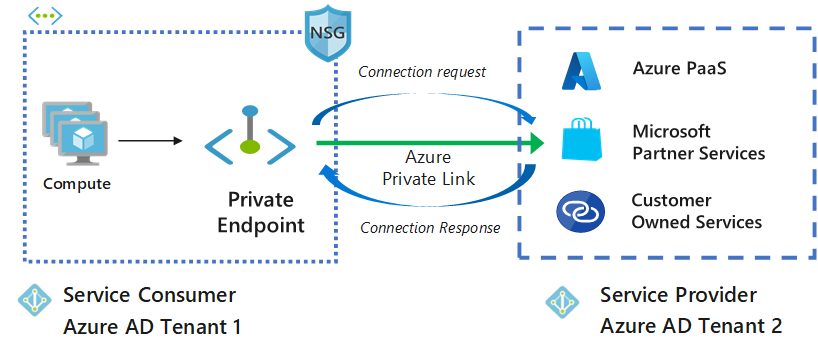
Azure Files SMB Access with private end point share a file on private network



Network and Systems Administration

Student ID:

Cybersecurity

Dublin Business School

Contents

[INTRODUCTION 5](#_Toc100270265)

[AIM OF PROJECT 6](#_Toc100270266)

[BACKGROUND 6](#_Toc100270267)

[Authentication in AzureAuthentication 6](#_Toc100270268)

[Azure AD Domain 6](#_Toc100270269)

[Azure AD AuthenticationAzure 6](#_Toc100270270)

[Azure FilesAzure 7](#_Toc100270271)

[Azure Files Share Access 7](#_Toc100270272)

[TECHNOLOGIES APPLIED IN THE PROJECT 9](#_Toc100270273)

[SMB 9](#_Toc100270274)

[Domain Name System 10](#_Toc100270275)

[Web technology 11](#_Toc100270276)

[DNS BIND 11](#_Toc100270277)

[Microsoft Azure 11](#_Toc100270278)

[TECHNICAL DESCRIPTION OF THE PROJECT 12](#_Toc100270279)

[Evaluation 28](#_Toc100270280)

[Appendix A 28](#_Toc100270281)

[Appendix B BIBLIOGRAPHY 30](#_Toc100270282)

Table of Figure

[Figure 1Partial DNS Name Space Hierarchy 8](#_Toc100370651)

[Figure 2Name Resolution Process (without cache search) 8](#_Toc100370652)

[Figure 3SMB 9](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370653)

[Figure 4SMB private zone 10](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370654)

[Figure 5DNS Concept 10](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370655)

[Figure 6working of dns 11](#_Toc100370656)

[Figure 7Web technology 11](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370657)

[Figure 8protocol of WEB Technology 11](#_Toc100370658)

[Figure 9concept of private end point 12](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370659)

[Figure 10azure portal 12](#_Toc100370660)

[Figure 11storage end point 13](#_Toc100370661)

[Figure 12vnet 13](#_Toc100370662)

[Figure 13storage vnet 14](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370663)

[Figure 14container 14](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370664)

[Figure 15private end point 15](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370665)

[Figure 16dns configure 15](file:///C:\Users\HafizUsama\Desktop\Private%20End%20Point%20on%20Azure%20access%20storage%20account%20.docx#_Toc100370666)

[Figure 17container block in publc ip 16](#_Toc100370667)

[Figure 18server machine 17](#_Toc100370668)

[Figure 19running 17](#_Toc100370669)

[Figure 20installing chrome 18](#_Toc100370670)

[Figure 21traffic pass the private ip 18](#_Toc100370671)

[Figure 22file uploading private network 19](#_Toc100370672)

[Figure 23uploaded successfull 19](#_Toc100370673)

[Figure 24server 2 20](#_Toc100370674)

[Figure 25file found on other server 20](#_Toc100370675)

[Figure 26file download 21](#_Toc100370676)

# INTRODUCTION

The Internet is the world's greatest enrolling network, with more than 580 million clients. As indicated by the perspective of a client, each center point or resource on this association is recognized by a phenomenal name: the space name.

Picture result for private end point A private endpoint is an organization interface that utilizes a private IP address from your virtual organization. This organization interface associates you secretly and safely to a help that is controlled by Azure Private Link. By empowering a private endpoint, you're bringing the assistance into your virtual organization

The SMB convention was initially made by IBM as a client-server convention for getting to shared documents, printers over network, and for empowering between process correspondences. Different renditions of the convention, generally called tongues, were made after some time to meet changing organization prerequisites. The convention works at the application layer and can impart on port 445 over TCP/IP

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services

# AIM OF PROJECT

In this project we can share a file one machine to other machine via private end point on azure using private network and making a private DNS zone

This distribution tries to help associations in getting the safe arrangement of Domain Name System (DNS) administrations in a venture. It gives down to earth, certifiable direction on getting every aspect of DNS inside an association in view of an examination of the working climate and related dangers.

Right now, the DNS isn't the objective of most assaults, however as hosts become greater security mindful, and applications start to depend on the DNS framework for network tasks, the DNS foundation will turn into a really enticing objective. A definitive objective for DNSSEC is full sending across the whole area tree on the foundation side, and execution in applications that can request the administrations given by DNSSEC. At present there are no functional hubs in the DNS area tree that gives DNSSEC capacities. Thus the initial move towards completely organization is to give DNSSEC ability to area subtrees that have high security needs. When DNSSEC abilities become generally accessible in the framework, application engineers will actually want to foster DNSSEC-mindful applications and subsequently use DNSSEC as a method for network security.

For quite a while I see a wide range of choices to utilize Azure documents, have a few good thoughts and contemplations. Associating this over the vpn of purpose the purplish blue documents with a dfs. Valuable perhaps? fun totally assembling things simply a way that is perhaps a piece different is tomfoolery and you might see different open doors on the best way to utilize the assets

# BACKGROUND

## Authentication in Azure Authentication

For assets in Azure purposes the RBAC model for the board plane or entryway level access. Nonetheless, individual administrations facilitated in Azure, including SMB, have their own verification components. The favored strategy for verification of uses in Azure is through Azure Active Directory. It is a cloud-based way of life as a help presenting from Azure that can be coordinated with a wide assortment of uses facilitated in cloud as well as in your corporate network.

## Azure AD Domain

When you pursue an Azure cloud membership, a case of Azure AD is provisioned for you, which is called an Azure AD inhabitant. A devoted Active Directory that has an area name in the configuration <domain name>.onmicrosoft.com is doled out to each occupant. All clients, gatherings, and applications connected to your association's Azure AD occupant will be essential for this Azure AD space. You can utilize custom space names with Azure AD, where clients can be made in Azure AD with your association's area name.

## Azure Files Azure

Files is the overseen document share in the cloud that can be gotten to over Server Message Protocol (SMB) from on-premises as well as cloud-based machines. The document offers can be straightforwardly provisioned from the Azure entryway, without going through the difficulty of provisioning a whole foundation to have the offers. It is a cross-stage administration, where the offers can be gotten to from Windows, Linux, or MAC OS, given that they support SMB.Azure Files additionally

## Azure Files Share Access

Azure Files utilizes SMB 3.0 and HTTPs for secure information access. You can likewise settle on REST API decisions from your applications to a facilitated Azure Files share. Validation to Azure documents is finished utilizing shared admittance signature (SAS) tokens while getting to the offers over REST API. For getting to over SMB, verification is finished utilizing stockpiling access keys. The disadvantage here is that anybody having capacity access keys can get to the record share, which is a degree of straightforwardness that a security review may be concerned with. Cloud Volumes ONTAP then again upholds AD-based confirmation for the document shares facilitated in the assistance, so clients can have fine-grain command over who approaches explicit offers and records provisioned utilizing the help

Root “.”

.gov

.com

.uk

.arpa

nist.gov dhs .gov

example.com

ac.uk co.u k

in-addr.arpa

Enterpri se- Level Domain

TLD

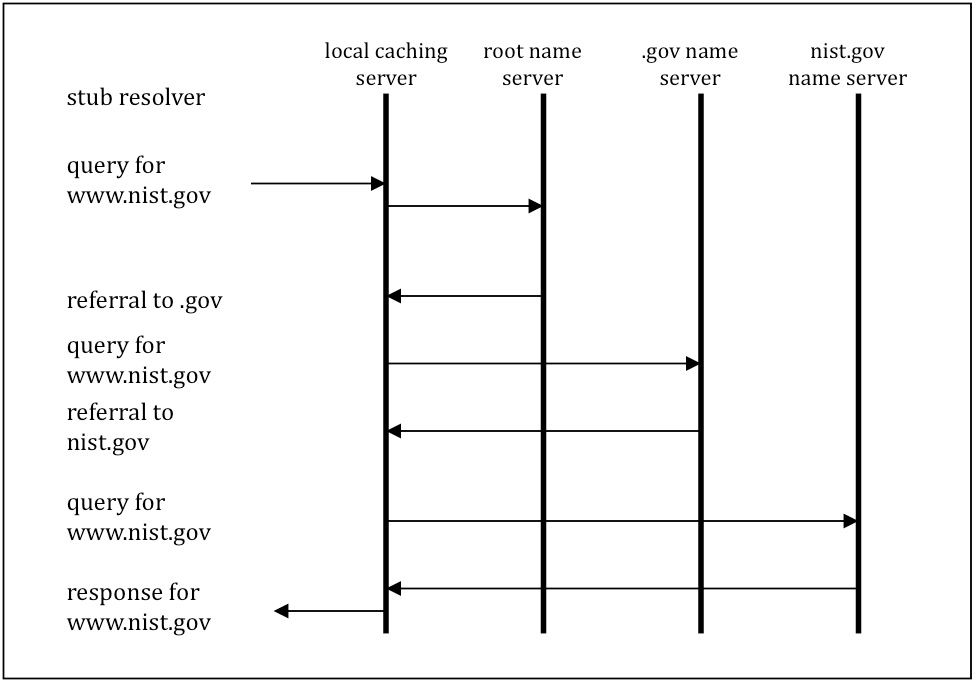
Figure 1Partial DNS Name Space Hierarchy

Figure 2Name Resolution Process (without cache search)

# TECHNOLOGIES APPLIED IN THE PROJECT

This venture included the creation and organization of a Virtual Network System fit to help web applications, which included the accompanying framework organization advancements

## SMB

The Server Message Block (SMB) convention is an organization record sharing convention that permits applications on a PC to peruse and write to documents and to demand administrations from server programs in a PC organization. The SMB convention can be utilized on top of its TCP/IP convention or other organization conventions

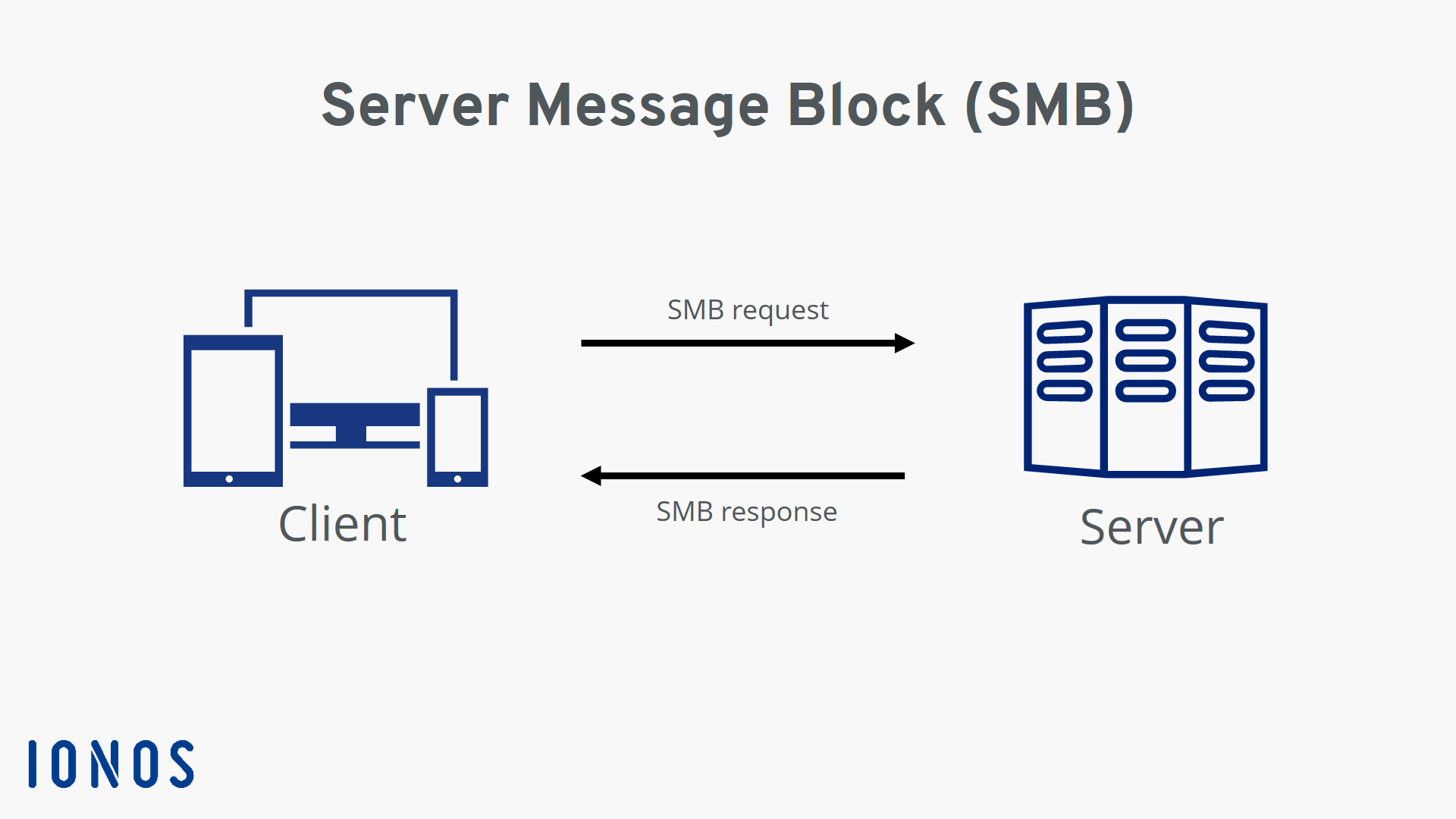


Figure SMB

The SMB convention permits clients to get to shared records on a far off server through a bunch of solicitations sent between the client and the server by means of information parcels. These incorporate fundamentally meeting control bundles and document access parcels

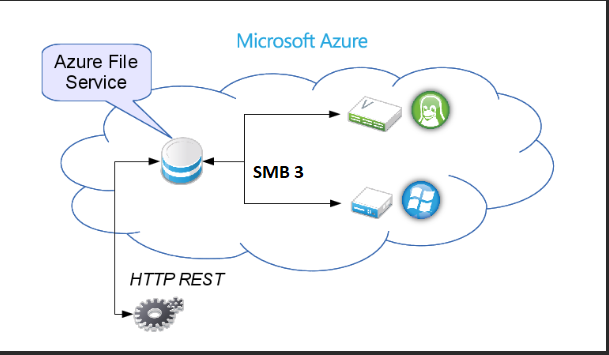


Figure SMB private zone

## Domain Name System

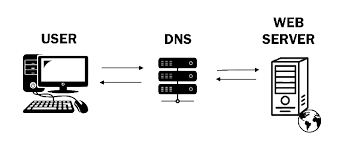
The Domain Name System is the various leveled and decentralized naming framework used to distinguish PCs, administrations, and different assets reachable through the Internet or other Internet Protocol organizations. The asset records contained in the DNS partner space names with different types of data

Figure DNS Concept

Figure 6working of dns

## Web technology

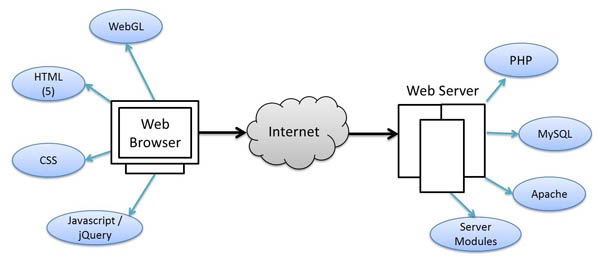
Web technology alludes to the means by which PCs speak with one another utilizing markup dialects and mixed media bundles. It gives us a method for interfacing with facilitated data, similar to sites. Web innovation includes the utilization of hypertext markup language (HTML) and falling templates (CSS)

Figure Web technology

Figure 8protocol of WEB Technology

## DNS BIND

Tie is an open source framework allowed to download and utilize, presented under the Mozilla Public License. Tie can be utilized to run a reserving DNS server or a legitimate name server, and gives highlights like burden adjusting, inform, dynamic update, split DNS, DNSSEC, IPv6, and then some

## Microsoft Azure

Azure creates a canonical name DNS record (CNAME) on the public DNS. The CNAME record redirects the resolution to the private domain name. You can override the resolution with the private IP address of your private endpoints. Your applications don't need to change the connection URL

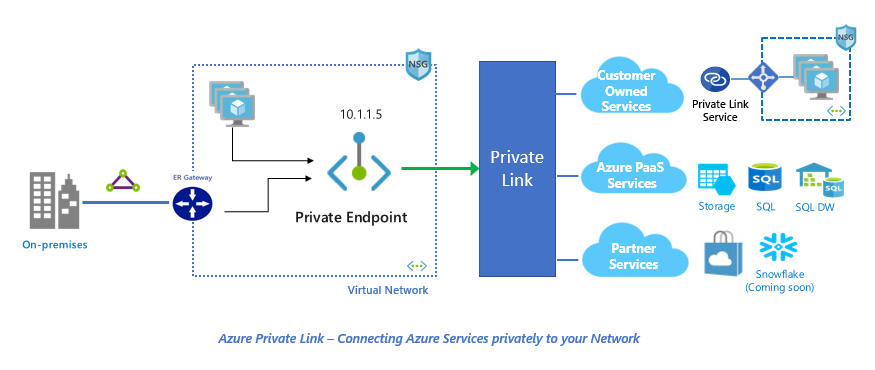


Figure concept of private end point

# TECHNICAL DESCRIPTION OF THE PROJECT

In this project we can share a file one machine to other machine via private end point on azure using private network and making a private DNS zone

Login to azure account and making a storage account , vnet , private end point and private DNS zone

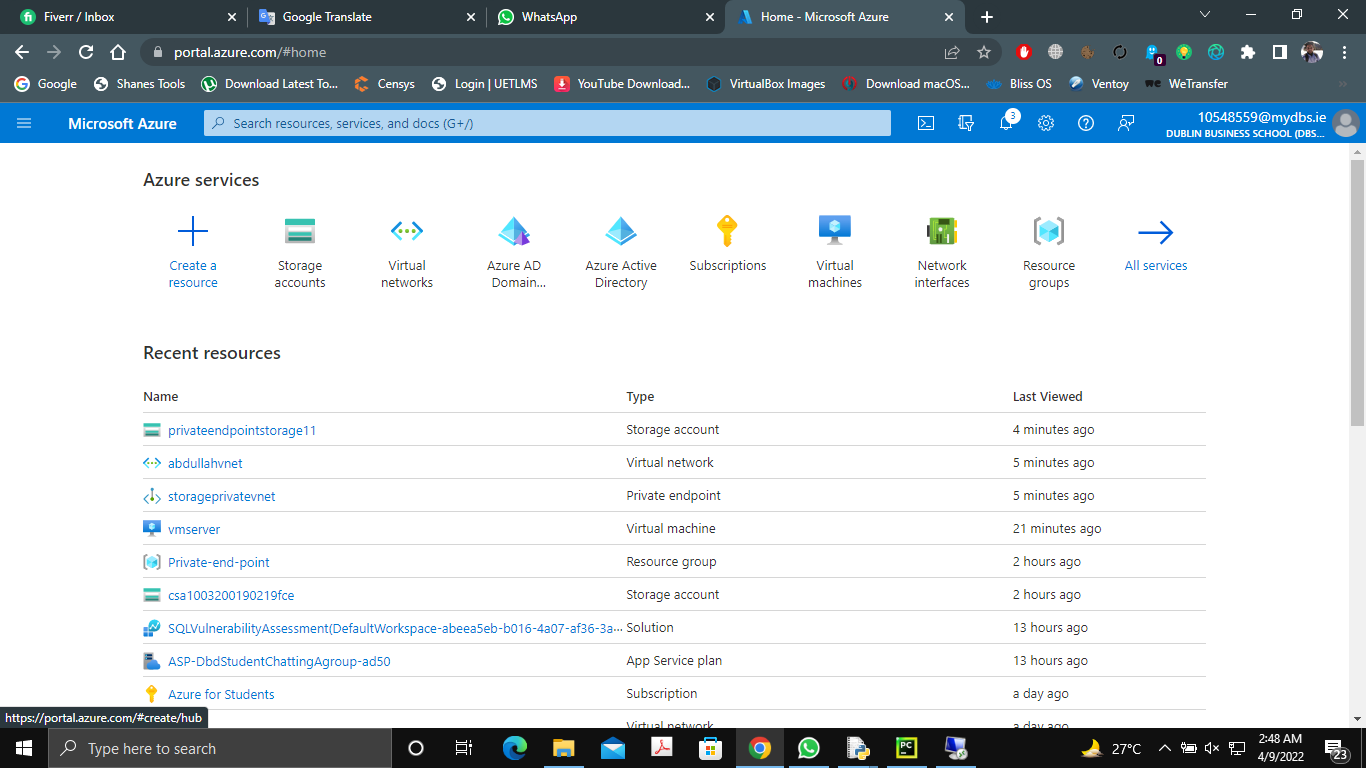


Figure 10azure portal

We have to successfully created storage account

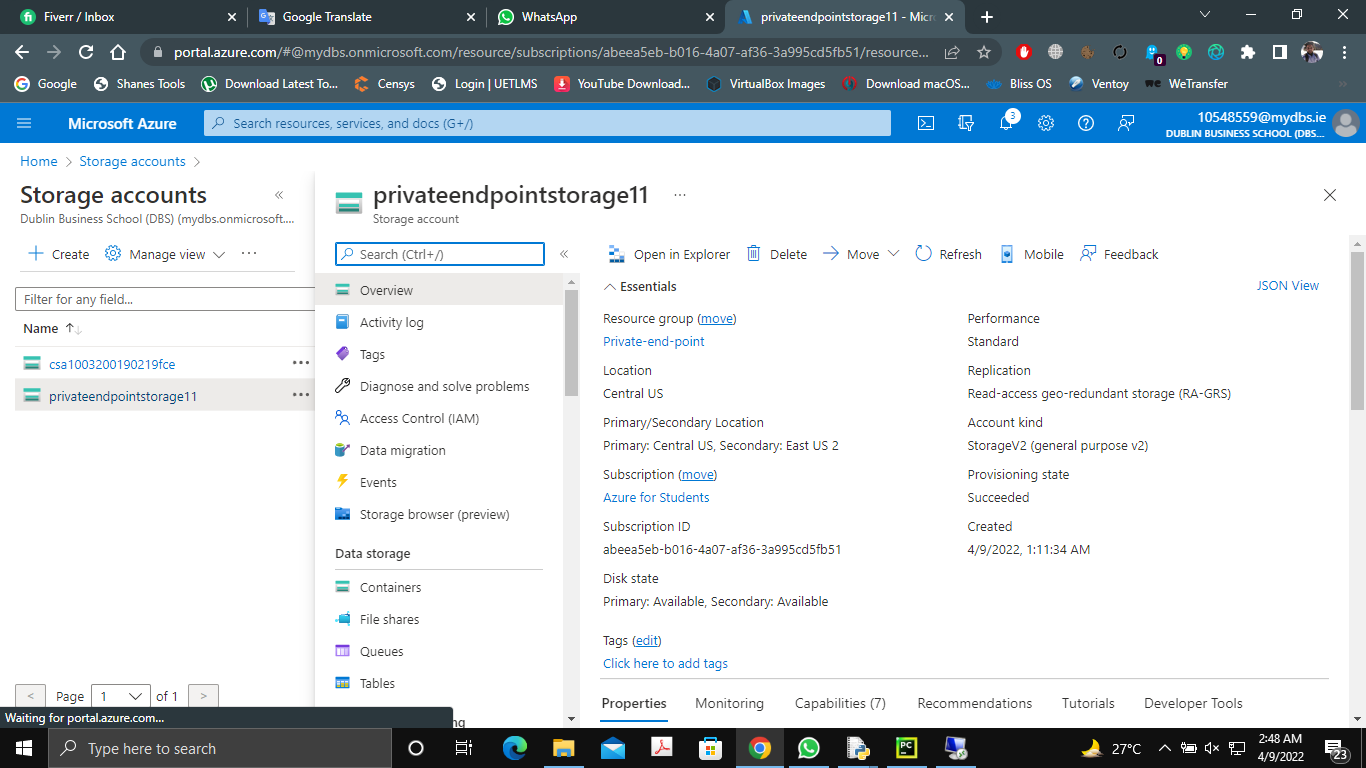


Figure 11storage end point

Now we create a vnet name of abdullah

# 

Figure 12vnet

Create a private end point

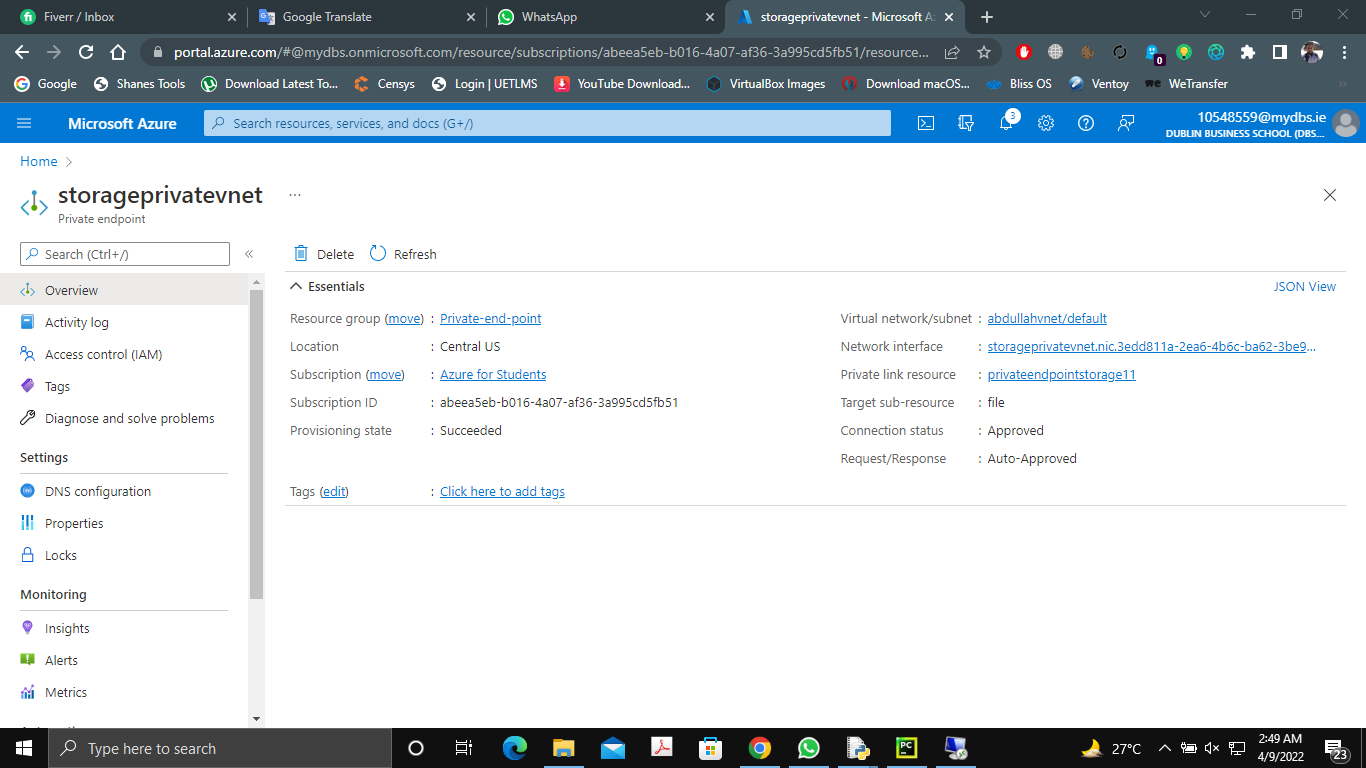


Figure storage vnet

Making a container to share a file this container not access the outside the private network

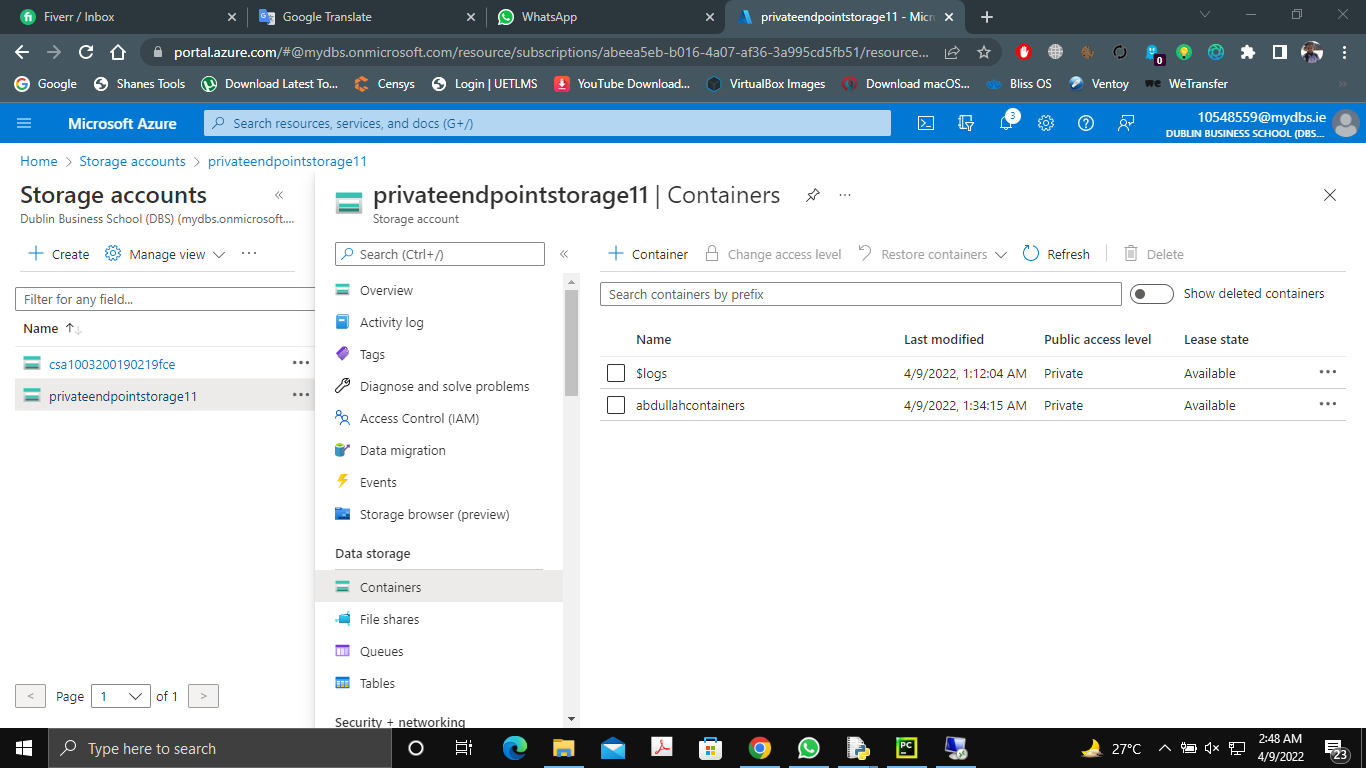


Figure container

Create a private DNS zones

# 

Figure private end point

Configuration of dns in storage end vnet

# 

Figure dns configure

Container not access from outside the private network

# 

Figure 17container block in publc ip

Create a virtual machine window 2016

# 

Figure 18server machine

Successfully created

# 

Figure 19running

Installing chrome in vm via CMD

# 

Figure 20installing chrome

Machine on a private network my machine traffic going to vnet private ent point

# 

Figure 21traffic pass the private ip

Container is access on vmserver due to which machine traffic going to private network

# 

Figure 22file uploading private network

File upload successfully

# 

Figure 23uploaded successfull

Now we create a second machine this machine traffic going to private network

# 

Figure 24server 2

File is also uploaded successfully

# 

Figure 25file found on other server

File dawnload on first machine which name is vmserver

# 

Figure 26file download

# Evaluation

The Internet's DNS framework works similar as a telephone directory by dealing with the planning among names and numbers. DNS servers make an interpretation of solicitations for names into IP addresses, controlling which server an end client will arrive at when they type an area name into their internet browser. These solicitations are called questions

Now we can share file using azure dns and private end point . Shared access. Azure file shares support the industry standard SMB and NFS protocols, meaning you can seamlessly replace your on-premises file shares with Azure file shares without worrying about application compatibility

Private Link gives a safe method for relocating jobs to Azure. Insurance against information spillage: A private endpoint is planned to a case of a PaaS asset rather than the whole assistance. Buyers can associate with the particular asset. Admittance to some other asset in the assistance is obstructed

Traffic can arrive at the help asset from on premises without utilizing public endpoints. A Service Endpoint stays a freely routable IP address. A Private Endpoint is a private IP in the location space of the virtual organization where the private endpoint is arranged

# Appendix A

Selected acronyms used in the  *DOMAIN NAME SYSTEM (DNS)* are defined below.

A Address

ACL Access Control List

AD Authenticated Data

ANSI American National Standards Institute

ARP Address Resolution Protocol

CA Certificate Authority

ccTLD Country-code Top-level Domain

CD Checking Disabled

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DNSSEC Domain Name System Security Extensions

DS Delegation Signer

DSA Digital Signature Algorithm

DSS Digital Signature Standard

ECDSA Elliptic Curve Digital Signature Algorithm

FIPS Federal Information Processing Standards FISMA Federal Information Security Management Act FQDN Fully Qualified Domain Name

gTLD Generic Top-level Domain

HINFO Host Information

HMAC Hash-based Message Authentication Code

ICANN Internet Corporation for Assigned Names and Numbers

IETF Internet Engineering Task Force

IN Internet

IP Internet Protocol

ISP Internet Service Provider

IT Information Technology

ITL Information Technology Laboratory

KSK Key Signing Key

LAN Local Area Network

LOC Location

MAC Message Authentication Code

MD Message Digest

MX Mail Exchanger

NIST National Institute of Standards and Technology

NS Name Server

NSEC Next Secure

NSEC3 Hashed Next Secure

NTP Network Time Protocol

OMB Office of Management and Budget

OS Operating System

PKI Public Key Infrastructure

PIR Public Internet Registry

RFC Request for Comments

RP Responsible Person

RR Resource Record

RRSIG Resource Record Signature

SEP Secure Entry Point

SHA Secure Hash Algorithm

SHS Secure Hash Standard

SOA Start of Authority

TCP Transmission Control Protocol

TLD Top-level Domain

TSIG Transaction Signature

TTL Time to Live

TXT Text

UDP User Datagram Protocol

ZSK Zone Signing Key

# Appendix B BIBLIOGRAPHY

[RFC3833] D. Atkins and R. Austein, “Threat Analysis of the Domain Name System (DNS)”, RFC 3833, August 2004.

[RFC2181] R. Elz and R. Bush, “Clarifications to the DNS Specification”, RFC 2181, July 1997. [RFC1912] D. Barr, “Common DNS Operational and Configuration Errors”, RFC 1912, Feb. 1996 [RFC1034] P. Mockapetris, “Domain Names - Concepts and Facilities”, STD 13, RFC 1034,

November 1987.

[RFC1035] P. Mockapetris, “Domain Names - Implementation and Specification”, STD 13, RFC 1035, November 1987.

[BCP140] J. Damas and F. Neves, “Preventing Use of Recursive Nameservers in Reflector Attacks”, BCP 140, RFC 5358. October 2008.

[RFC2671] P. Vixie, “Extension Mechanisms for DNS (EDNS0)” RFC 2671 August 1999 [RFC1996] P. Vixie, “A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)”

RFC 1996. August 1996.

[IEEE] S. Rose and A. Nakassis. “Minimizing Information Leakage in the DNS” IEEE Network Magazine vol. 22 no. 2 April 2008.

<https://www.youtube.com/watch?v=Up9yAWmJ6b0&ab_channel=TravisRoberts>

<https://www.youtube.com/watch?v=OQjK4gC89Xc&ab_channel=TravisRoberts>