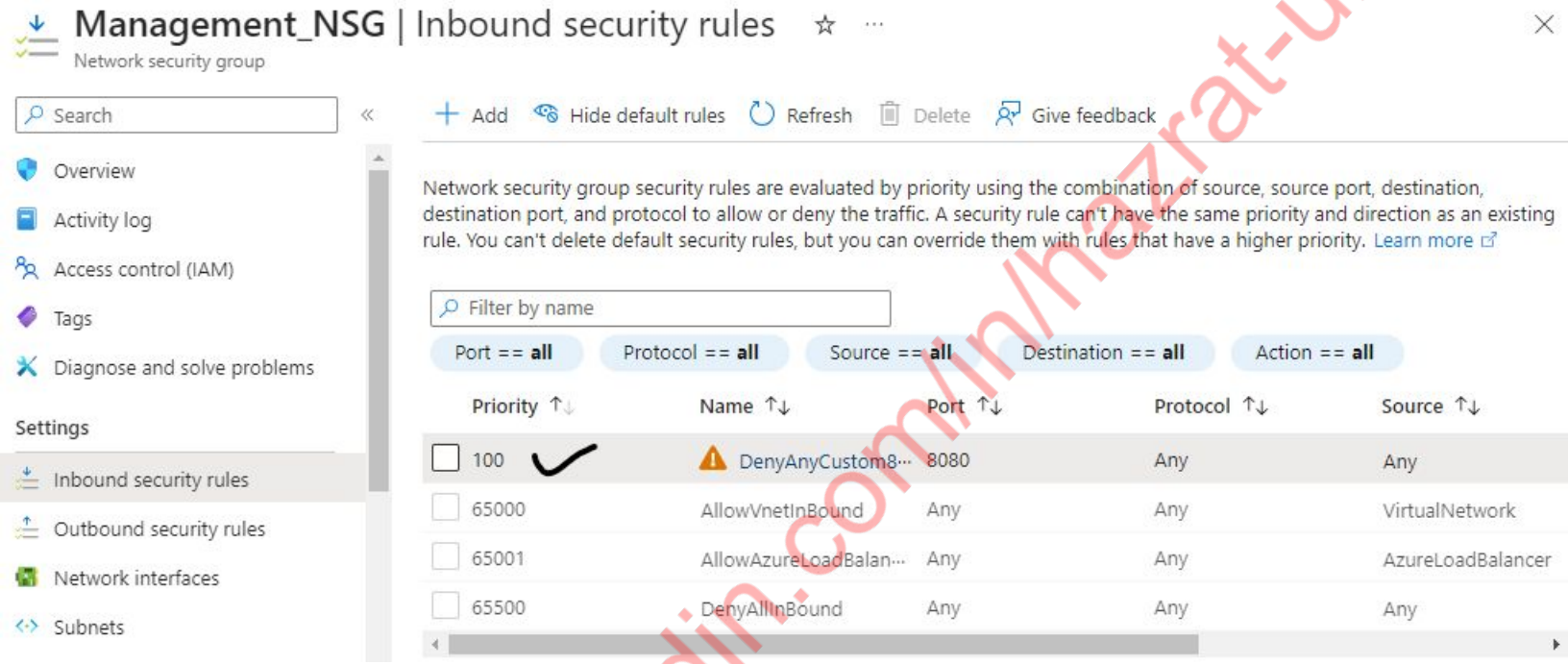


Private NSG Rules



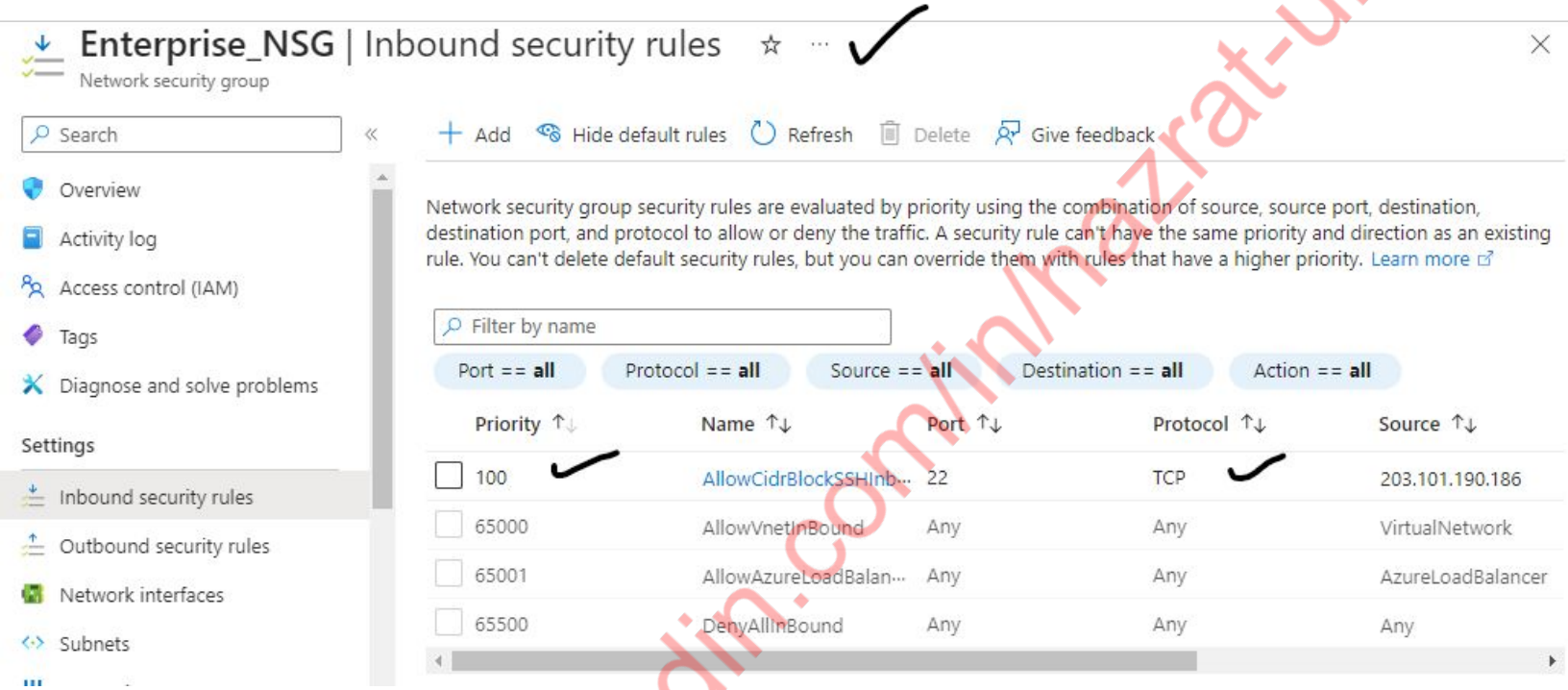
100	AllowCidrBlockSSHInb···	22	TCP	203.101.190.186
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any

Management NSG Inbound Rules



☐	100	DenyAnyCustom8···	8080	Any	Any
☐	65000	AllowVnetInBound	Any	Any	VirtualNetwork
☐	65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer
☐	65500	DenyAllInBound	Any	Any	Any

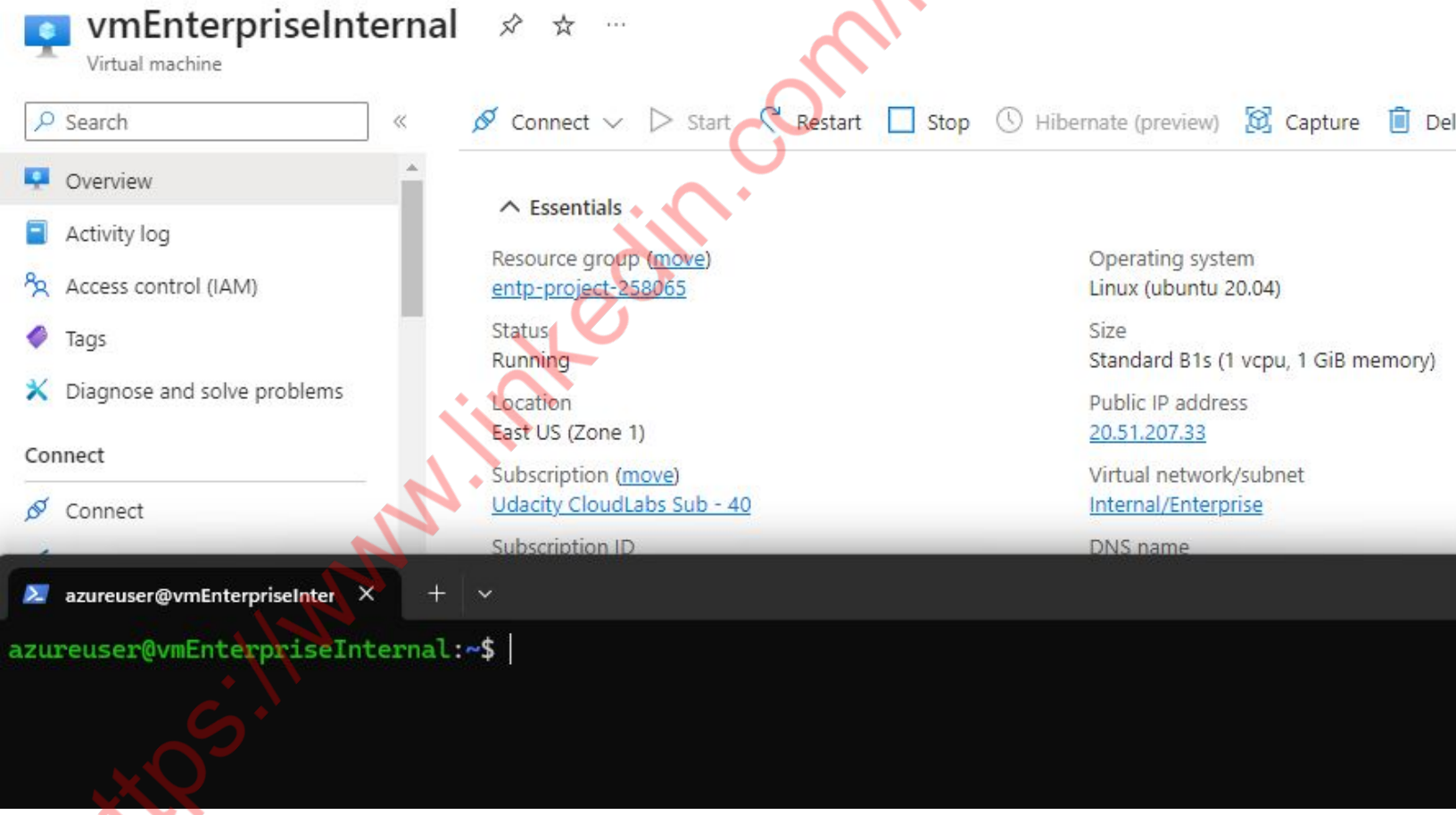
Enterprise NSG Inbound Rules



☐	100	AllowCidrBlockSSHInb···	22	TCP	203.101.190.186
☐	65000	AllowVnetInBound	Any	Any	VirtualNetwork
☐	65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer
☐	65500	DenyAllInBound	Any	Any	Any

Testing the inbound Rule and Accessing our Internal VM from my Laptop

SSHed from my Laptop and it works



2.4 VPN Access

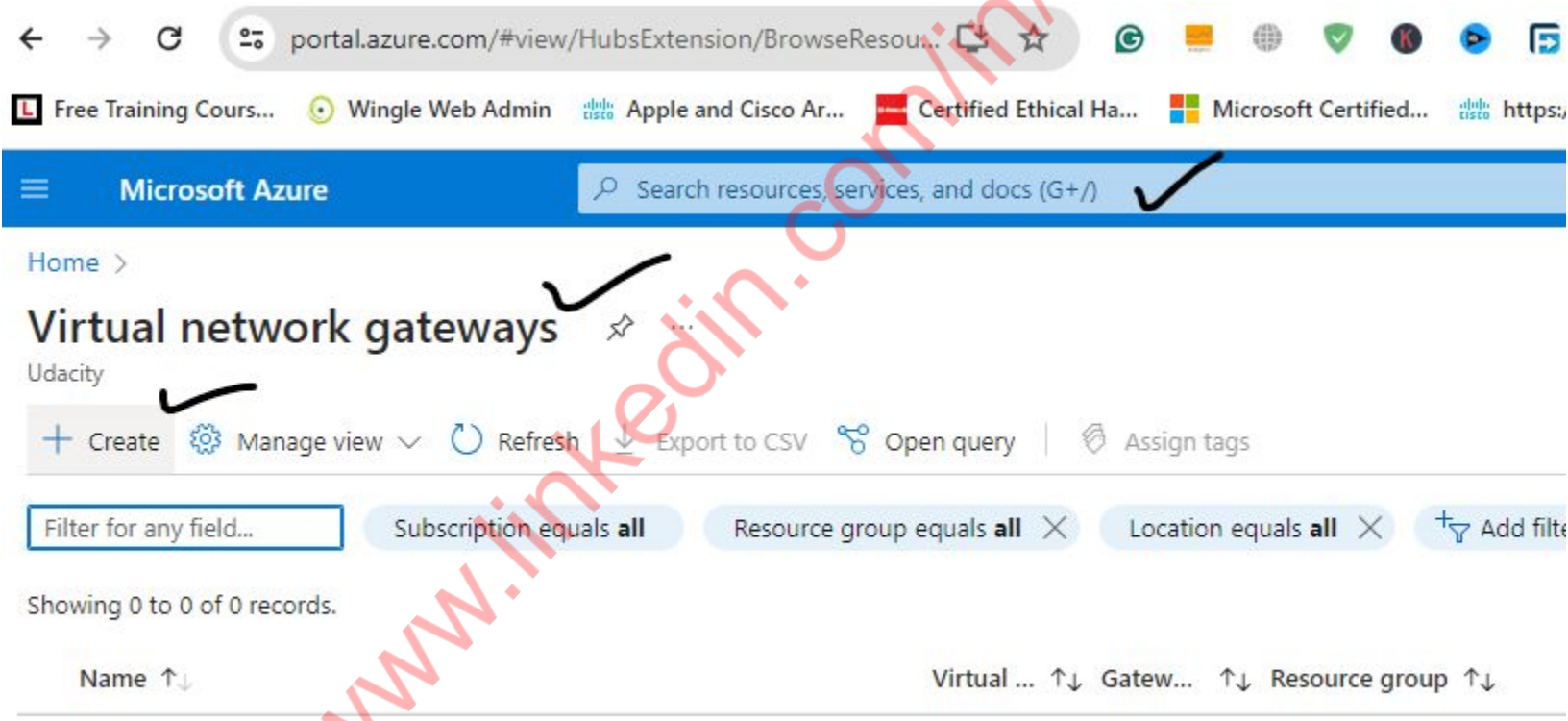
In this next section you will create a VPN to secure access to your internal network. After creating your VPN, test your VPN connection and attempt connecting to one of your VMs in your internal network.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

2.4.1 Screenshot

Create a VPN to connect to your internal network.

First Searching for Virtual Gateways in Azure portal and clicking on Create



Create virtual network gateway

Subscription * Udacity CloudLabs Sub - 40

Resource group entp-project-258065 (derived from virtual network's resource group)

Instance details

Name * Enterprise_VPN

Region * East US

Deploy to an edge zone

Gateway type * VPN ExpressRoute

SKU * VpnGw1

Generation Generation1

Virtual network * Internal

Create virtual network

Virtual network * ⓘ

Internal

Create virtual network

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range * ⓘ

10.0.4.0/24

10.0.4.0 - 10.0.4.255 (256 addresses)

Public IP address

Public IP address * ⓘ

(•) Create new ( ) Use existing

Public IP address name *

Public IP address SKU

Standard

Assignment

( ) Dynamic (•) Static

Enable active-active mode * ⓘ

(•) Enabled ( ) Disabled

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

Public IP address * ⓘ Create new Use existing

Public IP address name * EnterpriseVPNIp

Public IP address SKU Standard

Assignment Dynamic Static

Enable active-active mode * ⓘ Enabled Disabled

SECOND PUBLIC IP ADDRESS

SECOND PUBLIC IP ADDRESS * ⓘ Create new Use existing

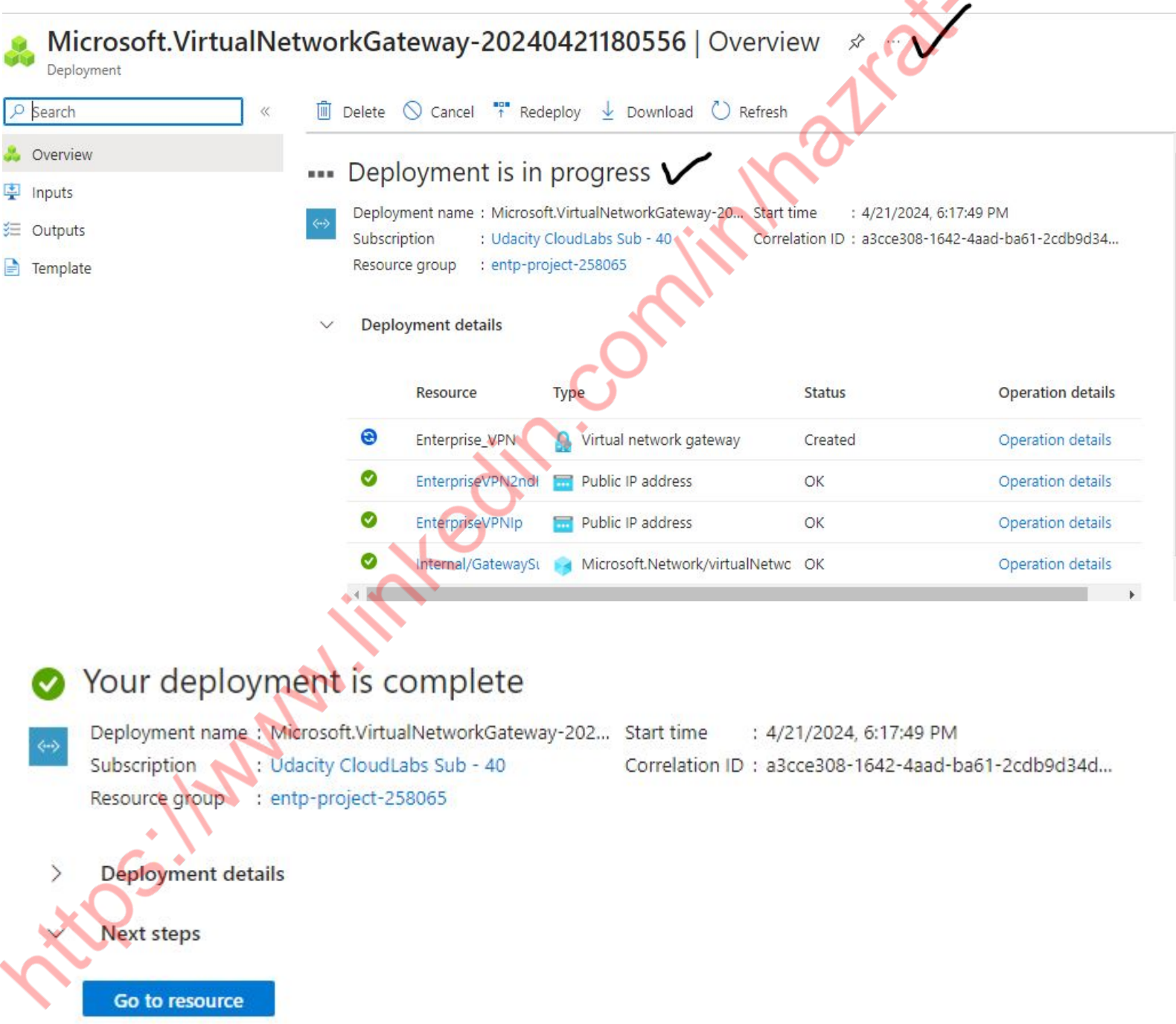
Public IP address name * EnterpriseVPN2ndIP

Configure BGP * ⓘ Enabled Disabled

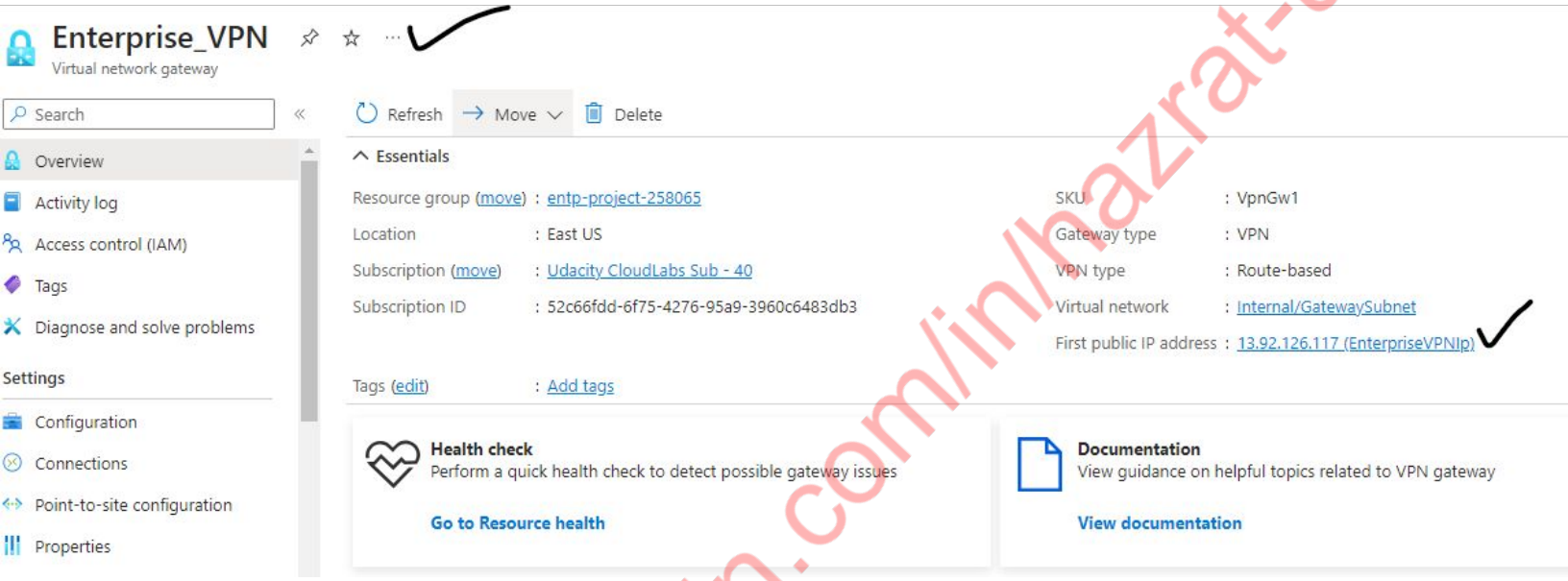
Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

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

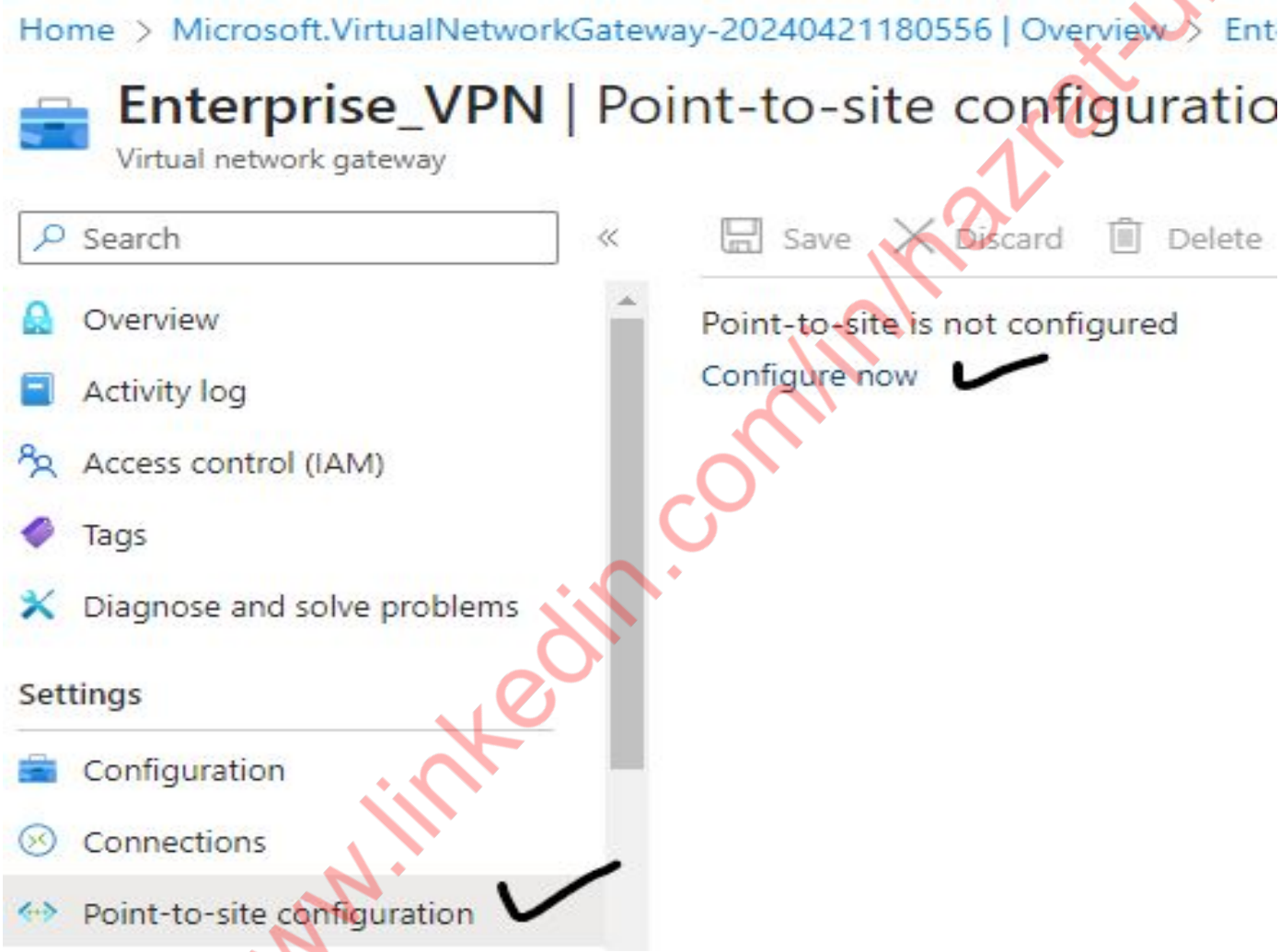
Waiting for its deployment

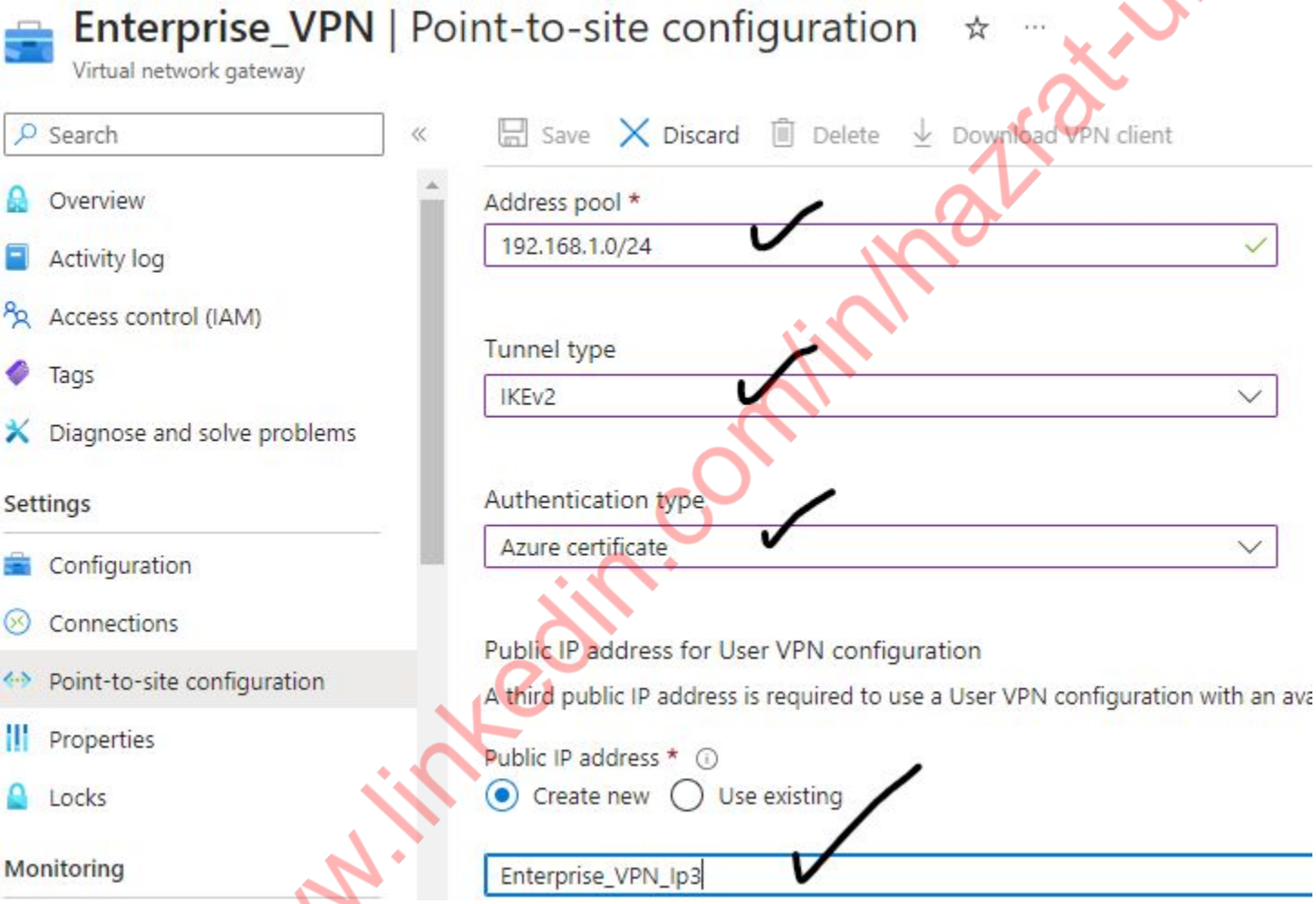


VPN deployed

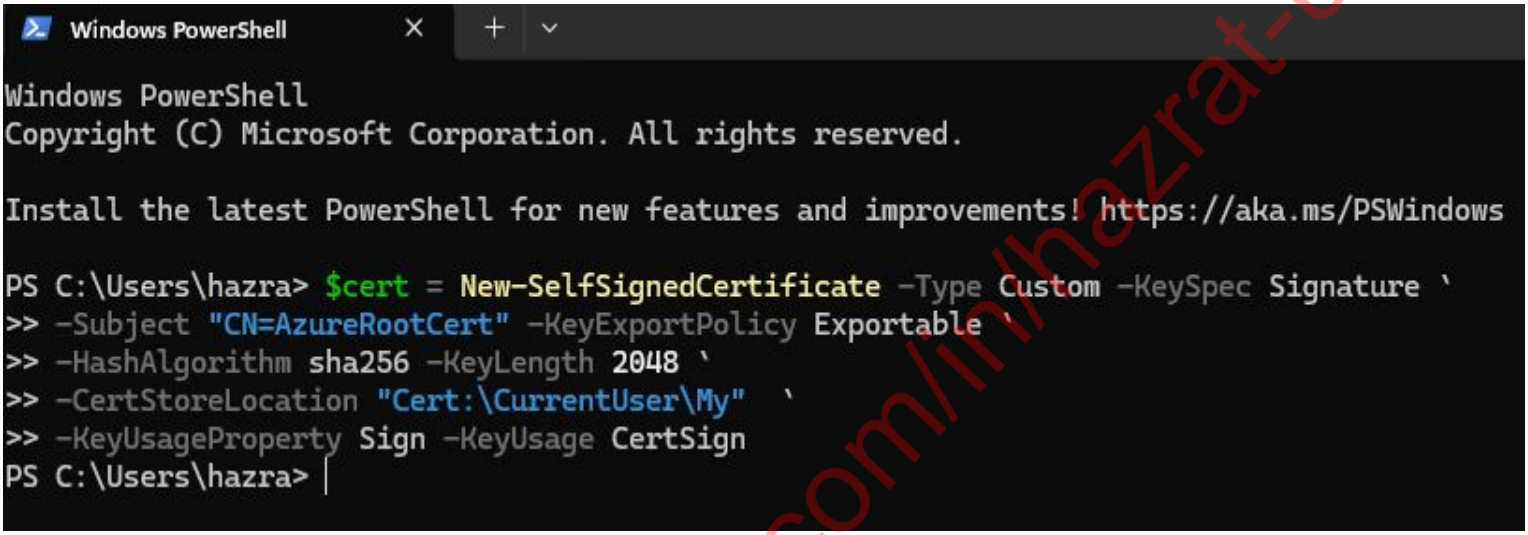


Point to Site Configuration





Creating Azure Root Cert



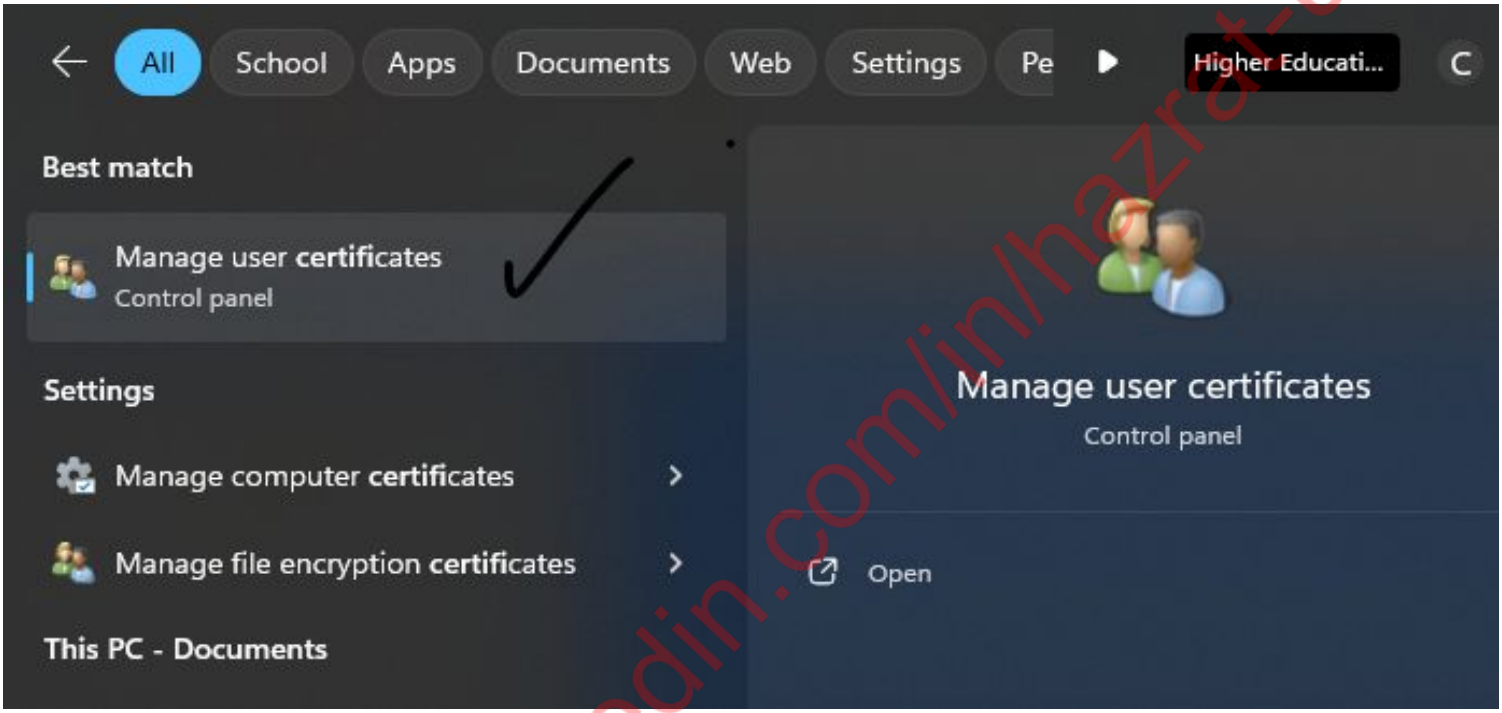

```
#Create the root cert
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=AzureRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My"  `
-KeyUsageProperty Sign -KeyUsage CertSign
```

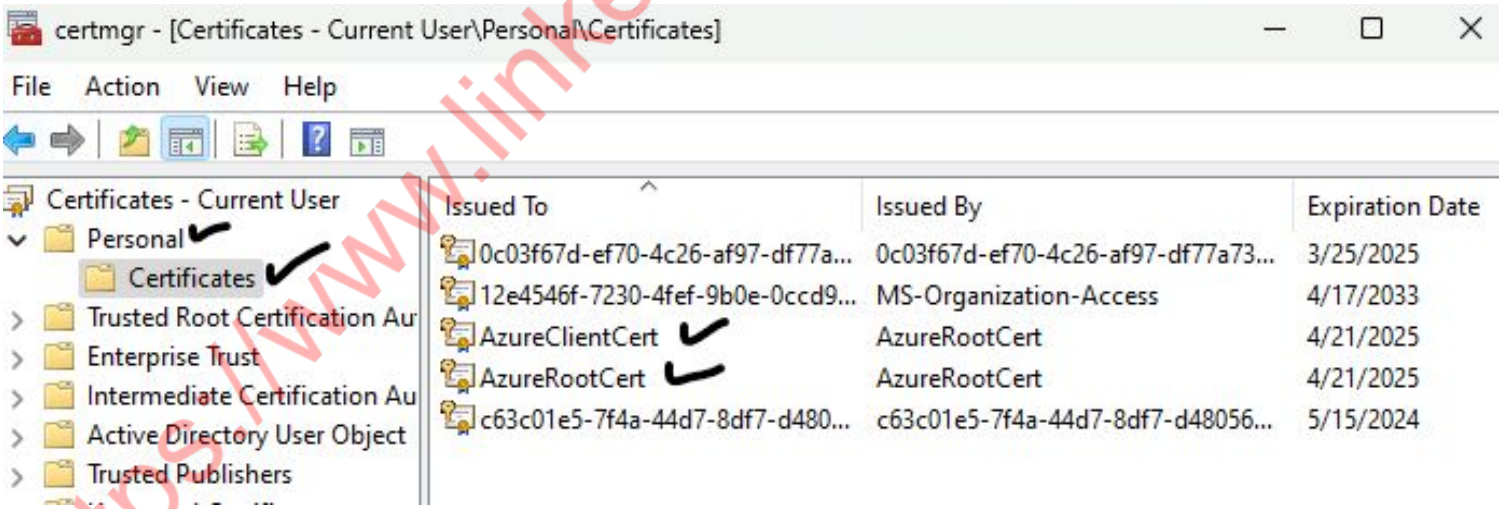
Creating Azure Client Cert

```
PS C:\Users\hazra>  # Create Client Cert
PS C:\Users\hazra> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
>> -Subject "CN=AzureClientCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" `
>> -Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
99BB155C1EB68B7831023BC43C757FE0EA845B47  CN=AzureClientCert
```

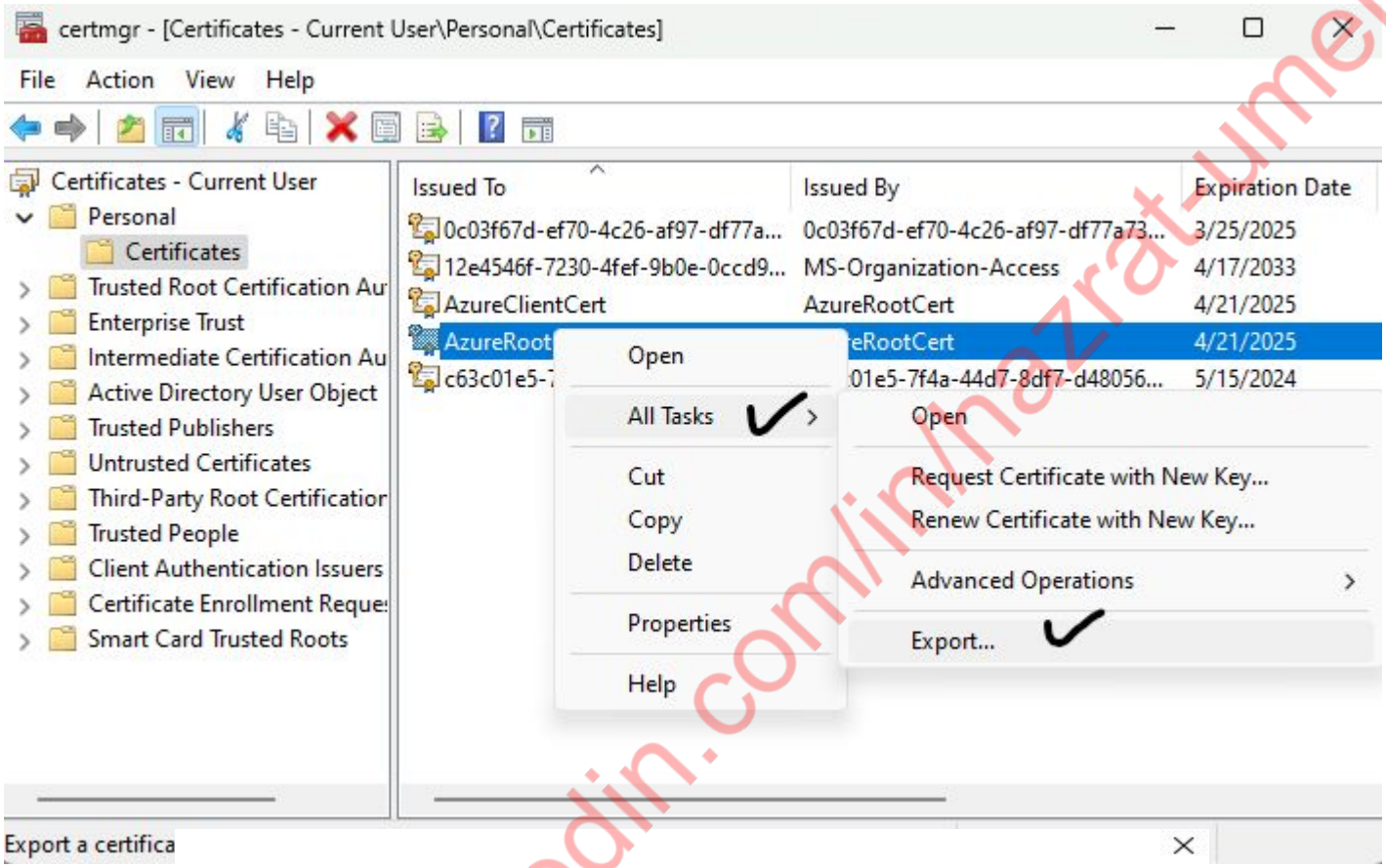
```
# Create Client Cert
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec
Signature `
-Subject "CN=AzureClientCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

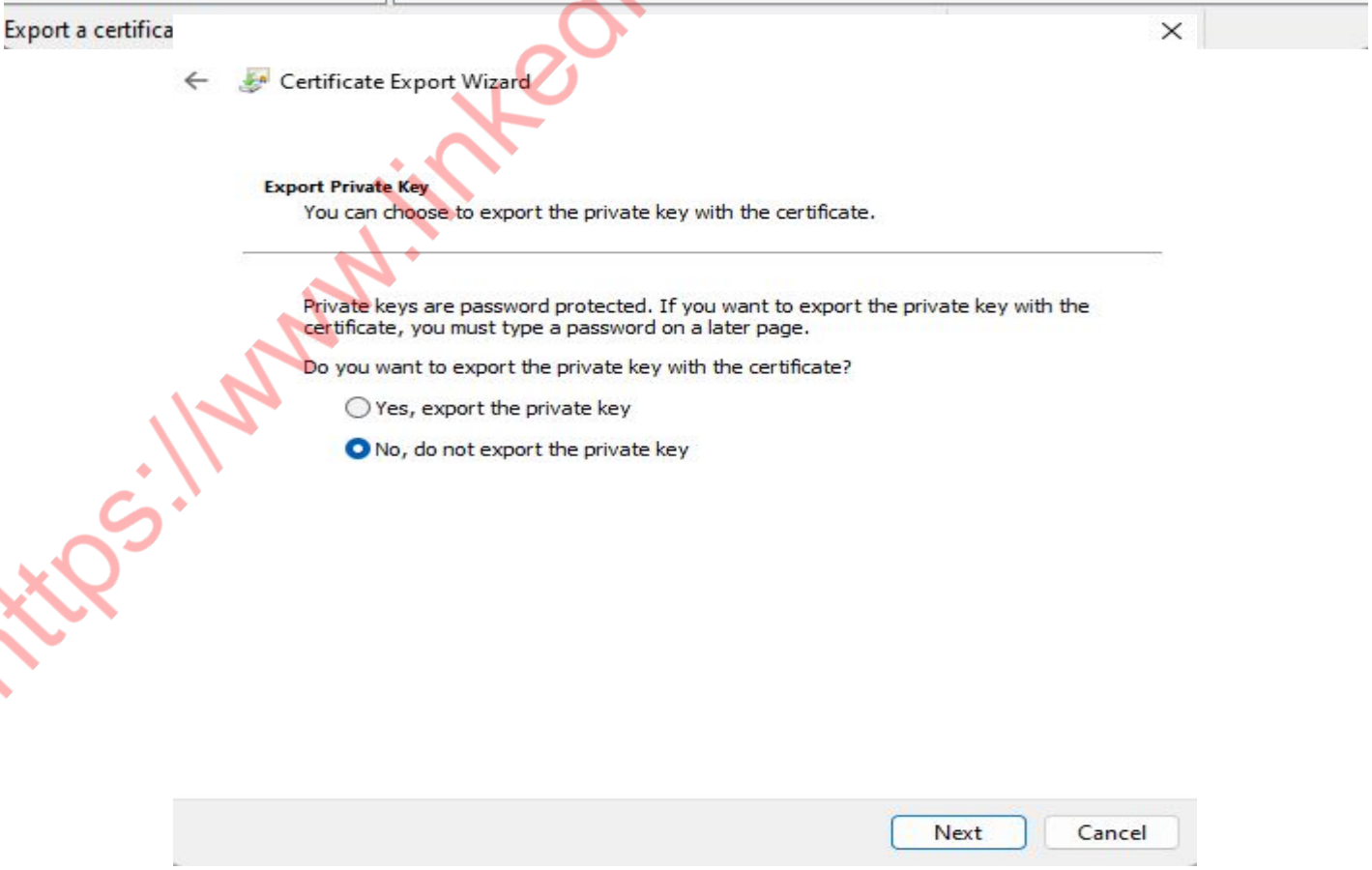
Accessing The created certificates

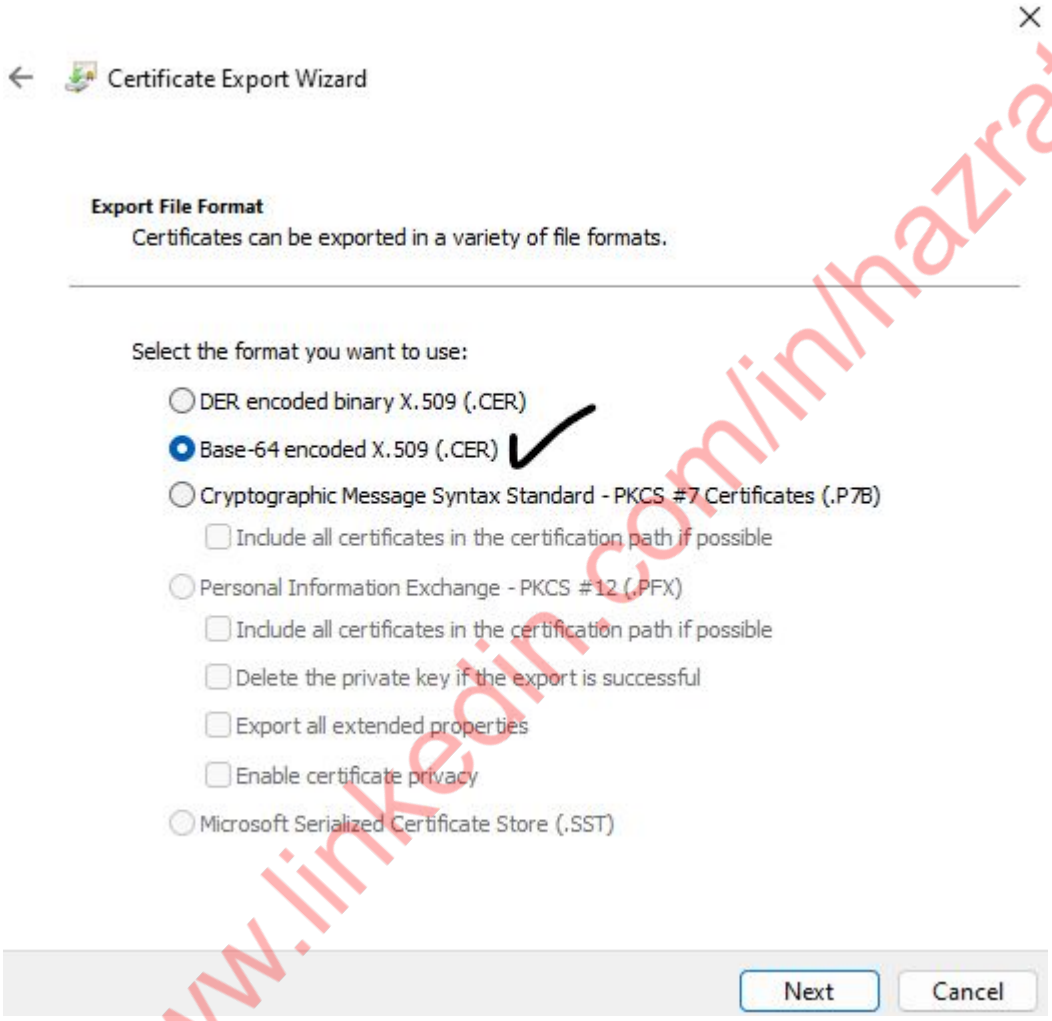


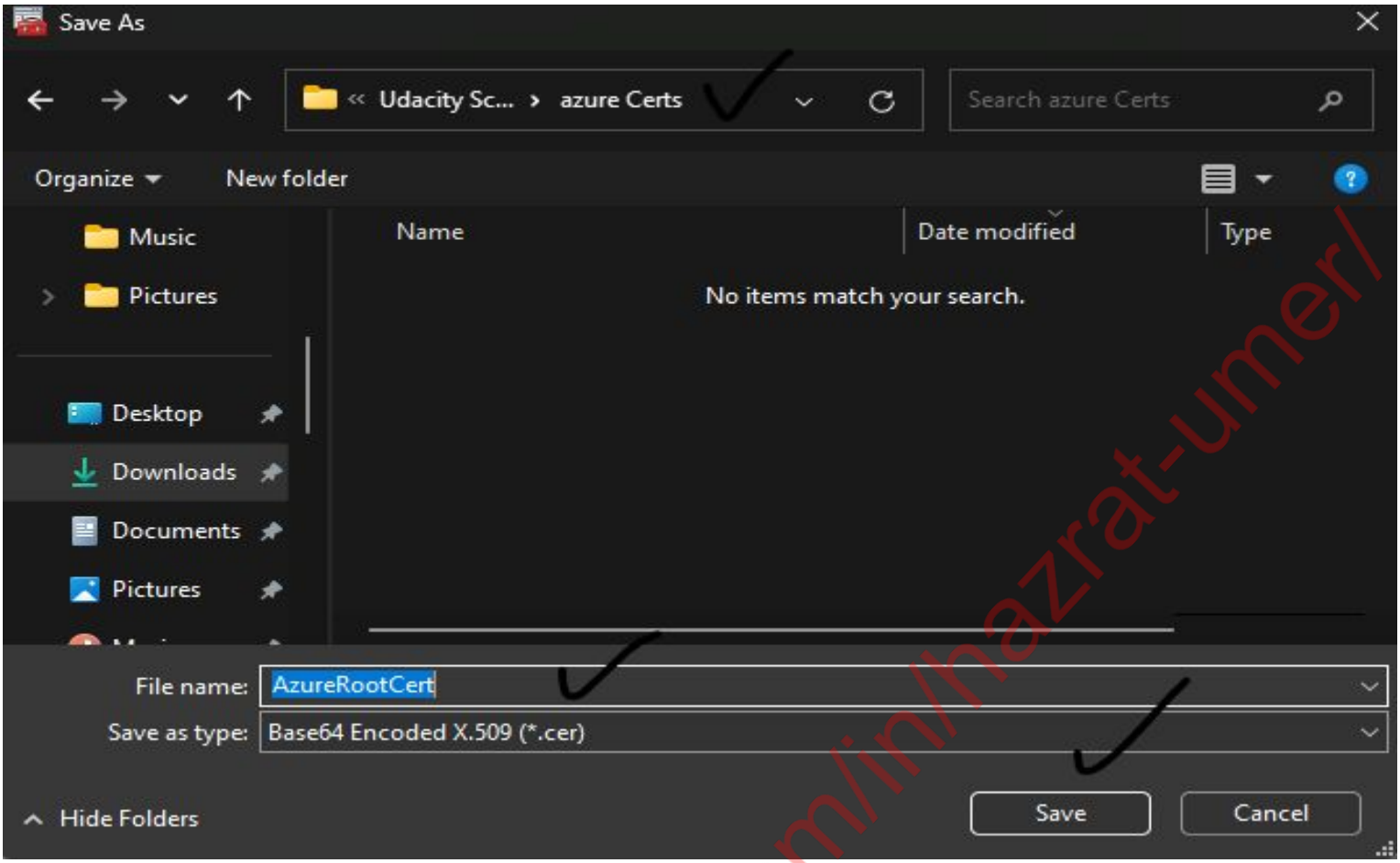


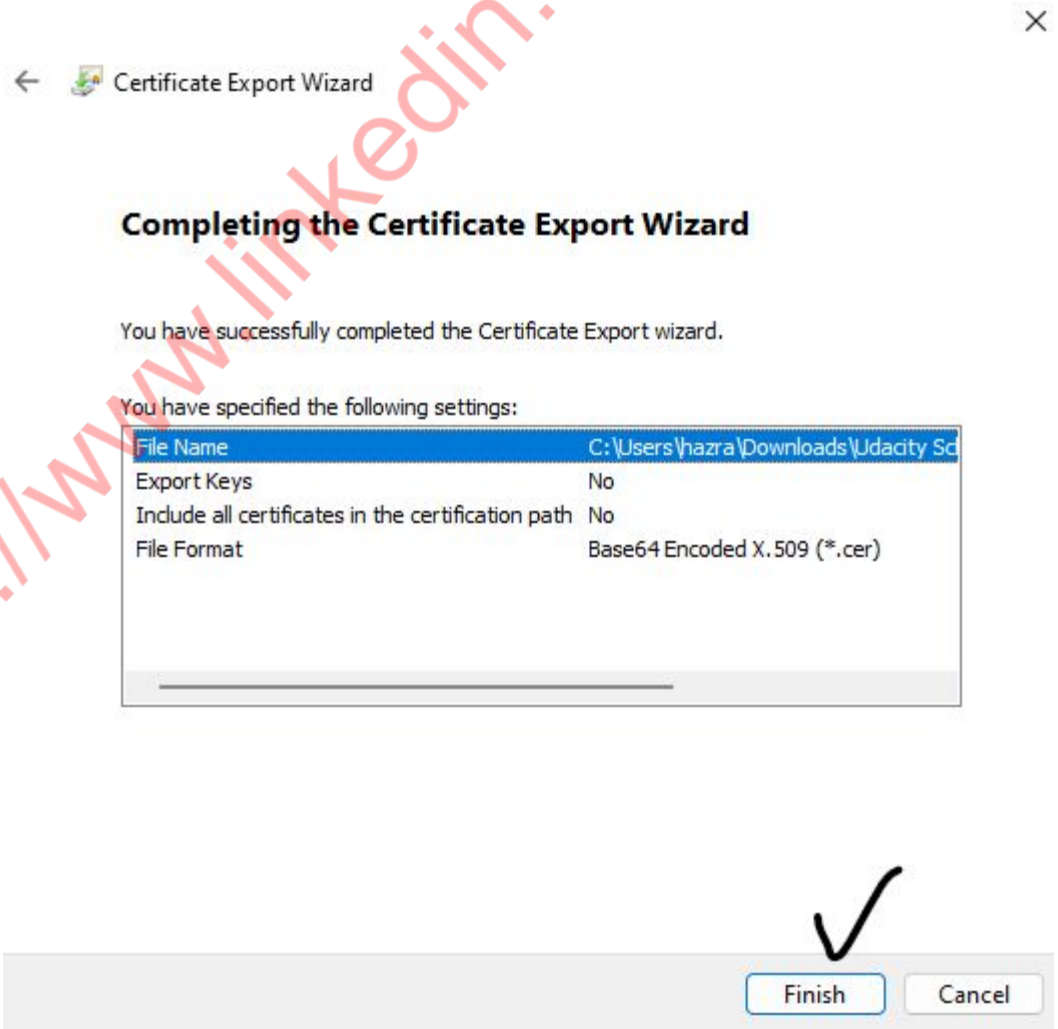
Exporting the root cert

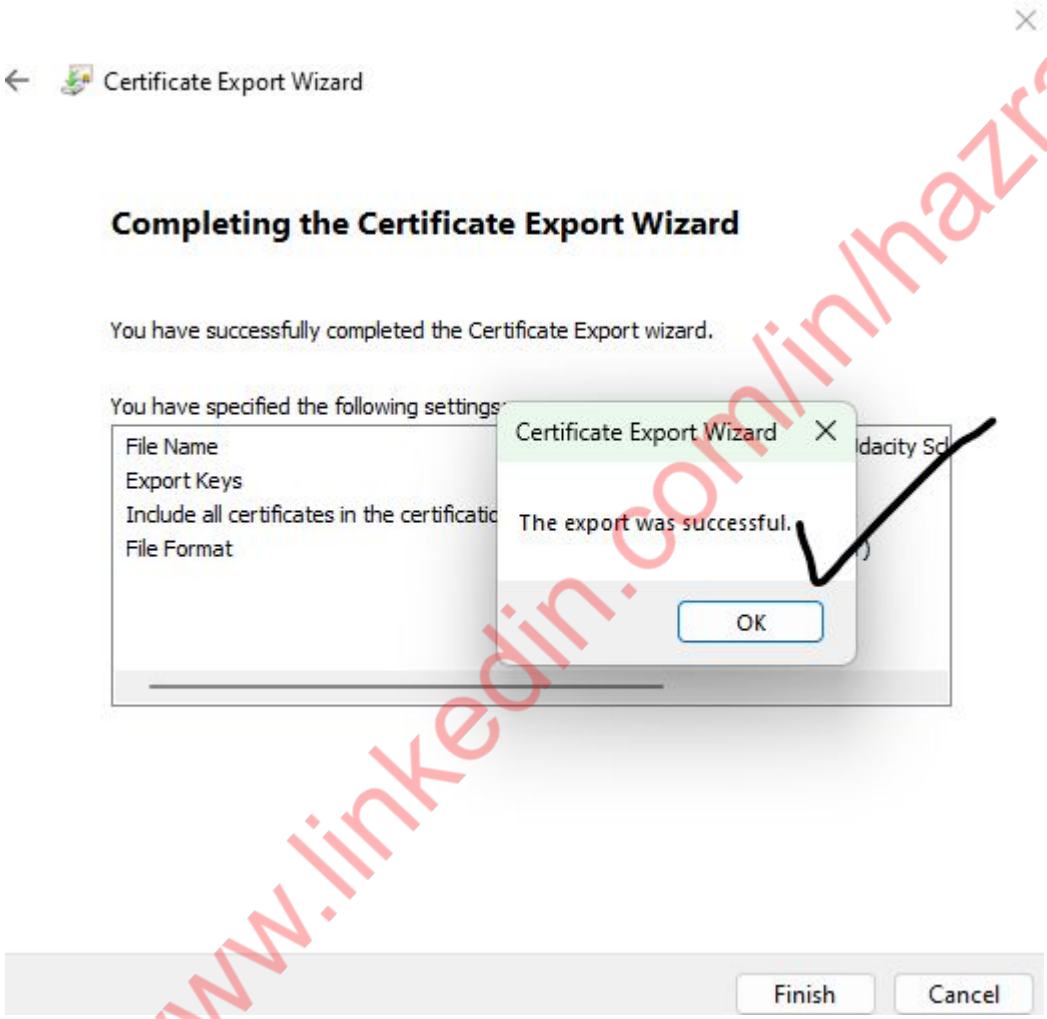






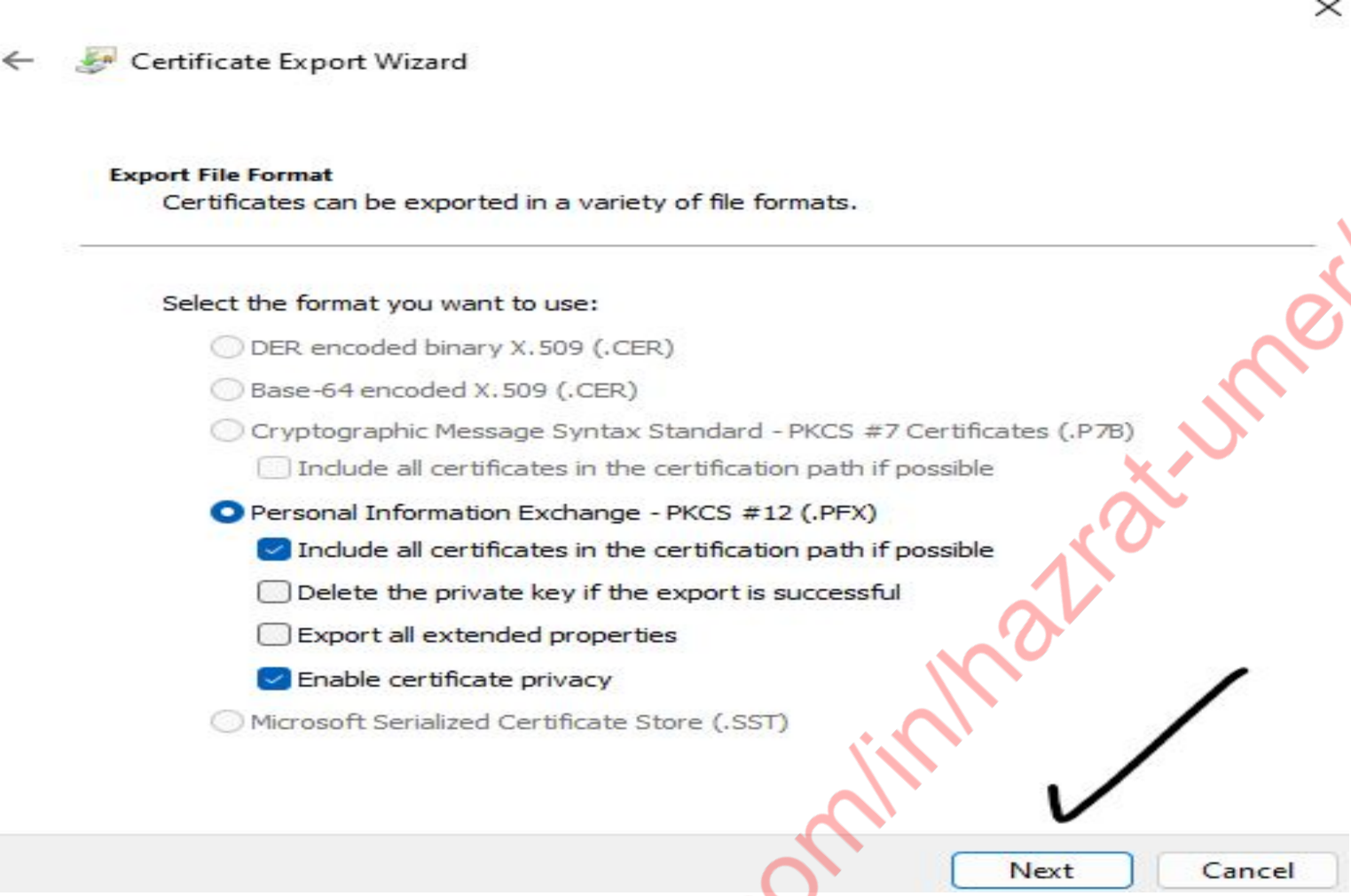


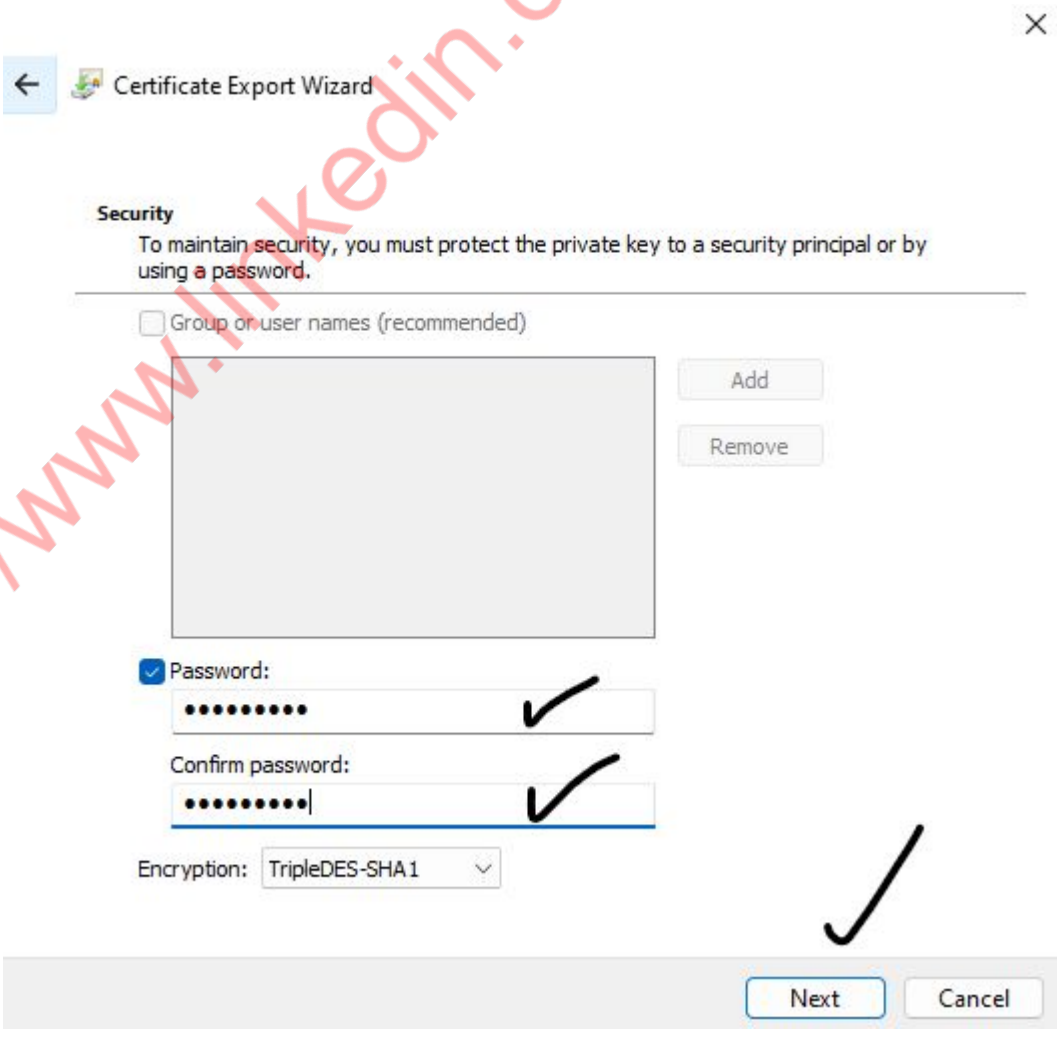


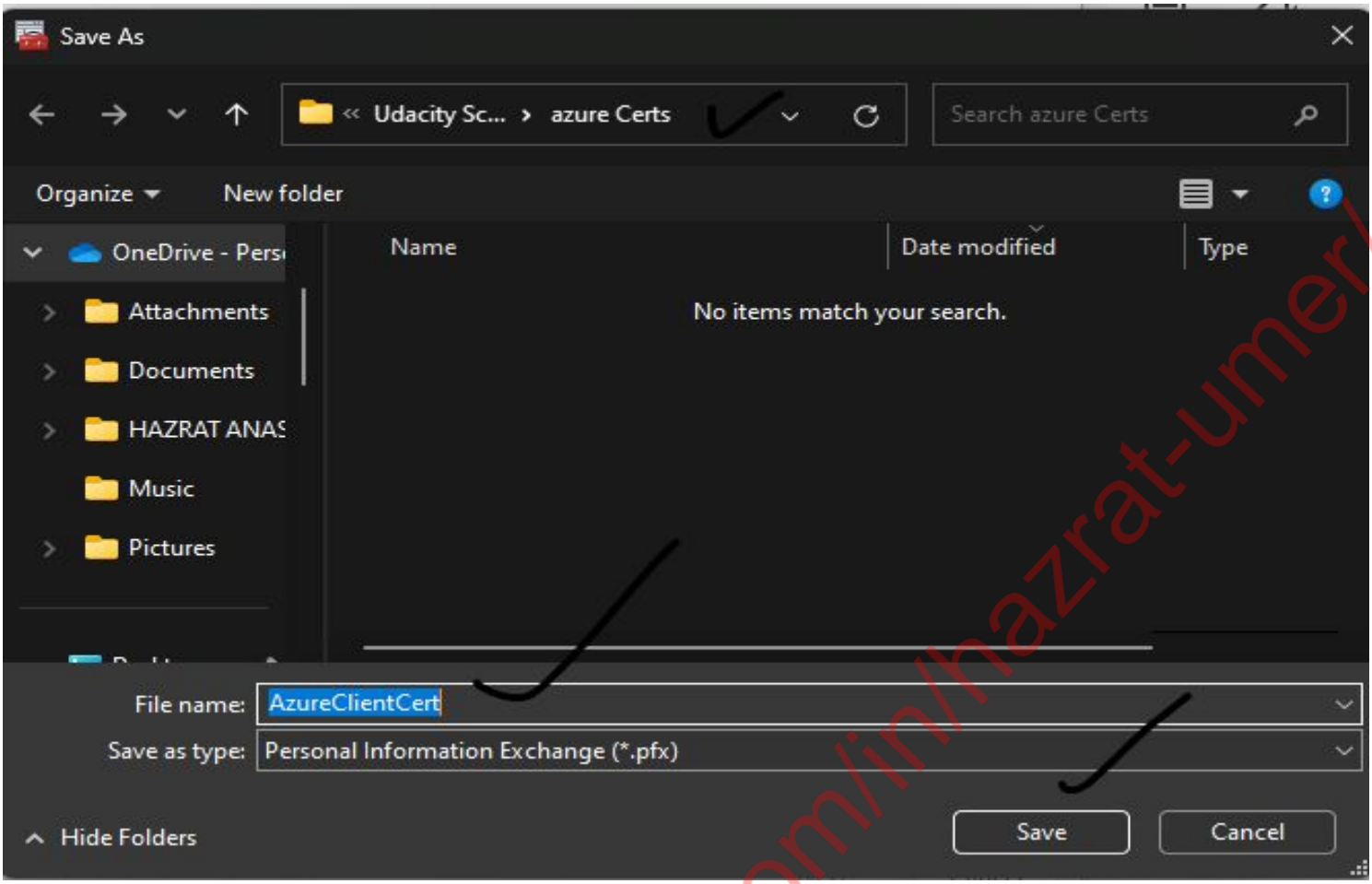


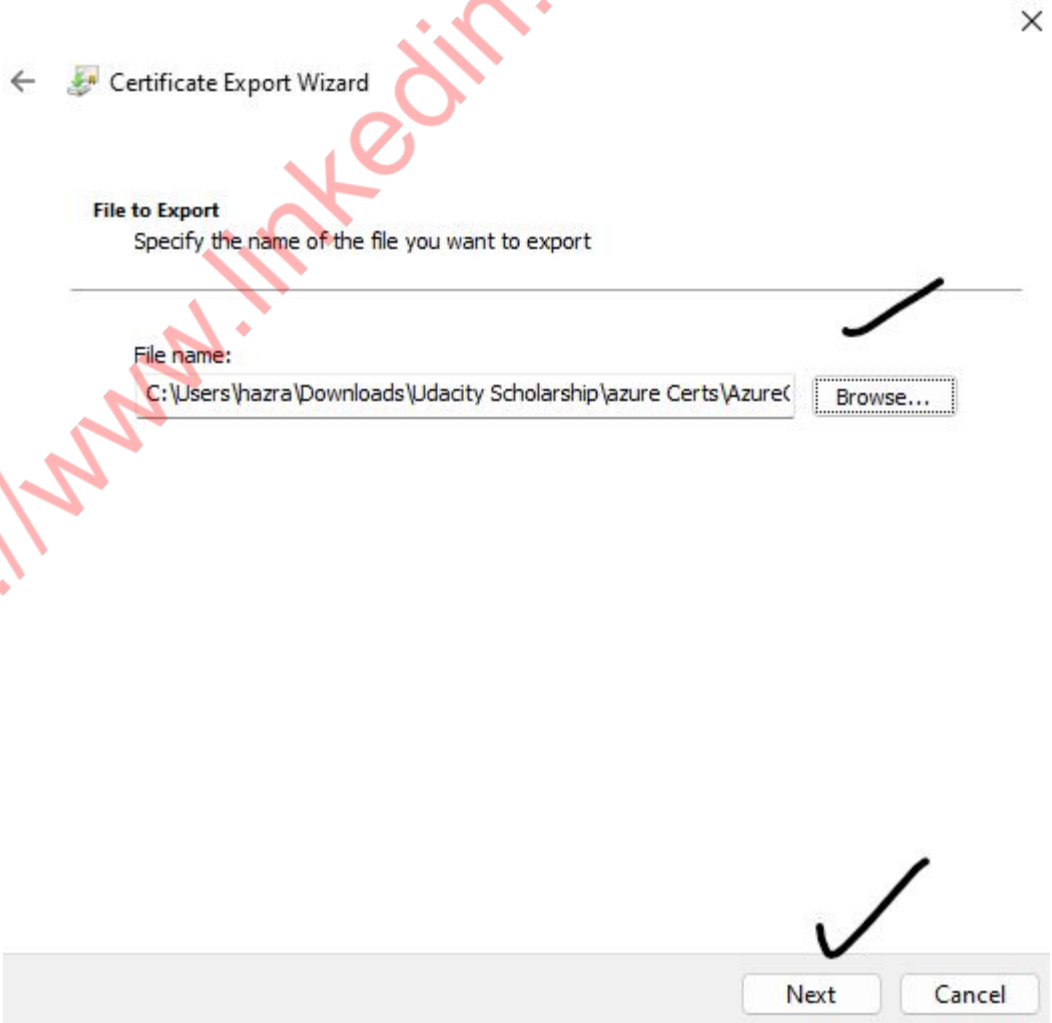
Exporting the Client Cert

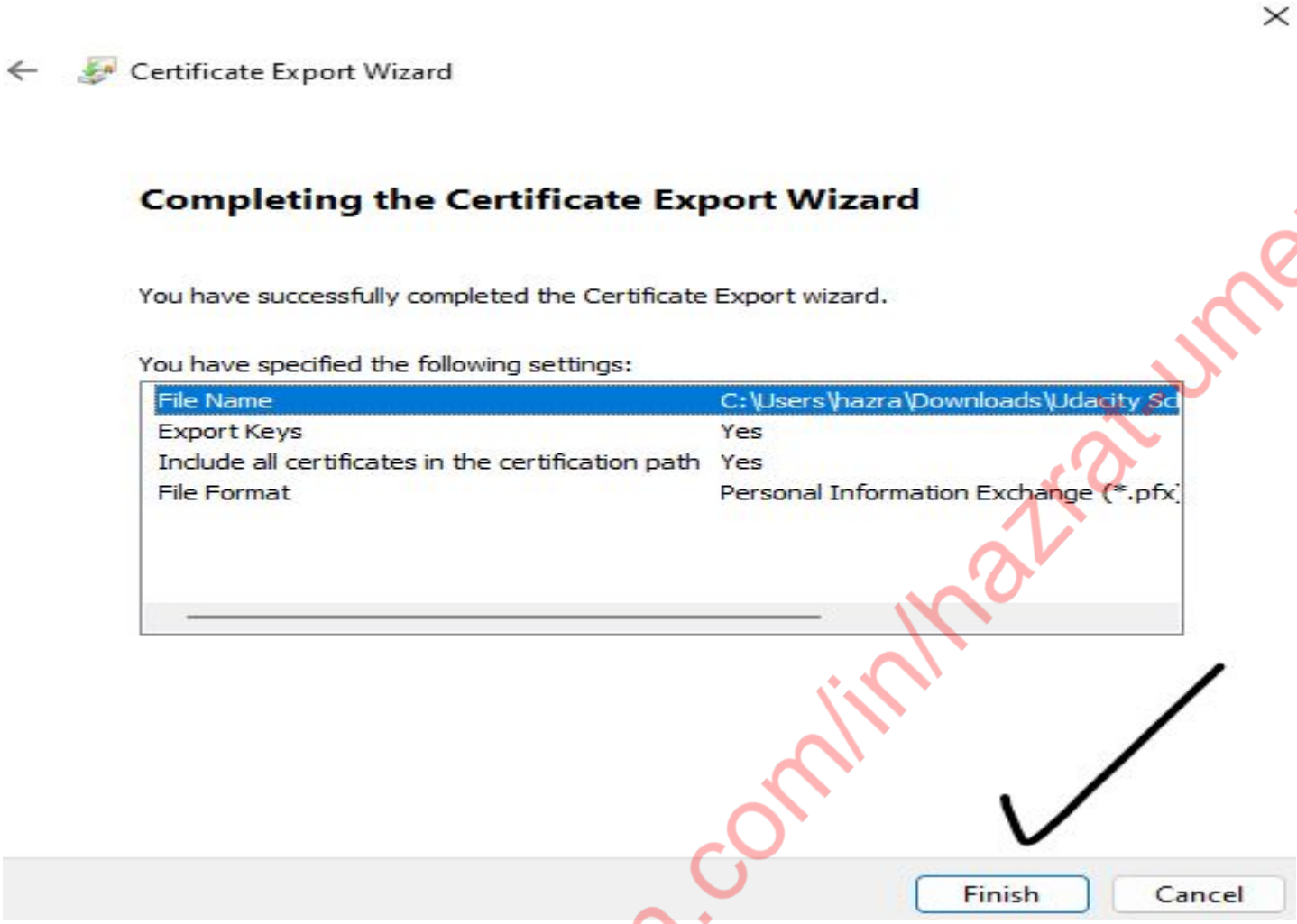
Doing the same process for the Client cert but here we are exporting the private key.

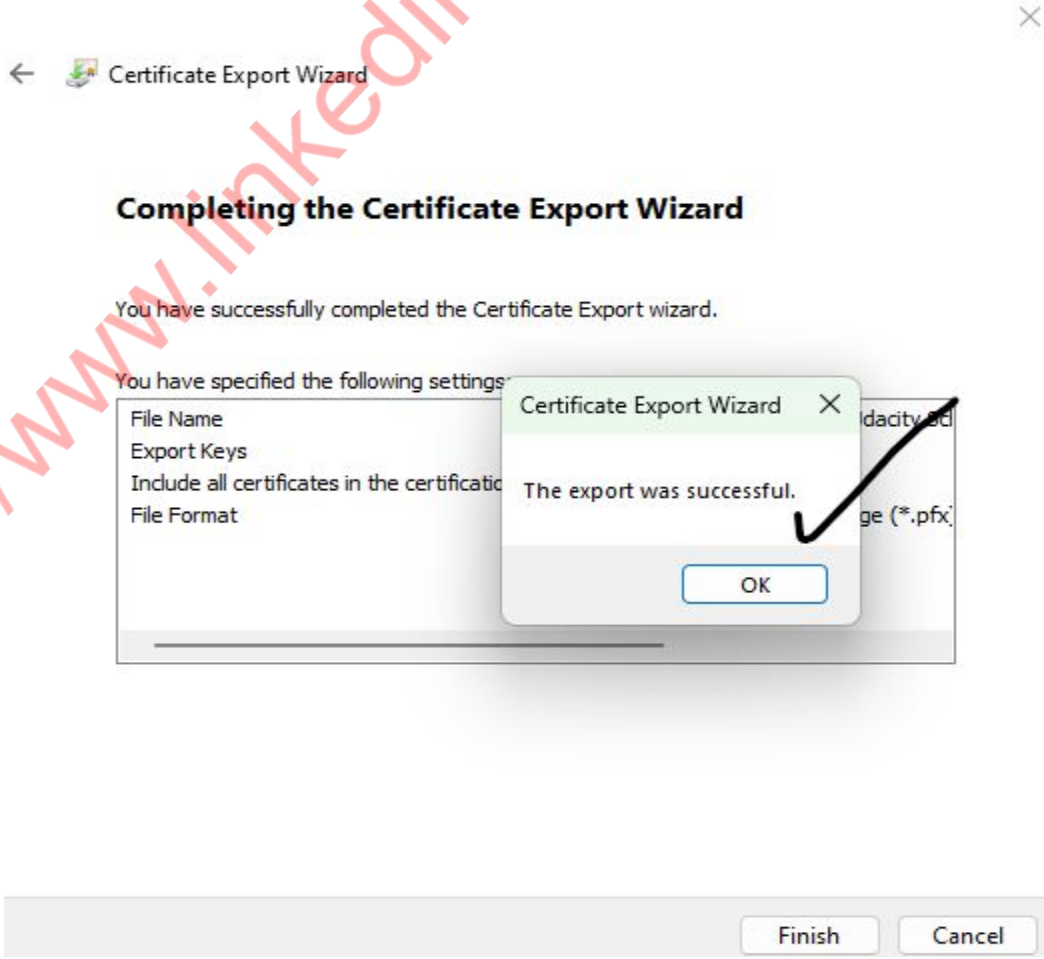




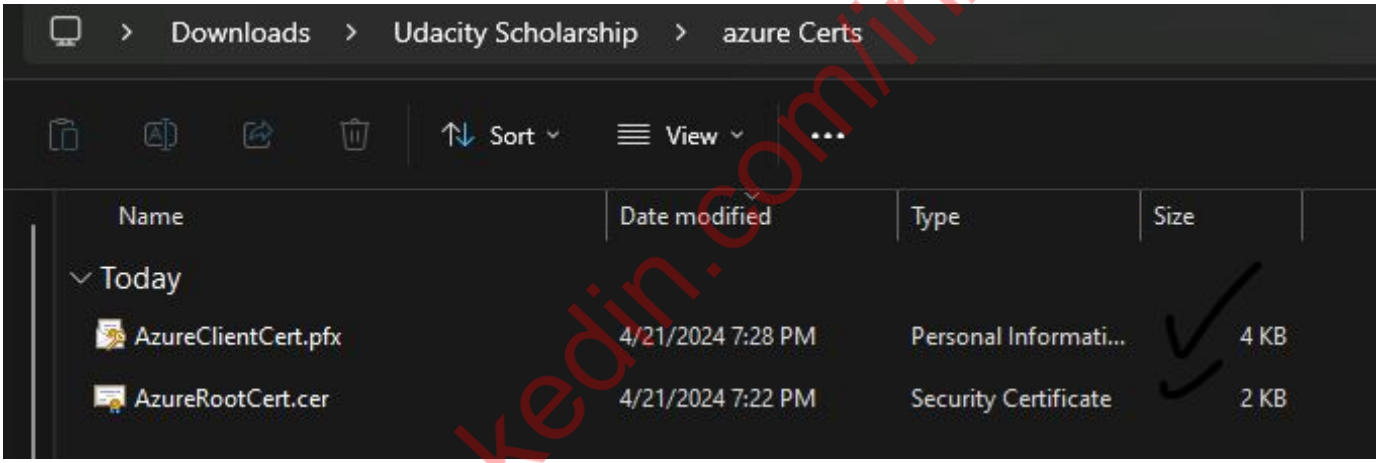




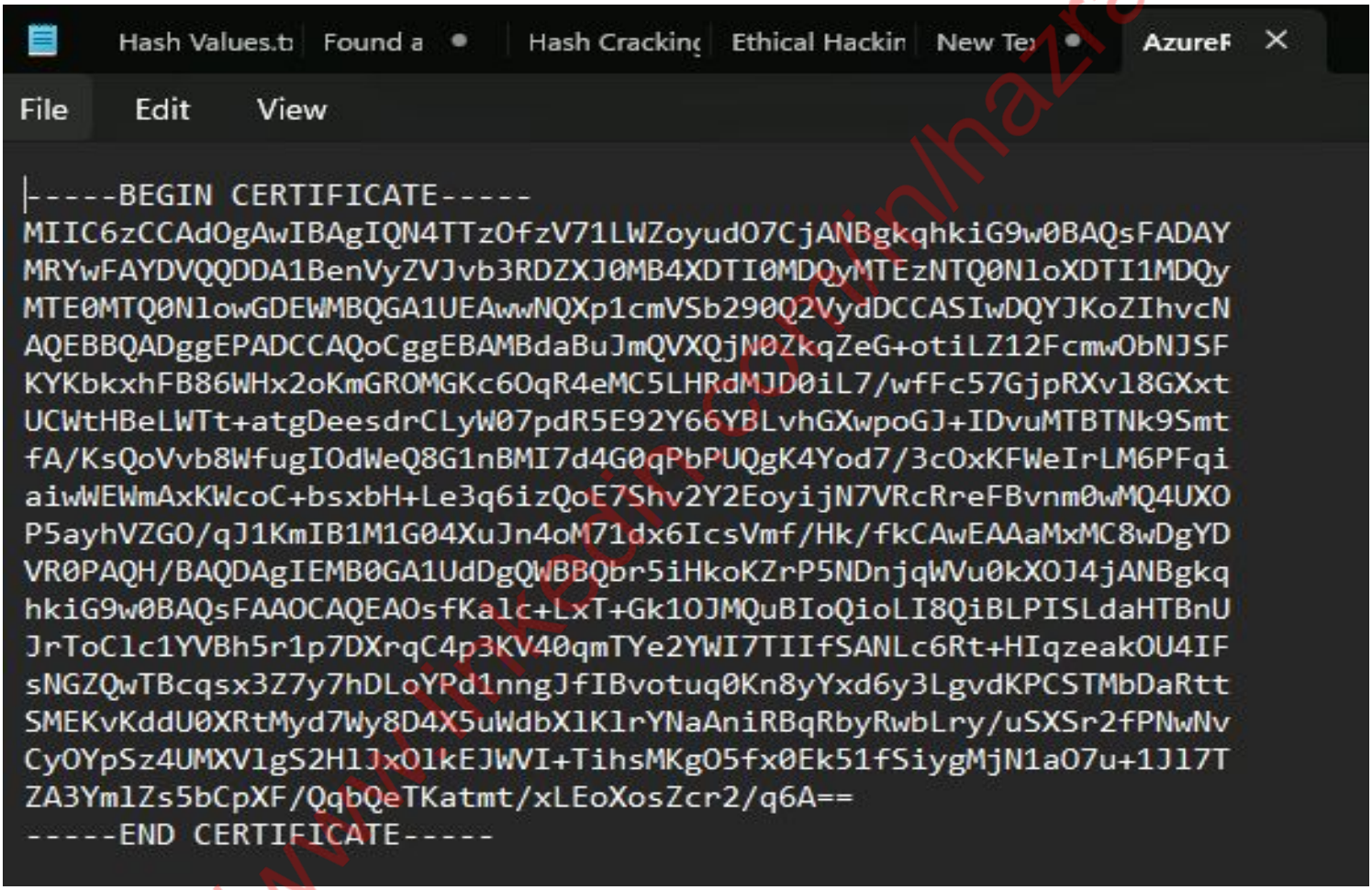




Both Root Cert and Client Certs Exported

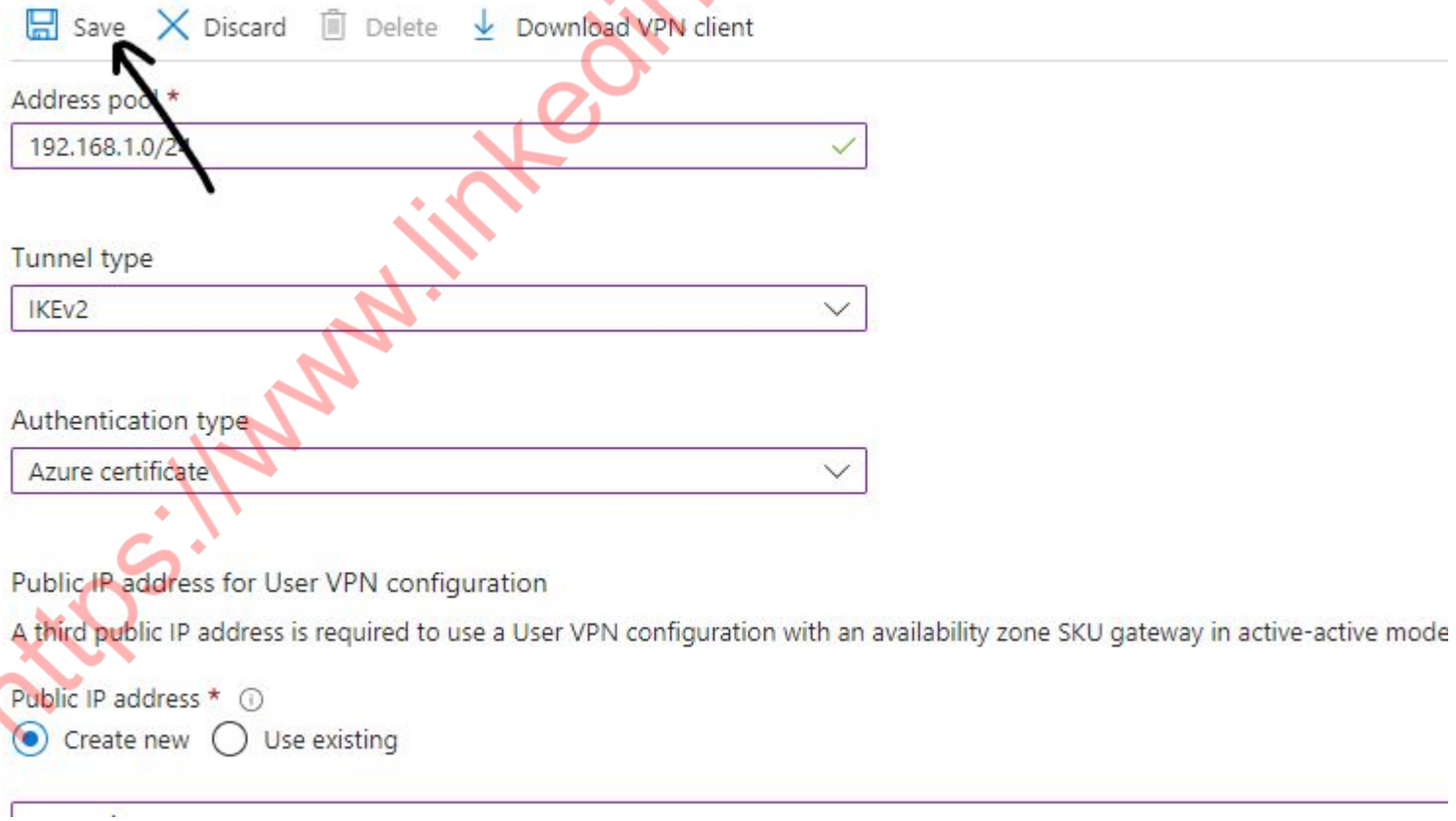


Opening the root cert through Notepad and copying its contents

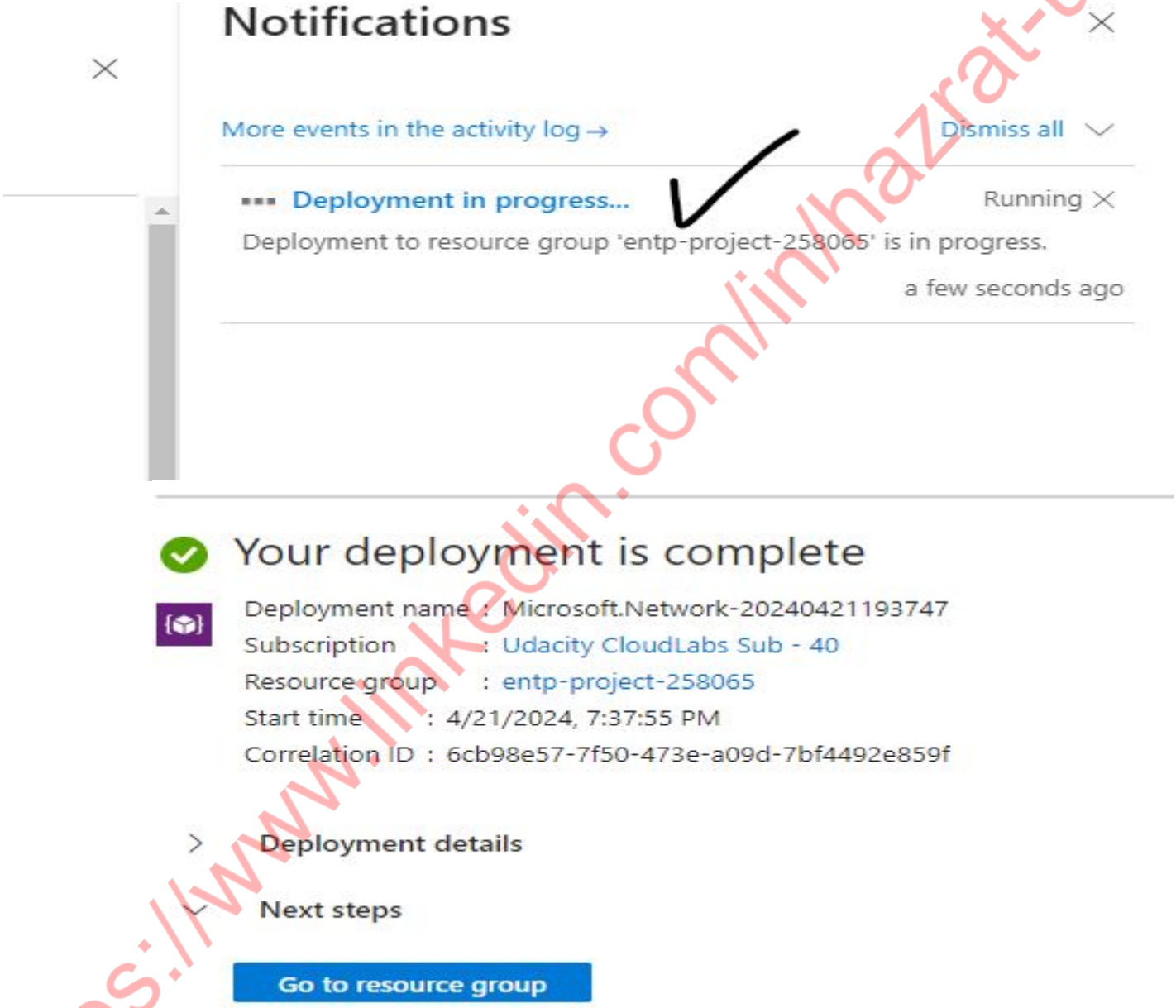


Pasting it in azure

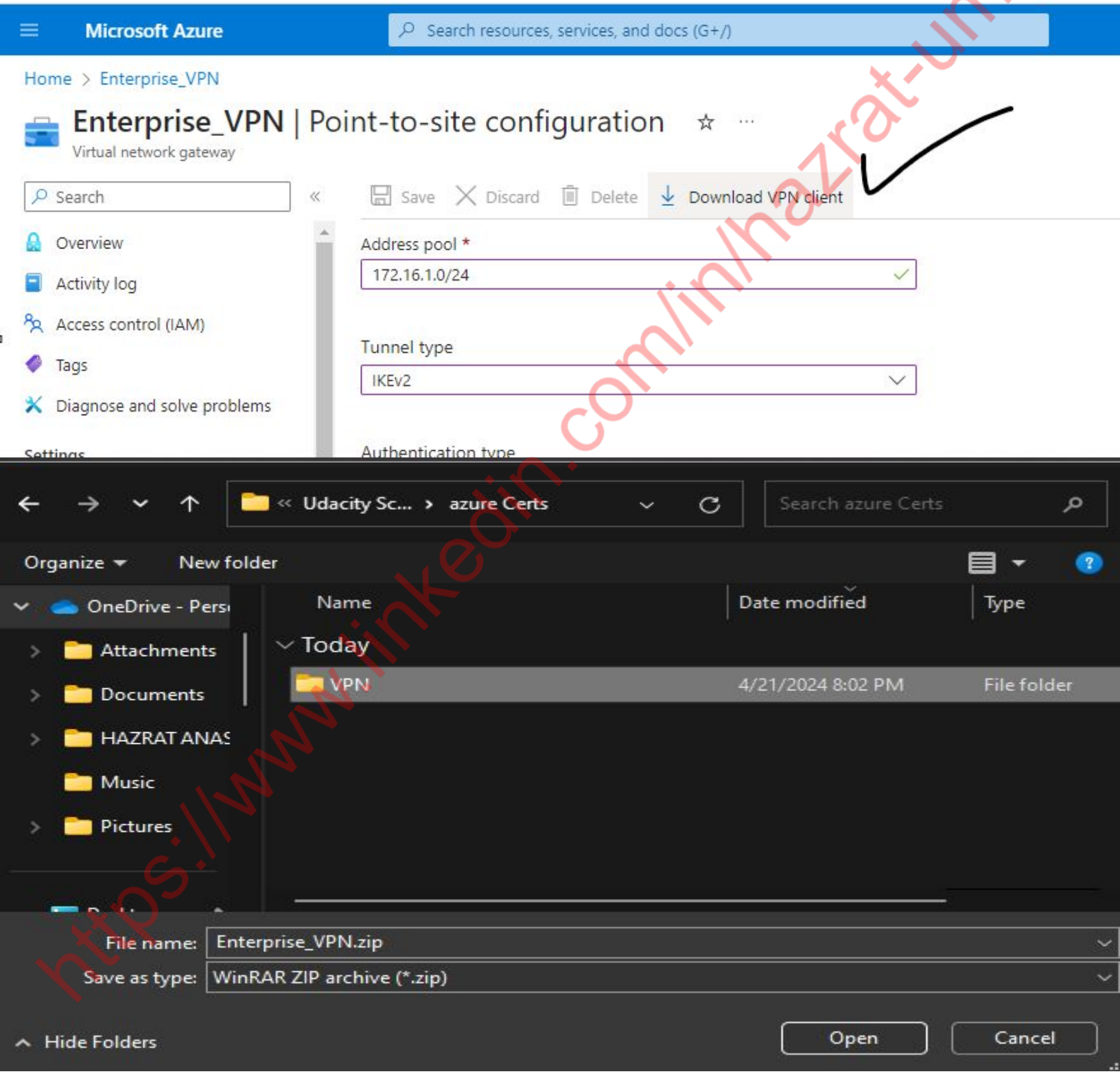
Saving it



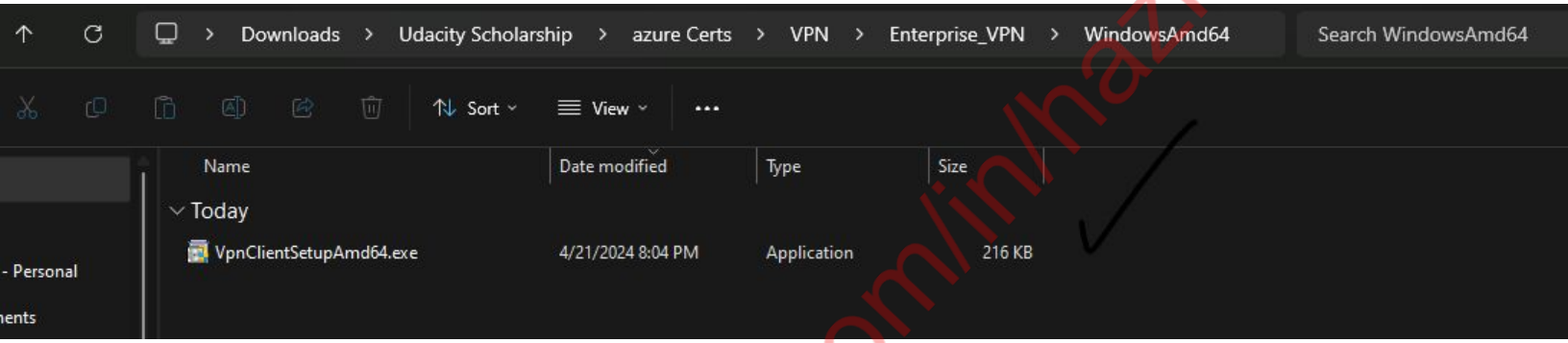
Waiting for its deployment

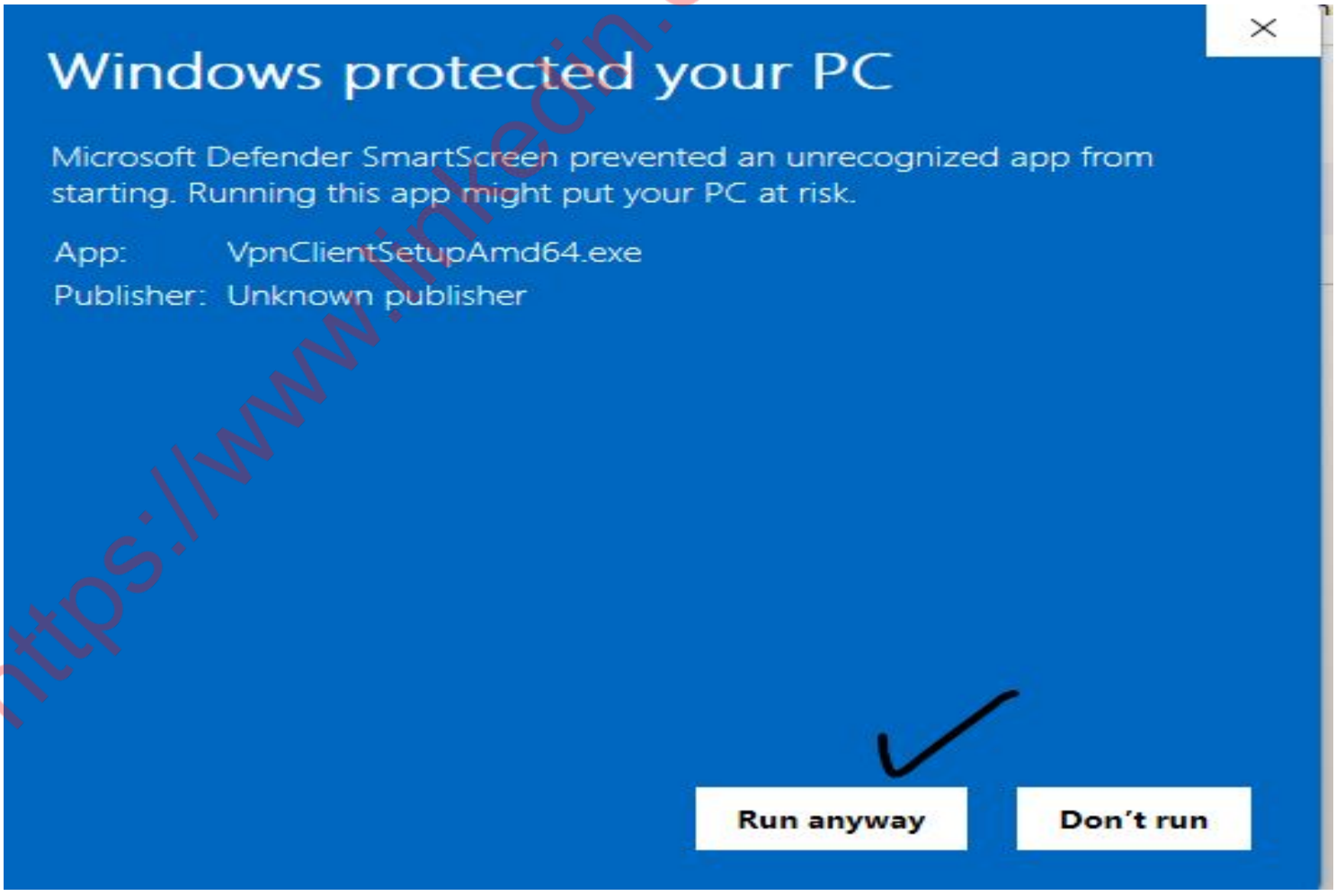


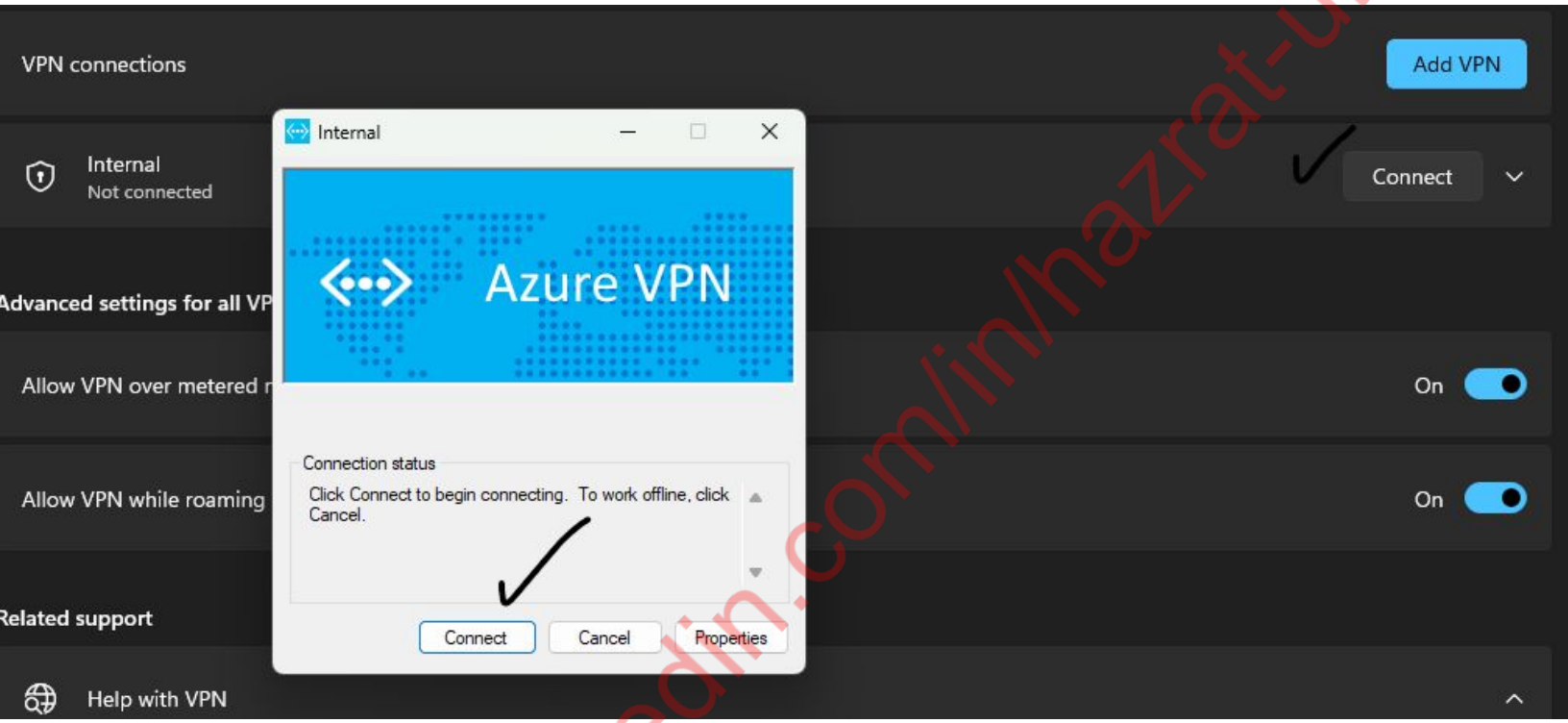
Downloading VPN client

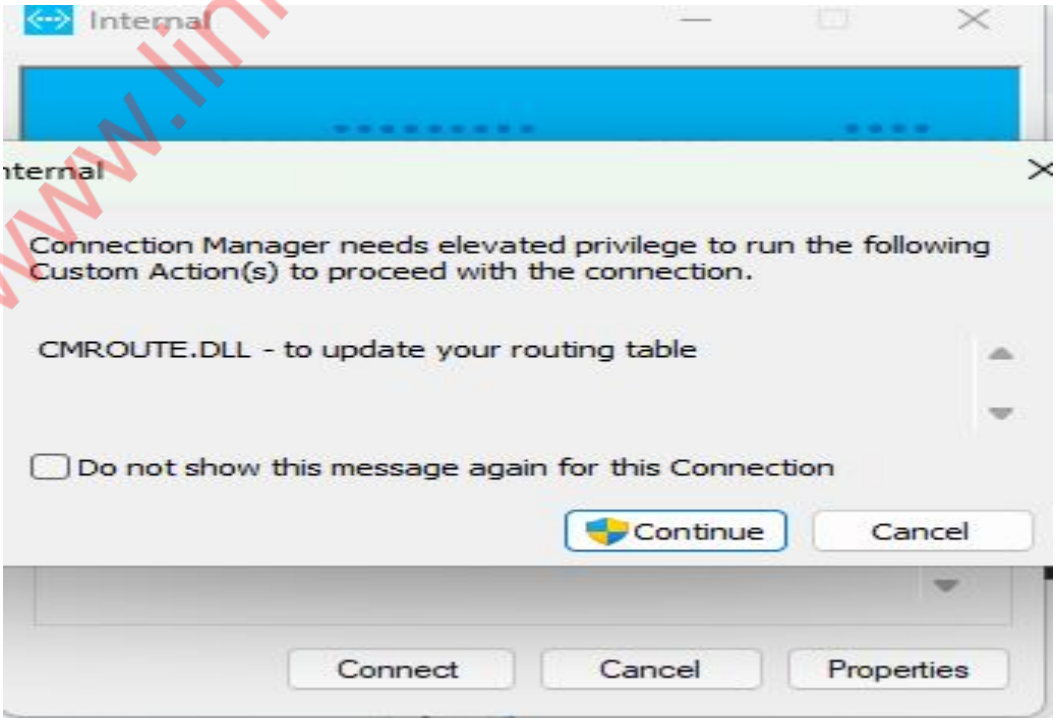


Installing the AMD 64

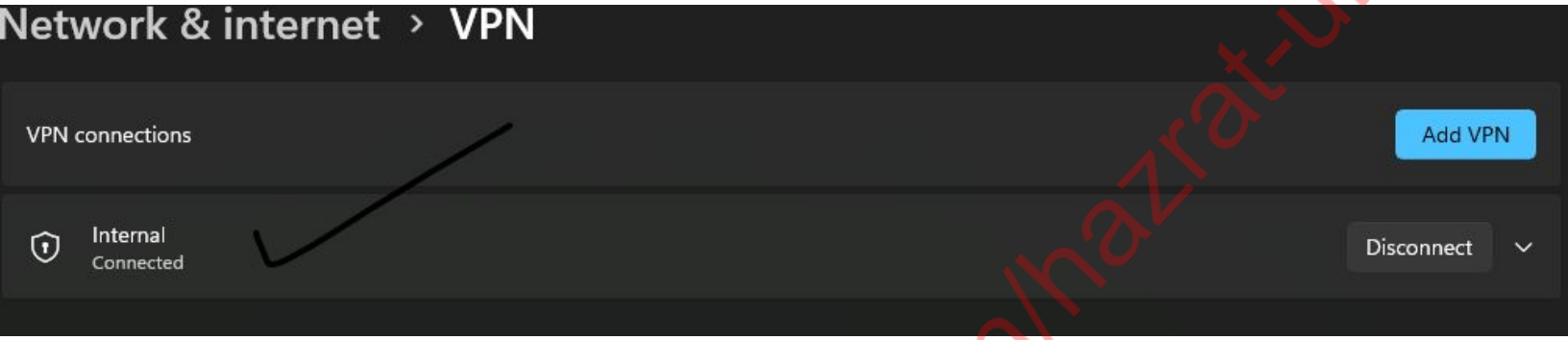








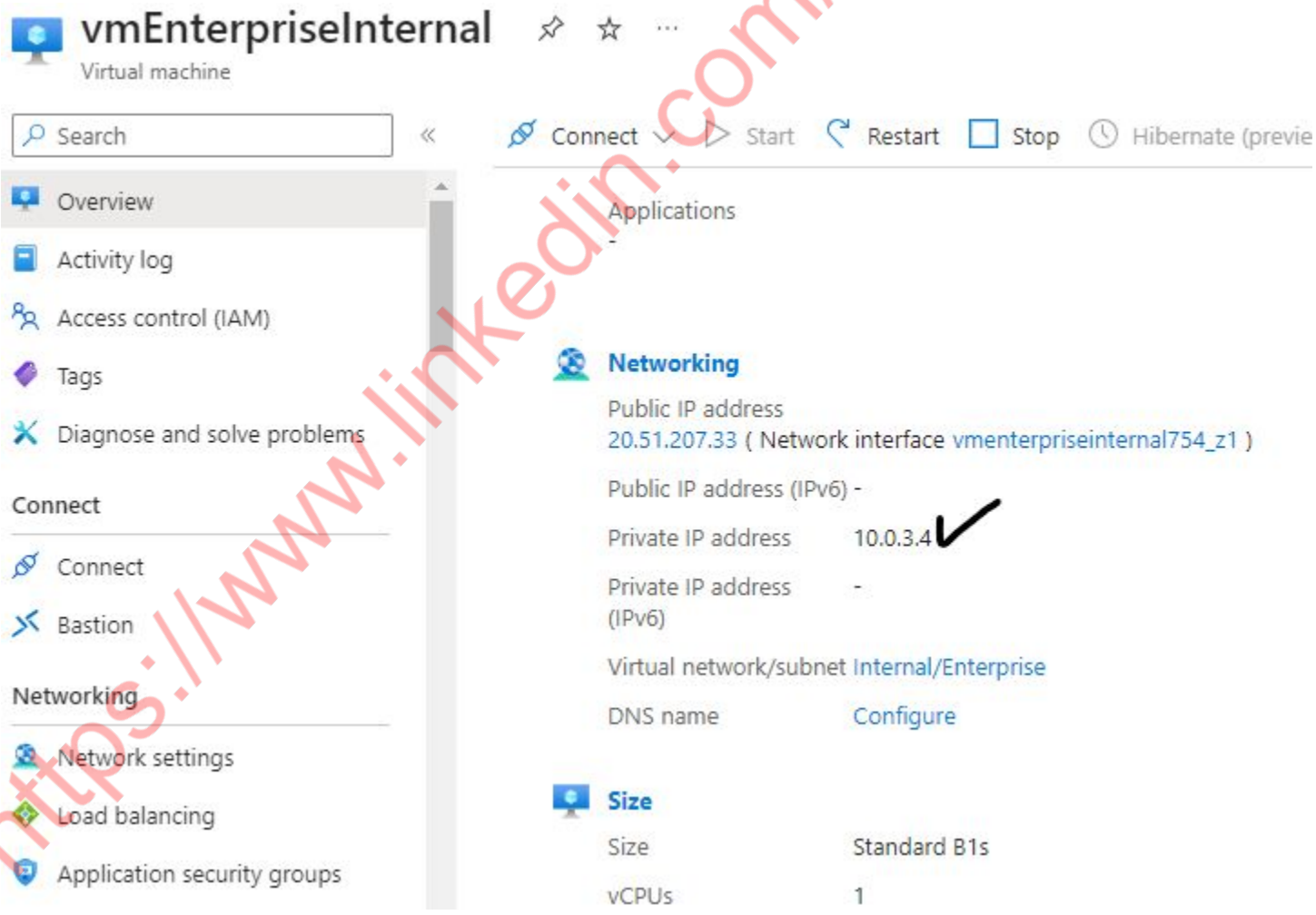
Successfully Connected



2.4.2 Screenshot

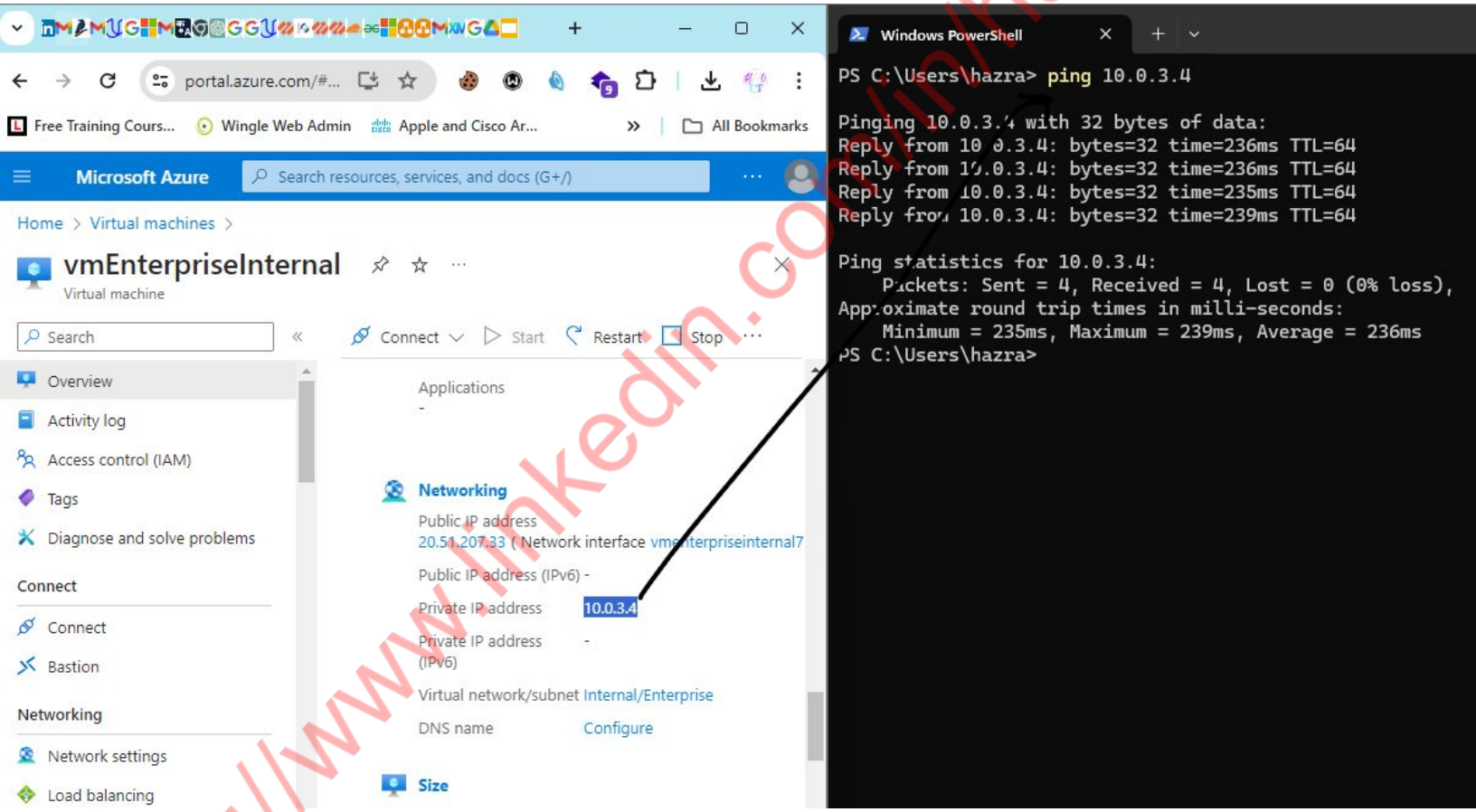
Test VPN connection by connecting to one of the VMs in your internal network.

Testing VPN Connection by pinging Enterprise Virtual Machine through its private IP from my Laptop.

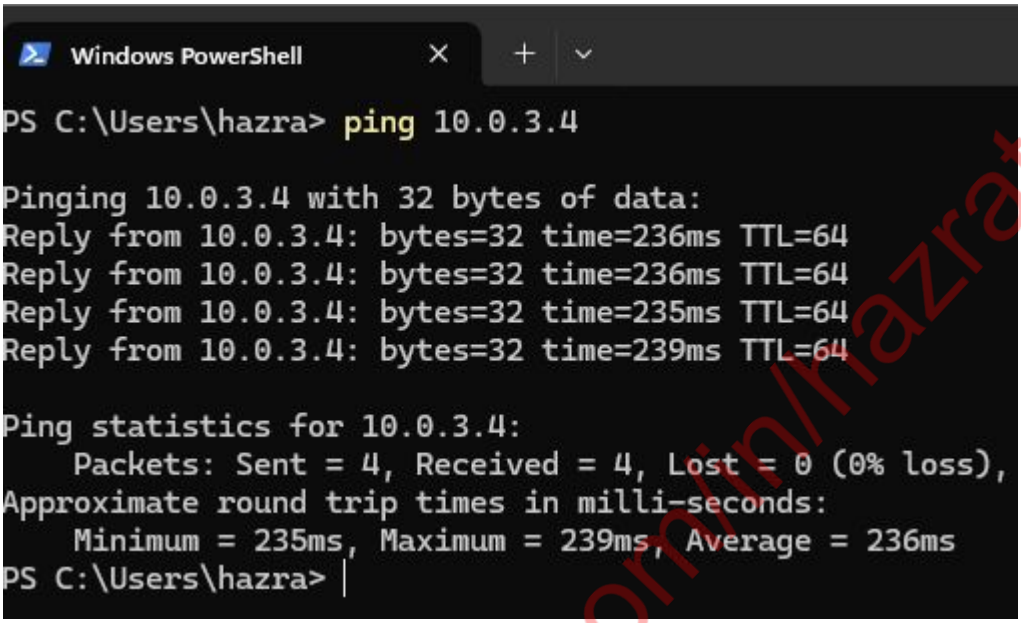


Pinging VM private IP from my laptop

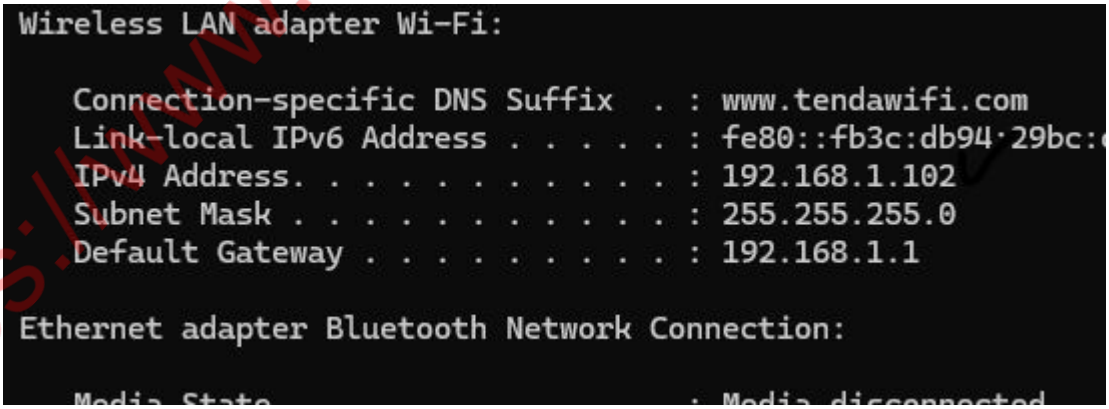
Successfully pinged



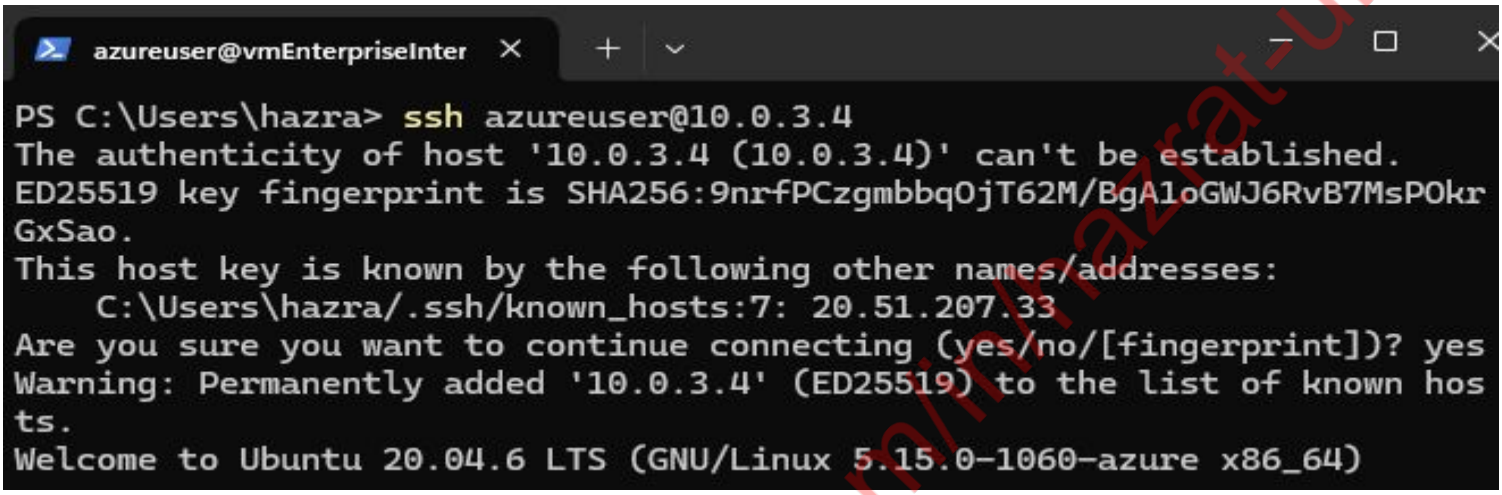
VM IP

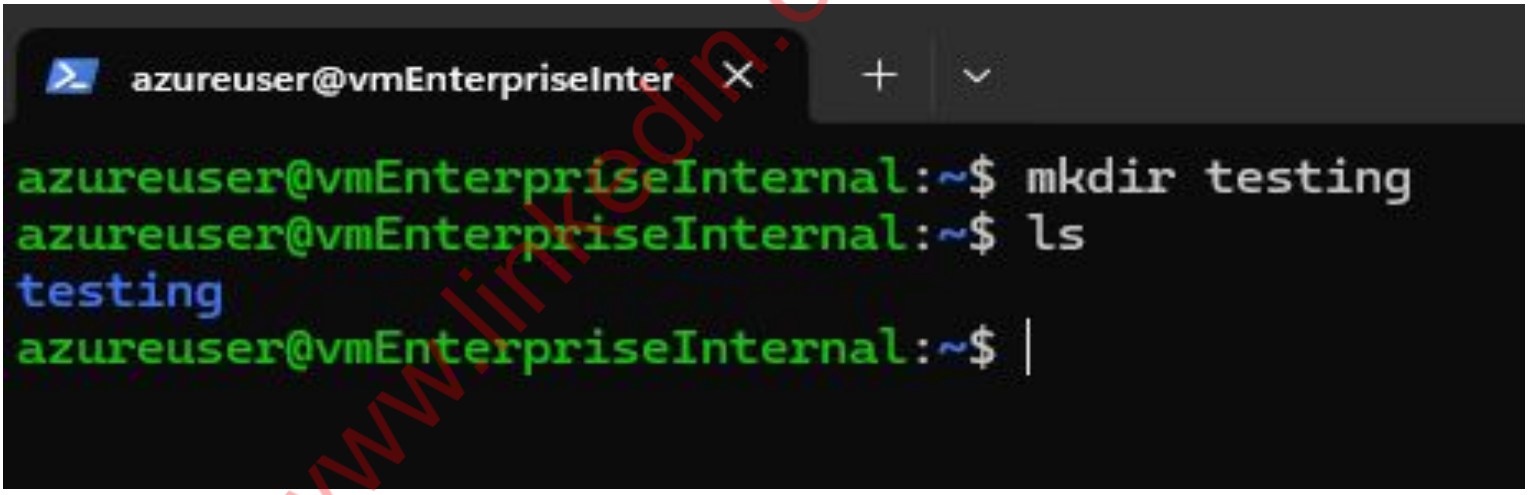


My Laptop Private IP



Access VM through its Private IP through VPN, using SSH





Section 3

Continuous Monitoring with a SIEM

Section 3: Build the SIEM

Now that you've built a secure network architecture and a Zero Trust model, you're ready to wrap up your contract and finish the last piece of work. Your last task is to set up a solution to monitor the enterprise network and alert you about potential attacks.

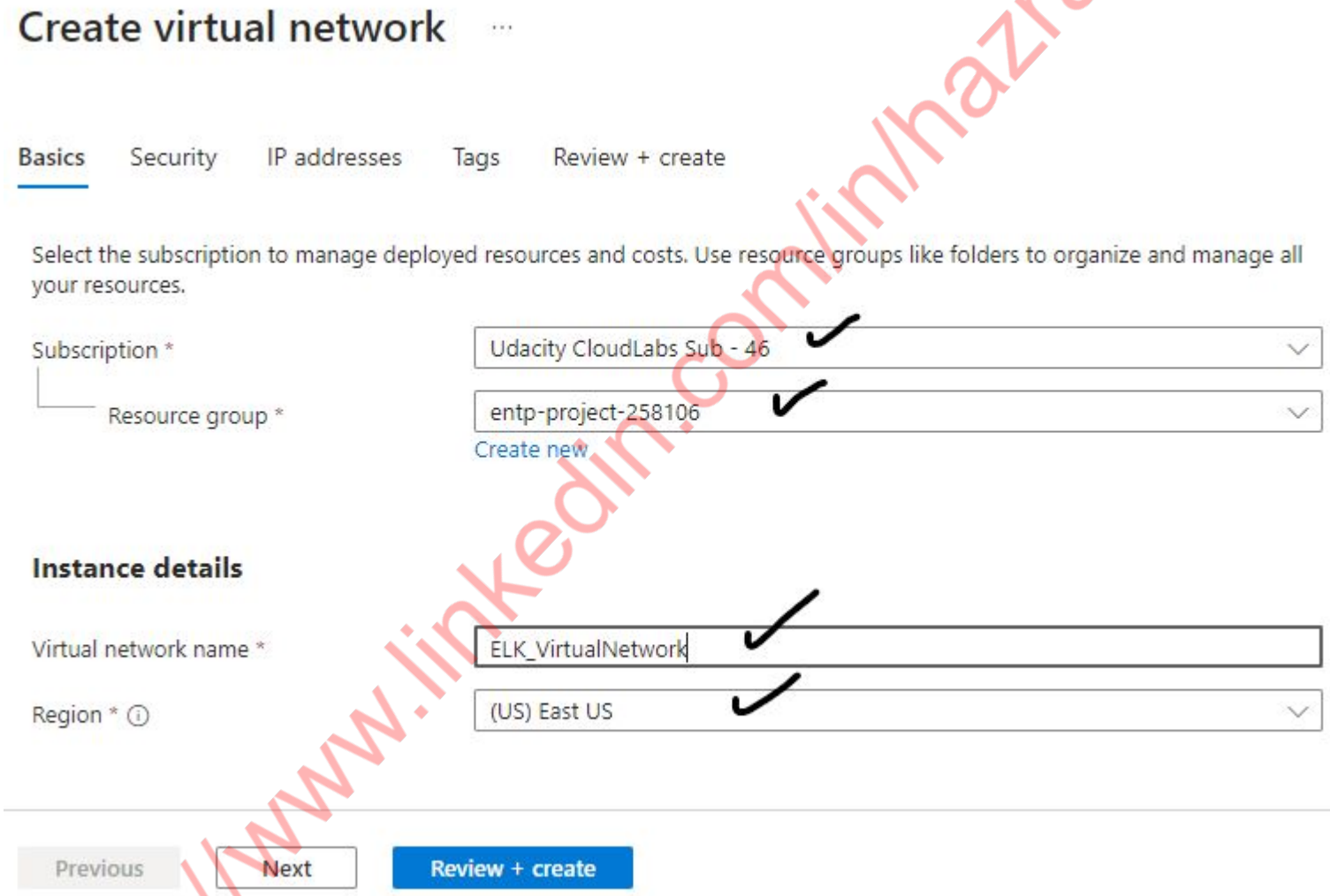
For this section, you will continue working in the Project Workspace in the classroom, then provide screenshots of your work here in this document.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

3.1.1 Screenshot

Create a VM in your private DMZ. On that VM, go through the process to create an ELK Server. For your Elk Server use the VM size DS1_v2 and Linux Ubuntu 18.04 image.

First Creating Virtual Network for the ELK Virtual Machine



Leaving the default IP addresses

Basics Security **IP addresses** Tags Review + create

10.0.0.0/16 Delete address space

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

Virtual Network is Created

Your deployment is complete

Deployment name : ELK_VirtualNetwork-1713728663893
Subscription : Udacity CloudLabs Sub - 46
Resource group : entp-project-258106

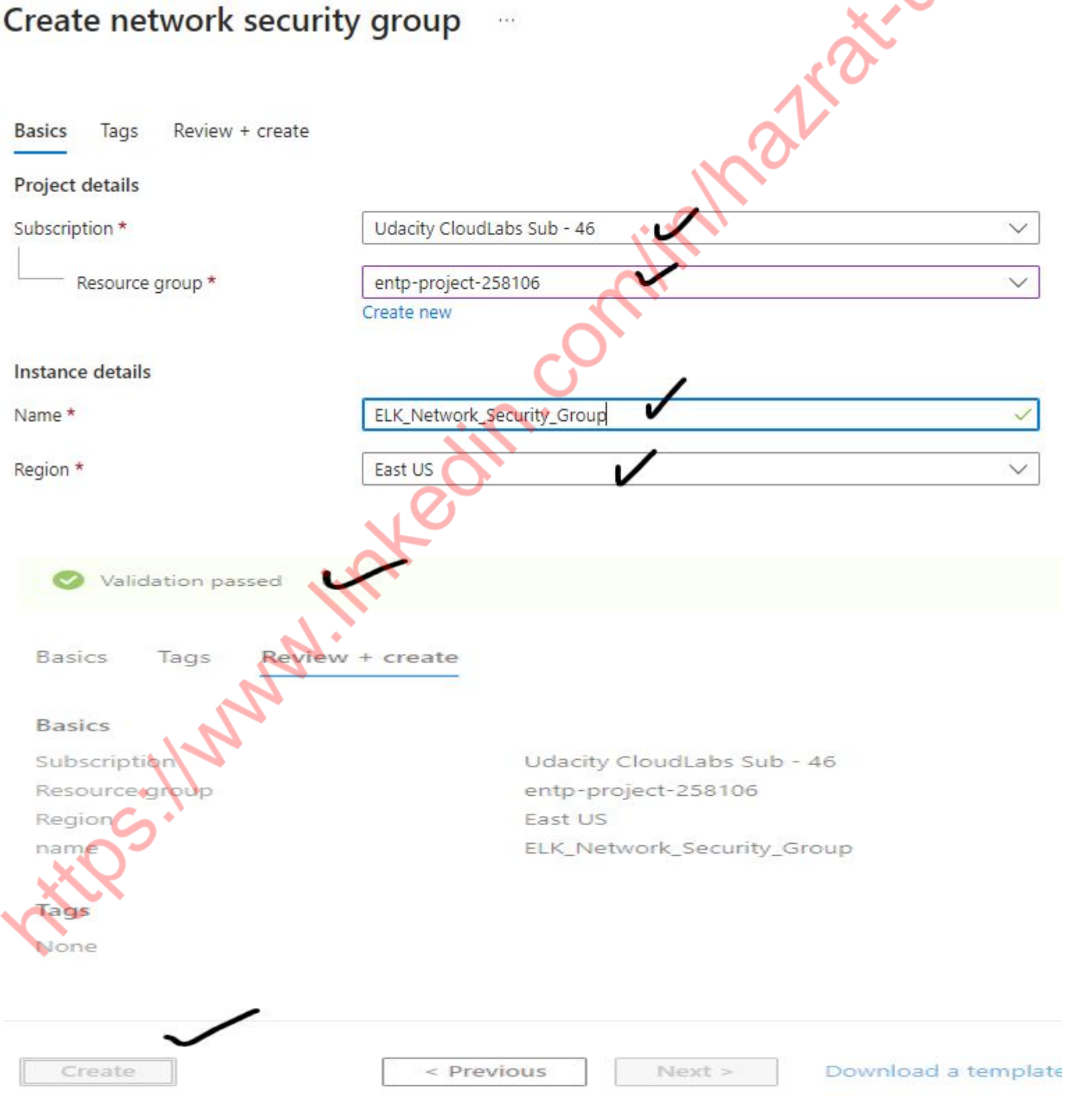
Start time : 4/22/2024, 12:44:34 AM
Correlation ID : 7dd40798-158c-4e1d-81a4-175591d8...

Deployment details

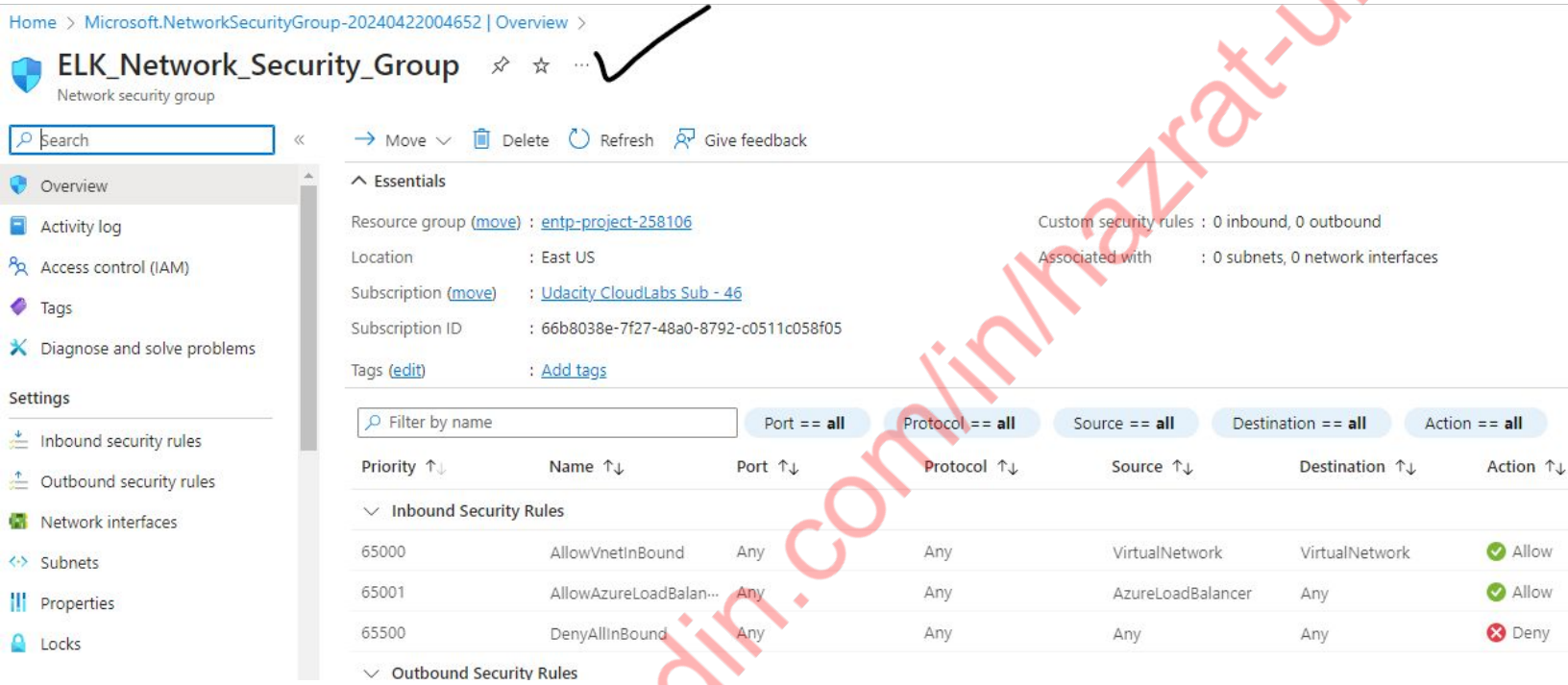
Next steps

Go to resource

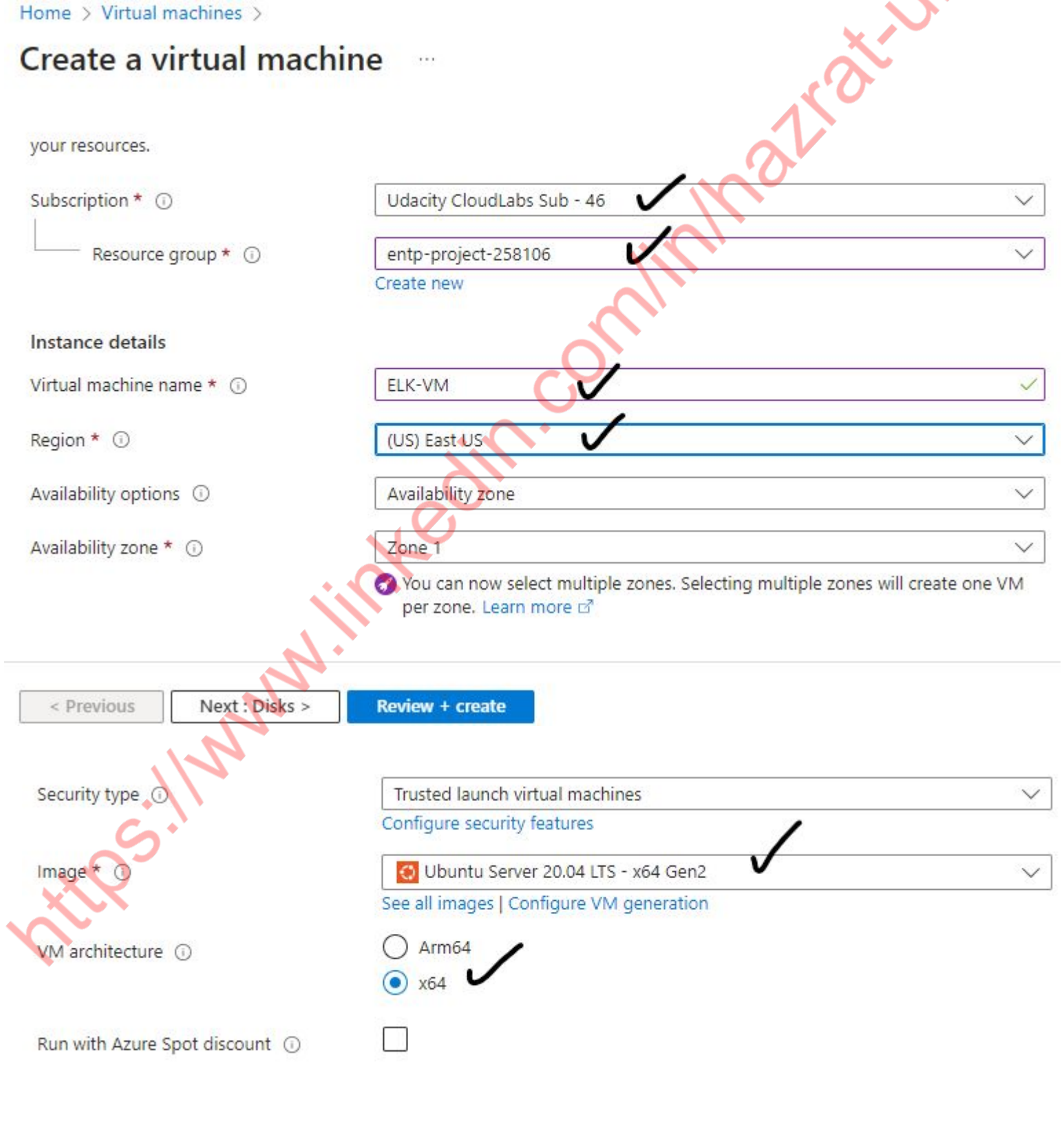
Now Creating Network Security Group



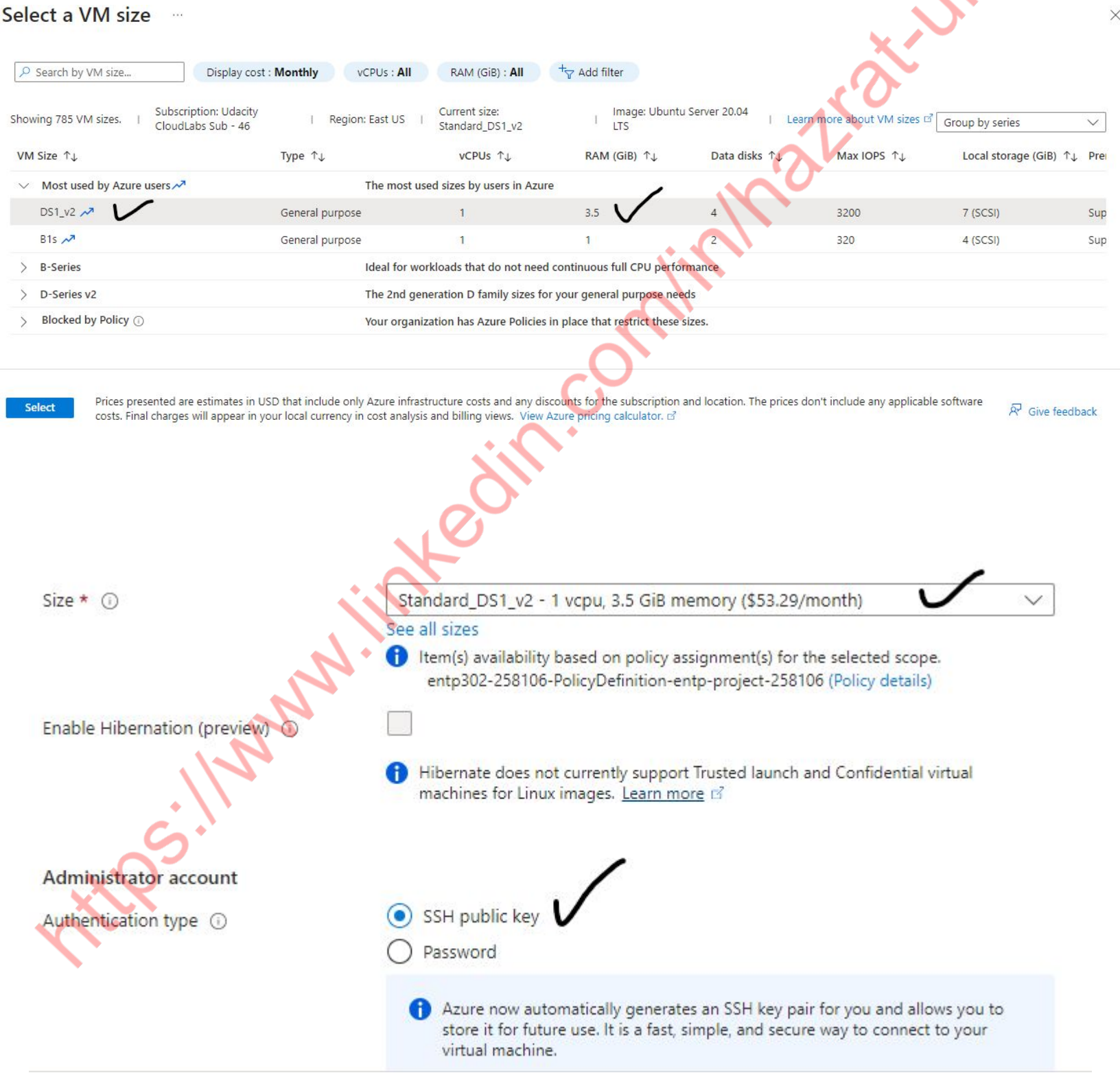
Network Security group created



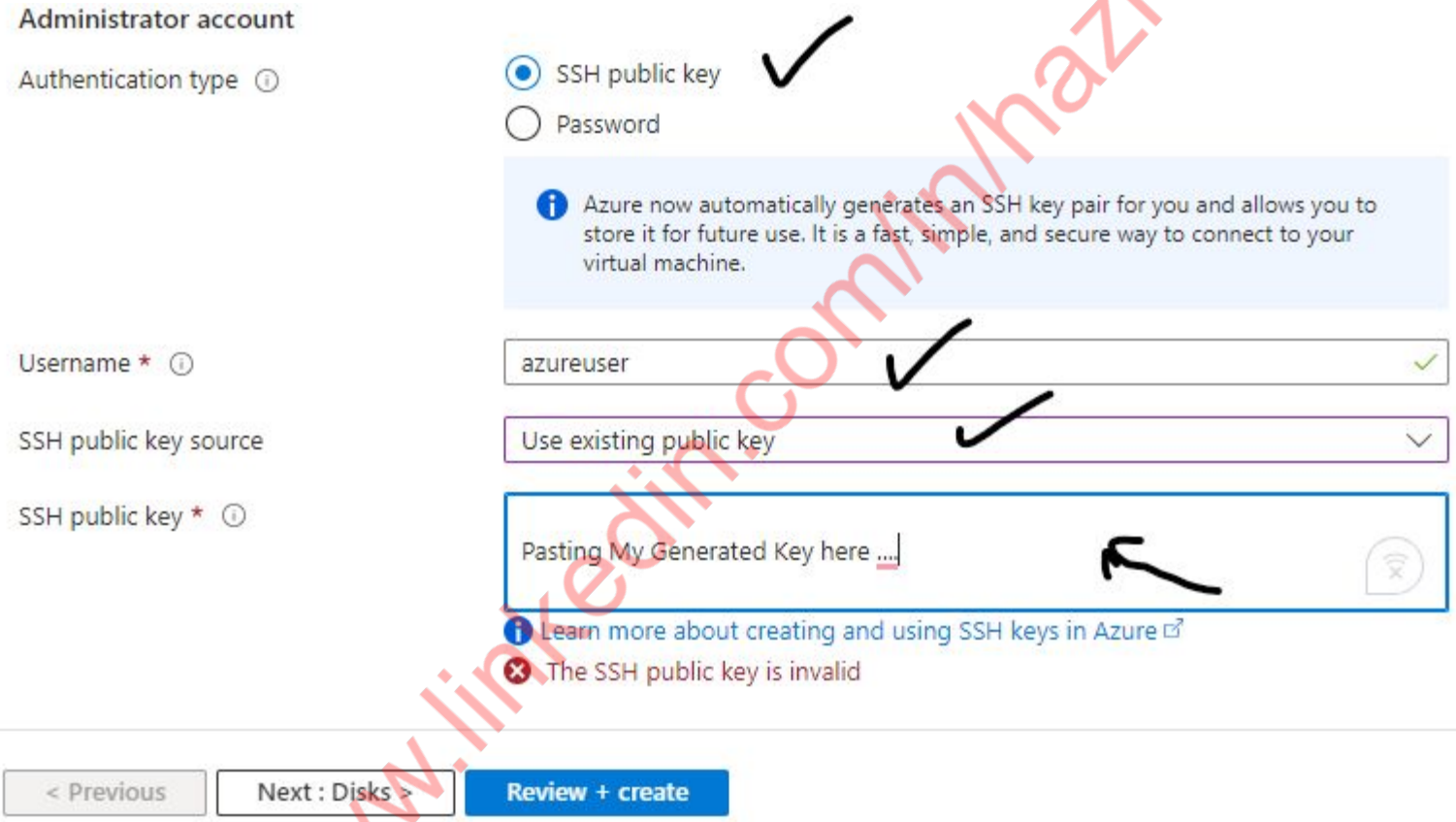
Now Creating Virtual Machine



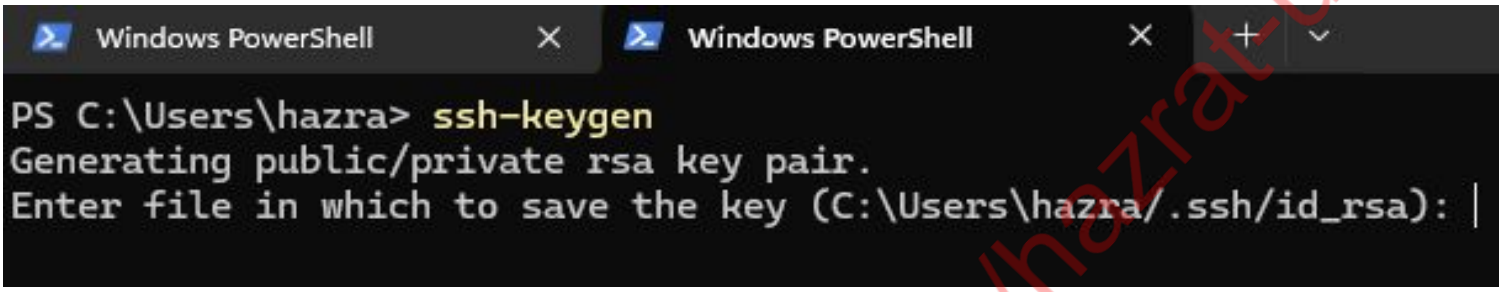
Selecting a VM Size DS1_V2



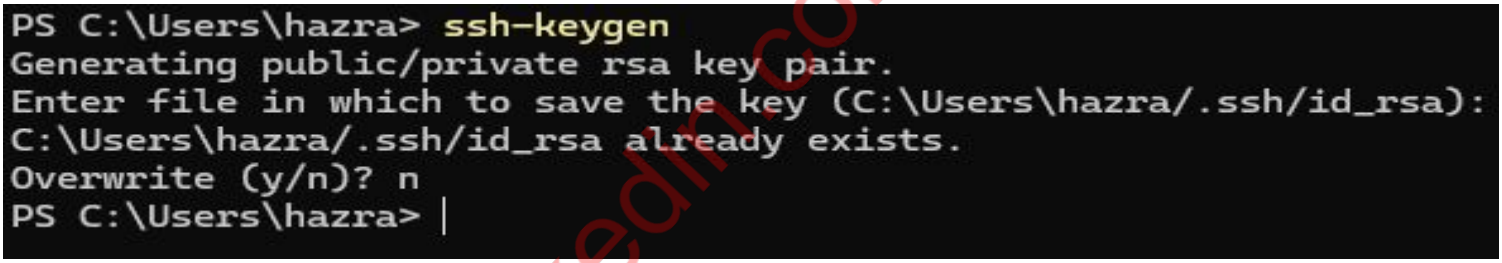
Creating a username and generating and pasting an SSH Key



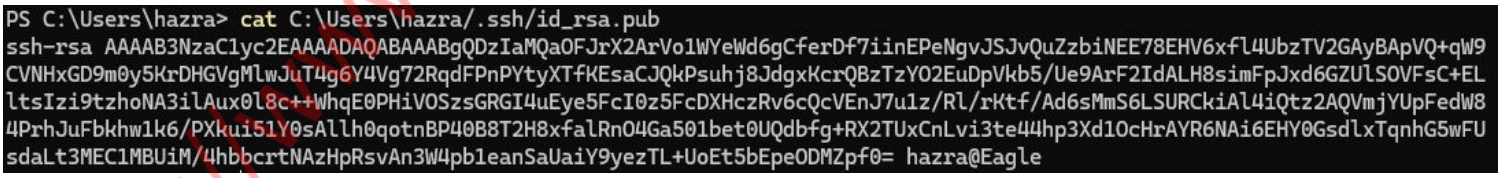
First Generating an SSH Key through Powershell



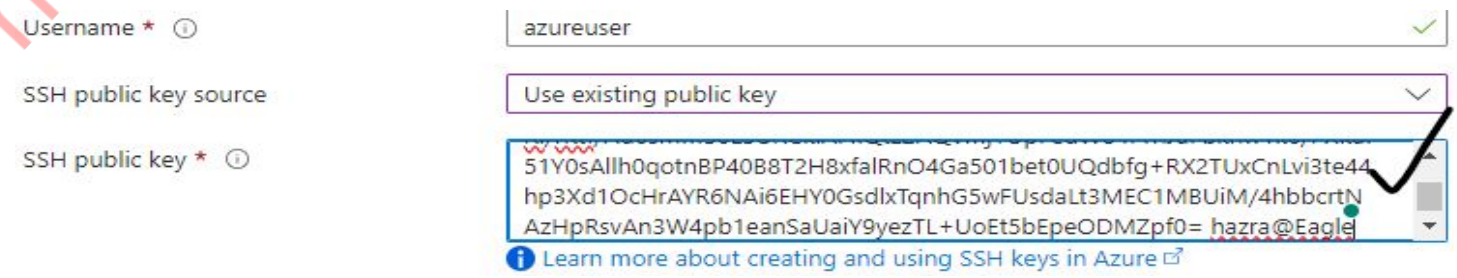
Key already exist



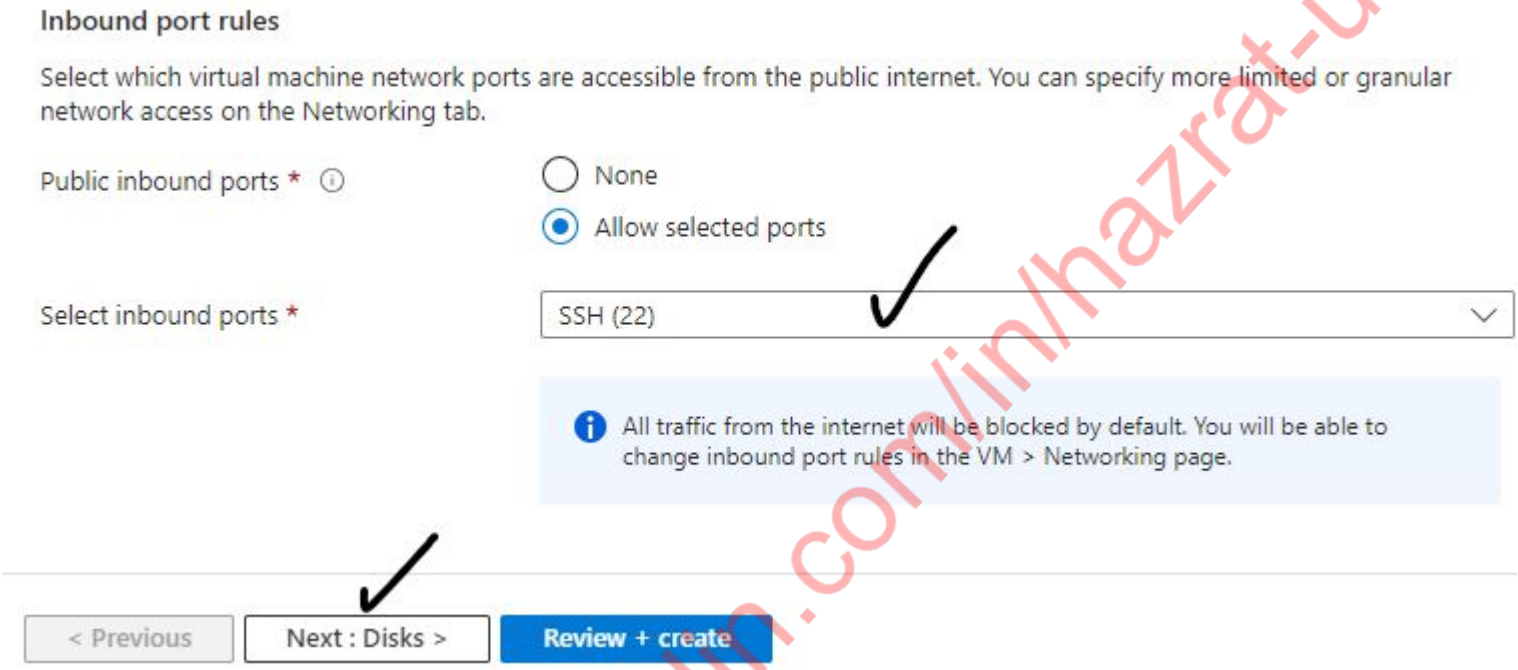
Showing the key



Copying and pasting public key to Azure Portal

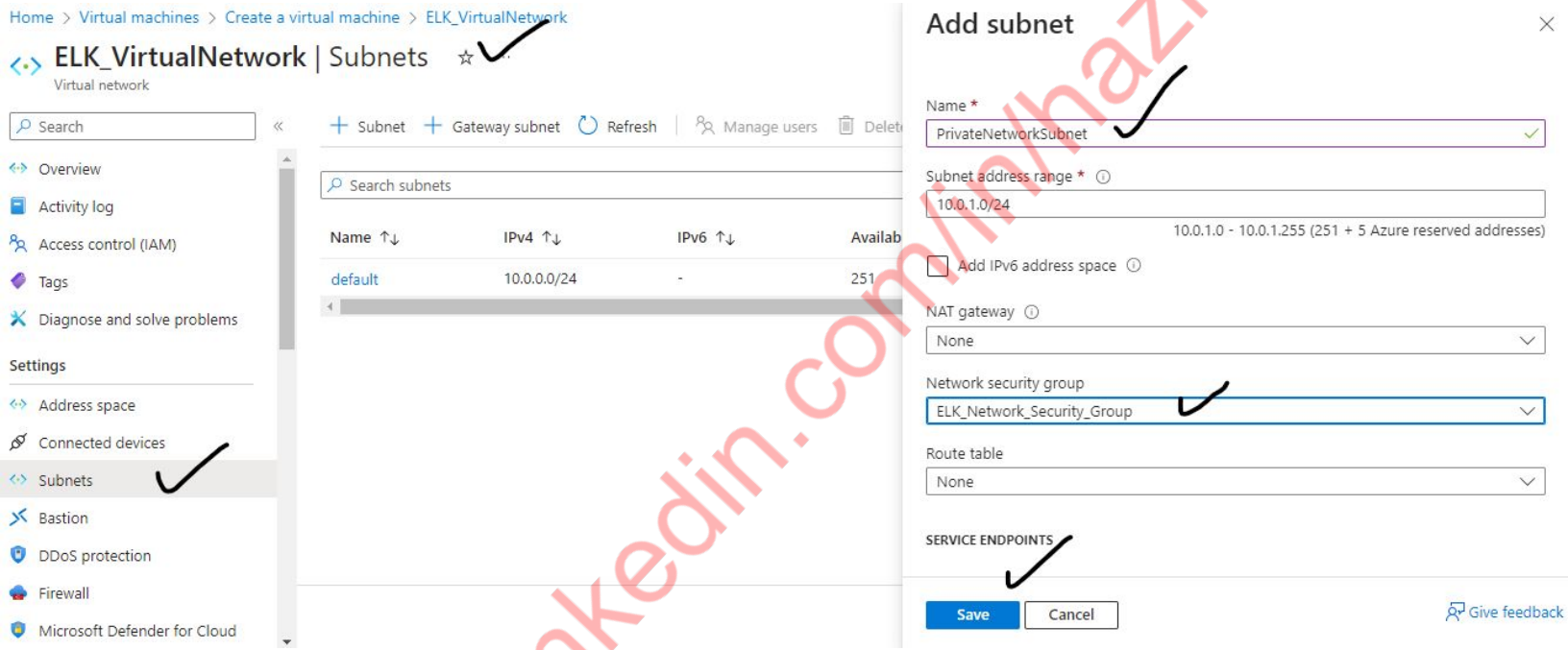


Selecting SSH to allow and click next

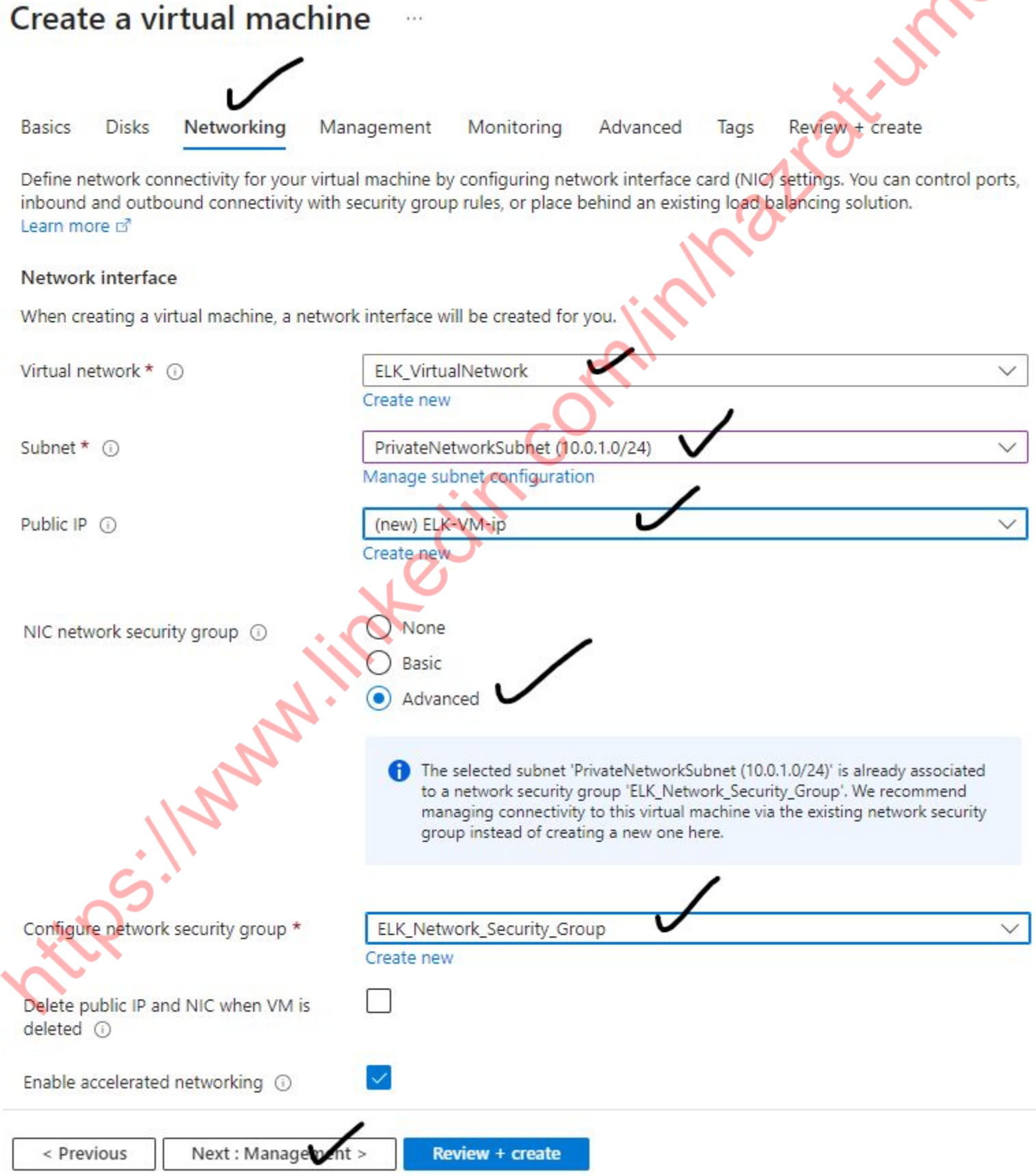


Leaving other things to default and click next, and go to Networking portion

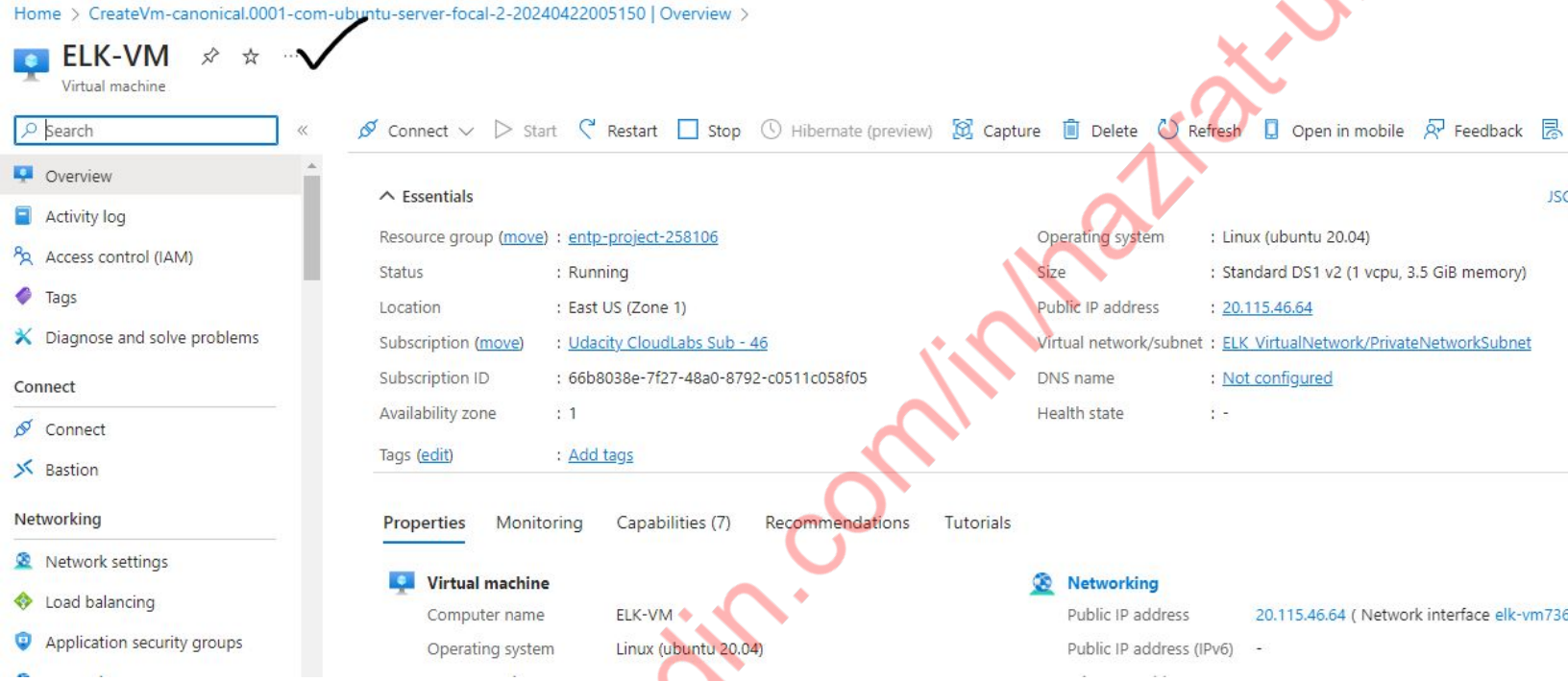
Create a subnet for your virtual network or you can leave as default subnet. I am creating it.



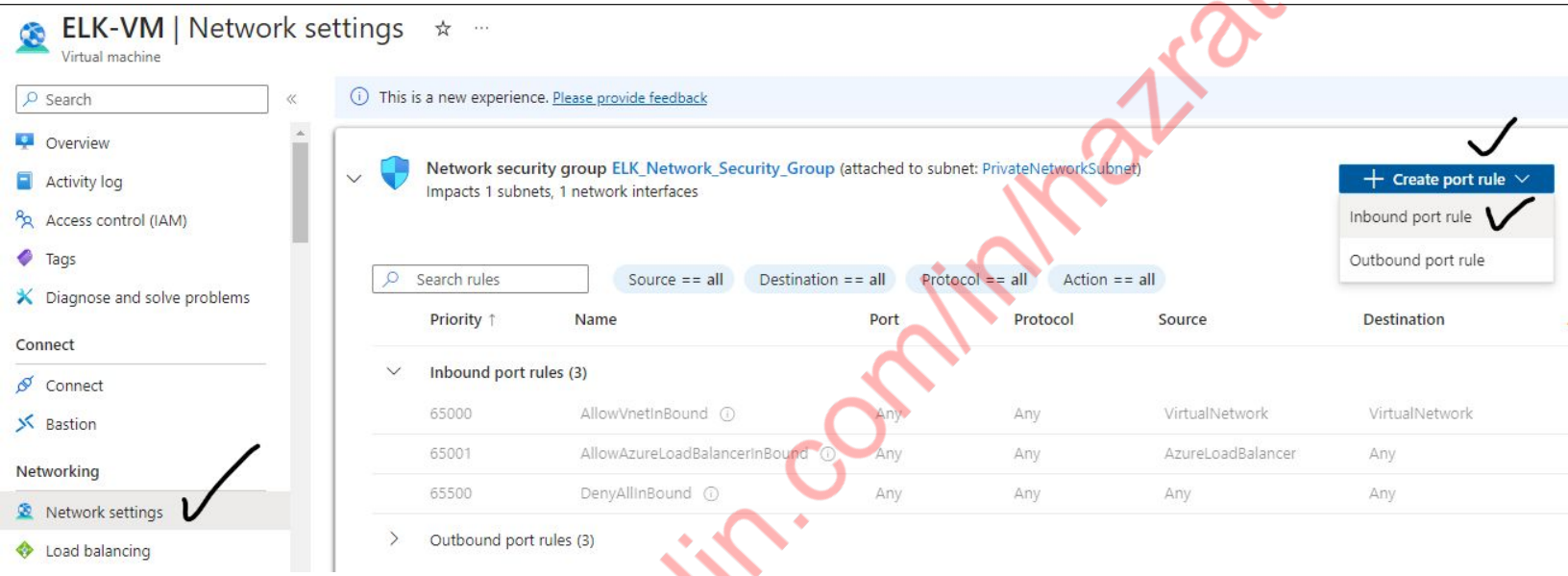
Network configurations for our VM

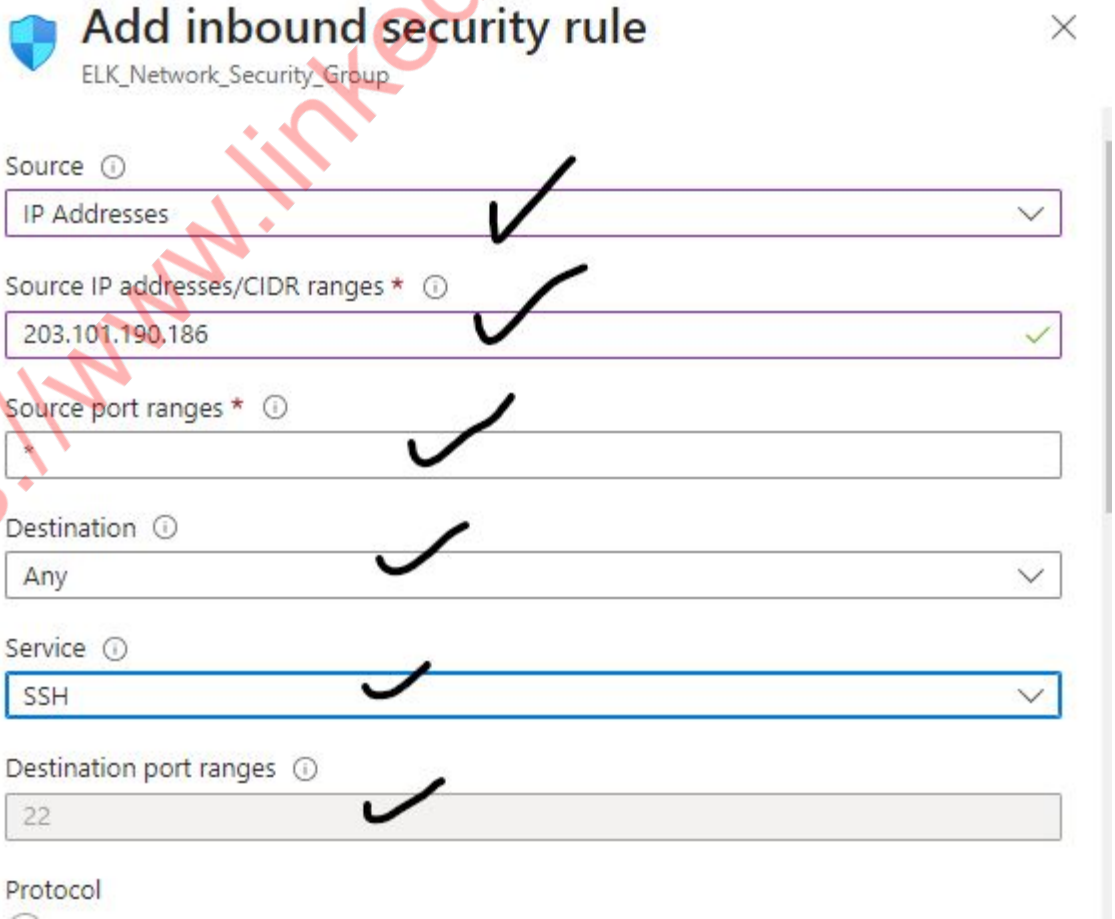


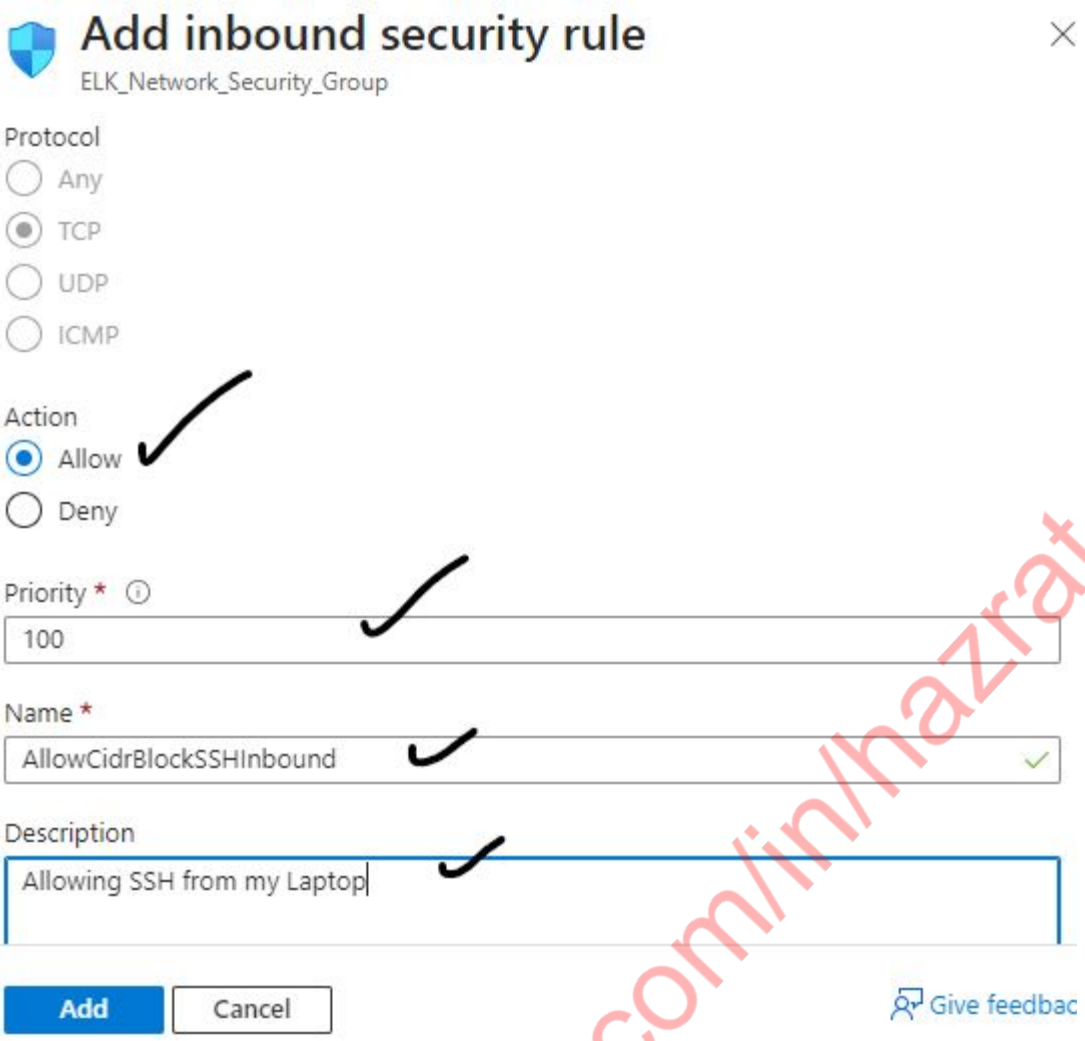
ELK Server VM is Created

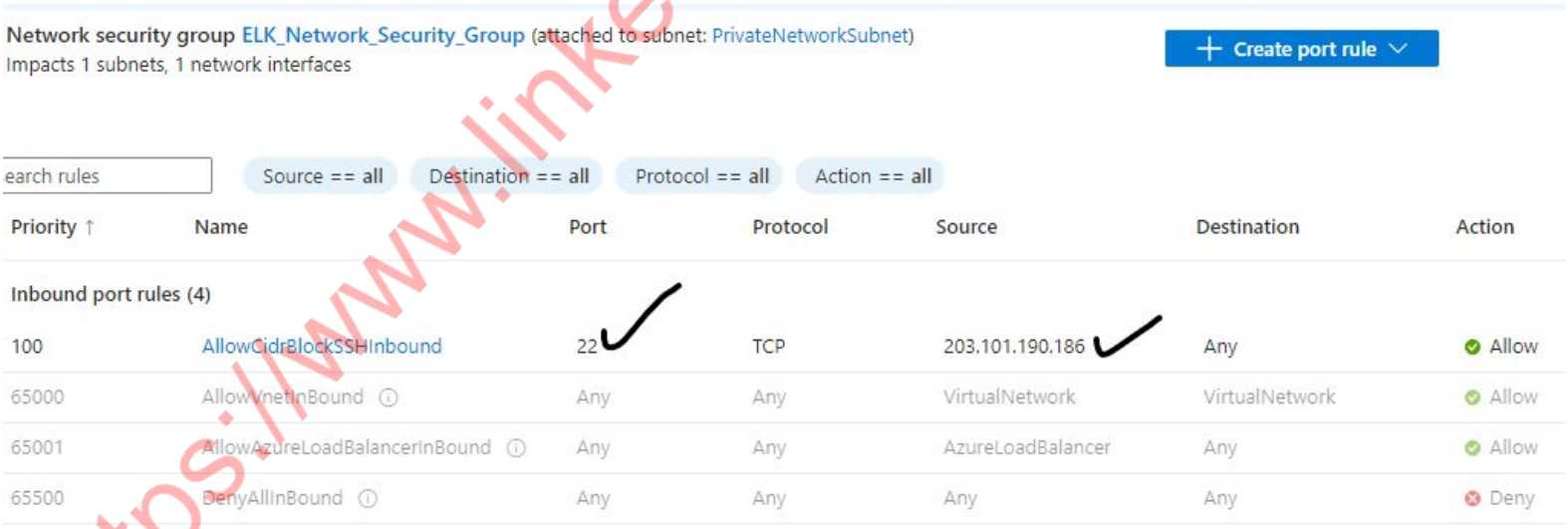


Allowing Traffic from our network (my laptop) to ELK Server. Creating Inbound port rule



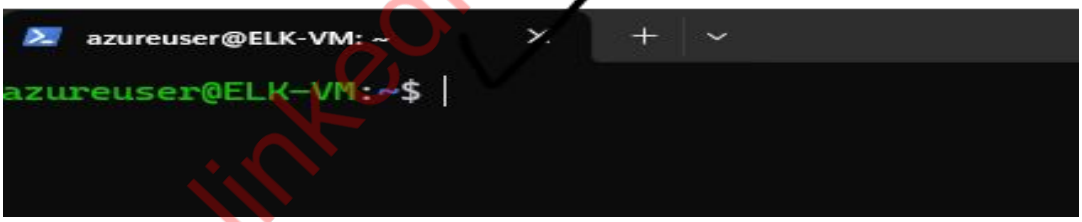






Accessing our ELK Server through SSH

```
PS C:\Users\hazra> ssh azureuser@20.115.46.64
The authenticity of host '20.115.46.64 (20.115.46.64)' can't be established.
ED25519 key fingerprint is SHA256:aMbW0LKcAvEDbcN9atjrAKKp2sGstHUYUiVxiBvOTLw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.115.46.64' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1060-azure x86_64)
```



I will be using the following commands to run ELK Server

```
Commands to run in ELK Server

sudo apt update

sudo apt install docker.io

sudo apt install python3-pip

sudo pip3 install docker

sudo sysctl -w vm.max_map_count=262144

sudo docker pull sebp/elk:761

sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk
sebp/elk:761
```

Updating our ELK Server

```
azureuser@ELK-VM: ~
azureuser@ELK-VM:~$ sudo apt update
Get:1 http://azure.archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Hit:4 http://azure.archive.ubuntu.com/ubuntu focal-security InRelease
Get:5 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 Packages [970 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu focal/main Translation-en [506 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 c-n-f Metadata [29.5
Get:8 http://azure.archive.ubuntu.com/ubuntu focal/restricted amd64 Packages [22.0
```

Installing Docker

Docker will be our containerization platform that will run our ELK stack

```
azureuser@ELK-VM: ~
azureuser@ELK-VM:~$ sudo apt install docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bridge-utils containerd dns-root-data dnsmasq-base libidn11 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 dns-root-data dnsmasq-base docker.io libidn11 pigz runc ubuntu-fan
0 upgraded, 9 newly installed, 0 to remove and 28 not upgraded.
Need to get 63.3 MB of archives.
After this operation, 267 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
Selecting previously unselected package ubuntu-fan.
Preparing to unpack .../8-ubuntu-fan_0.12.13ubuntu0.1_all.deb ...
Unpacking ubuntu-fan (0.12.13ubuntu0.1) ...
Setting up runc (1.1.7-0ubuntu1~20.04.2) ...
Setting up dns-root-data (2023112702~ubuntu0.20.04.1) ...
Setting up libidn11:amd64 (1.33-2.2ubuntu2) ...
Setting up bridge-utils (1.6-2ubuntu1) ...
Setting up pigz (2.4-1) ...
Setting up containerd (1.7.2-0ubuntu1~20.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service → /lib/systemd/system/containerd.servi
Setting up docker.io (24.0.5-0ubuntu1~20.04.1) ...
Adding group `docker' (GID 122) ...
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.
Setting up dnsmasq-base (2.90-0ubuntu0.20.04.1) ...

Progress: [ 89%] [#################################################################################.....]
```

Installing Python3-pip

```
azureuser@ELK-VM:~$ sudo apt install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dpkg-dev fakeroot g++ g++-9 gcc gcc-9
  gcc-9-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1 libbinutils
  libc-dev-bin libc6 libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdpkg-perl libexpat1-dev libfakeroot
  libfile-fcntllock-perl libgcc-9-dev libgomp1 libisl22 libitm1 liblsan0 libmpc3 libpython3-dev libpython3.8-dev
  libquadmath0 libstdc++-9-dev libtsan0 libubsan1 linux-libc-dev make manpages-dev python-pip-whl python3-dev
  python3-wheel python3.8-dev zlib1g-dev
Suggested packages:
  binutils-doc cpp-doc gcc-9-locales debian-keyring g++-multilib g++-9-multilib gcc-9-doc gcc-multilib autoconf
  automake libtool flex bison gdb gcc-doc gcc-9-multilib glibc-doc bzr libstdc++-9-doc make-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-9 dpkg-dev fakeroot g++ g++-9 gcc gcc-9
  gcc-9-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan5 libatomic1 libbinutils
  libc-dev-bin libc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdpkg-perl libexpat1-dev libfakeroot
  libfile-fcntllock-perl libgcc-9-dev libgomp1 libisl22 libitm1 liblsan0 libmpc3 libpython3-dev libpython3.8-dev
  libquadmath0 libstdc++-9-dev libtsan0 libubsan1 linux-libc-dev make manpages-dev python-pip-whl python3-dev
  python3-pip python3-wheel python3.8-dev zlib1g-dev
The following packages will be upgraded:
  libc6
1 upgraded, 50 newly installed, 0 to remove and 27 not upgraded.
Need to get 55.0 MB of archives.
After this operation, 228 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Now using pip 3 to install Docker

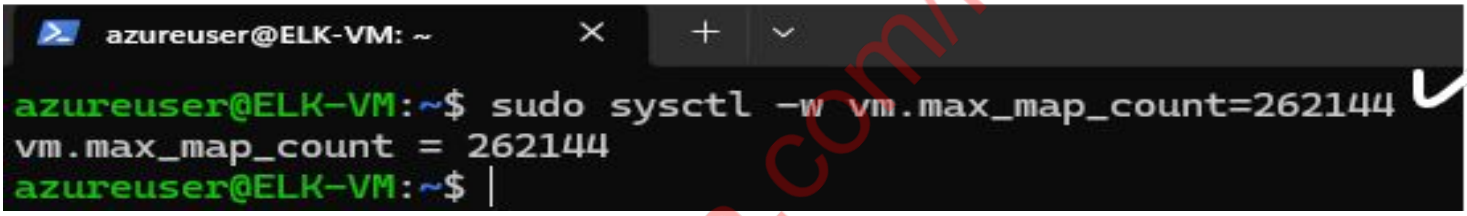
Now using pip3 to install Docker

Sudo pip3 install Docker

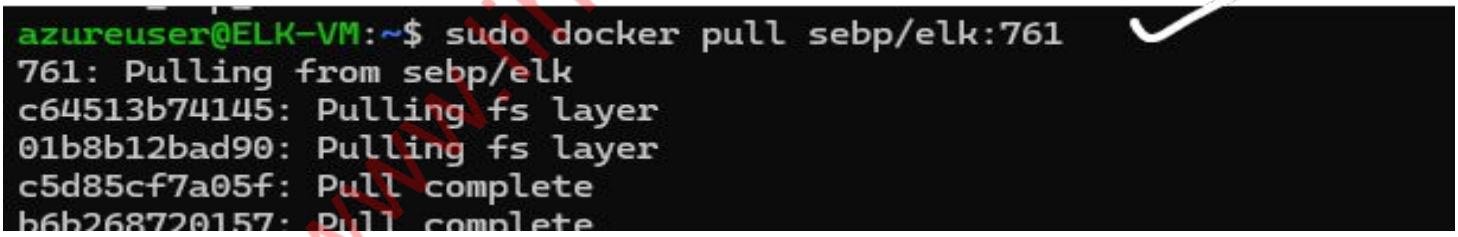
```
azureuser@ELK-VM:~$ sudo pip3 install docker
Collecting docker
  Downloading docker-7.0.0-py3-none-any.whl (147 kB)
     |████████████████████████████████| 147 kB 16.9 MB/s
Collecting packaging>=14.0
  Downloading packaging-24.0-py3-none-any.whl (53 kB)
     |████████████████████████████████| 53 kB 1.4 MB/s
Collecting urllib3>=1.26.0
  Downloading urllib3-2.2.1-py3-none-any.whl (121 kB)
     |████████████████████████████████| 121 kB 46.7 MB/s
Collecting requests>=2.26.0
  Downloading requests-2.31.0-py3-none-any.whl (62 kB)
     |████████████████████████████████| 62 kB 1.2 MB/s
Requirement already satisfied: idna<4,>=2.5 in /usr/lib/python3/dist-packages (from requests>=2.26.0->docker) (2.8)
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python3/dist-packages (from requests>=2.26.0->docker) (201
9.11.28)
Collecting charset-normalizer<4,>=2
  Downloading charset_normalizer-3.3.2-cp38-cp38-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (141 kB)
     |████████████████████████████████| 141 kB 50.2 MB/s
Installing collected packages: packaging, urllib3, charset-normalizer, requests, docker
  Attempting uninstall: urllib3
    Found existing installation: urllib3 1.25.8
    Not uninstalling urllib3 at /usr/lib/python3/dist-packages, outside environment /usr
    Can't uninstall 'urllib3'. No files were found to uninstall.
  Attempting uninstall: requests
    Found existing installation: requests 2.22.0
    Not uninstalling requests at /usr/lib/python3/dist-packages, outside environment /usr
    Can't uninstall 'requests'. No files were found to uninstall.
Successfully installed charset-normalizer-3.3.2 docker-7.0.0 packaging-24.0 requests-2.31.0 urllib3-2.2.1
```

Increasing the Virtual Machine allocated RAM Size

sudo sysctl -w vm.max_map_count=262144



Downloading the Docker Image that contain the ELK Stack



This Contain the ELK Server image that I am going to run

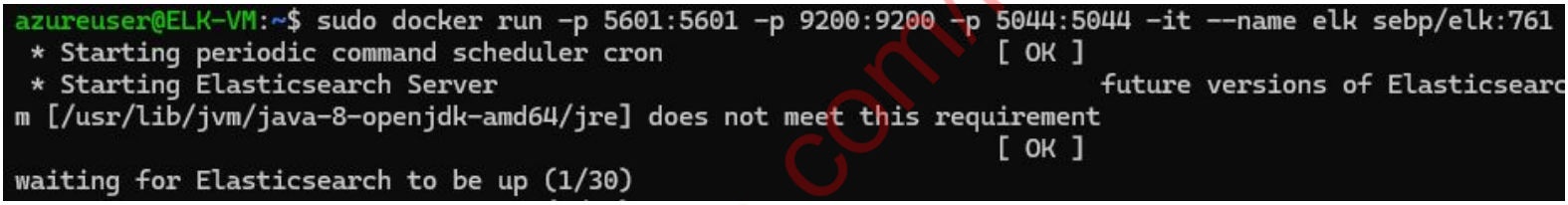
Allocating a port for the docker image to run

```
sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk:761
```

6501 port is for Kabana

9200 is for Elastic Search

5044 is for Logstash



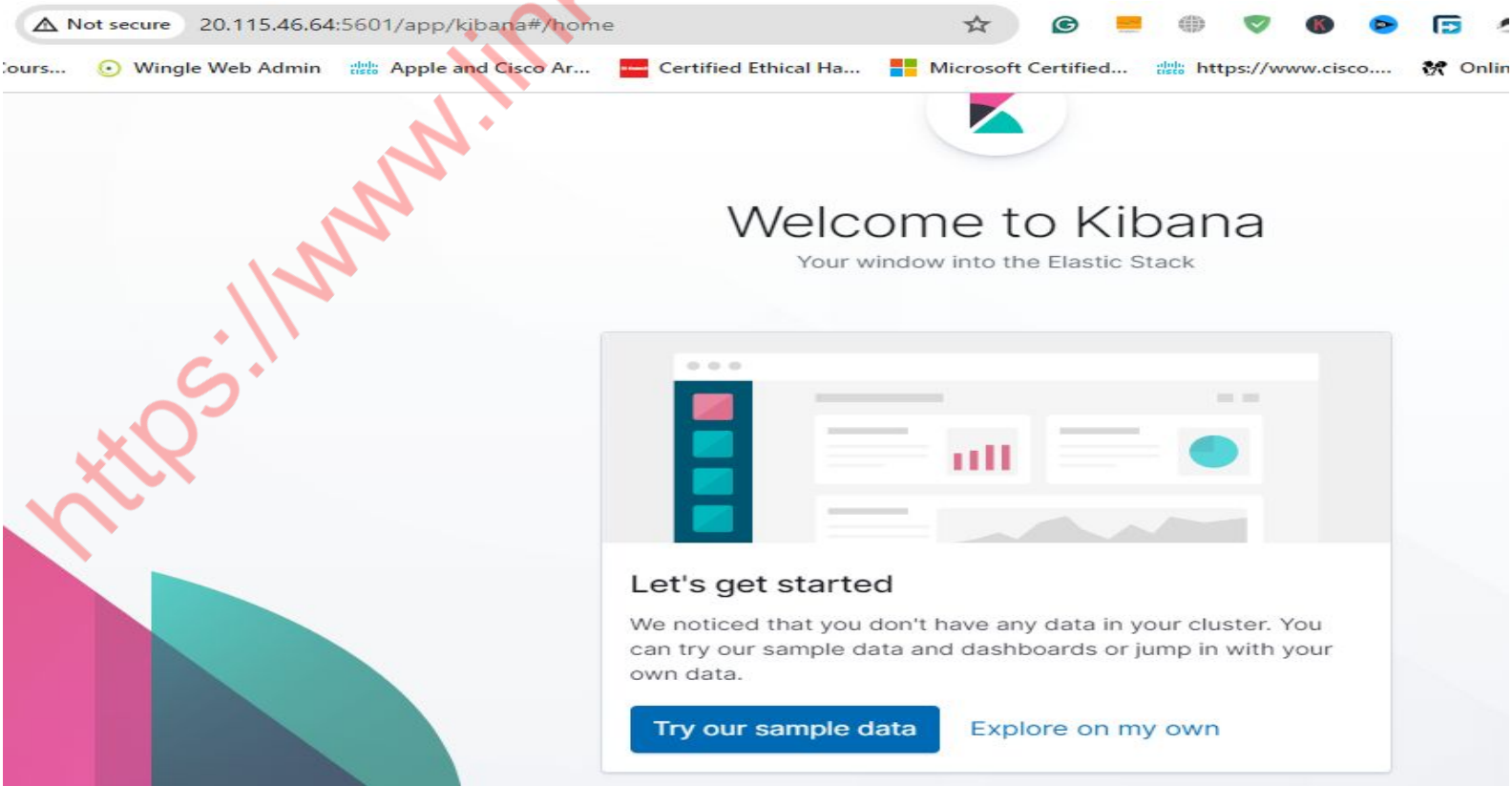
3.1.2 Screenshot

Set up routing to only allow traffic inbound to the server from both your virtual networks, and make sure Kibana is only accessible when you're on the network.

Creating inbound rule in ELK Server VM Network Security group for accessing Kabana landing page from my Laptop

170	AllowCidrBlockCustom5601Inbound5	5601	Any	203.101.190.186	Any	✓
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	
65500	DenyAllInBound	Any	Any	Any	Any	

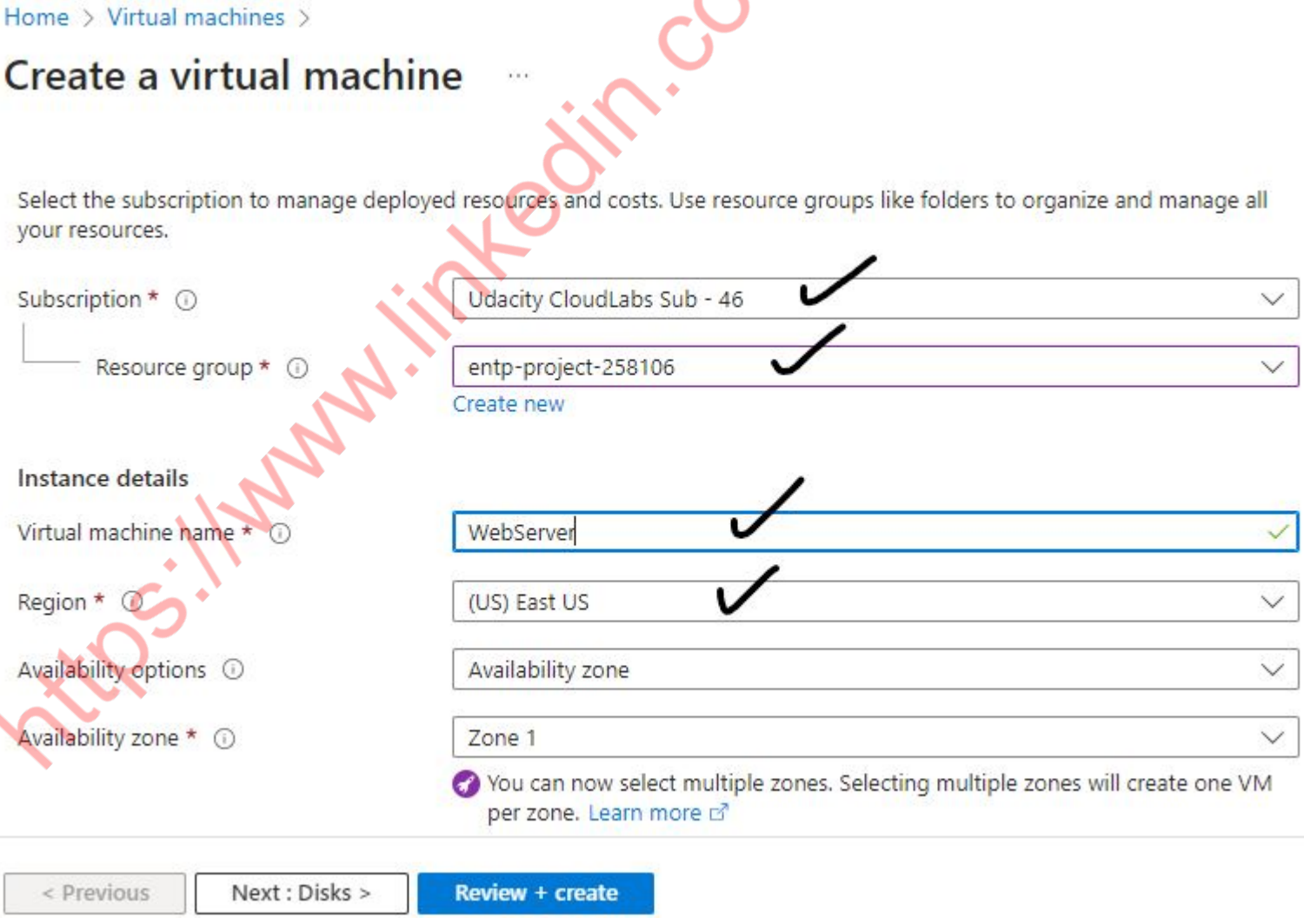
Outbound port rules (3)



Visualizing Web Server Logs into our ELK Server

First Creating Web Server

Creating it in the same virtual network as the ELK Server



Security type ⓘ — Trusted launch virtual machines

Configure security features

Image * ⓘ — Ubuntu Server 20.04 LTS - x64 Gen2

See all images | Configure VM generation

VM architecture ⓘ — Arm64 / x64

Run with Azure Spot discount ⓘ

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

See all sizes

Item(s) availability based on policy assignment(s) for the selected scope.
entp302-258106-PolicyDefinition-entp-project-258106 (Policy details)

Enable Hibernation (preview) ⓘ

Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. Learn more

Authentication type ⓘ — SSH public key / Password

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

Username * ⓘ — azureuser

SSH public key source — Use existing public key

SSH public key * ⓘ

```
51Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44
hp3Xd1OcHrAYR6NAi6EHY0GsdlxTqnhG5wFUsdaLt3MEC1MBUiM/4hbbcrtN
AzHpRsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMZpf0= hazra@Eagle
```

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 * ⓘ — None / Allow selected ports

Select inbound ports * — SSH (22)

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

< Previous | Next : Disks > | Review + create

Network Settings

Network interface

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

Virtual network * ⓘ — ELK_VirtualNetwork
Create new

Subnet * ⓘ — default (10.0.0.0/24)
Manage subnet configuration

Public IP ⓘ — (new) WebServer-ip
Create new

NIC network security group ⓘ
- ○ None
- ○ Basic
- ◉ Advanced ✓

Configure network security group * — NetworkSecrityGroupPrivateDMZ ✓
Create new

Delete public IP and NIC when VM is deleted ⓘ ☐

Enable 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

Load balancing options ⓘ
- ◉ None
- ○ Azure load balancer

< Previous | Next : Management > | Review + create ✓

Setting up the web server

SSH into web Server

```
azureuser@I  azureuser@I  azureuser@
PS C:\Users\hazra> ssh azureuser@20.51.200.144
The authenticity of host '20.51.200.144 (20.51.200.144)' can't be establ
ished.
ED25519 key fingerprint is SHA256:U7Den8JUOwfaOivlPNqNayVeQ0zm4+dDM3q4u1
x9voU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.51.200.144' (ED25519) to the list of know
n hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1060-azure x86_64)
```

Installing Apache
Sudo apt install apache2

```
azureuser@WebServer:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0
  ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
  www-browser openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libjansson4 liblua5.2-0
  ssl-cert
0 upgraded, 11 newly installed, 0 to remove and 28 not upgraded.
Need to get 1873 kB of archives.
After this operation, 8118 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Starting the Apache2 Service

```
azureuser@WebServer:~$ sudo service apache2 start
```

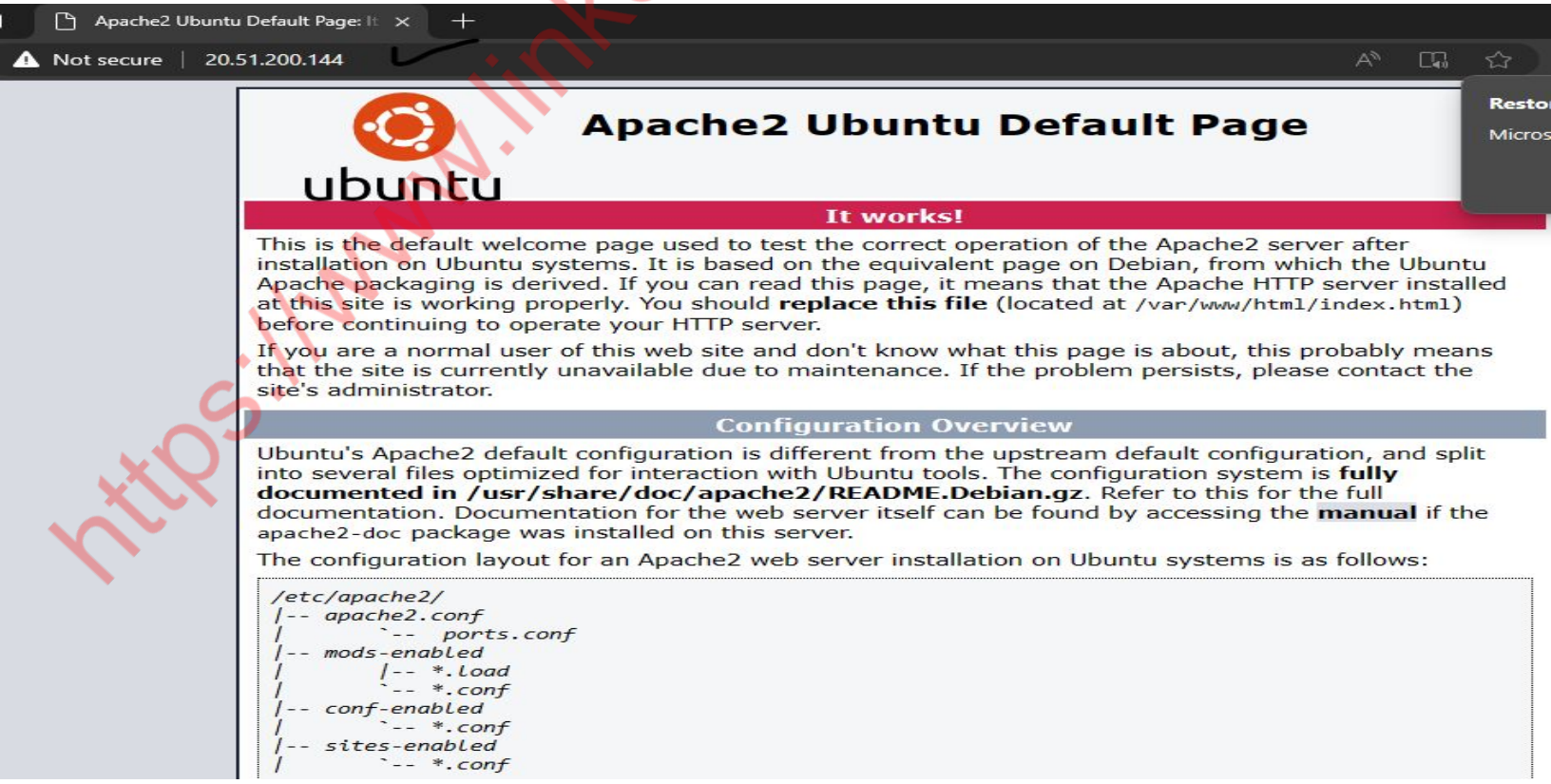
Checking the status of Apache2 Service

```
azureuser@WebServer:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2024-04-21 23:46:27 UTC; 8min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 3690 (apache2)
      Tasks: 55 (limit: 1002)
     Memory: 11.1M
     CGroup: /system.slice/apache2.service
             ├─3690 /usr/sbin/apache2 -k start
             ├─3693 /usr/sbin/apache2 -k start
             └─3694 /usr/sbin/apache2 -k start

Apr 21 23:46:27 WebServer systemd[1]: Starting The Apache HTTP Server...
Apr 21 23:46:27 WebServer systemd[1]: Started The Apache HTTP Server.
```

Creating inbound rule for HTTP port 80 In network Security group of Web Server Virtual Machine

120	AllowAnyHTTPInbound	80	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNe
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoa
65500	DenyAllInBound	Any	Any	Any

Now copy the public IP of web server and paste it in the browser. You will see a landing page will appear.



3.2 Ingest Logs

In this next section, you will start setting up ingest sources for your ELK server.

Insert screenshots on the following pages, showing completion of each of the specified tasks.

3.2.1 Screenshot

Install Filebeat on your web servers and show the Filebeat service as active.

Following Commands will be used for installing Filebeat

```
Command Sheet for installing Filebeat:



Install & start Apache2 on the webserver

curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.de
b

sudo dpkg -i filebeat-7.4.0-amd64.deb

cd /etc/filebeat

edit filebeat.yml and change the value for output.elasticsearch and
setup.kibana to reflect the IP of your Elk server

sudo filebeat modules enable system

sudo filebeat modules enable apache

sudo filebeat setup

sudo service filebeat start
```

Installing Filebeat for long ingestion

```
curl -L -O
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.de
b
```

```
azureuser@WebServer:~$ curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 23.1M  100 23.1M    0     0  35.9M      0 --:--:-- --:--:-- --:--:-- 35.9M
```

```
sudo dpkg -i filebeat-7.4.0-amd64.deb
```

```
azureuser@WebServer:~$ sudo dpkg -i filebeat-7.4.0-amd64.deb
Selecting previously unselected package filebeat.
(Reading database ... 59667 files and directories currently installed.)
Preparing to unpack filebeat-7.4.0-amd64.deb ...
Unpacking filebeat (7.4.0) ...
Setting up filebeat (7.4.0) ...
Processing triggers for systemd (245.4-4ubuntu3.23) ...
```

Navigating to the filebeat directory

```
azureuser@WebServer:~$ cd /etc/filebeat/
azureuser@WebServer:/etc/filebeat$
```

```
azureuser@WebServer:/etc/filebeat$ ls
fields.yml  filebeat.reference.yml  filebeat.yml  modules.d
```

3.2.2 Screenshot

Configure Filebeat to route web server logs to Elasticsearch.

Editing filebeat.yml file

Editing filebeat.yml and changing the value for output.elasticsearch and setup.kibana to the IP of Elk server

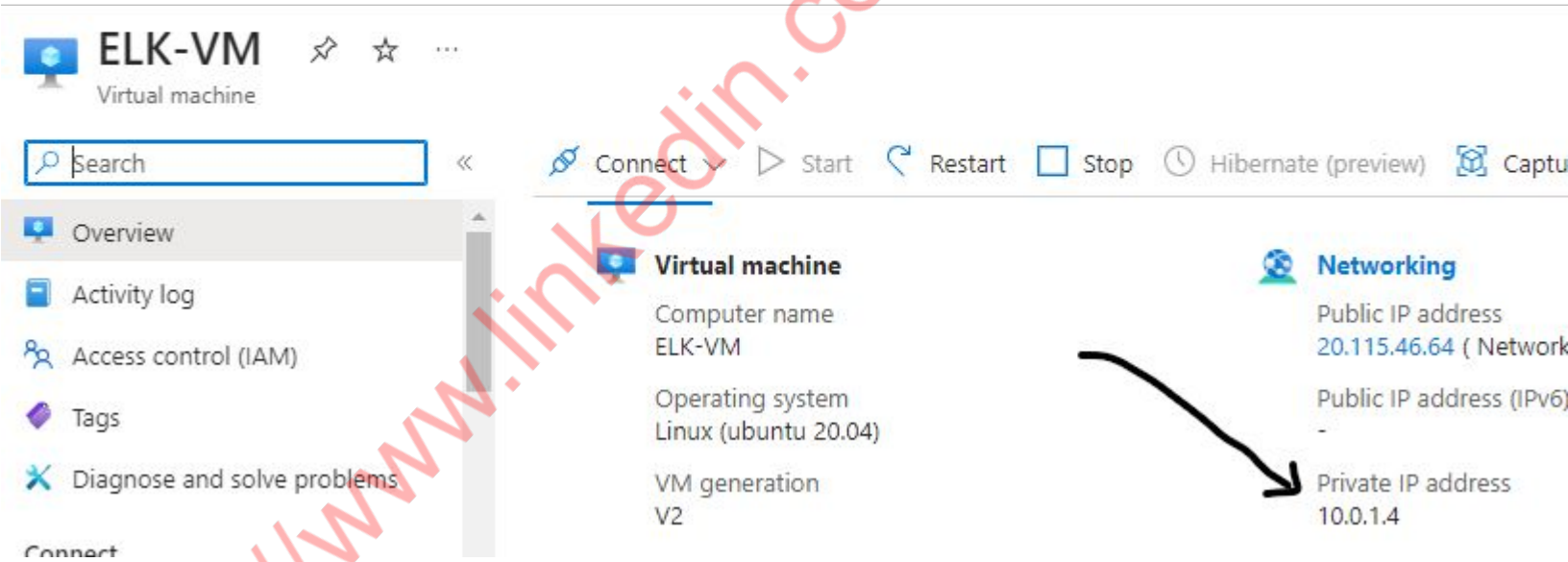
```
azureuser@WebServer:/etc/filebeat$ sudo nano filebeat.yml
```

Search for output.elastic

```
# These settings simplify using Filebeat with the Elastic Cloud (https://cloud.elas

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

Search [output.elastic]: output.elastic
^G Get Help   M-C Case Sens   M-B Backwards   ^P Older
^C Cancel     M-R Regexp      ^R Replace      ^N Newer
```

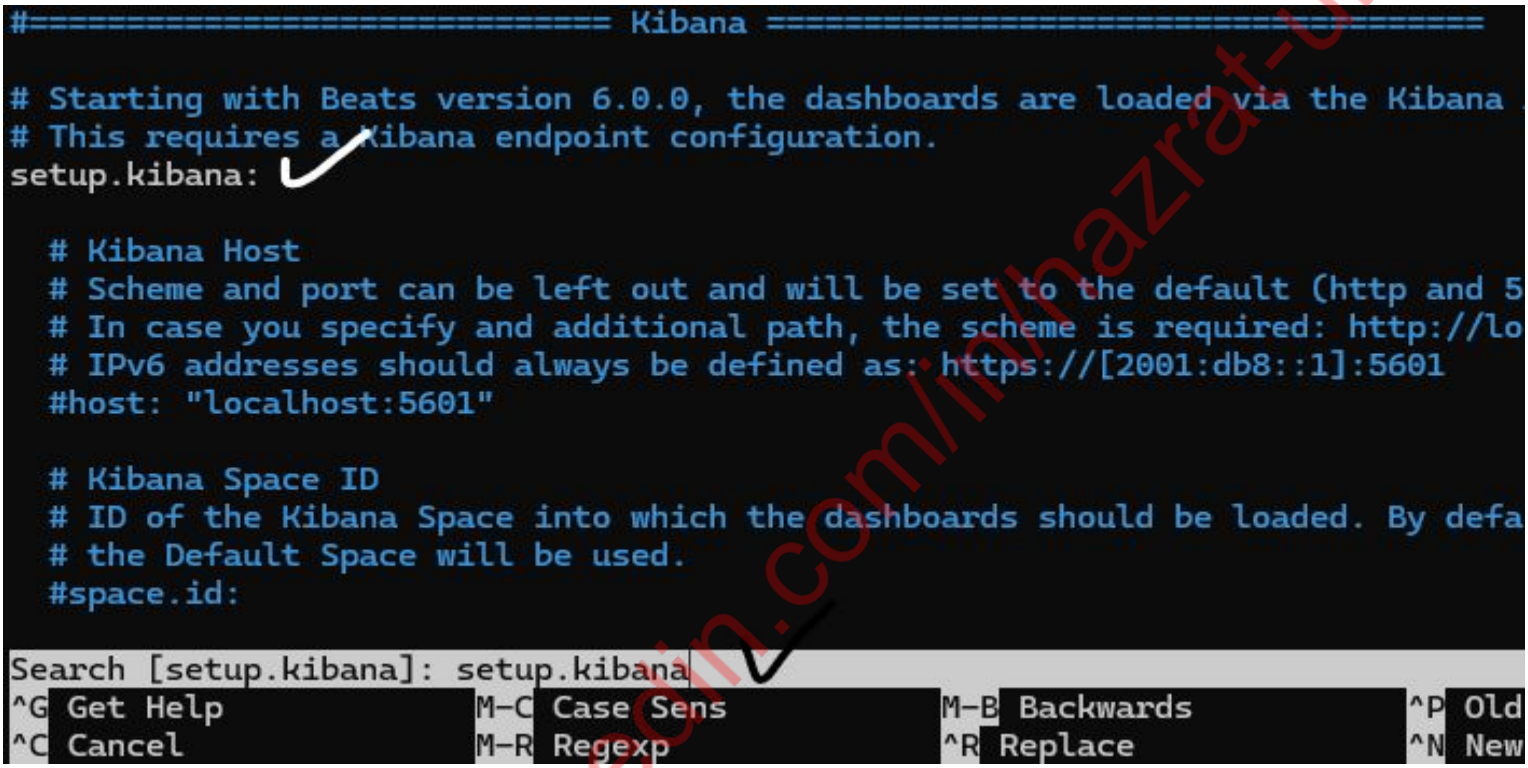
Replace Localhost with ELK Server Private IP

```
#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["localhost:9200"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"
```




```
# Configure what output to use when sending the da

#-------------------------- Elasticsearch output -
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.0.1.4:9200"]

  # Optional protocol and basic auth credentials.
```

Search for setup.kibana



Write the following line below setup.kabana
host:"ELK SERVERIP:5601"

Enable Filebeat module for Apache and for System

Enabling System Module

Sudo filebeat modules enable system

```
azureuser@WebServer:/etc/filebeat$ sudo filebeat modules enable system
Enabled system
azureuser@WebServer:/etc/filebeat$
```

Enabling Moduel for Apache

Sudo filebeat modules enable apache

```
azureuser@WebServer:/etc/filebeat$ sudo filebeat modules enable apache
Enabled apache
```

These modules enables filebeat to locate logs specific to system and Apache. Then forward these logs to elastic search

```
azureuser@WebServer:/etc/filebeat$ sudo filebeat setup
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
```

This command will start the installation setup for filebeat.

Starting the filebeat process

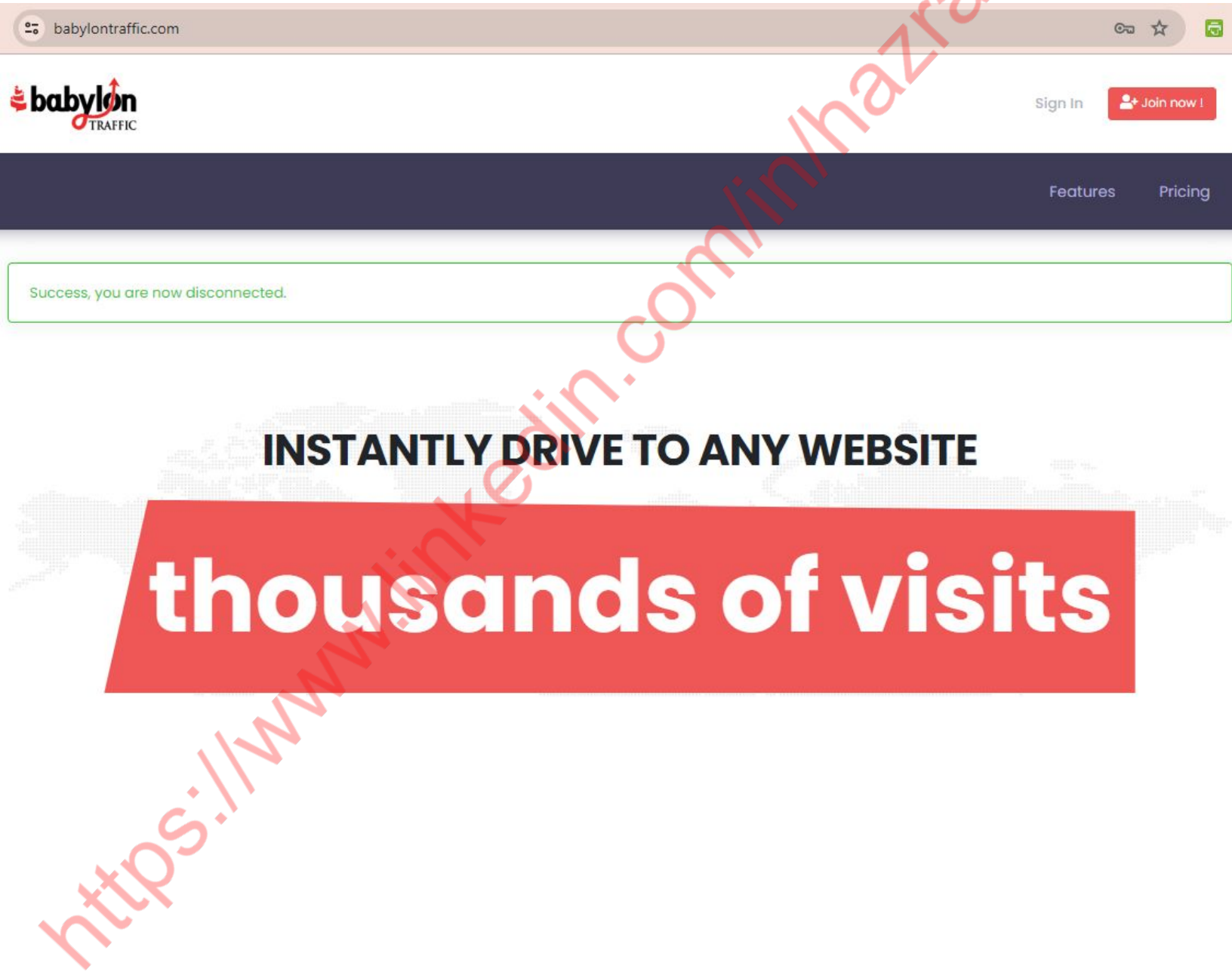
sudo service filebeat start

```
azureuser@WebServer:/$ sudo service filebeat start
azureuser@WebServer:/$
```

3.2.3 Screenshot

Simulate web traffic to your web servers using https://www.babylontraffic.com.

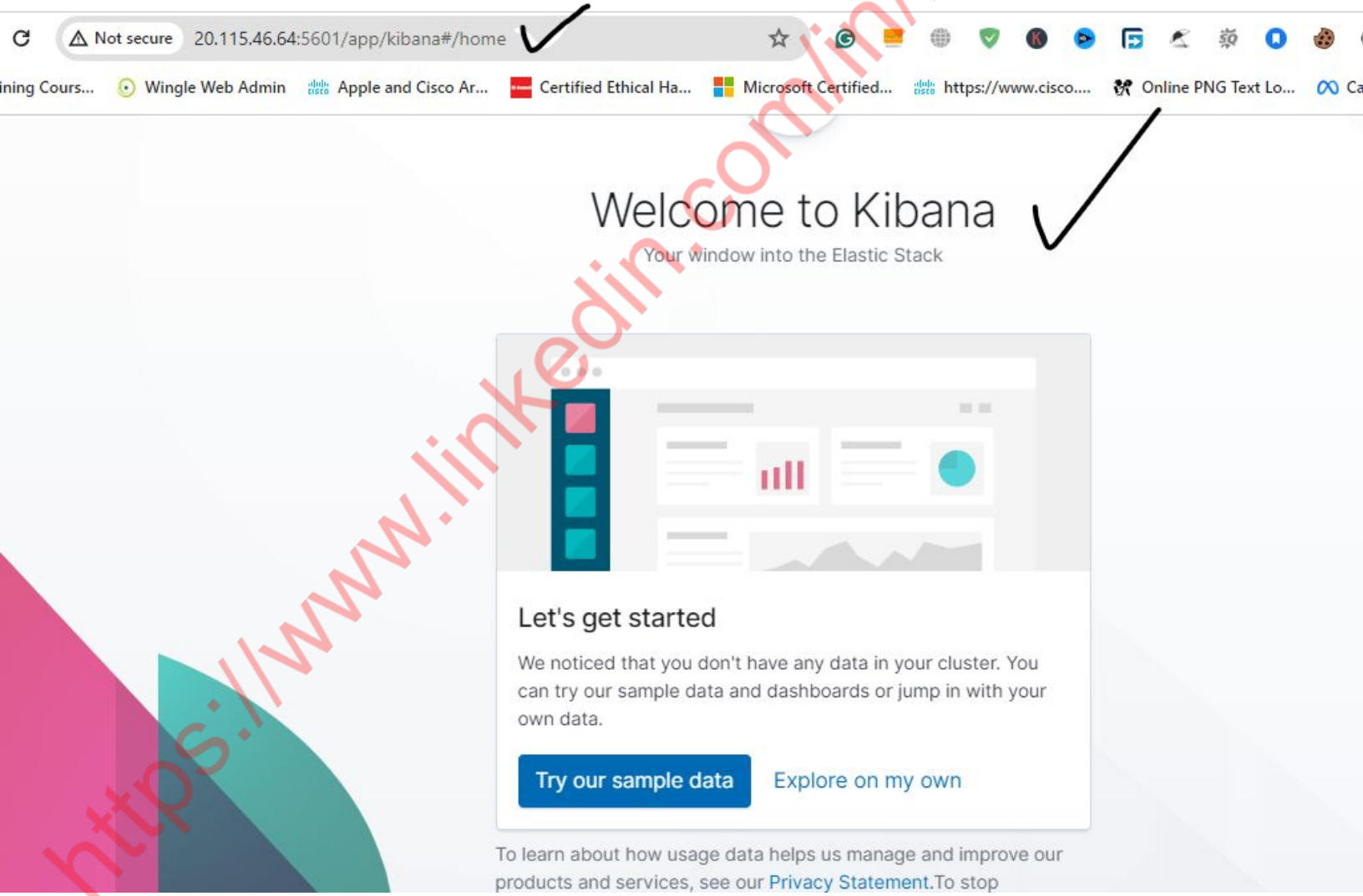
Simulating Weg Traffic using the above site



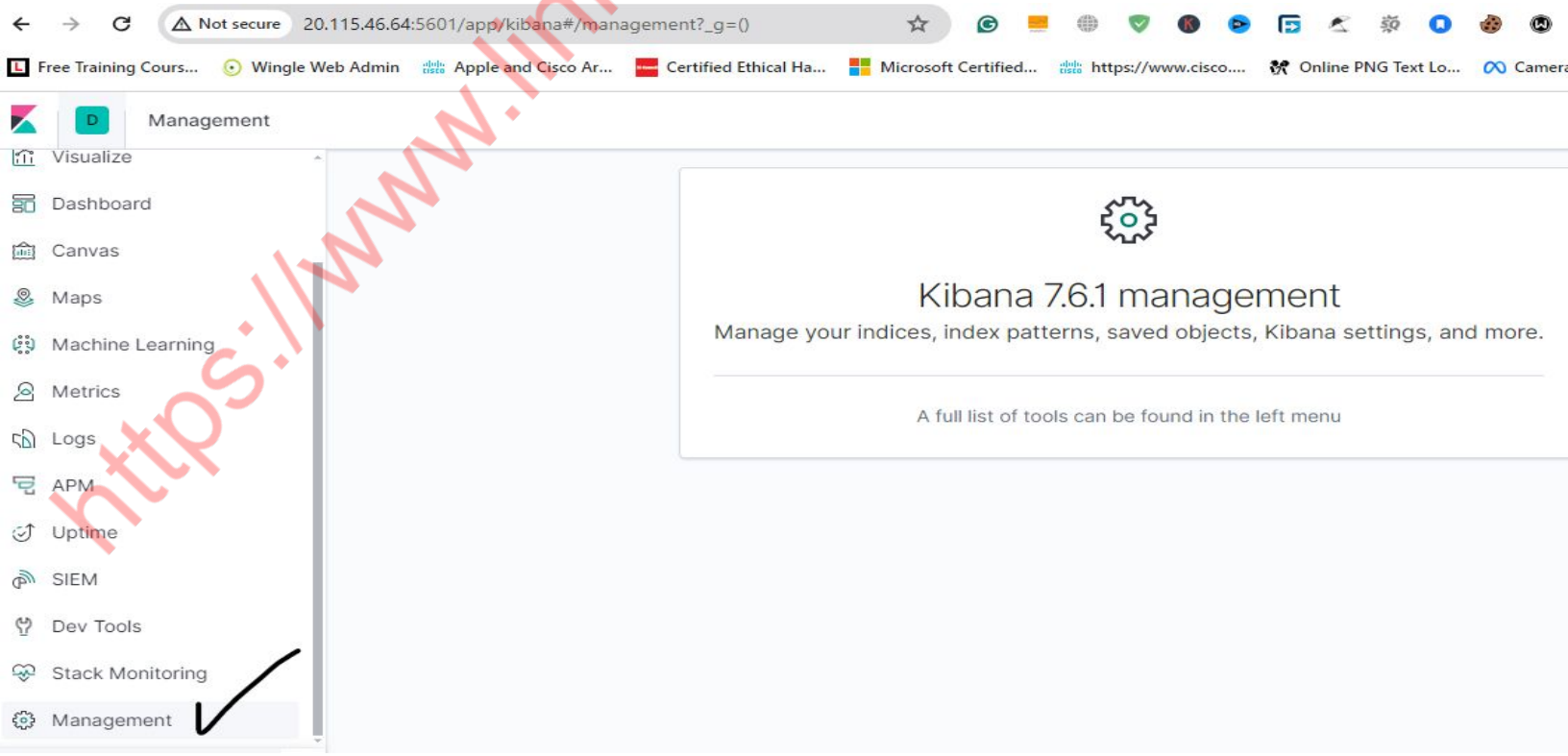
3.2.4 Screenshot

Web server logs appear in Kibana.

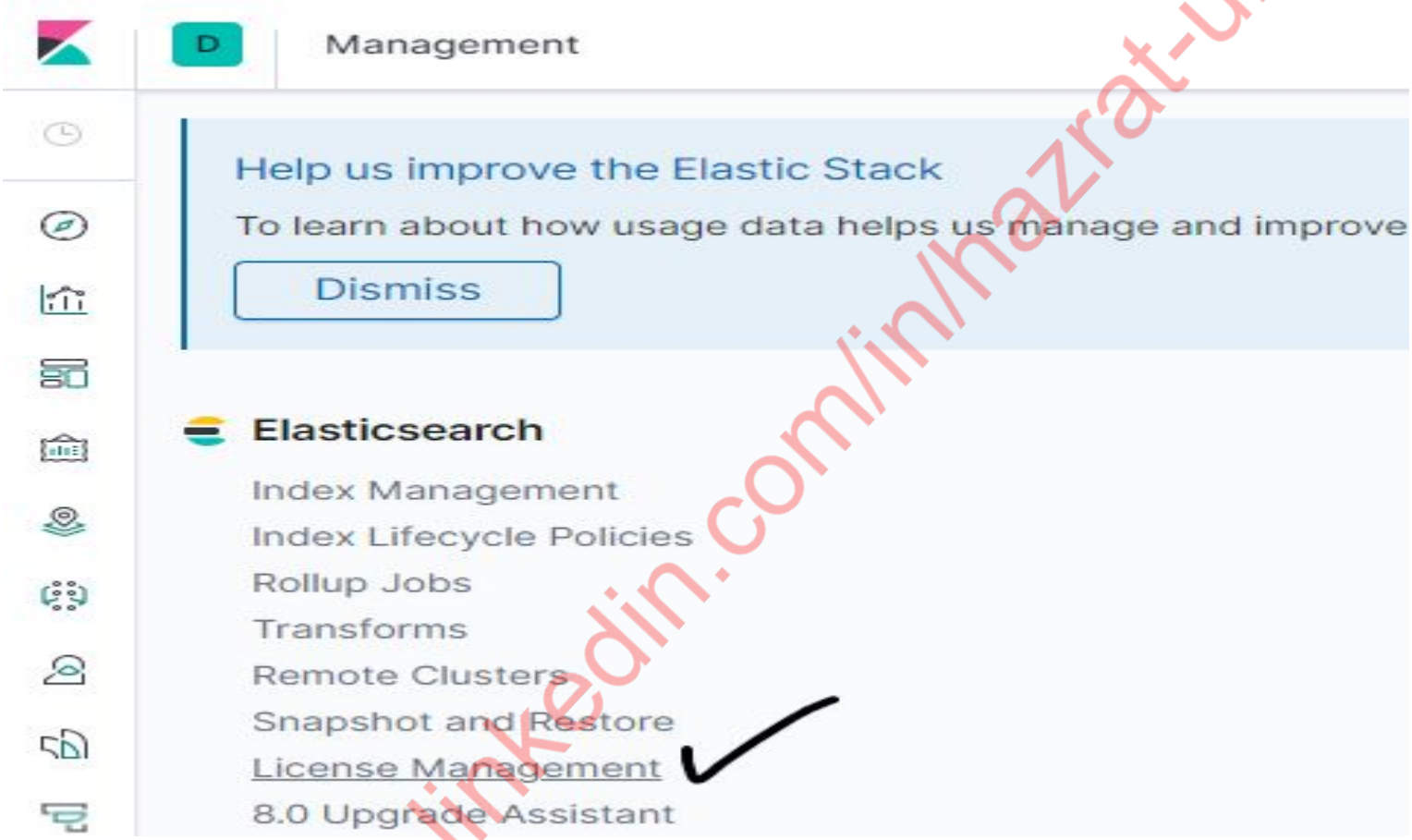
Accessing Kibana
Copy the public IP of ELK Server
Go to your browser and paste that IP along with Kibana port
You will see a Kibana screen



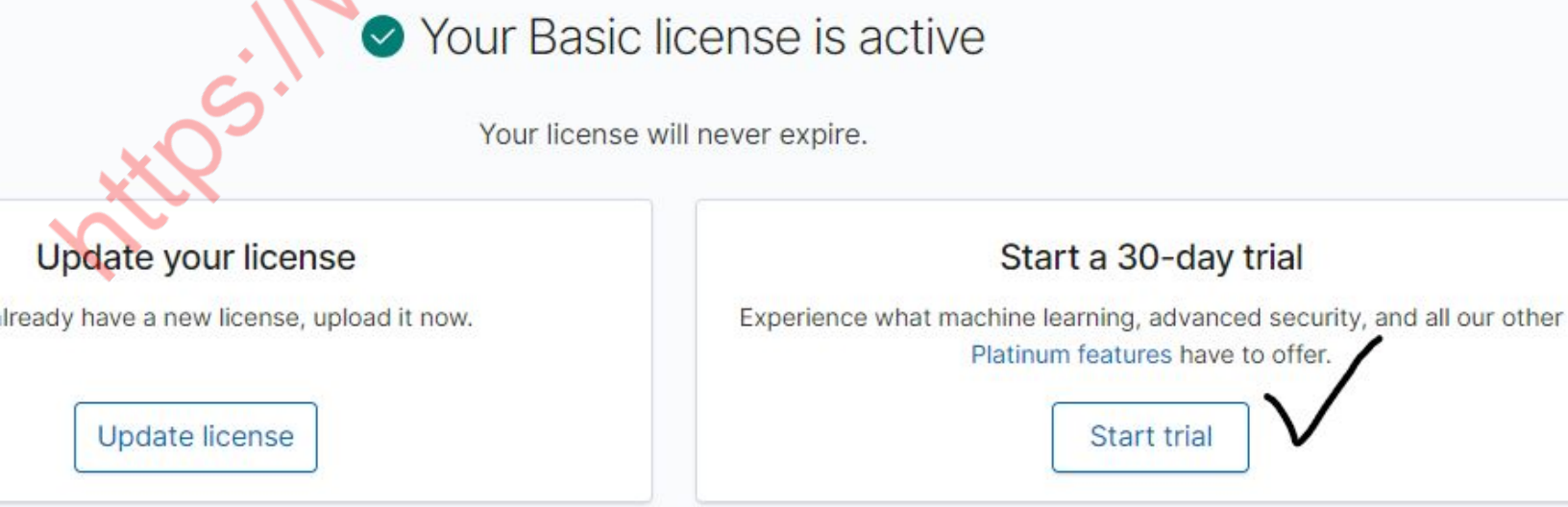
Click on Explore on my Own



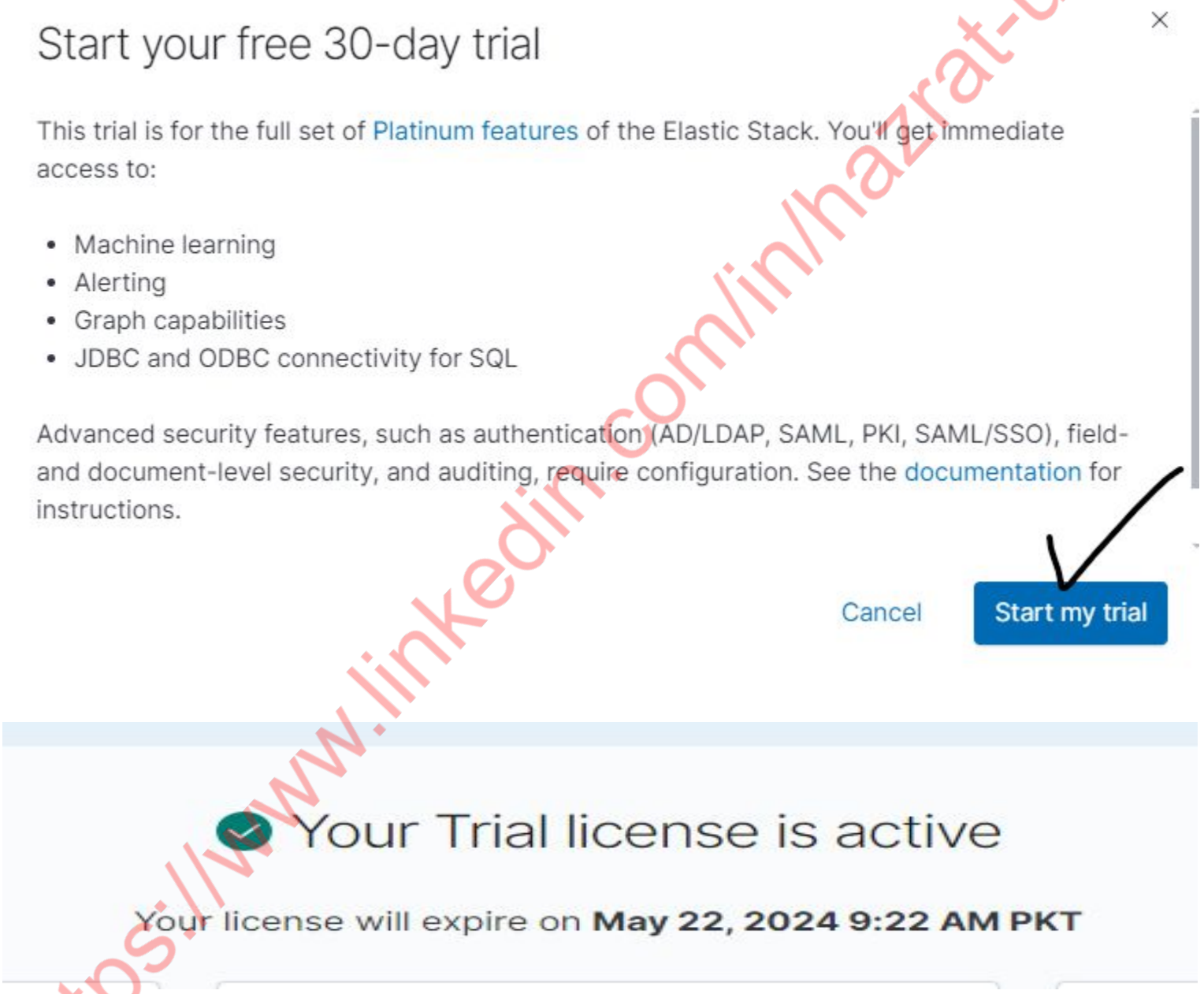
Licence Mangement



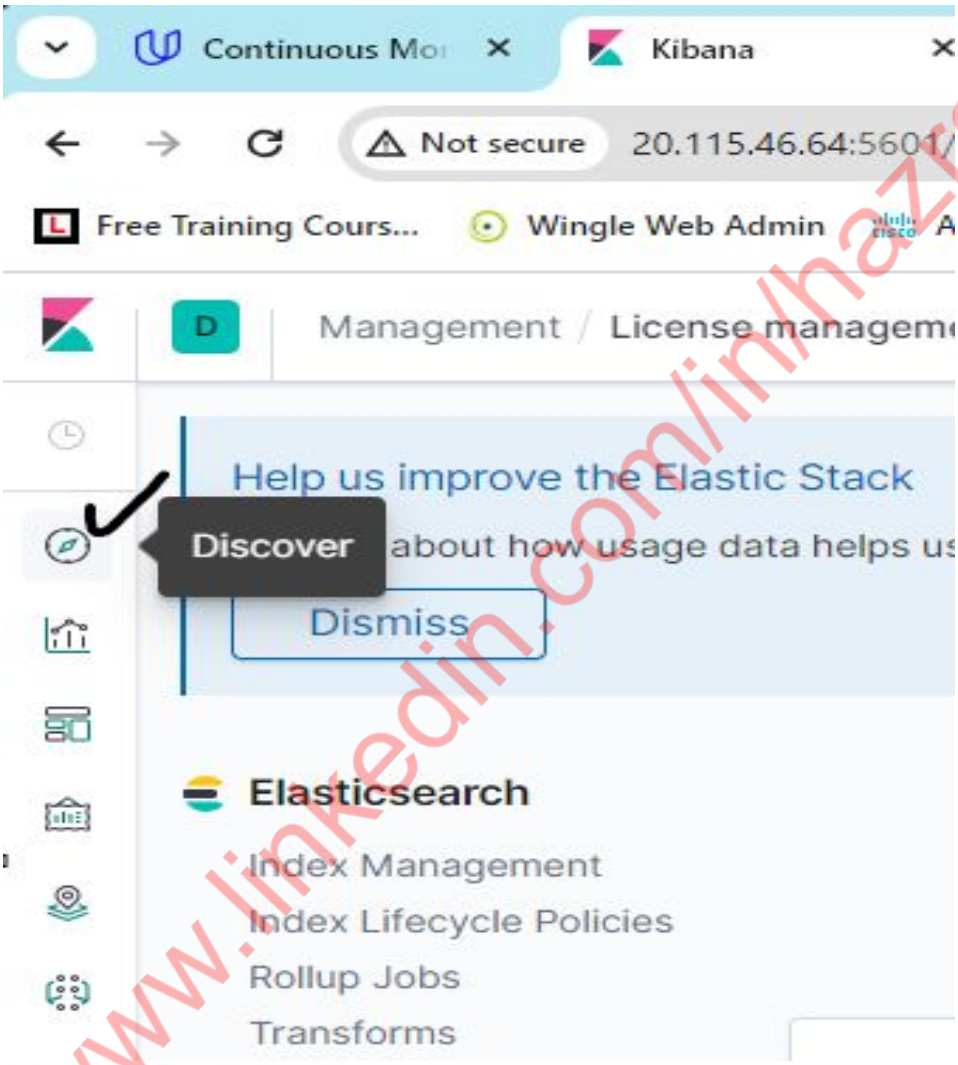
Click on start 30 days trial

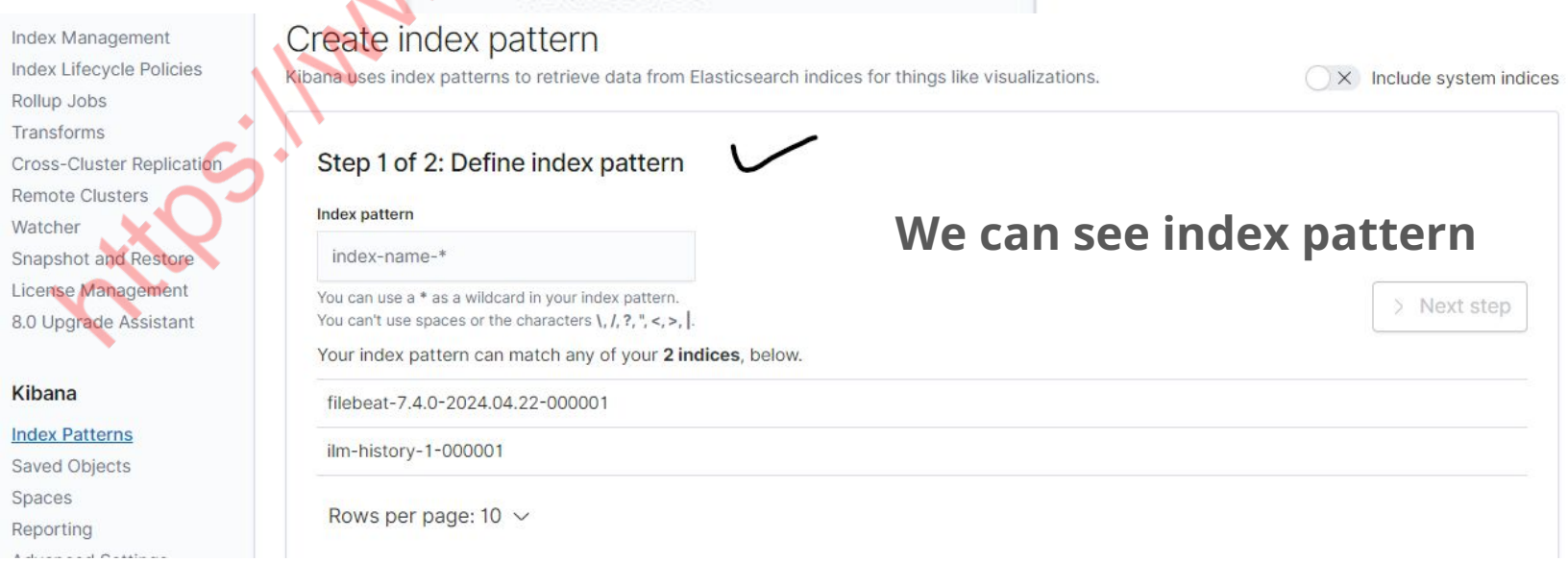


Start 30 Days Trial



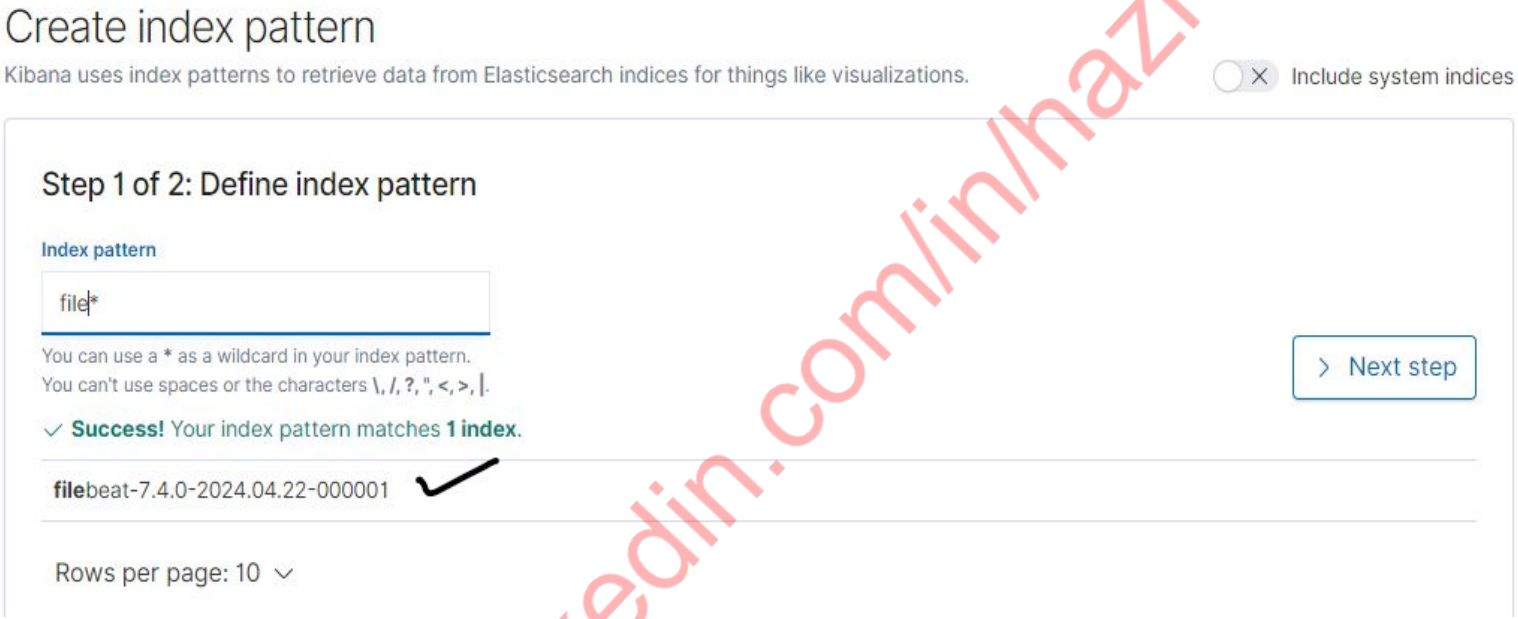
Click on Discover



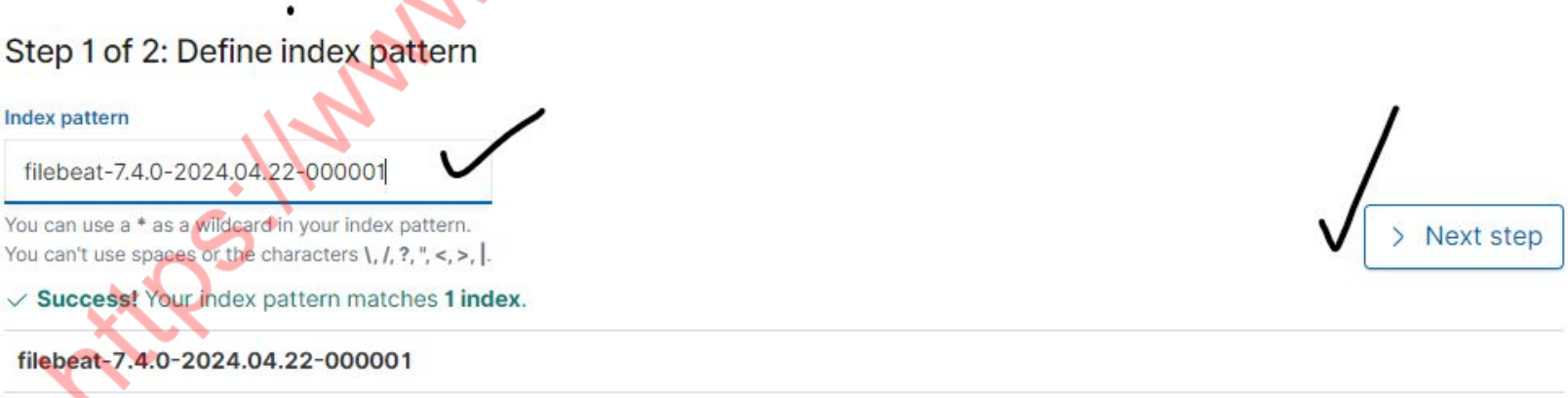


Defining Index Pattern

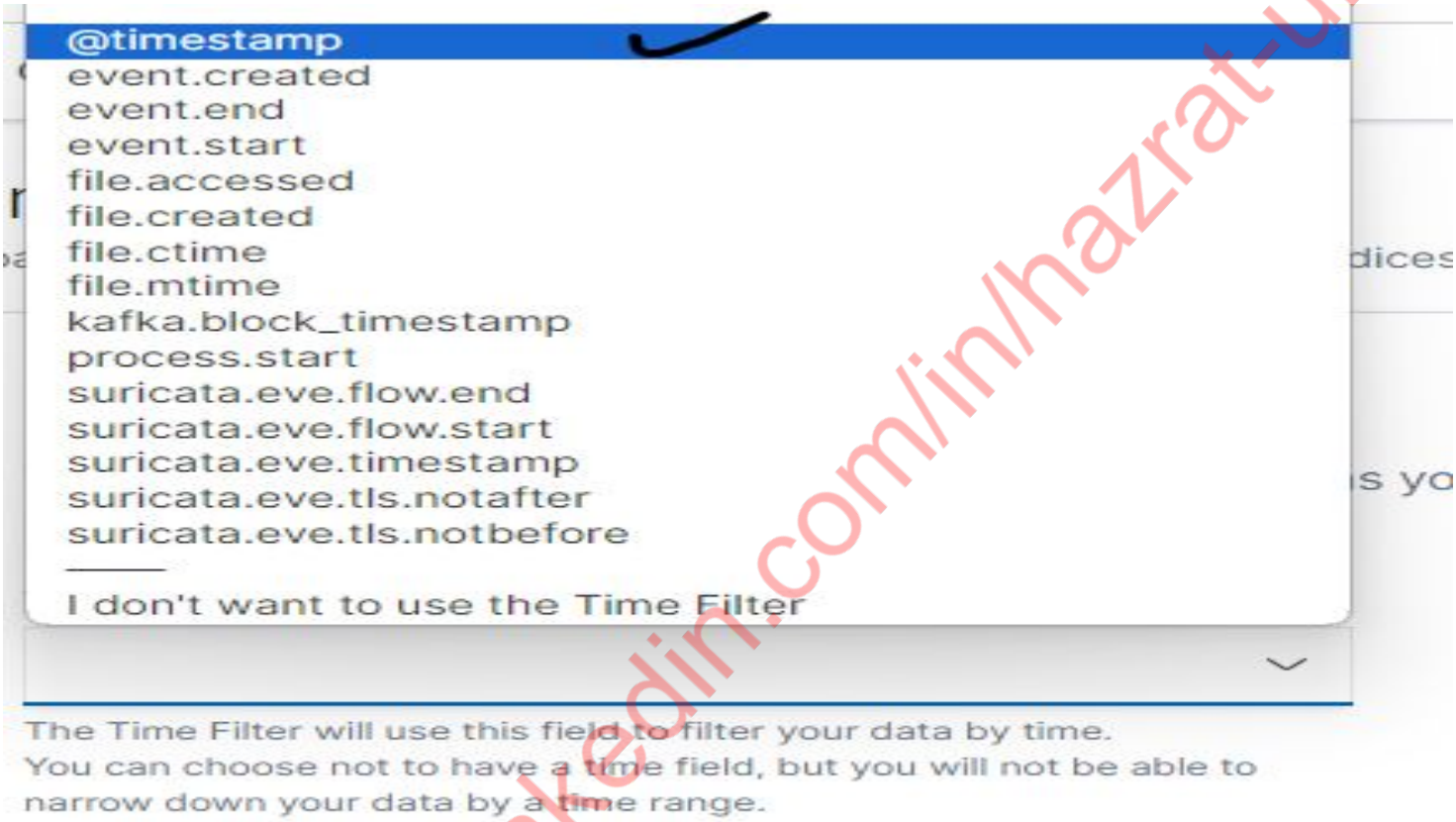
Type file the filebeat pattern will



Paste it and select next



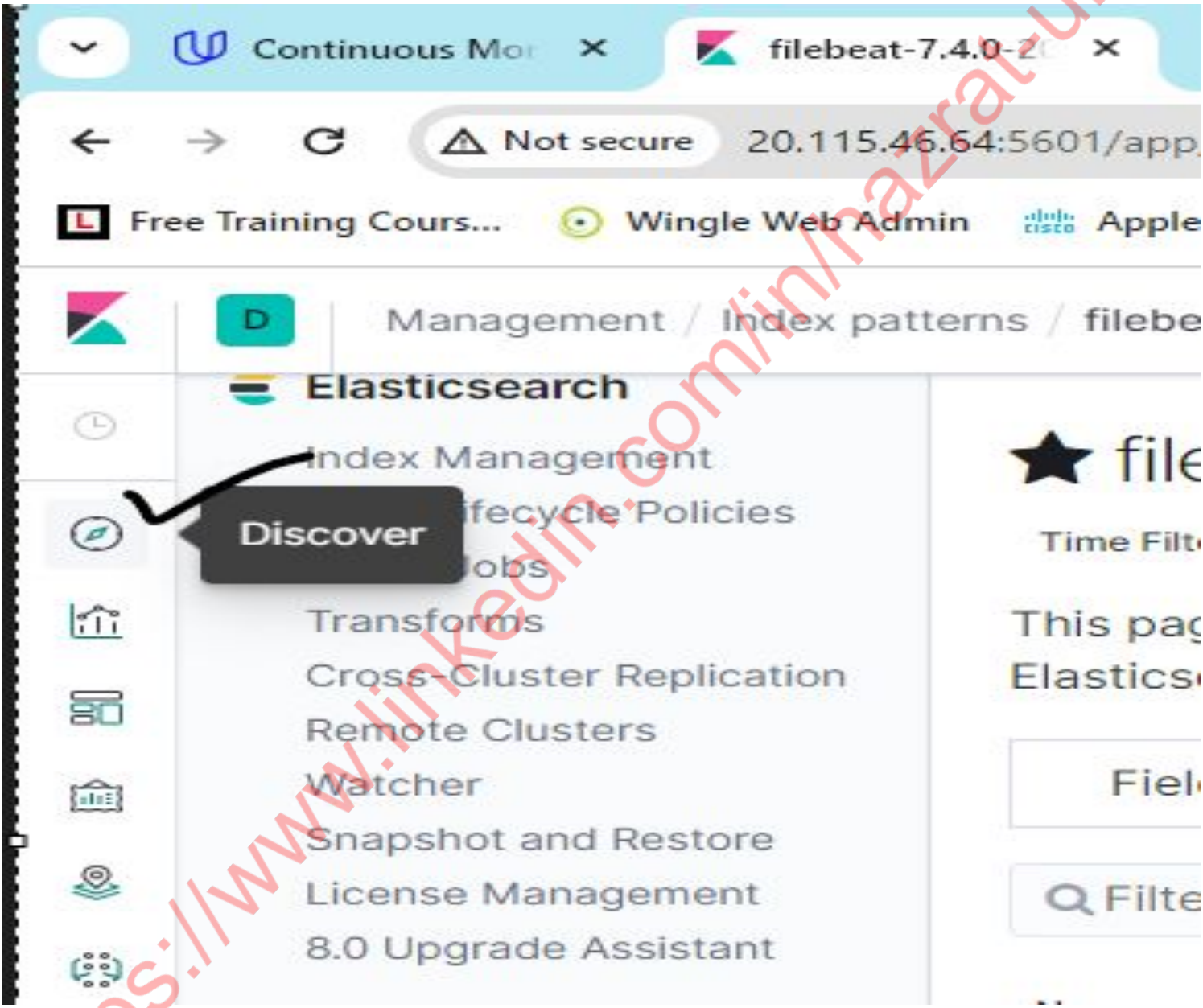
Select @timestap



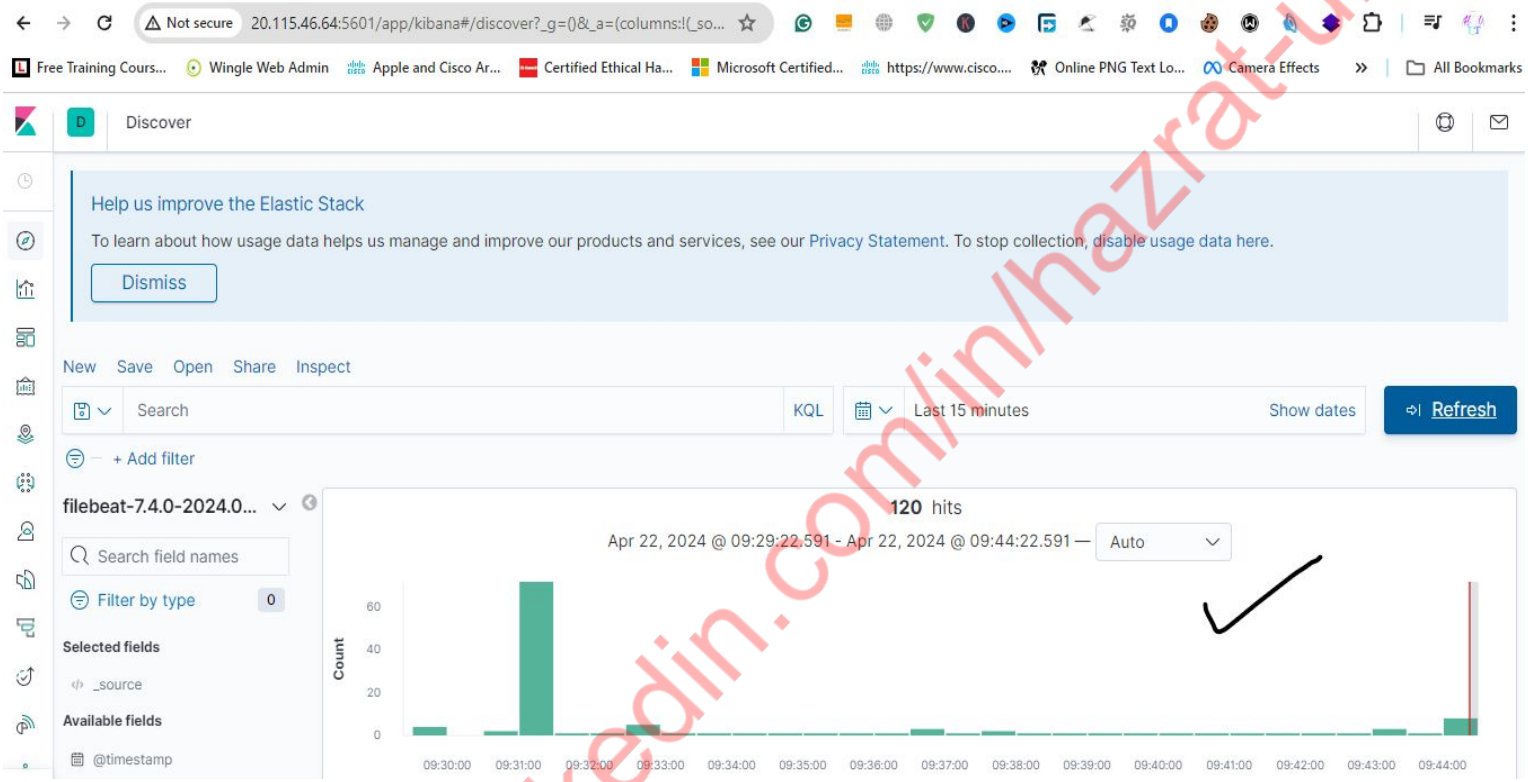
Then click on create index pattern

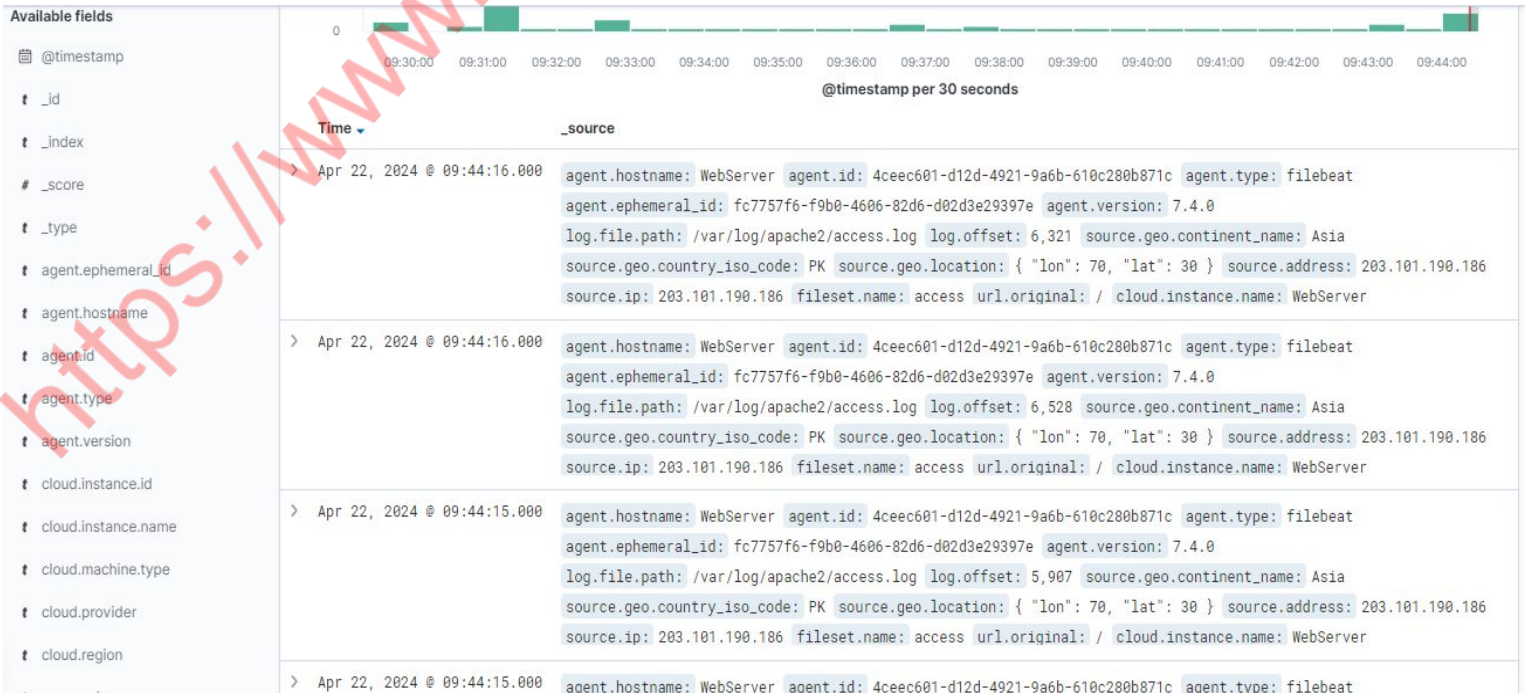
Index pattern generated

Now Click on Discover



We are able to visualize our web server logs





3.3 Build Alerts

In this next section, you will create alerts on the simulated web traffic you see. Build alerts to alert you of possible DoS, brute force, and probing attacks.

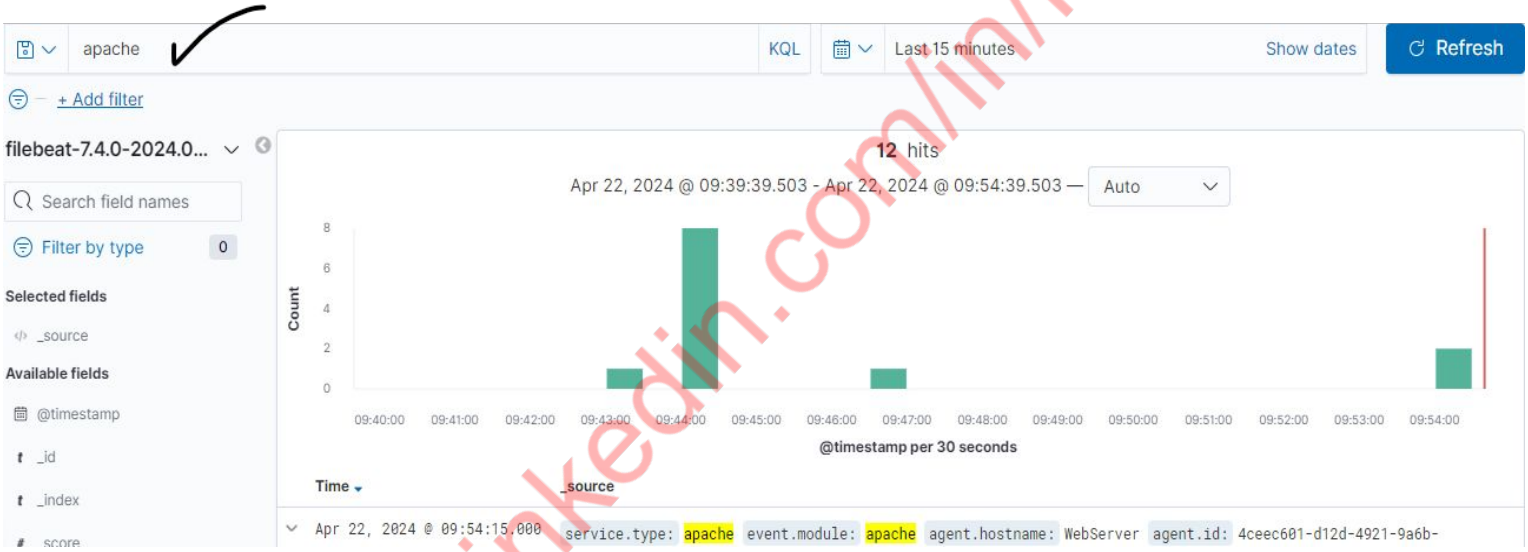
Insert screenshots on the following pages, showing completion of each of the specified tasks.

3.3.1 Screenshot

Create an alert for DoS attack.

STeps:

Searching for APache in the search bar to show only Apache logs



Apr 22, 2024 @ 09:54:15.000 service.type: apache event.module: apache agent.hostname: WebServer agent.id: 4ceec601-d12d-4921-9a6b-610c280b871c agent.type: filebeat agent.ephemeral_id: fc7757f6-f9b0-4606-82d6-d02d3e29397e agent.version: 7 log.file.path: /var/log/apache2/access.log log.offset: 7,148 source.geo.continent_name: North America source.geo.country_iso_code: CA source.geo.location: { "lon": -79.3716, "lat": 43.6319 } source.as.number: 21,992 source.as.organization.name: eHealth Ontario source.address: 205.210.31.148

Expanded document View surrounding documents View single docume

Table JSON

Now Expand one of the Apache log

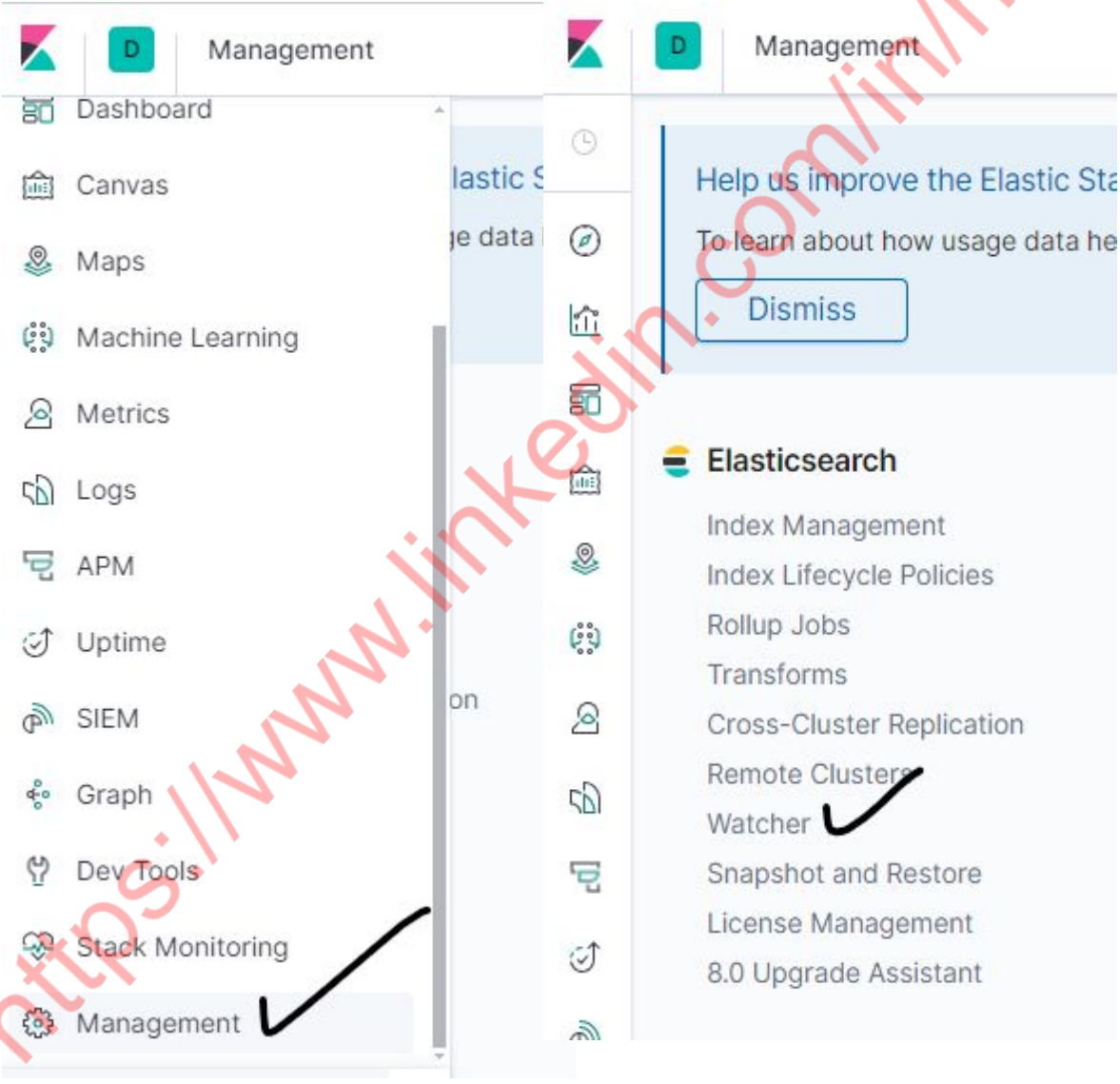
If someone is requesting to our Site it will be a an indicator for an alert. We can create an alert when someone Get Request to our site

t	host.os.name	Ubuntu
t	host.os.platform	ubuntu
t	host.os.version	20.04.6 LTS (Focal Fossa)
t	http.request.method	GET
t	http.request.referrer	-

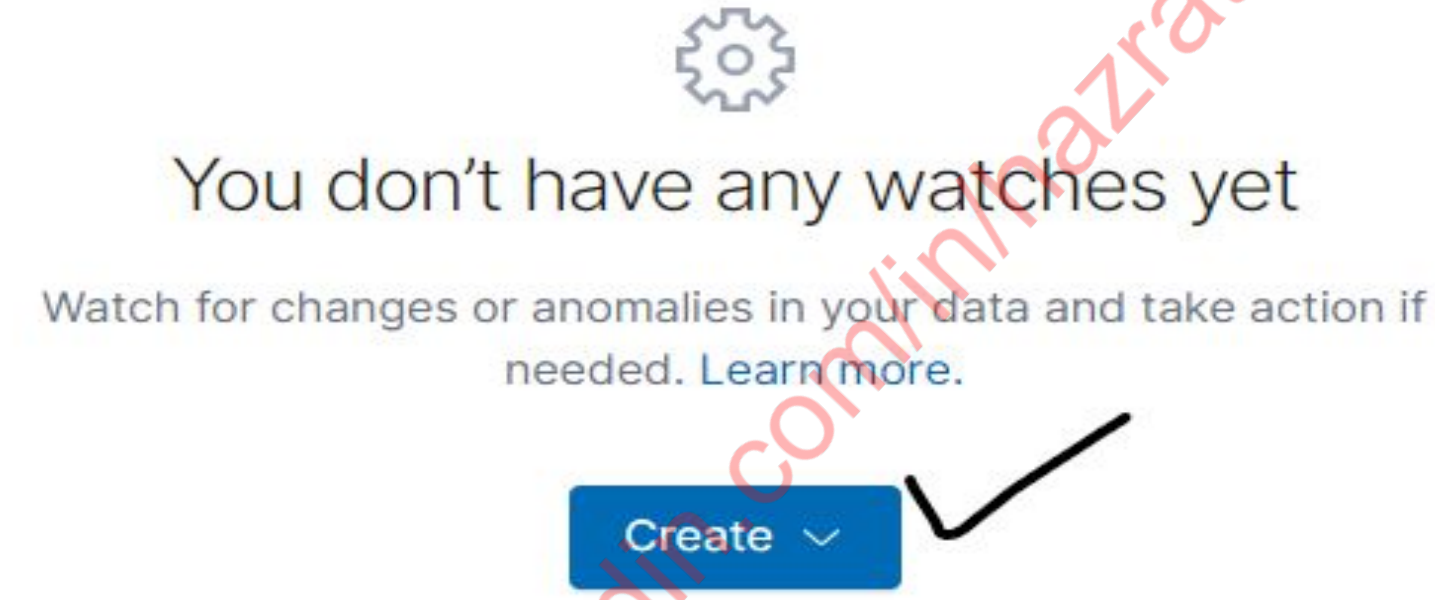
Creating an alert for DOS attack

Go to Management

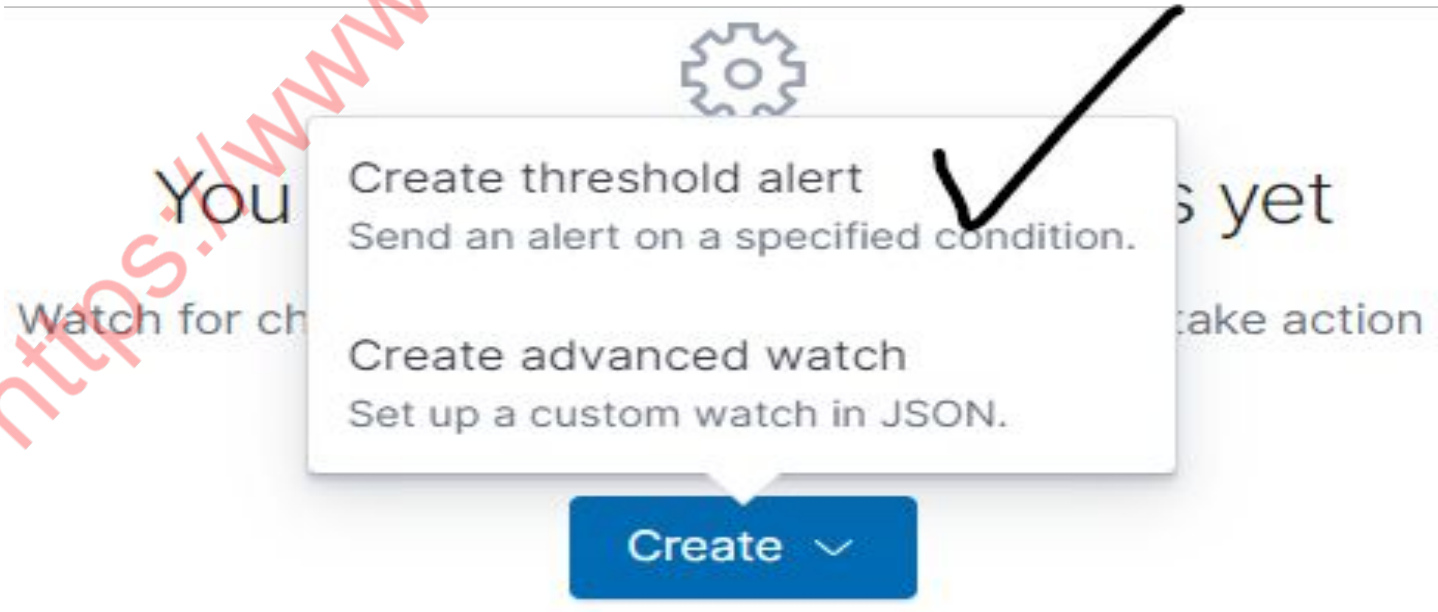
Click on Watcher



Click on Create



Select threshold Alert



Creating alert for Dos Attack

Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

DOS Attack

Indices to query

filebeat-7.4.0-2024.04.22-000001 ×

Use * to broaden your query.

Time field

@timestamp

Run watch every

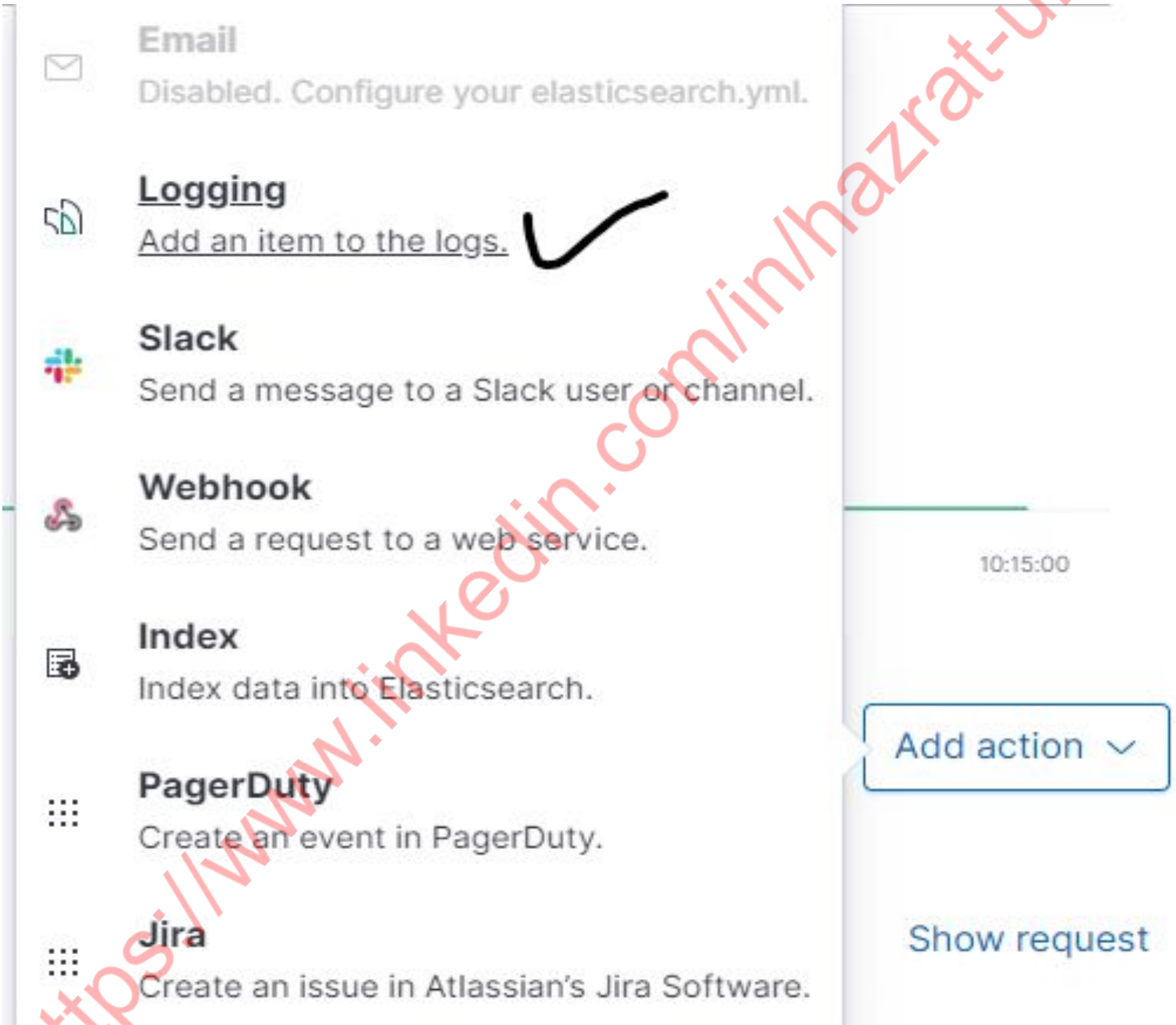
1

Match the following condition

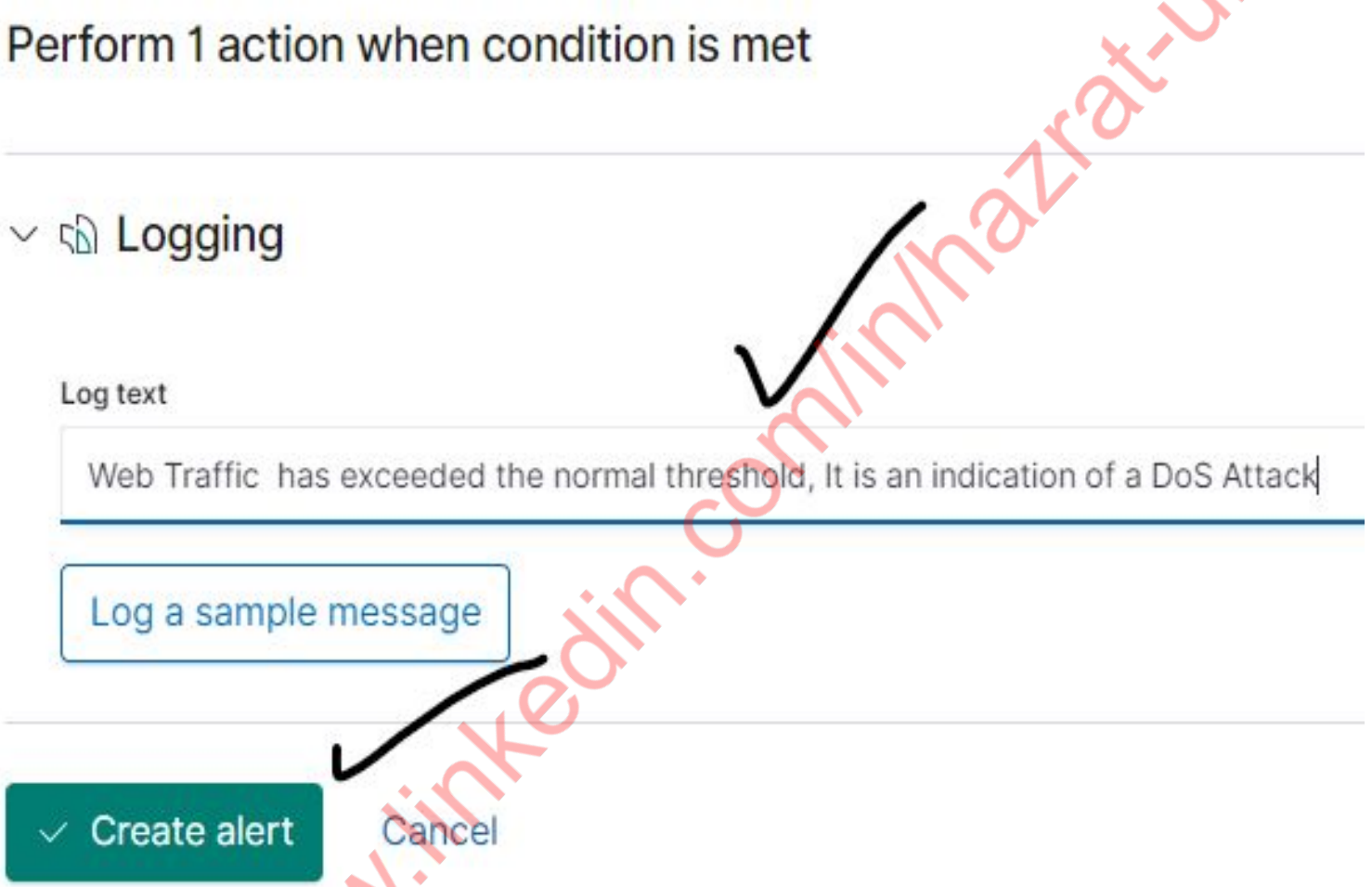
```
WHEN count() GROUPED OVER top 5 'http.request.method' IS ABOVE 1000 FOR THE LAST 5 minutes
```

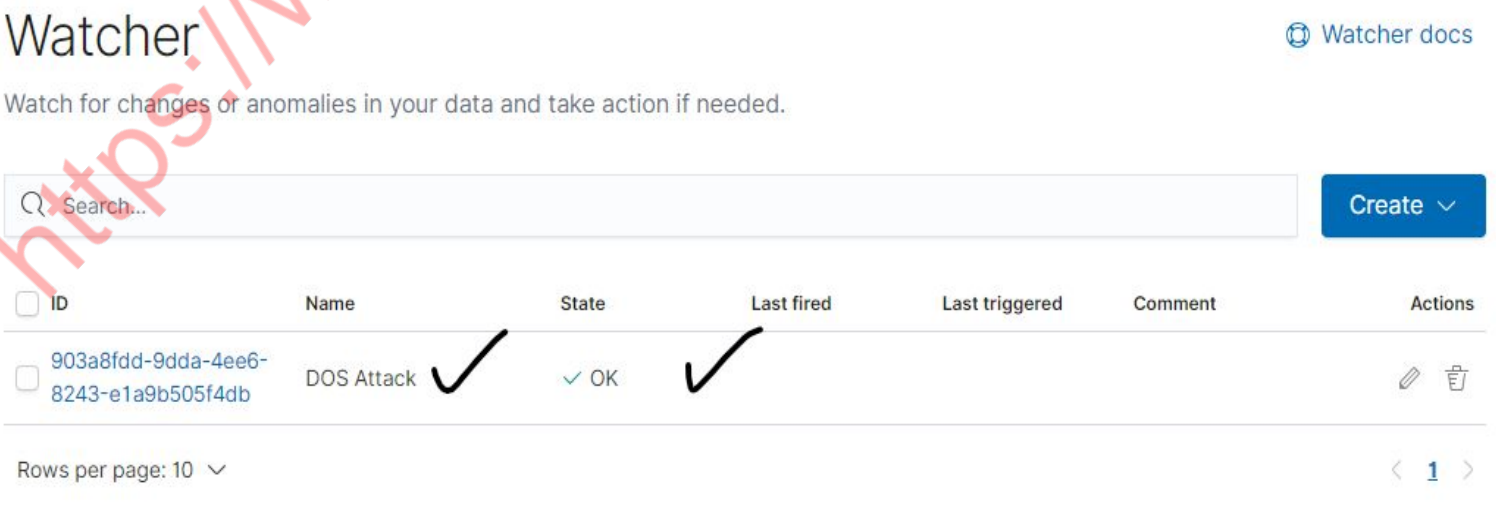
```
WHEN count()
GROUPED OVER top 5 'http.request.method'
IS ABOVE 1000
FOR THE LAST 5 minutes
```

Adding action



Create a text and click on create alert





3.3.2 Screenshot

Create an alert for Brute Force attack.

Edit BruteForceAttackRule

Edit | Simulate

Name (optional)

BruteForceAttackRule

ID

958cf330-29cb-4fdc-8c83-f05c9432d1f3

Watch JSON (API syntax)

```
{
  "trigger": {
    "schedule": {
      "interval": "5m"
    }
  },
  "input": {
    "search": {
      "request": {
        "search_type": "query_then_fetch",
        "indices": [
          "filebeat-7.4.0-2024.05.02-000001"
        ],
        "rest_total_hits_as_int": true,
        "body": {
          "query": {
            "bool": {
              "must": [
                {
                  "match": {
                    "Name": "BruteForceAttack"
                  }
                },
                {
                  "match": {
                    "event.code": "4625"
                  }
                },
                {
                  "exists": {
                    "field": "host.name"
                  }
                }
              ]
            }
          }
        }
      }
    },
    "condition": {
      "script": {
        "source": "return ctx.payload.hits.total.value > params.threshold",
        "lang": "painless",
        "params": {
          "threshold": 10
        }
      }
    },
    "actions": {
      "email_admin": {
        "email": {
          "profile": "standard",
          "to": [
            "admin@example.com"
          ],
          "subject": "Potential Brute Force Attack Detected",
          "body": {
            "text": "A potential brute force attack has been detected. Please investigate immediately."
          }
        }
      }
    }
  }
}
```

3.3.3 Screenshot

Create an alert for a scanning attack. During the scan, an attacker is looking to identify what ports are open.

Name (optional)

ScanningAttack

ID

f5231434-6064-4708-8112-23c8429000fc

Watch JSON (API syntax)

```
{
  "trigger": {
    "schedule": {
      "interval": "5m"
    }
  },
  "input": {
    "search": {
      "request": {
        "indices": [
          "filebeat-7.4.0-2024.05.02-000001"
        ],
        "body": {
          "query": {
            "bool": {
              "must": [
                { "match": { "event.type": "port_scan" } },
                { "range": { "@timestamp": { "gte": "now-5m" } } }
              ]
            }
          }
        }
      }
    }
  },
  "condition": {
    "script": {
      "source": "return ctx.payload.hits.total.value > params.threshold",
      "params": {
        "threshold": 50 // Adjust the threshold based on your environment and expected legitimate traffic
      }
    }
  },
  "actions": {
    "email_admin": {
      "email": {
        "to": "admin@example.com",
        "subject": "Potential Scanning Attack Detected",
        "body": {
          "text": "A potential scanning attack has been detected. Please investigate immediately."
        }
      }
    }
  }
}
```

3.4 Incident Response Playbook

Write a playbook below, detailing what the set of steps would be in response to each of the alerts you created in the last section 4.3. Add more pages if you need.

Incident Response Playbook

Introduction

This incident response playbook outlines the procedures to be followed in the event of attacks such as Denial of Service (DoS), Brute Force, or Scanning that target our organization's systems and services. This playbook provides guidelines for detecting, analyzing, containing, mitigating, and recovering from such attacks in a timely and effective way.

Incident Detection and Triage

Incident Detection:

For detection of an incident first monitor network traffic, different types of relevant server logs, intrusion detection/prevention systems (IDS/IPS) logs, and then security monitoring tools e.g SIEMs for signs of any abnormal activities, such as sudden increase in traffic is a symptom of DoS Attack, multiple failed login attempts is a symptom of brute force attack or suspicious scanning behavior is a scanning attack.

Triage:

Upon detection of these attacks, immediately assess the severity and scope of the incident to determine the appropriate response level and notify the incident response team.

Immediate Response Actions for the detected attacks:

Denial of Service (DoS) Attacks:

Activate DDoS Mitigation Services:

Make use of different cloud-based DDoS protection services to filter out any malicious traffic and maintain the availability of organizational resources.

Implement Rate Limiting:

Implement rate-limiting rules on different network devices, firewalls, and load balancers.

Distribute Load:

Distribute the incoming traffic across multiple data centers or servers to distribute the load and to minimize the impact of the DoS attack.

Brute Force Attack:

Implement Account Lockout Policies:

Implement account lockout policies to automatically lock user accounts if there are multiple failed login attempts in less amount of time from a certain user account.

Deploy Multi-Factor Authentication (MFA):

Deploy multi factor authentications on different user accounts such as passwords and one-time codes sent to the user's device via SMS or email.

Monitor and Analyze suspicious login attempts:

Monitor different authentication logs for any suspicious login attempt patterns such as multiple failed logins from the same IP address in less amount of time.

Scanning Attacks:

Block Suspicious IP Addresses:

Find out any IP address or ranges of IP addresses that are involved in scanning activity. Use firewall rules or network filtering rules to prevent further reconnaissance.

Monitoring Network Traffic:

Continuously monitor network traffic for scanning activity, such as port scanning, or vulnerability scanning.

Updating Security Policies:

Review the existing security policies and update them if needed. Review and different necessary configurations to restrict unnecessary access to network services and minimize the attack surface.

Analysis and Investigation:

Gather evidence:

Collect relevant data, logs, and other evidence that is related to the attack which includes IP addresses, network traffic patterns, timestamps, and attack vectors.

Conduct Forensic Analysis:

Perform the forensics analysis of anything suspicious found, to identify the root cause of an attack and assess the impact of an attack on organizational assets and data.

Collaborate with external partners:

Collaborate with different external partners such as internet service providers (ISPs), law enforcement agencies, and external vendors to gather additional intelligence and support the investigation efforts.

Mitigation & Recovery:

Implement remediation measures:

Implement remediation measures to strengthen the organization's defenses against future attacks by addressing vulnerabilities, applying security patches, updating configurations, and enhancing different types of security controls.

Restore Services:

Restore the affected critical systems/services to normal operations once the immediate threat has been mitigated and different adequate safeguards are in place to prevent further exploitation.

Monitor and Test:

Continuously monitor systems for signs of recurring attacks and conduct regular testing and different types of validation to test the effectiveness of the implemented security measures.

Communication and Reporting:

Internal Communication:

Communicate the incident details, different incident response actions, and updates with the relevant persons like internal stakeholders such as IT, security management, and legal teams for alignment and transparency purposes.

External Communication:

Notify partners, customers, regulators, and other relevant parties about the incident, the impact of the incident and the organization's response actions to the particular incident by following different established communication protocols and regulatory requirements.

Incident reporting:

Document incident response actions, findings, recommendations, and other details for post-incident analysis, regulatory compliance, and organizational learning purposes.

Post-Incident Analysis and Lesson Learned:

Review and Analysis:

Conduct a post-incident analysis for the evaluation of the effectiveness of incident response actions, and identify any gaps or weaknesses in incident response procedures and lessons learned for improvement.

Update Incident Response Plan:

Update the incident response plan based on lessons learned from the incident analysis to enhance our incident response capabilities for future incidents.

Conclusion:

This incident response playbook provides a structured framework for responding to Denial of Service (DoS) Attacks, Brute Force Attacks, and Scanning Attacks effectively. By following these procedures and guidelines we aim to minimize the impact of such type of attacks on our organization.

Section 4

Designing a Zero Trust Model

Section 4: Zero Trust Model

XYZ is elated with the work you've done so far! But they've been hearing about this new buzzword "Zero Trust" and are curious as to what it is and what the architecture would look like in a Zero Trust model. So your next task below is to design a Zero Trust model, then explain the differences between your network architecture and your Zero Trust model.

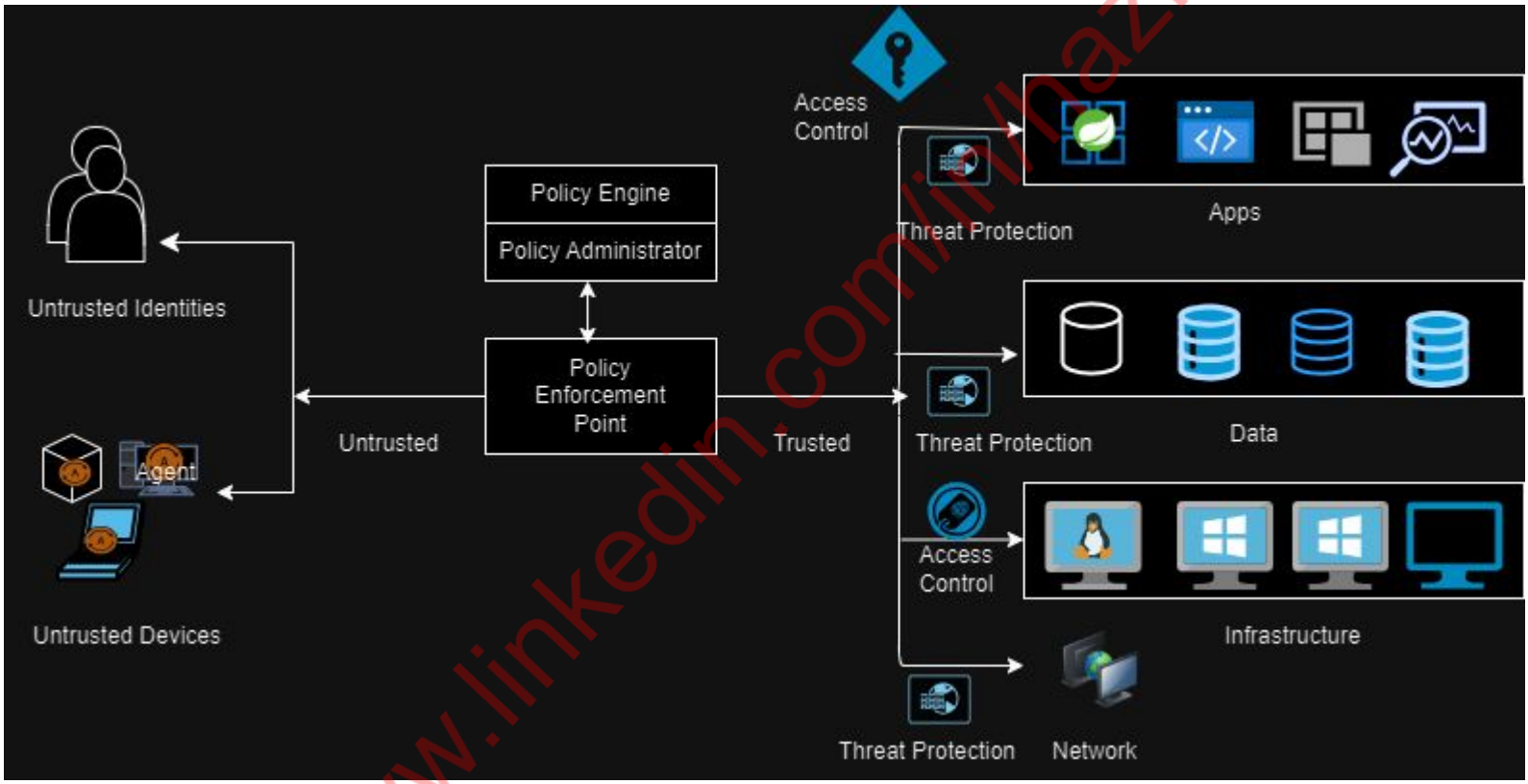
Design a Zero Trust model of your network architecture using https://app.diagrams.net/.

Make sure to incorporate the following into your design:

- Identity
- Devices
- Apps
- Network
- Data
- Infrastructure
- Trusted and Untrusted Devices
- Controls

4.1 Zero Trust Model

Paste your Zero Trust model diagram here:



Link:

https://drive.google.com/file/d/1pNBQ1zWzFTMwCsE5eZHS3H-PH7Omaggy/view?usp=sharing

4.2 Modern Architecture vs. Zero Trust

Write a detailed comparative analysis of the differences between your Zero Trust model and your secure network architecture design.

Zero Trust:

Zero Trust is enforcing the least privilege per request access decision in information systems and services. It means that in zero trust each device and service that is requesting information will have the least privilege and each access request to particular information from any device or service will be provided based on the decision made after the evaluation of a particular request such as by verifying the validity of every request that is made to access a particular service or information in enterprise data.

While in current perimeter network security architecture there is no procedure to verify the integrity of the request that is coming from any compromised machine.

There is no trust assumed in Zero Trust Architecture and here the network is viewed as compromised.

In a current perimeter and network security architecture trust is assumed in a trusted zone.

If there is a breached device in a trusted zone, we cannot protect the network because the breached device is already present in a trusted zone.

Whereas in Zero Trust enforces strict access controls through the principle of least privilege. It looks at each request and verifies its authenticity before granting any type of access to a particular request that is requesting for any resource.

In zero trust we are assuming no trust and we are assuming that the network is already compromised.

Zero trust architecture evaluates everything such as identity, credentials, access management, different operations, endpoints hosting environments, and infrastructure when dealing with access to enterprise data.

For Example

If we want to verify the requester identity that wants to access a particular service or resource, then through zero trust the requestor's identity, the security risk of the connecting device, the time that the requester is requesting, and from the location that a requester is requesting resource is verified. After validation and verification of these factors then a decision is made whether to grant access or deny it. If there is any breached device in our network then it will not be able to pass the policy decision point. The policy decision point is a point where all requests are checked. While there is no such scenario available in current perimeter network architecture.

References

https://discuss.elastic.co/t/eql-network-port-scan-watcher-to-eql/273104/3

https://discuss.elastic.co/t/brute-force-detection-rule/271713

https://discuss.elastic.co/t/brute-force-detection-rule/271713

https://www.hindawi.com/journals/itees/2023/6545323/