Project:
Securing the Perimeter

Directions and Submission Template

SIMPSON INNOCENT NANA
31ST MARCH, 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:

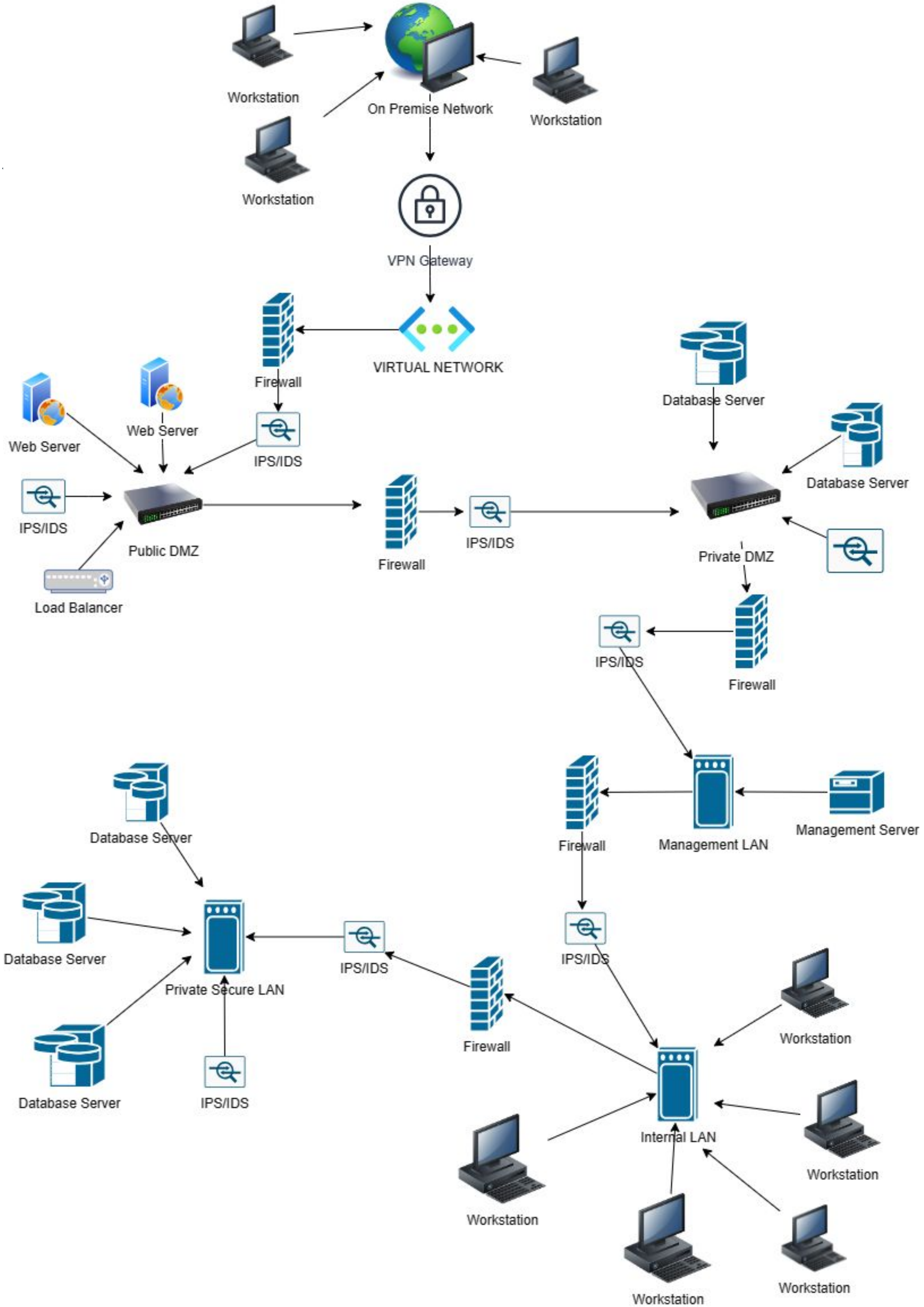
- Public DMZ with two web servers and a load balancer in it.
- Private DMZ with two database servers.
- Management LAN with one management server in it.
- Internal LAN with 5 workstations in it.
- Private Secure LAN with 3 database servers.

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.


Workstation
On Premise Network
Workstation
Workstation
VPN Gateway
VIRTUAL NETWORK
Firewall
Database Server
Web Server
Web Server
IPS/IDS
Database Server
IPS/IDS
Public DMZ
Firewall
IPS/IDS
Private DMZ
Load Balancer
IPS/IDS
Firewall
Database Server
Firewall
Management LAN
Management Server
Database Server
IPS/IDS
IPS/IDS
Private Secure LAN
Workstation
Firewall
Database Server
IPS/IDS
Internal LAN
Workstation
Workstation
Workstation
Workstation

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.

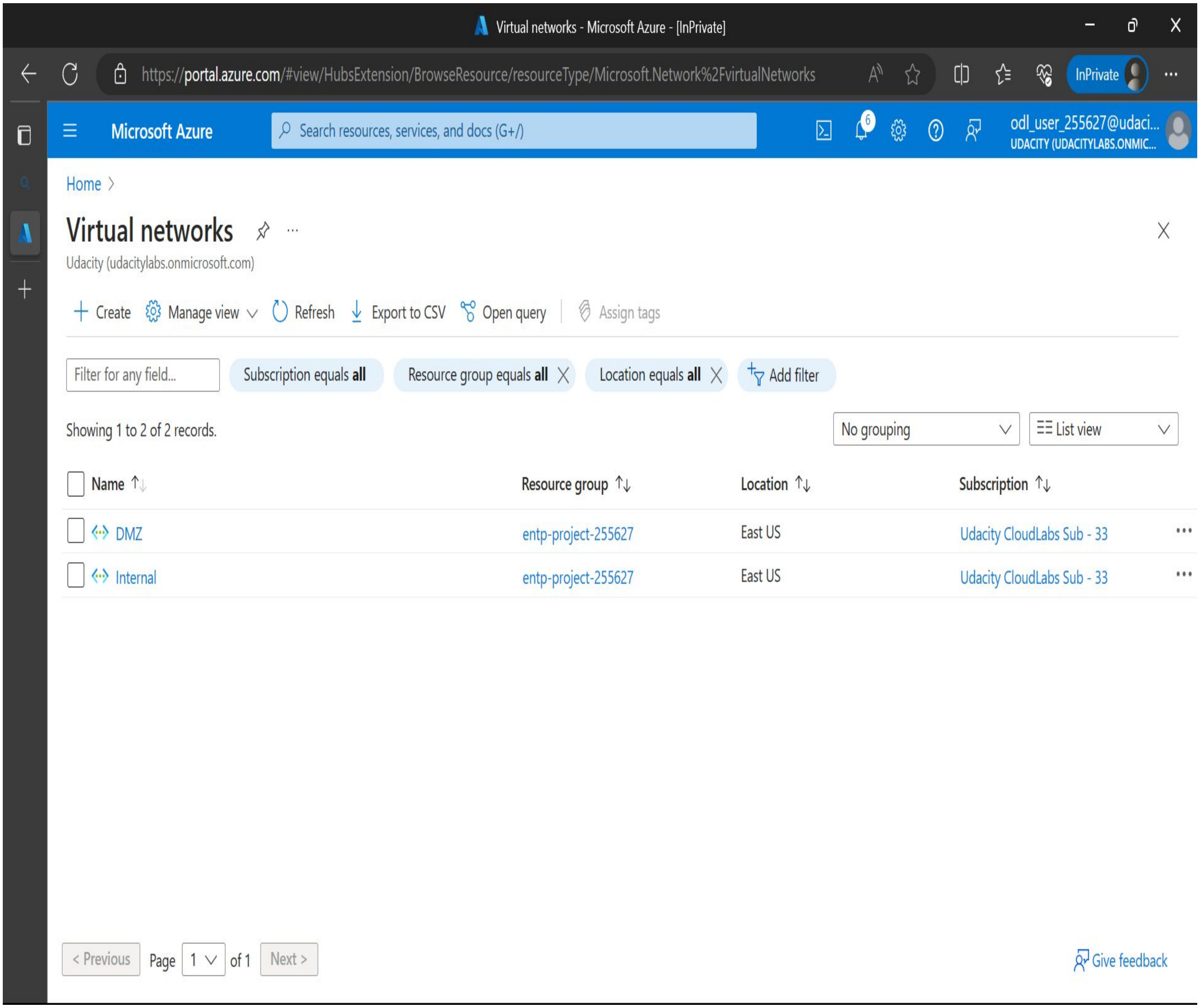
If you are accessing Azure using your own Azure account, first of all you should create a resource group called ‘entp-project’.

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.


Virtual networks - Microsoft Azure - [InPrivate]
https://portal.azure.com/#view/HubsExtension/BrowseResource/resourceType/Microsoft.Network%2FvirtualNetworks
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
odl_user_255627@udaci...
UDACITY (UDACITYLABS.ONMIC...
Home
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Filter for any field...
Add filter
No grouping
List view
< Previous
Page
1
of 1
Next >
Give feedback

Virtual networks

Udacity (udacitylabs.onmicrosoft.com)

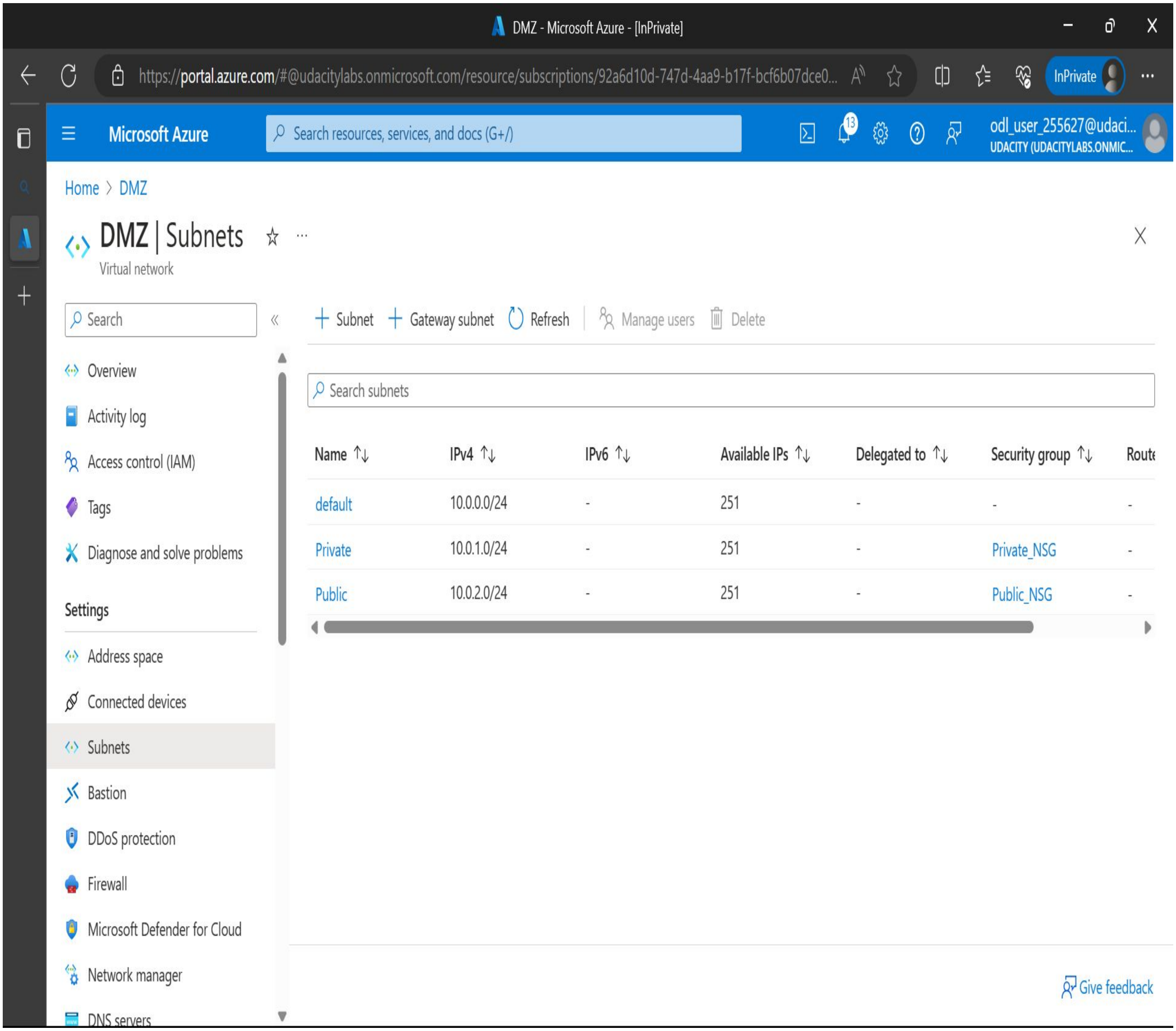
Subscription equals **all** | Resource group equals **all** | Location equals **all**

Showing 1 to 2 of 2 records.

Name	Resource group	Location	Subscription
DMZ	entp-project-255627	East US	Udacity CloudLabs Sub - 33
Internal	entp-project-255627	East US	Udacity CloudLabs Sub - 33

2.1.2 Screenshot

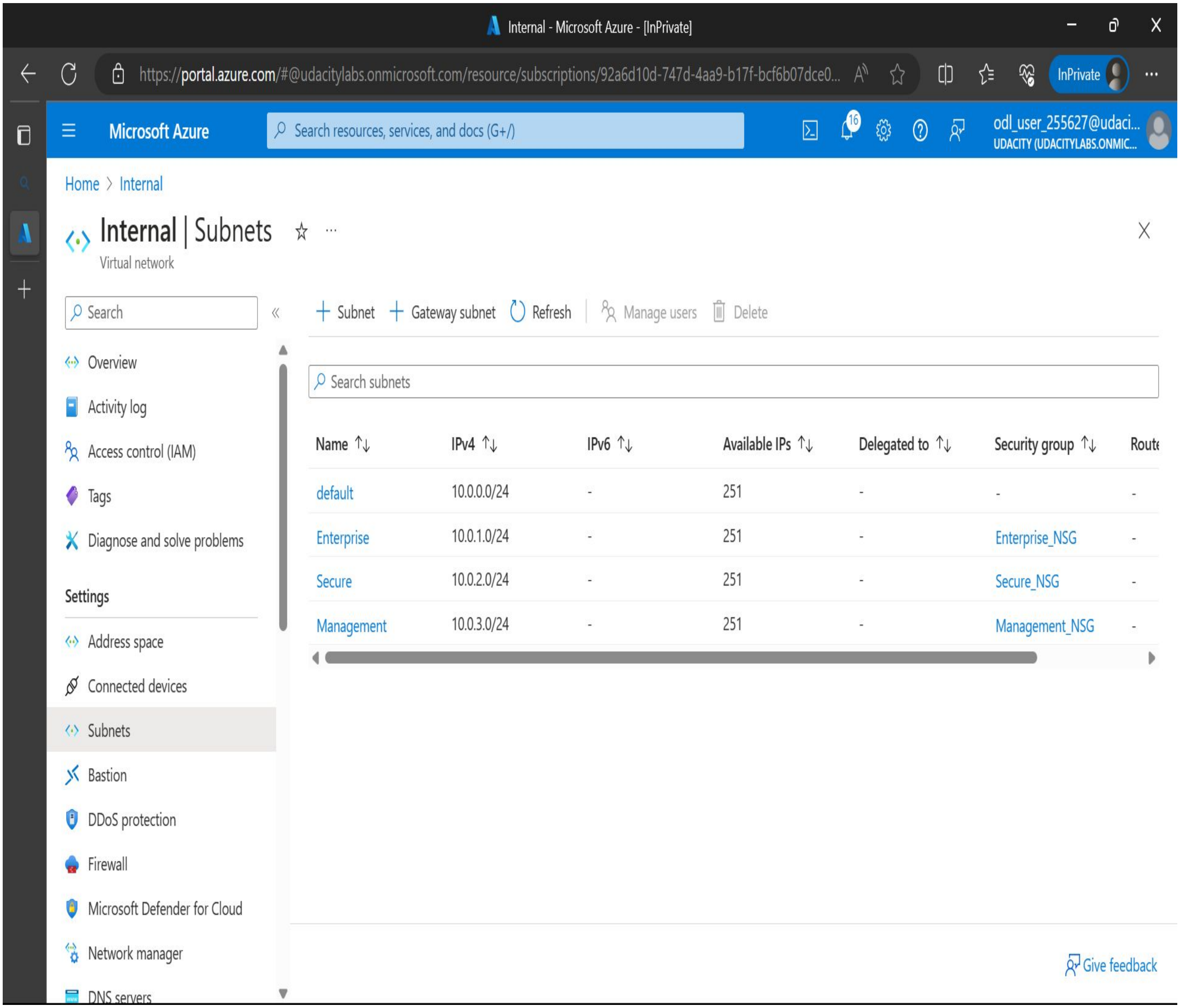
Create 2 subnets within your DMZ - subnets should be public and private.



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

2.1.3 Screenshot

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



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

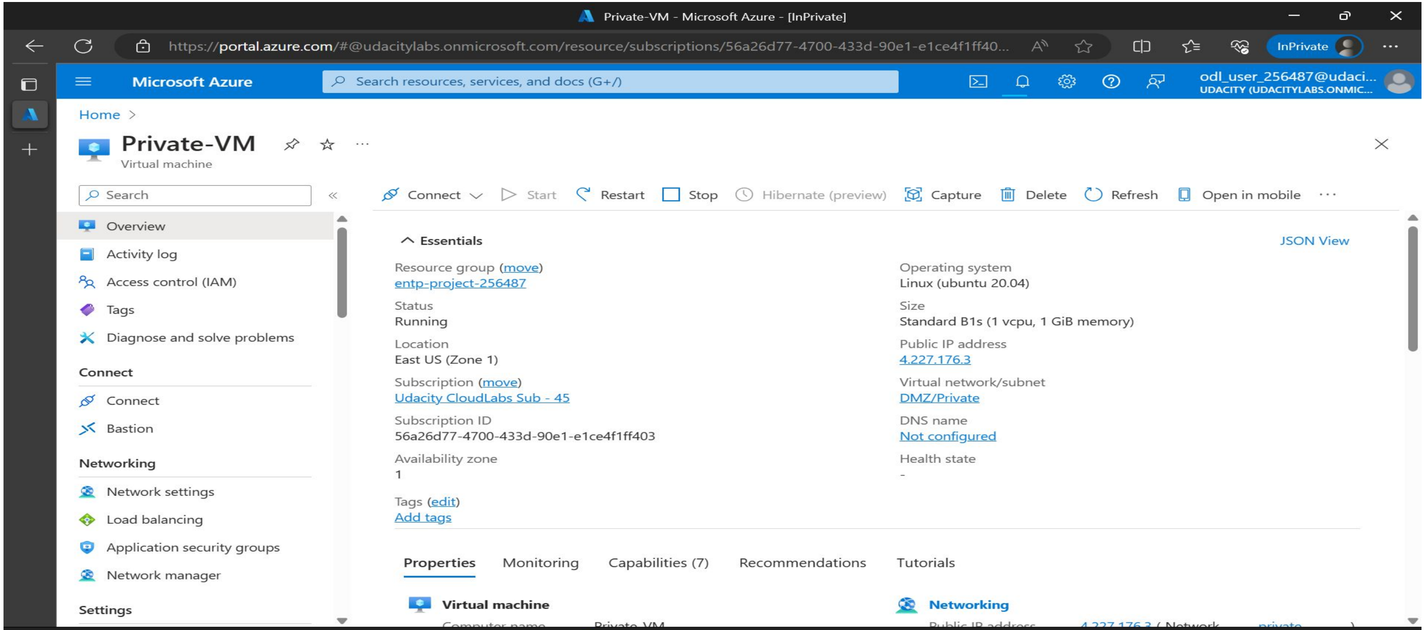
2.2 Creating Virtual Machines

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.



Private-VM - Microsoft Azure - [InPrivate]

https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/56a26d77-4700-433d-90e1-e1ce4f1ff40...

odl_user_256487@udaci...
UDACITY (UDACITYLABS.ONMIC...

Home >

Private-VM
Virtual machine

Resource group (move)
entp-project-256487

Status
Running

Location
East US (Zone 1)

Subscription (move)
Udacity CloudLabs Sub - 45

Subscription ID
56a26d77-4700-433d-90e1-e1ce4f1ff403

Availability zone
1

Tags (edit)
Add tags

Operating system
Linux (ubuntu 20.04)

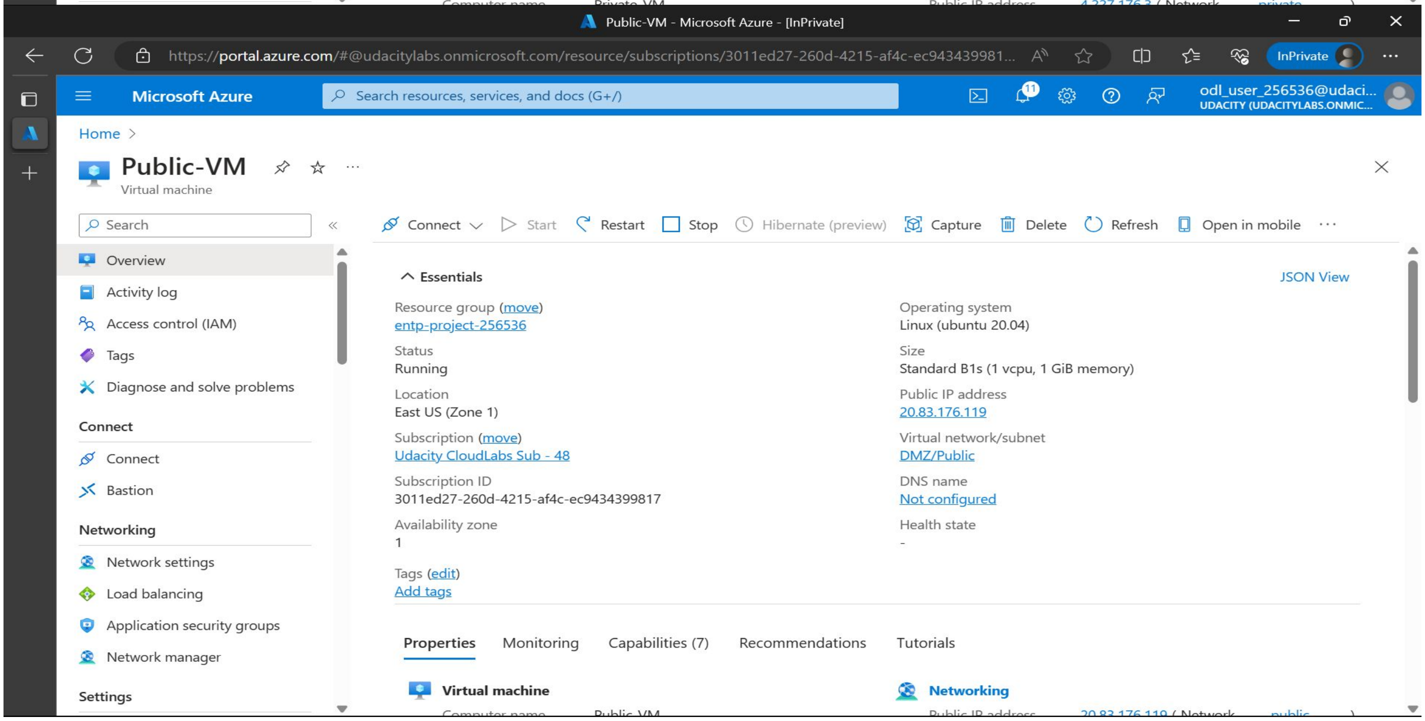
Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
4.227.176.3

Virtual network/subnet
DMZ/Private

DNS name
Not configured

Health state
-



Public-VM - Microsoft Azure - [InPrivate]

https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/3011ed27-260d-4215-af4c-ec943439981...

odl_user_256536@udaci...
UDACITY (UDACITYLABS.ONMIC...

Home >

Public-VM
Virtual machine

Resource group (move)
entp-project-256536

Status
Running

Location
East US (Zone 1)

Subscription (move)
Udacity CloudLabs Sub - 48

Subscription ID
3011ed27-260d-4215-af4c-ec9434399817

Availability zone
1

Tags (edit)
Add tags

Operating system
Linux (ubuntu 20.04)

Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
20.83.176.119

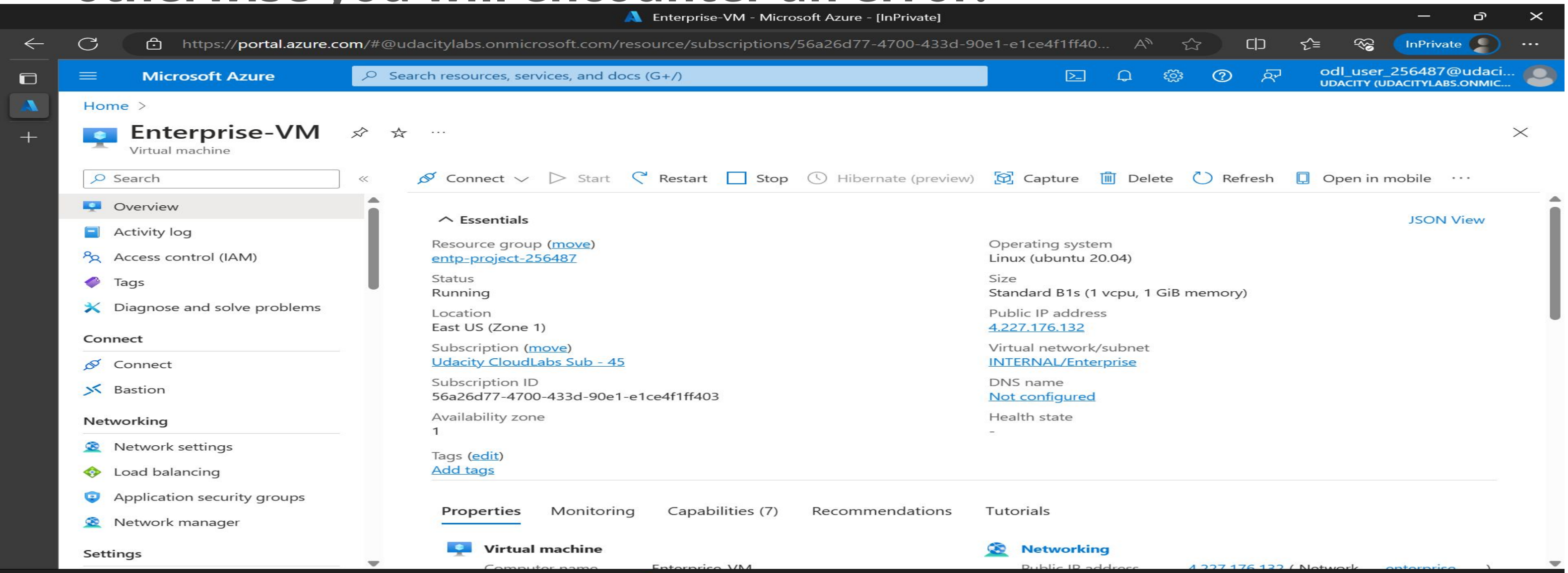
Virtual network/subnet
DMZ/Public

DNS name
Not configured

Health state
-

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.



Resource group (move)
entp-project-256487

Status
Running

Location
East US (Zone 1)

Subscription (move)
Udacity CloudLabs Sub - 45

Subscription ID
56a26d77-4700-433d-90e1-e1ce4f1ff403

Availability zone
1

Tags (edit)
Add tags

Operating system
Linux (ubuntu 20.04)

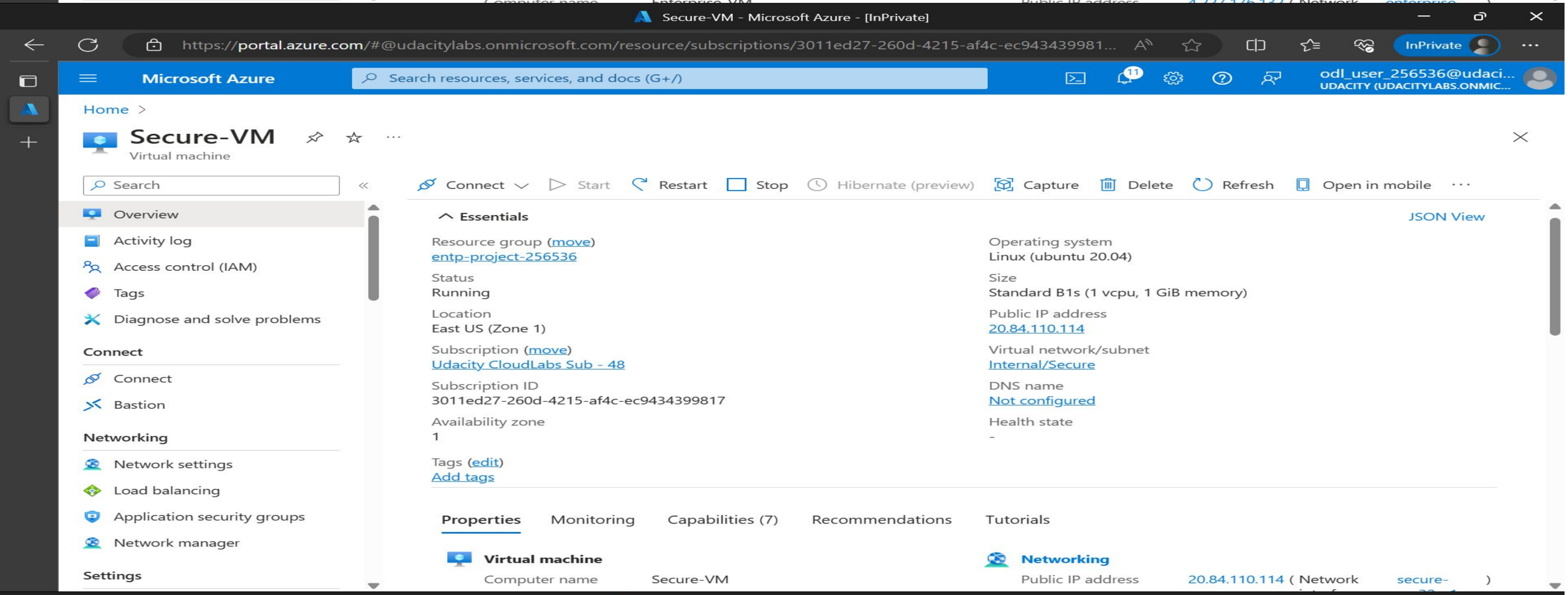
Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
4.227.176.132

Virtual network/subnet
INTERNAL/Enterprise

DNS name
Not configured

Health state
-



Resource group (move)
entp-project-256536

Status
Running

Location
East US (Zone 1)

Subscription (move)
Udacity CloudLabs Sub - 48

Subscription ID
3011ed27-260d-4215-af4c-ec9434399817

Availability zone
1

Tags (edit)
Add tags

Operating system
Linux (ubuntu 20.04)

Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
20.84.110.114

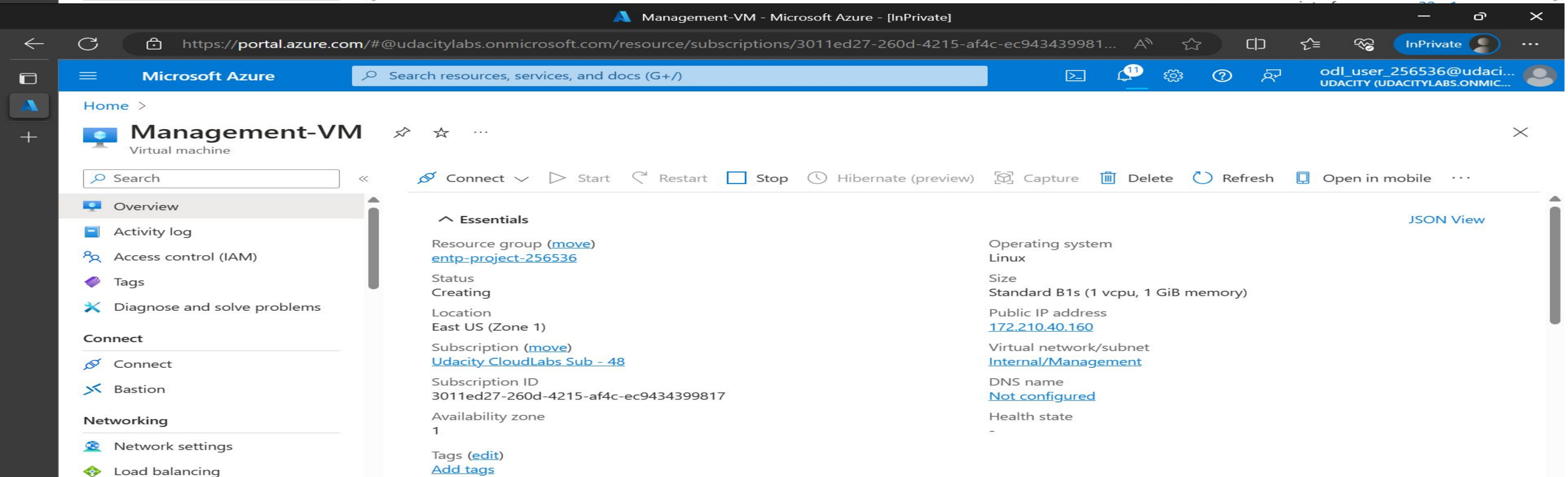
Virtual network/subnet
Internal/Secure

DNS name
Not configured

Health state
-

Computer name Secure-VM

Public IP address 20.84.110.114 (Network secure-)



Resource group (move)
entp-project-256536

Status
Creating

Location
East US (Zone 1)

Subscription (move)
Udacity CloudLabs Sub - 48

Subscription ID
3011ed27-260d-4215-af4c-ec9434399817

Availability zone
1

Tags (edit)
Add tags

Operating system
Linux

Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
172.210.40.160

Virtual network/subnet
Internal/Management

DNS name
Not configured

Health state
-

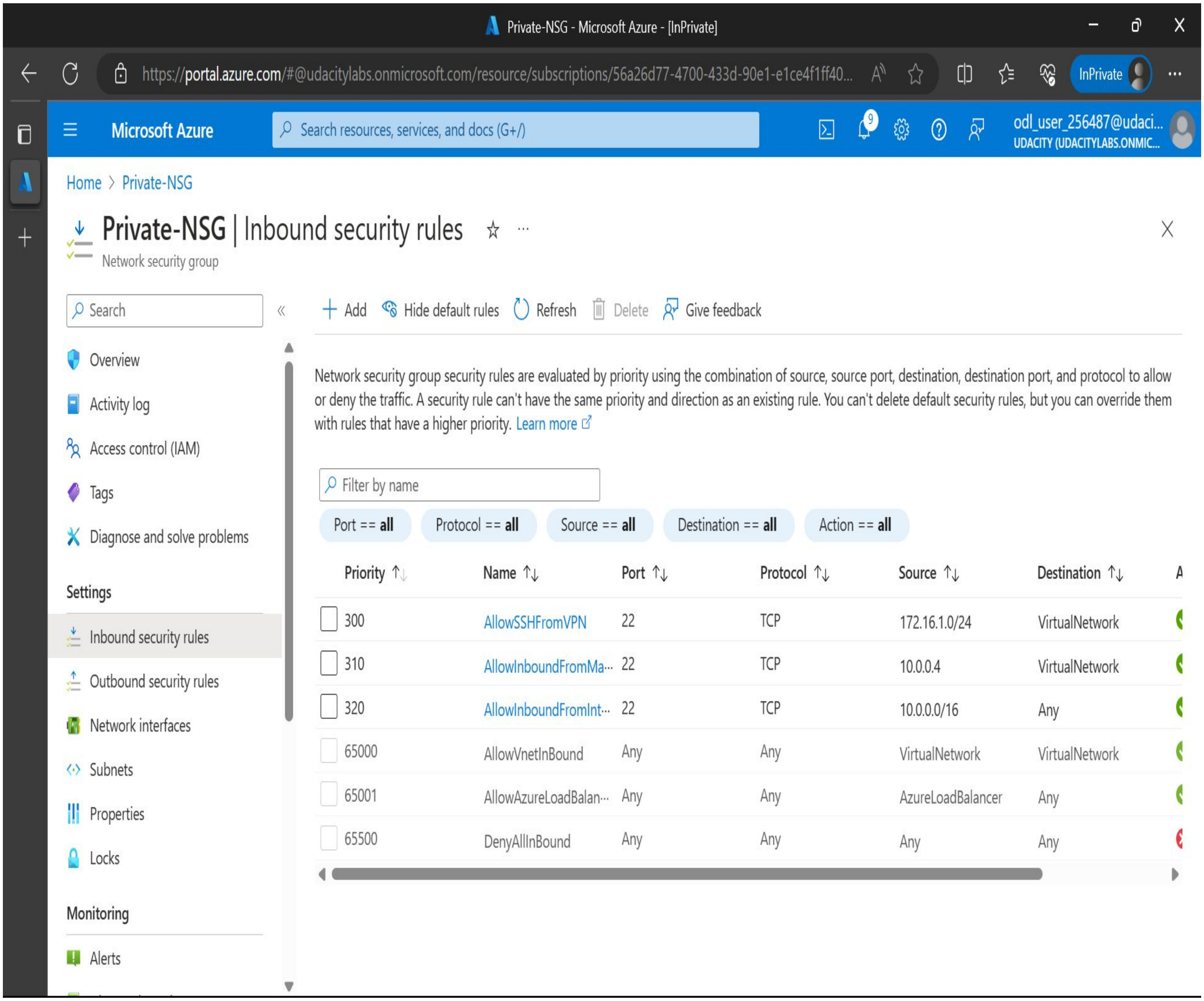
2.3 Secure Routing

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.

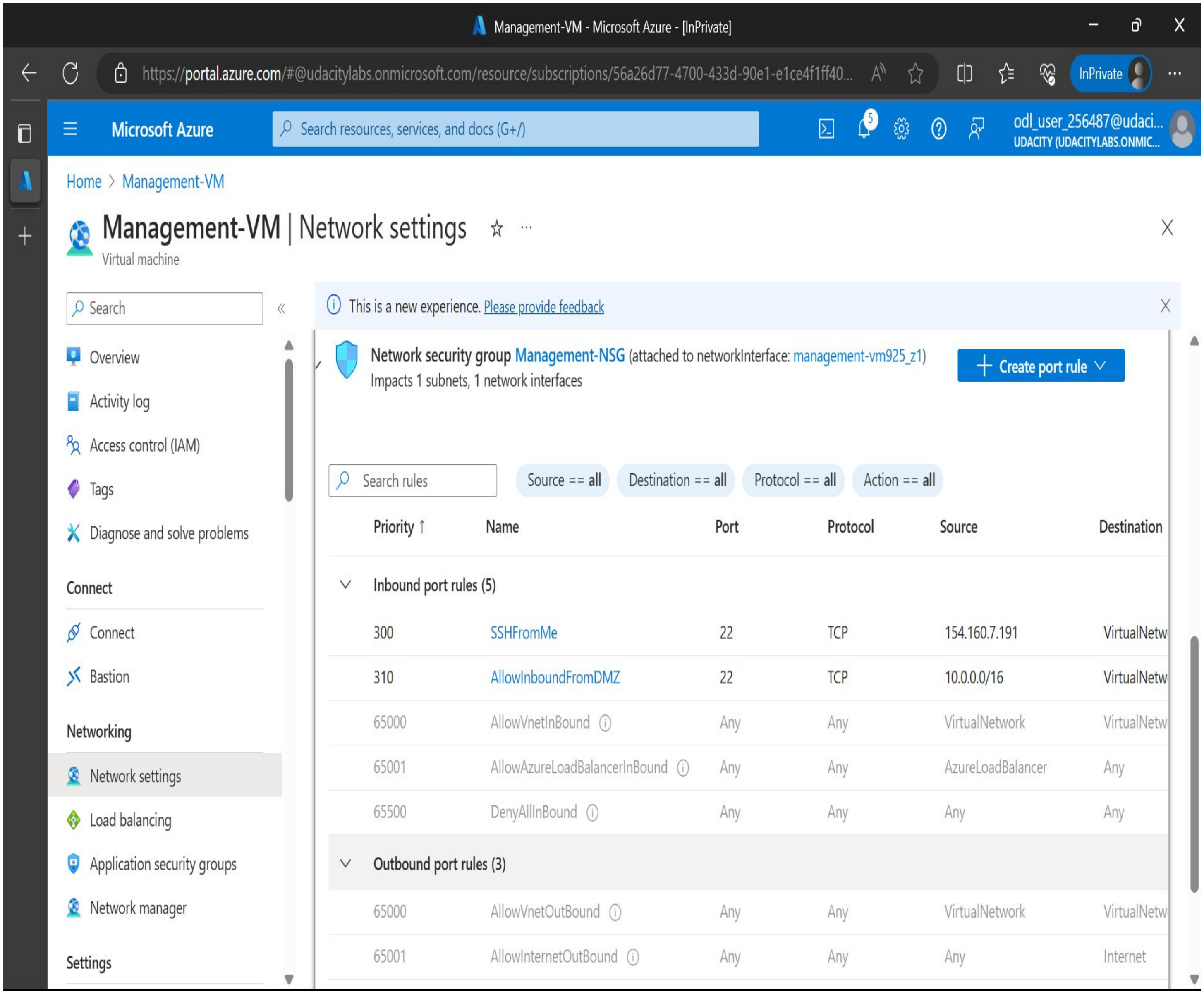


Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules,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

	Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	A
□	300	AllowSSHFromVPN	22	TCP	172.16.1.0/24	VirtualNetwork	✓
□	310	AllowInboundFromMa···	22	TCP	10.0.0.4	VirtualNetwork	✓
□	320	AllowInboundFromInt···	22	TCP	10.0.0.0/16	Any	✓
□	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓
□	65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer	Any	✓
□	65500	DenyAllInBound	Any	Any	Any	Any	✗

2.3.2 Screenshot

Traffic rules in your Internal network.



Management-VM - Microsoft Azure - [InPrivate]
https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/56a26d77-4700-433d-90e1-e1ce4f1ff40...
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
odl_user_256487@udaci...
UDACITY (UDACITYLABS.ONMIC...
Home > Management-VM
Management-VM | Network settings
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Connect
Bastion
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
+ Create port rule
Search rules
Source == all
Destination == all
Protocol == all
Action == all

This is a new experience. Please provide feedback

Network security group Management-NSG (attached to networkInterface: management-vm925_z1)
Impacts 1 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination
Inbound port rules (5)					
300	SSHFromMe	22	TCP	154.160.7.191	VirtualNetw
310	AllowInboundFromDMZ	22	TCP	10.0.0.0/16	VirtualNetw
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetw
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any
Outbound port rules (3)					
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetw
65001	AllowInternetOutBound	Any	Any	Any	Internet

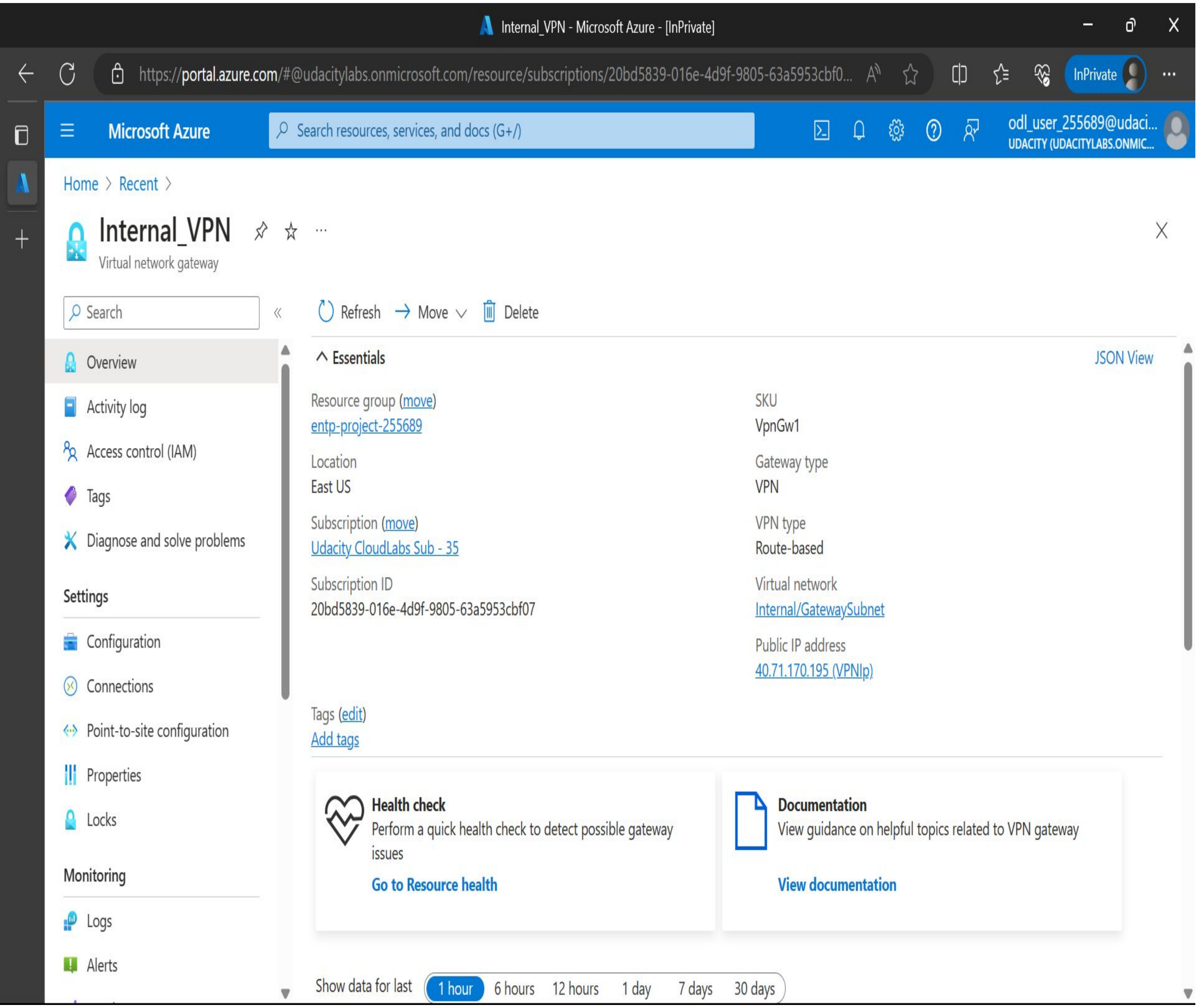
2.4 VPN Access

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.



Internal_VPN - Microsoft Azure - [InPrivate]
https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/20bd5839-016e-4d9f-9805-63a5953cbf0...
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
odl_user_255689@udaci...
UDACITY (UDACITYLABS.ONMIC...
Home > Recent >
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Connections
Point-to-site configuration
Properties
Locks
Monitoring
Logs
Alerts
Refresh
Move
Delete
Essentials
JSON View

Internal_VPN

Virtual network gateway

Resource group (move) entp-project-255689	SKU VpnGw1
Location East US	Gateway type VPN
Subscription (move) Udacity CloudLabs Sub - 35	VPN type Route-based
Subscription ID 20bd5839-016e-4d9f-9805-63a5953cbf07	Virtual network Internal/GatewaySubnet
	Public IP address 40.71.170.195 (VPNIp)

Tags (edit)
Add tags

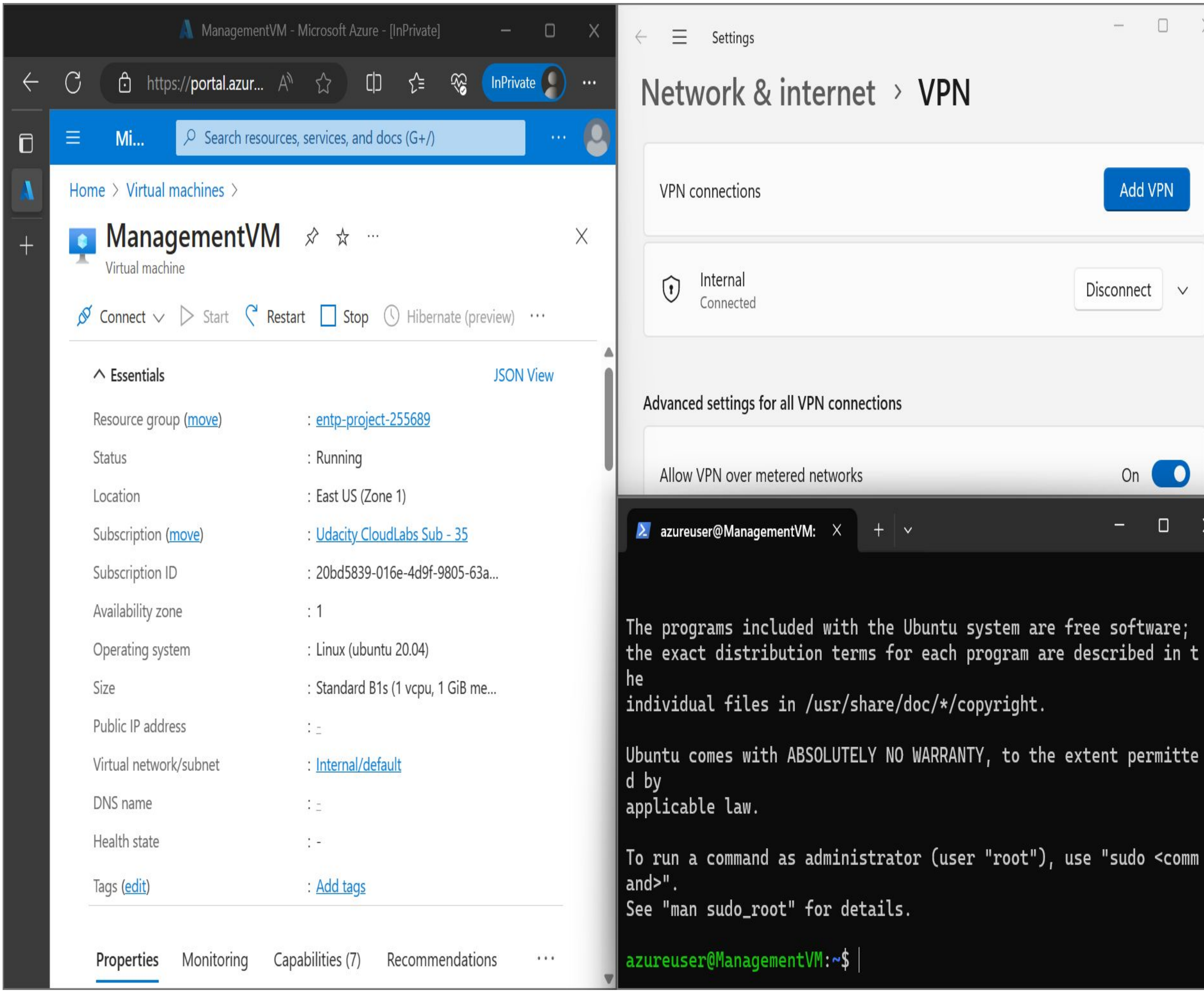
Health check
Perform a quick health check to detect possible gateway issues
Go to Resource health

Documentation
View guidance on helpful topics related to VPN gateway
View documentation

Show data for last 1 hour 6 hours 12 hours 1 day 7 days 30 days

2.4.2 Screenshot

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



Resource group (move) : entp-project-255689
Status : Running
Location : East US (Zone 1)
Subscription (move) : Udacity CloudLabs Sub - 35
Subscription ID : 20bd5839-016e-4d9f-9805-63a...
Availability zone : 1
Operating system : Linux (ubuntu 20.04)
Size : Standard B1s (1 vcpu, 1 GiB me...
Public IP address : -
Virtual network/subnet : Internal/default
DNS name : -
Health state : -
Tags (edit) : Add tags

Network & internet › VPN

VPN connections

Internal
Connected

Advanced settings for all VPN connections

Allow VPN over metered networks On

azureuser@ManagementVM:

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in t
he
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitte
d by
applicable law.

To run a command as administrator (user "root"), use "sudo <comm
and>".
See "man sudo_root" for details.

azureuser@ManagementVM:~$
```

Section 3

Continuous Monitoring with a SIEM

Section 3: Build the SIEM

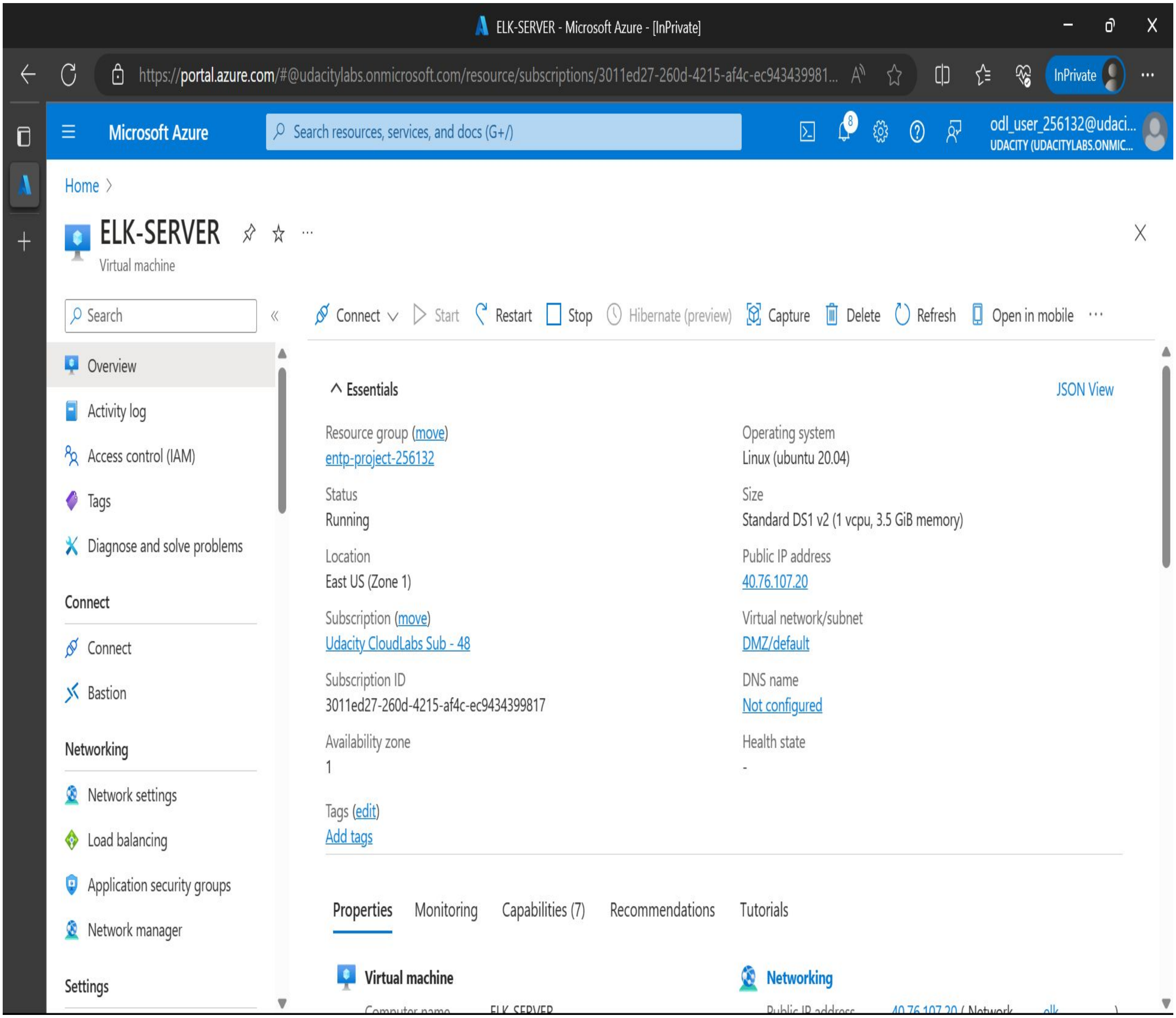
Now that you've built a secure network architecture and a Zero Trust model, you're ready to wrap up your contract and finish the last piece of work. Your last task is to set up a solution to monitor the enterprise network and alert you about potential attacks.

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.



ELK-SERVER - Microsoft Azure - [InPrivate]

https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/3011ed27-260d-4215-af4c-ec943439981...

odl_user_256132@udaci...
UDACITY (UDACITYLABS.ONMIC...

Home >

ELK-SERVER
Virtual machine

Essentials

Resource group (move)
entp-project-256132

Status
Running

Location
East US (Zone 1)

Subscription (move)
Udacity CloudLabs Sub - 48

Subscription ID
3011ed27-260d-4215-af4c-ec9434399817

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
40.76.107.20

Virtual network/subnet
DMZ/default

DNS name
Not configured

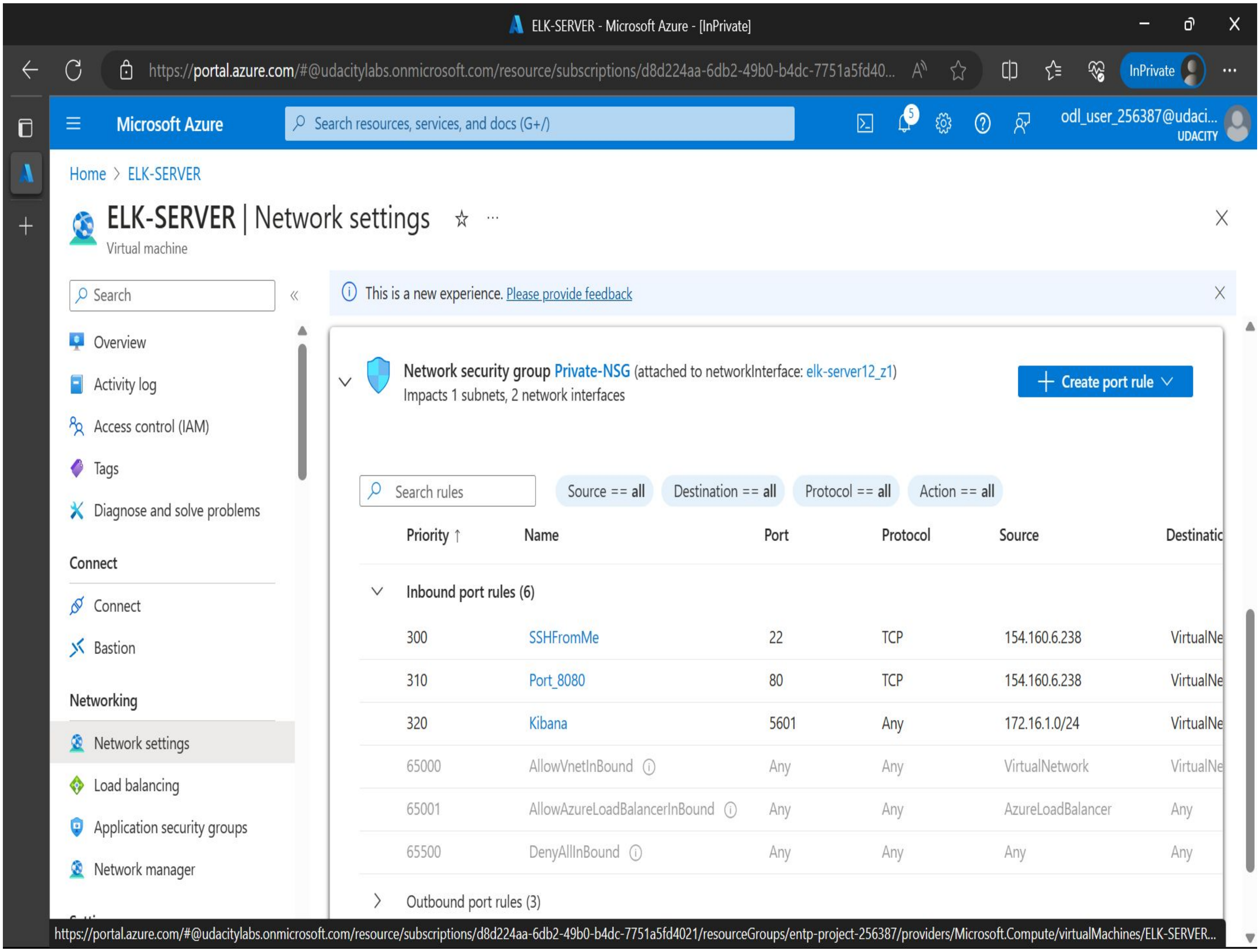
Health state
-

Virtual machine
Computer name ELK-SERVER

Networking
Public IP address 40.76.107.20 (Network ... elk...)

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.



ELK-SERVER - Microsoft Azure - [InPrivate]
https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/d8d224aa-6db2-49b0-b4dc-7751a5fd40...
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
odl_user_256387@udaci...
UDACITY
Home > ELK-SERVER
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Connect
Bastion
Networking
Network settings
Load balancing
Application security groups
Network manager
This is a new experience. Please provide feedback
Create port rule
Search rules
Source == all
Destination == all
Protocol == all
Action == all

ELK-SERVER | Network settings

Virtual machine

Network security group Private-NSG (attached to networkInterface: elk-server12_z1)

Impacts 1 subnets, 2 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destinatic
Inbound port rules (6)					
300	SSHFromMe	22	TCP	154.160.6.238	VirtualNe
310	Port_8080	80	TCP	154.160.6.238	VirtualNe
320	Kibana	5601	Any	172.16.1.0/24	VirtualNe
65000	AllowVnetInBound ⓘ	Any	Any	VirtualNetwork	VirtualNe
65001	AllowAzureLoadBalancerInBound ⓘ	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound ⓘ	Any	Any	Any	Any
Outbound port rules (3)					

https://portal.azure.com/#@udacitylabs.onmicrosoft.com/resource/subscriptions/d8d224aa-6db2-49b0-b4dc-7751a5fd4021/resourceGroups/entp-project-256387/providers/Microsoft.Compute/virtualMachines/ELK-SERVER...

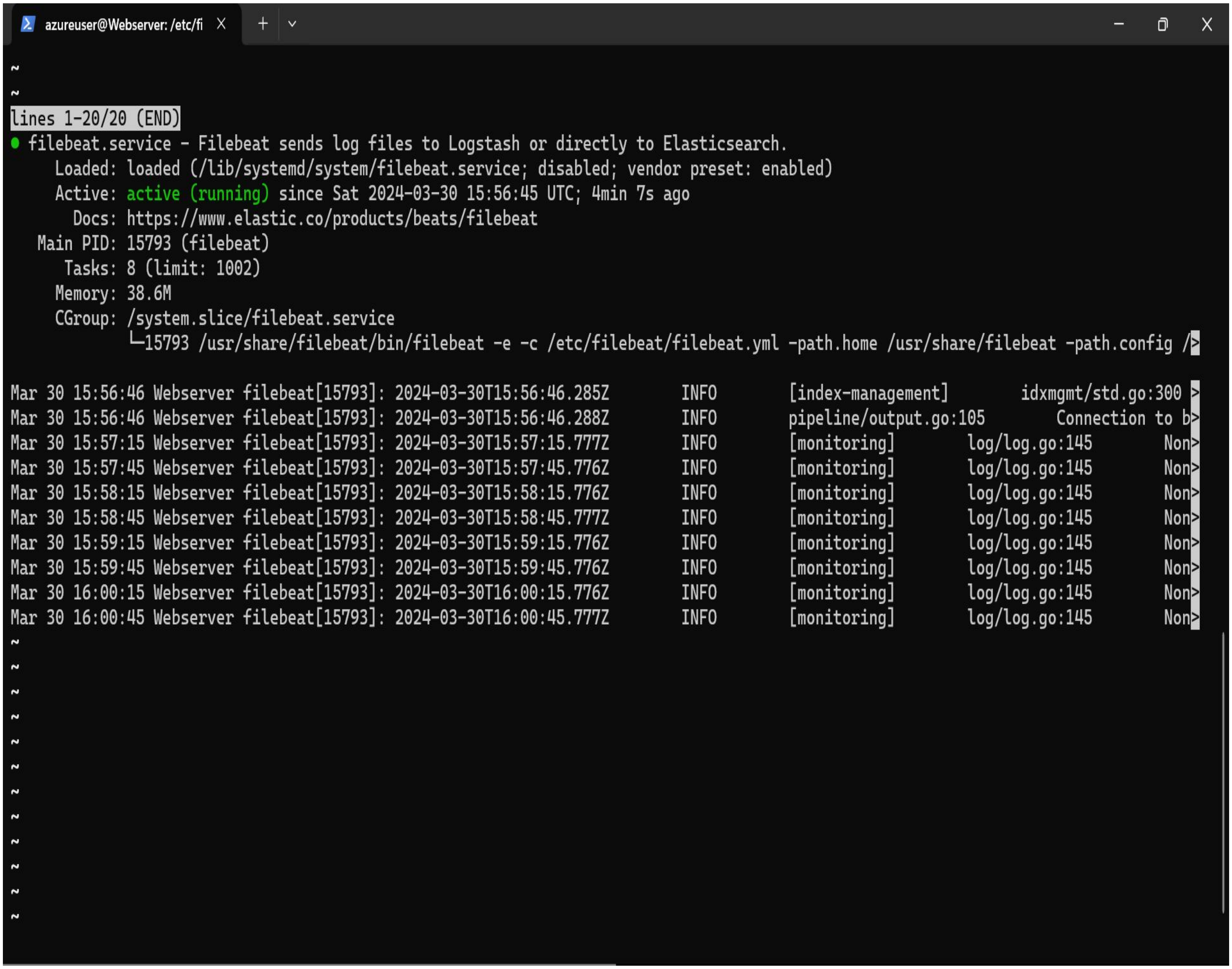
3.2 Ingest Logs

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

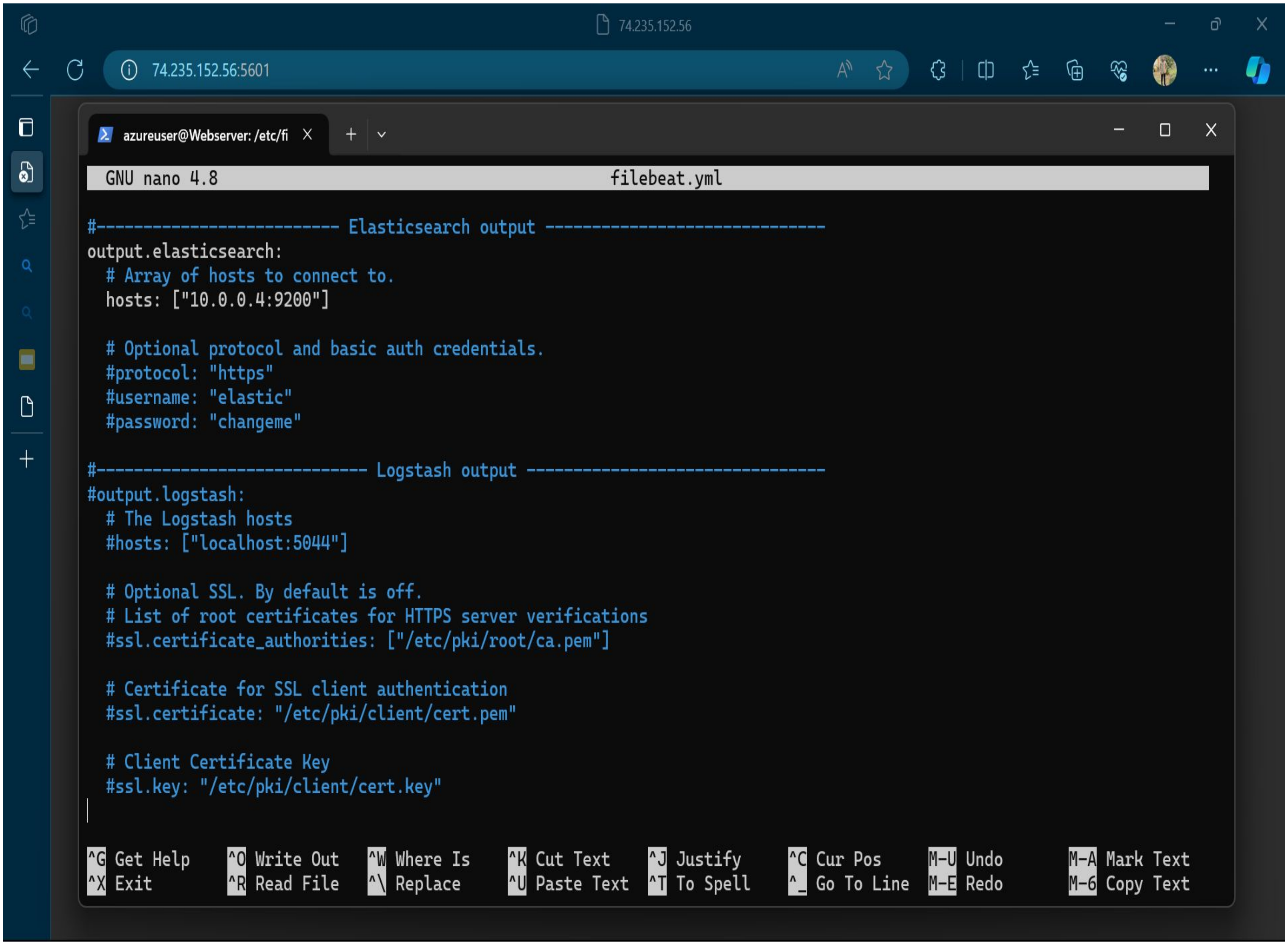
Install Filebeat on your web servers and show the Filebeat service as active.



```
~
~
lines 1-20/20 (END)
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
     Loaded: loaded (/lib/systemd/system/filebeat.service; disabled; vendor preset: enabled)
     Active: active (running) since Sat 2024-03-30 15:56:45 UTC; 4min 7s ago
       Docs: https://www.elastic.co/products/beats/filebeat
   Main PID: 15793 (filebeat)
      Tasks: 8 (limit: 1002)
     Memory: 38.6M
     CGroup: /system.slice/filebeat.service
             └─15793 /usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml -path.home /usr/share/filebeat -path.config />

Mar 30 15:56:46 Webserver filebeat[15793]: 2024-03-30T15:56:46.285Z       INFO       [index-management]       idxmgmt/std.go:300 >
Mar 30 15:56:46 Webserver filebeat[15793]: 2024-03-30T15:56:46.288Z       INFO       pipeline/output.go:105       Connection to b>
Mar 30 15:57:15 Webserver filebeat[15793]: 2024-03-30T15:57:15.777Z       INFO       [monitoring]       log/log.go:145       Non>
Mar 30 15:57:45 Webserver filebeat[15793]: 2024-03-30T15:57:45.776Z       INFO       [monitoring]       log/log.go:145       Non>
Mar 30 15:58:15 Webserver filebeat[15793]: 2024-03-30T15:58:15.776Z       INFO       [monitoring]       log/log.go:145       Non>
Mar 30 15:58:45 Webserver filebeat[15793]: 2024-03-30T15:58:45.777Z       INFO       [monitoring]       log/log.go:145       Non>
Mar 30 15:59:15 Webserver filebeat[15793]: 2024-03-30T15:59:15.776Z       INFO       [monitoring]       log/log.go:145       Non>
Mar 30 15:59:45 Webserver filebeat[15793]: 2024-03-30T15:59:45.776Z       INFO       [monitoring]       log/log.go:145       Non>
Mar 30 16:00:15 Webserver filebeat[15793]: 2024-03-30T16:00:15.776Z       INFO       [monitoring]       log/log.go:145       Non>
Mar 30 16:00:45 Webserver filebeat[15793]: 2024-03-30T16:00:45.777Z       INFO       [monitoring]       log/log.go:145       Non>
~
~
~
~
~
~
~
~
~
~
~
~
```

3.2.2 Screenshot

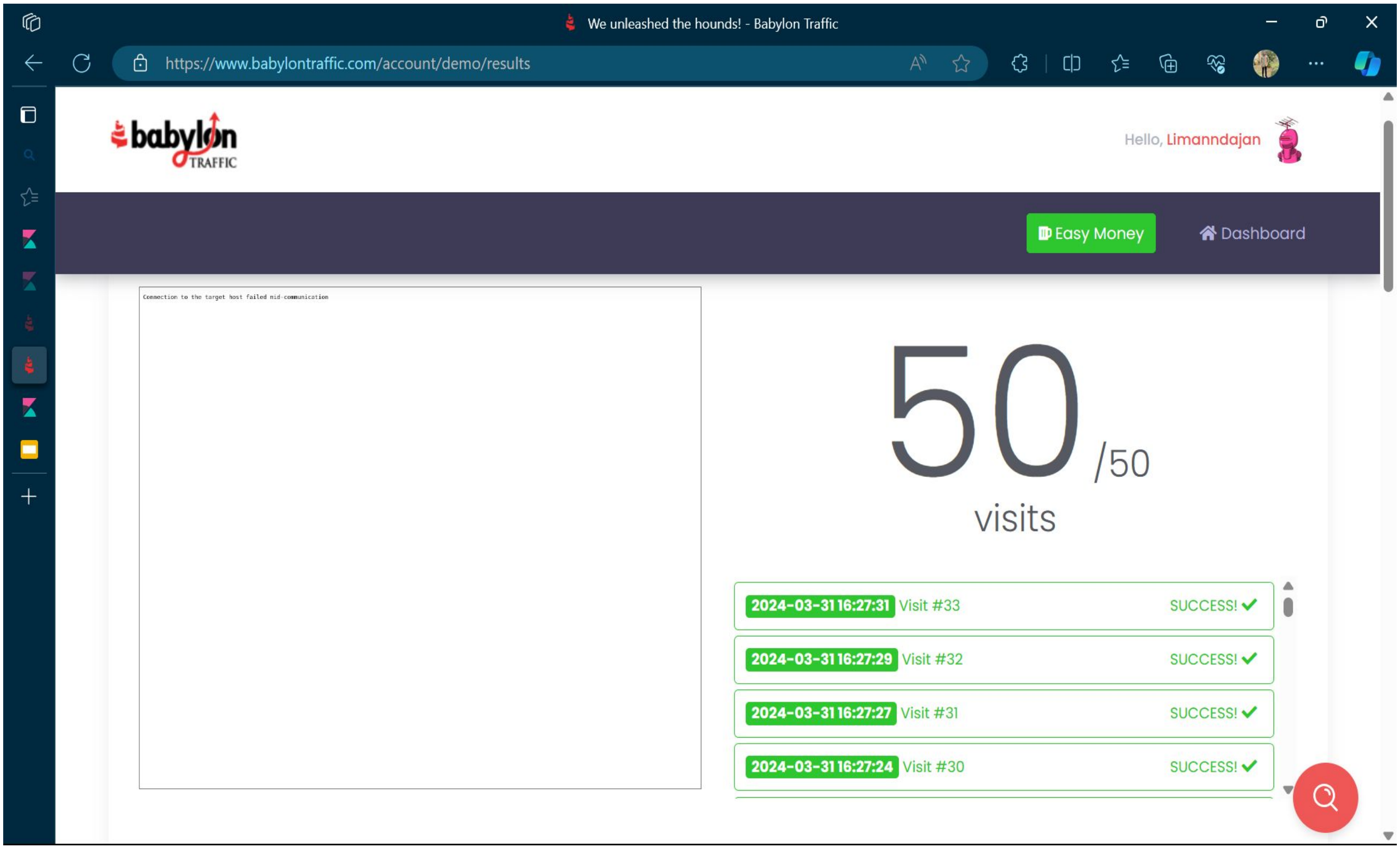
Configure Filebeat to route web server logs to Elasticsearch.



```
 GNU nano 4.8                                      filebeat.yml

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.0.0.4:9200"]

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

#----------------------------- Logstash output --------------------------------
#output.logstash:
  # The Logstash hosts
  #hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text   ^J Justify   ^C Cur Pos    M-U Undo   M-A Mark Text
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo   M-6 Copy Text
```

3.2.3 Screenshot

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



We unleashed the hounds! - Babylon Traffic

https://www.babylontraffic.com/account/demo/results

Hello, Limanndajan

```
Connection to the target host failed mid-communication
```

50 /50 visits

2024-03-31 16:27:31 Visit #33 SUCCESS! ✓

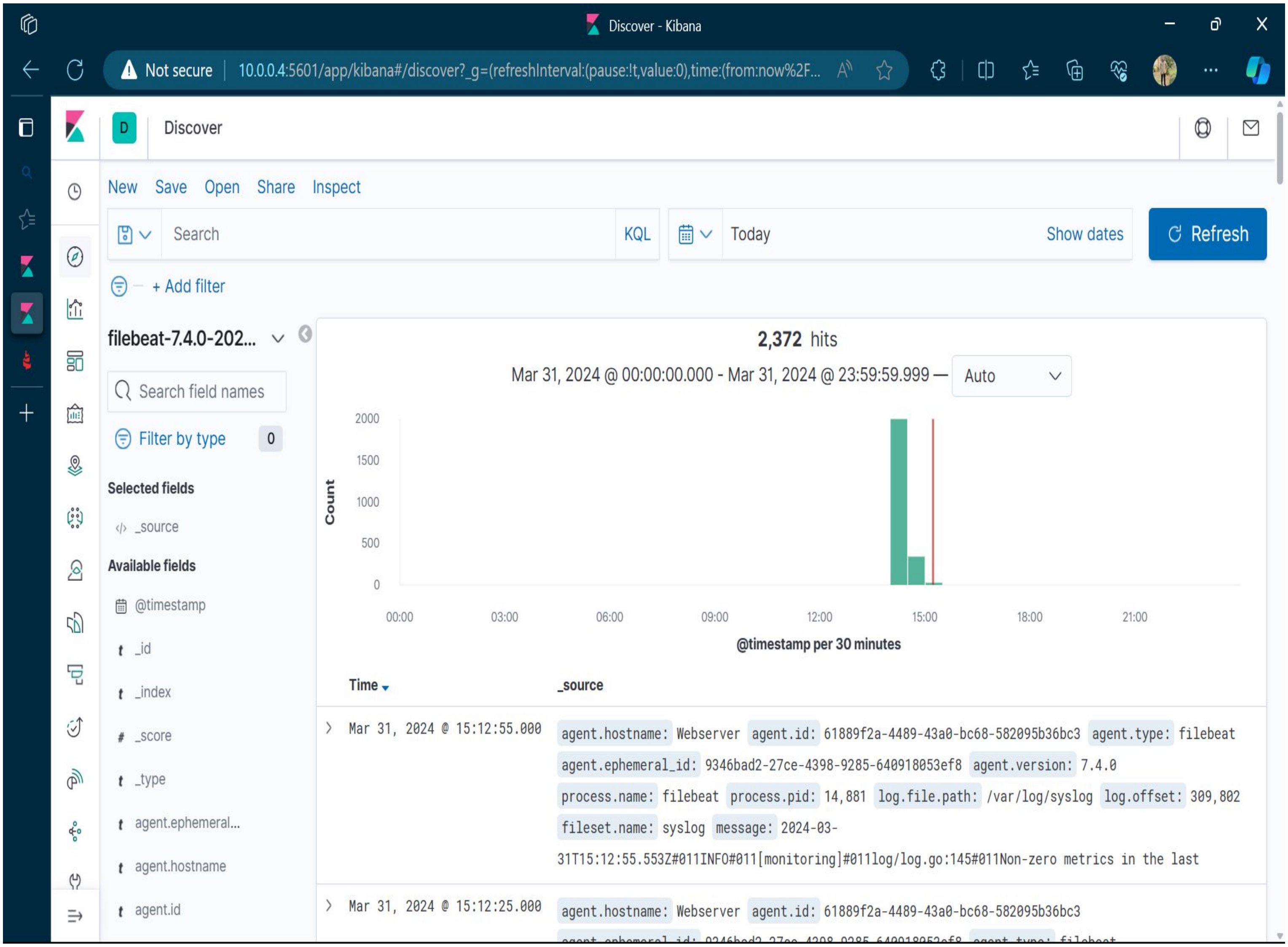
2024-03-31 16:27:29 Visit #32 SUCCESS! ✓

2024-03-31 16:27:27 Visit #31 SUCCESS! ✓

2024-03-31 16:27:24 Visit #30 SUCCESS! ✓

3.2.4 Screenshot

Web server logs appear in Kibana.



```
> Mar 31, 2024 @ 15:12:55.000   agent.hostname: Webserver agent.id: 61889f2a-4489-43a0-bc68-582095b36bc3 agent.type: filebeat
                                agent.ephemeral_id: 9346bad2-27ce-4398-9285-640918053ef8 agent.version: 7.4.0
                                process.name: filebeat process.pid: 14,881 log.file.path: /var/log/syslog log.offset: 309,802
                                fileset.name: syslog message: 2024-03-
                                31T15:12:55.553Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last
> Mar 31, 2024 @ 15:12:25.000   agent.hostname: Webserver agent.id: 61889f2a-4489-43a0-bc68-582095b36bc3
                                agent.ephemeral_id: 9346bad2-27ce-4398-9285-640918053ef8 agent.type: filebeat
```

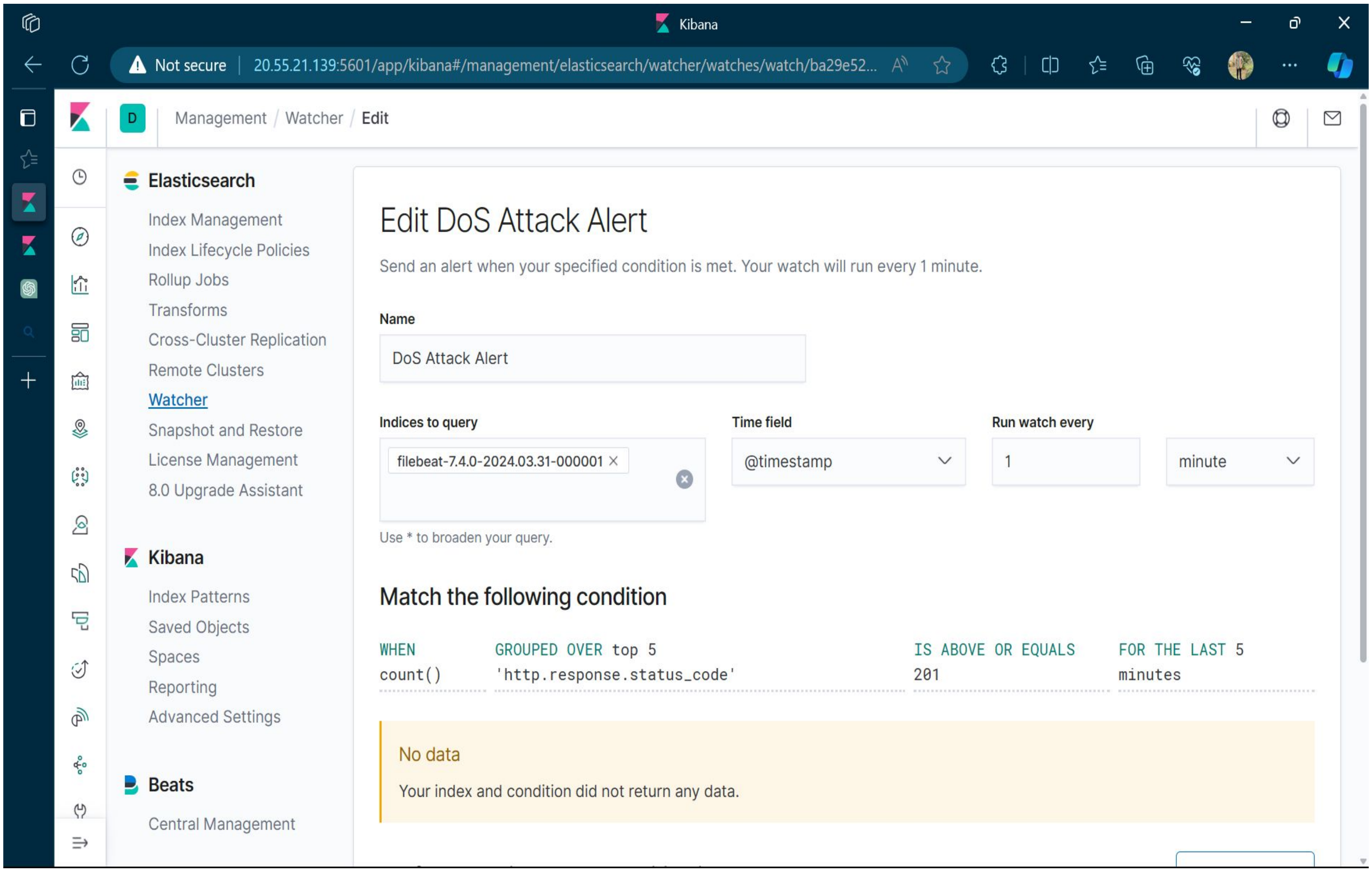
3.3 Build Alerts

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.



Edit DoS Attack Alert

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

Name: DoS Attack Alert

Indices to query: filebeat-7.4.0-2024.03.31-000001

Use * to broaden your query.

Time field: @timestamp

Run watch every: 1 minute

Match the following condition

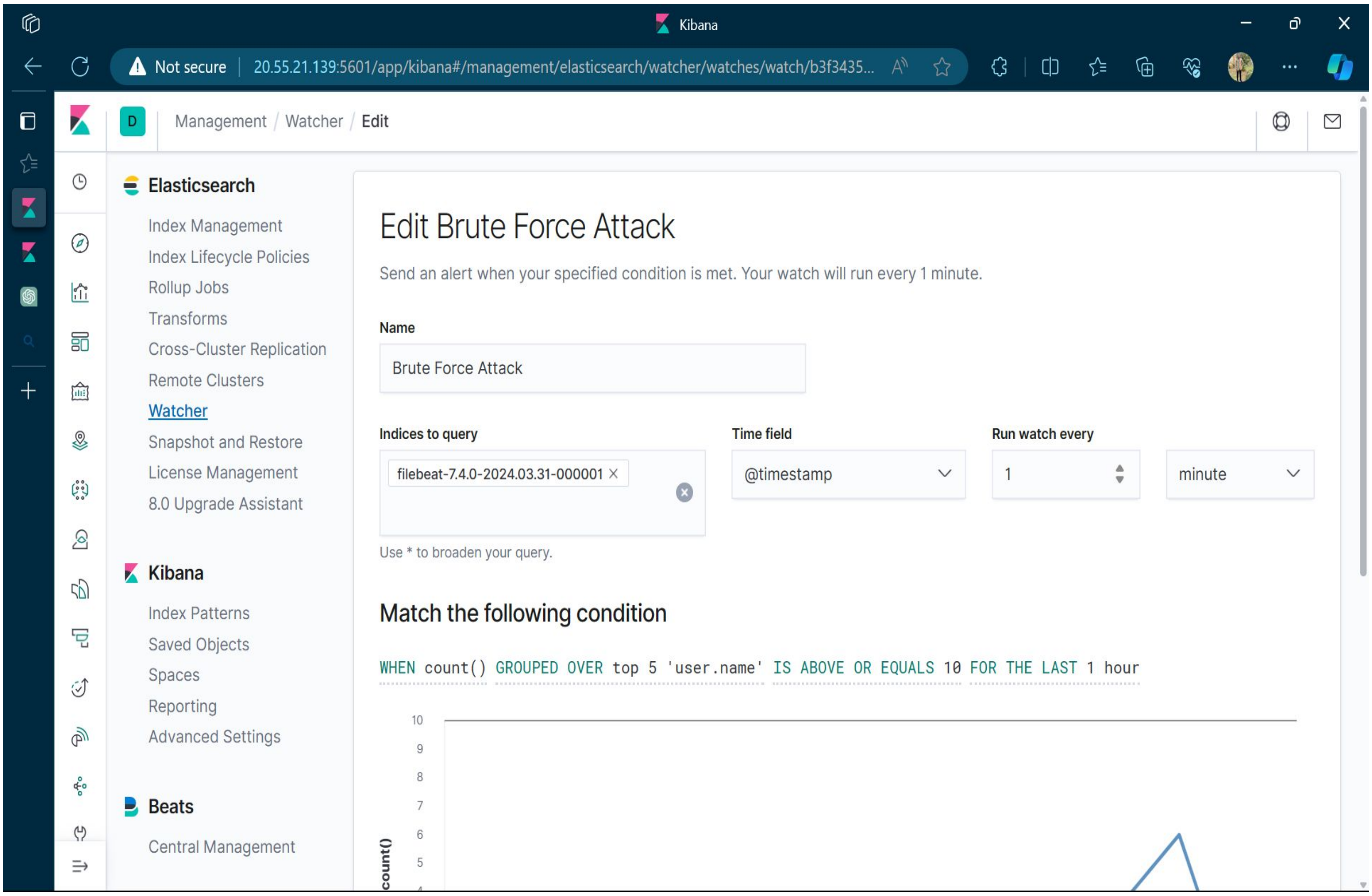
```
WHEN     GROUPED OVER top 5                  IS ABOVE OR EQUALS   FOR THE LAST 5
count()  'http.response.status_code'         201                  minutes
```

No data

Your index and condition did not return any data.

3.3.2 Screenshot

Create an alert for Brute Force attack.



Edit Brute Force Attack

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

Name: Brute Force Attack

Indices to query: filebeat-7.4.0-2024.03.31-000001

Use * to broaden your query.

Time field: @timestamp

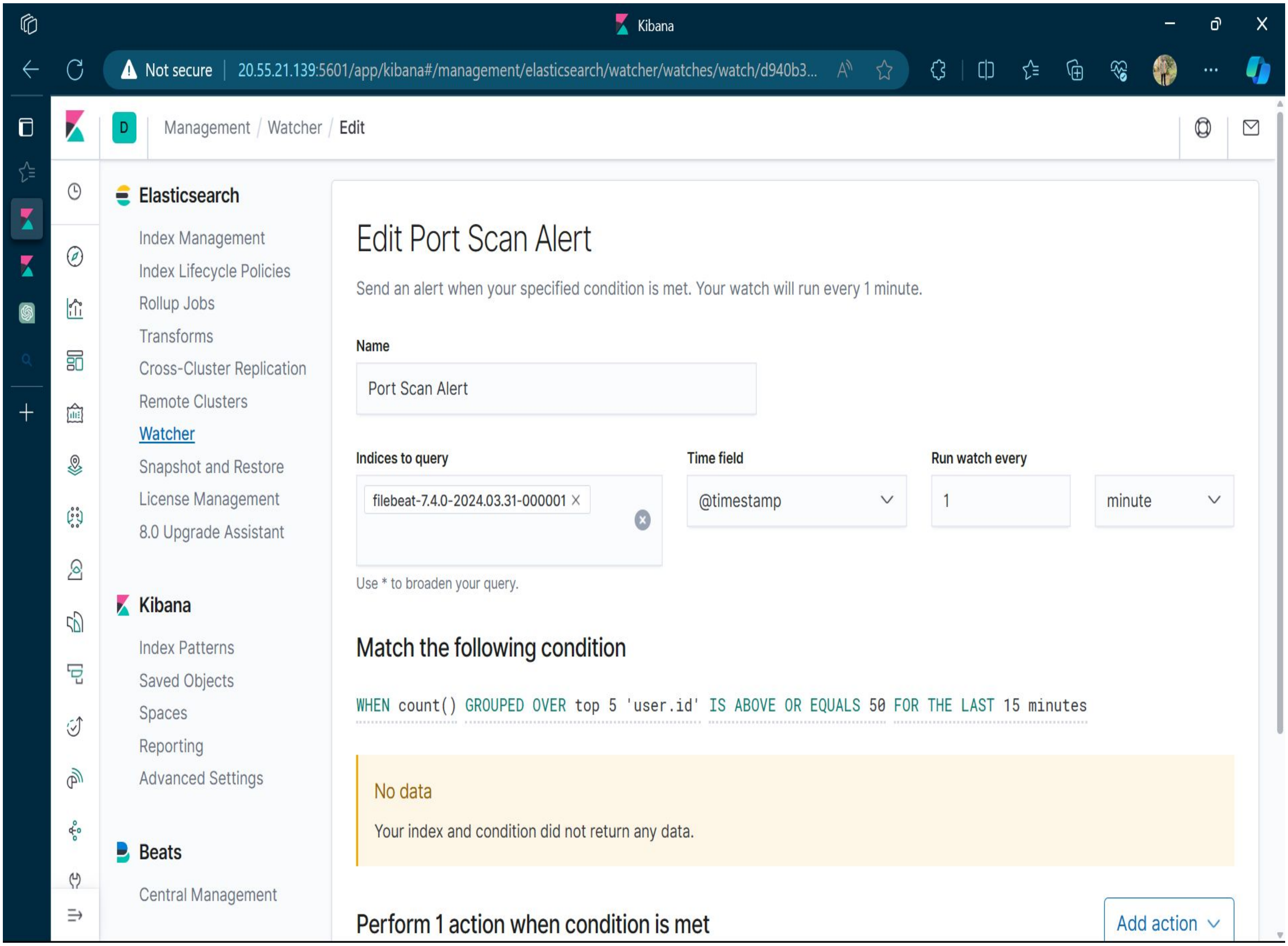
Run watch every: 1 minute

Match the following condition

```
WHEN count() GROUPED OVER top 5 'user.name' IS ABOVE OR EQUALS 10 FOR THE LAST 1 hour
```

3.3.3 Screenshot

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



Edit Port Scan Alert

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

Name: Port Scan Alert

Indices to query: filebeat-7.4.0-2024.03.31-000001

Use * to broaden your query.

Time field: @timestamp

Run watch every: 1 minute

Match the following condition

```
WHEN count() GROUPED OVER top 5 'user.id' IS ABOVE OR EQUALS 50 FOR THE LAST 15 minutes
```

No data

Your index and condition did not return any data.

Perform 1 action when condition is met

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.

DOS INCIDENT RESPONSE PLAYBOOK

PHASE 1: PREPARATION

To mitigate possible DoS attacks, identify important systems, services, and assets, establish mitigation measures including rate limiting, access restrictions, and traffic filtering, perform frequent staff training sessions on DoS attack indicators and actions, and stress reporting odd network activity. Implement network monitoring tools to identify aberrant traffic patterns and build alerting systems to inform the incident response team when a suspected DoS attack is discovered.

PHASE 2: DETECTION AND ANALYSIS

The incident response team conducts an investigation upon receiving warnings of unusual network behaviour, reviewing network traffic logs, server performance indicators, and other telemetry data to validate the existence of a DoS assault. They then detect the sort of DoS attack and identify the attack vectors employed.

PHASE 3: CONTAINMENT, ERADICATION, AND RECOVERY

To prevent assaults, install traffic filtering rules or DDoS mitigation services, reroute harmful traffic at the network perimeter, prioritize service restoration, and deploy extra resources or failover methods. Communicate with internal stakeholders, such as staff and system users, to advise them of the continuing assault and offer direction on essential steps.

PHASE 4: POST INCIDENT ACTIVITY

A detailed study of a DoS attack is important to discover the underlying cause and exploited vulnerabilities. Lessons learnt and ideas for strengthening network resilience are provided. Incident response duties may be automated to expedite response times. Continuous improvement entails integrating post-incident analysis results into security awareness training and processes, and upgrading the DoS attack playbook and response measures based on new threats and developing attack methodologies.

3.4 Incident Response Playbook

BRUTE FORCE ATTACK INCIDENT RESPONSE PLAYBOOK

PHASE 1: PREPARATION

In order to safeguard against brute force assaults, it is necessary to identify systems and services that are susceptible to such attacks. Once identified, mitigating measures such as implementing account lockout rules and enforcing strong password requirements should be put in place. Regular security awareness training courses provide staff with education on the vulnerabilities associated with weak passwords and emphasise the need of adopting strong and complicated credentials. Notify immediately about any login attempts that seem suspicious. Deploy intrusion detection and prevention systems (IDS/IPS) or log monitoring solutions to identify and notify about recurring unsuccessful login attempts. Set up logging tools to record pertinent details such as the originating IP addresses, timestamps of login attempts, and the specific accounts that are being targeted.

PHASE 2: DETECTION AND ANALYSIS

Upon receiving indications of unusual login behaviour, the incident response team commences an investigation. They examine logs and network data to verify the presence of a brute force assault, detecting recurring instances of failed login attempts from certain IP addresses or accounts. The attack vector is identified, such as focusing on remote login services or web application login forms. The level of complexity and magnitude of the assault are evaluated in order to determine the priority of response actions.

PHASE 3: CONTAINMENT, ERADICATION, AND RECOVERY

Account lockout and access limits are enforced to prevent additional unwanted access attempts. Password reset and credentials management are suggested to safeguard accounts against further intrusion. Service restoration is monitored to ensure important services stay operating.

PHASE 4: POST INCIDENT ACTIVITY

A detailed study of the brute force assault is undertaken to discover vulnerabilities exploited by the attacker and record lessons gained. Incident response automation is considered to expedite response activities and decrease manual interaction. Continuous improvement is included into ongoing security awareness training and password management rules, and the brute force attack playbook and response measures are frequently evaluated and modified depending on new threats and developing attack methodologies.

3.4 Incident Response Playbook

SCANNING ATTACK INCIDENT RESPONSE PLAYBOOK

PHASE 1: PREPARATION

Risk assessment and mitigation steps, such as identifying essential systems and services susceptible to scanning attacks, installing network segmentation and access rules, and deploying intrusion detection and prevention systems (IDS/IPS) or network monitoring tools.

PHASE 2: DETECTION AND ANALYSIS

The incident response team begins an investigation upon receiving notifications of suspected scanning behaviour. They evaluate network traffic logs and packet captures to corroborate the attack, discover patterns of port scans, and establish the attacker's scanning strategies. They examine the extent and size of the scanning activity to identify its possible effect on network security and operational continuity.

PHASE 3: CONTAINMENT, ERADICATION, AND RECOVERY

To prevent unauthorized access or lateral movement by attackers, network parts should be segregated from the rest of the network. Traffic filtering should be installed to control incoming and outgoing traffic. Vulnerability repair should be prioritized and done to increase network security. In event of an incident, cooperation with network administrators, system owners, and stakeholders is vital. Internal teams and external partners should be alerted to share threat information and coordinate response activities.

PHASE 4: POST INCIDENT ACTIVITY

Doing a detailed investigation of the scanning assault to discover vulnerabilities used by the attacker, recording lessons learned, and suggesting changes for network security controls and threat detection capabilities. Incident response automation may be assessed to boost efficiency, and continual improvement can be done by integrating results from the post-incident study into ongoing security awareness training and network hardening activities. Regularly assessing and upgrading the scanning attack playbook and response methods based on new threats and developing attack methodologies is also crucial.

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.

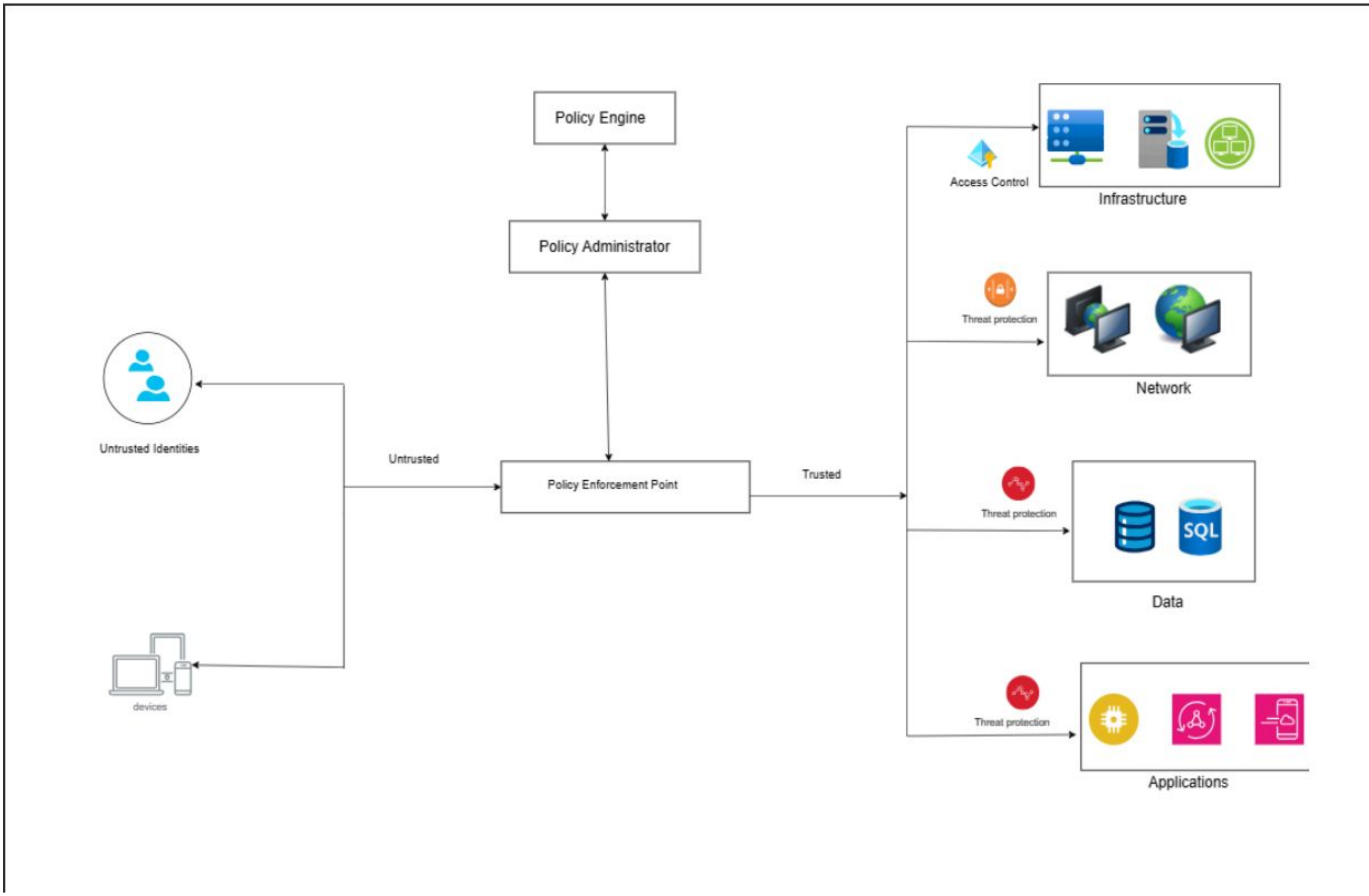
Design a Zero Trust model of your network architecture using https://app.diagrams.net/.

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:



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.

The Zero Trust model and traditional secure network designs vary dramatically in their approach to network security. The Zero Trust paradigm implies zero trust, decreasing the risk of insider attacks and granting access depending on dynamic criteria like user identification, device health, and contextual information. This method decreases the attack surface and mitigates the possibility of insider attacks. Traditional safe designs frequently utilise static access restrictions based on network location, which may need to be revised for new cyber threats and distant work situations. The Zero Trust strategy also promotes micro-segmentation, separating the network into smaller zones to limit and isolate any risks. It also combines continuous monitoring and adaptive security measures to identify and react to real-time security risks. This proactive method helps firms promptly spot abnormalities and possible breaches, decreasing attacker dwell time. The Zero Trust concept provides a paradigm leap in network security, overcoming the limitations of perimeter-based techniques.