

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).

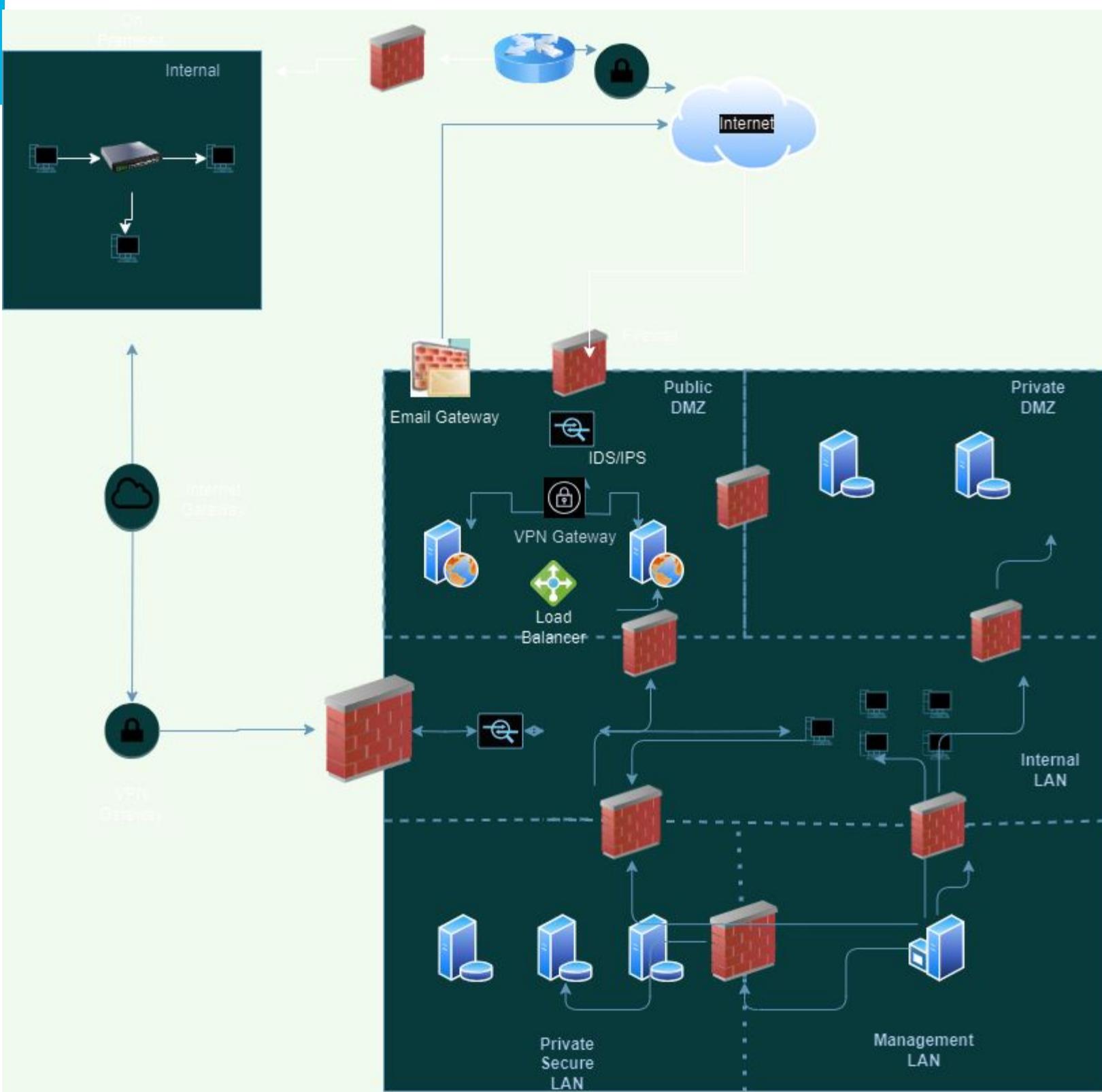
3) Show the flow of traffic, and remember to incorporate best security practices with the flow of traffic between the different subnets.

Designing the Network

Diagram Link:

<https://drive.google.com/file/d/1k9uTyJYEp7Kkr1NZdSMGWBlIf2az51W/view?usp=sharing>

1.1 Designing the Network



Digram URL:

https://drive.google.com/file/d/1k9uTyJYFp7Kkr1NZdSMGW_BIf2az51W/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 top navigation bar includes the Microsoft Azure logo, a search bar, and a 'Home > Virtual networks >' breadcrumb trail. The main title is 'Create virtual network' with a '...' button. Below the title, the 'Basics' tab is selected, followed by 'Security', 'IP addresses', 'Tags', and 'Review + create'. The 'Subscription' dropdown is set to 'Udacity CloudLabs Sub - 40'. The 'Resource group' dropdown is set to 'entp-project-258065' 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 'Deploy to an Azure Extended Zone' link is also present. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons.

DMZ Virtual Network Created

Home >

 DMZ   ...
Virtual network

 Move  Delete  Refresh  Give feedback

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

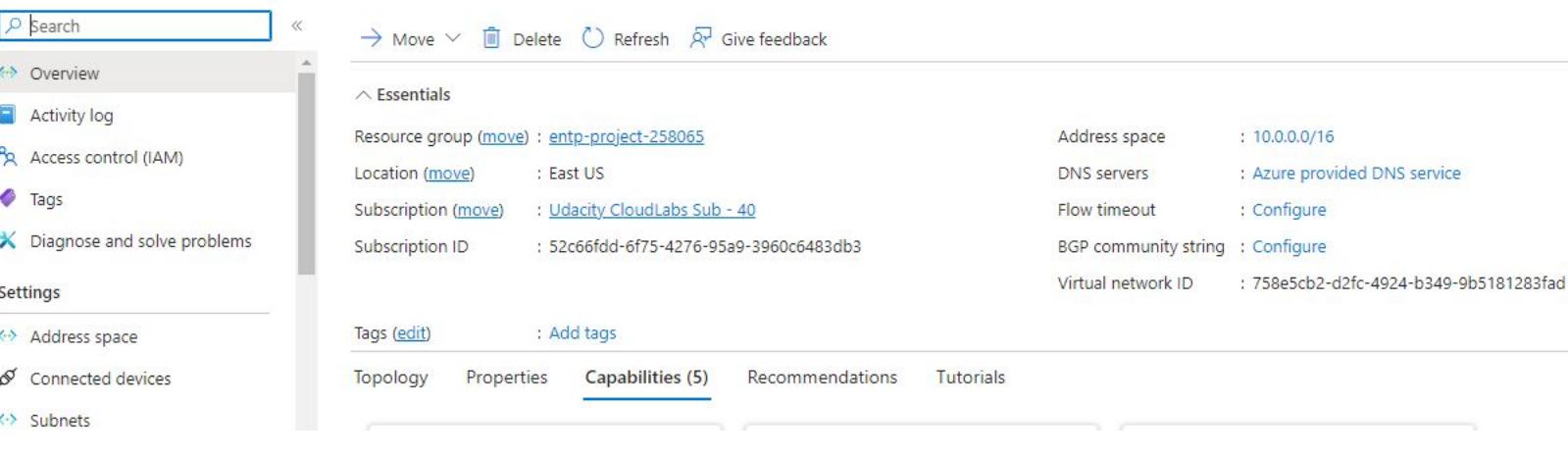
Settings

 Address space
 Connected devices
 Subnets

 Essentials

Resource group (move) : entp-project-258065	Address space : 10.0.0.0/16
Location (move) : East US	DNS servers : Azure provided DNS service
Subscription (move) : Udacity CloudLabs Sub - 40	Flow timeout : Configure
Subscription ID : 52c66fdd-6f75-4276-95a9-3960c6483db3	BGP community string : Configure
Tags (edit) : Add tags	Virtual network ID : 758e5cb2-d2fc-4924-b349-9b5181283fad

[Topology](#) [Properties](#) **Capabilities (5)** [Recommendations](#) [Tutorials](#)



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 *

[Default](#) [Avere Extended](#) [7](#) [...](#)

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"/>	<input type="text" value="/16"/>
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](#)

Internal

Virtual network

Search

Move Delete Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Essentials

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

Address space : 10.0.0.0/16

Location ([move](#)) : East US

DNS servers : Azure provided DNS service

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

Flow timeout : Configure

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

BGP community string : Configure

Virtual network ID : 3f79a235-f6b6-417f-8e92-e01671d7ec6b

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

Topology

Properties

Capabilities (5)

Recommendations

Tutorials

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 includes options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Deployments, Security, and Deployment slots. The main area displays the "Essentials" blade with the "Resources" tab selected. It lists two resources: "DMZ" and "Internal", both categorized as "Virtual network" and located in "East US". A search bar at the top is empty, and there are filter options for Type (set to "all") and Location (set to "all"). A large checkmark is drawn over both the "DMZ" and "Internal" entries.

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

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 managing subnets in a virtual network. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The 'Subnets' option is selected. The main area shows a list of existing subnets: 'default' with IPv4 range 10.0.0.0/24 and available IPs 251. A new subnet is being created with the name 'Public'. The 'Name' field is filled with 'Public'. The 'Subnet address range' is set to 10.0.1.0/24, which is highlighted with a green checkmark. Other fields include 'Add IPv6 address space' (unchecked), 'NAT gateway' (set to 'None'), 'Network security group' (set to 'None'), and 'Route table' (set to 'None'). At the bottom right of the dialog are 'Save' and 'Cancel' buttons, and a 'Give feedback' link.

The screenshot shows the Azure portal interface for managing subnets in a virtual network. The 'Subnets' option is selected in the sidebar. The main area displays a list of subnets. There are two entries: 'default' with IPv4 range 10.0.0.0/24 and available IPs 251, and 'Public' with IPv4 range 10.0.1.0/24 and available IPs 251. Both entries have green checkmarks next to them. The columns in the table are Name, IPv4, IPv6, and Available IPs. At the bottom right of the table are 'Save' and 'Cancel' buttons, and a 'Give feedback' link.

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

Address space Connected devices

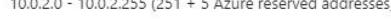
Subnets 

Search subnets

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

Add subnet

Name * 

Subnet address range * 10.0.2.0/24 

Add IPv6 address space 

NAT gateway 
None

Network security group 
None

Route table 
None

Service endpoints 

Save Cancel Give feedback

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

+ Subnet + Gateway subnet Refresh Manage users Delete

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

Subnet table data:

Name	IPv4 Range	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 visible with 'Subnets' selected. The main area displays the 'Internal | Subnets' page for a virtual network, showing one existing subnet named 'default' with the IPv4 range 10.0.0.0/24. A modal window titled 'Add subnet' is open on the right, prompting for a name ('Management') and an IPv4 address range ('10.0.1.0/24'). A checkmark is present above the 'Name' field in the modal. At the bottom right of the modal are 'Save' and 'Cancel' buttons.

The screenshot shows the 'Internal | Subnets' page after the 'Management' subnet has been added. The table now lists two subnets: 'default' (IPv4 10.0.0.0/24) and 'Management' (IPv4 10.0.1.0/24). A checkmark is present above the 'Management' row in the table. The left navigation menu shows 'Subnets' selected again.

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

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

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

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

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
Secure	10.0.2.0/24	-	251

Add subnet

Name * ✓ Enterprise

Subnet address range * 10.0.3.0/24 10.0.3.0 - 10.0.3.255 (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
Enterprise	10.0.3.0/24 ✓	-	251

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

Settings

Address space Connected devices Subnets

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
Enterprise	10.0.3.0/24	✓	251



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](#)

[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 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](#)

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

[Overview](#)

^ Essentials

[Activity log](#)

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

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

Location : East US

[Tags](#)

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

[Diagnose and solve problems](#)

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

[Settings](#)

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

🔗 ⭐ ...

Search



Move ↗ Delete Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

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

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, there's a list of existing subnets: 'default' (IPv4: 10.0.0.0/24), 'Private' (selected, IPv4: 10.0.2.0/24 with a checkmark), and 'Public' (IPv4: 10.0.1.0/24). On the right, a detailed configuration pane is open for the 'Private' subnet. It shows the subnet name is 'Private' and the address range is '10.0.2.0/24'. Under 'Network security group', the value 'Private_NSG' is selected with a checkmark. At the bottom of the pane are 'Save' and 'Cancel' buttons, and a 'Give feedback' link.

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

DMZ

Subnet Gateway subnet Refresh Manage users Delete

Search 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

Public

DMZ

Name: Public

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

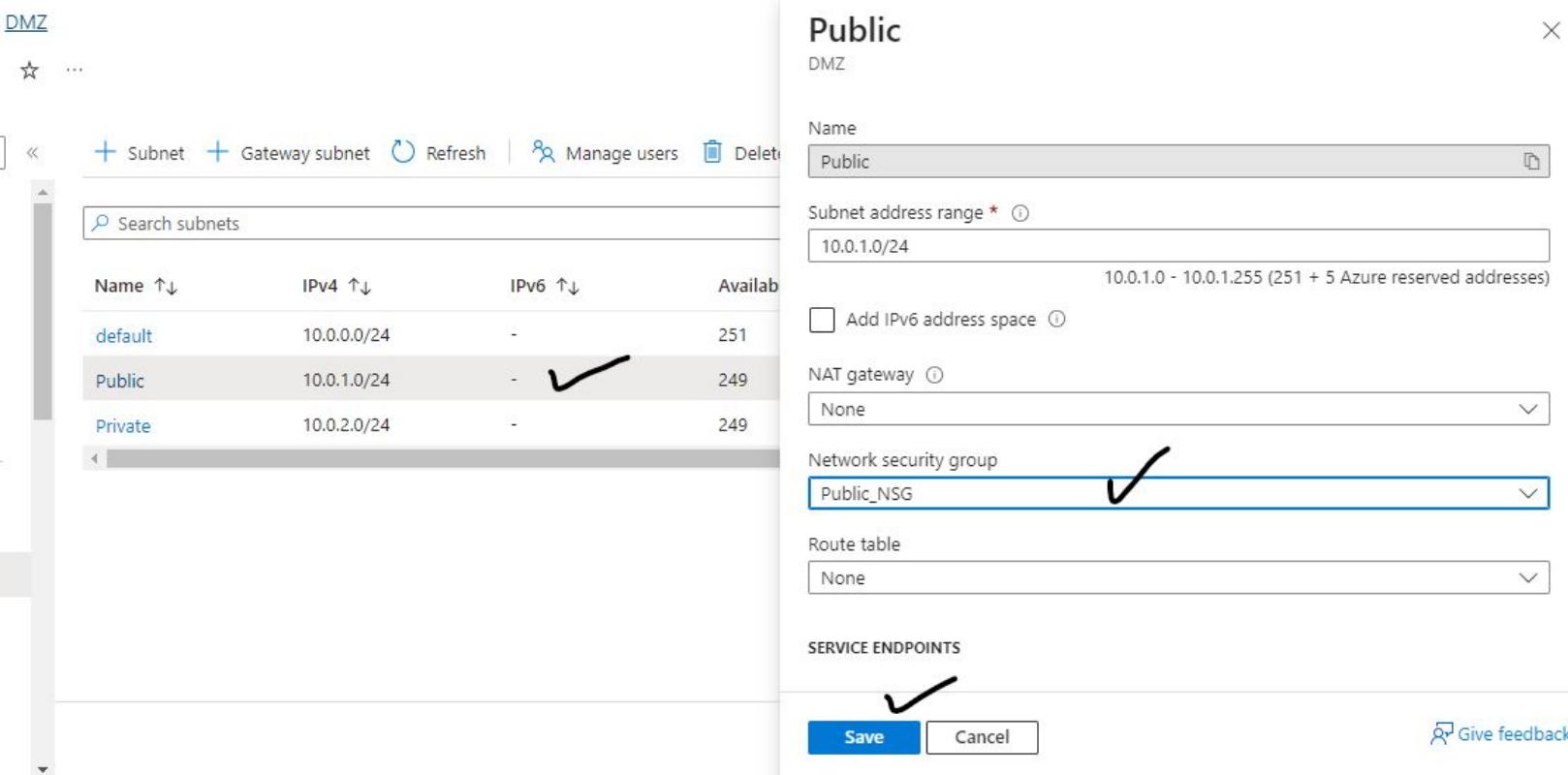
Add IPv6 address space:

NAT gateway: None

Network security group: Public_NSG ✓

Route table: None

Save Cancel Give feedback



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

Add IPv6 address space:

NAT gateway: None

Network security group: Management_NSG

Route table: None

SERVICE ENDPOINTS

Save Cancel

Give feedback

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

Screenshot of the Azure portal showing the creation of a new subnet named "Enterprise". The subnet has been assigned to the "Enterprise" Network Security Group (NSG). Handwritten checkmarks are present on the subnet table and the NSG dropdown.

Enterprise
Internal

Name: Enterprise ✓

Subnet address range * ⓘ
10.0.3.0/24
10.0.3.0 - 10.0.3.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ
None

Network security group
Enterprise_NSG ✓

Route table
None

SERVICE ENDPOINTS

✓

Save Cancel Give feedback

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

Screenshot of the Azure portal showing the subnet table. The "Enterprise" subnet is selected and associated with the "Enterprise_NSG" NSG. Handwritten checkmarks are present on the subnet table and the NSG dropdown.

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

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 IPs
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 detailed configuration pane for the 'Secure' subnet is open. It includes fields for Name (Secure), Subnet address range (10.0.2.0/24), NAT gateway (None), Network security group (Secure_NSG), and Route table (None). A large checkmark is placed over the 'Secure_NSG' selection. At the bottom are 'Save' and 'Cancel' buttons.

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	✓

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 AAAAB3NzaC1yc2EAAAQABAAQDzIaM0aOFJrX2ArVo1WYeWd6gCferDf7iinEPeNgvJSJvQuZzbNEE78EHV6xfL4UbzTV2GAyBApVQ+qW9
CVNHxD9m0y5KrDHGVgMlwJuT4g6Y4Vg72RqdFPnPYtyXTfKEsaCJQkPsuhj8JdgxKcrQBzTzY02EuDpVkb5/Ue9ArF2IdALH8simFpJxd6GZU1SOVFcC+EL
1tsIzi9tzhNA3ilAux0l8c++WhqE0PHiVOSzsGRGI4uEye5FcI0z5FcDXHczRv6cQcVEnJ7u1z/Rl/rKtf/Ad6sMmS6LSURCkiAl4iQtz2AQVmjYUpFedW8
4PrhJuFbkhw1k6/PXkui51Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44hp3Xd10cHrAYR6NAi6EHY0Gsd1xTqnhG5wFU
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 >

 **vmPublicDMZ** ⚡ ⭐ ...

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

Instance details

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

Overview

Essentials	
Resource group (move)	: entp-project-258065
Status	: Running
Location	: East US (Zone 1)
Subscription (move)	: Udacity CloudLabs Sub - 40
Subscription ID	: 52c66fdd-6f75-4276-95a9-3960c6483db3
Availability zone	: 1
Tags (edit)	: Add tags

[Properties](#) [Monitoring](#) [Capabilities \(7\)](#) [Recommendations](#) [Tutorials](#)

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 ↑↓	P
<input type="checkbox"/>	vmPrivateDMZ ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s	2
<input type="checkbox"/>	vmPublicDMZ ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s	2

No grouping List view

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

The screenshot shows the 'Create a virtual machine' wizard in the Azure portal. The 'Subscription' dropdown is set to 'Udacity CloudLabs Sub - 40' and has a checkmark. The 'Resource group' dropdown is set to 'entp-project-258065' and has a checkmark. The 'Virtual machine name' field is filled with 'vmManagementInternal' and has a checkmark. The 'Region' dropdown is set to '(US) East US' and has a checkmark. The 'Availability zone' dropdown is set to 'Zone 1'. A note at the bottom says 'You can now select multiple zones. Selecting multiple zones will create one VM per zone.' with a link to learn more. At the bottom, there are buttons for '< Previous', 'Next : Disks >', and a blue 'Review + create' button.

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 🔍 Feed

 Overview

 Activity log

 Access control (IAM)

 Tags

 Diagnose and solve problems

 Connect

 Connect

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 : -

Type ([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](#) ⌂ ⚡ 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

 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

Resource group : entp-project-258065
Status : Running
Location : East US (Zone 1)
Subscription : Udacity CloudLabs Sub - 40
Subscription ID : 52c66fdd-6f75-4276-95a9-3960c6483db3
Availability zone : 1
Tags : Add tags

Operating system : Linux (ubuntu 20.04)
Size : Standard B1s (1 vcpu, 1 GiB memory)
Public IP address : 51.8.90.86
Virtual network/subnet : Internal/Secure
DNS name : Not configured
Health state : -

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.

Name ↑↓	Type ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓	Status ↑↓	Operating system ↑↓	Size ↑↓
vmEnterpriseInternal ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s
vmManagementInternal ✓	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s
vmPrivateDMZ	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s
vmPublicDMZ	Virtual machine	Udacity CloudLabs Su...	entp-project-258065	East US	Running	Linux	Standard_B1s
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. On the left, the 'Public_NSG' network security group is selected. The 'Inbound security rules' section is open, showing a list of existing rules and a 'Add' button. A modal window titled 'Add inbound security rule' is displayed, allowing configuration of a new rule. The configuration includes: Source set to 'Any' (checked), Source port ranges set to '*', Destination set to 'Any' (checked), Service set to 'HTTP' (checked), and Destination port ranges set to '80' (checked). The 'Protocol' section shows 'TCP' selected. At the bottom of the modal are 'Add' and 'Cancel' buttons. The main pane shows the current list of rules:

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
<input type="checkbox"/> 100	AllowAnyHTTPInbound	80	TCP	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

Allowing inbound HTTPS Traffic for public DMZ

The screenshot shows the Azure portal interface for managing Network Security Groups. On the left, the 'Inbound security rules' section is selected under 'Public_NSG' settings. A new rule is being created, as indicated by the 'Add' button in the top right of the main pane. The 'Protocol' tab is selected in the 'Add inbound security rule' dialog. Handwritten checkmarks are present on the 'Source' field ('Any'), 'Source port ranges' ('*'), 'Destination' ('Any'), 'Service' ('HTTPS'), and 'Destination port ranges' ('443').

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
<input type="checkbox"/> 100	AllowAnyHTTPInbound	80	TCP	Any
<input type="checkbox"/> 110	AllowAnyHTTPSInbou...	443	TCP	Any
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any	VirtualNetwork
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalanc...
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any	Any

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

<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"/> 65500	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

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

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

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

Private NSG Rules

Private_NSG | Inbound security rules ... X

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	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

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

<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 star ... ✓

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 ✓	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

<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

The screenshot shows the Azure portal interface for a virtual machine named "vmEnterpriseInternal". The machine is listed as a "Virtual machine". The "Overview" tab is selected in the left sidebar. The main pane displays the following details:

Essential Information	Value
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	

At the bottom, a terminal window shows the user "azureuser" is connected to the VM via SSH, with the command "az user@vmEnterpriseInternal:~\$ |".

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. At the top, there is a navigation bar with icons for back, forward, refresh, and search. Below the navigation bar, the URL is shown as portal.azure.com/#view/HubsExtension/BrowseResou... . The main header says "Microsoft Azure" and has a search bar that reads "Search resources, services, and docs (G+/-)". A checkmark icon is present next to the search bar. The main content area is titled "Virtual network gateways". There is a "Udacity" watermark or filter applied to the page. Below the title, there are several buttons: "Create" (marked with a checkmark), "Manage view", "Refresh", "Export to CSV", "Open query", and "Assign tags". There are also filters for "Subscription equals all", "Resource group equals all", and "Location equals all", each with a close button. At the bottom, it says "Showing 0 to 0 of 0 records." and there are sorting options for "Name" and "Virtual ...".

Create virtual network gateway

Subscription * Udacity CloudLabs Sub - 40 ▼

Resource group ① 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 * ① ✓ VPN ExpressRoute

SKU * ① VpnGw1 ✓ ✓

Generation ① Generation1 ✓ ✓

Virtual network * ① Internal ✓ ✓

[Create virtual network](#)

Virtual network * ⓘ  
[Create virtual network](#)

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

Gateway subnet address range * ⓘ  
10.0.4.0 - 10.0.4.255 (256 addresses)

Public IP address

Public IP address * ⓘ Create new Use existing

Public IP address name *

Public IP address SKU Standard

Assignment Dynamic Static

Enable active-active mode * ⓘ Enabled Disabled

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

Public IP address   Create new  Use existing

Public IP address name * ✓ 

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 * ✓ 

Configure BGP *  Enabled Disabled

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

[Review + create](#)

[Previous](#)

[Next : Tags >](#)

[Download a template for automation](#)

Waiting for its deployment

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
EnterpriseVPN1ip	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

Enterprise_VPN ✓

Virtual network gateway

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

Refresh Move Delete

Resource group ([move](#)) : [entp-project-258065](#) SKU : VpnGw1

Location : East US Gateway type : VPN

Subscription ([move](#)) : [Udacity CloudLabs Sub - 40](#) VPN type : Route-based

Subscription ID : 52c66fdd-6f75-4276-95a9-3960c6483db3 Virtual network : [Internal/GatewaySubnet](#)

First public IP address : [13.92.126.117 \(EnterpriseVPNip\)](#) ✓

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

 **Health check**
Perform a quick health check to detect possible gateway issues
[Go to Resource health](#)

 **Documentation**
View guidance on helpful topics related to VPN gateway
[View documentation](#)

Point to Site Configuration

Home > Microsoft.VirtualNetworkGateway-20240421180556 | Overview > Ent

Enterprise_VPN | Point-to-site configuration

Virtual network gateway

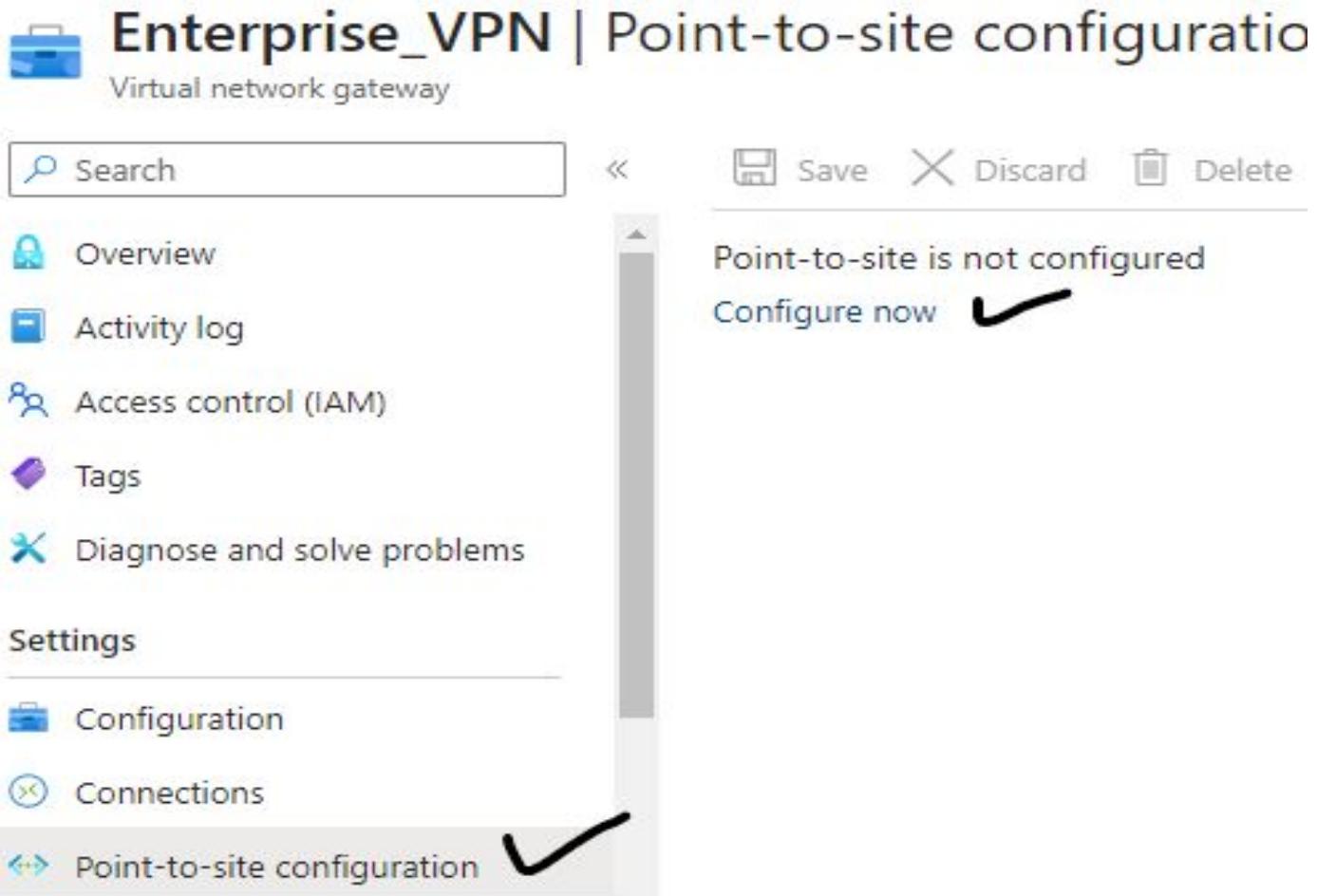
Search Save Discard Delete

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

Save Discard Delete Download VPN client

 Overview

 Activity log

 Access control (IAM)

 Tags

 Diagnose and solve problems

Settings

 Configuration

 Connections

 Point-to-site configuration

 Properties

 Locks

Monitoring

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 available port.

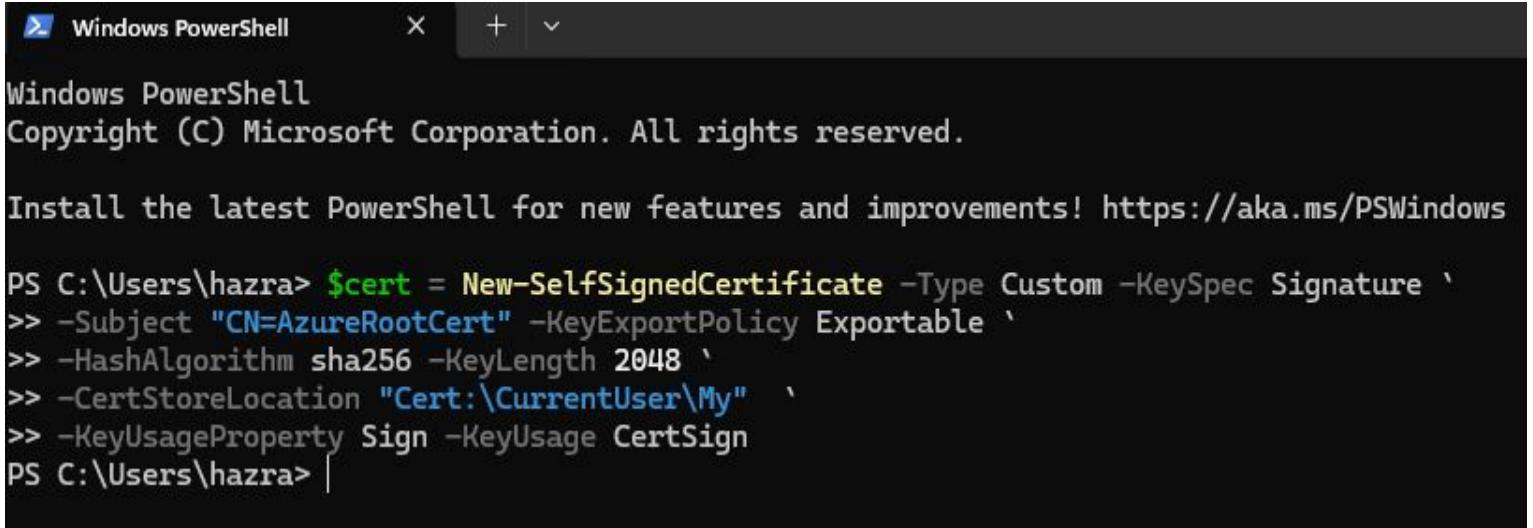
Public IP address *

 ⓘ

Create new Use existing

Enterprise_VPN_Ip3

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 like SHA256 hash algorithm and 2048 key length.

```
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
```

```
#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

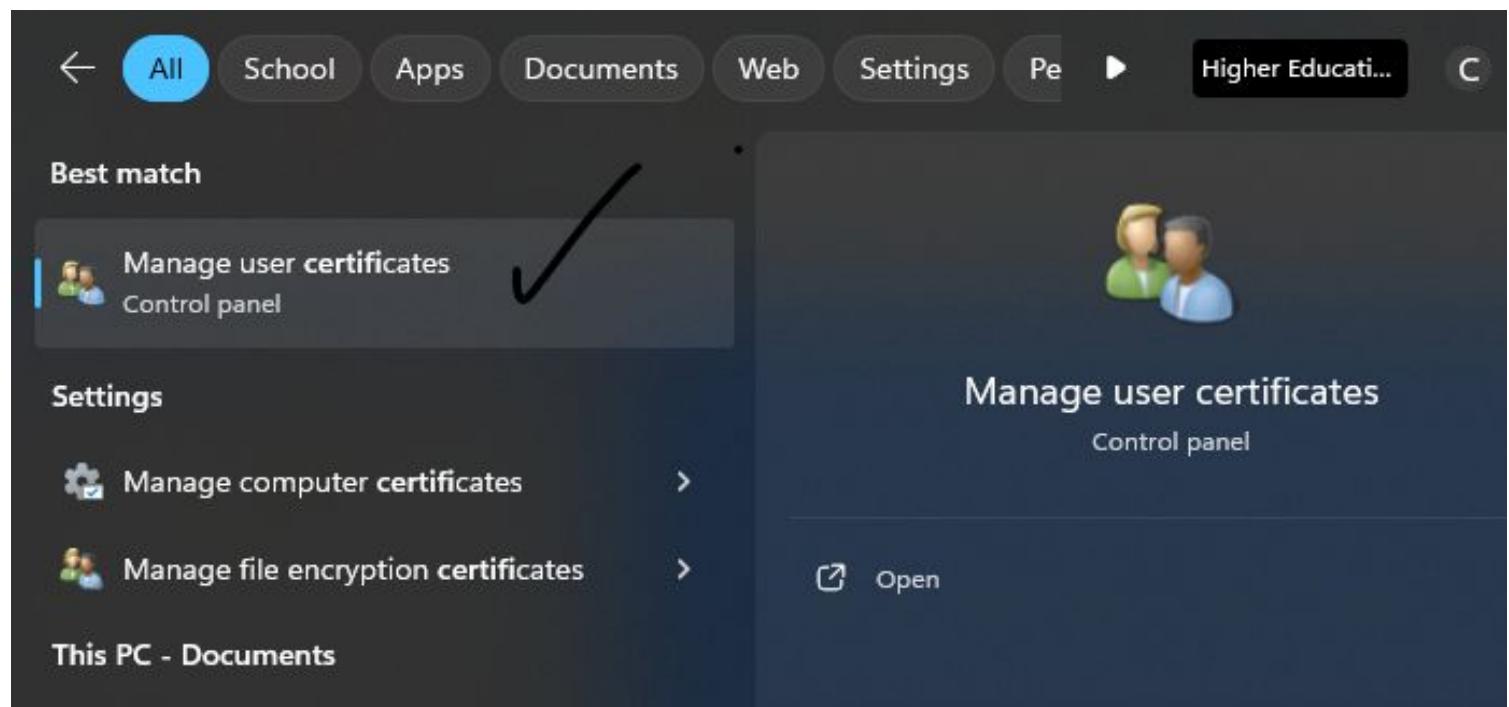
```
PS C:\Users\hazra> # Create Client Cert
PS C:\Users\hazra> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature ` 
>> -Subject "CN=AzureClientCert" -KeyExportPolicy Exportable ` 
>> -HashAlgorithm sha256 -KeyLength 2048 ` 
>> -CertStoreLocation "Cert:\CurrentUser\My" `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

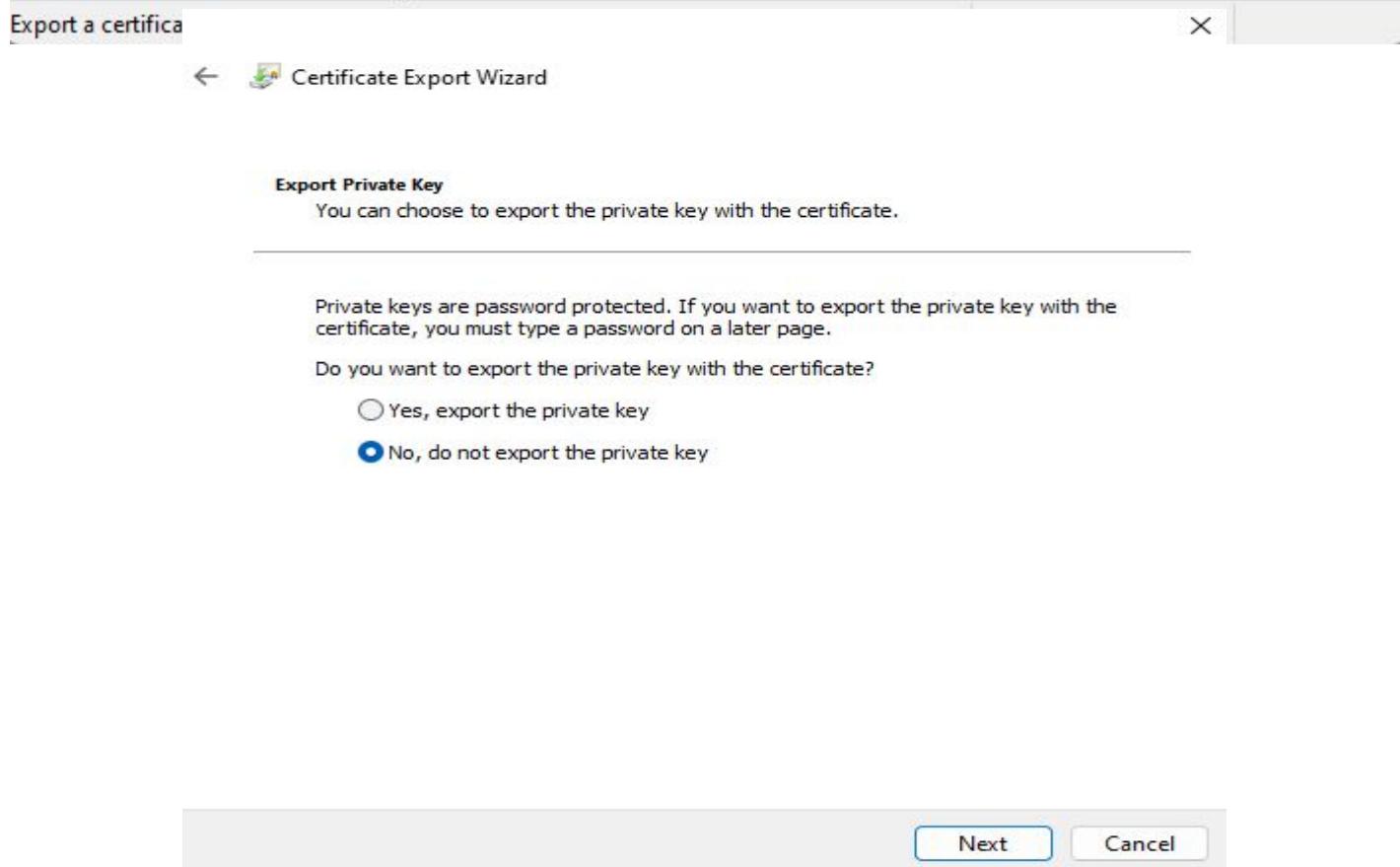
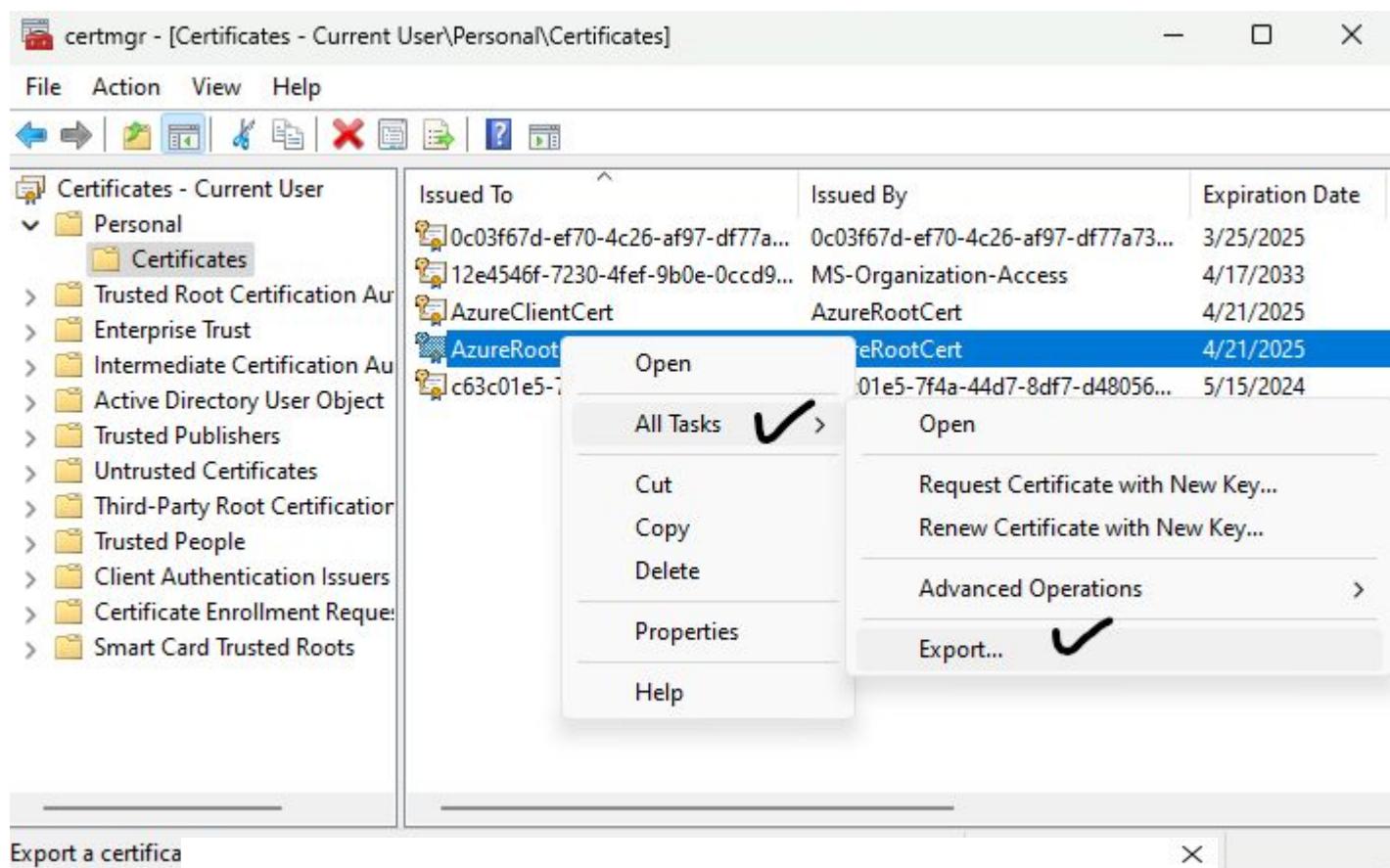
Accessing The created certificates



A screenshot of the Certmgr application window. The title bar reads "certmgr - [Certificates - Current User\Personal\Certificates]". The menu bar includes File, Action, View, and Help. Below the menu is a toolbar with various icons. On the left is a navigation pane with a tree view of certificate stores: "Certificates - Current User" (selected), "Personal" (selected), "Certificates" (selected), "Trusted Root Certification Au", "Enterprise Trust", "Intermediate Certification Au", "Active Directory User Object", and "Trusted Publishers". The main pane displays a table of certificates:

Issued To	Issued By	Expiration Date
0c03f67d-ef70-4c26-af97-df77a73...	0c03f67d-ef70-4c26-af97-df77a73...	3/25/2025
12e4546f-7230-4fef-9b0e-0cccd9...	MS-Organization-Access	4/17/2033
AzureClientCert	AzureRootCert	4/21/2025
AzureRootCert	AzureRootCert	4/21/2025
c63c01e5-7f4a-44d7-8df7-d480...	c63c01e5-7f4a-44d7-8df7-d48056...	5/15/2024

Exporting the root cert



X



Export File Format

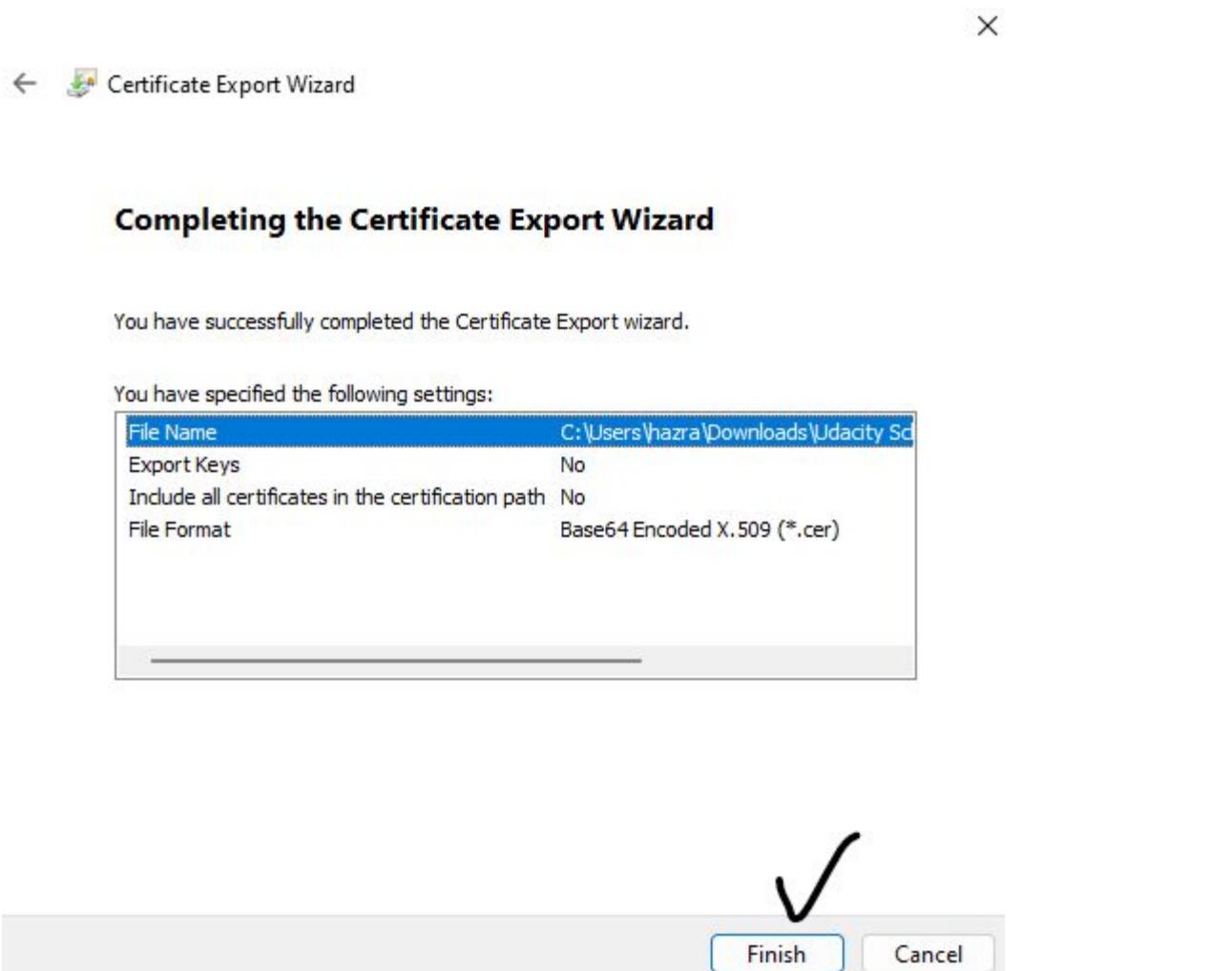
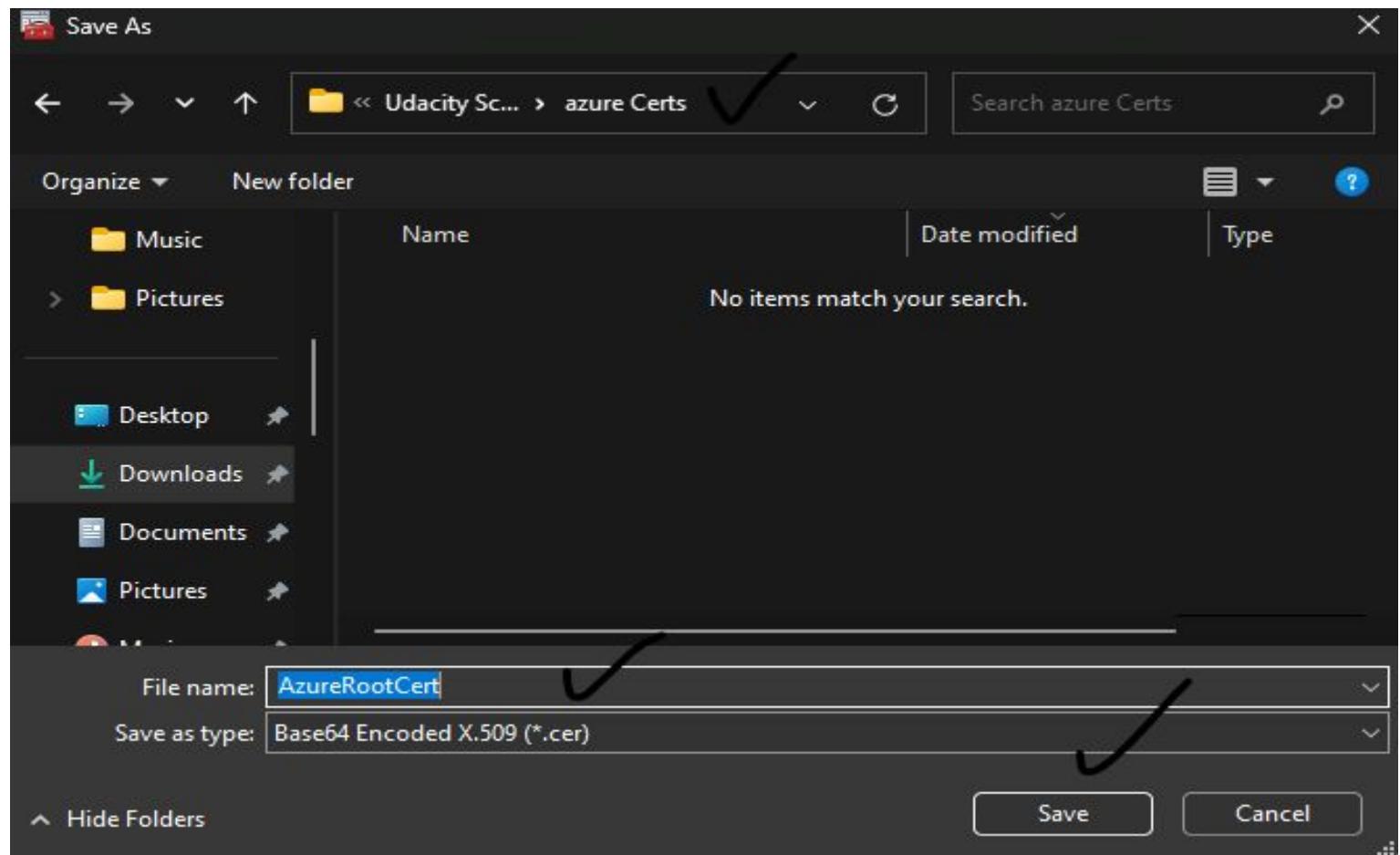
Certificates can be exported in a variety of file formats.

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



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
Export Keys
Include all certificates in the certificate chain
File Format



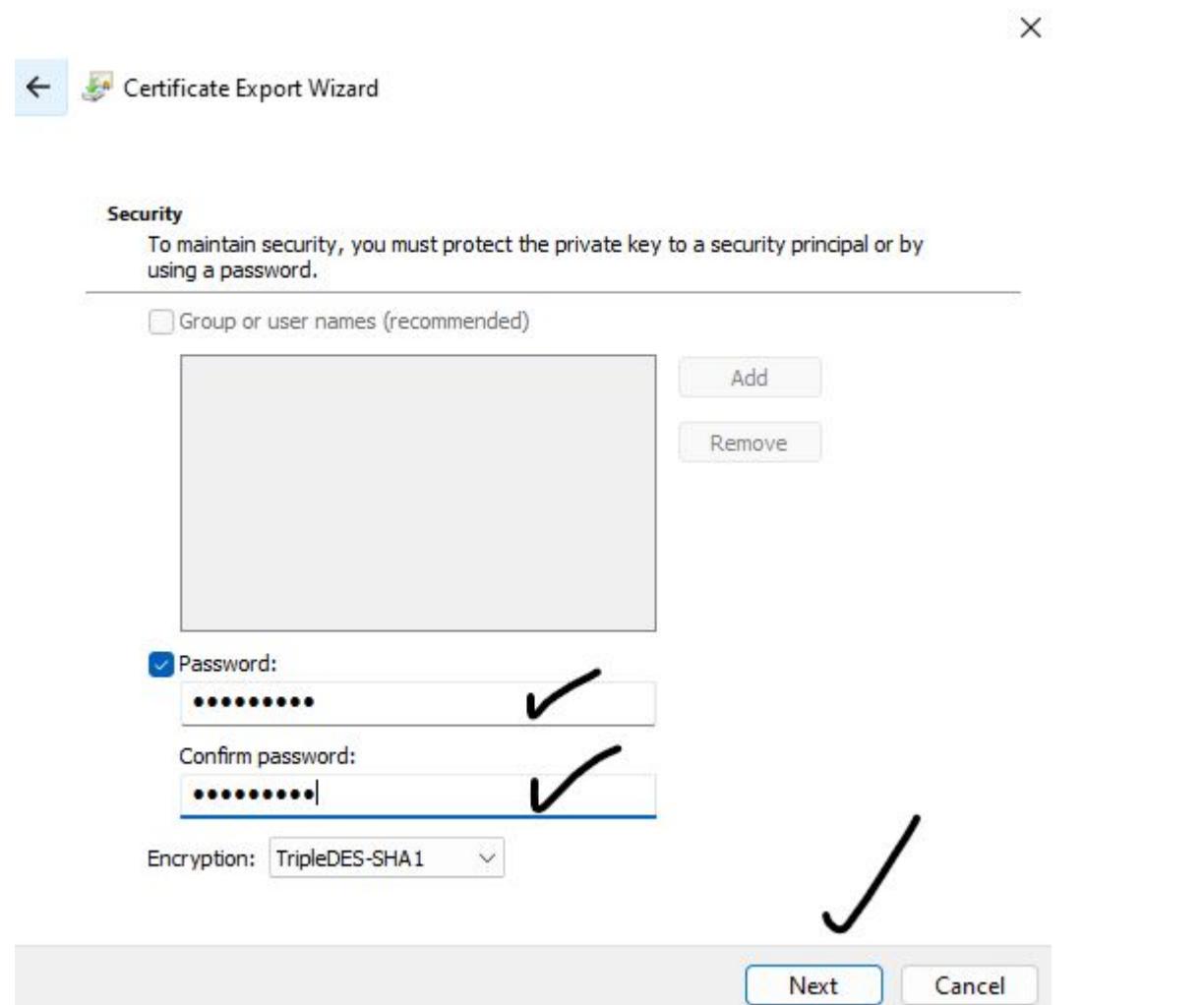
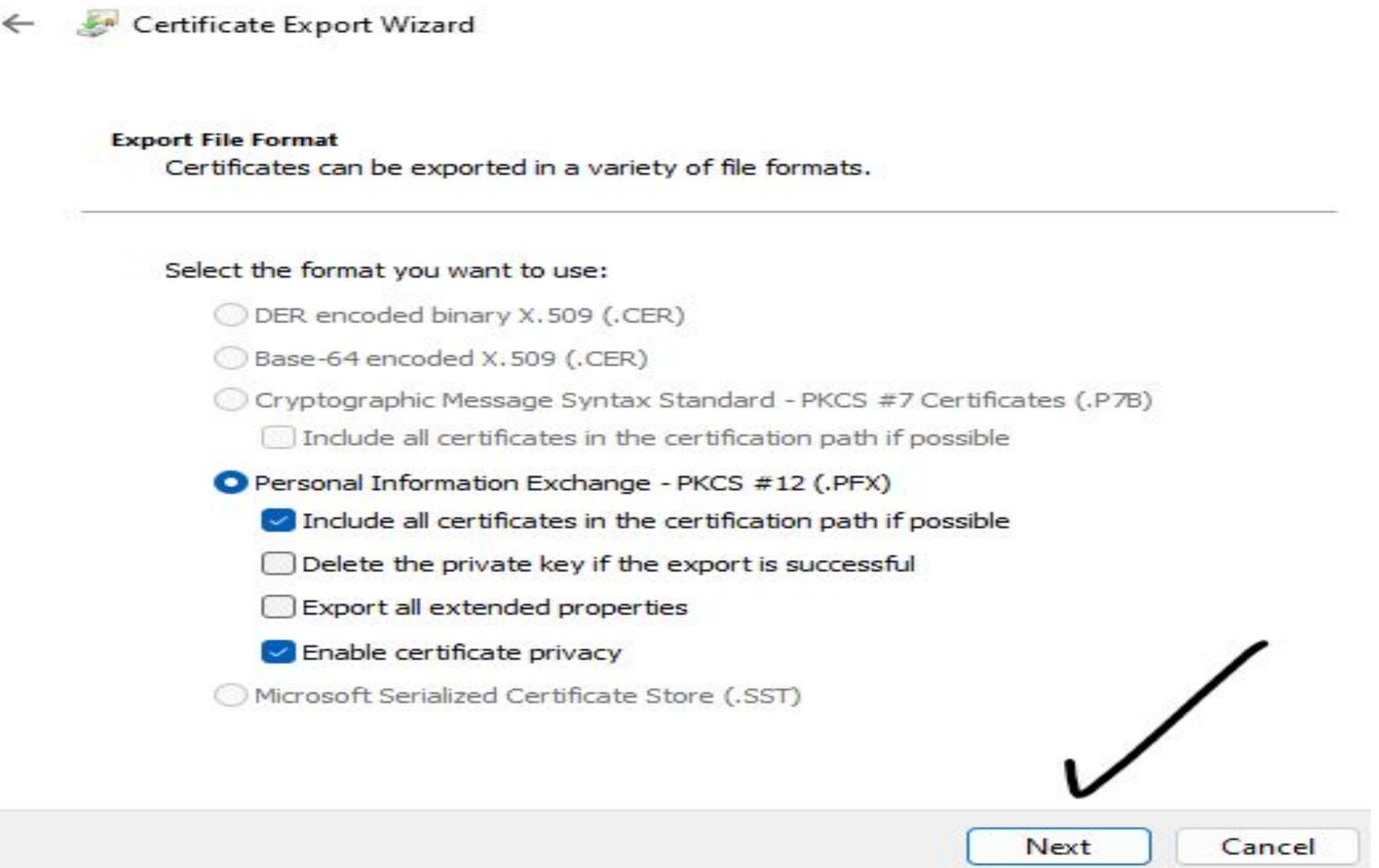
Finish

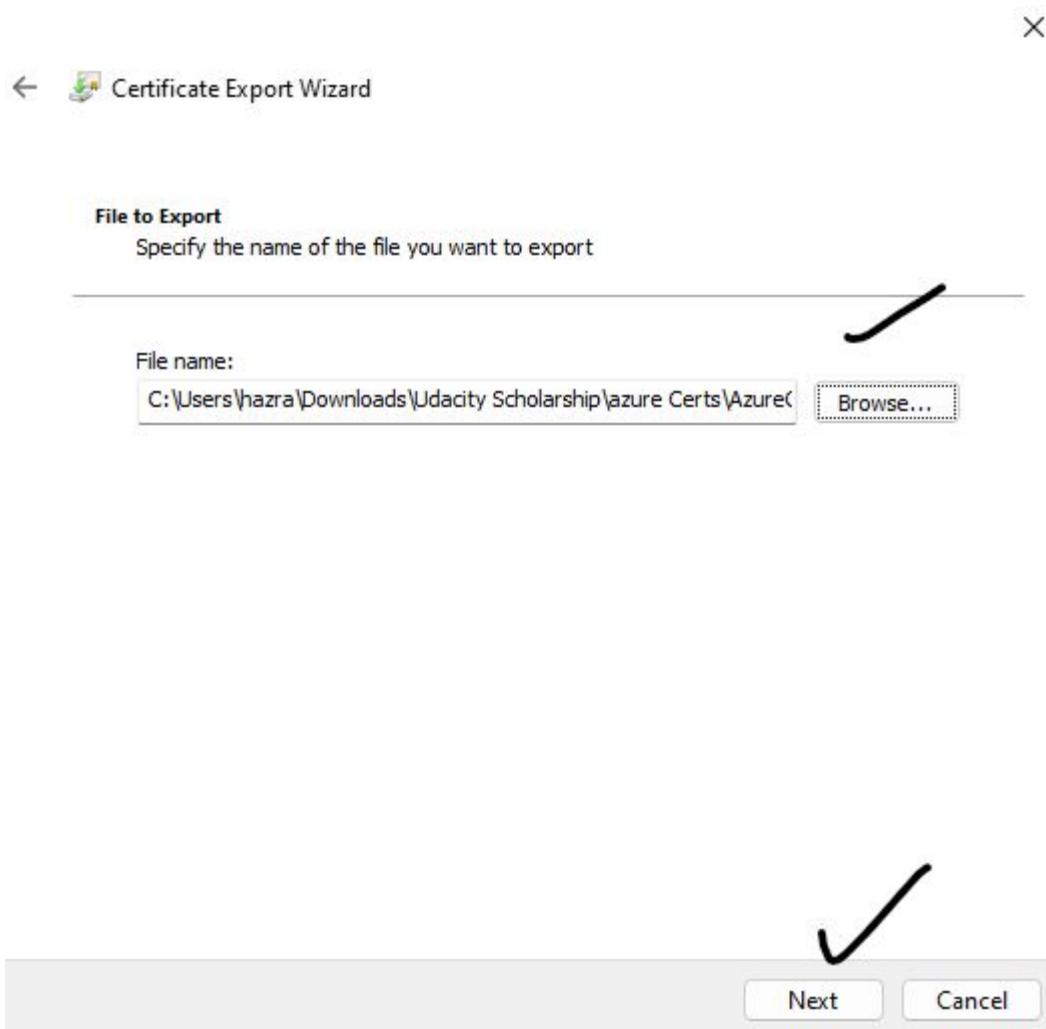
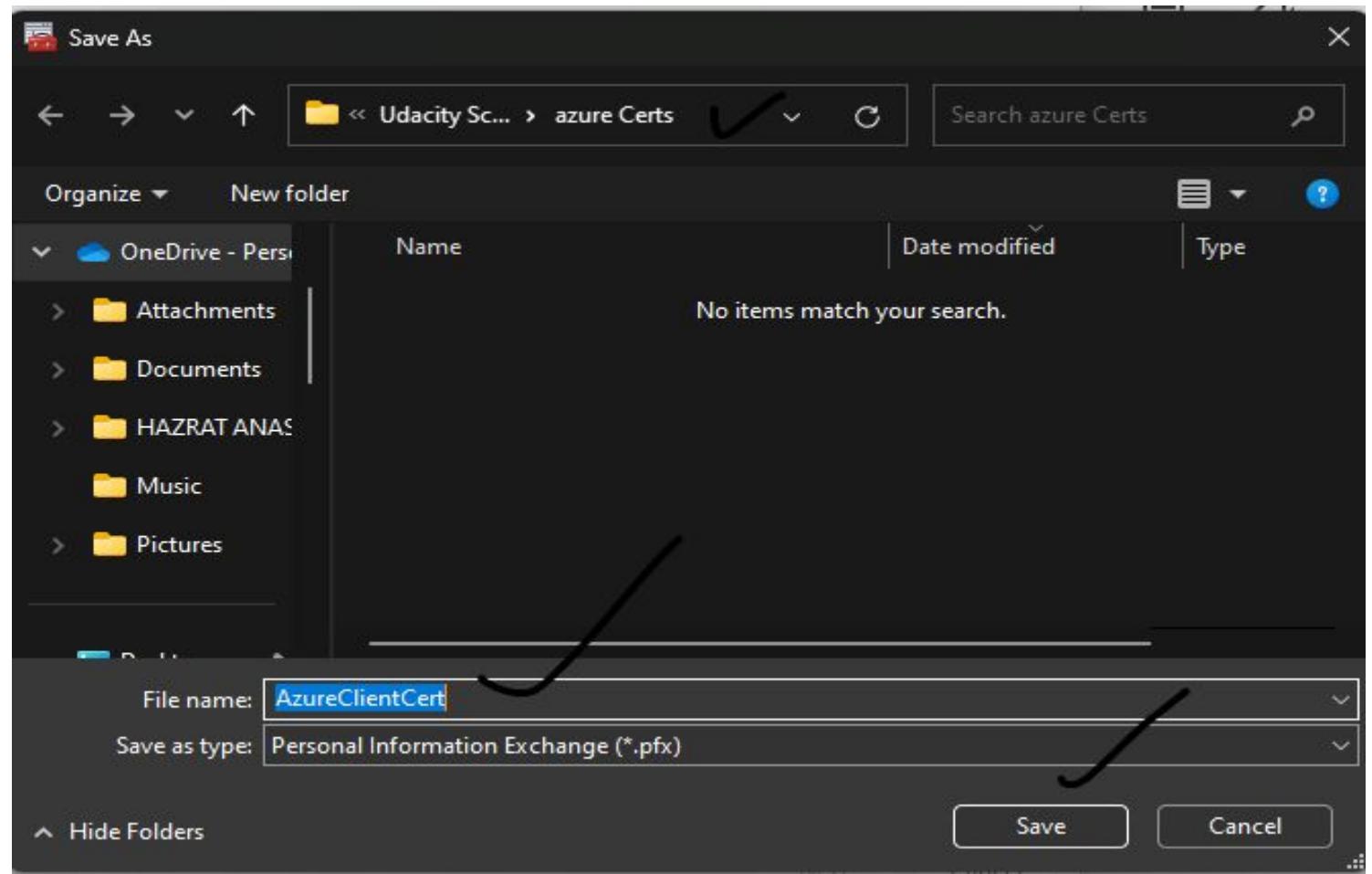
Cancel

Exporting the Client Cert

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









← 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



← Certificate Export Wizard



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

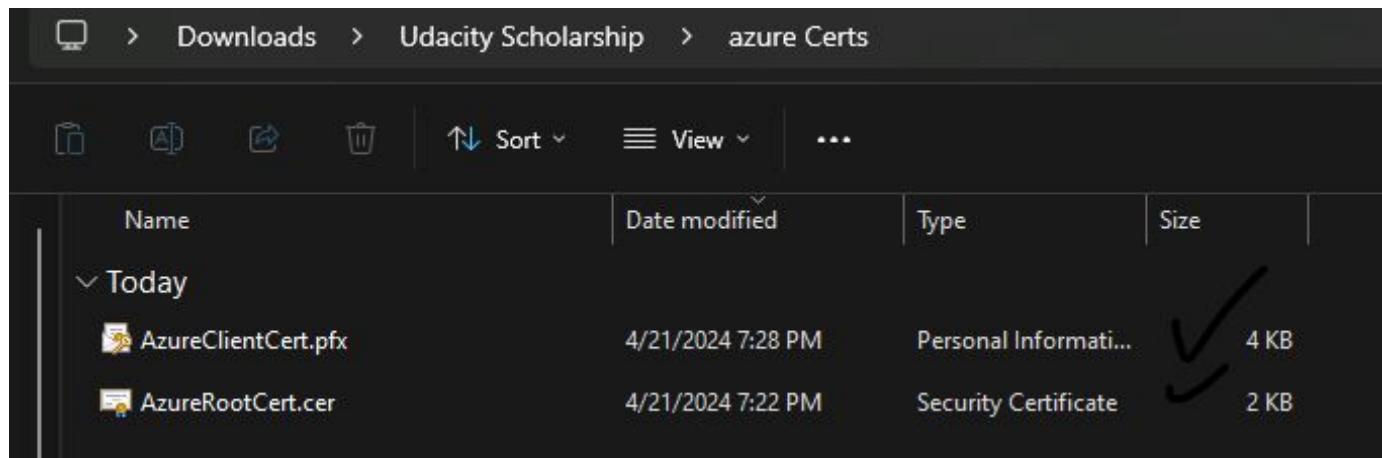
File Name
Export Keys
Include all certificates in the certification path
File Format



Finish

Cancel

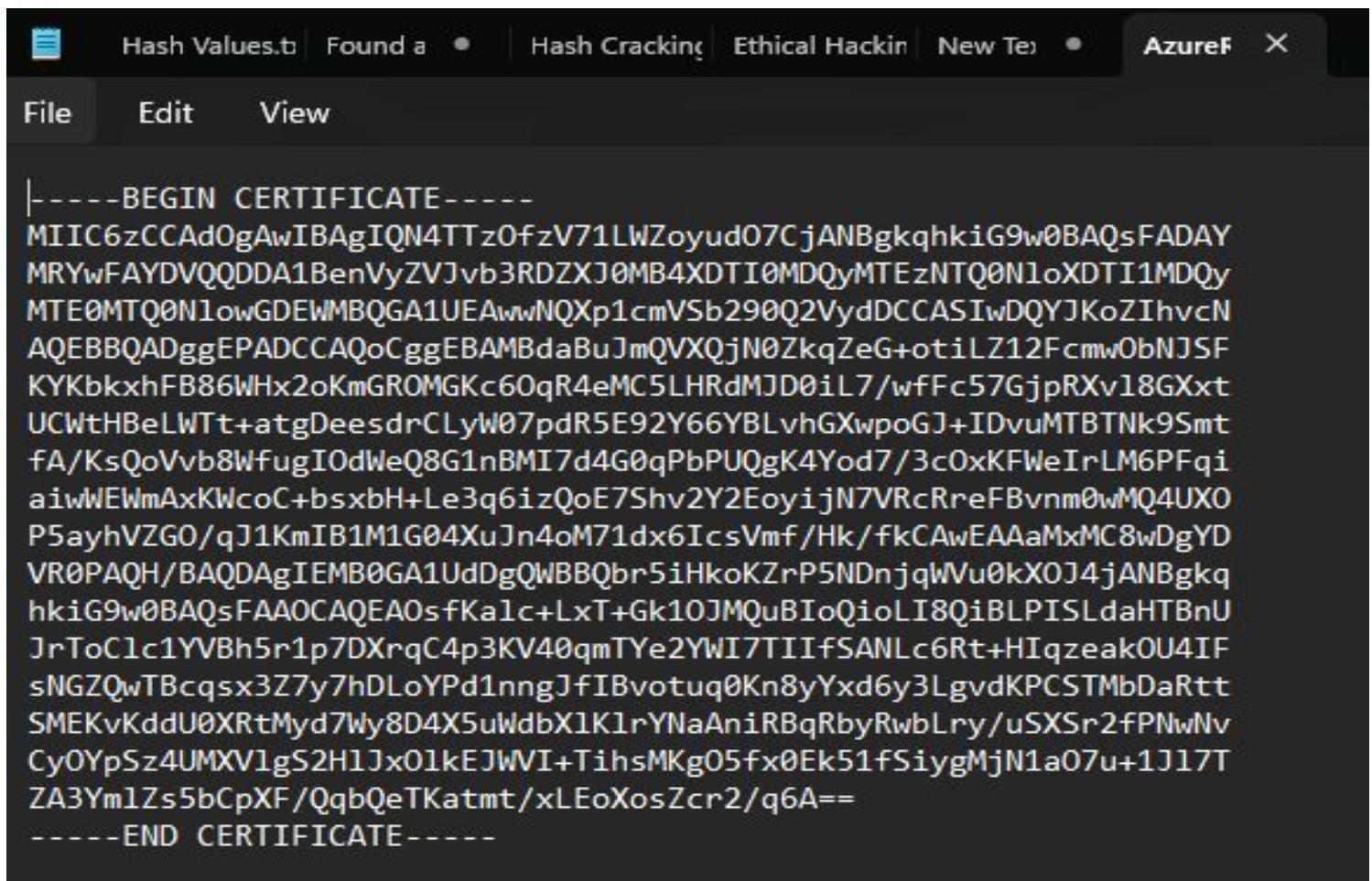
Both Root Cert and Client Certs Exported



A screenshot of a file explorer window titled "Downloads > Udacity Scholarship > azure Certs". The window shows a list of files with columns for Name, Date modified, Type, and Size. Two files are listed: "AzureClientCert.pfx" and "AzureRootCert.cer". Both files were modified on 4/21/2024 at 7:28 PM. "AzureClientCert.pfx" is a Personal Information file (4 KB) and "AzureRootCert.cer" is a Security Certificate (2 KB). Handwritten checkmarks are drawn next to both file names.

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

Opening the root cert through Notepad and copying its contents



The screenshot shows a Windows Notepad window with the title bar "Hash Values.txt" and the status bar "Found a". The menu bar includes "File", "Edit", and "View". The main content area displays the following text:

```
-----BEGIN CERTIFICATE-----
MIIC6zCCAdOgAwIBAgIQN4TTzOfzV71LWZoyud07CjANBgkqhkiG9w0BAQsFADAY
MRYwFAYDVQQDDA1BenVyZVJvb3RDZXJ0MB4XDTI0MDQyMTEzNTQ0N1oXTDI1MDQy
MTE0MTQ0N1owGDEWMBQGA1UEAwwNQXp1cmVSb290Q2VydDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMBdaBuJmQVXQjN0ZkqZeG+otilZ12Fcmmw0bNJSF
KYKbkxhFB86Whx2oKmGROMGKc60qR4eMC5LHRdMJD0iL7/wFFc57GjpRXv18GXxt
UCWtHBeLWTt+atgDeesdrCLyW07pdR5E92Y66YBLvhGXwpoGJ+IDvuMTBTNk9Smt
fA/KsQoVvb8WfugIOdWeQ8G1nBMI7d4G0qPbPUQgK4Yod7/3c0xKFWeIrLM6PFqi
aiwWEwmAxKwcoC+bsxbH+Le3q6izQoE7Shv2Y2EoyijN7VRcRreFBvnm0wMQ4UXO
P5ayhVZGO/qJ1KmIB1M1G04XuJn4oM71dx6IcsVm/ffkCAwEAAsMxMC8wDgYD
VR0PAQH/BAQDAgIE MB0GA1UdDgQWBHQbr5iHkoKZrP5NDnjqWVu0kXOJ4jANBgkq
hkiG9w0BAQsFAAOCAQEAsfKalc+LxT+Gk10JMQuBIoQioLI8QiBLPISLdaHTBnU
JrToC1c1YVBh5r1p7DXrqC4p3KV40qmTYe2YWI7TIIIfSANLc6Rt+HIqzeakOU4IF
sNGZQwTBcqsx3Z7y7hDLoYPd1nngJfIBvotuq0Kn8yYxd6y3LgvdKPCSTMbDaRtt
SMEKvKddU0XRtMyd7Wy8D4X5uWdbX1K1rYNaAniRBqRbyRwbLry/uSXSr2fPNwNv
Cy0YpSz4UMXV1gS2H1Jx01kEJWVI+TihsMKg05fx0Ek51fSiygMjN1a07u+1J17T
ZA3Ym1Zs5bCpXF/QqbQeTKatmt/xLEoXosZcr2/q6A==
-----END CERTIFICATE-----
```

Pasting it in azure

Root certificates

Name	Public certificate data
azureRoot	MIIC6zCCAdOgAwIBAgIQN4TTzOfzV71LWZoyudO7CjANB✓

✓ ✓

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

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

[info] 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

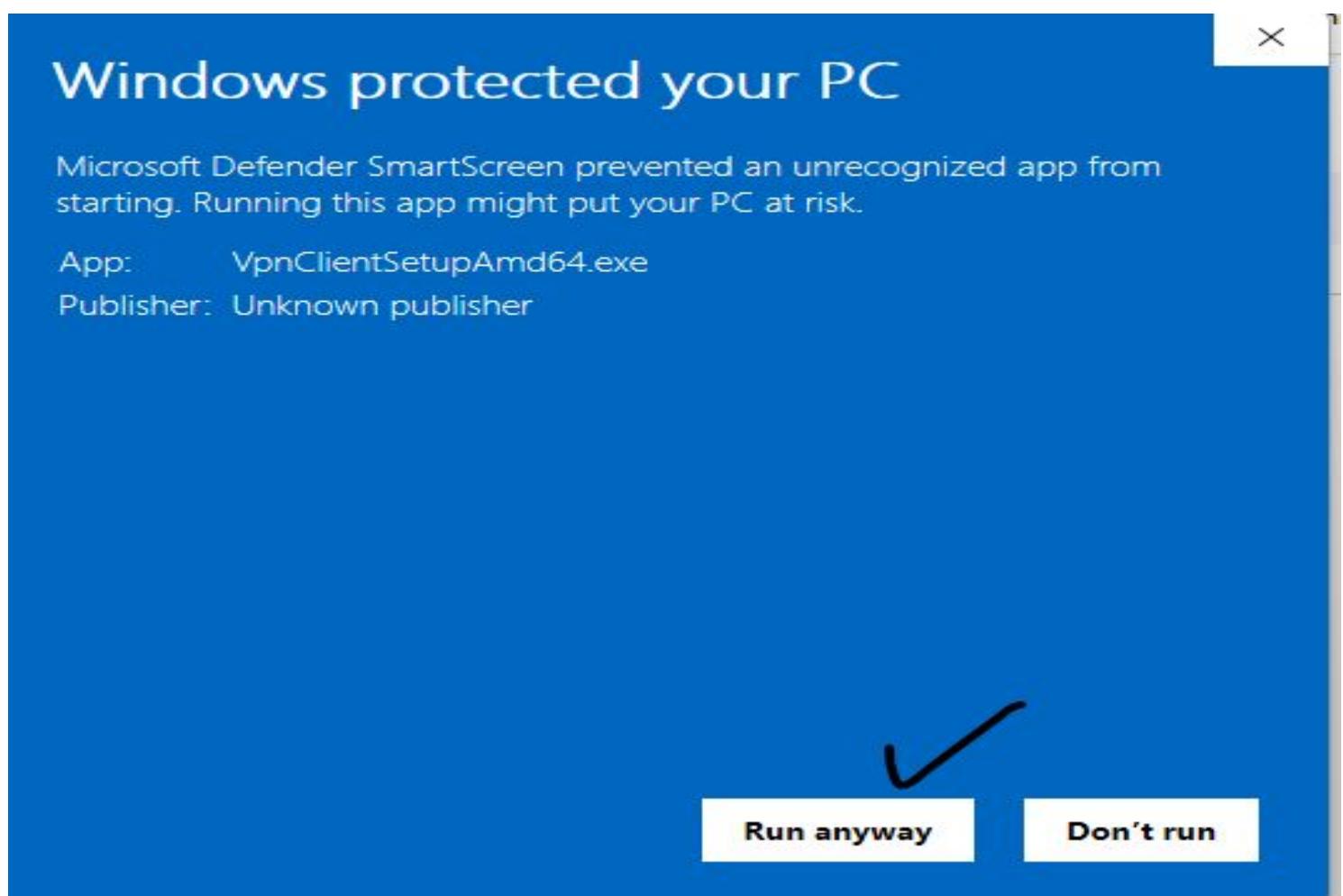
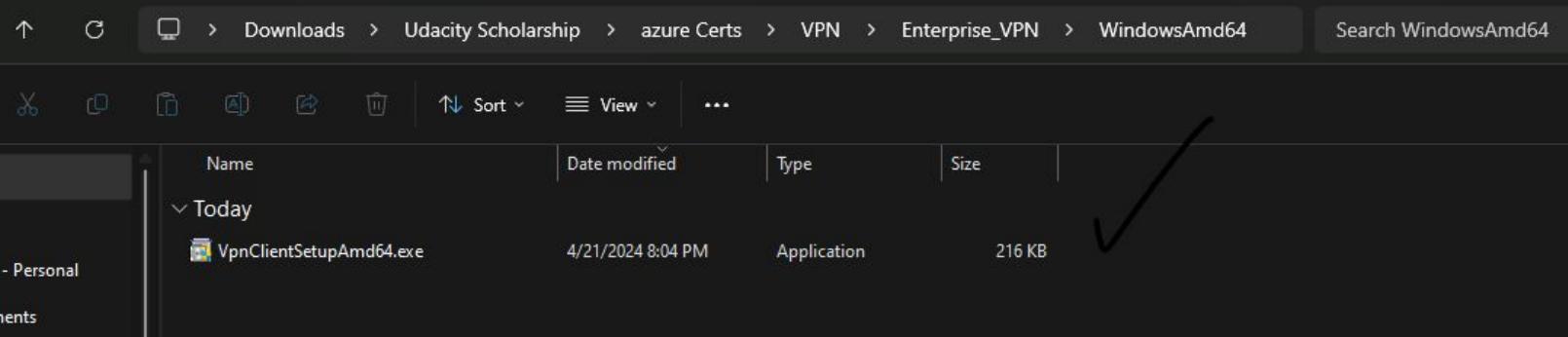
Name	Date modified	Type
VPN	4/21/2024 8:02 PM	File folder

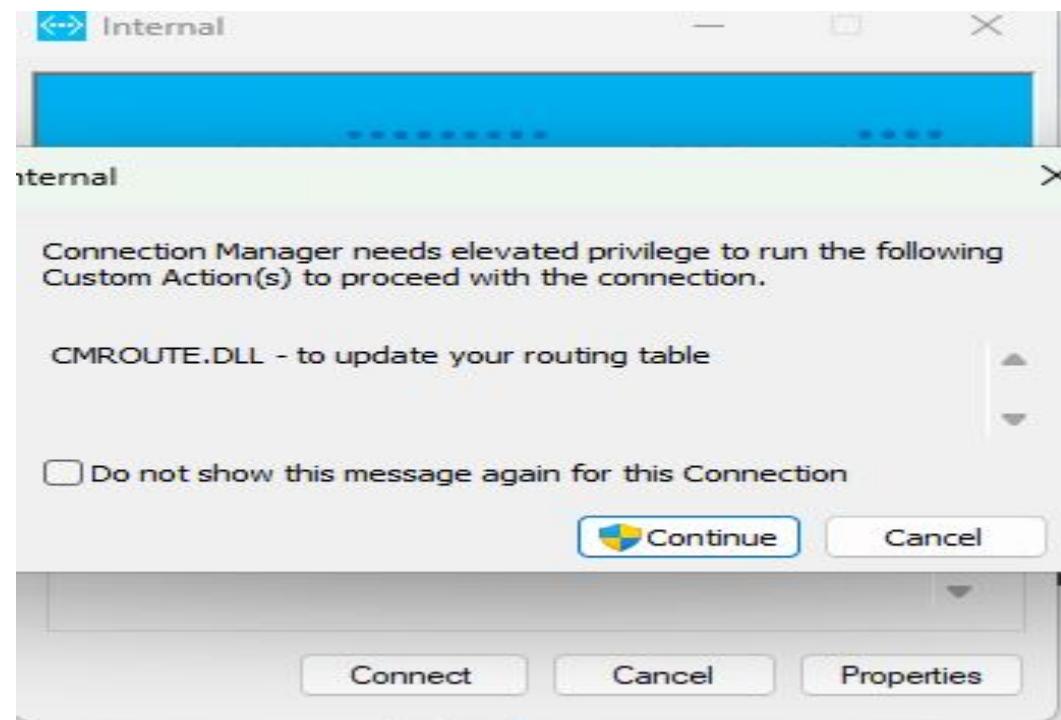
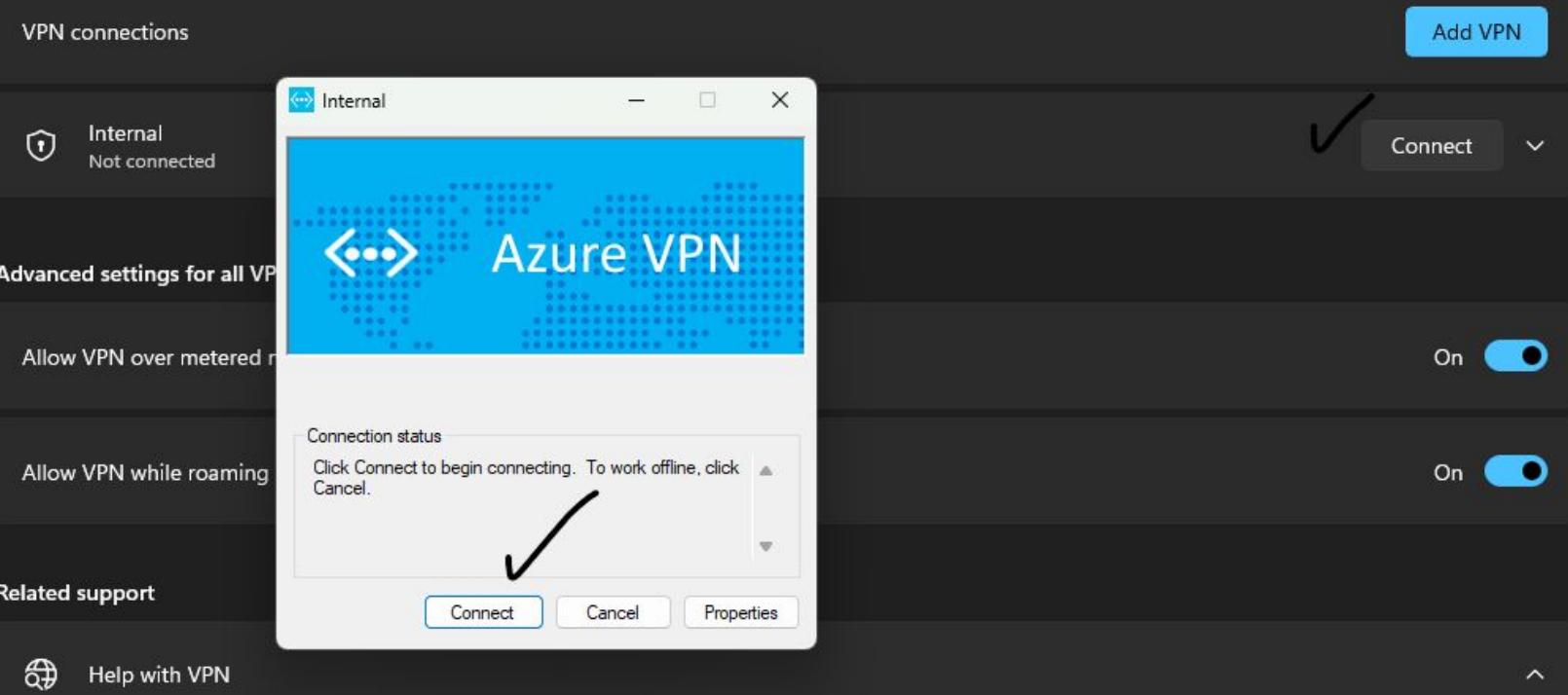
File name: Enterprise_VPN.zip
Save as type: WinRAR ZIP archive (*.zip)

Open Cancel

A large black checkmark is drawn over the 'Download VPN client' button in the Azure interface.

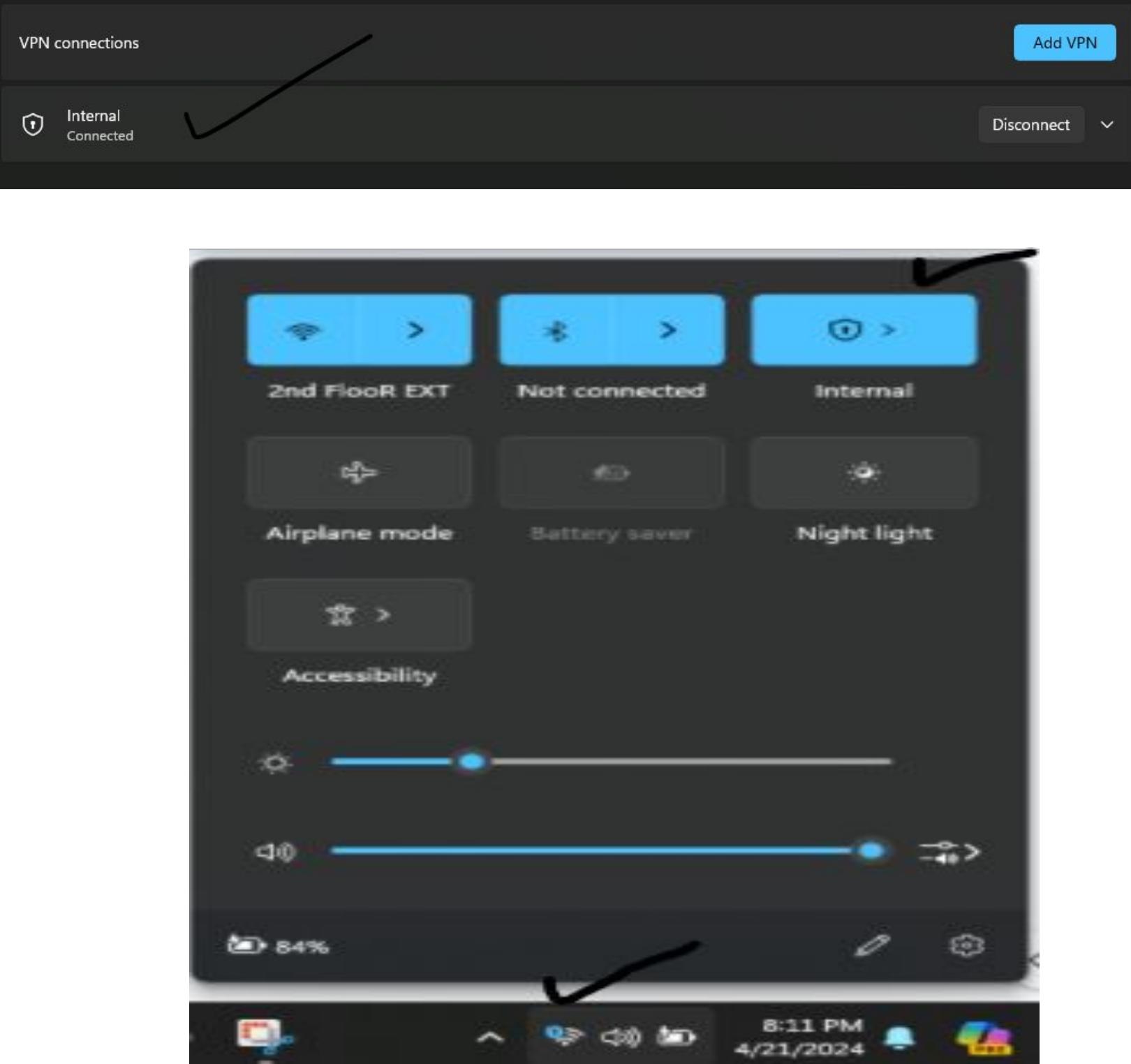
Installing the AMD 64





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.

vmEnterpriselInternal

Virtual machine

Search

Connect Start Restart Stop Hibernate (previe

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect Bastion

Networking

Network settings

Load balancing

Application security groups

Applications

Networking

Public IP address 20.51.207.33 (Network interface vmenterpriseinternal754_z1)

Public IP address (IPv6) -

Private IP address 10.0.3.4 ✓

Private IP address (IPv6) -

Virtual network/subnet Internal/Enterprise

DNS name Configure

Size

Standard B1s

vCPUs 1

Pinging VM private IP from my laptop

Successfully pinged

The screenshot shows the Microsoft Azure portal interface. On the left, a sidebar lists various options like Overview, Activity log, and Networking. The main area displays a virtual machine named "vmEnterpriseInternal". In the "Networking" section, the "Private IP address" is listed as "10.0.3.4". A black arrow points from this text to a Windows PowerShell window on the right. The PowerShell window shows the command "ping 10.0.3.4" and its output, which includes four successful replies from the private IP address.

```
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

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 *	Udacity CloudLabs Sub - 46 ✓
Resource group *	entp-project-258106 ✓ Create new

Instance details

Virtual network name *	ELK_VirtualNetwork ✓
Region * ⓘ	(US) East US ✓

[Previous](#)

[Next](#)

[Review + create](#)

Leaving the default IP addresses

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

10.0.0.0/16

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

Add a subnet

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

Virtual Network is Created

✓ Your deployment is complete

Deployment name : ELK_VirtualNetwork-1713728663893 Start time : 4/22/2024, 12:44:34 AM
Subscription : Udacity CloudLabs Sub - 46 Correlation ID : 7dd40798-158c-4e1d-81a4-175591d8...
Resource group : entp-project-258106

> 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

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

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

[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 ⓘ

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
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          Windows PowerShell          +  - 
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 AAAAB3NzaC1yc2EAAAQABAAQDzIaMqaOFJrX2ArVo1WYeWd6gCferDf7iinEPeNgvJSJvQuZzbNEE78EHV6xfL4UbzTV2GAyBApVQ+qW9
CVNhxDG9m0y5KrDHGVgMlwJuT4g6Y4Vg72RqdFPnPYtyXTfKEsaCJQkPsuhj8JdgxKcrBzTzY02EuDpVkb5/Ue9ArF2IdALH8simFpJxd6GZU1SOVFsc+EL
ltsIzi9tzhNA3ilAux0l8c++WhqEOPHiVOSzsGRGI4uEye5FcI0z5FcDXHczRv6cQcVENJ7u1z/Rl/rKtf/Ad6sMs6LSURCkiAL4iQtz2AQVm+jYUpFedw8
4PrhJuFbkhw1k6/PXkui51Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44hp3Xd10cHrAYR6NAi6EHY0GsdlxTqnhG5wFU
sdaLt3MEC1MBUiM/4hbbcrtnAzHpRsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMzpf0= hazra@Eagle
```

Copying and pasting public key to Azure Portal

Username *	azureuser
SSH public key source	Use existing public key
SSH public key *	<pre>51Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44hp3Xd10cHrAYR6NAi6EHY0GsdlxTqnhG5wFU sdaLt3MEC1MBUiM/4hbbcrtnAzHpRsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMzpf0= hazra@Eagle</pre>

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.

The screenshot shows the Azure portal interface for managing a virtual network. On the left, there's a sidebar with various settings like Address space, Connected devices, Subnets (which is selected and highlighted with a checkmark), Bastion, DDoS protection, Firewall, and Microsoft Defender for Cloud. The main area shows the 'Subnets' blade for the 'ELK_VirtualNetwork'. It lists one subnet named 'default' with an IPv4 range of 10.0.0.0/24 and 251 available IP addresses. A search bar at the top says 'Search subnets'. To the right, a modal window titled 'Add subnet' is open, prompting for details. The 'Name' field is filled with 'PrivateNetworkSubnet' (also marked with a checkmark). The 'Subnet address range' is set to '10.0.1.0/24', which is described as covering '10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)'. There's an unchecked checkbox for 'Add IPv6 address space'. The 'NAT gateway' dropdown is set to 'None'. The 'Network security group' dropdown is set to 'ELK_Network_Security_Group' (also marked with a checkmark). The 'Route table' dropdown is set to 'None'. Under 'SERVICE ENDPOINTS', there's a section with a checkmark. At the bottom of the modal are 'Save' and 'Cancel' buttons, and a 'Give feedback' link.

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 ✓

i 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

 Search

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

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

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

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

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings ✓

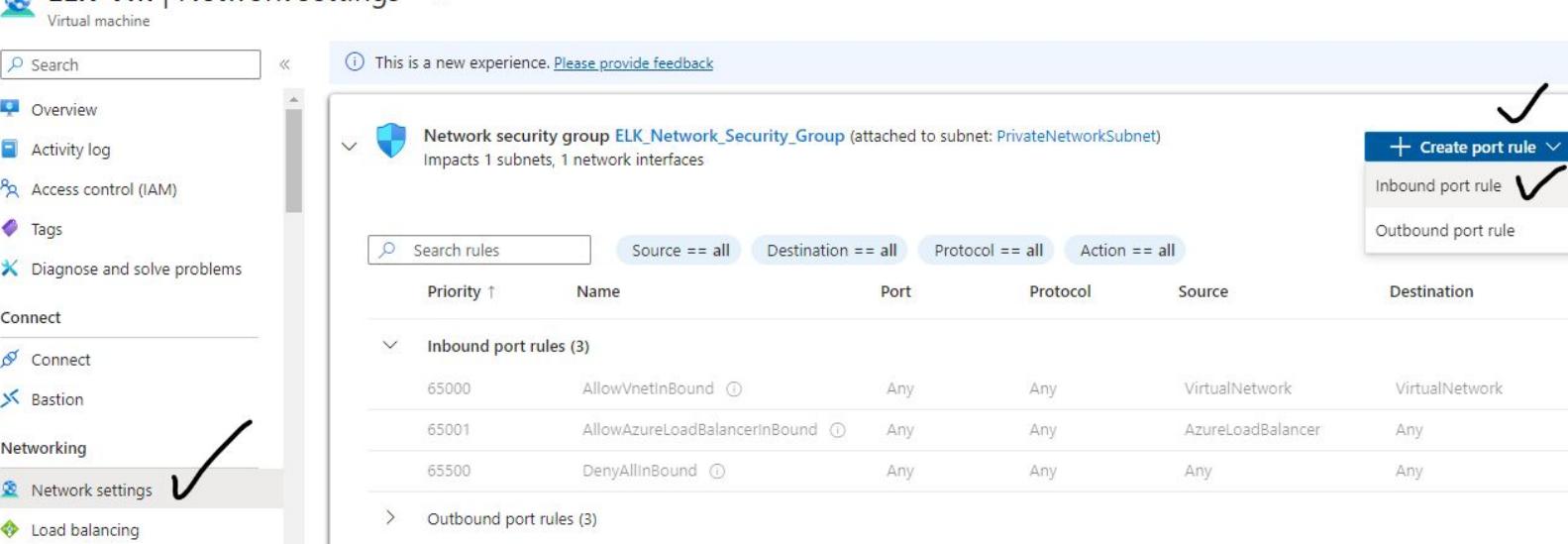
Load balancing

Search rules

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

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

> Outbound port rules (3)



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

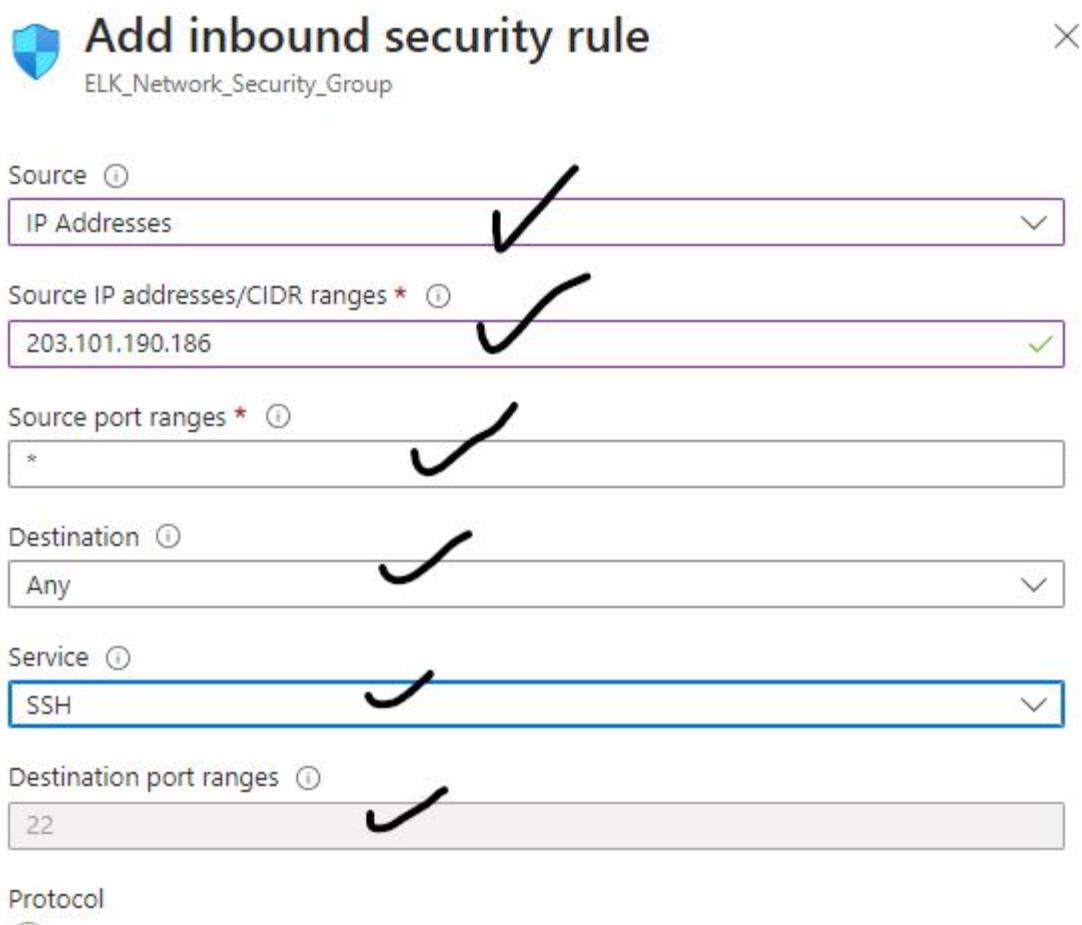
Service ① ✓

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

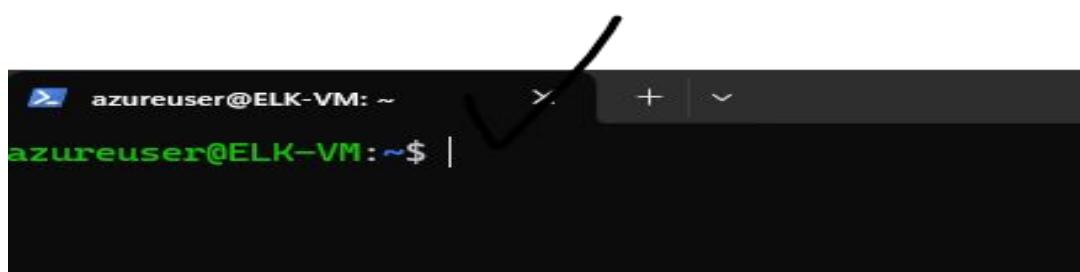
Action

Inbound port rules (4)

Priority	Name	Port	Protocol	Source	Destination	Action
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 [601 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: ~      x + ✓  
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 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	✗	✗

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	▼
Configure security features		
Image * ⓘ	Ubuntu Server 20.04 LTS - x64 Gen2	▼
See all images Configure VM generation		
VM architecture ⓘ	<input type="radio"/> Arm64	
	<input checked="" type="radio"/> x64	
Run with Azure Spot discount ⓘ	<input type="checkbox"/>	
Size * ⓘ	Standard_B1s - 1 vcpu, 1 GiB memory (\$7.59/month)	▼
See all sizes		
<p>i Item(s) availability based on policy assignment(s) for the selected scope. entp302-258106-PolicyDefinition-entp-project-258106 (Policy details)</p>		
Enable Hibernation (preview) ⓘ	<input type="checkbox"/>	
<p>i Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. Learn more ↴</p>		
Authentication type ⓘ	<input checked="" type="radio"/> SSH public key	✓
	<input type="radio"/> Password	
<p>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.</p>		
Username * ⓘ	azureuser	✓
SSH public key source	Use existing public key	✓
SSH public key * ⓘ	<pre>51Y0sAllh0qotnBP40B8T2H8xfalRnO4Ga501bet0UQdbfg+RX2TUxCnLvi3te44 hp3Xd1OcHrAYR6NAi6EHY0GsdIxTqnG5wFUsdaLt3MEC1MBUiM/4hbbcrtN AzHpRsvAn3W4pb1eanSaUaiY9yezTL+UoEt5bEpeODMZpf0= hazra@Eagle</pre>	
<p>i Learn more about creating and using SSH keys in Azure ↴</p>		

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.

Network Settings

Network interface

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

Virtual network * ⓘ


[Create new](#)

Subnet * ⓘ


[Manage subnet configuration](#)

Public IP ⓘ


[Create new](#)

NIC network security group ⓘ

None
 Basic
 Advanced 

Configure network security group *


[Create new](#)

Delete public IP and NIC when VM is deleted ⓘ

Enable accelerated networking ⓘ

The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more ↗](#)

Load balancing options ⓘ

None
 Azure load balancer 

< Previous

Next : Management >

Review + create

Setting up the web server

SSH into web Server

```
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

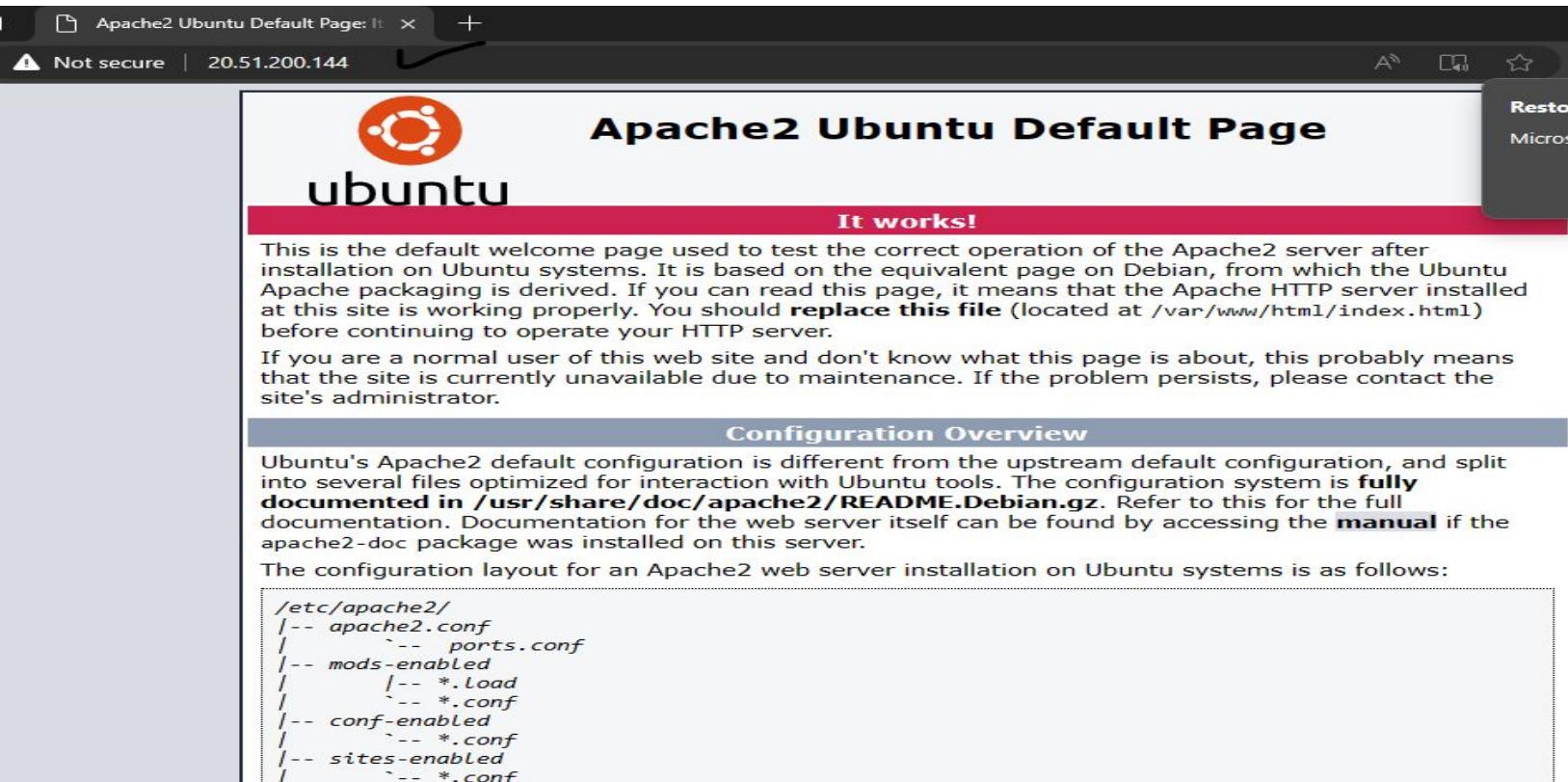
```
azureuser@WebServer:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Active: active (running) ✓ since Sun 2024-04-21 23:46:27 UTC; 8min ago
    Docs: https://httpd.apache.org/docs/2.4/
 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 itself features the Ubuntu logo and the text "Apache2 Ubuntu Default Page". Below this, a red banner displays the message "It works!". The main content area explains that this is the default welcome page for an Apache2 server on Ubuntu. It includes a note about maintenance and a "Configuration Overview" section detailing the file structure of the configuration files. The browser's address bar shows the URL "20.51.200.144".

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"
```

ELK-VM

Virtual machine

Search

Connect Start Restart Stop Hibernate (preview) Capture

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Computer name: ELK-VM

Operating system: Linux (ubuntu 20.04)

VM generation: V2

Networking

Public IP address: 20.115.46.64 (Network)

Public IP address (IPv6): -

Private IP address: 10.0.1.4

```
# 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 ^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 on the left, a "Sign In" button, and a "Join now!" button. Below the header, there are "Features" and "Pricing" links. A green success message box displays the text "Success, you are now disconnected." In the center, a large red button with white text reads "INSTANTLY DRIVE TO ANY WEBSITE" and "thousands of visits". The background of the main content area features a world map pattern.

3.2.4 Screenshot

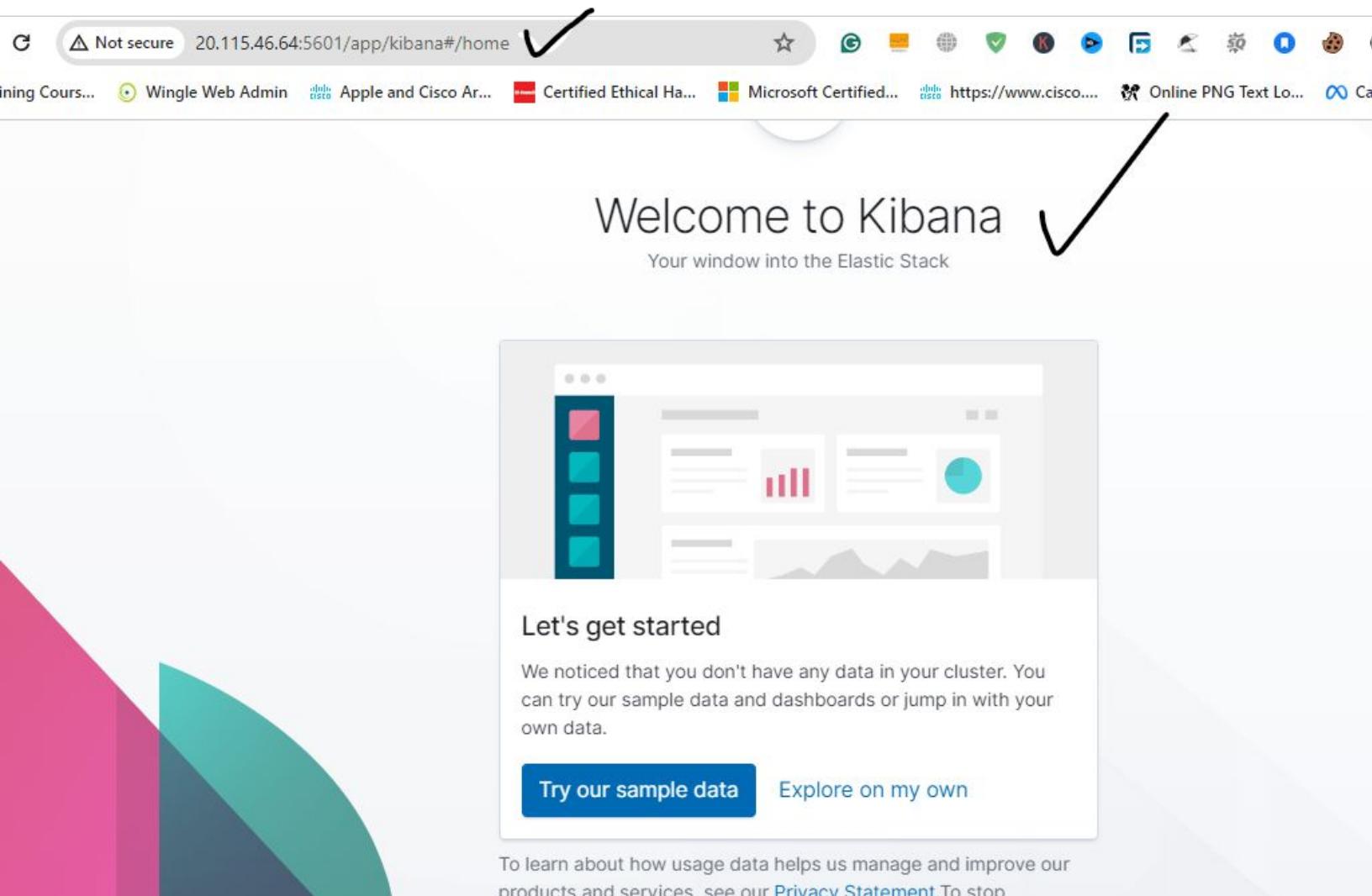
Web server logs appear in Kibana.

Accessing Kibana

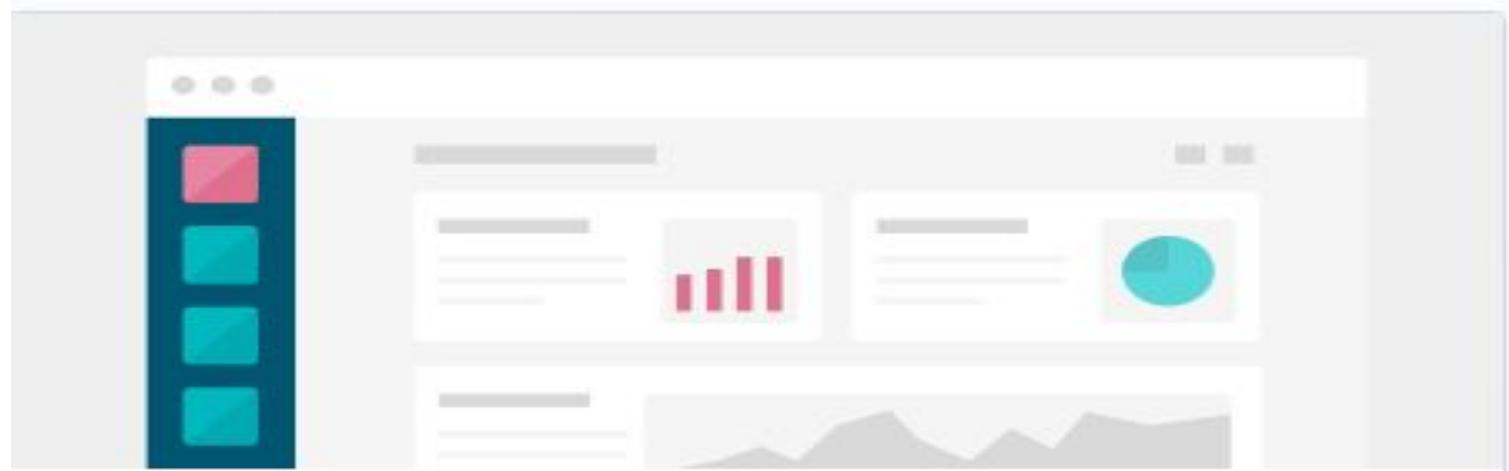
Copy the public IP of ELK Server

Go to your browser and paste that IP along with Kibana port

You will see a Kibana screen



Click on Explore on my Own



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](#)

Not secure 20.115.46.64:5601/app/kibana#/management?_g=()

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

Management

Visualize

Dashboard

Canvas

Maps

Machine Learning

Metrics

Logs

APM

Uptime

SIEM

Dev Tools

Stack Monitoring

Management

Kibana 7.6.1 management

Manage your indices, index patterns, saved objects, Kibana settings, and more.

A full list of tools can be found in the left menu

Licence Management

The screenshot shows the Elastic Stack interface with a sidebar on the left containing various icons and a main content area on the right.

Management (highlighted with a teal box)

Help us improve the Elastic Stack
To learn about how usage data helps us manage and improve

Elasticsearch

- Index Management
- Index Lifecycle Policies
- Rollup Jobs
- Transforms
- Remote Clusters
- Snapshot and Restore
- License Management ✓
- 8.0 Upgrade Assistant

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 modal dialog overlaid. The modal has a title 'Help us improve the Elastic Stack' and a large button labeled 'Discover' with a checkmark icon. Below the button is a 'Dismiss' button. The background shows the 'Management / License management' section of Kibana, with icons for Index Management, Elasticsearch, and other features like Index Lifecycle Policies and Rollup Jobs.

Continuous Monitoring & Observability

Kibana

Not secure 20.115.46.64:5601/

Free Training Courses Wingle Web Admin Cisco Analytics

D Management / License management

Help us improve the Elastic Stack

Discover about how usage data helps us

Dismiss

Elasticsearch

Index Management

Index Lifecycle Policies

Rollup Jobs

Transforms

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

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

> Next step

Index Management

Index Lifecycle Policies

Rollup Jobs

Transforms

Cross-Cluster Replication

Remote Clusters

Watcher

Snapshot and Restore

License Management

8.0 Upgrade Assistant

Kibana

Index Patterns

Saved Objects

Spaces

Reporting

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

@timestamp ✓

- event.created
- event.end
- event.start
- file.accessed
- file.created
- file.ctime
- file.mtime
- kafka.block_timestamp
- process.start
- suricata.eve.flow.end
- suricata.eve.flow.start
- suricata.eve.timestamp
- suricata.eve.tls.notafter
- suricata.eve.tls.notbefore

I don't want to use the Time Filter

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

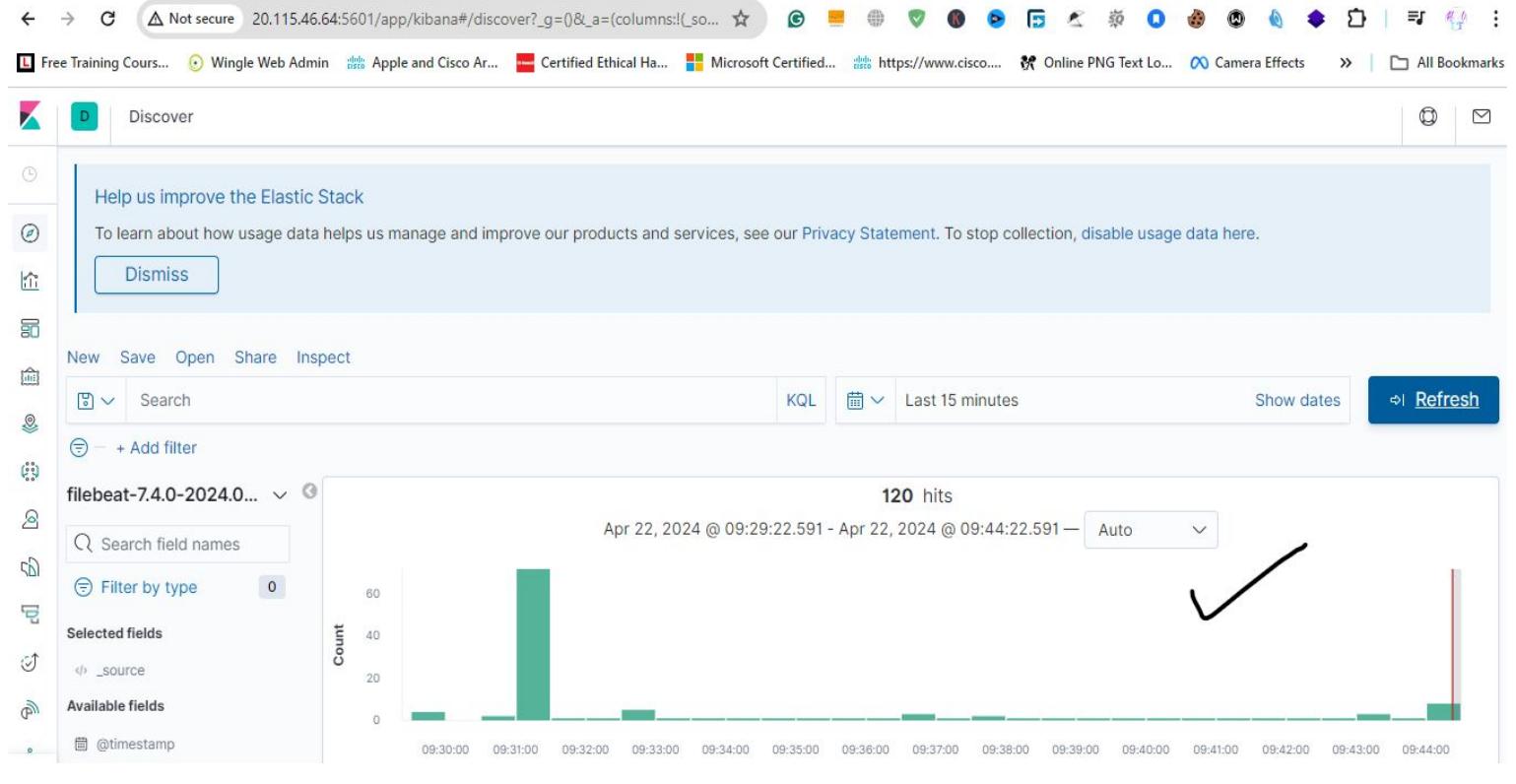
This page lists every field in the **filebeat-7.4.0-2024.04.22-000001** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#)

Fields (1130)	Scripted fields (0)	Source filters (0)				
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-7.4.0-2023-07-10-12-00". Below the tabs, the URL bar shows "Not secure" and the address "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 a "Discover" button, which is highlighted with a black callout bubble and a hand-drawn arrow pointing to it. The main content area is titled "Management / Index patterns / filebeat-7.4.0-2023-07-10-12-00" and contains sections for "Elasticsearch", "Index Management", "Discover", "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".

We are able to visualize our web server logs



Available fields	Time	_source
@timestamp	09:30:00 - 09:44:00	@timestamp per 30 seconds
t _id	> 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
t _index	> 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
# _score	> 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
t _type	> 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
t agent.ephemeral_id	> 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
t agent.hostname	> 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
t agent.id	> 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
t agent.type	> 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
t agent.version	> 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
t cloud.instance.id	> 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
t cloud.instance.name	> 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
t cloud.machine.type	> 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
t cloud.provider	> 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
t cloud.region	> 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

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.

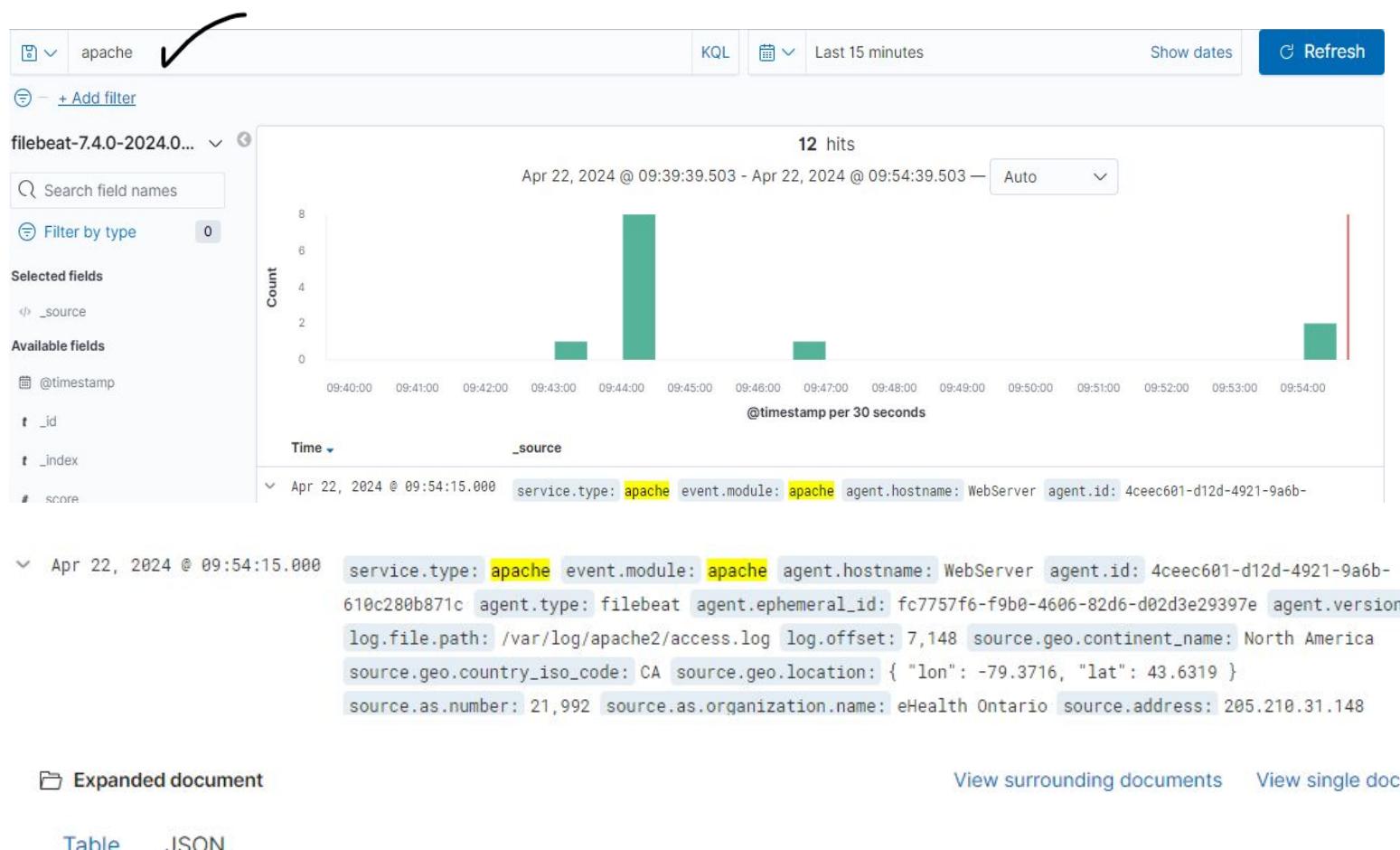
Insert screenshots on the following pages, showing completion of each of the specified tasks.

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

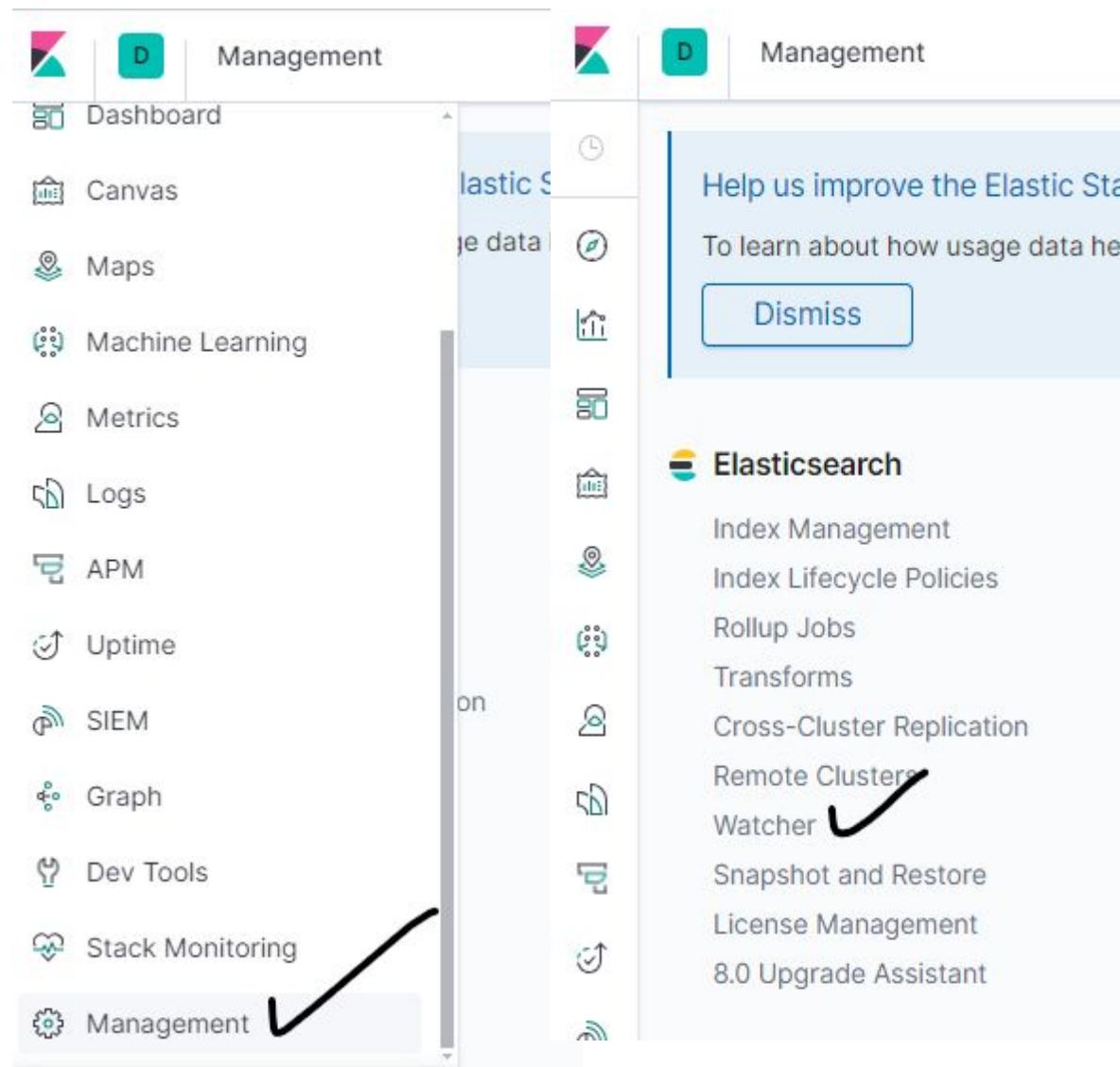
If someone is requesting to our Site it will be a an indicator for an alert. We can create an alert when someone Get Request to our site

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.

You

yet

Watch for ch

take action if

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 X



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.

10:15:00

Index



Index data into Elasticsearch.

Add action ▾

PagerDuty



Create an event in PagerDuty.

Jira



Create an issue in Atlassian's Jira Software.

Show request

Create a text and click on create alert

Perform 1 action when condition is met

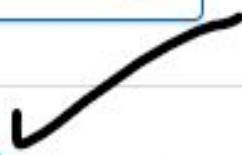
Logging

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.

Search...

[Create](#)

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

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 }
```

```
{  
  "trigger": {  
    "schedule": {  
      "interval": "5m"  
    }  
  },  
  "input": {  
    "search": {  
      "request": {  
        "search_type": "query_then_fetch",  
        "indices": [  
          "filebeat-7.4.0-2024.05.02-000001"  
        ],  
        "rest_total_hits_as_int": true,  
        "body": {  
          "query": {  
            "bool": {  
              "must": [  
                {  
                  "match": {  
                    "Name": "BruteForceAttack"  
                  }  
                },  
                {  
                  "match": {  
                    "event.code": "4625"  
                  }  
                },  
                {  
                  "exists": {  
                    "field": "host.name"  
                  }  
                }  
              ]  
            }  
          }  
        }  
      }  
    }  
  }  
}
```

```
,  
  "condition": {  
    "script": {  
      "source": "return ctx.payload.hits.total.value > params.threshold",  
      "lang": "painless",  
      "params": {  
        "threshold": 10  
      }  
    }  
  },  
  "actions": {  
    "email_admin": {  
      "email": {  
        "profile": "standard",  
        "to": [  
          "admin@example.com"  
        ],  
        "subject": "Potential Brute Force Attack Detected",  
        "body": {  
          "text": "A potential brute force attack has been detected. Please investigate immediately."  
        }  
      }  
    }  
  }  
}
```

3.3.3 Screenshot

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

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 ▾ }
```

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          "script": "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    },
27    "condition": {
28      "script": {
29        "source": "return ctx.payload.hits.total.value > params.threshold",
30        "params": {
31          "threshold": 50 // Adjust the threshold based on your environment and expected legitimate traffic
32        }
33      }
34    },
35    "actions": {
36      "email_admin": {
37        "email": {
38          "to": "admin@example.com",
39          "subject": "Potential Scanning Attack Detected",
40          "body": {
41            "text": "A potential scanning attack has been detected. Please investigate immediately."
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.

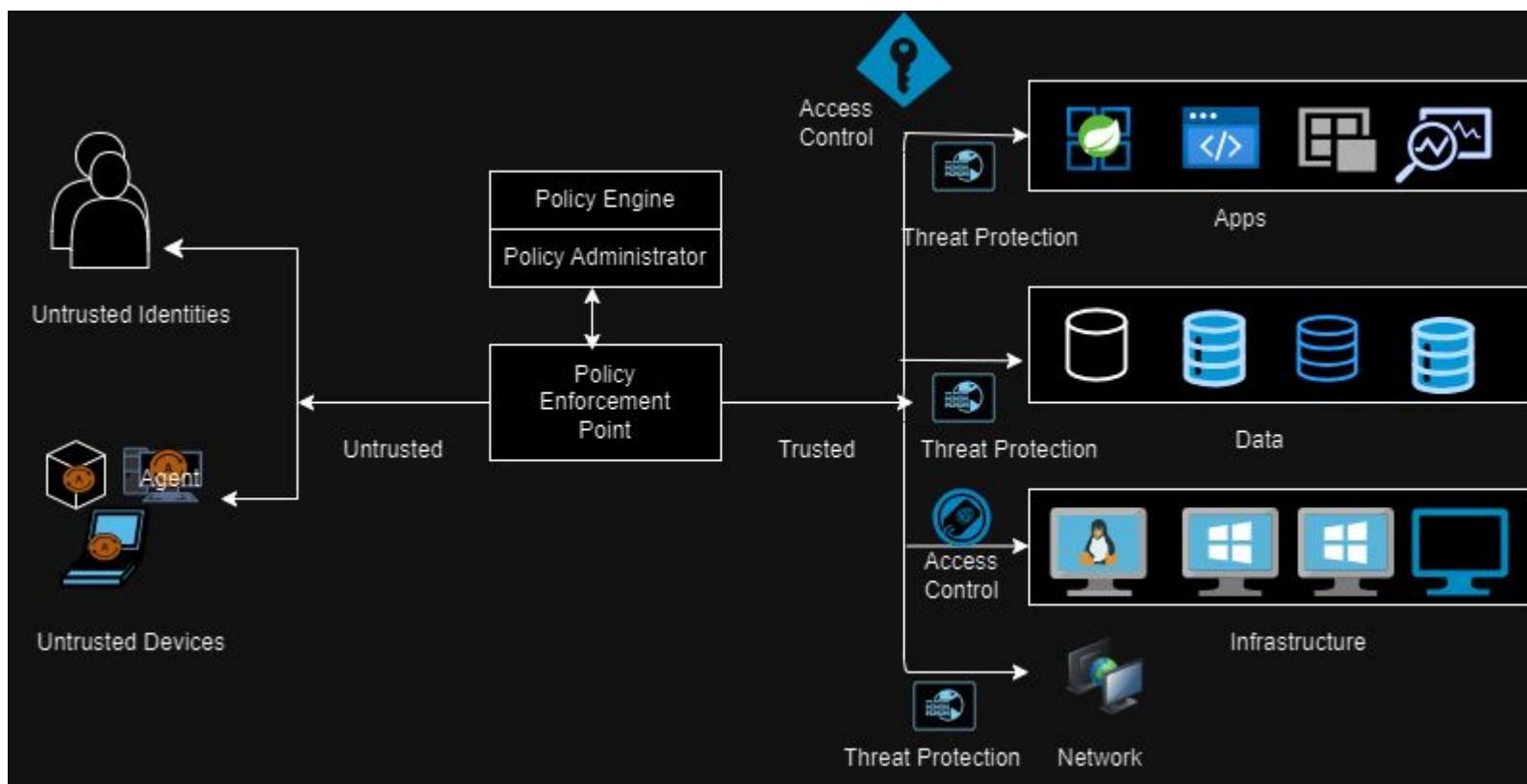
Design a Zero Trust model of your network architecture using <https://app.diagrams.net/>.

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/>