

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).

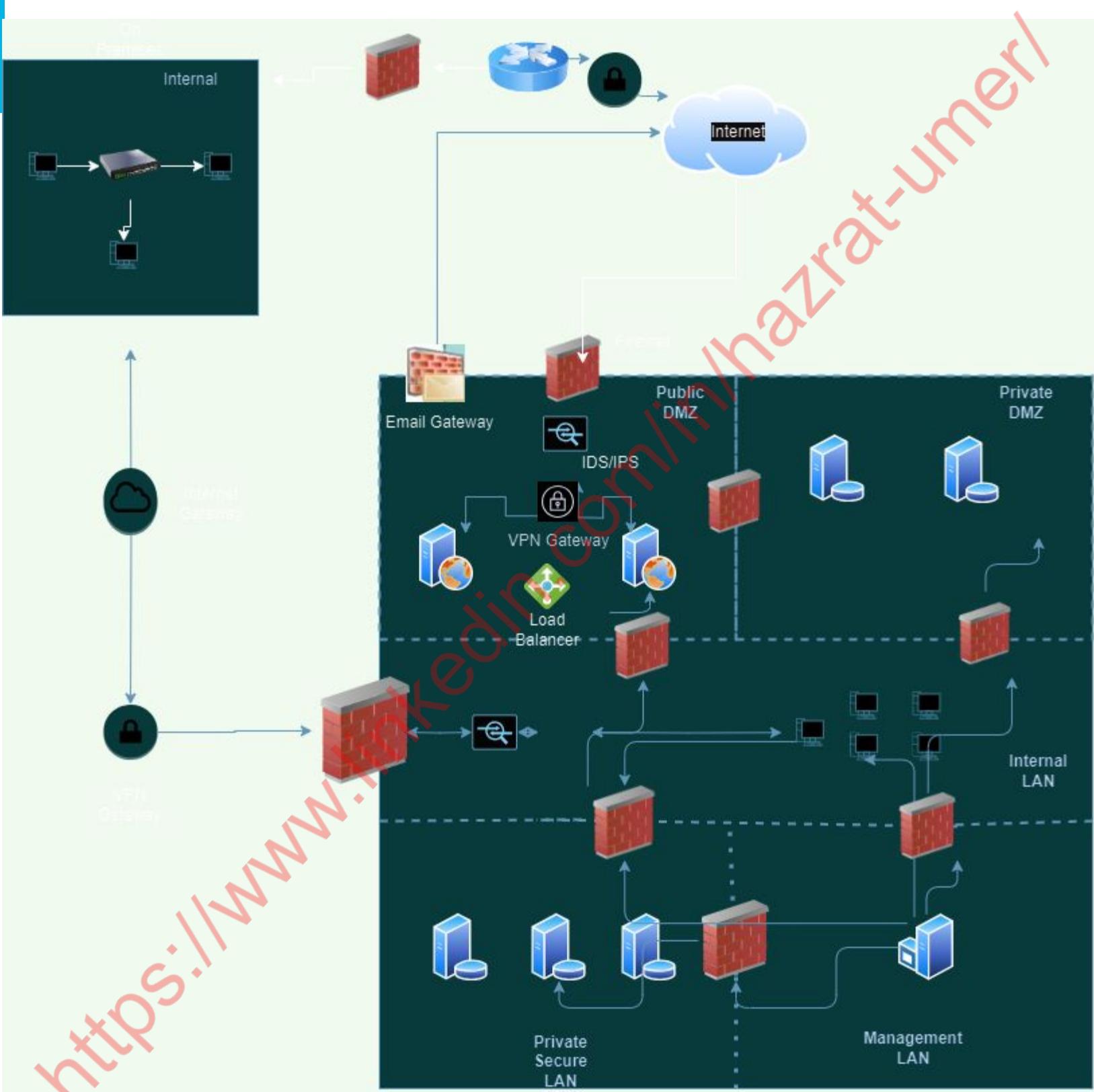
3) Show the flow of traffic, and remember to incorporate best security practices with the flow of traffic between the different subnets.

Designing the Network

Diagram Link:

https://drive.google.com/file/d/1k9uTyJYFp7Kkr1NZdSMGW_Blf2az51W/view?usp=sharing

1.1 Designing the Network



Digram URL:

https://drive.google.com/file/d/1k9uTyJYFp7Kkr1NZdSMGW_Blf2az51W/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

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The page title is 'Create virtual network' under 'Virtual networks'. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Home > Virtual networks >' breadcrumb. The main content area has tabs for 'Basics', 'Security', 'IP addresses', 'Tags', and 'Review + create'. The 'Basics' tab is selected. Under 'Subscription *', 'Udacity CloudLabs Sub - 40' is chosen. Under 'Resource group *', 'entp-project-258065' is selected, with a 'Create new' link below it. The 'Instance details' section contains fields for 'Virtual network name *' (set to 'DMZ') and 'Region *' (set to '(US) East US'). A link 'Deploy to an Azure Extended Zone' is also present. At the bottom are buttons for 'Previous', 'Next', and 'Review + create'.

DMZ Virtual Network Created

Home >

DMZ

Virtual network

Move Delete Refresh Give feedback

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

Settings

Address space Connected devices Subnets

Essentials

Resource group ([move](#)) : [entp-project-258065](#)
Location ([move](#)) : East US
Subscription ([move](#)) : [Udacity CloudLabs Sub - 40](#)
Subscription ID : 52c66fdd-6f75-4276-95a9-3960c6483db3

Address space : 10.0.0.0/16
DNS servers : Azure provided DNS service
Flow timeout : Configure
BGP community string : Configure
Virtual network ID : 758e5cb2-d2fc-4924-b349-9b5181283fad

Tags ([edit](#)) : Add tags

Topology Properties **Capabilities (5)** Recommendations Tutorials

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

Creating Virtual Network named “Internal”

Create virtual network ...

Basics Security IP addresses Tags Review + create

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

Subscription *

Resource group *

[Create new](#)

Instance details

Virtual network name *

Region * ⓘ

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

Leaving the security option as default

Create virtual network ...

Basics Security IP addresses Tags Review + create

Enhance the security of your virtual network with these additional paid security services. [Learn more ↗](#)

Virtual network encryption

Enable Virtual network encryption to encrypt traffic traveling within the virtual network. Virtual machines must have accelerated networking enabled. Traffic to public IP addresses is not encrypted. [Learn more ↗](#)

Virtual network encryption

Azure Bastion

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more ↗](#)

[Previous](#)

[Next](#)

[Review + create](#)

Leaving the IP addresses as default

Home > Virtual networks >

Create virtual network

...

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

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space |

<input type="button" value="^"/> 10.0.0.0/16	<input type="button" value="Delete address space"/>
<input type="text" value="10.0.0.0"/> /16	<input type="button" value="▼"/>
10.0.0.0 - 10.0.255.255	
65,536 addresses	
<input type="button" value="+ Add a subnet"/>	

[Previous](#) [Next](#) **Review + create**

Internal Virtual Network is Created

Home >

 Internal-1713686903049 | Overview Deployment

Search Delete Cancel Redeploy Download Refresh

Overview Inputs Outputs Template

✓ Your deployment is complete

Deployment name : Internal-1713686903049
Subscription : Udacity CloudLabs Sub - 40
Resource group : entp-project-258065

Start time : 4/21/2024, 1:08:33 PM
Correlation ID : 4de5a131-bcb0-4310-8cdc-9cb70e5aff...

> Deployment details
▼ Next steps

Go to resource

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

Home > Internal-1713687583314 | Overview >

Internal Virtual network

Search

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

Address space Connected devices

Move Delete Refresh Give feedback

Essentials

Resource group ([move](#)) : [entp-project-258065](#)
Location ([move](#)) : East US
Subscription ([move](#)) : [Udacity CloudLabs Sub - 40](#)
Subscription ID : 52c66fdd-6f75-4276-95a9-3960c6483db3

Address space : 10.0.0.0/16
DNS servers : Azure provided DNS service
Flow timeout : Configure
BGP community string : Configure
Virtual network ID : 3f79a235-f6b6-417f-8e92-e01671d7ec6b

Tags ([edit](#)) : Add tags

Topology Properties Capabilities (5) Recommendations Tutorials

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

Both the Virtual Networks are present in Resource Group

The screenshot shows the Azure portal interface for a resource group named "entp-project-258065". The left sidebar lists various navigation options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Deployments, Security, and Deployment slots. The main content area is titled "Essentials" and contains a "Resources" tab. A search bar at the top allows filtering by field, type, and location. The results table shows two entries:

Name	Type	Location
DMZ	Virtual network	East US
Internal	Virtual network	East US

Two black arrows point to the "DMZ" and "Internal" entries in the list.

2.1.2 Screenshot

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

Creating public Subnet

The screenshot shows the Azure portal interface for creating a subnet. On the left, the navigation bar includes Home, entp-project-258065, DMZ, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Address space, Connected devices, Subnets (selected), Bastion, DDoS protection, Firewall, and Microsoft Defender for Cloud. The main area displays the 'Subnets' blade for the 'DMZ' virtual network. A table lists one subnet: 'default' with IPv4 range 10.0.0.0/24 and available IPs 251. A red checkmark is placed over the 'Subnet' button. A modal window titled 'Add subnet' is open, showing fields for Name (set to 'Public'), Subnet address range (set to 10.0.1.0/24), and other options like NAT gateway (None) and Network security group (None). A red checkmark is placed over the 'Name' field. At the bottom of the modal are 'Save' and 'Cancel' buttons, and a 'Give feedback' link.

The screenshot shows the Azure portal interface after the public subnet has been created. The navigation bar and Subnets blade are identical to the previous screenshot. The table now shows two subnets: 'default' (IPv4 10.0.0.0/24, available IPs 251) and 'Public' (IPv4 10.0.1.0/24, available IPs 251). A red checkmark is placed over the 'Public' row. The 'Save' and 'Cancel' buttons are visible at the bottom of the blade.

Creating Private Subnet in DMZ

Home > entp-project-258065 > DMZ

DMZ | Subnets Virtual network

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

Subnets

Bastion DDoS protection Firewall Microsoft Defender for Cloud

Add subnet

Name * Private

Subnet address range * 10.0.2.0/24
10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)

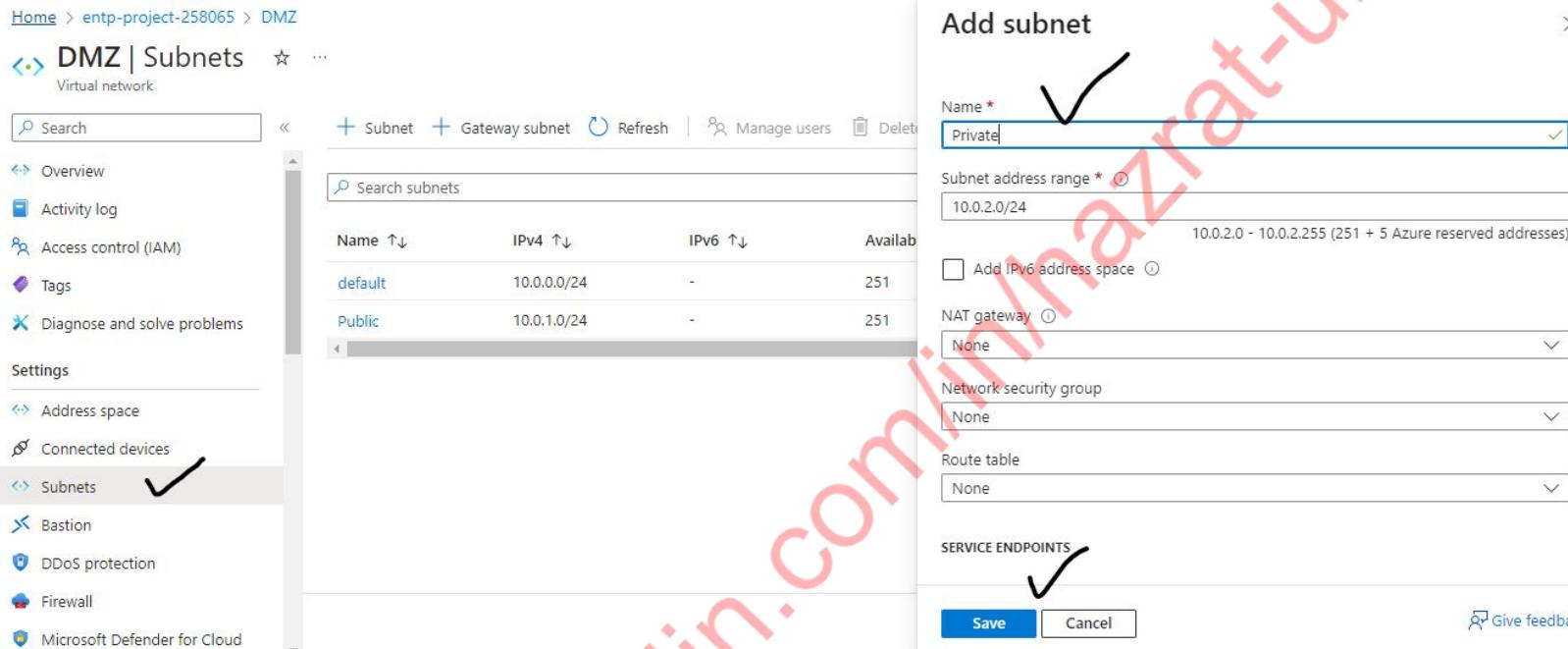
Add IPv6 address space

NAT gateway None

Network security group None

Route table None

Save Cancel



Home > entp-project-258065 > DMZ

DMZ | Subnets Virtual network

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

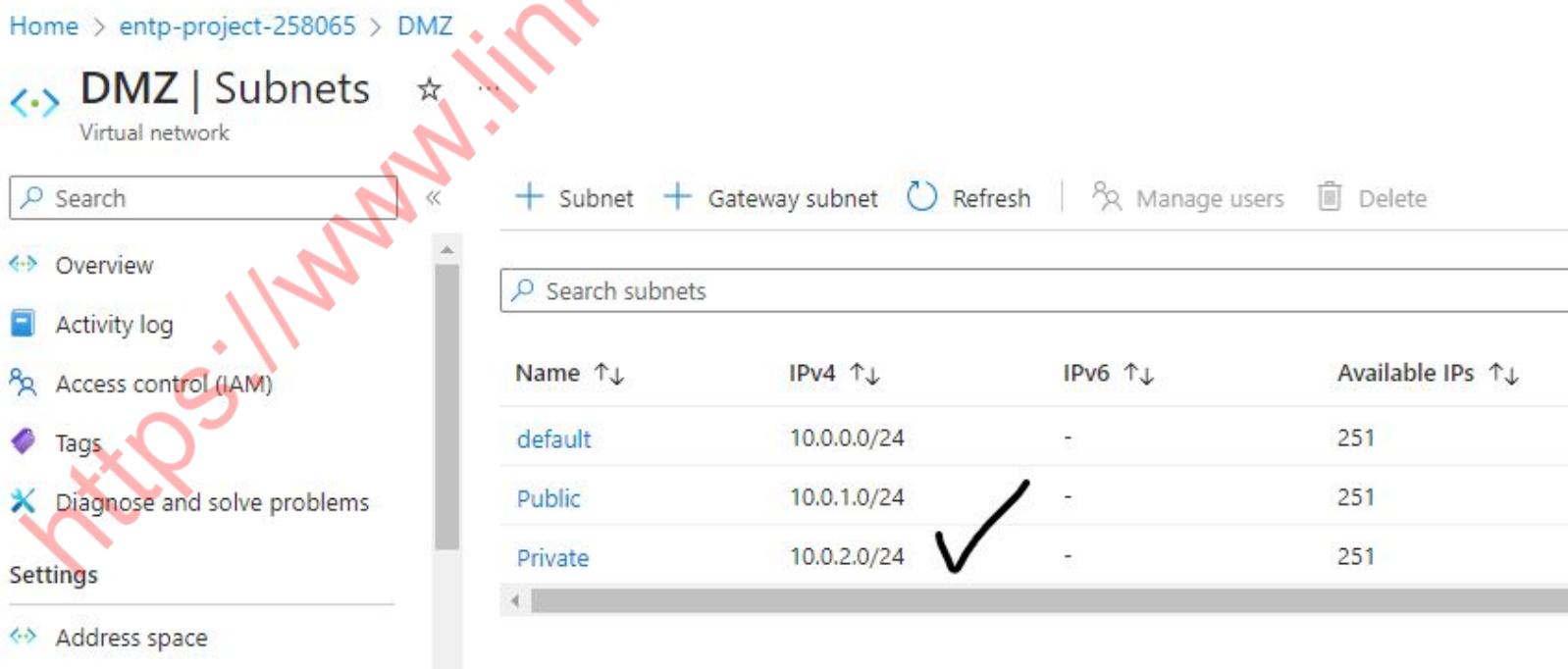
Address space

Subnets

+

Search subnets

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓
default	10.0.0.0/24	-	251
Public	10.0.1.0/24	-	251
Private	10.0.2.0/24	-	251



Both Private and Public Subnets created in DMZ

Home > entp-project-258065 > DMZ ✓

DMZ | Subnets Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

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

Search subnets

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓
default	10.0.0.0/24	-	251
Public	10.0.1.0/24	-	251
Private	10.0.2.0/24	✓	251

2.1.3 Screenshot

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

Creating Management Subnet in Internal Network

The screenshot shows the Azure portal interface for creating a subnet. On the left, the navigation menu is open, with 'Subnets' selected under the 'Internal' section. The main area displays the current subnets: 'default' with IP range 10.0.0.0/24 and 251 available IPs. A modal window titled 'Add subnet' is open, prompting for a name ('Management'), which has a checkmark. The 'Subnet address range' is set to 10.0.1.0/24, with a note indicating it covers 10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses). Other fields include 'Add IPv6 address space' (unchecked), 'NAT gateway' (None), 'Network security group' (None), and 'Route table' (None). At the bottom are 'Save' and 'Cancel' buttons, with a 'Give feedback' link at the very bottom right.

The screenshot shows the same portal interface after the 'Management' subnet has been created. The 'Subnets' section now lists two subnets: 'default' (IP range 10.0.0.0/24, 251 available IPs) and 'Management' (IP range 10.0.1.0/24, 251 available IPs). A checkmark is placed next to the 'Management' entry in the list. The rest of the interface remains consistent with the previous screenshot, showing the navigation menu and the 'Add subnet' modal closed.

Creating a Secure Subnet in Internal Virtual Network

Home > entp-project-258065 > Internal ✓

Internal | Subnets Virtual network

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

Settings Address space Connected devices Subnets ✓ Bastion DDoS protection Firewall Microsoft Defender for Cloud

+ Subnet + Gateway subnet Refresh Manage users Delete

Search subnets

Name	IPv4	IPv6	Available IPs
default	10.0.0.0/24	-	251
Management	10.0.1.0/24	-	251

Add subnet ✓

Name * Secure

Subnet address range * 10.0.2.0/24 10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space

NAT gateway None

Network security group None

Route table None

SERVICE ENDPOINTS

Save Cancel Give feedback

Home > entp-project-258065 > Internal ✓

Internal | Subnets Virtual network

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

Settings Address space Connected devices Subnets

+ Subnet + Gateway subnet Refresh Manage users Delete

Search subnets

Name	IPv4	IPv6	Available IPs
default	10.0.0.0/24	-	251
Management	10.0.1.0/24	-	251
Secure	10.0.2.0/24 ✓	-	251

Creating Enterprise Subnet in Internal Virtual Network

The screenshot shows the Azure portal interface for managing subnets in a virtual network. On the left, a sidebar lists various management options like Overview, Activity log, and Subnets. The main area displays a list of existing subnets: default (10.0.0.0/24), Management (10.0.1.0/24), and Secure (10.0.2.0/24). A modal window titled "Add subnet" is open, prompting for a name (set to "Enterprise"), a subnet address range (set to "10.0.3.0/24"), and other optional settings like NAT gateway and network security group. A large checkmark is overlaid on the top right of the modal.

The screenshot shows the same Azure portal interface after the "Enterprise" subnet has been successfully created. The list of subnets now includes the new entry: default (10.0.0.0/24), Management (10.0.1.0/24), Secure (10.0.2.0/24), and Enterprise (10.0.3.0/24). A large checkmark is overlaid on the bottom right of the subnet table.

Management, Secure and Enterprise Subnets created in Internal Virtual Network

Home > entp-project-258065 > Internal ✓

Internal | Subnets

Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

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

Address space Connected devices Subnets

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓
default	10.0.0.0/24	-	251
Management	10.0.1.0/24	-	251
Secure	10.0.2.0/24	-	251
Enterprise	10.0.3.0/24	-	251

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

Creating Network Security Groups for the Subnets

Creating Public Network Security Group
for public Subnet of DMZ

Home > Network security groups >

Create network security group



Basics Tags Review + create

Project details

Subscription *

Udacity CloudLabs Sub - 40

Resource group *

entp-project-258065

[Create new](#)

Instance details

Name *

Public_NSG

Region *

East US

[Review + create](#)

< Previous

Next : Tags >

[Download a template for automation](#)

Creating Private Network Security group for Private subnet of DMZ

Home > Network security groups >

Create network security group

Basics Tags Review + create

Project details

Subscription *

Udacity CloudLabs Sub - 40 ✓

Resource group *

entp-project-258065 ✓

Create new

Instance details

Name *

Private_NSG ✓

Region *

East US ✓

Review + create

< Previous

Next : Tags >

Download a template for automation

Home > Microsoft.NetworkSecurityGroup-20240421144605 | Overview >



Search ↵ → Move ⏺ Delete Refresh Give feedback

Overview

Resource group (move)	: entp-project-258065
Location	: East US
Subscription (move)	: Udacity CloudLabs Sub - 40
Subscription ID	: 52c66fdd-6f75-4276-95a9-3960c6483db3
Tags (edit)	: Add tags

Creating Network Security Groups for Management, Secure and Enterprise

Creating NSG for Management Subnet

[Home](#) > [Network security groups](#) >  Create network security group 

Basics Tags Review + create

Project details

Subscription *

Udacity CloudLabs Sub - 40 

Resource group *

entp-project-258065 

[Create new](#)

Instance details

Name *

Management_NSG 

Region *

East US 

[Review + create](#)

< Previous

Next : Tags >

[Download a template for automation](#)

Home >
 **Management_NSG**
Network security group

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

Settings
Inbound security rules 
Outbound security rules

  Move  Delete  Refresh  Give feedback

Essentials

Resource group (move)	: entp-project-258065
Location	: East US
Subscription (move)	: Udacity CloudLabs Sub - 40
Subscription ID	: 52c66fdd-6f75-4276-95a9-3960c6483db3
Tags (edit)	: Add tags

 Filter by name
Priority ↑↓ Name ↑↓ Port ↑↓

Creating NSG for Secure Subnet

[Home](#) > [Network security groups](#) >

Create network security group

[Basics](#) [Tags](#) [Review + create](#)

Project details

Subscription *

Udacity CloudLabs Sub - 40

Resource group *

entp-project-258065

[Create new](#)

Instance details

Name *

Secure_NSG

Region *

East US

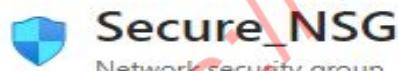
[Review + create](#)

[< Previous](#)

[Next : Tags >](#)

[Download a template for automation](#)

[Home](#) >



[Search](#)



[Overview](#)

[Activity log](#)

[Access control \(IAM\)](#)

[Tags](#)

[Diagnose and solve problems](#)

[Settings](#)

[Move](#) [Delete](#) [Refresh](#) [Give feedback](#)

^ Essentials

Resource group ([move](#)) : [entp-project-258065](#)

Location : East US

Subscription ([move](#)) : [Udacity CloudLabs Sub - 40](#)

Subscription ID : 52c66fdd-6f75-4276-95a9-3960c6483db3

Tags ([edit](#)) : [Add tags](#)

Creating NSG for Enterprise

Home > Network security groups >

Create network security group

Basics Tags Review + create

Project details

Subscription *

Udacity CloudLabs Sub - 40 ✓

Resource group *

entp-project-258065 ✓



Create new

Instance details

Name *

Enterprise_NSG ✓



Region *

East US ✓



Review + create

< Previous

Next : Tags >

Download a template for automation

Home > Microsoft.NetworkSecurityGroup-20240421145849 | Overview >



Enterprise_NSG

Network security group



Search



→ Move ↴ Delete ⌂ Refresh ⌂ Give feedback

Essentials

Resource group ([move](#)) : [entp-project-258065](#)

Location : East US

Subscription ([move](#)) : [Udacity CloudLabs Sub - 40](#)

Subscription ID : 52c66fdd-6f75-4276-95a9-3960c6483db3

Tags ([edit](#)) : [Add tags](#)

Filter by name

Port == all

Protocol

Settings

Network Security Groups created for all the subnets

Network security groups ...

Udacity (udacitylabs.onmicrosoft.com)

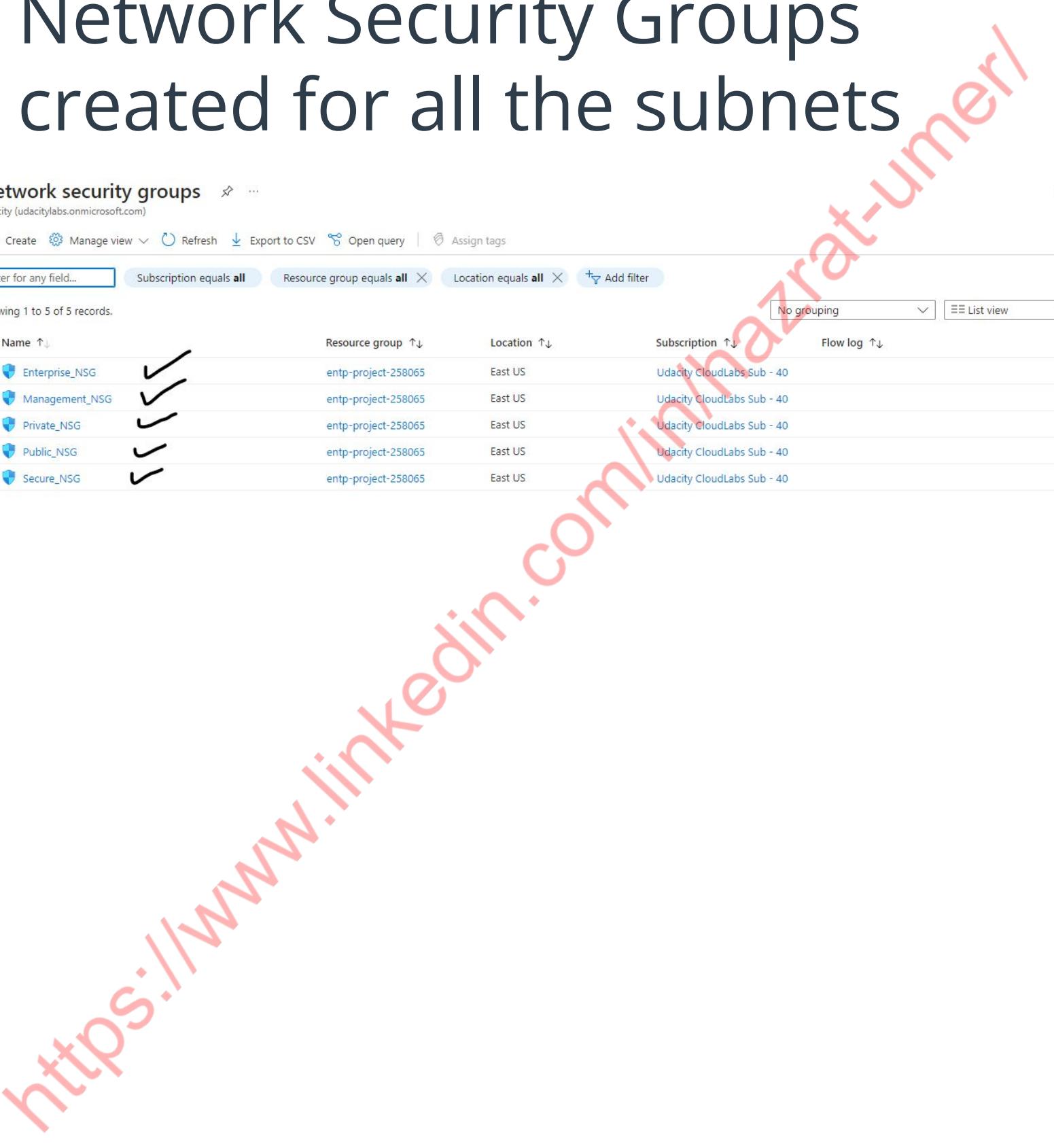
+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 5 of 5 records.

Name ↑	Resource group ↑	Location ↑	Subscription ↑	Flow log ↑
<input type="checkbox"/> Enterprise_NSG	entp-project-258065	East US	Udacity CloudLabs Sub - 40	
<input type="checkbox"/> Management_NSG	entp-project-258065	East US	Udacity CloudLabs Sub - 40	
<input type="checkbox"/> Private_NSG	entp-project-258065	East US	Udacity CloudLabs Sub - 40	
<input type="checkbox"/> Public_NSG	entp-project-258065	East US	Udacity CloudLabs Sub - 40	
<input type="checkbox"/> Secure_NSG	entp-project-258065	East US	Udacity CloudLabs Sub - 40	

No grouping List view



Associating subnets with Network Security Groups

Associating private DMZ Subnet with Private Network Security Group.

The screenshot shows the Azure portal interface for managing subnets. On the left, a sidebar lists 'Subnet', 'Gateway subnet', 'Refresh', 'Manage users', and 'Delete'. Below it is a search bar for 'Search subnets'. A table lists existing subnets: 'default' (IPv4: 10.0.0.0/24, Available IPs: 251), 'Private' (selected, IPv4: 10.0.2.0/24, Available IPs: 249), and 'Public' (IPv4: 10.0.1.0/24, Available IPs: 249). A checkmark is placed under the 'Private' row.

The main pane shows the configuration for a new 'Private' subnet under the 'DMZ' category. The 'Name' field is set to 'Private'. The 'Subnet address range' is '10.0.2.0/24', with a note below stating '10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)'. An unchecked checkbox for 'Add IPv6 address space' is present. The 'NAT gateway' dropdown is set to 'None'. The 'Network security group' dropdown is set to 'Private_NSG', with a checkmark indicating selection. The 'Route table' dropdown is also set to 'None'. At the bottom are 'Save' and 'Cancel' buttons, and a 'Give feedback' link.

At the very bottom of the page, another table displays the list of subnets again, showing the 'Security group' column where 'Private_NSG' is assigned to the 'Private' subnet, indicated by a checkmark.

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

The screenshot shows the Azure portal interface for managing subnets. On the left, a sidebar lists 'DMZ' and other options. The main area displays a table of existing subnets:

Name	IPv4	IPv6	Available IPs
default	10.0.0.0/24	-	251
Public	10.0.1.0/24	-	249
Private	10.0.2.0/24	-	249

A modal window titled 'Public' is open for creating a new subnet. It includes fields for Name (set to 'Public'), Subnet address range (set to '10.0.1.0/24'), NAT gateway (set to 'None'), Network security group (set to 'Public_NSG'), and Route table (set to 'None'). The 'Save' button is highlighted with a checkmark.

Below the modal, another table shows the updated list of subnets, where the 'Public' subnet now has 'Public_NSG' assigned under the 'Security group' column.

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

Home > Internal

Internal | Subnets ✓ ...

Virtual network

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

+ Subnet + Gateway subnet Refresh Manage users Delete

Search subnets

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓
default	10.0.0.0/24	-	251
Management	10.0.1.0/24	-	250
Secure	10.0.2.0/24	-	250
Enterprise	10.0.3.0/24	-	250

Management

Internal

Name: Management

Subnet address range: 10.0.1.0/24 (10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses))

Add IPv6 address space:

NAT gateway: None

Network security group: Management_NSG

Route table: None

SERVICE ENDPOINTS

Save Cancel

Give feedback

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

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

The screenshot shows two main sections of the Azure portal interface:

Left Panel (Subnets List):

- Search bar: Search subnets
- Table headers: Name ↑, IPv4 ↑↓, IPv6 ↑↓, Available IPs
- Subnets:
 - default: 10.0.0.0/24, Available IPs: 251
 - Secure: 10.0.2.0/24, Available IPs: 250
 - Enterprise**: 10.0.3.0/24, Available IPs: 250 (highlighted with a checkmark)
 - Management: 10.0.1.0/24, Available IPs: 250

Right Panel (Enterprise Subnet Configuration):

- Name:** Enterprise (checkmark)
- Subnet address range ***: 10.0.3.0/24 (checkmark)
- Add IPv6 address space**:
- NAT gateway**: None
- Network security group**: Enterprise_NSG (highlighted with a checkmark)
- Route table**: None
- SERVICE ENDPOINTS**: (checkmark)
- Buttons:** Save (highlighted with a checkmark), Cancel, Give feedback

A large red watermark with the URL <https://www.linkedin.com/in/mazrat-umer/> is diagonally overlaid across both panels.

Associating Internal Secure DMZ subnet with Secure NSG

The screenshot shows the Azure portal interface for managing subnets. On the left, a list of existing subnets is displayed:

Name	IPv4	IPv6	Available
default	10.0.0.0/24	-	251
Secure	10.0.2.0/24	✓	250
Management	10.0.1.0/24	-	250
Enterprise	10.0.3.0/24	-	250

On the right, a modal window titled "Secure" is open for creating a new subnet. The "Name" field is set to "Secure". The "Subnet address range" is specified as "10.0.2.0/24", which is highlighted with a checkmark. The "Network security group" dropdown is set to "Secure_NSG", also highlighted with a checkmark. The "Save" button at the bottom is also marked with a checkmark.

Below the modal, the main subnet list is shown again, with the "Secure" row highlighted by a checkmark.

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

Home > Virtual machines >

Create a virtual machine ✓

Project details

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

Subscription * ⓘ

Udacity CloudLabs Sub - 40 ✓

Resource group * ⓘ

entp-project-258065 ✓

[Create new](#)

Instance details

Virtual machine name * ⓘ

vmPublicDMZ ✓

Region * ⓘ

(US) East US ✓

Availability options ⓘ

Availability zone

Availability zone * ⓘ

Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM.

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.
entp302-258065-PolicyDefinition-entp-project-258065 ([Policy details](#))

Enable Hibernation (preview) ⓘ

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 AAAAB3NzaC1yc2EAAAQABAAQDzIaM0a0FJrX2ArVo1WYeWd6gCferDf7iinEPeNgvJSJvQuZzbNEE78EHV6xfL4UbzTV2GAyBApVQ+qW9
CVNHxD9m0y5KrdHGvgMlwJuT4g6Y4Vg72RqdFPnPYtyXTfKEsaCJQkPsuhj8JdgxKcrQBzTzY02EuDpVkb5/Ue9ArF2IdALH8simFpJxd6GZU1SOVFsc+EL
1tsIzi9tzhNA3ilAux0l8c++WhqE0PHiVOSzsGRGI4uEye5FcI0z5FcDXHczRv6cQcVEnJ7u1z/Rl/rKtf/Ad6sMmS6LSURCkiAl4iQtz2AQVmjYUpFedW8
4PrhJuFbkhw1k6/PXkui51Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44hp3Xd10cHrAYR6NAi6EHY0GsdlxTqnhG5wFU
sdaLt3MEC1MBUiM/4hbbcrtnAzHpRsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMZpF0= hazra@Eagle
```

Username * ✓

SSH public key source

SSH public key * i Learn more about creating and using SSH keys in Azure ↗

Inbound port rules

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

Public inbound ports * None

Allow selected ports

Select inbound ports *

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

i 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

Home > Create a resource >

Create a virtual machine

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

Virtual network * ⓘ

DMZ

[Create new](#)

Subnet * ⓘ

Public (10.0.1.0/24)

[Manage subnet configuration](#)

Public IP ⓘ

(new) vmPublicDMZip632

[Create new](#)

NIC network security group ⓘ

None

Basic

Advanced

Configure network security group *

Public_NSG

[Create new](#)

Delete public IP and NIC when VM is

[< Previous](#)

[Next : Management >](#)

[Review + create](#)

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20240421151012 | Overview >



Virtual machine

[Search](#)

[Connect](#) [Start](#) [Restart](#) [Stop](#) [Hibernate \(preview\)](#) [Capture](#) [Delete](#) [Refresh](#) [Open in mobile](#) [Feed](#)

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 : [20.51.192.102](#)

Subscription ([move](#)) : [Udacity CloudLabs Sub - 40](#)

Virtual network/subnet : [DMZ/Public](#)

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

Creating VM in Private DMZ subnet

Home > Virtual machines >

Create a virtual machine

Subscription * ⓘ Udacity CloudLabs Sub - 40

Resource group * ⓘ entp-project-258065 ✓

Create new

Virtual machine name * ⓘ vmPrivateDMZ ✓

Region * ⓘ (US) East US

Availability options ⓘ Availability zone

Availability zone * ⓘ Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#) ↗

Security type ⓘ Trusted launch virtual machines

< Previous Next : Disks > Review + create

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 *	<input type="text" value="DMZ"/>  Create new
Subnet *	<input type="text" value="Private (10.0.2.0/24)"/>  Manage subnet configuration
Public IP	<input type="text" value="(new) vmPrivateDMZ-ip"/>  Create new
NIC network security group	<input type="radio"/> None

[< Previous](#)
[Next : Management >](#)
Review + create

vmPrivateDMZ created



vmPrivateDMZ

Virtual machine

- [Search](#)
- [Overview](#)
- [Activity log](#)
- [Access control \(IAM\)](#)
- [Tags](#)
- [Diagnose and solve problems](#)
- [Connect](#)
- [Bastion](#)

^ 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		

VMs Created in Public and Private DMZ subnets

Virtual machines ...

Udacity (udacitylabs.onmicrosoft.com)

+ Create Switch to classic Reservations Manage view Refresh Export to CSV Open query | Assign tags Start Restart Stop Delete ...

Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all + Add filter

Showing 1 to 2 of 2 records.

	Name ↑↓	Type ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓	Status ↑↓	Operating system ↑↓	Size ↑↓	Power state
<input type="checkbox"/>	vmPrivateDMZ ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s	On
<input type="checkbox"/>	vmPublicDMZ ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s	On

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

Home > Virtual machines >

Create a virtual machine ...

Subscription * ⓘ Udacity CloudLabs Sub - 40 ✓

Resource group * ⓘ entp-project-258065 ✓

Create new

Virtual machine name * ⓘ vmManagementInternal ✓

Region * ⓘ (US) East US ✓

Availability options ⓘ Availability zone

Availability zone * ⓘ Zone 1 ✓

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more ↗](#)

Security type ⓘ Trusted launch virtual machines ✓

< Previous Next : Disks > Review + create

https://www.linkedin.com/in/hazratumer/

Assigning Virtual Network, Internal Subnet and NSG

Home > Virtual machines >

Create a virtual machine



Network interface

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

Virtual network * ⓘ

Internal ✓

[Create new](#)

Subnet * ⓘ

Management (10.0.1.0/24) ✓

[Manage subnet configuration](#)

Public IP ⓘ

(new) vmManagementInternal-ip ✓

[Create new](#)

NIC network security group ⓘ

- None
- Basic
- Advanced

Configure network security group *

Management_NSG ✓

[Create new](#)

[< Previous](#)

[Next : Management >](#)

Review + create

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20240421153632 | Overview >

 **vmManagementInternal** ⚡ ☆ ... ✓

Virtual machine

[Search](#)

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

[Overview](#)

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 : [20.51.197.194](#)

Subscription ([move](#)) : [Udacity CloudLabs Sub - 40](#)

Virtual network/subnet : [Internal/Management](#) ✓

Subscription ID : 52c66ffd-6f75-4276-95a9-3960c6483db3

DNS name : [Not configured](#)

Availability zone : 1

Health state : -

Tags ([edit](#)) : [Add tags](#)

Creating VM in Enterprise Internal Subnet

Create a virtual machine ...

Instance details

Virtual machine name * ⓘ

vmEnterpriseInternal ✓

Region * ⓘ

(US) East US ✓

Availability options ⓘ

Availability zone ✓

Availability zone * ⓘ

Zone 1 ✓

💡 You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#) ↗

Security type ⓘ

Trusted launch virtual machines ✓

[Configure security features](#)

Image * ⓘ

Ubuntu Server 20.04 LTS - x64 Gen2 ✓

[See all images](#) | [Configure VM generation](#)

[< Previous](#)

[Next : Disks >](#)

[Review + create](#)

Assigning Virtual Network, Internal Subnet and NSG

Network interface

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

Virtual network * ⓘ

Internal ✓
Create new

Subnet * ⓘ

Enterprise (10.0.3.0/24) ✓
Manage subnet configuration

Public IP ⓘ

(new) vmEnterpriseInternal-ip
Create new

NIC network security group ⓘ

None
 Basic
 Advanced

Configure network security group *

Enterprise_NSG ✓
Create new

< Previous Next : Management > Review + create

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20240421161730 | Overview >

vmEnterpriseInternal ✓

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Action

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	: 20.51.207.33
Subscription (move)	: Udacity CloudLabs Sub - 40	Virtual network/subnet	: Internal/Enterprise ✓
Subscription ID	: 52c66fdd-6f75-4276-95a9-3960c6483db3	DNS name	: Not configured
Availability zone	: 1	Health state	: -
Tags (edit)	: Add tags		

Creating VM in Secure Subnet

Home > Virtual machines >

Create a virtual machine

Subscription * ⓘ

Udacity CloudLabs Sub - 40 ✓

Resource group * ⓘ

entp-project-258065 ✓

[Create new](#)

Instance details

Virtual machine name * ⓘ

vmSecureInternal ✓

Region * ⓘ

(US) East US ✓

Availability options ⓘ

Availability zone

Availability zone * ⓘ

Zone 1

 You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#) ↗

[< Previous](#)

[Next : Disks >](#)

[Review + create](#)

Assigning Virtual Network, Network Security Group and Subnet

Network interface

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

Virtual network * ⓘ

Internal ✓

Create new

Subnet * ⓘ

Secure (10.0.2.0/24) ✓

Manage subnet configuration

Public IP ⓘ

(new) vmSecureInternal-ip ✓

Create new

NIC network security group ⓘ

None

Basic

Advanced

Configure network security group *

Secure_NSG ✓

Create new

< Previous

Next : Management >

Review + create

vmSecureInternal

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 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 :	51.8.90.86
Subscription (move) :	Udacity CloudLabs Sub - 40	Virtual network/subnet :	Internal/Secure
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

Three VMs deployed in Internal

Virtual machines ...

Udacity

+ Create Switch to classic Reservations Manage view Refresh Export to CSV Open query | Assign tags Start Restart Stop Delete

Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all Add filter

Showing 1 to 5 of 5 records.

<input type="checkbox"/> Name ↑↓	Type ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓	Status ↑↓	Operating system ↑↓	Size ↑↓
<input checked="" type="checkbox"/> vmEnterpriseInternal ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s
<input checked="" type="checkbox"/> vmManagementInternal ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s
<input checked="" type="checkbox"/> vmPrivateDMZ	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s
<input checked="" type="checkbox"/> vmPublicDMZ	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s
<input checked="" type="checkbox"/> vmSecureInternal ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s

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

The screenshot shows the Azure portal interface for managing Network Security Groups (NSGs). On the left, the 'Inbound security rules' section is selected under the 'Public_NSG' network security group. A new rule is being created, as indicated by the 'Add inbound security rule' dialog box on the right. The dialog box contains the following settings:

- Source: Any
- Source port ranges: *
- Destination: Any
- Service: HTTP
- Destination port ranges: 80
- Protocol: TCP (selected)

Below the dialog box, the current list of inbound security rules is displayed:

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
100	AllowAnyHTTPInbound	80	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any

Allowing inbound HTTPS Traffic for public DMZ

The screenshot shows the Azure portal interface for managing Network Security Groups (NSGs). On the left, the 'Public_NSG' network security group is selected. The main pane displays the 'Inbound security rules' section, which includes a table of existing rules and a 'Add inbound security rule' dialog box.

Inbound security rules table:

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

Add inbound security rule dialog:

Source: Any ✓

Source port ranges: * ✓

Destination: Any ✓

Service: HTTPS ✓

Destination port ranges: 443 ✓

Protocol: TCP

Add Cancel

Created following inbound Rules for Public DMZ

Public_NSG | Inbound security rules

Network security group

Search

Add Hide default rules Refresh Delete Give feedback

existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority.
Learn more

Filter by name

Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑
<input type="checkbox"/> 100	AllowAnyHTTPInbound	80	TCP	Any
<input type="checkbox"/> 110	AllowAnyHTTPSInbou...	443	TCP	Any
<input type="checkbox"/> 120	AllowAnySMTPInbound	25	TCP	Any
<input type="checkbox"/> 130	AllowMyIpAddressSS...	22	TCP	203.101.190.186
<input type="checkbox"/> 140	AllowAnyDNS-TCPInb...	53	TCP	Any
<input type="checkbox"/> 150	AllowAnyDNS-UDPInb...	53	UDP	Any

Inbound security rules

Outbound security rules

Network interfaces

Subnets

...

<input type="checkbox"/> 100	AllowAnyHTTPInbound	80	TCP	Any
<input type="checkbox"/> 110	AllowAnyHTTPSInbou...	443	TCP	Any
<input type="checkbox"/> 120	AllowAnySMTPInbound	25	TCP	Any
<input type="checkbox"/> 130	AllowMyIpAddressSS...	22	TCP	203.101.190.186
<input type="checkbox"/> 140	AllowAnyDNS-TCPInb...	53	TCP	Any
<input type="checkbox"/> 150	AllowAnyDNS-UDPInb...	53	UDP	Any
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalance
<input type="checkbox"/> 65002	DenyAllInbound	Any	Any	Any

2.3.2 Screenshot

Traffic rules in your Internal network.

Secure NSG

Secure_NSG | Inbound security rules

Network security group

Search Add Hide default rules Refresh Delete Give feedback

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

Inbound security rules Outbound security rules Network interfaces

Priority ↑ Name ↑ Port ↑ Protocol ↑ Source ↑ Destination ↑ Action ↑

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowCidrBlockSSHInb...	22	TCP	203.101.190.186	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowCidrBlockSSHInb...	22	TCP	203.101.190.186	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Private NSG Rules

Private_NSG | Inbound security rules ...

Network security group

Search Add Hide default rules Refresh Delete Give feedback

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

Inbound security rules Outbound security rules Network interfaces Subnets

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
<input type="checkbox"/> 100	AllowCidrBlockSSHInb...	22	TCP	203.101.190.186
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

100 AllowCidrBlockSSHInb... 22 TCP 203.101.190.186
65000 AllowVnetInBound Any Any VirtualNetwork
65001 AllowAzureLoadBalanc... Any Any AzureLoadBalancer
65500 DenyAllInBound Any Any Any

Management NSG Inbound Rules

Management_NSG | Inbound security rules

Network security group

Search Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
<input type="checkbox"/> 100 ✓	⚠ DenyAnyCustom8... 8080	Any	Any	Any
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets

<input type="checkbox"/> 100	⚠ DenyAnyCustom8... 8080	Any	Any
<input type="checkbox"/> 65000	AllowVnetInBound	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	AzureLoadBalancer
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any

Enterprise NSG Inbound Rules

Enterprise_NSG | Inbound security rules ✓

Network security group

Search + Add Hide default rules Refresh Delete Give feedback

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

Settings

Inbound security rules Outbound security rules Network interfaces Subnets

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
<input type="checkbox"/> 100 ✓	AllowCidrBlockSSHInb...	22	TCP ✓	203.101.190.186
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

✓

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
<input type="checkbox"/> 100	AllowCidrBlockSSHInb...	22	TCP	203.101.190.186
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

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

SSHed from my Laptop and it works

vmEnterpriseInternal Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

azureuser@vmEnterpriseInternal ~\$ |

Connect Start Restart Stop Hibernate (preview) Capture Delete

Resource group (move)
[entp-project-258065](#)

Status
Running

Location
East US (Zone 1)

Subscription (move)
[Udacity CloudLabs Sub - 40](#)

Subscription ID

Operating system
Linux (ubuntu 20.04)

Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
[20.51.207.33](#)

Virtual network/subnet
[Internal/Enterprise](#)

DNS name

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes links for 'Free Training Courses', 'Wingle Web Admin', 'Apple and Cisco Ar...', 'Certified Ethical Ha...', 'Microsoft Certified...', and 'https://'. The main title 'Microsoft Azure' is followed by a search bar 'Search resources, services, and docs (G+ /)'. Below the title, the breadcrumb navigation shows 'Home >'. The main content area is titled 'Virtual network gateways' with a 'Udacity' tag. A 'Create' button is highlighted with a black checkmark. The page features several filter options: 'Filter for any field...', 'Subscription equals all', 'Resource group equals all', 'Location equals all', and 'Add filter'. At the bottom, it says 'Showing 0 to 0 of 0 records.' and has columns for 'Name' and 'Virtual ...'.

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 *

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 Download a template for automation

Waiting for its deployment

Microsoft.VirtualNetworkGateway-20240421180556 | Overview

Deployment

Search Delete Cancel Redeploy Download Refresh

Overview Inputs Outputs Template

Deployment is in progress ✓

Deployment name : Microsoft.VirtualNetworkGateway-20... Start time : 4/21/2024, 6:17:49 PM
Subscription : Udacity CloudLabs Sub - 40 Correlation ID : a3cce308-1642-4aad-ba61-2cdb9d34...
Resource group : entp-project-258065

Deployment details

Resource	Type	Status	Operation details
Enterprise_VPN	Virtual network gateway	Created	Operation details
EnterpriseVPN2ndl	Public IP address	OK	Operation details
EnterpriseVPNip	Public IP address	OK	Operation details
Internal/GatewayS	Microsoft.Network/virtualNetwo	OK	Operation details

✓ Your deployment is complete

Deployment name : Microsoft.VirtualNetworkGateway-202... Start time : 4/21/2024, 6:17:49 PM
Subscription : Udacity CloudLabs Sub - 40 Correlation ID : a3cce308-1642-4aad-ba61-2cdb9d34...
Resource group : entp-project-258065

> Deployment details

> Next steps

Go to resource

VPN deployed

The screenshot shows the Azure portal interface for a 'Virtual network gateway' named 'Enterprise_VPN'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, Connections, Point-to-site configuration, and Properties. The main content area displays the 'Essentials' section with the following details:

Setting	Value
Resource group (move)	entp-project-258065
Location	East US
Subscription (move)	Udacity CloudLabs Sub - 40
Subscription ID	52c66fdd-6f75-4276-95a9-3960c6483db3
SKU	VpnGw1
Gateway type	VPN
VPN type	Route-based
Virtual network	Internal/GatewaySubnet
First public IP address	13.92.126.117 (EnterpriseVPNIP)

Below the essentials, there is a 'Tags' section with a link to 'Add tags'. To the right, there is a 'Health check' section with a 'Go to Resource health' button, and a 'Documentation' section with a 'View documentation' button.

Point to Site Configuration

Home > Microsoft.VirtualNetworkGateway-20240421180556 | Overview > Ent

Enterprise_VPN | Point-to-site configuration

Virtual network gateway

Search Save Discard Delete

Point-to-site is not configured
Configure now ✓

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

Settings

Configuration Connections Point-to-site configuration ✓



Enterprise_VPN | Point-to-site configuration ☆ ...

Virtual network gateway

Search

Save Discard Delete Download VPN client

Address pool * ✓

Tunnel type ✓

Authentication type ✓

Public IP address for User VPN configuration
A third public IP address is required to use a User VPN configuration with an available public IP address.

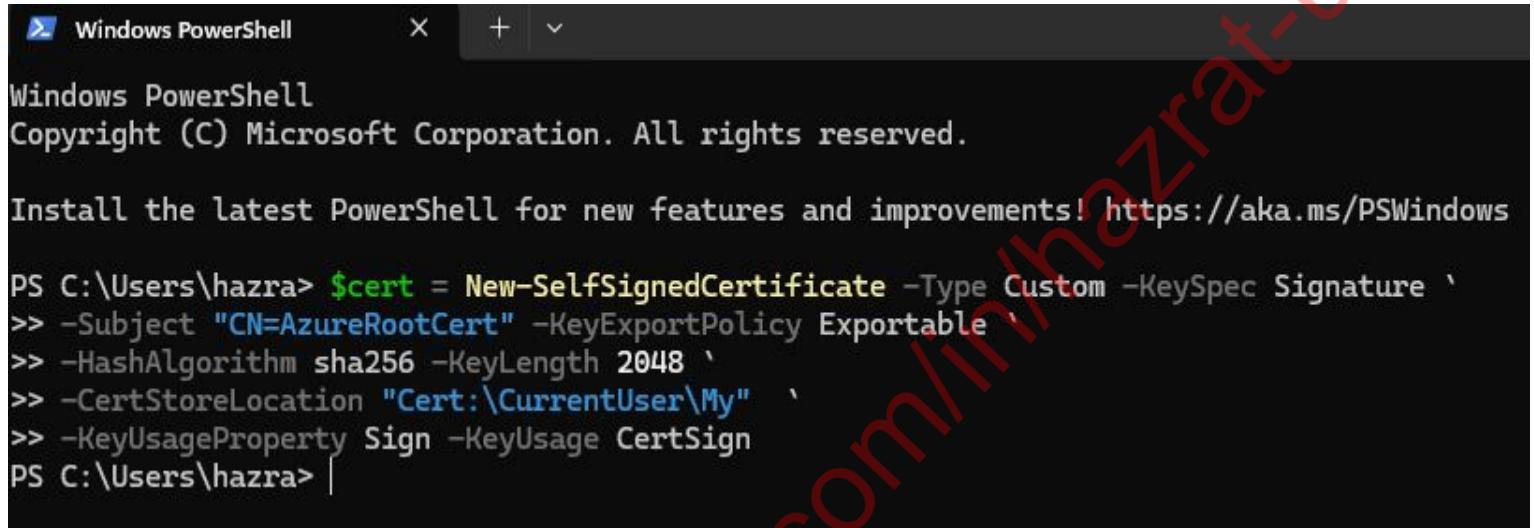
Public IP address * ⓘ
 Create new Use existing ✓

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

Settings Configuration Connections Point-to-site configuration Properties Locks

Monitoring

Creating Azure Root Cert



A screenshot of a Windows PowerShell window titled "Windows PowerShell". The window shows the command to create a self-signed certificate named "AzureRootCert" with specific parameters: Type Custom, KeySpec Signature, Subject CN=AzureRootCert, HashAlgorithm sha256, KeyLength 2048, CertStoreLocation Cert:\CurrentUser\My, and KeyUsageProperty Sign.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\hazra> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `>> -Subject "CN=AzureRootCert" -KeyExportPolicy Exportable `>> -HashAlgorithm sha256 -KeyLength 2048 `>> -CertStoreLocation "Cert:\CurrentUser\My" `>> -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\Users\hazra> |
```

```
#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

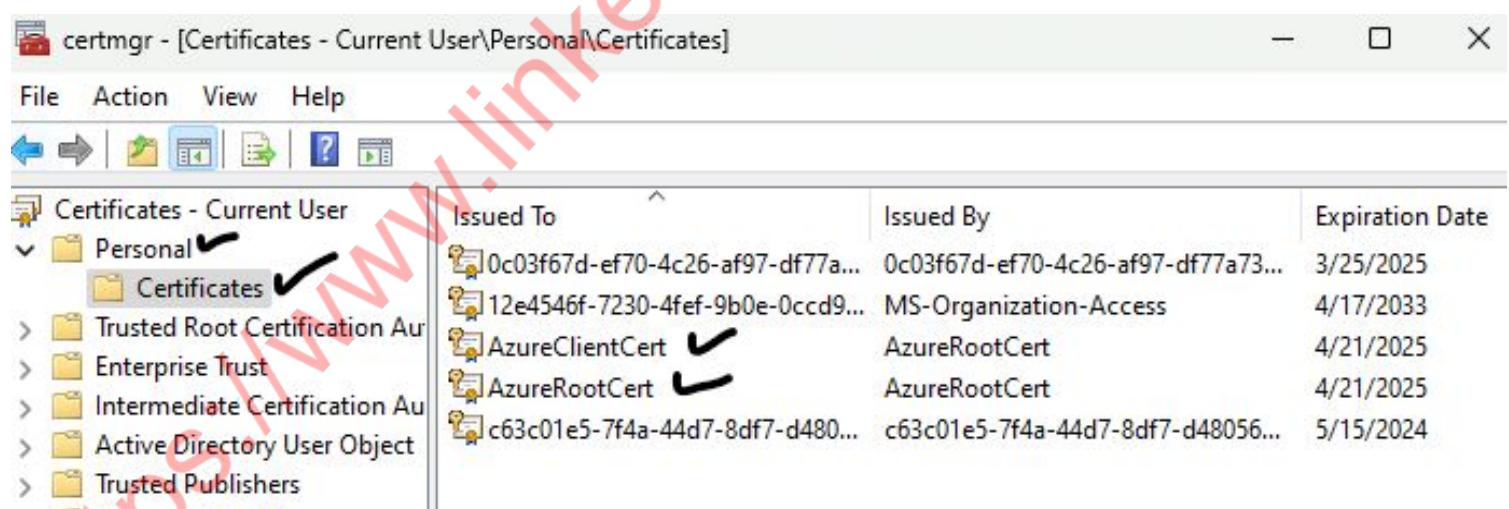
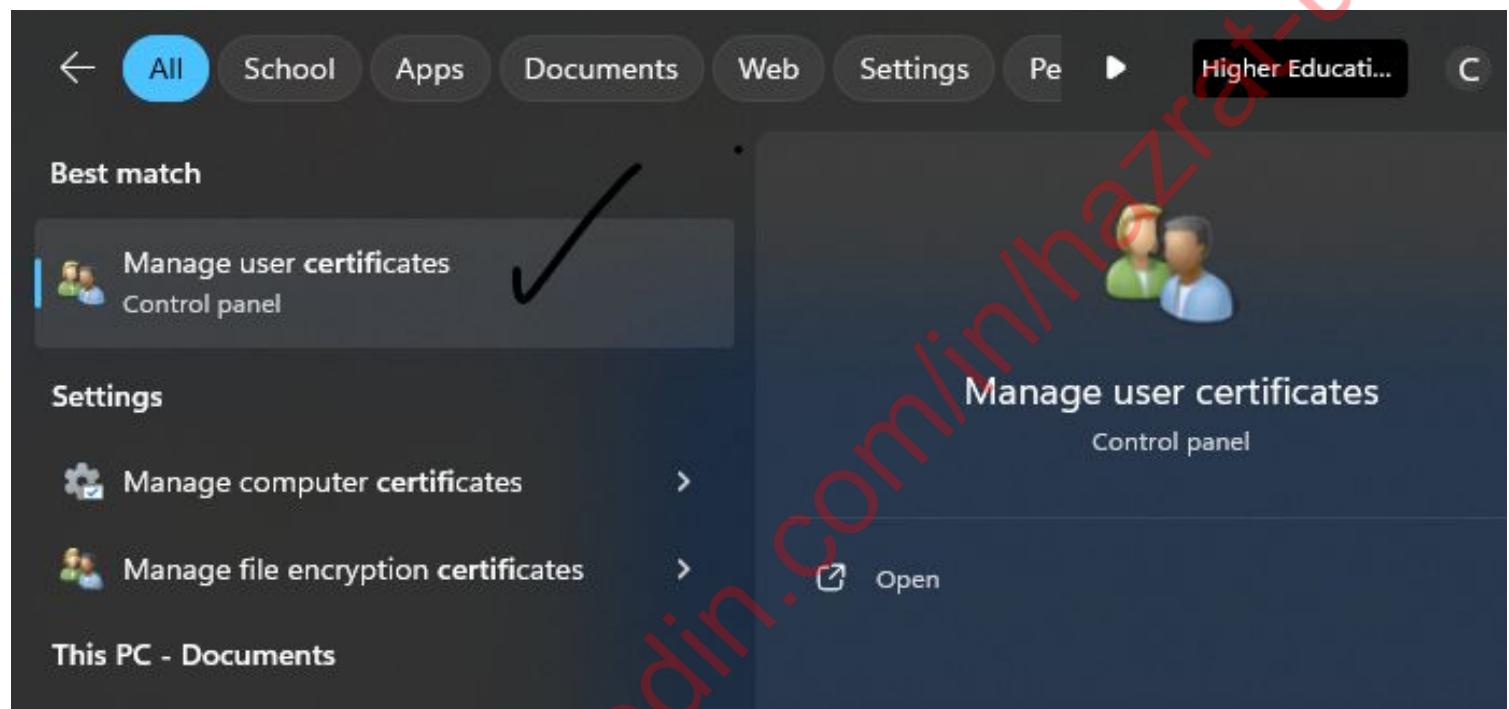
```
PS C:\Users\hazra> # Create Client Cert
PS C:\Users\hazra> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature ` 
>> -Subject "CN=AzureClientCert" -KeyExportPolicy Exportable ` 
>> -HashAlgorithm sha256 -KeyLength 2048 ` 
>> -CertStoreLocation "Cert:\CurrentUser\My" ` 
>> -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

The screenshot shows the Windows Certificates snap-in window titled "certmgr - [Certificates - Current User\Personal\Certificates]". The left pane displays a tree view of certificate categories under "Certificates - Current User", including "Personal", "Trusted Root Certification Authority", "Enterprise Trust", etc. The right pane lists certificates with columns for "Issued To", "Issued By", and "Expiration Date". A context menu is open over the "AzureRoot" certificate, which has the following options:

- Open
- All Tasks
- Cut
- Copy
- Delete
- Properties
- Help
- Request Certificate with New Key...
- Renew Certificate with New Key...
- Advanced Operations >
- Export...

Below the main window, a smaller "Export a certificate" dialog box is visible, showing the "Certificate Export Wizard" and the "Export Private Key" step.

Export a certificate

← Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key
 No, do not export the private key

Next Cancel

X



Export File Format

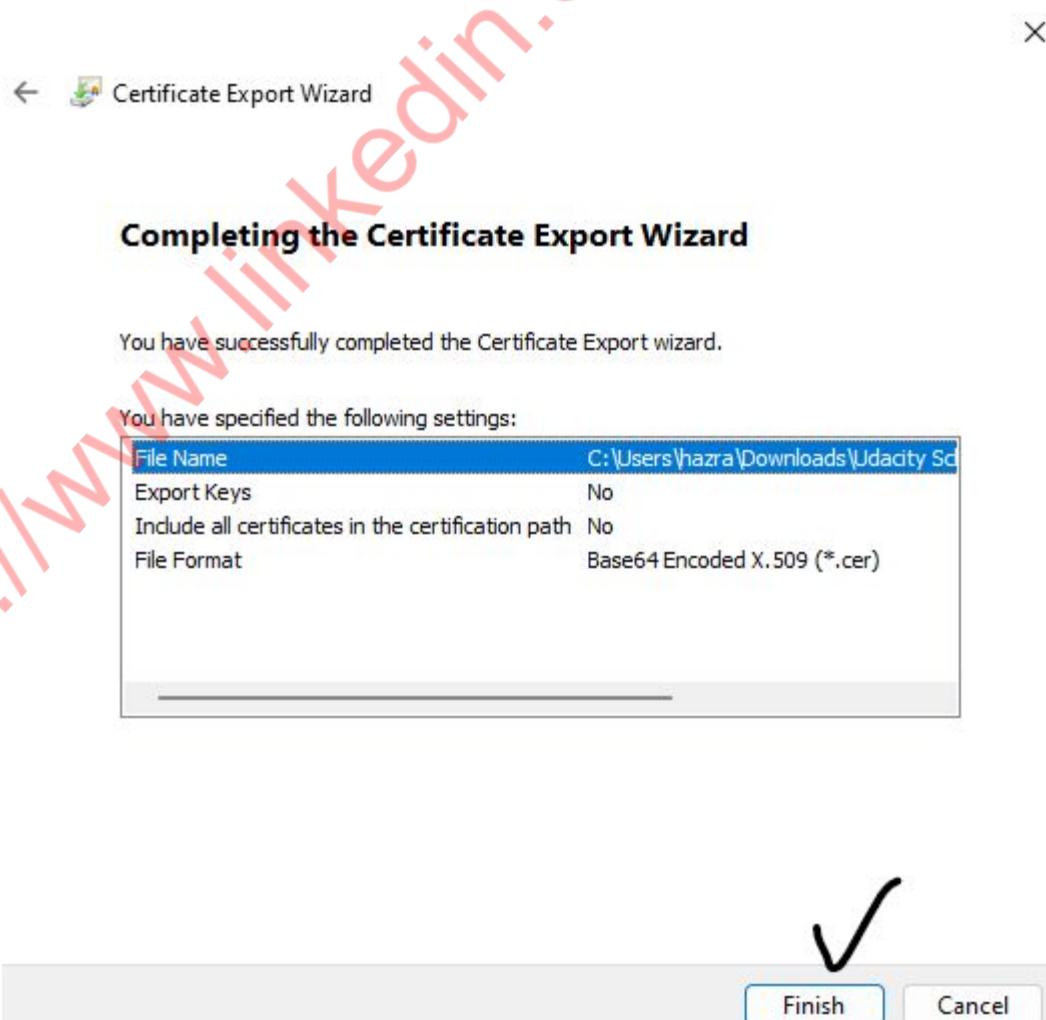
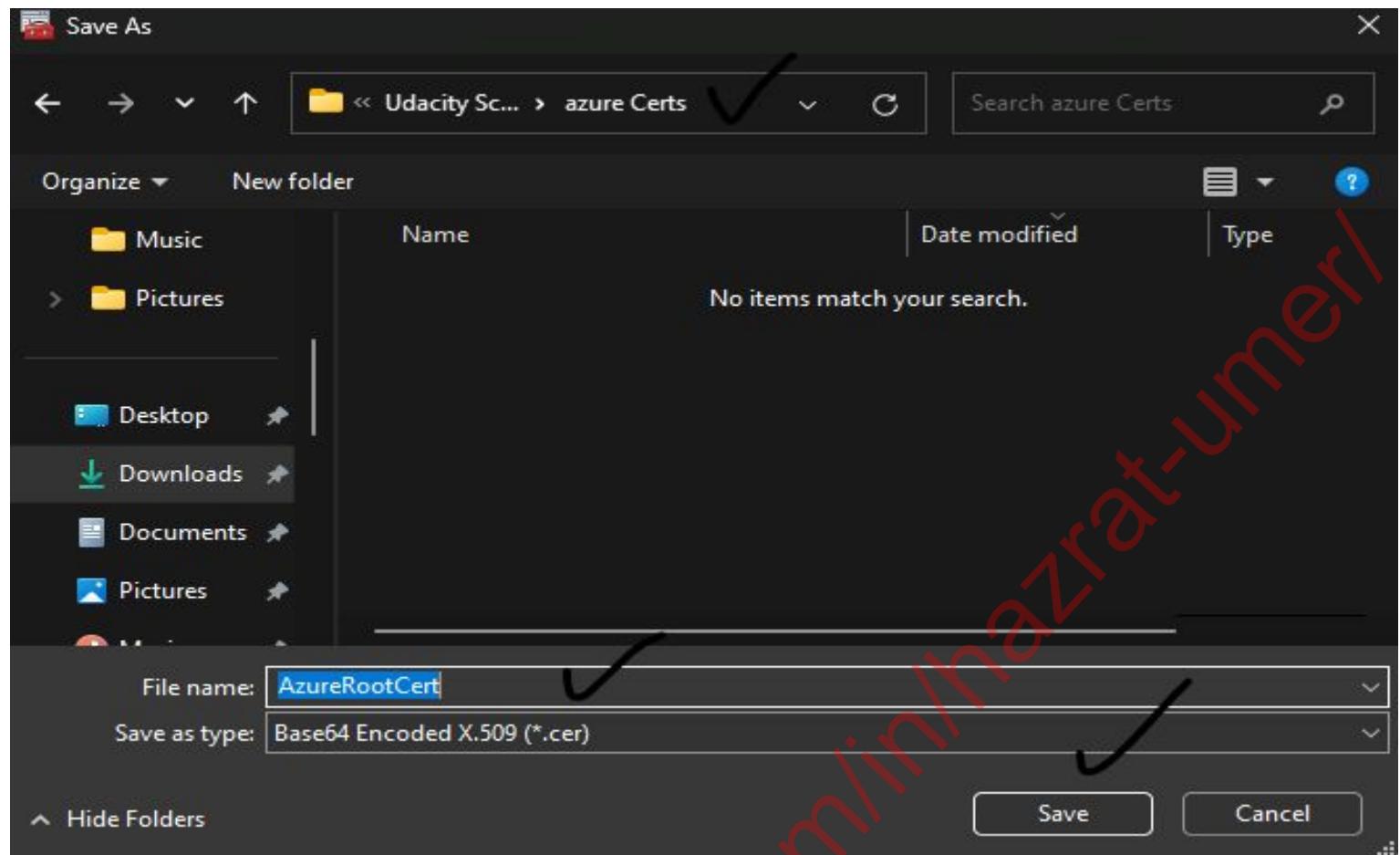
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER) ✓
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Delete the private key if the export is successful
 - Export all extended properties
 - Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

Next

Cancel

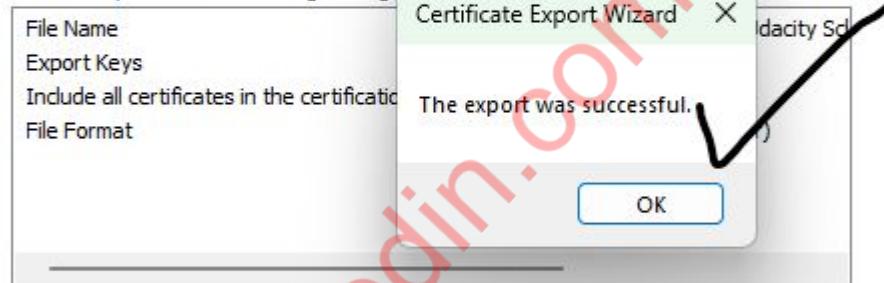




Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

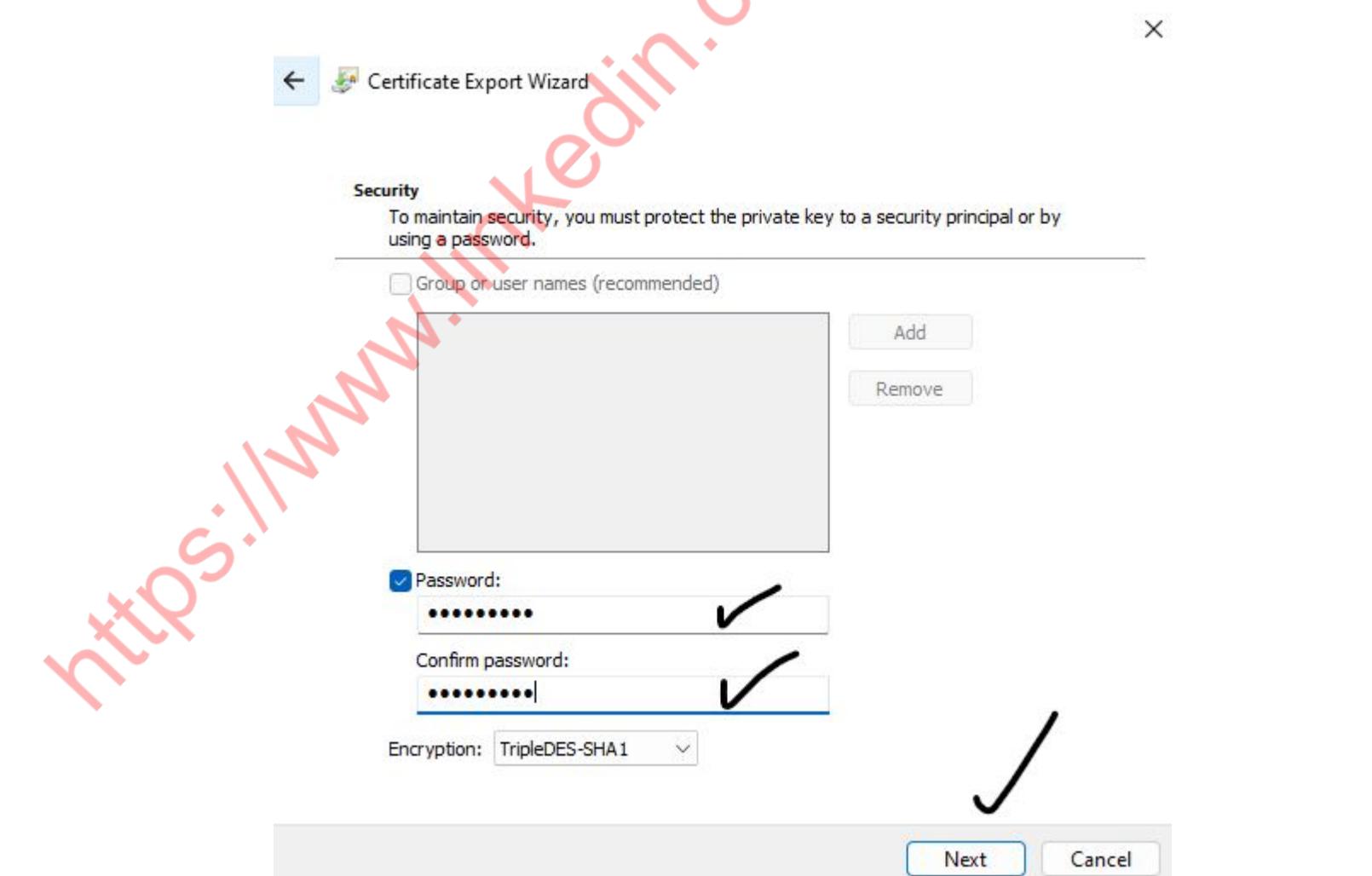
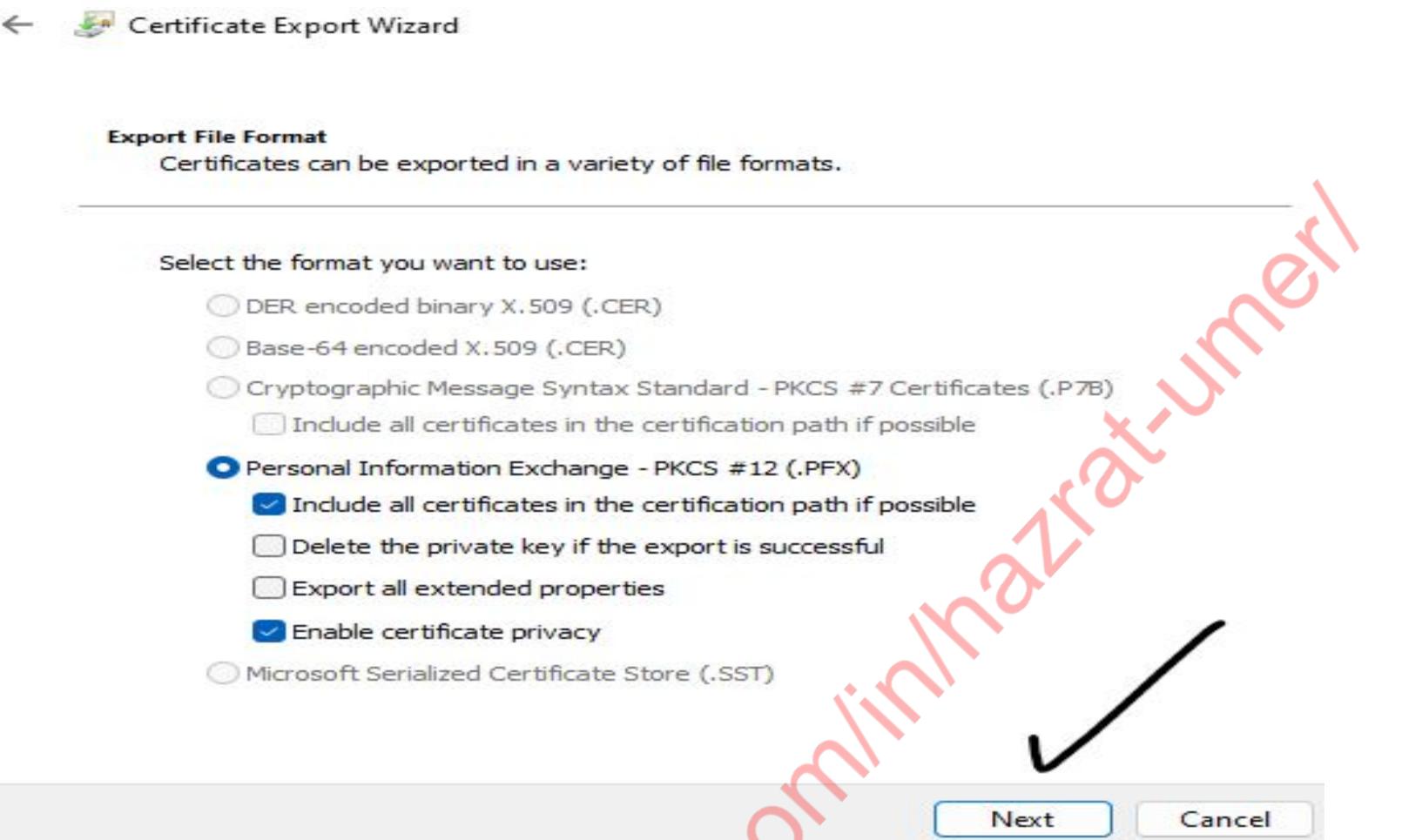


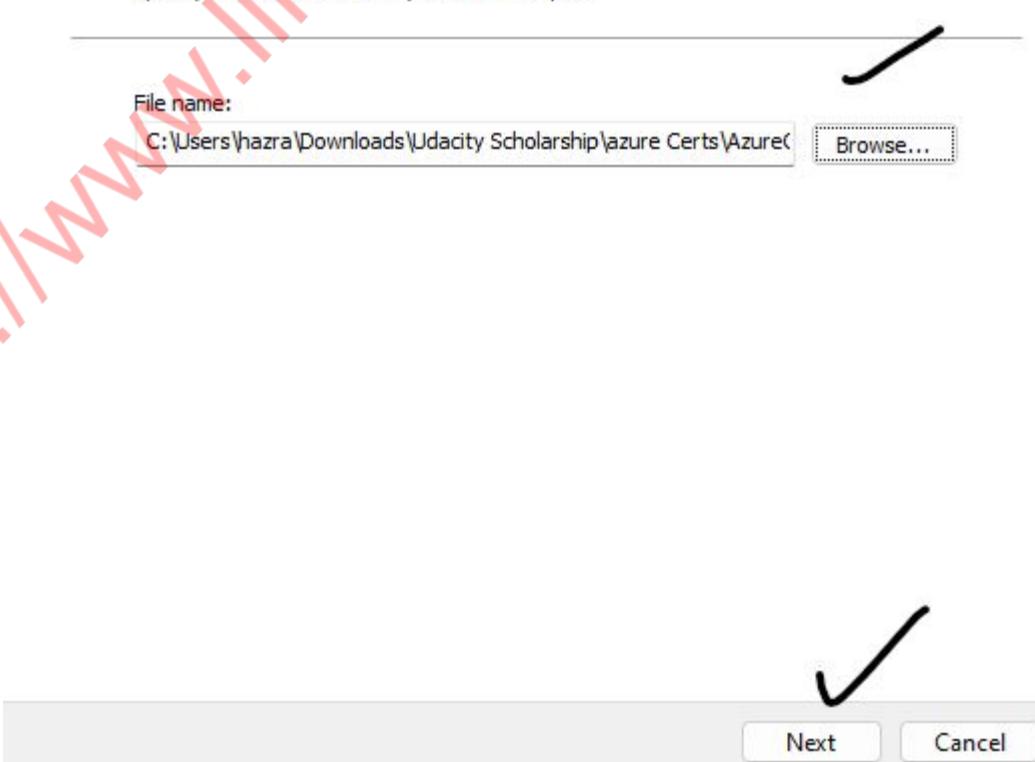
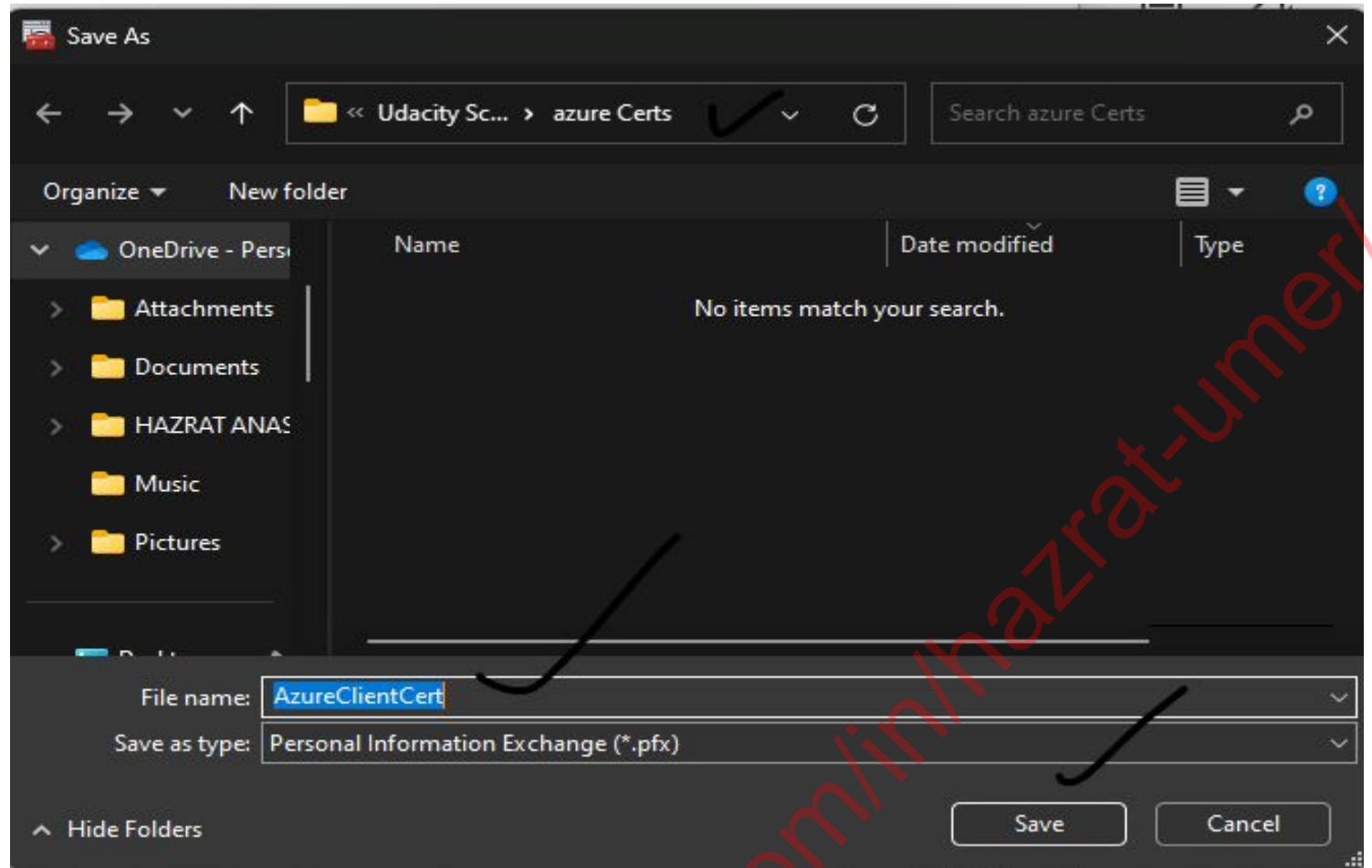
Finish Cancel

Exporting the Client Cert

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







X

Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\hazra\Downloads\Udacity Sc
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx)

Finish

Cancel

X

Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	Certificate Export Wizard
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx)

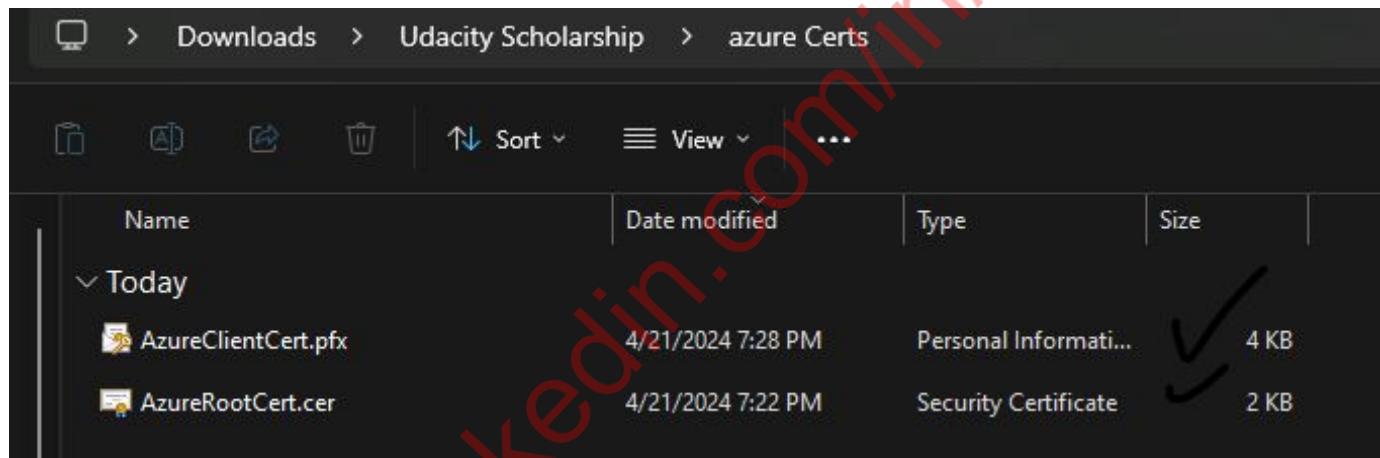
The export was successful.

OK

Finish

Cancel

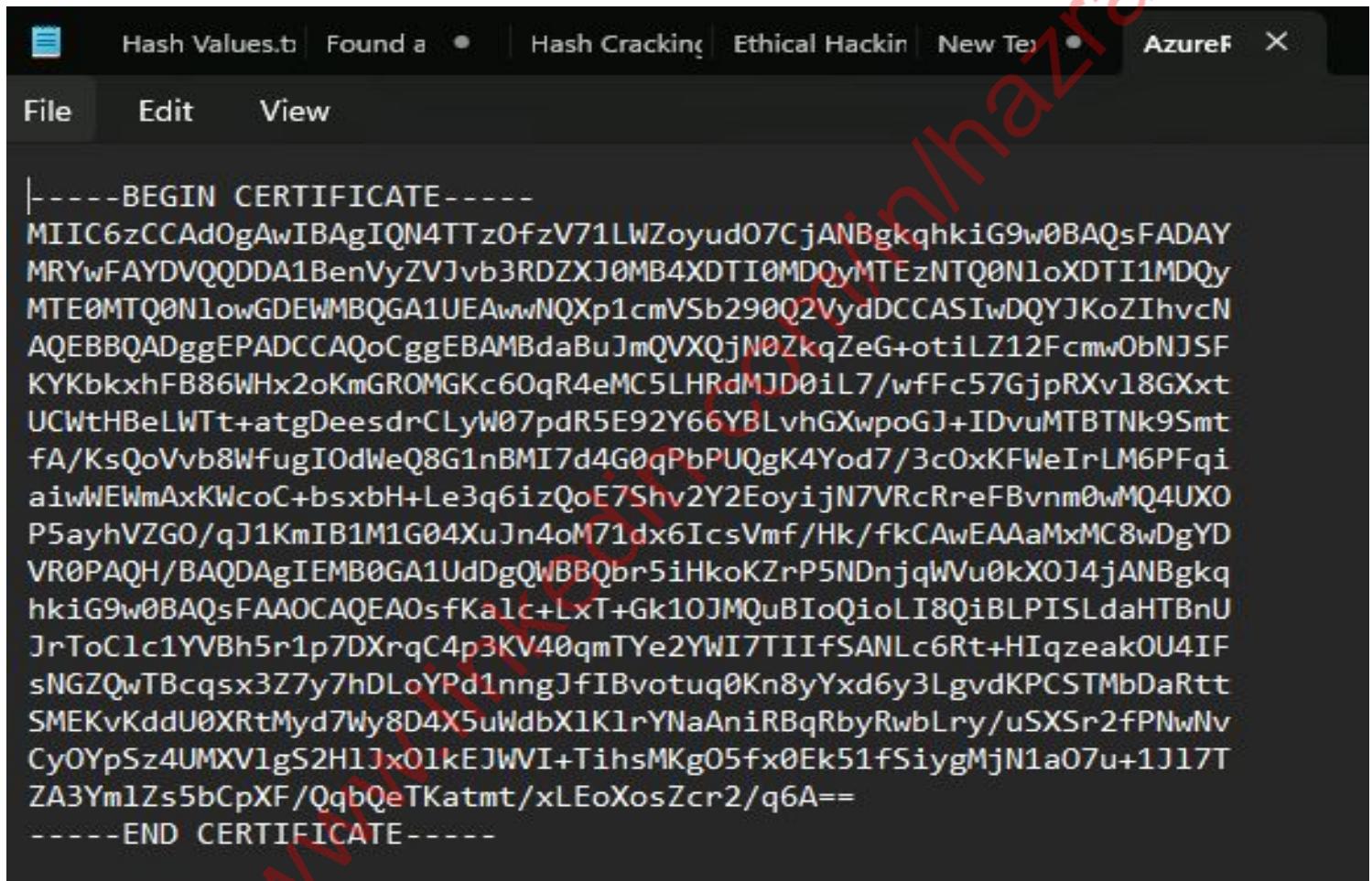
Both Root Cert and Client Certs Exported



A screenshot of a file explorer window titled "Downloads > Udacity Scholarship > azure Certs". The window shows a list of files with the following details:

Name	Date modified	Type	Size
✓ Today			
AzureClientCert.pfx	4/21/2024 7:28 PM	Personal Information Exchange (PFX)	4 KB
AzureRootCert.cer	4/21/2024 7:22 PM	Security Certificate (X.509)	2 KB

Opening the root cert through Notepad and copying its contents



A screenshot of a Windows Notepad window. The title bar says "Hash Values.txt" and the status bar shows "Found a". The menu bar includes "File", "Edit", and "View". The main content area displays a certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIC6zCCAdOgAwIBAgIQN4TTzOfzV71LWZoyud07CjANBgkqhkiG9w0BAQsFADAY
MRYwFAYDVQQDDA1BenVyZVJvb3RDZXJ0MB4XDTI0MDQyMTEzNTQ0N1oXTDI1MDQy
MTE0MTQ0N1owGDEwMBQGA1UEAwwNQXp1cmVSb290Q2VydDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMBdaBuJmQVXQjN0ZkqZeG+otilZ12Fcmmw0bNJSF
KYKbkxhFB86Whx2oKmGROMGKc60qR4eMC5LHRdMJD0iL7/wFFc57GjpRXv18GXxt
UCWtHBeLWTt+atgDeesdrCLyW07pdR5E92Y66YBLvhGXwpoGJ+IDvuMTBTNk9Smt
fA/KsQoVvb8WfugIOdWeQ8G1nBMI7d4G0qPbPUQgK4Yod7/3c0xKFWeIrLM6PFqi
aiwWEwmAxKWcoC+bsxbH+Le3q6izQoE7Shv2Y2EoyijN7VRcRreFBvnm0wMQ4UXO
P5ayhVZGO/qJ1KmIB1M1G04XuJn4oM71dx6IcsVm/ffkCAwEAAsMxMC8wDgYD
VR0PAQH/BAQDAgIE MB0GA1UdDgQWBQBqr5iHkoKZrP5NDnjqWVu0kXOJ4jANBgkq
hkiG9w0BAQsFAAOCAQEAsfKa1c+LxT+Gk10JMQuBIoQioLI8QiBLPISLdaHTBnU
JrToC1c1YVBh5r1p7DXrqC4p3KV40qmTYe2YWI7TIIIfSANLc6Rt+HIqzeakOU4IF
sNGZQwTBcqxs3Z7y7hDL0YPd1nngJfIBvotuq0Kn8yYxd6y3LgvdkPCSTMbDaRtt
SMEKvKddU0XRtMyd7Wy8D4X5uWdbX1K1rYNaAniRBqRbyRwbLry/uSXSr2fPNwNv
Cy0YpSz4UMXV1gS2H1Jx01kEJWVI+TihsMKg05fx0Ek51fSiygMjN1a07u+1J17T
ZA3Ym1Zs5bCpXF/QqbQeTKatmt/xLEoXosZcr2/q6A==
-----END CERTIFICATE-----
```

Pasting it in azure

Root certificates

Name	Public certificate data
azureRoot	MII...ANB✓

✓ ✓

Saving it

Save Discard Delete Download VPN client

Address pool *

192.168.1.0/24 ✓

Tunnel type

IKEv2

Authentication type

Azure certificate

Public IP address for User VPN configuration

A third public IP address is required to use a User VPN configuration with an availability zone SKU gateway in active-active mode

Public IP address * ⓘ

Create new Use existing

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

Waiting for its deployment

Notifications

More events in the activity log → Dismiss all

Deployment in progress... Running ✓ Deployment to resource group 'entp-project-258065' is in progress. a few seconds ago

Your deployment is complete

Deployment name : Microsoft.Network-20240421193747
Subscription : Udacity CloudLabs Sub - 40
Resource group : entp-project-258065
Start time : 4/21/2024, 7:37:55 PM
Correlation ID : 6cb98e57-7f50-473e-a09d-7bf4492e859f

> Deployment details

Next steps

[Go to resource group](#)

Downloading VPN client

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

Home > Enterprise_VPN

Enterprise_VPN | Point-to-site configuration

Virtual network gateway

Search Save Discard Delete Download VPN client

Address pool * 172.16.1.0/24

Tunnel type IKEv2

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

Settings Authentication type

Udacity Sc... > azure Certs

Organize New folder

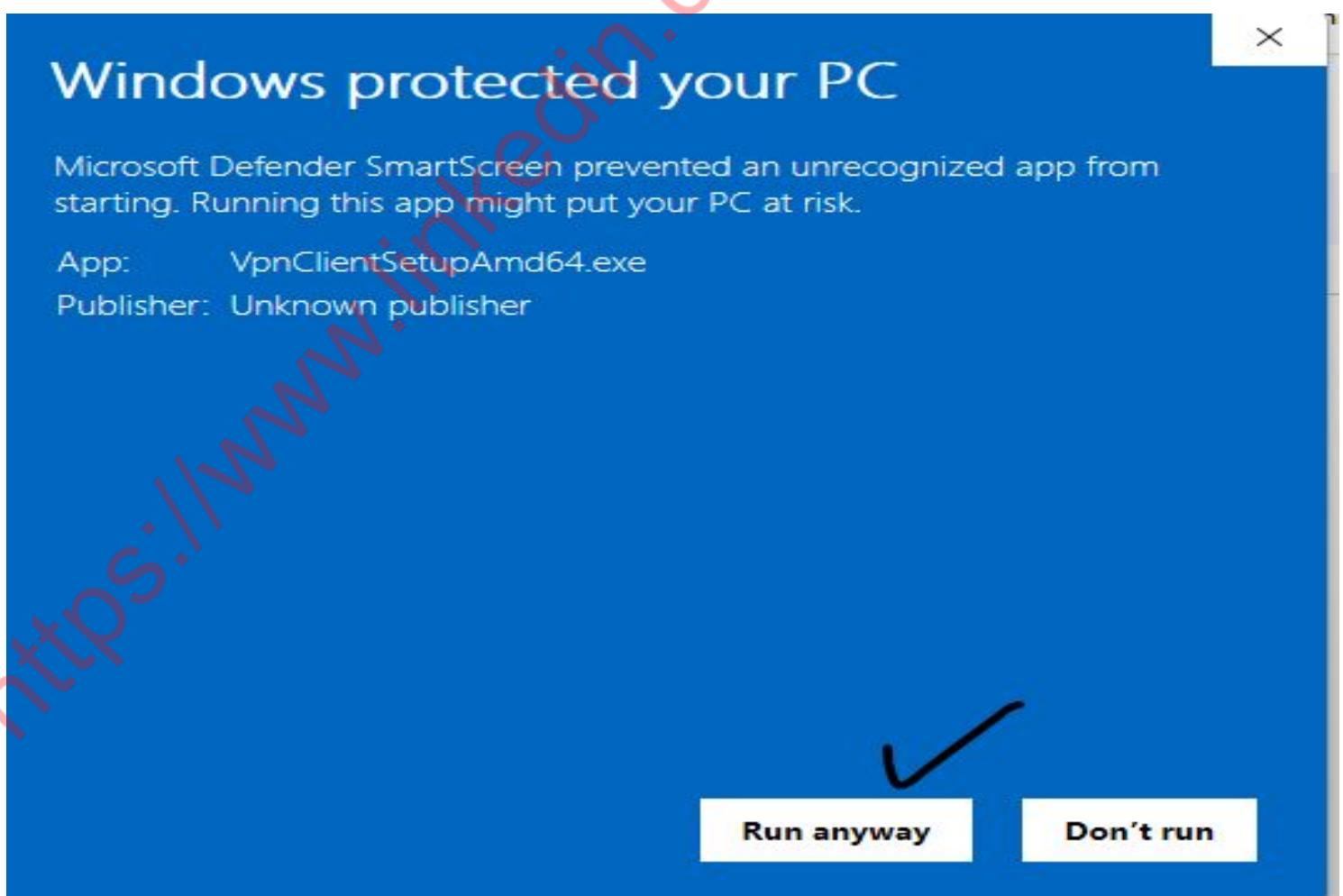
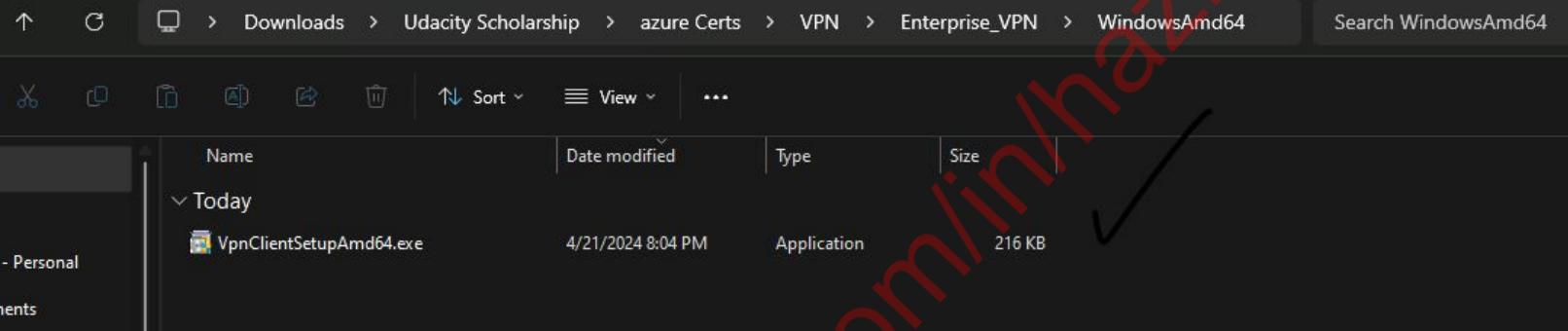
Name	Date modified	Type
VPN	4/21/2024 8:02 PM	File folder

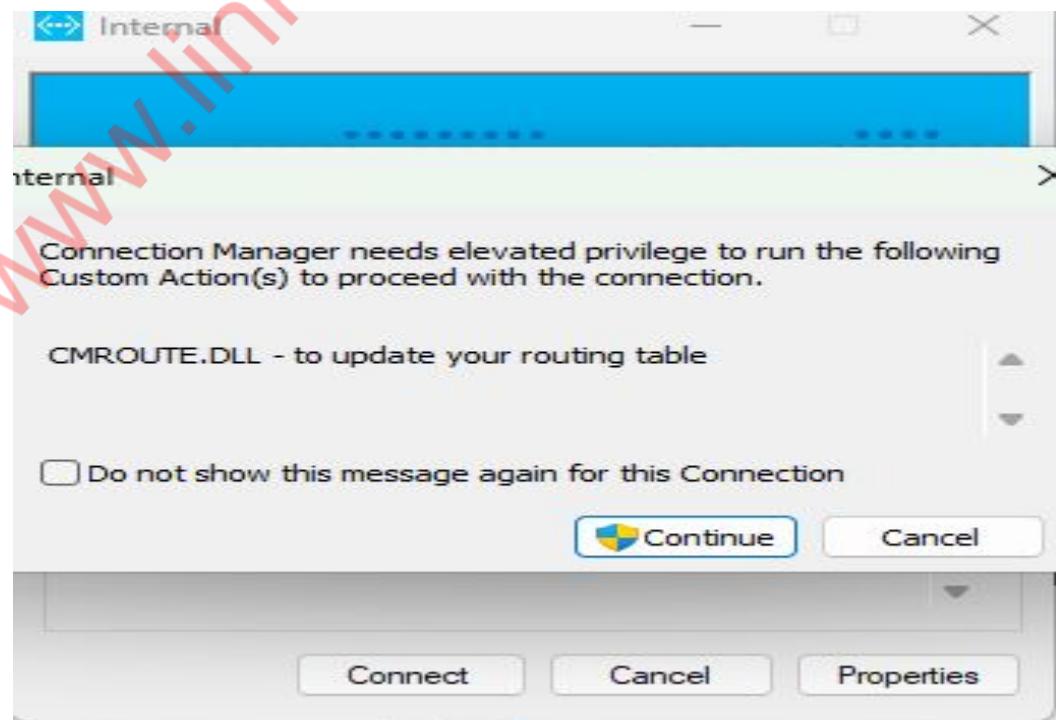
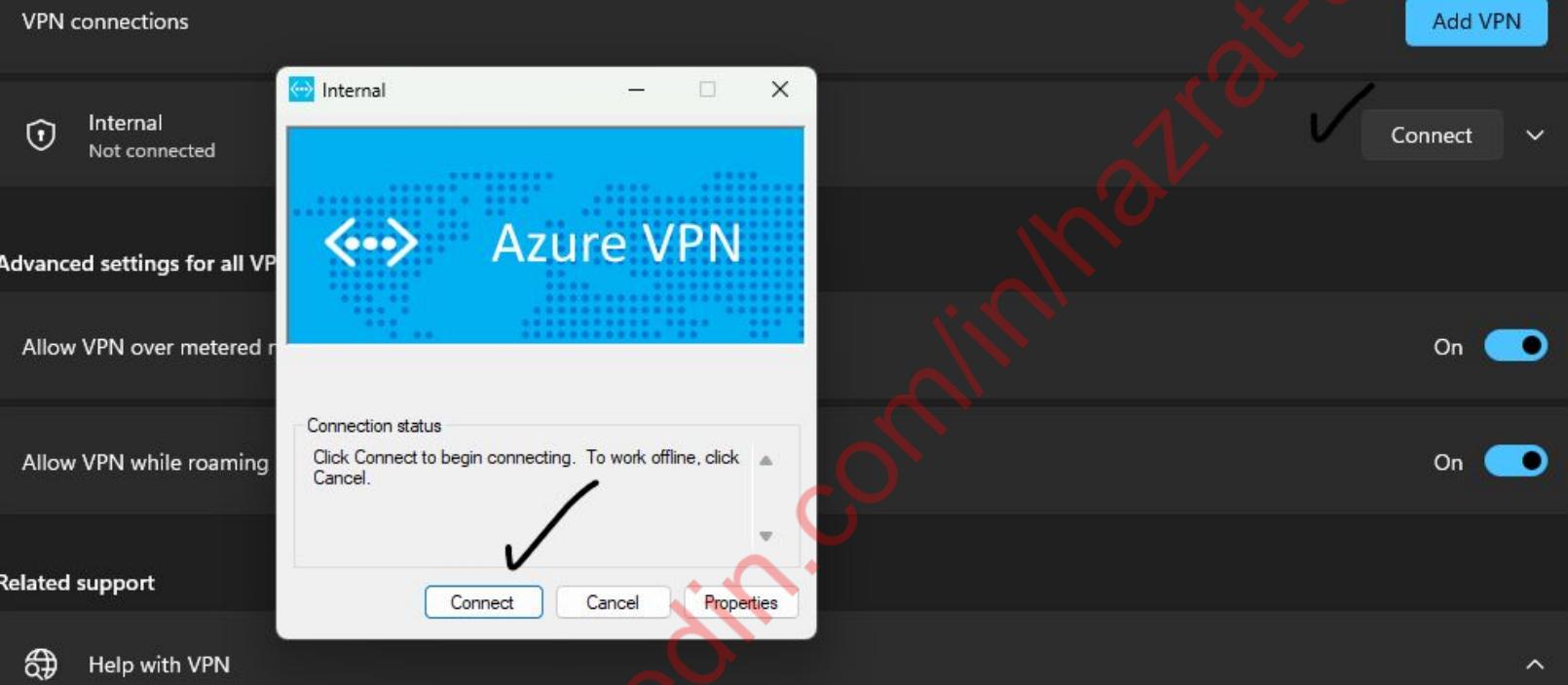
File name: Enterprise_VPN.zip
Save as type: WinRAR ZIP archive (*.zip)

Open Cancel

A screenshot of the Microsoft Azure portal showing the configuration of a Point-to-site virtual network gateway named "Enterprise_VPN". The "Download VPN client" button is highlighted with a black checkmark. Below the configuration, a file explorer window shows a folder structure under "Udacity Sc... > azure Certs". A file named "Enterprise_VPN.zip" is selected for download. A red watermark reading "https://www.linkedin.com/in/hafrat-umer/" is diagonally overlaid across the entire image.

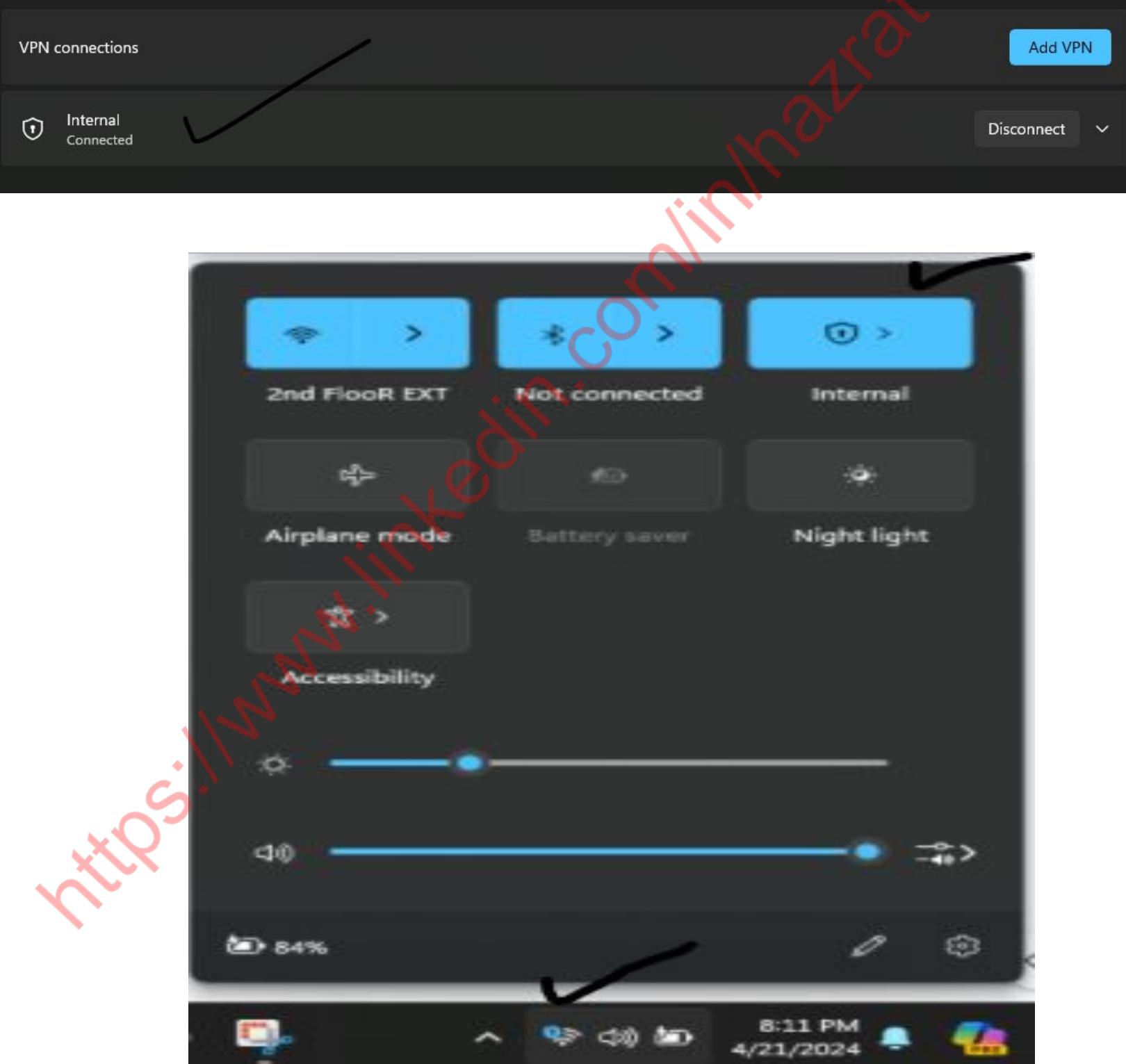
Installing the AMD 64





Successfully Connected

Network & internet > VPN



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.

The screenshot shows the Azure portal interface for a virtual machine named "vmEnterpriseInternal". The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Network settings, Load balancing, and Application security groups. The main content area displays the "Overview" tab for the virtual machine. Key details shown include:

- Networking:** Public IP address: 20.51.207.33 (Network interface: vmenterpriseinternal754_z1)
- Networking:** Private IP address: 10.0.3.4 ✓
- Networking:** Private IP address (IPv6): -
- Networking:** Virtual network/subnet: Internal/Enterprise
- Networking:** DNS name: Configure
- Size:** Standard B1s
- Size:** vCPUs: 1

Pinging VM private IP from my laptop

Successfully pinged

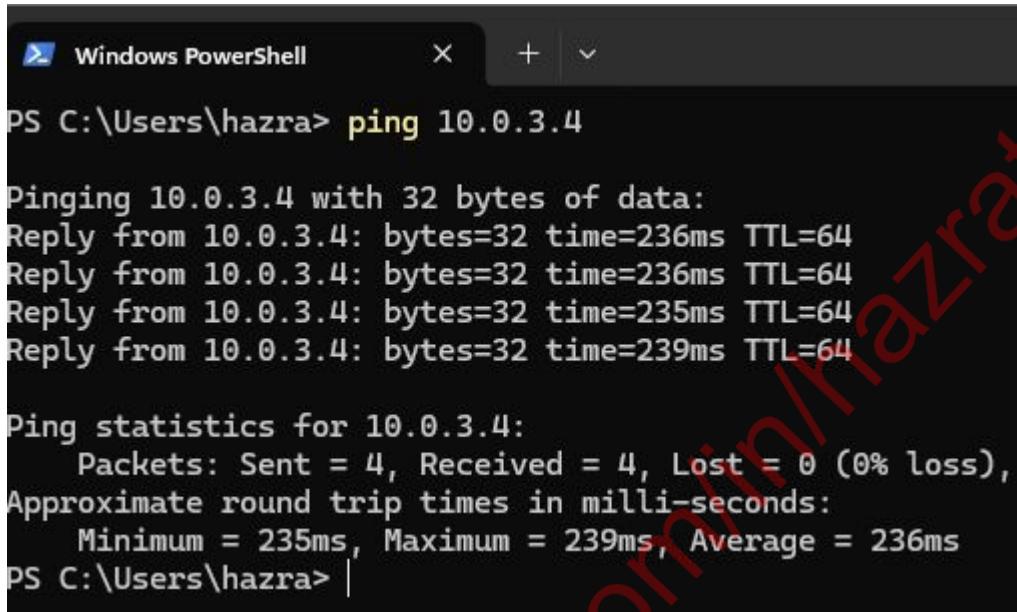
The screenshot displays two windows side-by-side. On the left is the Microsoft Azure portal interface, specifically the 'Virtual machines' section. It shows a single virtual machine named 'vmEnterpriseInternal'. Under the 'Networking' tab, the 'Private IP address' is listed as '10.0.3.4'. On the right is a 'Windows PowerShell' window with the following command and output:

```
PS C:\Users\hazra> ping 10.0.3.4

Pinging 10.0.3.4 with 32 bytes of data:
Reply from 10.0.3.4: bytes=32 time=236ms TTL=64
Reply from 10.0.3.4: bytes=32 time=236ms TTL=64
Reply from 10.0.3.4: bytes=32 time=235ms TTL=64
Reply from 10.0.3.4: bytes=32 time=239ms TTL=64

Ping statistics for 10.0.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 235ms, Maximum = 239ms, Average = 236ms
PS C:\Users\hazra>
```

VM IP

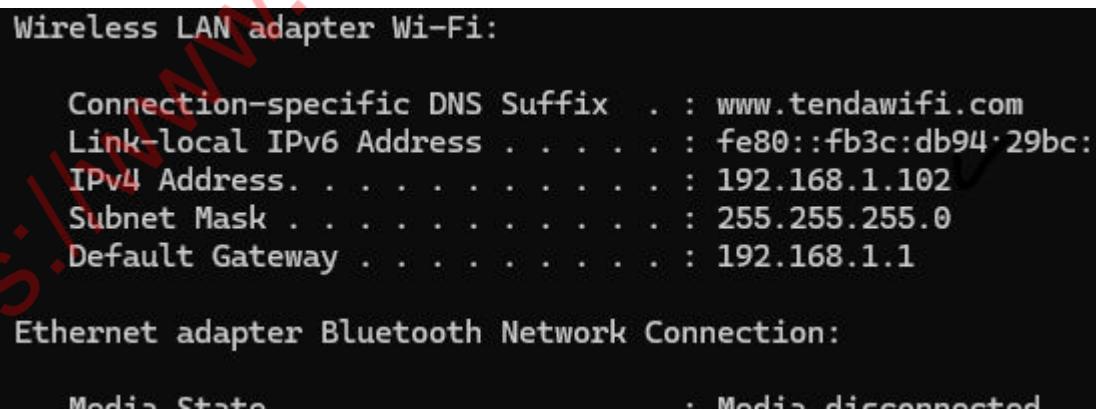


```
PS C:\Users\hazra> ping 10.0.3.4

Pinging 10.0.3.4 with 32 bytes of data:
Reply from 10.0.3.4: bytes=32 time=236ms TTL=64
Reply from 10.0.3.4: bytes=32 time=236ms TTL=64
Reply from 10.0.3.4: bytes=32 time=235ms TTL=64
Reply from 10.0.3.4: bytes=32 time=239ms TTL=64

Ping statistics for 10.0.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 235ms, Maximum = 239ms, Average = 236ms
PS C:\Users\hazra> |
```

My Laptop Private IP



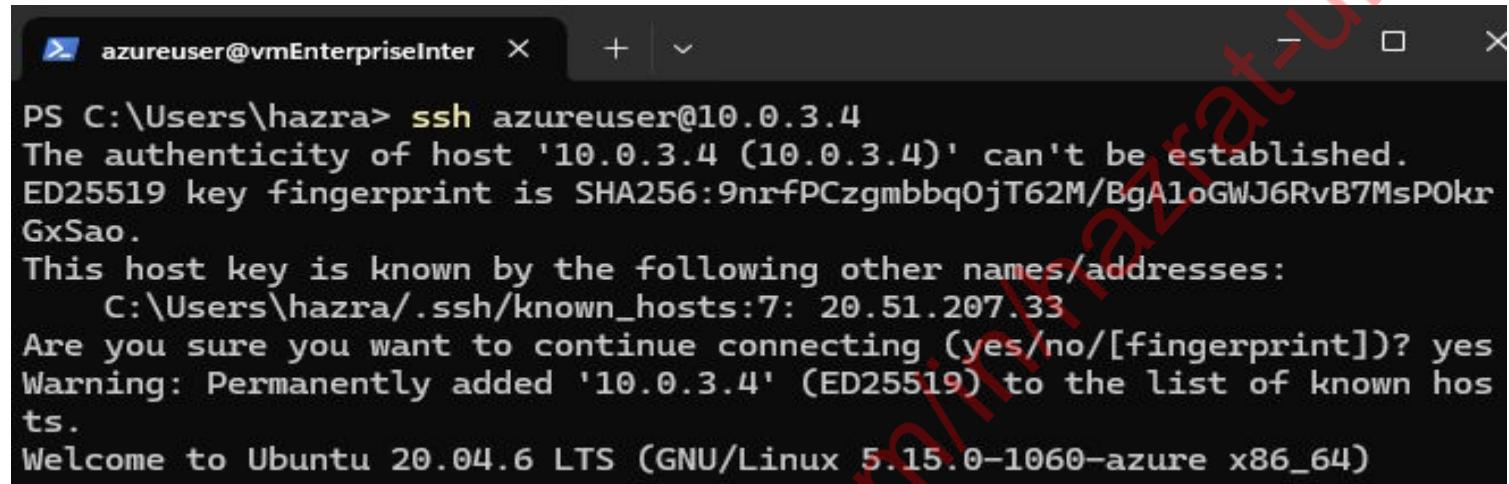
```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : www.tendawifi.com
Link-local IPv6 Address . . . . . : fe80::fb3c:db94%29bc
IPv4 Address . . . . . : 192.168.1.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

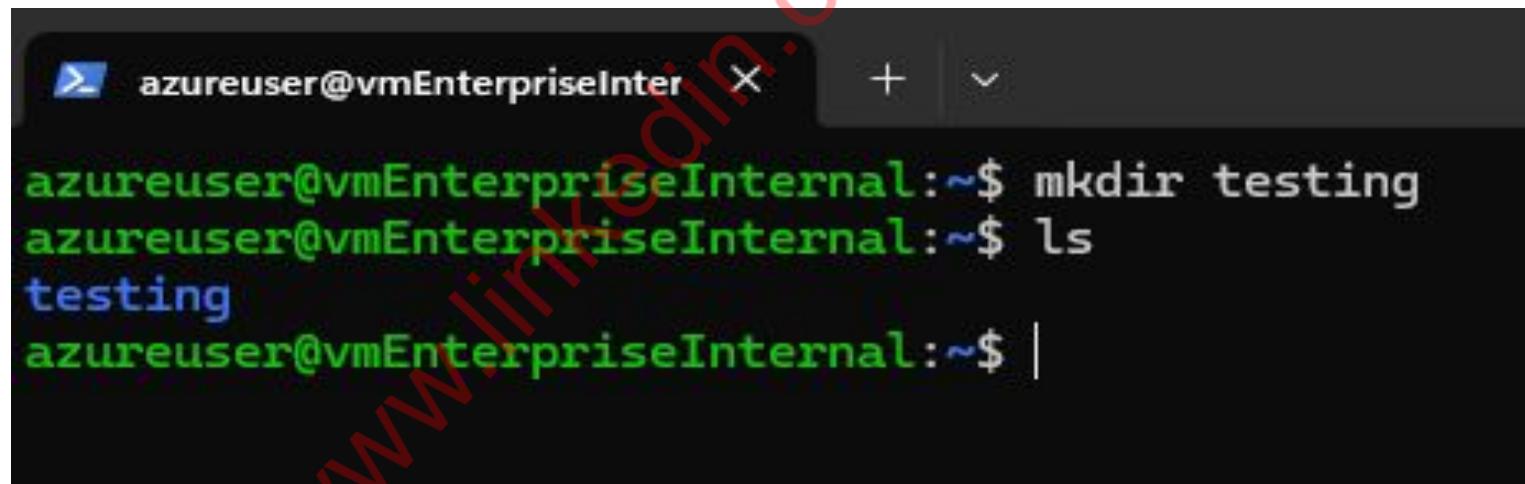
Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
```

Access VM through its Private IP through VPN, using SSH



```
PS C:\Users\hazra> ssh azureuser@10.0.3.4
The authenticity of host '10.0.3.4 (10.0.3.4)' can't be established.
ED25519 key fingerprint is SHA256:9nrfPCzgmbbq0jT62M/BgA1oGWJ6RvB7MsP0kr
GxSao.
This host key is known by the following other names/addresses:
  C:\Users\hazra/.ssh/known_hosts:7: 20.51.207.33
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.4' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1060-azure x86_64)
```



```
azureuser@vmEnterpriseInternal:~$ mkdir testing
azureuser@vmEnterpriseInternal:~$ ls
testing
azureuser@vmEnterpriseInternal:~$ |
```

Section 3

Continuous Monitoring with a SIEM

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

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

Create virtual network ...

Basics Security IP addresses Tags Review + create

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

Subscription * ✓

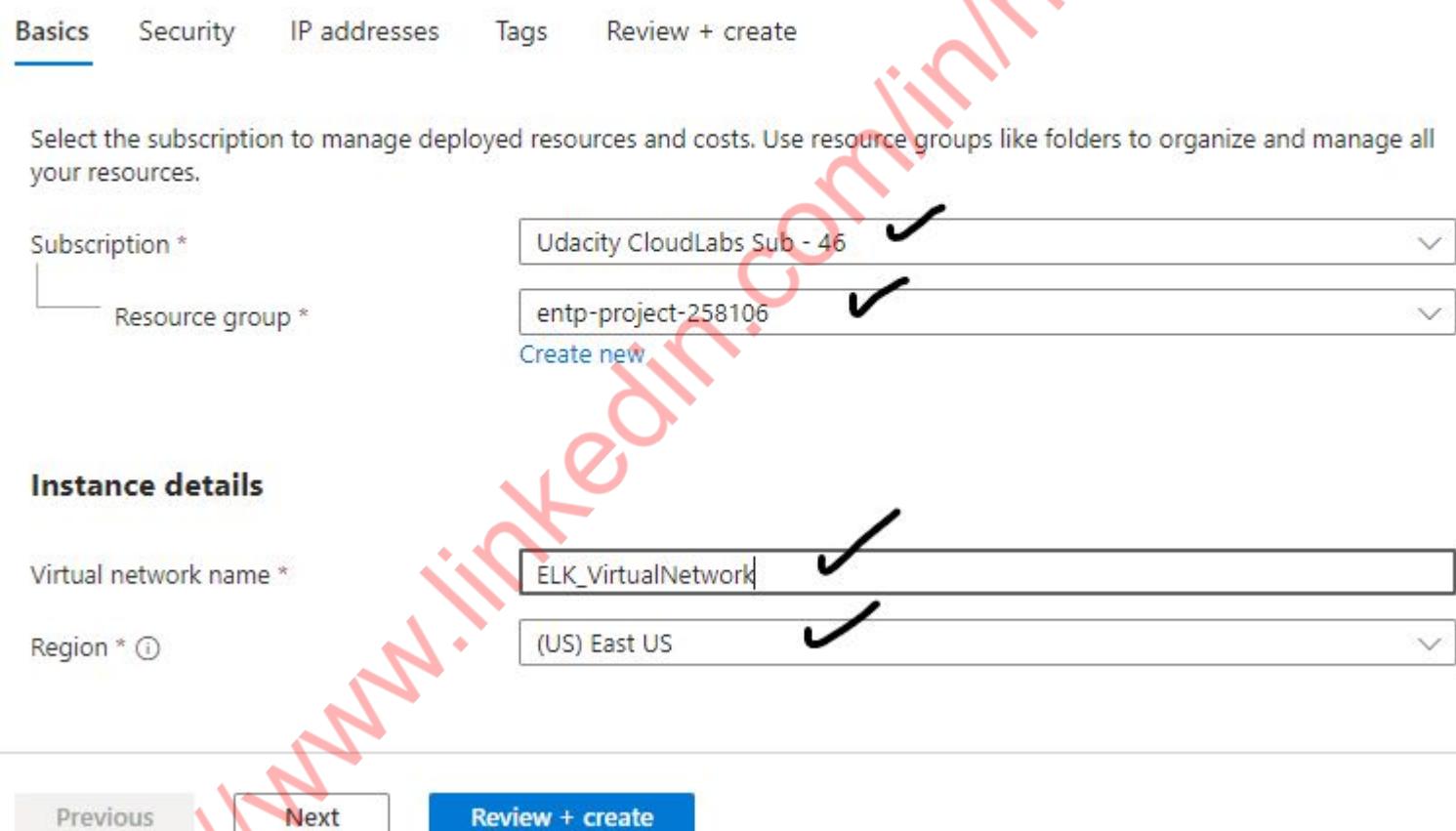
Resource group * ✓
[Create new](#)

Instance details

Virtual network name * ✓

Region * ⓘ ✓

[Previous](#) [Next](#) [Review + create](#)



Leaving the default IP addresses

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

The screenshot shows the 'IP addresses' tab of a virtual network configuration. A new subnet '10.0.0.0/16' has been created, indicated by a checkmark next to its name. The subnet range is 10.0.0.0 - 10.0.255.255, which covers 65,536 addresses. A sub-subnet 'default' has been added within this range, spanning from 10.0.0.0 to 10.0.0.255 (256 addresses). The 'NAT gateway' column shows a '-' sign, indicating no NAT gateway is assigned. There are edit and delete icons for each row.

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

Create network security group

Basics Tags Review + create

Project details

Subscription *

Udacity CloudLabs Sub - 46

Resource group *

entp-project-258106

[Create new](#)

Instance details

Name *

ELK_Network_Security_Group

Region *

East US

Validation passed

Basics Tags Review + create

Basics

Subscription

Udacity CloudLabs Sub - 46

Resource group

entp-project-258106

Region

East US

name

ELK_Network_Security_Group

Tags

None

[Create](#)

[< Previous](#)

[Next >](#)

[Download a template](#)

Network Security group created

Home > Microsoft.NetworkSecurityGroup-20240422004652 | Overview >

 ELK_Network_Security_Group    

Network security group

Search  Move  Delete  Refresh  Give feedback

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

 Inbound security rules  Outbound security rules  Network interfaces  Subnets  Properties  Locks

 Essentials

Resource group ([move](#)) : [entp-project-258106](#) Custom security rules : 0 inbound, 0 outbound
Location : East US Associated with : 0 subnets, 0 network interfaces
Subscription ([move](#)) : [Udacity CloudLabs Sub - 46](#)
Subscription ID : 66b8038e-7f27-48a0-8792-c0511c058f05
Tags ([edit](#)) : [Add tags](#)

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

 Inbound Security Rules

 Outbound Security Rules

Now Creating Virtual Machine!

Home > Virtual machines >

Create a virtual machine

your resources.

Subscription * ⓘ

Udacity CloudLabs Sub - 46 ✓

Resource group * ⓘ

entp-project-258106 ✓

[Create new](#)

Instance details

Virtual machine name * ⓘ

ELK-VM ✓

Region * ⓘ

(US) East US ✓

Availability options ⓘ

Availability zone

Availability zone * ⓘ

Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#) ↗

[< Previous](#)

[Next : Disks >](#)

Review + create

Security type ⓘ

Trusted launch virtual machines

Image * ⓘ

Configure security features

Ubuntu Server 20.04 LTS - x64 Gen2 ✓

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ

Arm64

x64 ✓

Run with Azure Spot discount ⓘ

Selecting a VM Size DS1_V2

Select a VM size ...

Search by VM size...		Display cost : Monthly	vCPUs : All	RAM (GiB) : All	+ Add filter			
Showing 785 VM sizes.	Subscription: Udacity CloudLabs Sub - 46	Region: East US	Current size: Standard_DS1_v2	Image: Ubuntu Server 20.04 LTS	Learn more about VM sizes ↗	Group by series		
VM Size ↑	Type ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Local storage (GiB) ↑↓	Pre	
▼ Most used by Azure users ↗	The most used sizes by users in Azure							
DS1_v2 ↗ ✓	General purpose	1	3.5 ✓	4	3200	7 (SCSI)	Sup	
B1s ↗	General purpose	1	1	2	320	4 (SCSI)	Sup	
➤ B-Series	Ideal for workloads that do not need continuous full CPU performance							
➤ D-Series v2	The 2nd generation D family sizes for your general purpose needs							
➤ Blocked by Policy ⓘ	Your organization has Azure Policies in place that restrict these sizes.							

Select

Prices presented are estimates in USD that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Final charges will appear in your local currency in cost analysis and billing views. [View Azure pricing calculator.](#) ↗

Give feedback

Size * ⓘ

Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (\$53.29/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](#) ↗

Administrator account

Authentication type ⓘ

SSH public key ✓

Password

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

Creating a username and generating and pasting an SSH Key

Administrator account

Authentication type ⓘ

- SSH public key
 Password



i 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 * ⓘ

Pasting My Generated Key here ...



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

x The SSH public key is invalid

< Previous

Next : Disks >

Review + create

First Generating an SSH Key through Powershell

```
Windows PowerShell x Windows PowerShell x + 
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): |
```

Key already exist

```
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.
Overwrite (y/n)? n
PS C:\Users\hazra> |
```

Showing the key

```
PS C:\Users\hazra> cat C:\Users\hazra/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQDzIaMQaOFJrX2ArVo1WYeWd6gCferDf7iinEPeNgvJSJvQuZzbNEE78EHV6xfL4UbzTV2GAyBApVQ+qW9
CVNhxDG9m0y5KrDHGVgMLwJuT4g6Y4Vg72RqdFPnPYtyXTfKEsaCJQkPsuhj8JdgxKcrBzTzY02EuDpVkb5/Ue9ArF2IdALH8simFpJxd6GZU1SOVFsc+EL
ltsIzi9tzhNA3ilAux8l8c++WhqEOPHiVOSzsGRGI4uEye5FcI0z5FcDXHczRv6cQcVENJ7u1z/Rl/rKtf/Ad6sMmS6LSURCkiA14iQtz2AQVm+jYUpFedW8
4PrhJuFbkhw1k6/PXku151Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44hp3Xd10cHrAYR6NAi6EHY0GsdlxTqnG5wFU
sdaLt3MEC1MBUiM/4hbbcrtnAzHpRsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMZpf0= hazra@Eagle
```

Copying and pasting public key to Azure Portal

The screenshot shows the 'Create a new SSH key' form in the Azure portal. It includes fields for 'Username' (set to 'azureuser'), 'SSH public key source' (set to 'Use existing public key'), and 'SSH public key' (containing the copied public key). A note at the bottom says 'Learn more about creating and using SSH keys in Azure'.

Username *	azureuser
SSH public key source	Use existing public key
SSH public key *	<pre>ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgQDzIaMQaOFJrX2ArVo1WYeWd6gCferDf7iinEPeNgvJSJvQuZzbNEE78EHV6xfL4UbzTV2GAyBApVQ+qW9 CVNhxDG9m0y5KrDHGVgMLwJuT4g6Y4Vg72RqdFPnPYtyXTfKEsaCJQkPsuhj8JdgxKcrBzTzY02EuDpVkb5/Ue9ArF2IdALH8simFpJxd6GZU1SOVFsc+EL ltsIzi9tzhNA3ilAux8l8c++WhqEOPHiVOSzsGRGI4uEye5FcI0z5FcDXHczRv6cQcVENJ7u1z/Rl/rKtf/Ad6sMmS6LSURCkiA14iQtz2AQVm+jYUpFedW8 4PrhJuFbkhw1k6/PXku151Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44hp3Xd10cHrAYR6NAi6EHY0GsdlxTqnG5wFU sdaLt3MEC1MBUiM/4hbbcrtnAzHpRsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMZpf0= hazra@Eagle</pre>
<small>i Learn more about creating and using SSH keys in Azure</small>	

Selecting SSH to allow and click next

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)

i 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

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.

Home > Virtual machines > Create a virtual machine > ELK_VirtualNetwork

ELK_VirtualNetwork | Subnets

Virtual network

Search

Subnet Gateway subnet Refresh Manage users Delete

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

Address space Connected devices Subnets Bastion DDoS protection Firewall Microsoft Defender for Cloud

Add subnet

Name * PrivateNetworkSubnet

Subnet address range * 10.0.1.0/24 10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space

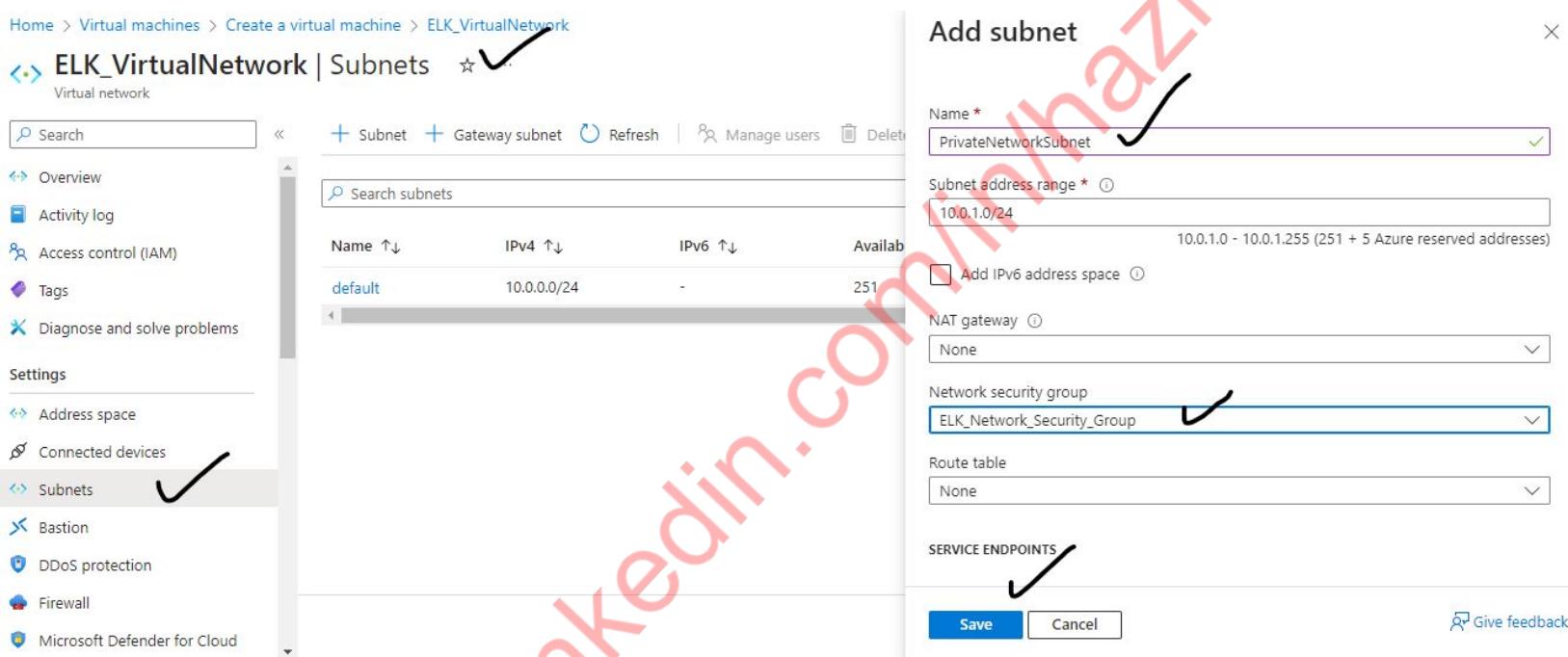
NAT gateway None

Network security group ELK_Network_Security_Group

Route table None

SERVICE ENDPOINTS

Save Cancel Give feedback



Network configurations for our VM

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 * ELK_VirtualNetwork

[Create new](#)

Subnet * PrivateNetworkSubnet (10.0.1.0/24)

[Manage subnet configuration](#)

Public IP (new) ELK-VM-ip

[Create new](#)

NIC network security group None

Basic

Advanced

The selected subnet 'PrivateNetworkSubnet (10.0.1.0/24)' is already associated to a network security group 'ELK_Network_Security_Group'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Configure network security group * ELK_Network_Security_Group

[Create new](#)

Delete public IP and NIC when VM is deleted

Enable accelerated networking

< Previous

Next : Management

Review + create

ELK Server VM is Created

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20240422005150 | Overview >

 ELK-VM Virtual machine

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

Network settings Load balancing Application security groups

Essentials

Resource group ([move](#)) : [entp-project-258106](#)
Status : Running
Location : East US (Zone 1)
Subscription ([move](#)) : [Udacity CloudLabs Sub - 46](#)
Subscription ID : 66b8038e-7f27-48a0-8792-c0511c058f05
Availability zone : 1
Tags ([edit](#)) : [Add tags](#)

Operating system : Linux (ubuntu 20.04)
Size : Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
Public IP address : [20.115.46.64](#)
Virtual network/subnet : [ELK VirtualNetwork/PrivateNetworkSubnet](#)
DNS name : [Not configured](#)
Health state : -

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

Virtual machine

Computer name	ELK-VM
Operating system	Linux (ubuntu 20.04)

Networking

Public IP address	20.115.46.64 (Network interface elk-vm736)
Public IP address (IPv6)	-

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

ELK-VM | Network settings ...

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings ✓

Load balancing

This is a new experience. [Please provide feedback](#)

Network security group **ELK_Network_Security_Group** (attached to subnet: PrivateNetworkSubnet)
Impacts 1 subnets, 1 network interfaces

+ Create port rule ✓

Inbound port rule ✓

Outbound port rule

Priority ↑	Name	Port	Protocol	Source	Destination
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

Add inbound security rule ×

ELK_Network_Security_Group

Source ①

IP Addresses ✓

Source IP addresses/CIDR ranges ★ ① ✓

203.101.190.186 ✓

Source port ranges ★ ① ✓

*

Destination ① ✓

Any

Service ① ✓

SSH

Destination port ranges ① ✓

22

Protocol



Add inbound security rule

X

ELK_Network_Security_Group

Protocol

- Any
- TCP
- UDP
- ICMP

Action

- Allow
- Deny

Priority *

100

Name *

AllowCidrBlockSSHInbound

Description

Allowing SSH from my Laptop

Add

Cancel

Give feedback

Network security group ELK_Network_Security_Group (attached to subnet: PrivateNetworkSubnet)
Impacts 1 subnets, 1 network interfaces

+ Create port rule ▾

Search rules

Source == all

Destination == all

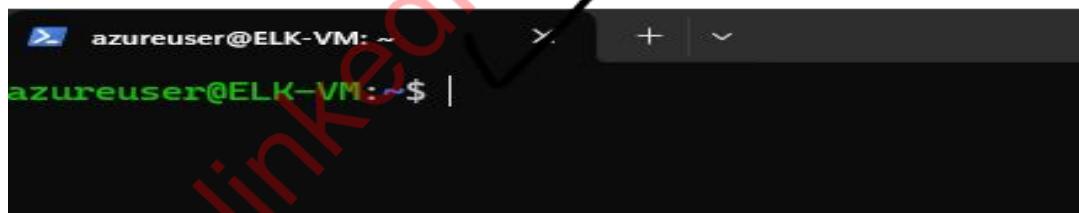
Protocol == all

Action == all

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (4)						
100	AllowCidrBlockSSHInbound	22	TCP	203.101.190.186	Any	Allow
65000	AllowVnetInbound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound ⓘ	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound ⓘ	Any	Any	Any	Any	Deny

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:~$ 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 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu focal/restricted amd64 Packages [22.0 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [661 kB]
```

Installing Docker

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

```
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.service
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

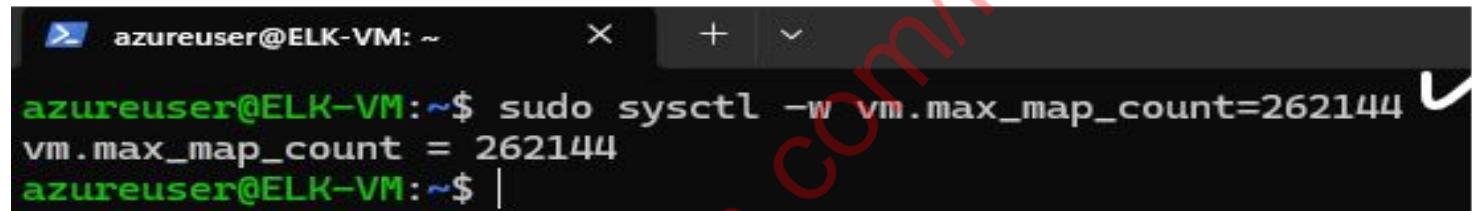
Now using pip3 to install Docker

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) (2019.11.28)
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
```

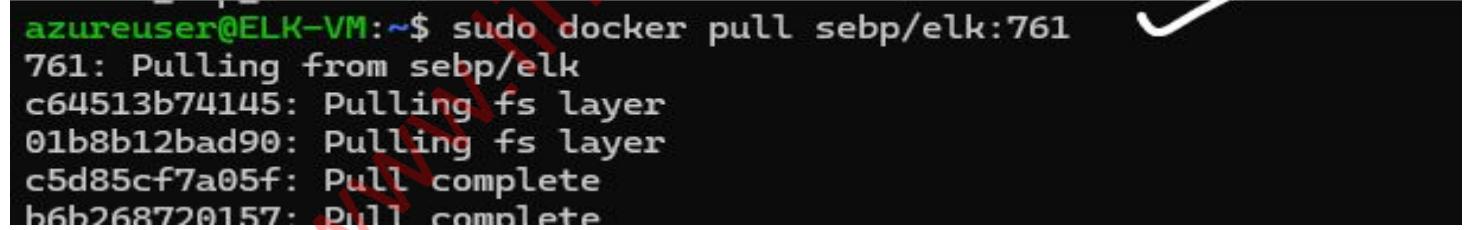
Increasing the Virtual Machine allocated RAM Size

```
sudo sysctl -w  
vm.max_map_count=262144
```



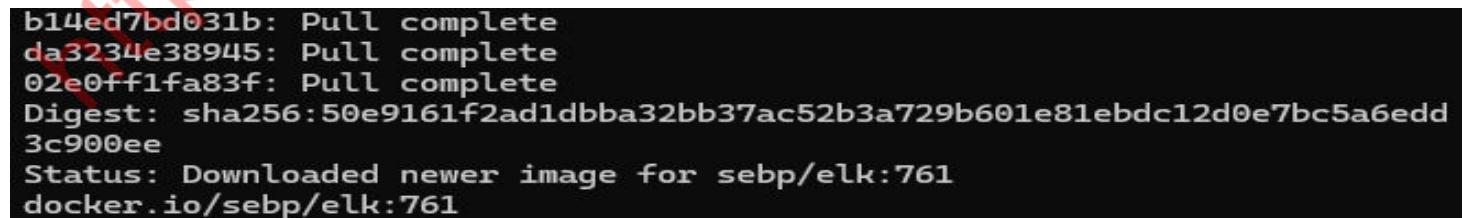
```
azureuser@ELK-VM: ~  
azureuser@ELK-VM:~$ sudo sysctl -w vm.max_map_count=262144  
vm.max_map_count = 262144  
azureuser@ELK-VM:~$ |
```

Downloading the Docker Image that contain the ELK Stack



```
azureuser@ELK-VM:~$ sudo docker pull sebp/elk:761  
761: Pulling from sebp/elk  
c64513b74145: Pulling fs layer  
01b8b12bad90: Pulling fs layer  
c5d85cf7a05f: Pull complete  
b6b268720157: Pull complete
```

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



```
b14ed7bd031b: Pull complete  
da3234e38945: Pull complete  
02e0ff1fa83f: Pull complete  
Digest: sha256:50e9161f2ad1dbba32bb37ac52b3a729b601e81ebdc12d0e7bc5a6edd  
3c900ee  
Status: Downloaded newer image for sebp/elk:761  
docker.io/sebp/elk:761
```

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

```
azureuser@ELK-VM:~$ sudo docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name elk sebp/elk:761  
* Starting periodic command scheduler cron [ OK ]  
* Starting Elasticsearch Server [ OK ] future versions of Elasticsearch  
m [/usr/lib/jvm/java-8-openjdk-amd64/jre] does not meet this requirement [ OK ]  
waiting for Elasticsearch to be up (1/30)
```

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)

Not secure 20.115.46.64:5601/app/kibana#/home

Wingle Web Admin Apple and Cisco Ar... Certified Ethical Ha... Microsoft Certified... https://www.cisco.... Online

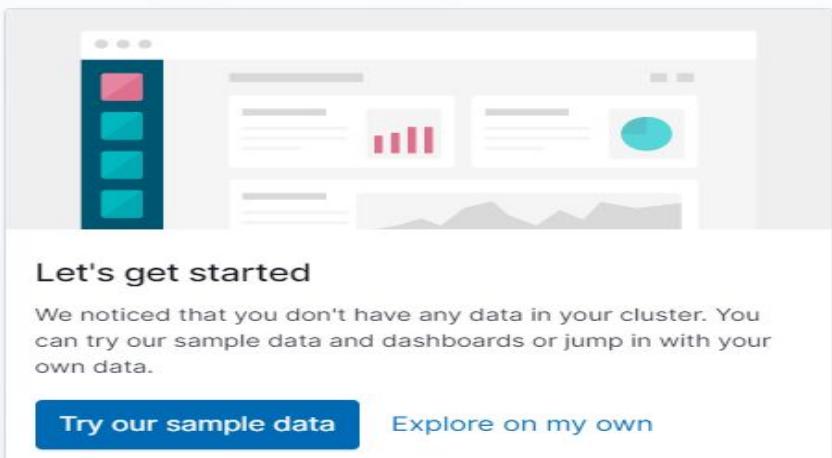
Welcome to Kibana

Your window into the Elastic Stack

Let's get started

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

Try our sample data Explore on my own



Visualizing Web Server Logs into our ELK Server

First Creating Web Server

Creating it in the same virtual network as
the ELK Server

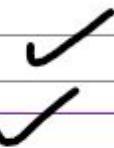
Home > Virtual machines >

Create a virtual machine

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

Subscription * ⓘ

Udacity CloudLabs Sub - 46



Resource group * ⓘ

entp-project-258106

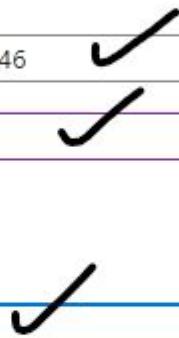


[Create new](#)

Instance details

Virtual machine name * ⓘ

WebServer



Region * ⓘ

(US) East US



Availability options ⓘ

Availability zone

Availability zone * ⓘ

Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

< Previous

Next : Disks >

Review + create

Security type ⓘ

Trusted launch virtual machines

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](#)

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

Enable Hibernation (preview) ⓘ



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

Authentication type ⓘ

SSH public key ✓

Password

i 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+RX2TUxCnLvi3te44hp3Xd1OcHrAYR6NAi6EHY0GsdIxTqngh5wFUUsdaLt3MEC1MBUiM/4hbbcrtNAzHprsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMZpf0= hazra@Eagle ✓

i 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) ✓

i 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 * ⓘ

Subnet * ⓘ

Public IP ⓘ

NIC network security group ⓘ

- None
- Basic
- Advanced

Configure network security group *

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

```
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 established.
ED25519 key fingerprint is SHA256:U7Den8JU0wFa0ivlPNqNayVeQ0zm4+dDM3q4u1x9voU.
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 known 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	Any	VirtualNe
65001	AllowAzureLoadBalancerInBound	ⓘ	Any	Any	Any	AzureLoa
65500	DenyAllInBound	ⓘ	Any	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.

The screenshot shows a web browser window with the title "Apache2 Ubuntu Default Page". The page features the Ubuntu logo and the text "It works!". Below this, there is a "Configuration Overview" section with detailed information about the Apache2 configuration files. The URL in the address bar is "https://www.linkedin.com/in/hazrat-umer/".

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```

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      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"
```

The screenshot shows the Azure portal interface for a virtual machine named 'ELK-VM'. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area displays the VM details. Under 'Virtual machine', it shows the Computer name as 'ELK-VM', Operating system as 'Linux (ubuntu 20.04)', and VM generation as 'V2'. To the right, under 'Networking', it lists the Public IP address as '20.115.46.64 (Network)' and the Private IP address as '10.0.1.4'. A red arrow points from the 'Private IP address' text to the 'hosts' field in the configuration file below.

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

#----- 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

```
#===== Kibana =====  
  
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana  
# This requires a Kibana endpoint configuration.  
setup.kibana: ✓  
  
# Kibana Host  
# Scheme and port can be left out and will be set to the default (http and 5  
# In case you specify an additional path, the scheme is required: http://lo  
# IPv6 addresses should always be defined as: https://[2001:db8::1]:5601  
#host: "localhost:5601"  
  
# Kibana Space ID  
# ID of the Kibana Space into which the dashboards should be loaded. By defa  
# the Default Space will be used.  
#space.id:  
  
Search [setup.kibana]: setup.kibana ✓  
^G Get Help M-C Case Sens M-B Backwards ^P Old  
^C Cancel M-R Regexp M-R Replace ^N New
```

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

```
# Starting with Beats version 6.0.0, the dashboards  
# This requires a Kibana endpoint configuration.  
setup.kibana:  
host: "10.0.1.4:5601" | ✓
```

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

The screenshot shows a web browser window with the URL [babylontraffic.com](https://www.babylontraffic.com) in the address bar. The page features a dark header with the Babylon Traffic logo, a 'Sign In' button, and a 'Join now!' button. Below the header, there's a green success message box containing the text 'Success, you are now disconnected.' The main content area has a world map background and features two prominent buttons: a dark blue one with white text that reads 'INSTANTLY DRIVE TO ANY WEBSITE' and a large red one with white text that reads 'thousands of visits'.

3.2.4 Screenshot

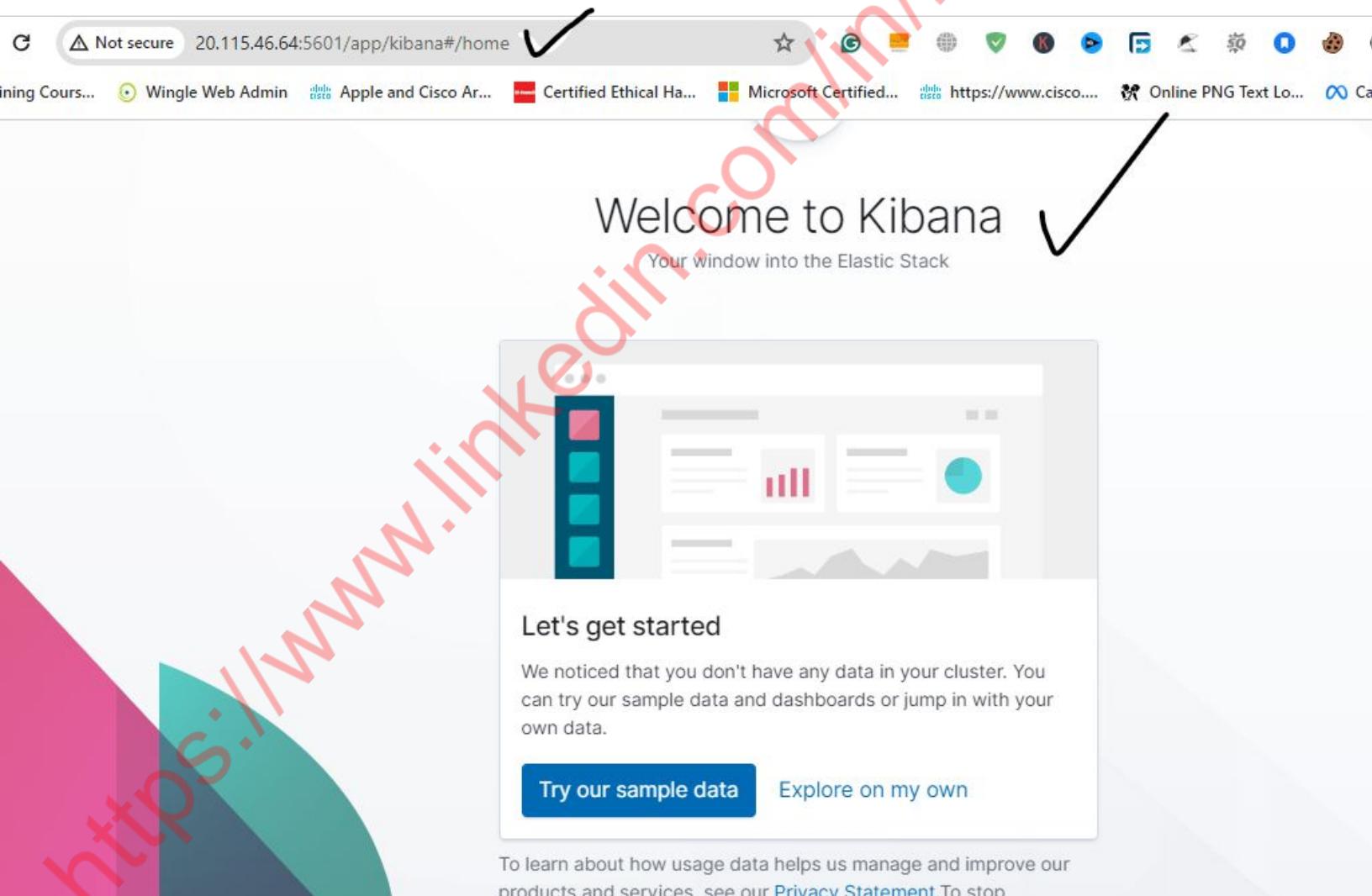
Web server logs appear in Kibana.

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

The screenshot shows the Kibana 7.6.1 management interface. At the top, there's a large blue button with white text that says "Try our sample data". To its right is another button with blue text that says "Explore on my own". A large black checkmark is positioned to the right of the "Explore on my own" button. The background features a blurred view of a dashboard with various charts and graphs.

Let's get started

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

This screenshot shows a web browser window with the URL <https://www.linkedin.com/in/hazrat-umer/>. The page title is "Management". On the left, there's a sidebar with various icons and labels: Management (selected), Visualize, Dashboard, Canvas, Maps, Machine Learning, Metrics, Logs, APM, Uptime, SIEM, Dev Tools, Stack Monitoring, and Management. A large black checkmark is at the bottom of the sidebar. The main content area is titled "Kibana 7.6.1 management" and contains the sub-instruction "Manage your indices, index patterns, saved objects, Kibana settings, and more.". Below this, it says "A full list of tools can be found in the left menu".

Licence Management

The screenshot shows the Elasticsearch License Management interface. On the left is a vertical sidebar with icons for different management tasks: D (Management), Clock (Timeline), Leaf (Usage Data), Bar chart (Index Management), Book (Index Lifecycle Policies), Radar (Rollup Jobs), Cloud (Transforms), Cloud (Remote Clusters), Camera (Snapshot and Restore), a checkmark icon (License Management), and a gear (8.0 Upgrade Assistant). The main panel has a header "Help us improve the Elastic Stack" with a "Dismiss" button. Below it, under "Elasticsearch", is a list of items: Index Management, Index Lifecycle Policies, Rollup Jobs, Transforms, Remote Clusters, Snapshot and Restore, License Management, and 8.0 Upgrade Assistant. A large checkmark is drawn over the "License Management" item.

Click on start 30 days trial

✓ Your Basic license is active

Your license will never expire.

Update your license

already have a new license, upload it now.

Update license

Start a 30-day trial

Experience what machine learning, advanced security, and all our other Platinum features have to offer.

Start trial

Start 30 Days Trial

Start your free 30-day trial

This trial is for the full set of [Platinum features](#) of the Elastic Stack. You'll get immediate access to:

- Machine learning
- Alerting
- Graph capabilities
- JDBC and ODBC connectivity for SQL

Advanced security features, such as authentication (AD/LDAP, SAML, PKI, SAML/SSO), field- and document-level security, and auditing, require configuration. See the [documentation](#) for instructions.

[Cancel](#)

[Start my trial](#)

Your Trial license is active
Your license will expire on **May 22, 2024 9:22 AM PKT**

Click on Discover

The screenshot shows the Kibana interface with a prominent 'Discover' button highlighted by a black arrow. The interface includes a navigation bar with tabs like 'Management / License management' and 'Elasticsearch'. A modal window is open, asking for feedback on improving the Elastic Stack, with 'Discover' and 'Dismiss' buttons. Below the modal, there are links for 'Index Management', 'Index Lifecycle Policies', 'Rollup Jobs', 'Transforms', and 'Cross-Cluster Replication'. On the left, a sidebar lists various management options. At the bottom, a 'Create index pattern' section is shown, with a checked checkbox labeled 'Step 1 of 2: Define index pattern'. The text 'We can see index pattern' is overlaid on the right side of the interface.

Continuous Monitoring & Analytics

Kibana

Management / License management

Elasticsearch

Discover

Dismiss

Help us improve the Elastic Stack

Index Management

Index Lifecycle Policies

Rollup Jobs

Transforms

Cross-Cluster Replication

Remote Clusters

Watcher

Snapshot and Restore

License Management

8.0 Upgrade Assistant

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Step 1 of 2: Define index pattern

Index pattern

index-name-*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

Your index pattern can match any of your 2 indices, below.

filebeat-7.4.0-2024.04.22-000001

ilm-history-1-000001

Rows per page: 10

We can see index pattern

Defining Index Pattern

Type file the filebeat pattern will

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Include system indices

Step 1 of 2: Define index pattern

Index pattern

file*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ Success! Your index pattern matches 1 index.

filebeat-7.4.0-2024.04.22-000001



> Next step

Rows per page: 10

Paste it and select next

Step 1 of 2: Define index pattern

Index pattern

filebeat-7.4.0-2024.04.22-000001



You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

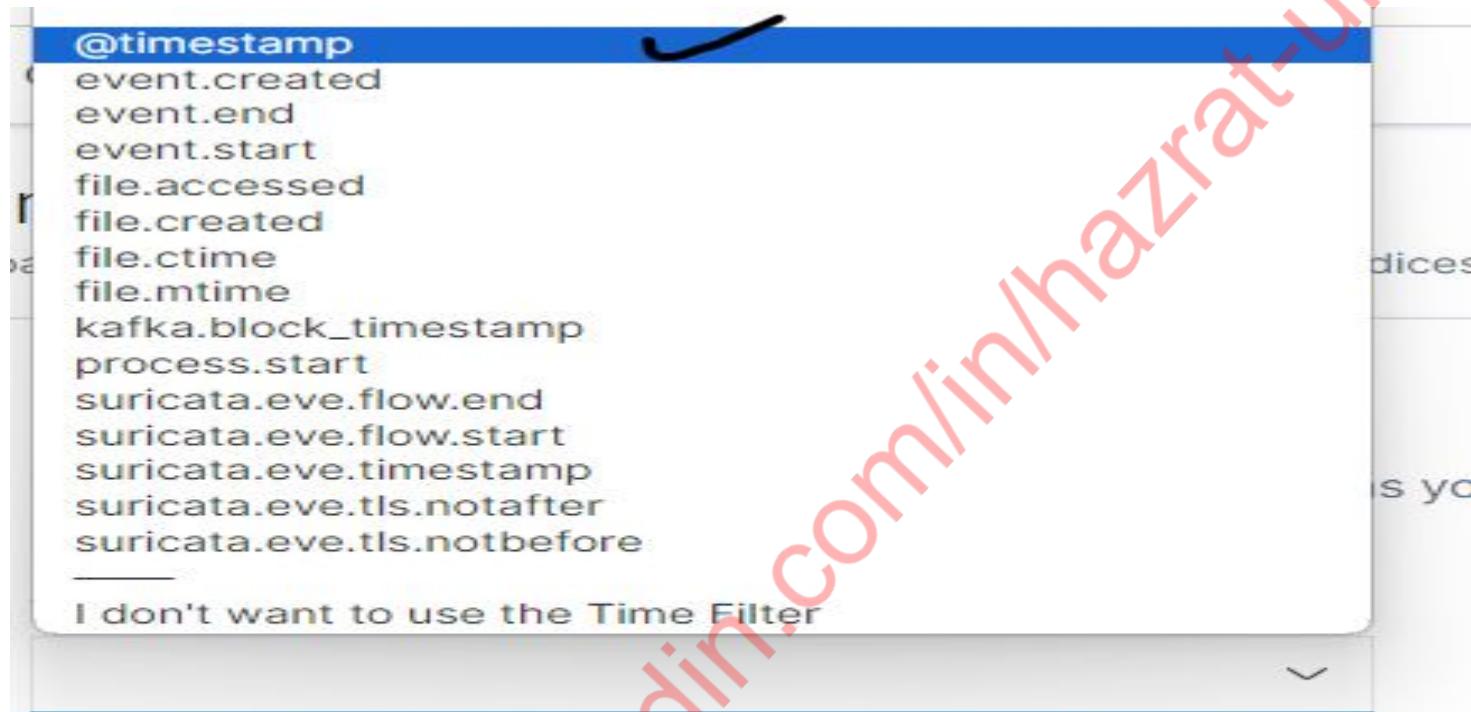
✓ Success! Your index pattern matches 1 index.

filebeat-7.4.0-2024.04.22-000001



> Next step

Select @timestamp



The Time Filter will use this field to filter your data by time.
You can choose not to have a time field, but you will not be able to
narrow down your data by a time range.

> Show advanced options

Then click on create index pattern

Index pattern generated

★ filebeat-7.4.0-2024.04.22-000001 ✓

Time Filter field name: @timestamp Default

This page lists every field in the **filebeat-7.4.0-2024.04.22-000001** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#) ↗

Fields (1130)	Scripted fields (0)	Source filters (0)				
Q Filter						All field types ▾
Name	Type	Format	Searchable	Aggregatable	Excluded	
@timestamp ⓘ	date		•	•		✎
_id	string		•	•		✎
_index	string		•	•		✎
_score	number					✎
_source	source					✎

Now Click on Discover

The screenshot shows the Elasticsearch Management interface. At the top, there are two tabs: "Continuous Monitoring" and "filebeat-7.4.0-20210720". Below the tabs, the URL bar shows "Not secure 20.115.46.64:5601/app". The main navigation bar includes links for "Free Training Courses", "Wingle Web Admin", and "Apple". On the left, there's a sidebar with various icons and labels: "Management / Index patterns / filebe", "Elasticsearch", "Index Management", "Discover" (which is highlighted with a black callout bubble and a black arrow pointing to it), "Lifecycle Policies", "Jobs", "Transforms", "Cross-Cluster Replication", "Remote Clusters", "Watcher", "Snapshot and Restore", "License Management", and "8.0 Upgrade Assistant". To the right, there are sections for "Time Filter", "This page", "Elastics", "Fields", and "Filters". A red watermark with the URL "https://www.linkedin.com/in/nazatumer/" is diagonally across the page.

We are able to visualize our web server logs

Not secure 20.115.46.64:5601/app/kibana#/discover?_g=()&_a=(columns:_source,...)

Free Training Cours... Wingle Web Admin Apple and Cisco Ar... Certified Ethical Ha... Microsoft Certified... https://www.cisco... Online PNG Text Lo... Camera Effects > All Bookmarks

Discover

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

New Save Open Share Inspect

filebeat-7.4.0-2024.0... ▾

Search KQL Last 15 minutes Show dates Refresh

Count

120 hits

Apr 22, 2024 @ 09:29:22.591 - Apr 22, 2024 @ 09:44:22.591 — Auto

0 20 40 60

09:30:00 09:31:00 09:32:00 09:33:00 09:34:00 09:35:00 09:36:00 09:37:00 09:38:00 09:39:00 09:40:00 09:41:00 09:42:00 09:43:00 09:44:00

✓

Selected fields

_source

Available fields

@timestamp

120 hits

0 20 40 60

09:30:00 09:31:00 09:32:00 09:33:00 09:34:00 09:35:00 09:36:00 09:37:00 09:38:00 09:39:00 09:40:00 09:41:00 09:42:00 09:43:00 09:44:00

Available fields

@timestamp

_id

_index

_score

_type

agent.ephemeral_id

agent.hostname

agent.id

agent.type

agent.version

cloud.instance.id

cloud.instance.name

cloud.machine.type

cloud.provider

cloud.region

Time ▾

09:31:00 09:32:00 09:33:00 09:34:00 09:35:00 09:36:00 09:37:00 09:38:00 09:39:00 09:40:00 09:41:00 09:42:00 09:43:00 09:44:00

_source

Apr 22, 2024 @ 09:44:16.000

agent.hostname: WebServer agent.id: 4ceec601-d12d-4921-9a6b-610c280b871c agent.type: filebeat
agent.ephemeral_id: fc7757f6-f9b0-4606-82d6-d02d3e29397e agent.version: 7.4.0
log.file.path: /var/log/apache2/access.log log.offset: 6,321 source.geo.continent_name: Asia
source.geo.country_iso_code: PK source.geo.location: { "lon": 70, "lat": 30 } source.address: 203.101.190.186
source.ip: 203.101.190.186 fileset.name: access url.original: / cloud.instance.name: WebServer

Apr 22, 2024 @ 09:44:16.000

agent.hostname: WebServer agent.id: 4ceec601-d12d-4921-9a6b-610c280b871c agent.type: filebeat
agent.ephemeral_id: fc7757f6-f9b0-4606-82d6-d02d3e29397e agent.version: 7.4.0
log.file.path: /var/log/apache2/access.log log.offset: 6,528 source.geo.continent_name: Asia
source.geo.country_iso_code: PK source.geo.location: { "lon": 70, "lat": 30 } source.address: 203.101.190.186
source.ip: 203.101.190.186 fileset.name: access url.original: / cloud.instance.name: WebServer

Apr 22, 2024 @ 09:44:15.000

agent.hostname: WebServer agent.id: 4ceec601-d12d-4921-9a6b-610c280b871c agent.type: filebeat
agent.ephemeral_id: fc7757f6-f9b0-4606-82d6-d02d3e29397e agent.version: 7.4.0
log.file.path: /var/log/apache2/access.log log.offset: 5,907 source.geo.continent_name: Asia
source.geo.country_iso_code: PK source.geo.location: { "lon": 70, "lat": 30 } source.address: 203.101.190.186
source.ip: 203.101.190.186 fileset.name: access url.original: / cloud.instance.name: WebServer

Apr 22, 2024 @ 09:44:15.000

agent.hostname: WebServer agent.id: 4ceec601-d12d-4921-9a6b-610c280b871c agent.type: filebeat
agent.ephemeral_id: fc7757f6-f9b0-4606-82d6-d02d3e29397e agent.version: 7.4.0
log.file.path: /var/log/apache2/access.log log.offset: 5,907 source.geo.continent_name: Asia
source.geo.country_iso_code: PK source.geo.location: { "lon": 70, "lat": 30 } source.address: 203.101.190.186
source.ip: 203.101.190.186 fileset.name: access url.original: / cloud.instance.name: WebServer

https://www.linkedin.com/in/hazratumer/

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.

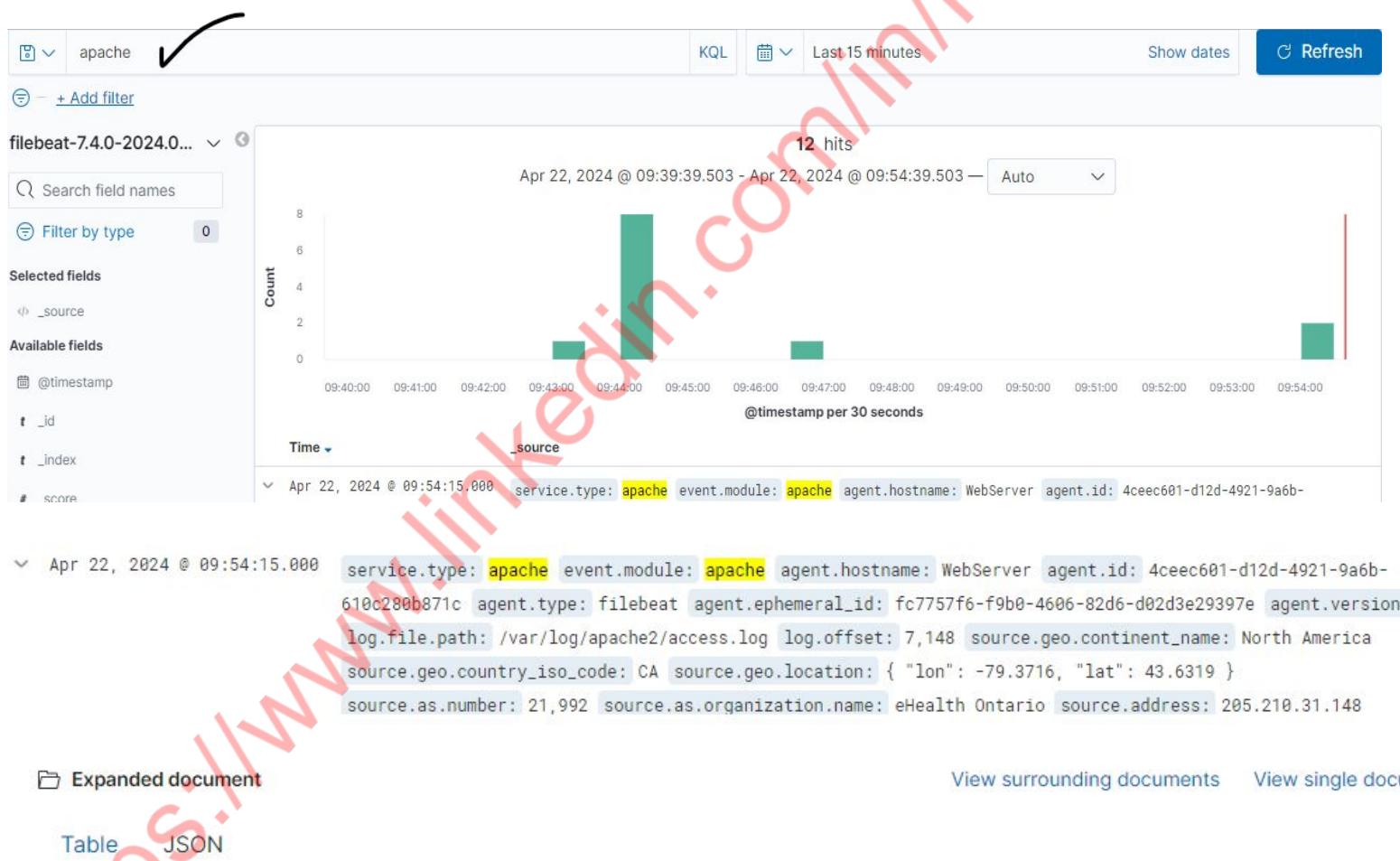
Insert screenshots on the following pages, showing completion of each of the specified tasks.

3.3.1 Screenshot

Create an alert for DoS attack.

STeps:

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



Now Expand one of the Apache log

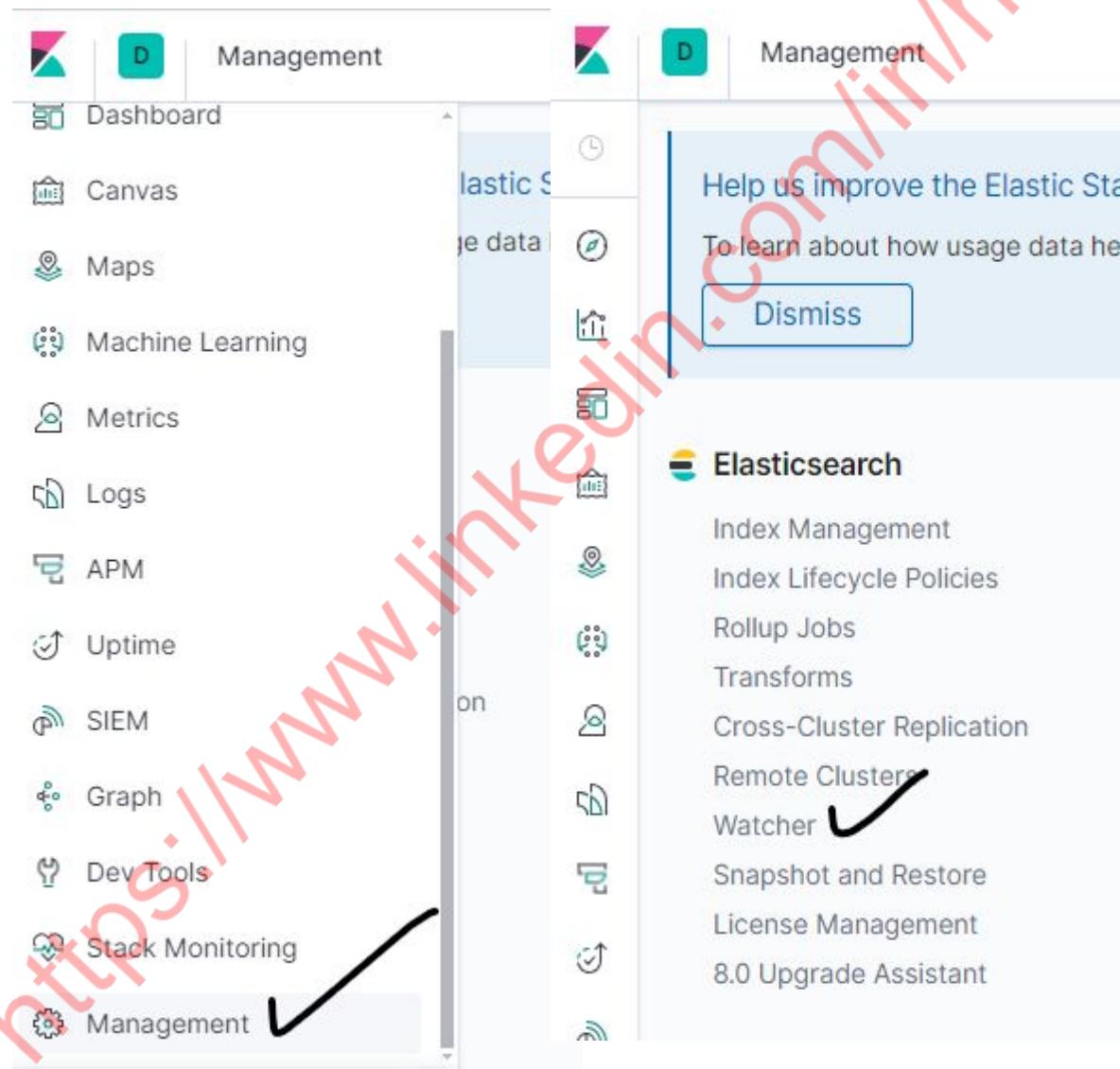
If someone is requesting to our Site it will be a an indicator for an alert. We can create an alert when someone Get Request to our site

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



You don't have any watches yet

Watch for changes or anomalies in your data and take action if needed. [Learn more.](#)

Create ▾

Select threshold Alert



Create threshold alert

Send an alert on a specified condition.

Create advanced watch

Set up a custom watch in JSON.

Create ▾

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

Time field

@timestamp

Run watch every

1

Use * to broaden your query.

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

Email



Disabled. Configure your elasticsearch.yml.

Logging



Add an item to the logs.



Slack



Send a message to a Slack user or channel.

Webhook



Send a request to a web service.

Index



Index data into Elasticsearch.

PagerDuty



Create an event in PagerDuty.

Jira



Create an issue in Atlassian's Jira Software.

Add action ▾

Show request

10:15:00

Create a text and click on create alert

Perform 1 action when condition is met

Logging

Log text

Web Traffic has exceeded the normal threshold, It is an indication of a DoS Attack

Log a sample message

✓ Create alert

Cancel

Watcher

Watcher docs

Watch for changes or anomalies in your data and take action if needed.

Q Search...

Create ▾

ID	Name	State	Last fired	Last triggered	Comment	Actions
903a8fdd-9dda-4ee6-8243-e1a9b505f4db	DOS Attack	✓	✓	✓	OK	 

Rows per page: 10 ▾

< 1 >

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)

```
1 {  
2   "trigger": {  
3     "schedule": {  
4       "interval": "5m"  
5     }  
6   },  
7   "input": {  
8     "search": {  
9       "request": {  
10         "search_type": "query_then_fetch",  
11         "indices": [  
12           "filebeat-7.4.0-2024.05.02-000001"  
13         ]  
14       }  
15     }  
16   },  
17   "condition": {  
18     "script": {  
19       "source": "return ctx.payload.hits.total.value > params.threshold",  
20       "lang": "painless",  
21       "params": {  
22         "threshold": 10  
23       }  
24     }  
25   },  
26   "actions": {  
27     "email_admin": {  
28       "email": {  
29         "profile": "standard",  
30         "to": [  
31           "admin@example.com"  
32         ],  
33         "subject": "Potential Brute Force Attack Detected",  
34         "body": {  
35           "text": "A potential brute force attack has been detected. Please investigate immediately."  
36         }  
37       }  
38     }  
39   }  
40 }
```

3.3.3 Screenshot

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

Create advanced watch

Edit Simulate

Name (optional)

ScanningAttack

ID

f5231434-6064-4708-8112-23c8429000fc

Watch JSON (API syntax)

```
1 {  
2   "trigger": {  
3     "schedule": {  
4       "interval": "5m"  
5     }  
6   },  
7   "input": {  
8     "search": {  
9       "request": {  
10      "indices": [  
11        "filebeat-7.4.0-2024.05.02-000001"  
12      ],  
13    },  
14  },  
15},  
16},  
17},  
18},  
19},  
20},  
21},  
22},  
23},  
24},  
25},  
26},  
27},  
28},  
29},  
30},  
31},  
32},  
33},  
34},  
35},  
36},  
37},  
38},  
39},  
40},  
41},  
42},  
43},  
44},  
45},  
46},  
47},  
48},  
49},  
50},  
51},  
52},  
53},  
54},  
55},  
56},  
57},  
58},  
59},  
60},  
61},  
62},  
63},  
64},  
65},  
66},  
67},  
68},  
69},  
70},  
71},  
72},  
73},  
74},  
75},  
76},  
77},  
78},  
79},  
80},  
81},  
82},  
83},  
84},  
85},  
86},  
87},  
88},  
89},  
90},  
91},  
92},  
93},  
94},  
95},  
96},  
97},  
98},  
99},  
100},  
101},  
102},  
103},  
104},  
105},  
106},  
107},  
108},  
109},  
110},  
111},  
112},  
113},  
114},  
115},  
116},  
117},  
118},  
119},  
120},  
121},  
122},  
123},  
124},  
125},  
126},  
127},  
128},  
129},  
130},  
131},  
132},  
133},  
134},  
135},  
136},  
137},  
138},  
139},  
140},  
141},  
142},  
143},  
144},  
145},  
146},  
147},  
148},  
149},  
150},  
151},  
152},  
153},  
154},  
155},  
156},  
157},  
158},  
159},  
160},  
161},  
162},  
163},  
164},  
165},  
166},  
167},  
168},  
169},  
170},  
171},  
172},  
173},  
174},  
175},  
176},  
177},  
178},  
179},  
180},  
181},  
182},  
183},  
184},  
185},  
186},  
187},  
188},  
189},  
190},  
191},  
192},  
193},  
194},  
195},  
196},  
197},  
198},  
199},  
200},  
201},  
202},  
203},  
204},  
205},  
206},  
207},  
208},  
209},  
210},  
211},  
212},  
213},  
214},  
215},  
216},  
217},  
218},  
219},  
220},  
221},  
222},  
223},  
224},  
225},  
226},  
227},  
228},  
229},  
230},  
231},  
232},  
233},  
234},  
235},  
236},  
237},  
238},  
239},  
240},  
241},  
242},  
243},  
244},  
245},  
246},  
247},  
248},  
249},  
250},  
251},  
252},  
253},  
254},  
255},  
256},  
257},  
258},  
259},  
260},  
261},  
262},  
263},  
264},  
265},  
266},  
267},  
268},  
269},  
270},  
271},  
272},  
273},  
274},  
275},  
276},  
277},  
278},  
279},  
280},  
281},  
282},  
283},  
284},  
285},  
286},  
287},  
288},  
289},  
290},  
291},  
292},  
293},  
294},  
295},  
296},  
297},  
298},  
299},  
300},  
301},  
302},  
303},  
304},  
305},  
306},  
307},  
308},  
309},  
310},  
311},  
312},  
313},  
314},  
315},  
316},  
317},  
318},  
319},  
320},  
321},  
322},  
323},  
324},  
325},  
326},  
327},  
328},  
329},  
330},  
331},  
332},  
333},  
334},  
335},  
336},  
337},  
338},  
339},  
340},  
341},  
342},  
343},  
344},  
345},  
346},  
347},  
348},  
349},  
350},  
351},  
352},  
353},  
354},  
355},  
356},  
357},  
358},  
359},  
360},  
361},  
362},  
363},  
364},  
365},  
366},  
367},  
368},  
369},  
370},  
371},  
372},  
373},  
374},  
375},  
376},  
377},  
378},  
379},  
380},  
381},  
382},  
383},  
384},  
385},  
386},  
387},  
388},  
389},  
390},  
391},  
392},  
393},  
394},  
395},  
396},  
397},  
398},  
399},  
400},  
401},  
402},  
403},  
404},  
405},  
406},  
407},  
408},  
409},  
410},  
411},  
412},  
413},  
414},  
415},  
416},  
417},  
418},  
419},  
420},  
421},  
422},  
423},  
424},  
425},  
426},  
427},  
428},  
429},  
430},  
431},  
432},  
433},  
434},  
435},  
436},  
437},  
438},  
439},  
440},  
441},  
442},  
443},  
444},  
445},  
446},  
447},  
448},  
449},  
450},  
451},  
452},  
453},  
454},  
455},  
456},  
457},  
458},  
459},  
460},  
461},  
462},  
463},  
464},  
465},  
466},  
467},  
468},  
469},  
470},  
471},  
472},  
473},  
474},  
475},  
476},  
477},  
478},  
479},  
480},  
481},  
482},  
483},  
484},  
485},  
486},  
487},  
488},  
489},  
490},  
491},  
492},  
493},  
494},  
495},  
496},  
497},  
498},  
499},  
500},  
501},  
502},  
503},  
504},  
505},  
506},  
507},  
508},  
509},  
510},  
511},  
512},  
513},  
514},  
515},  
516},  
517},  
518},  
519},  
520},  
521},  
522},  
523},  
524},  
525},  
526},  
527},  
528},  
529},  
530},  
531},  
532},  
533},  
534},  
535},  
536},  
537},  
538},  
539},  
540},  
541},  
542},  
543},  
544},  
545},  
546},  
547},  
548},  
549},  
550},  
551},  
552},  
553},  
554},  
555},  
556},  
557},  
558},  
559},  
560},  
561},  
562},  
563},  
564},  
565},  
566},  
567},  
568},  
569},  
570},  
571},  
572},  
573},  
574},  
575},  
576},  
577},  
578},  
579},  
580},  
581},  
582},  
583},  
584},  
585},  
586},  
587},  
588},  
589},  
590},  
591},  
592},  
593},  
594},  
595},  
596},  
597},  
598},  
599},  
600},  
601},  
602},  
603},  
604},  
605},  
606},  
607},  
608},  
609},  
610},  
611},  
612},  
613},  
614},  
615},  
616},  
617},  
618},  
619},  
620},  
621},  
622},  
623},  
624},  
625},  
626},  
627},  
628},  
629},  
630},  
631},  
632},  
633},  
634},  
635},  
636},  
637},  
638},  
639},  
640},  
641},  
642},  
643},  
644},  
645},  
646},  
647},  
648},  
649},  
650},  
651},  
652},  
653},  
654},  
655},  
656},  
657},  
658},  
659},  
660},  
661},  
662},  
663},  
664},  
665},  
666},  
667},  
668},  
669},  
670},  
671},  
672},  
673},  
674},  
675},  
676},  
677},  
678},  
679},  
680},  
681},  
682},  
683},  
684},  
685},  
686},  
687},  
688},  
689},  
690},  
691},  
692},  
693},  
694},  
695},  
696},  
697},  
698},  
699},  
700},  
701},  
702},  
703},  
704},  
705},  
706},  
707},  
708},  
709},  
710},  
711},  
712},  
713},  
714},  
715},  
716},  
717},  
718},  
719},  
720},  
721},  
722},  
723},  
724},  
725},  
726},  
727},  
728},  
729},  
730},  
731},  
732},  
733},  
734},  
735},  
736},  
737},  
738},  
739},  
740},  
741},  
742},  
743},  
744},  
745},  
746},  
747},  
748},  
749},  
750},  
751},  
752},  
753},  
754},  
755},  
756},  
757},  
758},  
759},  
760},  
761},  
762},  
763},  
764},  
765},  
766},  
767},  
768},  
769},  
770},  
771},  
772},  
773},  
774},  
775},  
776},  
777},  
778},  
779},  
780},  
781},  
782},  
783},  
784},  
785},  
786},  
787},  
788},  
789},  
790},  
791},  
792},  
793},  
794},  
795},  
796},  
797},  
798},  
799},  
800},  
801},  
802},  
803},  
804},  
805},  
806},  
807},  
808},  
809},  
810},  
811},  
812},  
813},  
814},  
815},  
816},  
817},  
818},  
819},  
820},  
821},  
822},  
823},  
824},  
825},  
826},  
827},  
828},  
829},  
830},  
831},  
832},  
833},  
834},  
835},  
836},  
837},  
838},  
839},  
840},  
841},  
842},  
843},  
844},  
845},  
846},  
847},  
848},  
849},  
850},  
851},  
852},  
853},  
854},  
855},  
856},  
857},  
858},  
859},  
860},  
861},  
862},  
863},  
864},  
865},  
866},  
867},  
868},  
869},  
870},  
871},  
872},  
873},  
874},  
875},  
876},  
877},  
878},  
879},  
880},  
881},  
882},  
883},  
884},  
885},  
886},  
887},  
888},  
889},  
890},  
891},  
892},  
893},  
894},  
895},  
896},  
897},  
898},  
899},  
900},  
901},  
902},  
903},  
904},  
905},  
906},  
907},  
908},  
909},  
910},  
911},  
912},  
913},  
914},  
915},  
916},  
917},  
918},  
919},  
920},  
921},  
922},  
923},  
924},  
925},  
926},  
927},  
928},  
929},  
930},  
931},  
932},  
933},  
934},  
935},  
936},  
937},  
938},  
939},  
940},  
941},  
942},  
943},  
944},  
945},  
946},  
947},  
948},  
949},  
950},  
951},  
952},  
953},  
954},  
955},  
956},  
957},  
958},  
959},  
960},  
961},  
962},  
963},  
964},  
965},  
966},  
967},  
968},  
969},  
970},  
971},  
972},  
973},  
974},  
975},  
976},  
977},  
978},  
979},  
980},  
981},  
982},  
983},  
984},  
985},  
986},  
987},  
988},  
989},  
990},  
991},  
992},  
993},  
994},  
995},  
996},  
997},  
998},  
999},  
1000},  
1001},  
1002},  
1003},  
1004},  
1005},  
1006},  
1007},  
1008},  
1009},  
1010},  
1011},  
1012},  
1013},  
1014},  
1015},  
1016},  
1017},  
1018},  
1019},  
1020},  
1021},  
1022},  
1023},  
1024},  
1025},  
1026},  
1027},  
1028},  
1029},  
1030},  
1031},  
1032},  
1033},  
1034},  
1035},  
1036},  
1037},  
1038},  
1039},  
1040},  
1041},  
1042},  
1043},  
1044},  
1045},  
1046},  
1047},  
1048},  
1049},  
1050},  
1051},  
1052},  
1053},  
1054},  
1055},  
1056},  
1057},  
1058},  
1059},  
1060},  
1061},  
1062},  
1063},  
1064},  
1065},  
1066},  
1067},  
1068},  
1069},  
1070},  
1071},  
1072},  
1073},  
1074},  
1075},  
1076},  
1077},  
1078},  
1079},  
1080},  
1081},  
1082},  
1083},  
1084},  
1085},  
1086},  
1087},  
1088},  
1089},  
1090},  
1091},  
1092},  
1093},  
1094},  
1095},  
1096},  
1097},  
1098},  
1099},  
1100},  
1101},  
1102},  
1103},  
1104},  
1105},  
1106},  
1107},  
1108},  
1109},  
1110},  
1111},  
1112},  
1113},  
1114},  
1115},  
1116},  
1117},  
1118},  
1119},  
1120},  
1121},  
1122},  
1123},  
1124},  
1125},  
1126},  
1127},  
1128},  
1129},  
1130},  
1131},  
1132},  
1133},  
1134},  
1135},  
1136},  
1137},  
1138},  
1139},  
1140},  
1141},  
1142},  
1143},  
1144},  
1145},  
1146},  
1147},  
1148},  
1149},  
1150},  
1151},  
1152},  
1153},  
1154},  
1155},  
1156},  
1157},  
1158},  
1159},  
1160},  
1161},  
1162},  
1163},  
1164},  
1165},  
1166},  
1167},  
1168},  
1169},  
1170},  
1171},  
1172},  
1173},  
1174},  
1175},  
1176},  
1177},  
1178},  
1179},  
1180},  
1181},  
1182},  
1183},  
1184},  
1185},  
1186},  
1187},  
1188},  
1189},  
1190},  
1191},  
1192},  
1193},  
1194},  
1195},  
1196},  
1197},  
1198},  
1199},  
1200},  
1201},  
1202},  
1203},  
1204},  
1205},  
1206},  
1207},  
1208},  
1209},  
1210},  
1211},  
1212},  
1213},  
1214},  
1215},  
1216},  
1217},  
1218},  
1219},  
1220},  
1221},  
1222},  
1223},  
1224},  
1225},  
1226},  
1227},  
1228},  
1229},  
1230},  
1231},  
1232},  
1233},  
1234},  
1235},  
1236},  
1237},  
1238},  
1239},  
1240},  
1241},  
1242},  
1243},  
1244},  
1245},  
1246},  
1247},  
1248},  
1249},  
1250},  
1251},  
1252},  
1253},  
1254},  
1255},  
1256},  
1257},  
1258},  
1259},  
1260},  
1261},  
1262},  
1263},  
1264},  
1265},  
1266},  
1267},  
1268},  
1269},  
1270},  
1271},  
1272},  
1273},  
1274},  
1275},  
1276},  
1277},  
1278},  
1279},  
1280},  
1281},  
1282},  
1283},  
1284},  
1285},  
1286},  
1287},  
1288},  
1289},  
1290},  
1291},  
1292},  
1293},  
1294},  
1295},  
1296},  
1297},  
1298},  
1299},  
1300},  
1301},  
1302},  
1303},  
1304},  
1305},  
1306},  
1307},  
1308},  
1309},  
1310},  
1311},  
1312},  
1313},  
1314},  
1315},  
1316},  
1317},  
1318},  
1319},  
1320},  
1321},  
1322},  
1323},  
1324},  
1325},  
1326},  
1327},  
1328},  
1329},  
1330},  
1331},  
1332},  
1333},  
1334},  
1335},  
1336},  
1337},  
1338},  
1339},  
1340},  
1341},  
1342},  
1343},  
1344},  
1345},  
1346},  
1347},  
1348},  
1349},  
1350},  
1351},  
1352},  
1353},  
1354},  
1355},  
1356},  
1357},  
1358},  
1359},  
1360},  
1361},  
1362},  
1363},  
1364},  
1365},  
1366},  
1367},  
1368},  
1369},  
1370},  
1371},  
1372},  
1373},  
1374},  
1375},  
1376},  
1377},  
1378},  
1379},  
1380},  
1381},  
1382},  
1383},  
1384},  
1385},  
1386},  
1387},  
1388},  
1389},  
1390},  
1391},  
1392},  
1393},  
1394},  
1395},  
1396},  
1397},  
1398},  
1399},  
1400},  
1401},  
1402},  
1403},  
1404},  
1405},  
1406},  
1407},  
1408},  
1409},  
1410},  
1411},  
1412},  
1413},  
1414},  
1415},  
1416},  
1417},  
1418},  
1419},  
1420},  
1421},  
1422},  
1423},  
1424},  
1425},  
1426},  
1427},  
1428},  
1429},  
1430},  
1431},  
1432},  
1433},  
1434},  
1435},  
1436},  
1437},  
1438},  
1439},  
1440},  
1441},  
1442},  
1443},  
1444},  
1445},  
1446},  
1447},  
1448},  
1449},  
1450},  
1451},  
1452},  
1453},  
1454},  
1455},  
1456},  
1457},  
1458},  
1459},  
1460},  
1461},  
1462},  
1463},  
1464},  
1465},  
1466},  
1467},  
1468},  
1469},  
1470},  
1471},  
1472},  
1473},  
1474},  
1475},  
1476},  
1477},  
1478},  
1479},  
1480},  
1481},  
1482},  
1483},  
1484},  
1485},  
1486},  
1487},  
1488},  
1489},  
1490},  
1491},  
1492},  
1493},  
1494},  
1495},  
1496},  
1497},  
1498},  
1499},  
1500},  
1501},  
1502},  
1503},  
1504},  
1505},<br
```

Name (optional)

ScanningAttack

ID

f5231434-6064-4708-8112-23c8429000fc

Watch JSON (API syntax)

```
1 {  
2   "trigger": {  
3     "schedule": {  
4       "interval": "5m"  
5     }  
6   },  
7   "input": {  
8     "search": {  
9       "request": {  
10         "indices": [  
11           "filebeat-7.4.0-2024.05.02-000001"  
12         ],  
13         "filebeat-7.4.0-2024.05.02-000001"  
14       ],  
15       "body": {  
16         "query": {  
17           "bool": {  
18             "must": [  
19               { "match": { "event.type": "port_scan" } },  
20               { "range": { "@timestamp": { "gte": "now-5m" } } }  
21             ]  
22           }  
23         }  
24       }  
25     },  
26     "condition": {  
27       "script": {  
28         "source": "return ctx.payload.hits.total.value > params.threshold",  
29         "params": {  
30           "threshold": 50 // Adjust the threshold based on your environment and expected legitimate traffic  
31         }  
32       }  
33     },  
34     "actions": {  
35       "email_admin": {  
36         "email": {  
37           "to": "admin@example.com",  
38           "subject": "Potential Scanning Attack Detected",  
39           "body": {  
40             "text": "A potential scanning attack has been detected. Please investigate immediately."  
41           }  
42         }  
43       }  
44     }  
45   }  
46 }
```

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.

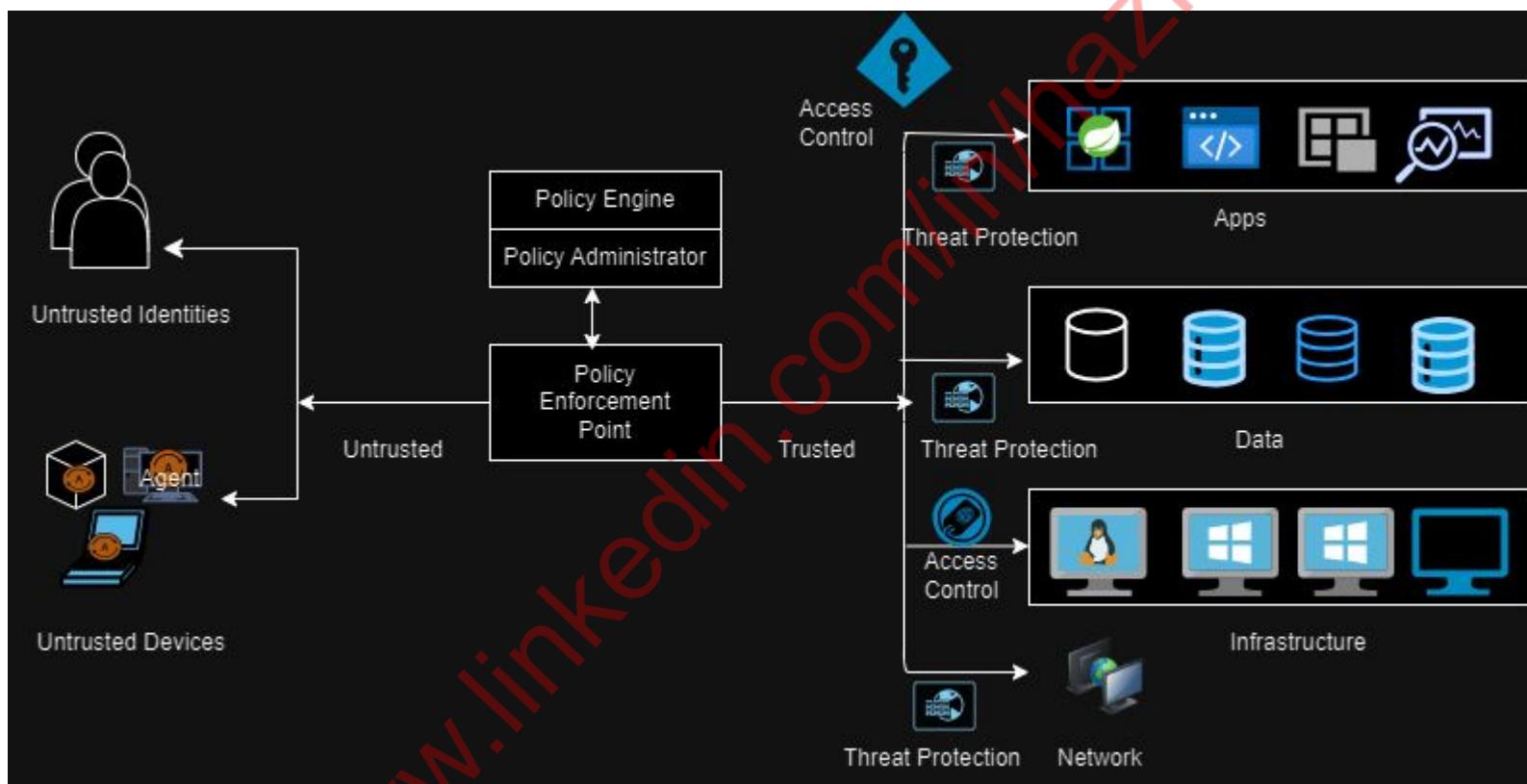
Design a Zero Trust model of your network architecture using <https://app.diagrams.net/>.

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/>