

Cloud Computing

Assignment 3

Harshpreet singh (43501)

Sukhwinder singh (44300)

Table of Contents

Task 1: Connecting two VMS.....	2
Executive summary	2
Configuring VNet-to-VNet gateway connection	3
Task 2: Risk management plan	14
Executive Summary	14
Distributed-Denial-of-Service Attacks	14
Shared Cloud Computing Services	15
Employee Negligence	15
References	17

Task 1: Connecting two VMS

Executive summary

The report has designed and implement a cloud solution for an IT infrastructure. The main objective of this paper is the deployment of two virtual networks and secure communication within two virtual machines in the Microsoft Azure platform. Microsoft Azure is a public cloud computing infrastructure utilized for networking, storage, virtual computing, analytics, and much more. The Microsoft Azure cloud platform contains more than 200 cloud services and helps its clients to manage, run, and build applications across multiple clouds. The Virtual network provides secure communication within multiple virtual servers, virtual machines, computers, or other devices across different regions. While the virtual machine is one type of computer resource that utilizes software instead of utilizing physical networking devices to deploy applications and run programs. The virtual machine provides a safe environment and protects the network from various kinds of security issues.

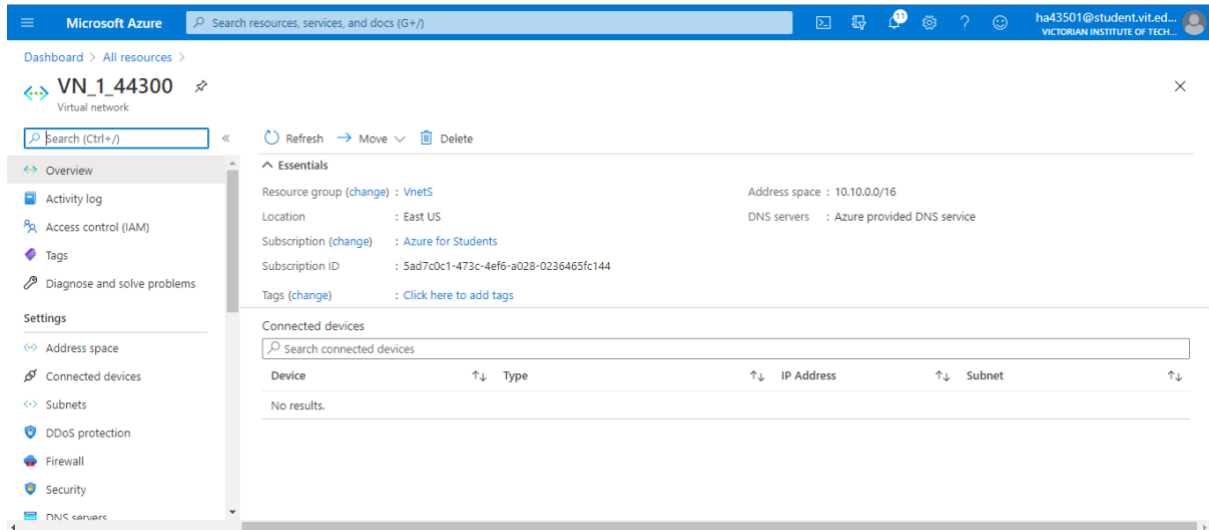
In this project, two virtual networks have been created within the Microsoft Azure platform with specific address space and specific subnet range. After the development of two Virtual Networks Gateway subnets are added under each subnet. Therefore, two public IP address has been created for two virtual networks and both the public address are dynamic. Further, two Virtual gateway network has been created and both are connected with each other. Finally, the VM has been created and connected with two virtual machines. By deploying two virtual machines into the virtual network both the user can securely communicate with each other. The virtual network of the Microsoft azure is the basic building block of the private network that permits the utilization of any type of Azure resources like virtual machines in order to securely communicate with each other on the internet. In this project, both the VMs are connected with Connected through the putty application. Further, the 'ifconfig' command has been utilized to check the IP address configuration of both the virtual machines. Finally, both the connected virtual machines are tested by ping from one machine to another.

Therefore, once the virtual network has peered then both the virtual networks can communicate and share resources securely within each other with the same bandwidth and latency. In this project, both the virtual machines have been created in the same virtual network and both of the VMs utilizes a private IP address to communicate securely. Both the virtual machines are allocated with a dynamic IP address during deployment. Virtual network and virtual machine limit the cost of the network by reducing the requirements of the physical hardware network. Moreover, in this project, both the virtual networks are connected in such a way that they can

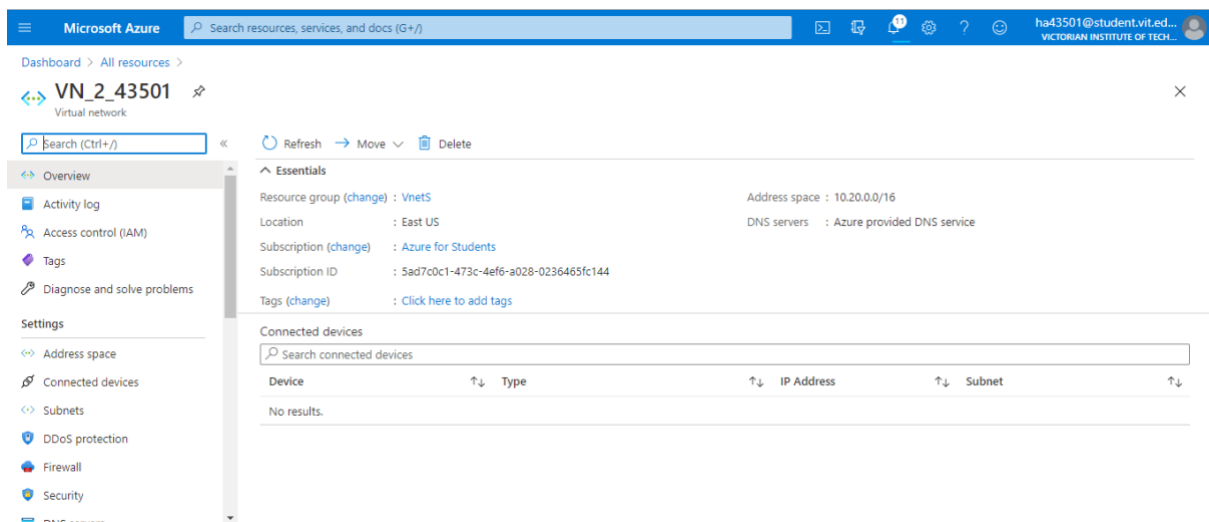
securely communicate with each other and protect the network from various kinds of security issues.

Configuring VNet-to-VNet gateway connection

Step 1



Screenshot 1: Virtual network 1 (VN_1_44300)



Screenshot 2: Virtual Network 2 (VN_2_43501)

Step 2

Dashboard > All resources > VN_1_44300

>> <> VN_1_44300 | Subnets

Virtual network

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

+ Subnet + Gateway subnet Refresh Manage users Delete

Search subnets

Name ↑↓	IPv4 ↑↓	IPv6 (many available) ↑↓	Delegated to ↑↓	Security group ↑↓	
VN_1_44300	10.10.0.0/24 (251 available)	-	-	-	...
GatewaySubnet	10.10.1.0/24 (251 available)	-	-	-	...

Screenshot 3: Gateway Subnet for VN_1_44300

Dashboard > All resources > VN_2_43501

>> <> VN_2_43501 | Subnets

Virtual network

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

Service endpoints

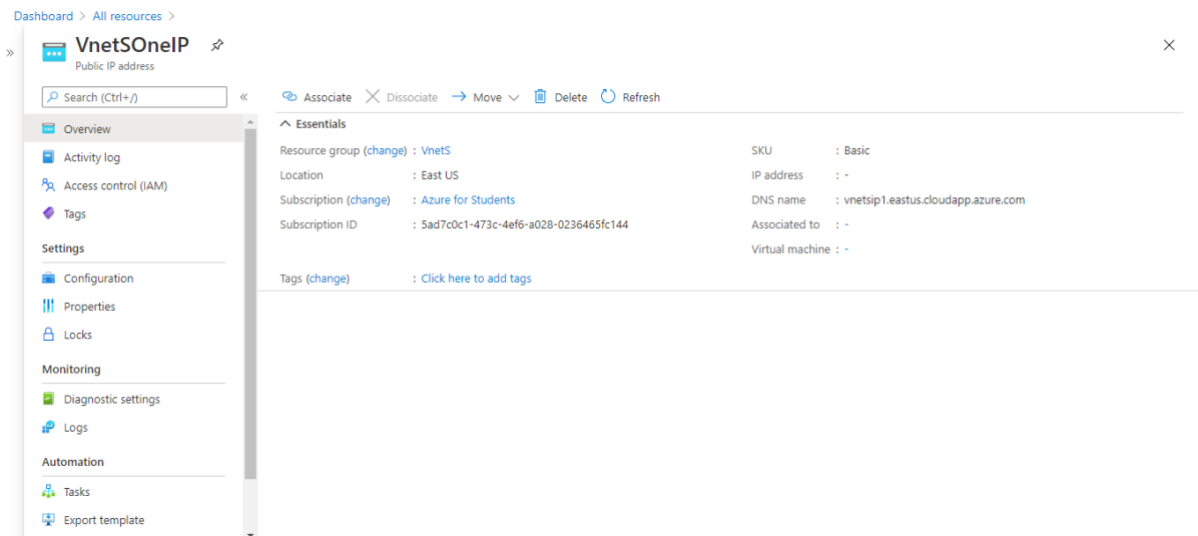
+ Subnet + Gateway subnet Refresh Manage users Delete

Search subnets

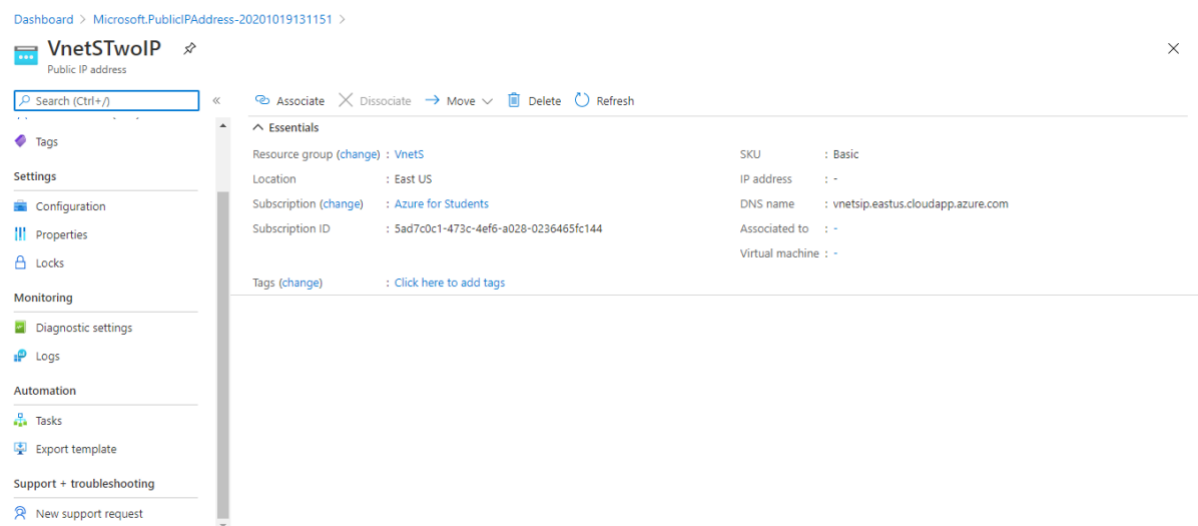
Name ↑↓	IPv4 ↑↓	IPv6 (many available) ↑↓	Delegated to ↑↓	Security group ↑↓	
VN_2_43501	10.20.0.0/24 (251 available)	-	-	-	...
GatewaySubnet	10.20.1.0/24 (251 available)	-	-	-	...

Screenshot 4: Gateway subnet for VN_2_43501

Step 3



Screenshot 5: Public IP address for VN_1_44300



Screenshot 6: Public IP address for VN_2_43501

Step 4

The screenshot displays the Azure portal interface for the Virtual Network Gateway **VN_1_44300_Gateway**. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Configuration, Connections, Point-to-site configuration, Properties, Locks), and Monitoring (Logs, Alerts). The main content area shows the gateway's details under the 'Essentials' tab. Key properties include: Resource group (VnetS), Location (East US), Subscription (Azure for Students), and Subscription ID (5ad7c0c1-473c-4ef6-a028-0236465fc144). The gateway is configured with SKU VpnGw1, Gateway type VPN, VPN type Route-based, and is connected to virtual network VN_1_44300. Its public IP address is 104.211.24.29 (VnetSOneIP). Below the properties, there are sections for 'Health check' (with a 'Go to Resource health' link) and 'Documentation' (with a 'View documentation' link). At the bottom, monitoring charts for 'Total tunnel ingress' and 'Total tunnel egress' are shown, both with a scale of 1008 and a selected time range of 1 hour.

Screenshot 7: Virtual Network gateway for student 1

The screenshot displays the Azure portal interface for the Virtual Network Gateway **VN_2_43501_Gateway**. The layout is identical to Screenshot 7, with the same sidebar and navigation options. The main content area shows the details for this specific gateway. Key properties include: Resource group (VnetS), Location (East US), Subscription (Azure for Students), and Subscription ID (5ad7c0c1-473c-4ef6-a028-0236465fc144). The gateway is configured with SKU VpnGw1, Gateway type VPN, VPN type Route-based, and is connected to virtual network VN_2_43501. Its public IP address is 13.82.199.19 (VnetSTwoIP). The 'Health check' and 'Documentation' sections are also present. The monitoring charts at the bottom show 'Total tunnel ingress' and 'Total tunnel egress' with a scale of 1008 and a selected time range of 1 hour.

Screenshot 8: Virtual Network Gateway for student 2

Step 5:

Microsoft Azure

Search resources, services, and docs (G+)

Dashboard > New > Marketplace > Connection > Create connection >

Settings

*First virtual network gateway

VN_1_44300_Gateway

*Second virtual network gateway

VN_2_43501_Gateway

☒ Establish bidirectional connectivity

First connection name *

VN_1_44300_Gateway-to-VN_2_43501_G...

Second connection name *

VN_2_43501_Gateway-to-VN_1_44300_G...

Shared key (PSK) *

12345678

IKE Protocol

☐ IKEv1

☒ IKEv2

☐ Use Azure Private IP Address

OK

Screenshot 9: Gateway Connection

Microsoft Azure

Search resources, services, and docs (G+)

Dashboard > New > Marketplace > Connection > Create connection >

Summary

Basics

Connection type

VNet-to-VNet

Subscription

Azure for Students

Resource Group

Vnets

Location

East US

Settings

First virtual network gateway

VN_1_44300_Gateway

Second virtual network gateway

VN_2_43501_Gateway

Establish bidirectional connectivity

Yes

First connection name

VN_1_44300_Gateway-to-VN_2_43501_Gateway

Second connection name

VN_2_43501_Gateway-to-VN_1_44300_Gateway

Shared key (PSK)

12345678

Enable BGP

No

IKE Protocol

OK

Screenshot 10: Connection between two Vnets

Step 6

Dashboard > New > × **Create a virtual machine**

✓ Validation passed

Basics

Subscription	Azure for Students
Resource group	VnetS
Virtual machine name	VM1-144300
Region	East US
Availability options	No infrastructure redundancy required
Image	Ubuntu Server 18.04 LTS - Gen1
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Authentication type	SSH public key
Username	azureuser
Public inbound ports	SSH
Azure Spot	No

Disks

OS disk type	Premium SSD
Use managed disks	Yes

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#)

Screenshot 11: Virtual machine 1 creation

Dashboard > New > × **Create a virtual machine**

✓ Validation passed

Disks

OS disk type	Premium SSD
Use managed disks	Yes
Use ephemeral OS disk	No

Networking

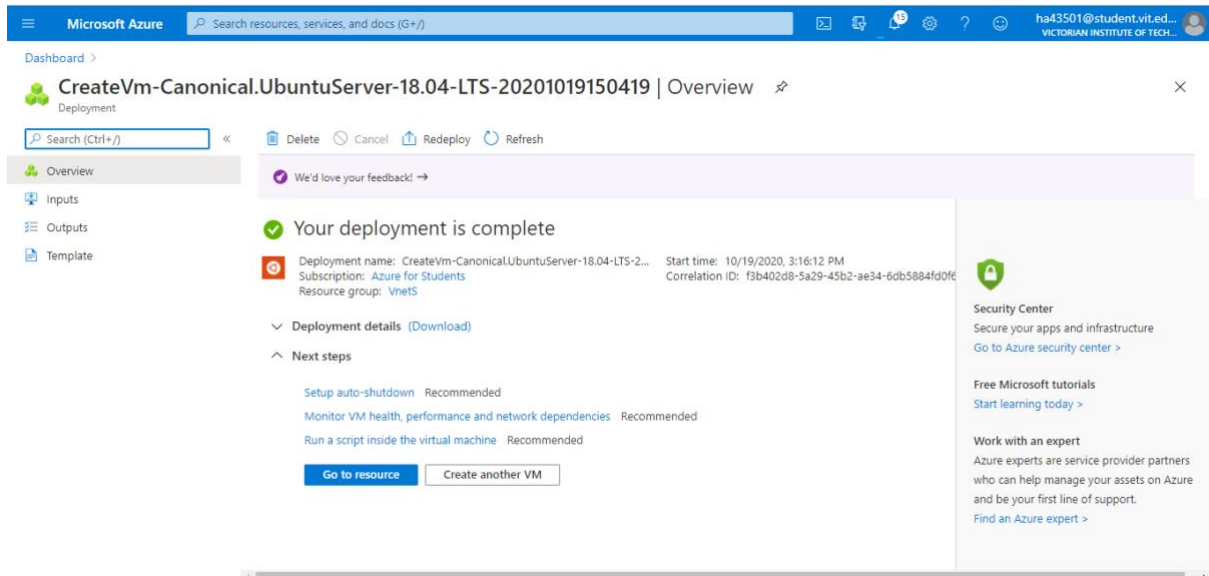
Virtual network	VN_1_44300
Subnet	VN_1_44300 (10.10.0.0/24)
Public IP	(new) VM1-144300-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

Management

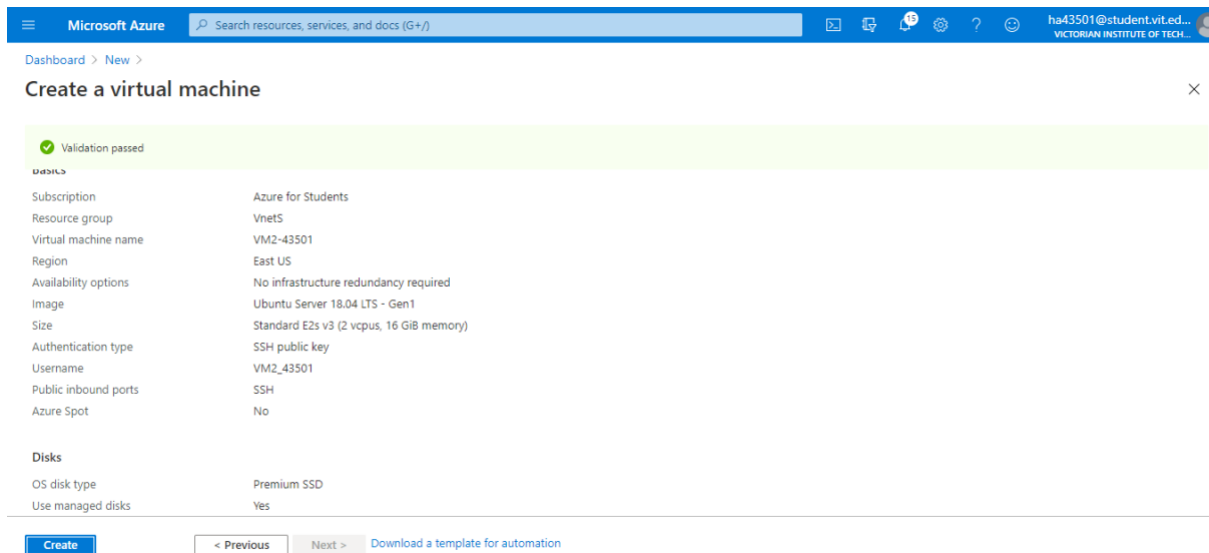
Boot diagnostics	On
------------------	----

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#)

Screenshot 12: Virtual machine 1 creation



Screenshot 13: Virtual machine 1 creation



Screenshot 14: Virtual machine 2 creation

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

Dashboard > New >

Create a virtual machine

Validation passed

Disks

OS disk type	Premium SSD
Use managed disks	Yes
Use ephemeral OS disk	No

Networking

Virtual network	VN_2_43501
Subnet	VN_2_43501 (10.20.0.0/24)
Public IP	(new) VM2-43501-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No

Management

Boot diagnostics	On
------------------	----

[Create](#)
[< Previous](#)
[Next >](#)
[Download a template for automation](#)

Screenshot 15: Virtual machine 2 creation

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

Dashboard >

CreateVm-Canonical.UbuntuServer-18.04-LTS-20201019151751 | Overview

Deployment

Search (Ctrl+/) Delete Cancel Redeploy Refresh

Overview

Your deployment is complete

Deployment name: CreateVm-Canonical.UbuntuServer-18.04-LTS-2... Start time: 10/19/2020, 3:25:15 PM
 Subscription: Azure for Students Correlation ID: 314ab478-ee02-4a62-b504-71af7e46f01b
 Resource group: VNetS

Deployment details (Download)

Next steps

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

[Go to resource](#)
[Create another VM](#)

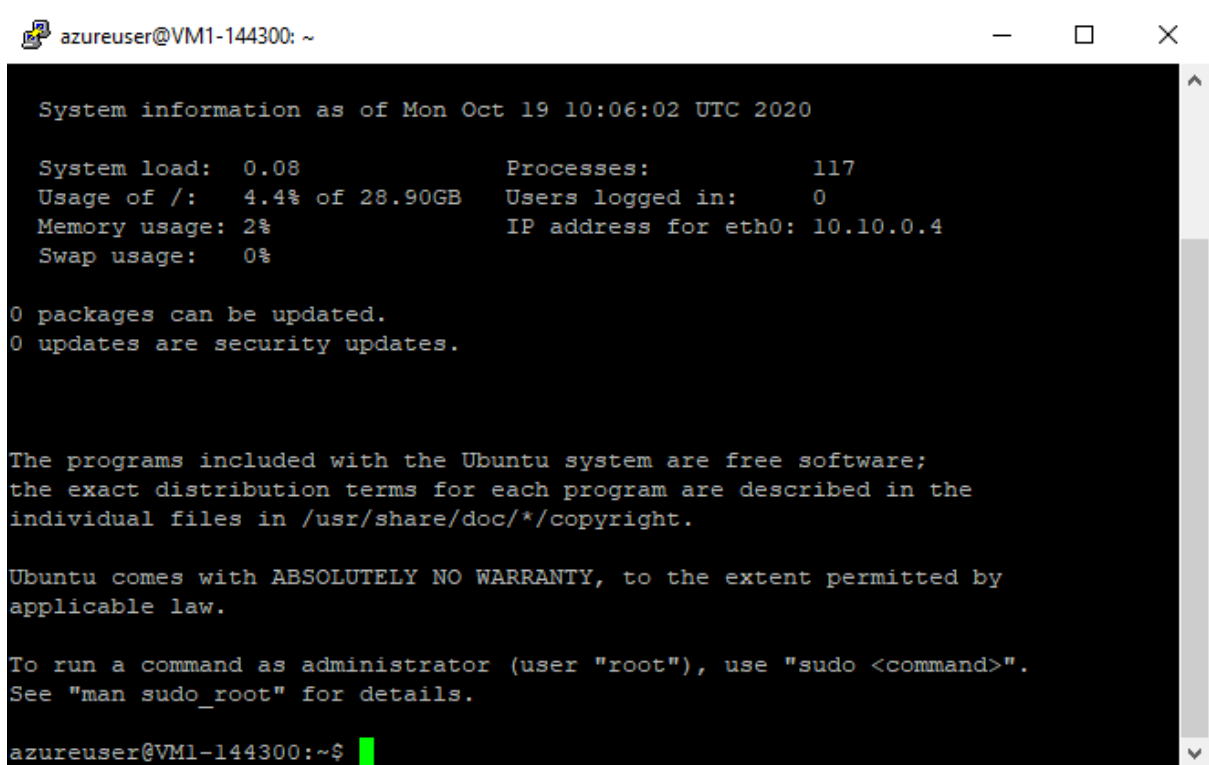
Security Center
 Secure your apps and infrastructure
[Go to Azure security center >](#)

Free Microsoft tutorials
[Start learning today >](#)

Work with an expert
 Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
[Find an Azure expert >](#)

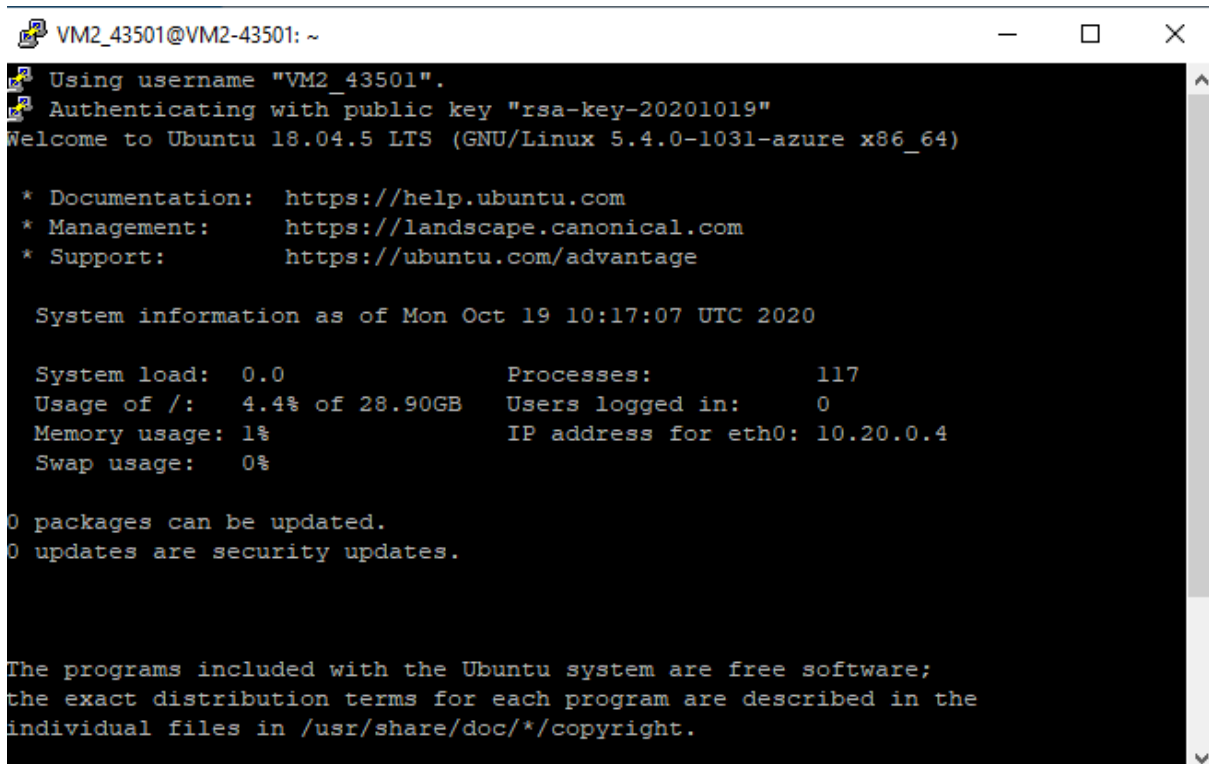
Screenshot 16: Virtual machine 2 creation

Step 7



```
azureuser@VM1-144300: ~  
  
System information as of Mon Oct 19 10:06:02 UTC 2020  
  
System load: 0.08      Processes:           117  
Usage of /:  4.4% of 28.90GB  Users logged in:    0  
Memory usage: 2%      IP address for eth0: 10.10.0.4  
Swap usage:  0%  
  
0 packages can be updated.  
0 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
azureuser@VM1-144300:~$
```

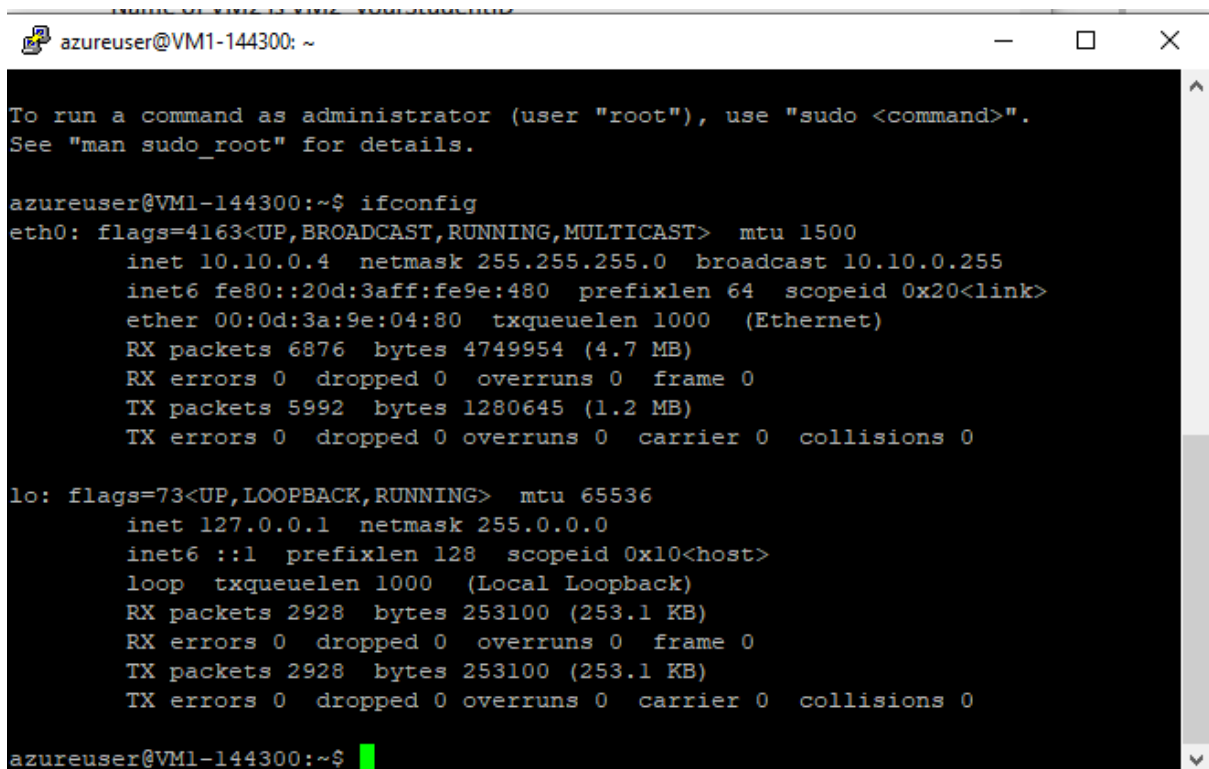
Screenshot 17: VM1 connection through putty



```
VM2_43501@VM2-43501: ~  
Using username "VM2_43501".  
Authenticating with public key "rsa-key-20201019"  
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1031-azure x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Mon Oct 19 10:17:07 UTC 2020  
  
System load: 0.0      Processes:           117  
Usage of /:  4.4% of 28.90GB  Users logged in:    0  
Memory usage: 1%      IP address for eth0: 10.20.0.4  
Swap usage:  0%  
  
0 packages can be updated.  
0 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

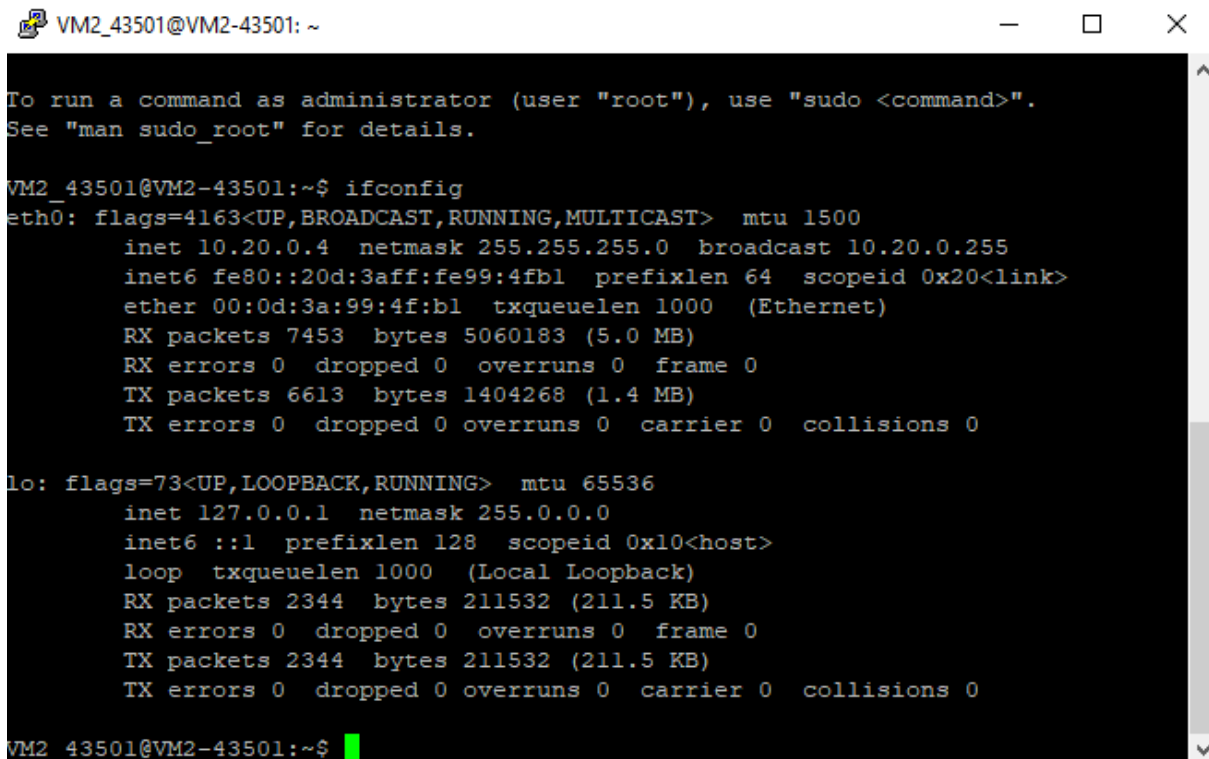
Screenshot 18: VM2 connection through putty

Step 8:



```
azureuser@VM1-144300: ~  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
azureuser@VM1-144300:~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.10.0.4 netmask 255.255.255.0 broadcast 10.10.0.255  
    inet6 fe80::20d:3aff:fe9e:480 prefixlen 64 scopeid 0x20<link>  
    ether 00:0d:3a:9e:04:80 txqueuelen 1000 (Ethernet)  
    RX packets 6876 bytes 4749954 (4.7 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 5992 bytes 1280645 (1.2 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 2928 bytes 253100 (253.1 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2928 bytes 253100 (253.1 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
azureuser@VM1-144300:~$
```

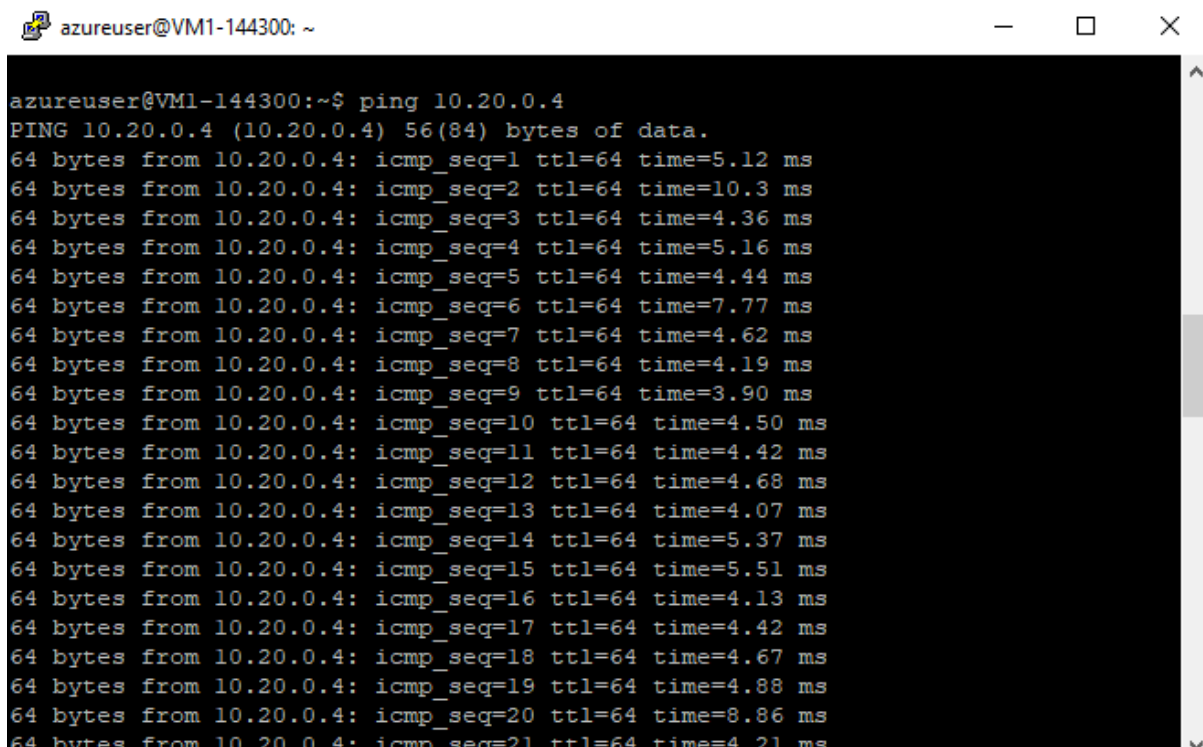
Screenshot 19: Ifconfig of VM1



```
VM2_43501@VM2-43501: ~  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
VM2_43501@VM2-43501:~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.20.0.4 netmask 255.255.255.0 broadcast 10.20.0.255  
    inet6 fe80::20d:3aff:fe99:4fb1 prefixlen 64 scopeid 0x20<link>  
    ether 00:0d:3a:99:4f:b1 txqueuelen 1000 (Ethernet)  
    RX packets 7453 bytes 5060183 (5.0 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 6613 bytes 1404268 (1.4 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 2344 bytes 211532 (211.5 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2344 bytes 211532 (211.5 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
VM2_43501@VM2-43501:~$
```

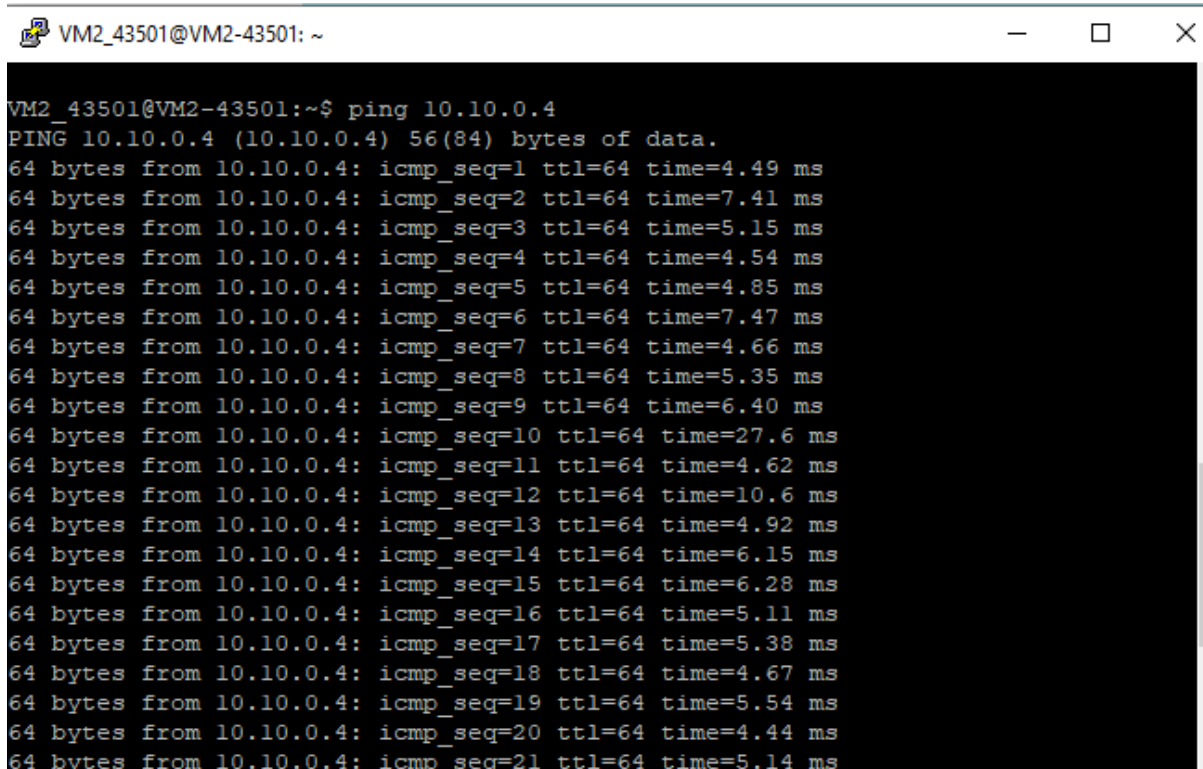
Screenshot 20: Ifconfig of VM2

Step 9:



```
azureuser@VM1-144300: ~  
azureuser@VM1-144300:~$ ping 10.20.0.4  
PING 10.20.0.4 (10.20.0.4) 56(84) bytes of data.  
64 bytes from 10.20.0.4: icmp_seq=1 ttl=64 time=5.12 ms  
64 bytes from 10.20.0.4: icmp_seq=2 ttl=64 time=10.3 ms  
64 bytes from 10.20.0.4: icmp_seq=3 ttl=64 time=4.36 ms  
64 bytes from 10.20.0.4: icmp_seq=4 ttl=64 time=5.16 ms  
64 bytes from 10.20.0.4: icmp_seq=5 ttl=64 time=4.44 ms  
64 bytes from 10.20.0.4: icmp_seq=6 ttl=64 time=7.77 ms  
64 bytes from 10.20.0.4: icmp_seq=7 ttl=64 time=4.62 ms  
64 bytes from 10.20.0.4: icmp_seq=8 ttl=64 time=4.19 ms  
64 bytes from 10.20.0.4: icmp_seq=9 ttl=64 time=3.90 ms  
64 bytes from 10.20.0.4: icmp_seq=10 ttl=64 time=4.50 ms  
64 bytes from 10.20.0.4: icmp_seq=11 ttl=64 time=4.42 ms  
64 bytes from 10.20.0.4: icmp_seq=12 ttl=64 time=4.68 ms  
64 bytes from 10.20.0.4: icmp_seq=13 ttl=64 time=4.07 ms  
64 bytes from 10.20.0.4: icmp_seq=14 ttl=64 time=5.37 ms  
64 bytes from 10.20.0.4: icmp_seq=15 ttl=64 time=5.51 ms  
64 bytes from 10.20.0.4: icmp_seq=16 ttl=64 time=4.13 ms  
64 bytes from 10.20.0.4: icmp_seq=17 ttl=64 time=4.42 ms  
64 bytes from 10.20.0.4: icmp_seq=18 ttl=64 time=4.67 ms  
64 bytes from 10.20.0.4: icmp_seq=19 ttl=64 time=4.88 ms  
64 bytes from 10.20.0.4: icmp_seq=20 ttl=64 time=8.86 ms  
64 bytes from 10.20.0.4: icmp_seq=21 ttl=64 time=4.21 ms
```

Screenshot 21: Ping from VM 1 to VM 2



```
VM2_43501@VM2-43501: ~  
VM2_43501@VM2-43501:~$ ping 10.10.0.4  
PING 10.10.0.4 (10.10.0.4) 56(84) bytes of data.  
64 bytes from 10.10.0.4: icmp_seq=1 ttl=64 time=4.49 ms  
64 bytes from 10.10.0.4: icmp_seq=2 ttl=64 time=7.41 ms  
64 bytes from 10.10.0.4: icmp_seq=3 ttl=64 time=5.15 ms  
64 bytes from 10.10.0.4: icmp_seq=4 ttl=64 time=4.54 ms  
64 bytes from 10.10.0.4: icmp_seq=5 ttl=64 time=4.85 ms  
64 bytes from 10.10.0.4: icmp_seq=6 ttl=64 time=7.47 ms  
64 bytes from 10.10.0.4: icmp_seq=7 ttl=64 time=4.66 ms  
64 bytes from 10.10.0.4: icmp_seq=8 ttl=64 time=5.35 ms  
64 bytes from 10.10.0.4: icmp_seq=9 ttl=64 time=6.40 ms  
64 bytes from 10.10.0.4: icmp_seq=10 ttl=64 time=27.6 ms  
64 bytes from 10.10.0.4: icmp_seq=11 ttl=64 time=4.62 ms  
64 bytes from 10.10.0.4: icmp_seq=12 ttl=64 time=10.6 ms  
64 bytes from 10.10.0.4: icmp_seq=13 ttl=64 time=4.92 ms  
64 bytes from 10.10.0.4: icmp_seq=14 ttl=64 time=6.15 ms  
64 bytes from 10.10.0.4: icmp_seq=15 ttl=64 time=6.28 ms  
64 bytes from 10.10.0.4: icmp_seq=16 ttl=64 time=5.11 ms  
64 bytes from 10.10.0.4: icmp_seq=17 ttl=64 time=5.38 ms  
64 bytes from 10.10.0.4: icmp_seq=18 ttl=64 time=4.67 ms  
64 bytes from 10.10.0.4: icmp_seq=19 ttl=64 time=5.54 ms  
64 bytes from 10.10.0.4: icmp_seq=20 ttl=64 time=4.44 ms  
64 bytes from 10.10.0.4: icmp_seq=21 ttl=64 time=5.14 ms
```

Screenshot 22: Ping from VM 2 to VM 1

Task 2: Risk management plan

Executive Summary

Risk treatment is the procedure of picking and implementing security measures to limit the risk. Risk treatment measures can contain retaining, transferring, optimizing, or avoiding risks and risks can be controlled internally by avoiding or by preventing the risks. Therefore, the report has been provided a risk assessment plan that will mitigate three identified security issues such as the distributed denial of service attacks, shared cloud computing services, and employee negligence. A distributed denial of service attack is a malevolent attempt by the attacker to interrupt the normal traffic of a targeted network, service, or server by flooding the target server. Shared cloud computing services is another security issues in cloud computing as it increases the chances of data theft or a breach in cloud computing. Finally, another security issue discussed in the report is employee negligence that will cause many data thefts or data breaches within the organization.

Distributed-Denial-of-Service Attacks

An attack of DDoS can be very much disruptive and they are being risen. It targets the IT services, cloud computing, and software. It is an attack that is intended to take offline a service or organization or otherwise render unusable resources that have an origin from hosts multiple in number (Bhushan & Gupta, 2019). The multiple host part of this attack is what makes it called distributed and this part makes the attack much more difficult to defend it.

- **Risk Mitigation Plan:** Protection of the network from the DDoS attack requires correct response planning. The mitigation plan's first step is to make the infrastructure DDoS resistant by having sufficient bandwidth in order to handle any kind of spikes that arise in the traffic which can be caused due to various malicious activities (Bawany, Shamsi & Salah, 2017). Having a secured DNS server is one of the ways of mitigating the attack from DDoS. The DNS server should have enough redundancy to make sure that such an attack does not happen. Another way is of installing anti-DDoS hardware and modules of the software.
- **Risk Monitoring Plan:** The steps that can be taken include performing frequent scans on the web services and fixing any type of vulnerable web applications in order to lessen the compromise risk, ensuring that the network used is protected with the help of prevention of intrusion and other threat management systems in order to help protect the assets of the network, ensuring that there is a presence of advance SIEM (Security Information and Event Management) solution in hands to

take care of security that is consolidated. There is also a need for a 24/7 monitoring and mitigation solution process.

Shared Cloud Computing Services

Cloud environments also experience threats at a very high level and the same ones as the traditional data center environments face. Actually, cloud computing run software, and software always face vulnerabilities (Abrar et al., 2018). There are problems like the consumers gets reduced visibility and control over the assets present there. There are also other problems faced like that of exposure to a set of application programming interfaces that are used by the customer in order to manage and interact with cloud services. The threat posing actors looks for various vulnerabilities that can be turned into successful attacks.

- **Risk Mitigation Plan:** There are several ways to mitigate it. They include, encryption of data at rest which means encrypting data at the situation where it protects the data that is used or in transit, then there is a two-factor authentication plan, elimination of the shared accounts, and insisting on a well-defined shared model of responsibility (Kar & Mishra, 2016). There are also other ways like usage of standardized cloud assessment questions and so on.
- **Risk Monitoring Plan:** In monitoring the risk, the ways include there should be two-factor authentication provided at the doorstep of this because that provides a high level of monitoring of the data at the primary position.

Employee Negligence

Cloud security is very much important for an organization as it protects the data stored on the internet from deletion, leakage, and theft. Employment negligence is an area of law that seriously affects the organization, other employees, and causes data breach. Therefore, employee negligence is the biggest cybersecurity risk for organizations all around the world. The laptops and computers used by the employee contain highly sensitive information and most of the organization's sensitive data breach or security incident happens due to a negligent or malicious activity.

- **Mitigation policy:** In order to mitigate the employee negligence risk, the organization needs to train out the employees about cybersecurity. Most of the riskiest offenses consider by the employees are potentially dangerous or negligent behavior such as leaves the computer unlocked while leaving the office. Therefore, organizations need to provide security training in their onboarding process to teach employees about

cybersecurity and data protection best practices (Cunningham, Jones & Dreschler, 2018). When employees of an organization get frequent and proper training, they will become more sensitive and effectively protect the data of the organization. The organization also needs to develop security-focused culture by providing accessible training opportunities and by conducting regular information sessions for both old and new staff. Regular review procedure implementation helps to identify the negligence employees as well as the various security issues. Therefore, in order to manage the employee's negligence, the organization also needs to establish remote control over mobile security because the risks taken by employees are increase when they are working remotely such as in-home or coffee office. Therefore, an organization needs to implement all the above risk mitigation policies to mitigate employee negligence.

- **Risk monitoring and risk reviewing plan:** Risk monitoring and reviewing plan is a significant way to protect the organization's significant data from employee's negligence (Brown, 2020). The risk monitoring plan also helps to identify all the risks that harm the workplace of the organization. The organization needs to continuously monitor all the employees to protect the organization's sensitive data from breaches. The risk assessment plan will also contain good management practices that will train the employees about cyber security.

References

- Abrar, H., Hussain, S. J., Chaudhry, J., Saleem, K., Orgun, M. A., Al-Muhtadi, J., & Valli, C. (2018). Risk analysis of cloud sourcing in healthcare and public health industry. *IEEE Access*, 6, 19140-19150.
- Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, 42(2), 425-441.
- Bhushan, K., & Gupta, B. B. (2019). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. *Journal of Ambient Intelligence and Humanized Computing*, 10(5), 1985-1997.
- Brown, A. (2020). *Why Are Non-Malicious Employees Non-Compliant: Guidance for Identifying Employee Negligence and Implementing Information Security Policies to Reduce Employees Inadvertently Becoming Insider Threats* (Doctoral dissertation, Utica College).
- Cunningham, M. R., Jones, J. W., & Dreschler, B. W. (2018). Personnel risk management assessment for newly emerging forms of employee crimes. *International Journal of Selection and Assessment*, 26(1), 5-16.
- Kar, J., & Mishra, M. R. (2016). Mitigating Threats and Security Metrics in Cloud Computing. *JIPS*, 12(2), 226-233.