# Enhanced storage security risk management

**Abstract**

In this project we are fixing storage account problems, for example, we have a company that has a file storage server and this server is connected to many networks. If we are connected to a network, then we can switch from one network to another network easily. For example, my system is connected to a single network which is 192.168.3.0 (the public network of the company) and the private network of that company is 10.70.0.1 now i can easily switch between these two networks both have their firewalls but both are connected to a single router. In this way, a person who is not a part of the admin can easily access file storage servers and can retrieve important information. So, to fix this problem we switch from non-cloud to cloud and use the private endpoint zone.

In this project, we can share a file from one machine to a different machine on azure exploitation personal network and can create a non-public dns zone. This distribution tries to assist associations in obtaining the safe arrangement of domain name system (dns) administrations during a process. The dns is not being the objective of many attacks, but as a combination of multiple hosts can protect itself from being attacked. The applications begin to depend on the dns framework for network tasks, the dns foundation can then be changed into main objective. The main aim for dnssec (domain name system security) is to authenticate dns responses with the major goal of prevent spoofing. Nowadays there are not any useful hubs within the dns space tree that offers dnssec functions. So the initial move towards full organization is to offer dnssec that has the ability to space subtrees which requires more security. Once dnssec is typically accessible within the framework, application engineers can easily develop dnssec-mindful applications and then use dnssec as a way for network security.

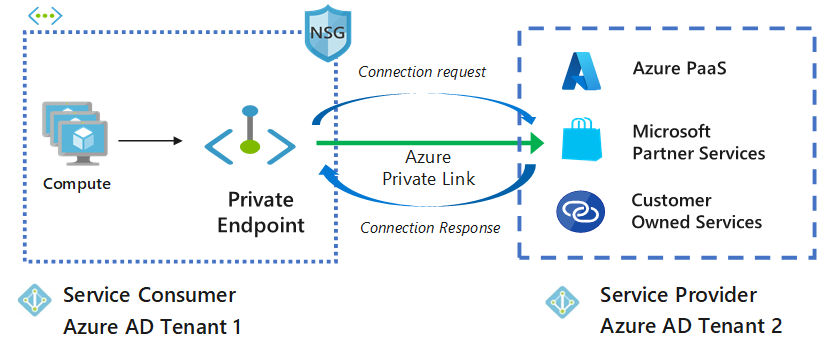
**Introduction**

The internet is the globe's greatest enrolling network, with a capacity of 580 million purchasers. As indicated by the perspective of a shopper, every purpose or a resource on this association is recognized by an outstanding name: the house name. Searching results from the picture for personal purpose uses a corporation interface that utilizes a personal informatics address from your virtual organization. This organization interface safely associates you to a facility that's controlled by azure personal link.

The smb convention was first created by ibm as a client-server convention for sharing documents and printers over the network. To fulfill dynamic organization conditions different types of the conventions were created. The convention works at the appliance layer and communicate on port 445 over tcp/ip. Azure dns is a service of hosting for domains that gives an outcome of name by victimization infrastructure of microsoft azure. Your domains would be hosted in azure, your dns records will be managed by victimization constant credentials and rest of others like api, tools would be by azure service [1].

**Related work / literature review**

Storage security is basically referring to securing information of storage systems and ecosystem. The storage security will depict the convergence of the given network, storage and security disciplines, technologies, and method plan for the aim of protecting and securing digital resources. Security of storage is targeted on the physical, technical, and body control, similarly because detective, preventive, and corrective controls are related to systems of storage and infrastructure. [8]



To ensure the confidentiality, stability, and convenience of the information, we need a joint effort on the ict layer (information and communications technology). Several protection efforts are listed below:

1. Safeguarding the capacity, the board (activities and interfaces), and the data restoration and recuperation assets.
2. Guaranteeing the sufficient declaration and trust of the board.
3. Information is moving, rest, and in accommodation security.
4. Calamity recuperation and business congruity support.
5. Appropriate disinfection and removal.
6. Secure autonomous information movement and secure multi-tenancy.

**Storage security risk**

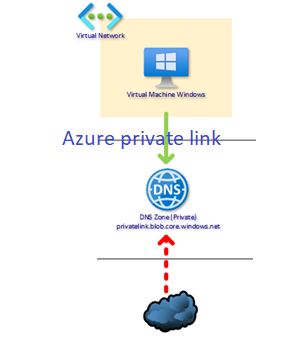
The risk of security is made by an associate organization's use of a specific storage system or infrastructure. Storage security risk is raised by the threats focusing on the data being managed by the storage system and the infrastructure, flaws (both technical and non-technical), and also the effect of roaring exploitation of the flaws by a warning.

Risk management could be a key construct in the data security and this method applies to the organization as a whole, or to a specific portion of the organization. The given method is formed on the context institution, assessment of warning, treatment of the risk, acceptance of the risk, communication of the risk, watching, and also a review of risk.

Given warnings will create huge risk alert. However, the risks related to information breach, information corruption, and destruction, can be temporary or permanent. Complete loss of access and availability, failure satisfaction statutory, managerial, legal necessities area unit are the most important considerations.

**Private dns zone resource**

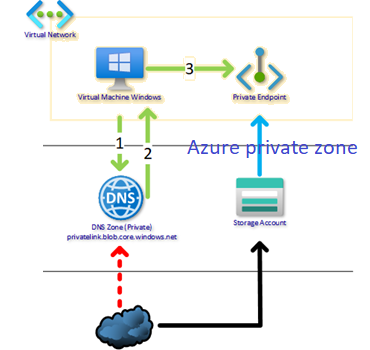
My best methods for implementing dns resolution in various contexts are described. Before that, i'll show you how to use azure's private dns zone resource. It's a private dns zone that only azure may access. Only from the azure public ip addresses, not from the internet.



You can utilize azure to construct the necessary private link dns zone, such as privatelink.blob.core.windows.net. You can tell the system to add the a-record to the private dns zone automatically when constructing a private endpoint. Your dns infrastructure, such as windows server active directory, does not need to be accessible to an azure engineer. When you use azure private dns zones to delete a private endpoint, the a-record is also deleted automatically.

Next, simply add a private dns zone to azure with the domain name of the private endpoint domain name for your resource, such as privatelink.blob.storage.windows.net. Simply choose the dedicated zone for automatic dns registration when constructing the private endpoint and you're done.

If a call to the public dns name (public.blob.core.windows.net) comes from a *vnet*, the private dns zone responds with the private endpoint's internal ip; but, if the request comes from the internet, azure's own dns responds with the public ip [3].



**Data breaches**

The breach of data may be one of the security compromise, having several shapes. The unauthorized access and revelation of protected data are usually recognized kinds of information breaches. An information breach will uncover the organization to severe threat starting from the prices concerned in work info breach, pinging up notifications to attacked people.

Non-trusted or unauthorized bodies seek to leak spilled data that comes from a broad variety of sources. While cloud storage suppliers do much of the work once it involves making your knowledge secure, you got a very important role to act on additionally [6].

**Activate two-step verification**

Every cloud provider provides a facility to defend the account with two-step verification. It needs us to simply avail each watchword (a sign of recognition i.e. Otp code) and one-time confirmation code distributed to our device or any given email address. Due to this, attackers won’t be able to attack and crack your password. Two-factor authentication is usually switched off by default, you can turn this on by going into the settings. Choose two step to enhance security.

**Protect the secret writing key**

The secret key is owned by one person or he can give to other person and gets his one to send the encrypted messages. If both the users have only one is key available for encryption and decryption , so both the sender and receiver of a message needs to have a copy unique secret key to read the message. The major threat to end-to-end secret writing is not to public the secret key that usually checks for the authentication. In other case, you should have a duplicate code in case you don’t remember secret key. Nevertheless, you do not need a duplicate secret writing code for hackers to get their hands on. It’s recommended to write down key in safe and assure its security. It’s up to you if you wish to have a digital copy of the code. This puts the key behind a firewall, so it can’t have access to your pc when hacked.

**Check the shared files**

Cloud storage allows to shares files with anyone. However, when we share with too many people, we can be at risk. We should audit the shared files on regular basis, and cancel the grant for any individual that does not want it. If out cloud provider provides the facility password protected file shared or time limited file sharing, then we should utilize these options instead of unprotected files sharing.

Cloud providers provide maximum data and information security. Once you store data within the cloud, the files area unit is encrypted and incessantly monitored against cyber security threats.

**Proposed project**

Secure accessibility – resources with personal endpoints are accessible from the customers at identical virtual network (ivn) intervals, regionally/globally or peered virtual network.

Unidirectional property – network connections are one-way and are initiated by the customers from the personal end resource. Connections can't be started from the personal link resource to the customers [2].

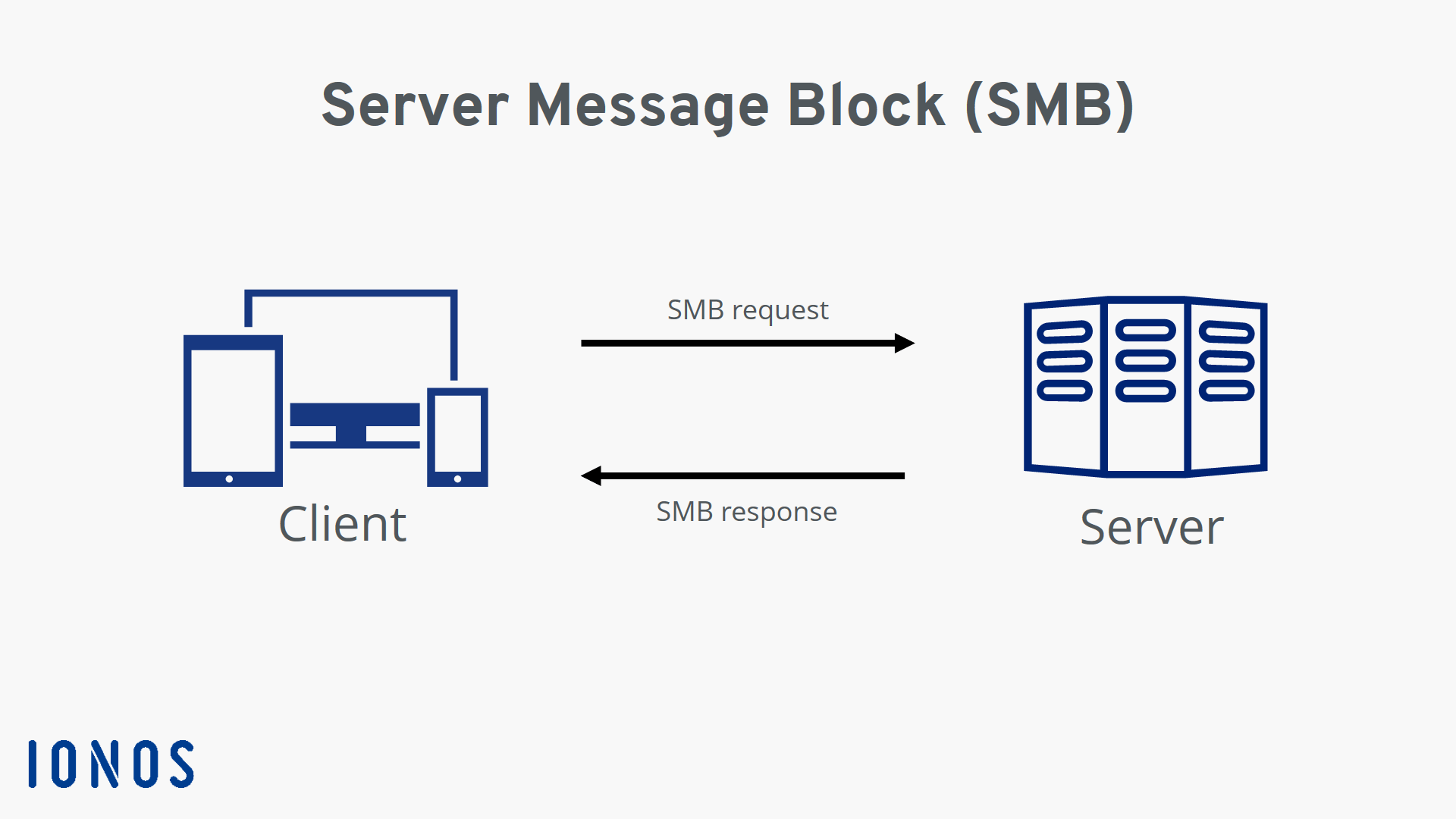
Consistent ip address – once a personal endpoint is made for a resource, a personal ip address is allocated to that end point from the virtual network dynamically, and that doesn't affect other resources in the network.

Same region existence – the personal end should be identically redistributed in the same area whereas personal link resources will be deployed in an increasingly identical area.

Private endpoints limitations – multiple personal endpoints will be created at intervals with identical virtual networks. There will be thousands of personal endpoints per virtual network and most probably 64000 personal endpoints per subscription.

Just one personal dns zone sort (e.g., privatelink.blob.core.windows.net) will be connected to virtual network vnet. The reason for that is virtual network would already know where to send the traffic now.

Resource teams’ area units are typically simply logical containers used for access management. Resources you place in every resource cluster typically depend on your organization's necessities or location necessities. In line therewith, it might solely be that your personal dns zone is within the same resource cluster as your vnet.



In the future, you may have extra storage accounts. All the resource teams can use constant personal dns. Hence, it would be difficult to connect shared resource to a specific project/resource cluster. On contrary to this, personal endpoints connect to a particular resource. This will restrict them to that particular resource only. Hence, it makes a lot of sense for them to be within the same resource cluster because they are already communicating with that resource. The recommendation of design is simple: every project (scopes of however resource area units are managed by identical teams) should have its dns zone.

**Project details / proposed solution**

A private terminus may be a network interface that utilizes a personal web address from your internet. This network interface connects in private and firmly to a service that is powered by an azure non-public link.

Following are the azure services such as:

1. Azure storage
2. Azure cosmos sound unit
3. Azure sql information
4. Your service, victimization non-public link service.

## Authentication in azure authentication

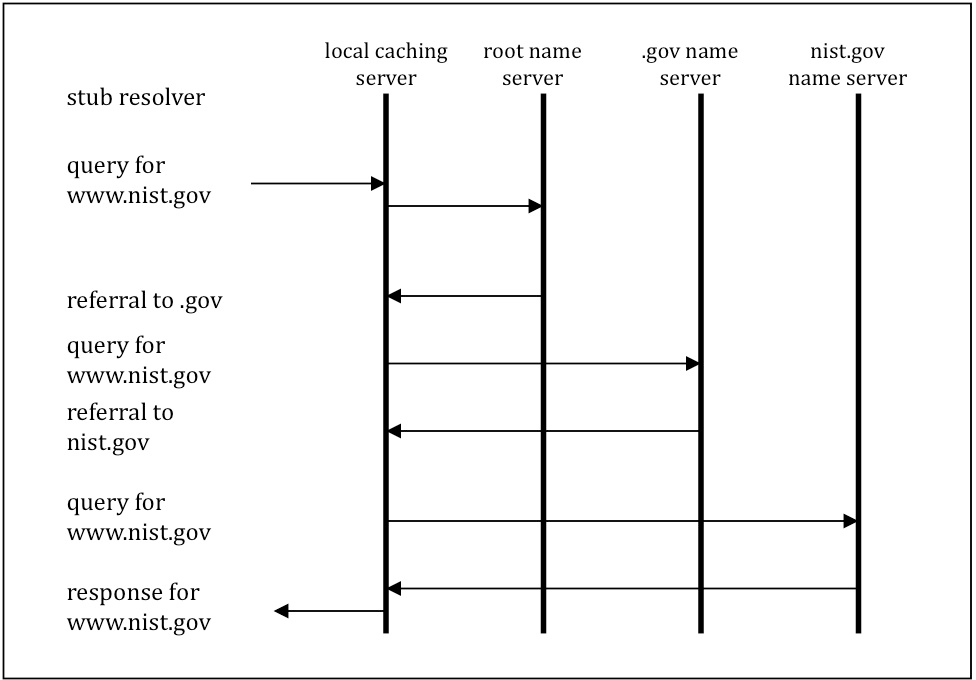
## **Azure ad domain**

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 distributed 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.

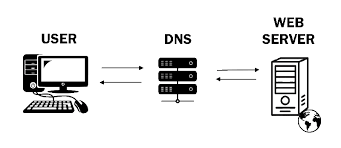
## **Azure files**

Files are the overseen documents shared in the cloud by server message protocol (smb) from on-premises as well as from cloud-based machines. The document offers can be straightforwardly provisioned from the azure entryway, without [4] going through the difficulty of provisioning a whole foundation to have the offers. It is a cross-stage administration, where offers can be gotten from windows, linux, or mac os, given that they support smb and azure files additionally.

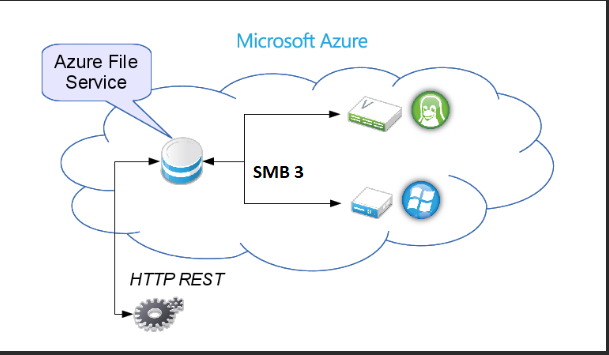
**Azure files share access**

Azure files utilizes smb 3.0 and https for secure information access. You can likewise use rest api decisions from your applications to a facilitated azure files sharing. Validation of azure documents is done by utilizing shared admittance signature (sas) tokens while getting requests from rest api. To get access to the shared files using smb, verification is first one utilizing the stockpiling access keys. The disadvantage here is that anybody [5] who can access the keys, can reach out to the record which is a serious security concern. The cloud gives access on ontap (volumes of clouds enterprise users may use ontap to satisfy a variety of cloud needs, including data transfer, disaster recovery, and backup.) After confirmation for the ad-based assistance. This is done to validate that who tries to see files.

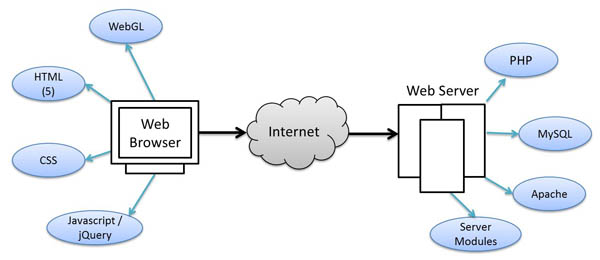
## **Smb**

The server message block (smb) standard is an organization record sharing standard that allows pc applications to read and write documents as well as request services from server programs in a pc network. The smb convention can be used in conjunction with the tcp/ip or other organization standards. The smb convention permits clients to shared records on a far-off server through a bunch of solicitations sent between the client and the server through information parcels. These incorporate fundamentally meeting control bundles and document access parcels.

## **Domain name system**

The domain name system (dns) is a multi-leveled, decentralized name system for distinguishing pcs, administrations, and other assets accessible over the internet or other internet protocol organizations.

## **Web technology**

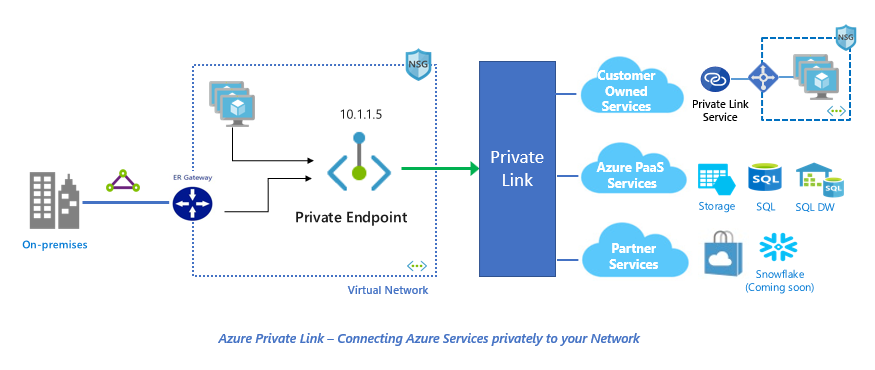
Web technology refers to how computers communicate with one another using markup languages and mixed media files. It provides a site-like interface for interacting with assisted data. Hypertext markup language (html) and cascading style sheets (css) are examples of web innovation.

## **Dns bind**

A dns bind is an open-source framework allows to download and utilize files, presented under the mozilla public license. A 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**

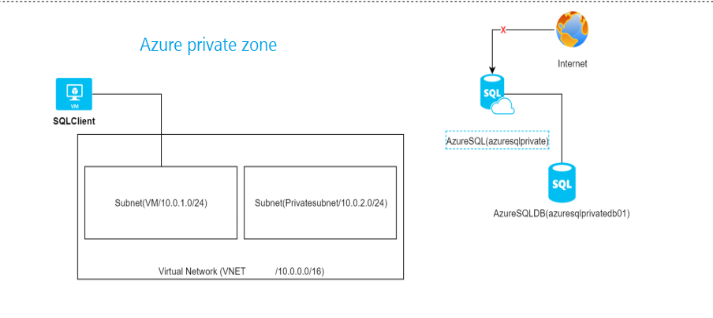
On the public platform dns, azure produces a canonical name dns record (cname). The cname record redirects the resolution to a private domain name. The private ip address of your private endpoints can be used to override the resolution. The connection url does not need to be changed in your apps.



**Discussion and future work**

The requested scenario is to reach azure sql database secretly through virtual network without using public ip address or through internet.

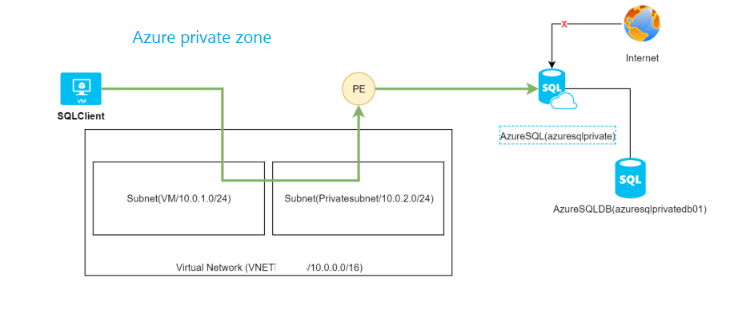
The below picture is shown as a practical device (sqlclient) positioned on a subnet of virtual network (vnet). An *azuresqldb(azuresqlprivatedb01)* is deployed within an *azuresql(azuresqlprivate)*.



The main goal is to reach *azuresqlprivate* from *sqlclient* on a personal association, not through the web (won't permit any scientific discipline for consuming the azure sql server via the firewall).

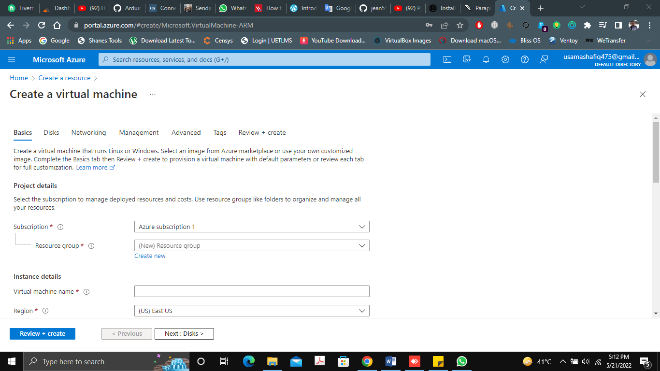
**Solution via private endpoints**

The solution is to make a personal endpoint that can reveal the azure sql server through a personal information processing address on a net mask. The below image shows a personal endpoint (pe) that is the under threat of information processing address from the private subnet that is connected to azure sql private.



**Deploy the answer via the azure gateway**

1. Visit non-public link center –> non-public endpoint –> add
2. Fill in the essential fields, such as subscription.



1. Select the resource which is needed to from a personal end point. In my case it is *azuresqlprivate*.
2. Select the vnet/subnet that will provide access to your resource. A network interface card (nic) will be built behind the scenes, given an ip address, and allocated to your resource. You may integrate the resource with an azure private dns zone if you want to use a dns name to call the private endpoint. You can build your own dns record on your own dns service, therefore this isn't necessary (a record)
3. The connection state is approved and the private endpoint is formed. The private endpoint has been accepted by the azure sql party. This is handy when both parties are not from the same group, since the requester may request the private endpoint connection and wait for the owner to approve it. You can also reject the connection at any moment.
4. Access to the private endpoint should be secured.

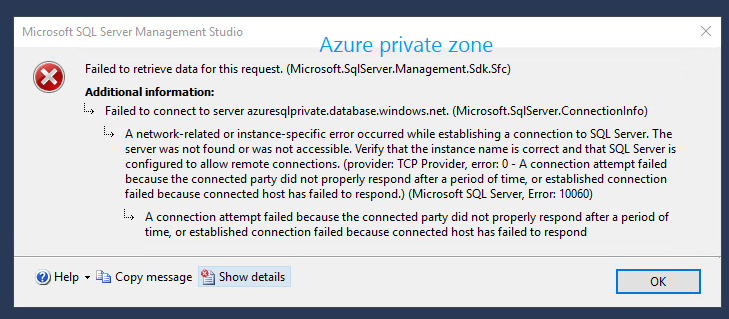
There are a number of ways to secure access to a paas service now that we have private access to it:

For the pe inbound, use network security groups and you may establish an nsg, apply it to the subnet nic or the private endpoint nic, and use it to filter inbound rules just like any other network security group (nsg).

* This appears to be unavailable in the public preview.
* It is not possible to apply an nsg to the nic.

Private endpoints are unaffected by applying an nsg to the subnet.

Use network security groups for outbound traffic: you may restrict outgoing traffic to your private endpoints from your sources: when it comes to securing access from a destination aspect, it's best to filter at the destination rather than at the source, which is supported but inconvenient. (the image displays a rule that applies to the *sqlclient* vm and prevents access to the private ip of the private endpoint.)

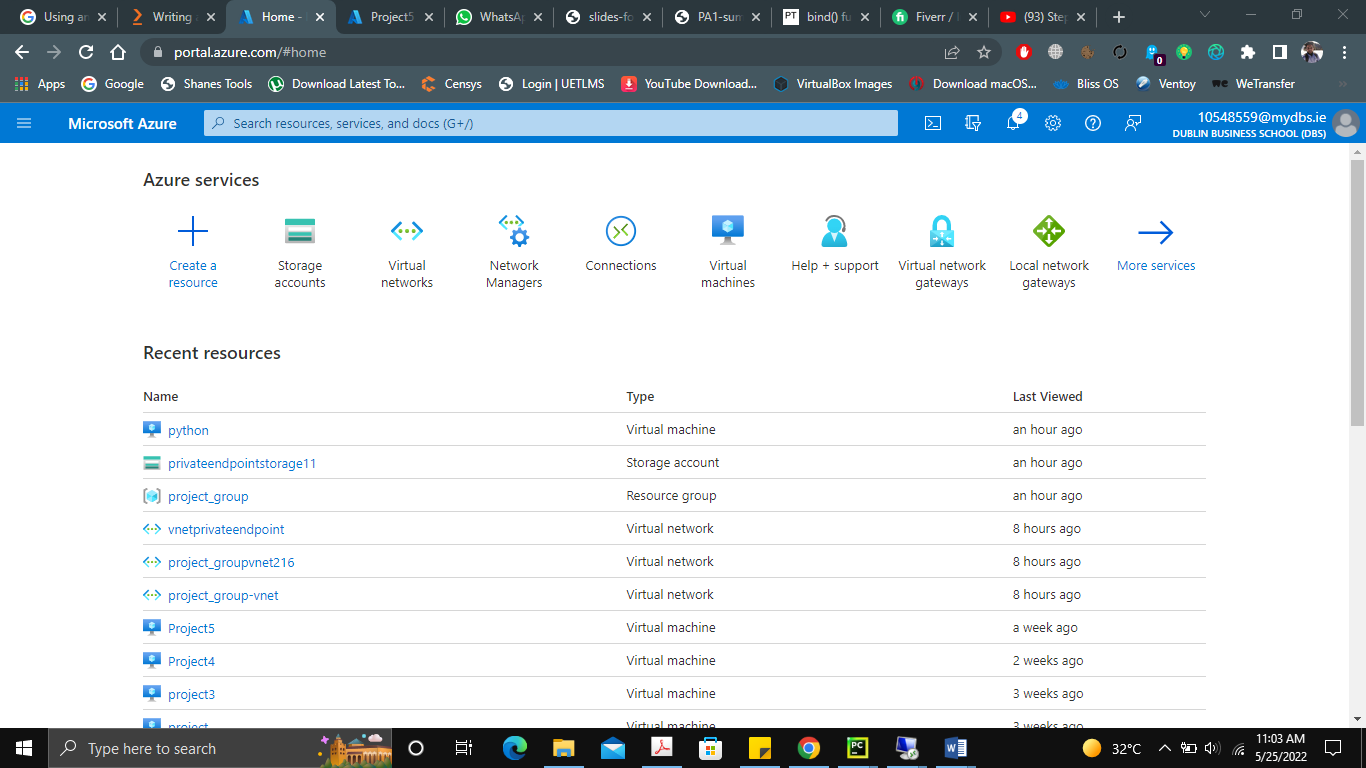


Since the ip address of the private endpoint is within your vnet, you can filter access to it on your perimeter firewalls, like azure firewall or your own firewall [7]

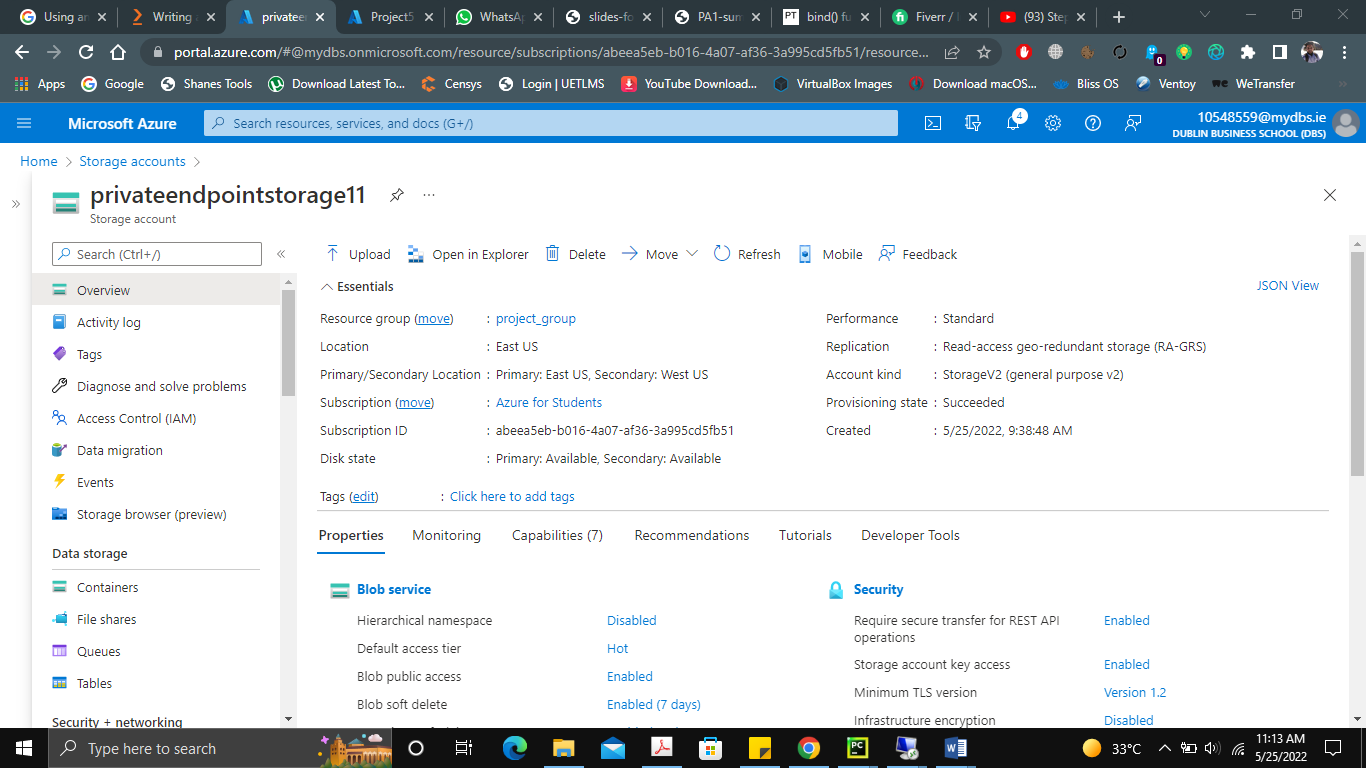
**Implementation details**

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

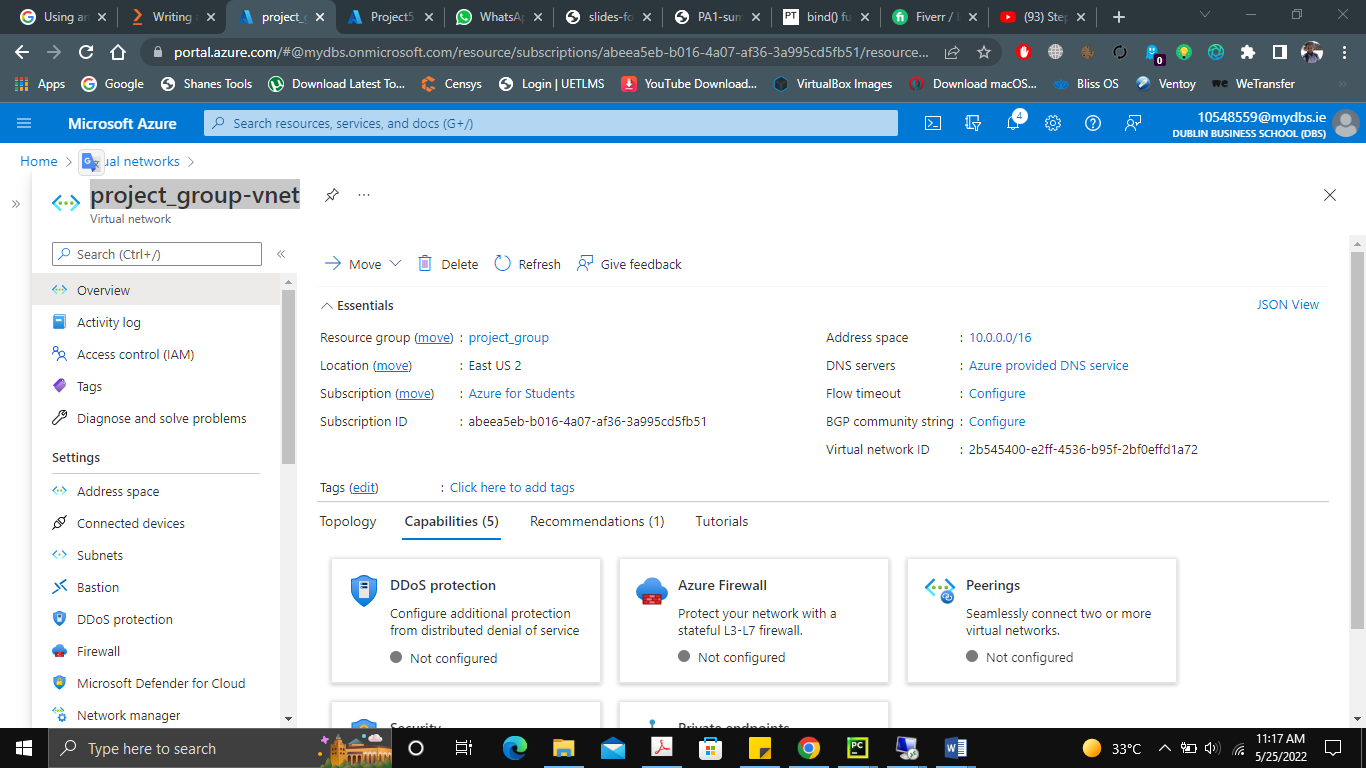
1. Login to azure account and make a storage account, vnet, private endpoint and private dns zone to secure our network.



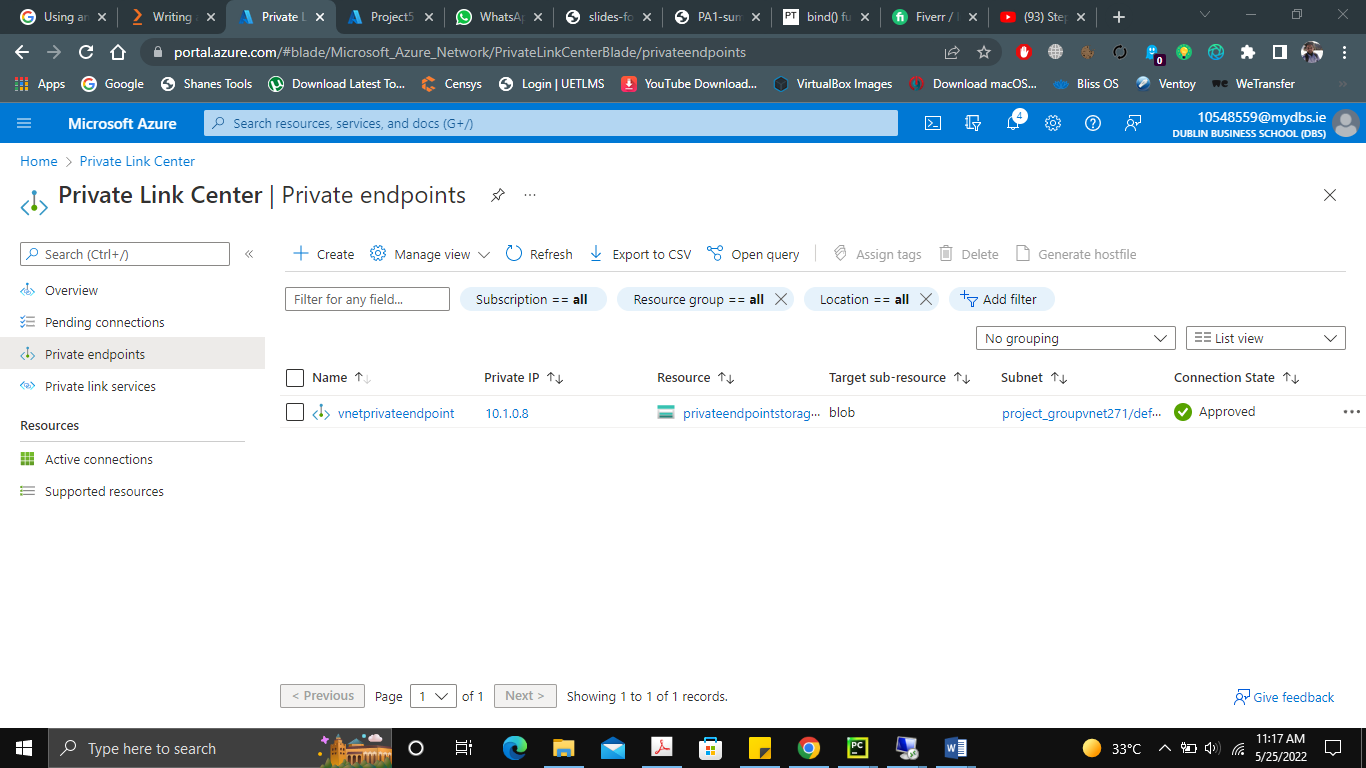
1. We have to successfully create storage account in virtual network which is created before and add that network interface in storage account to secure our network and save file securely. We create a container in storage account and upload and download file from this container. A container, like a directory in a file system, arranges a collection of blobs. A container can hold an unlimited amount of blobs, and a storage account can have an unlimited number of containers. The container name must be written in lowercase letters.



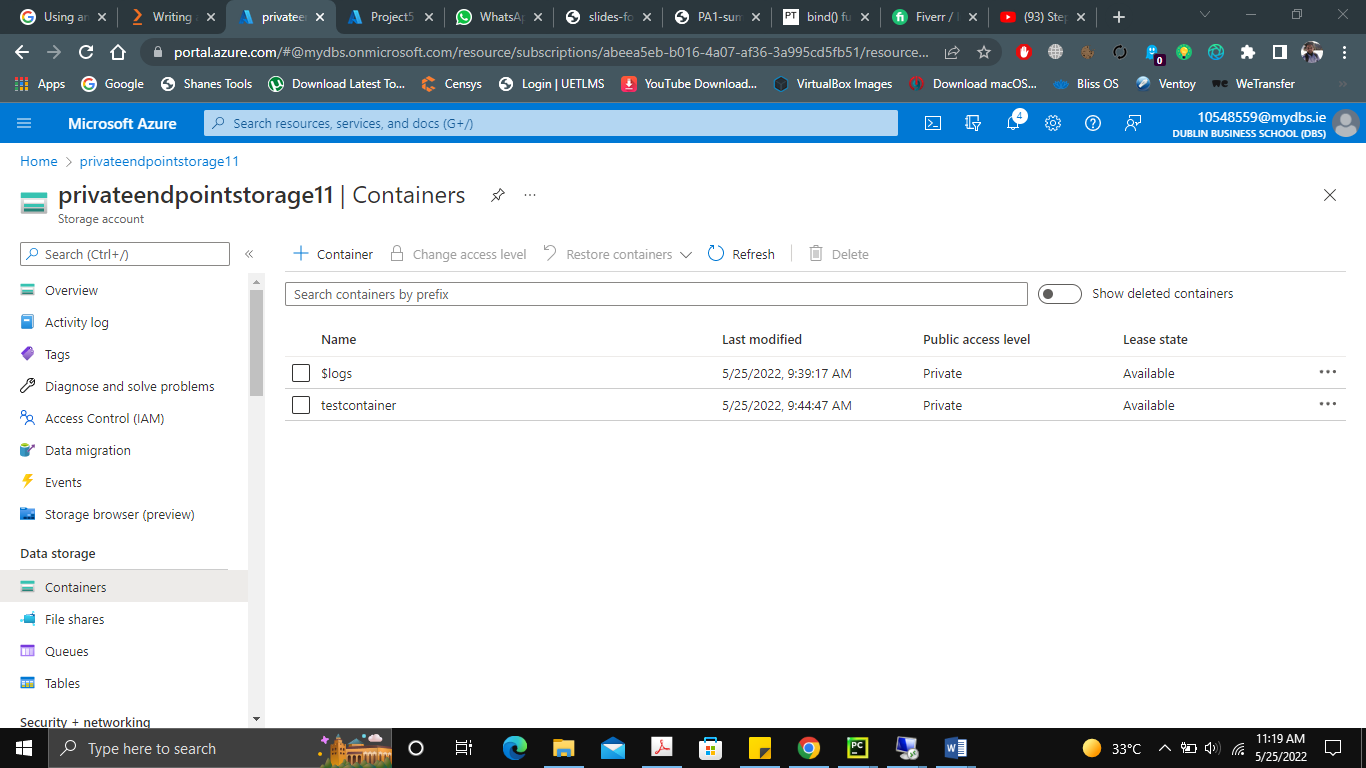
1. Now we create a vent name of project *group-vnet*. The main purpose of virtual network is to secure our network and all the machines and storage account on same network and this network is different from public network. A private endpoint is a network interface that uses a virtual network's private ip address. This network interface links us to a service enabled by azure private link in a private and secure manner. We are introducing the service into our virtual network by activating a private endpoint.



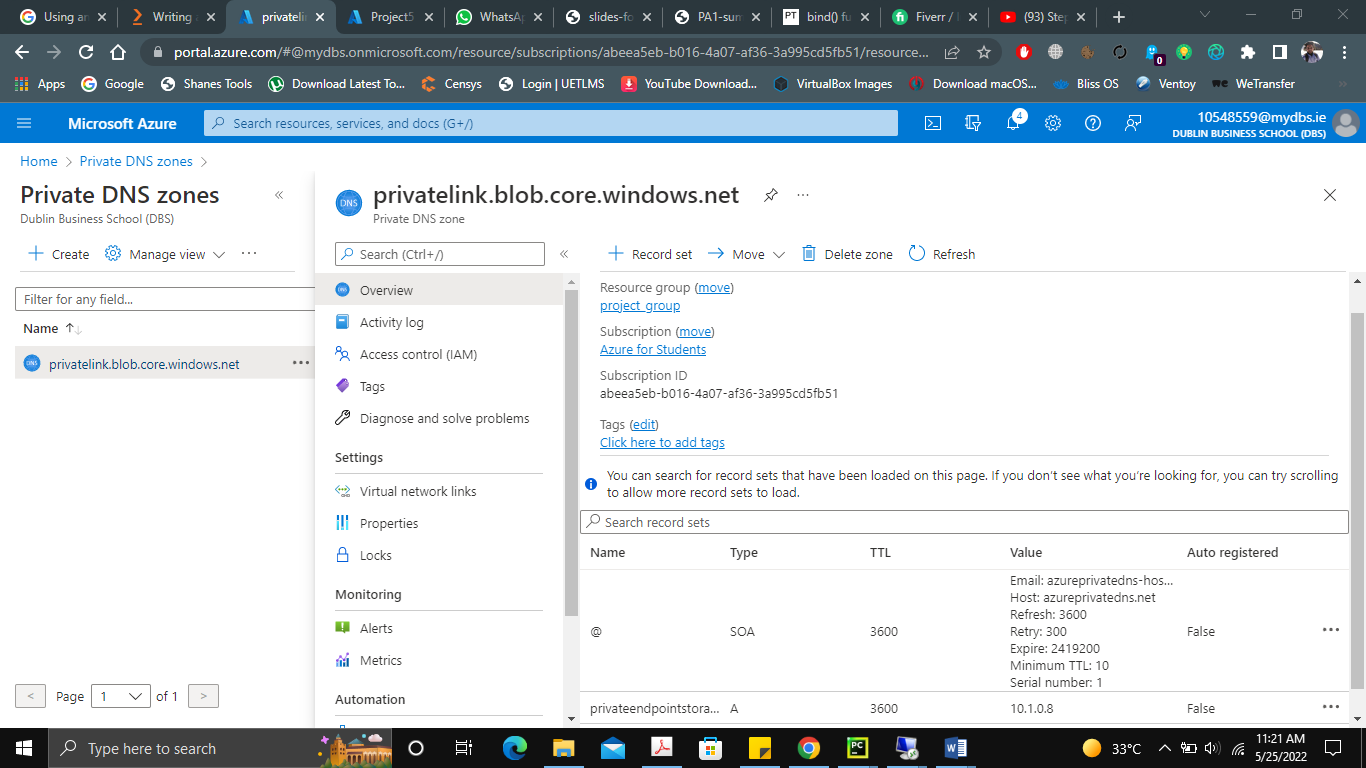
1. Now. We will create a private end point to create end to end protection. A private endpoint in our virtual network is a unique network interface for an azure service (vnet). When we build a private endpoint for our storage account, it allows clients on our vnet to connect securely to our storage.



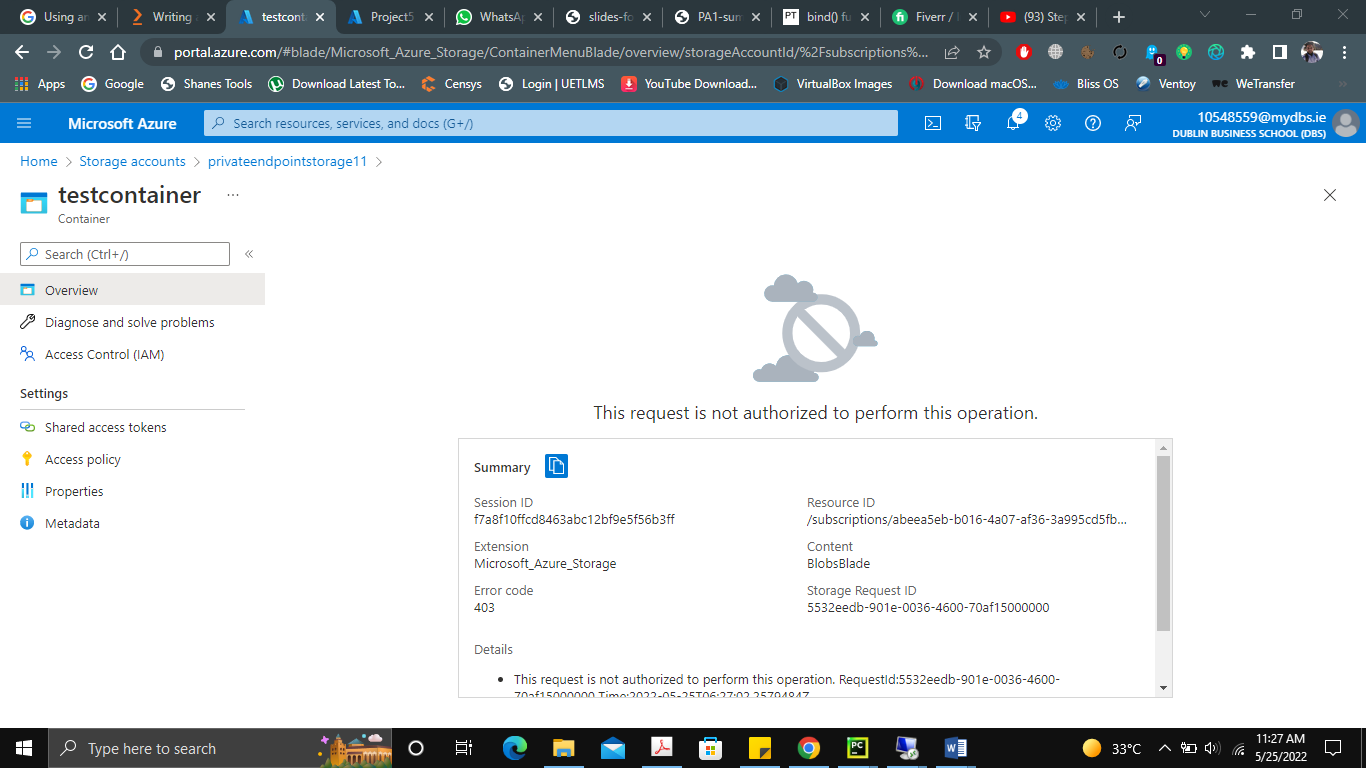
1. We will make a container to share a file and this container cannot access the private network from outside. We use a blob feature. Blob storage is a microsoft azure feature that allows developers to store unstructured data in the cloud. This information, which might include audio, video, and text, is accessible from anywhere on the planet. Blobs are organized into "containers" that are associated with certain user accounts.



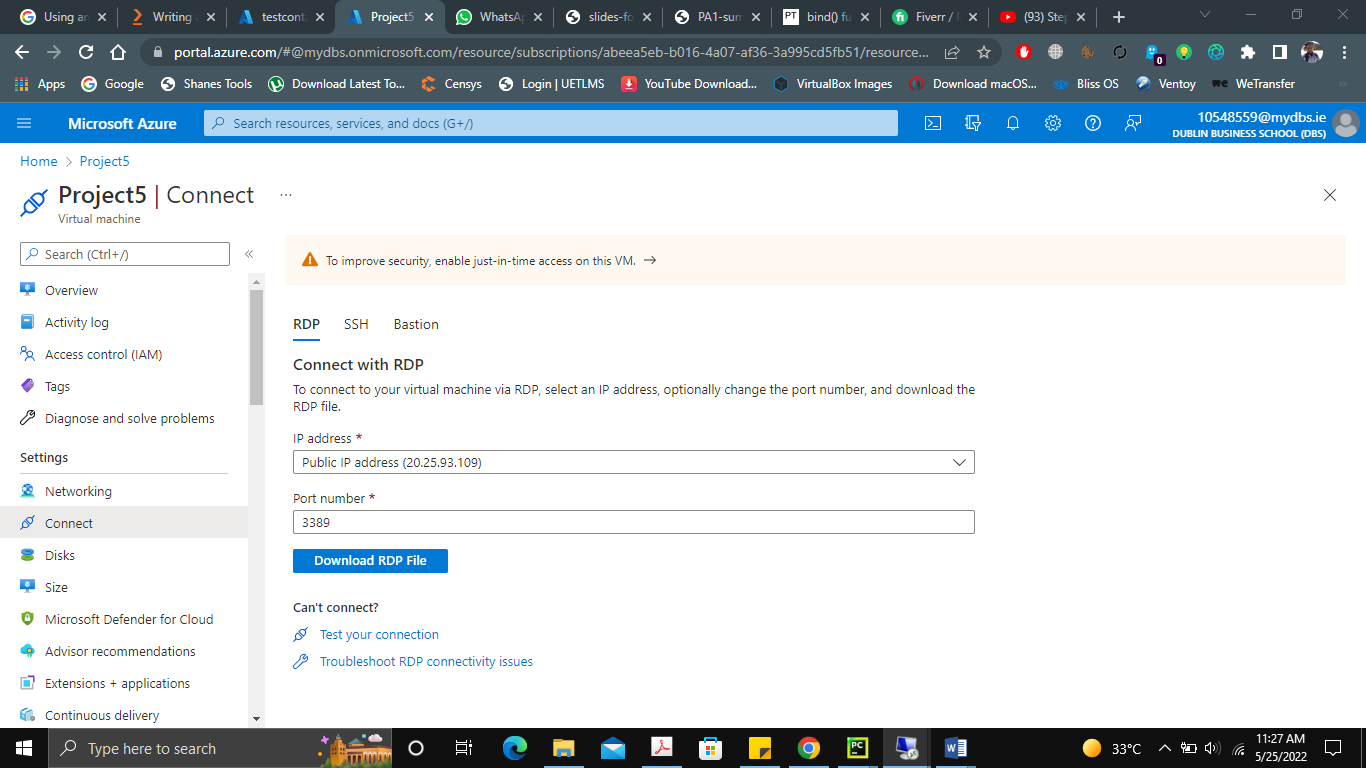
1. Now, we will create a private dns zone for all the traffic of virtual network which will pass from this dns zone. Any other machine, connected to this private network but not a part of this zone, cannot access the storage account. Without the need for a proprietary dns solution, azure private dns delivers a dependable and secure dns service for managing and resolving domain names in a virtual network. We may utilize our own unique domain names instead of the azure-provided domains available today by employing private dns zones.



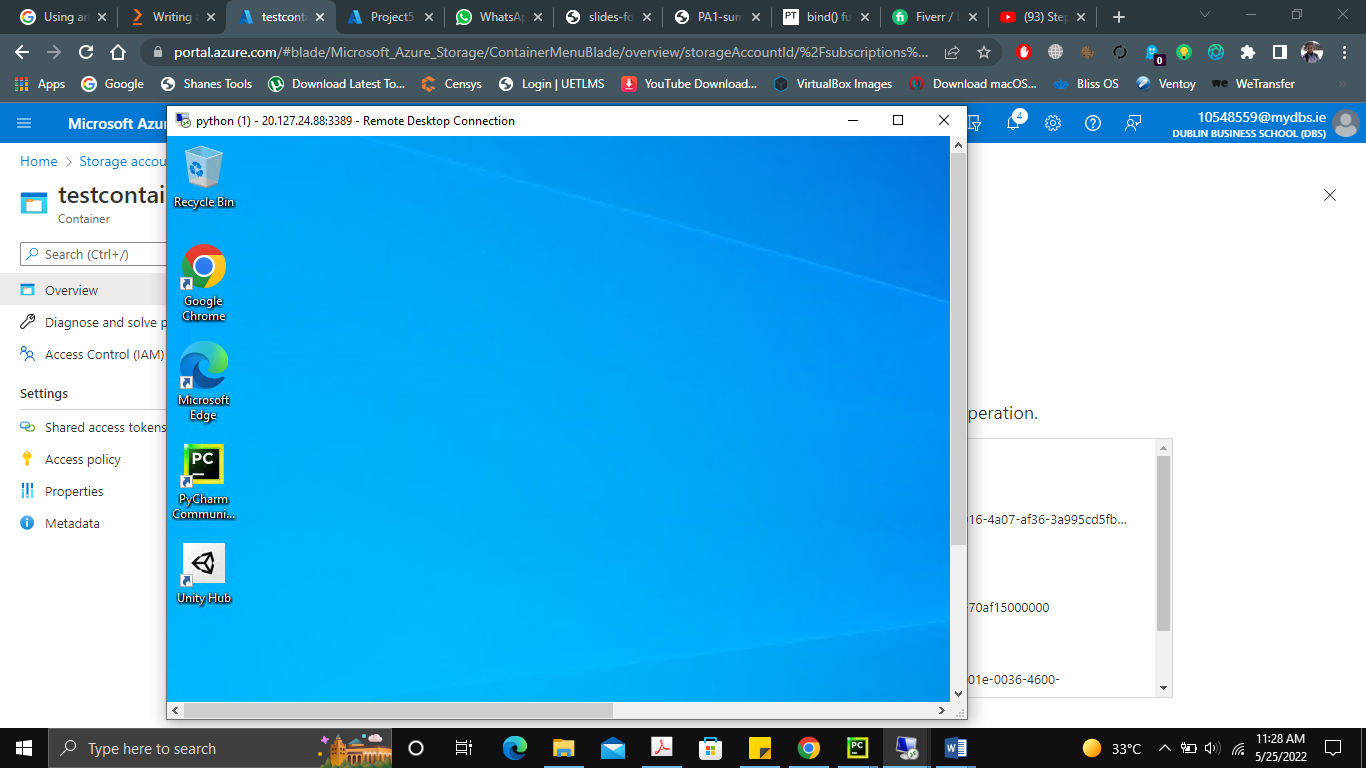
1. Now, container cannot be accessible from outside of the private network. Due to addition of some rules during the creation of storage account, now container can only be accessible from private end point.



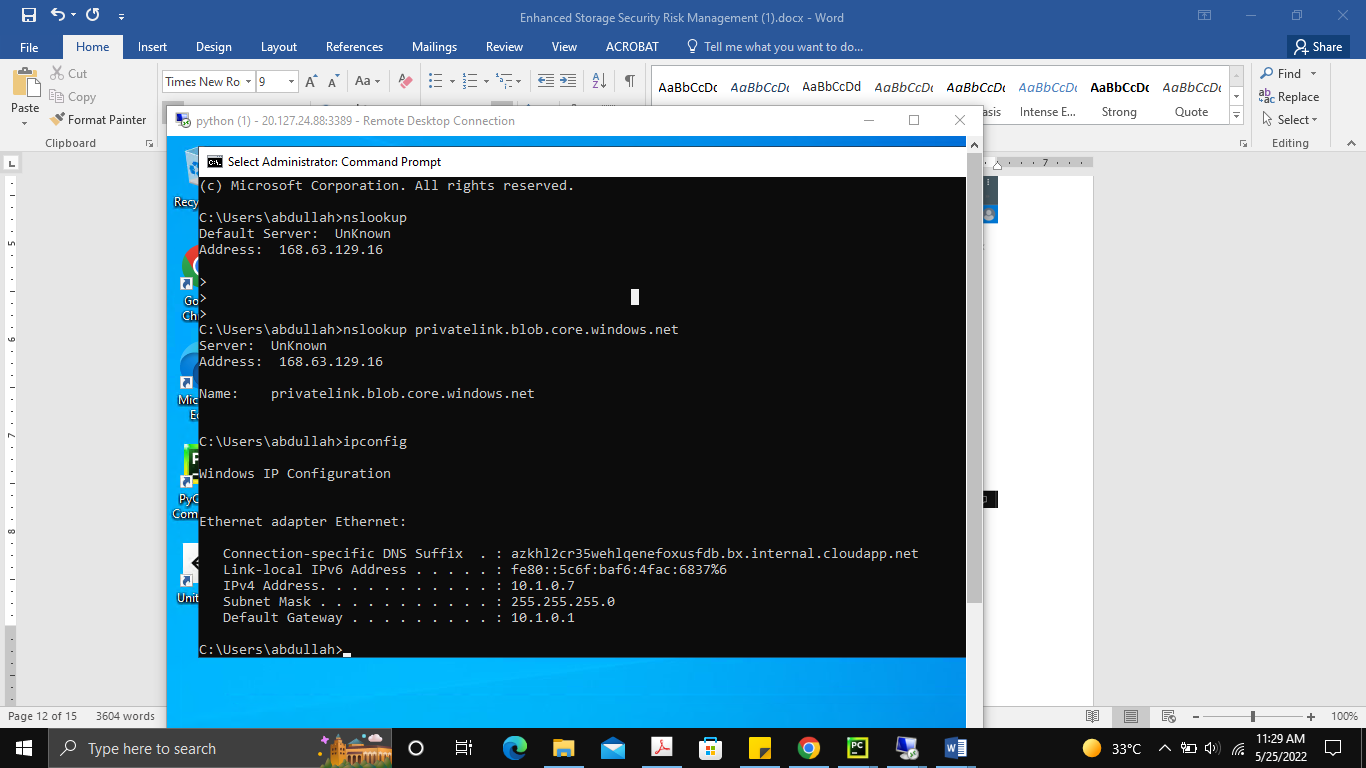
1. Create a virtual machine which is window 10 and this machine is connected with end point virtual network.



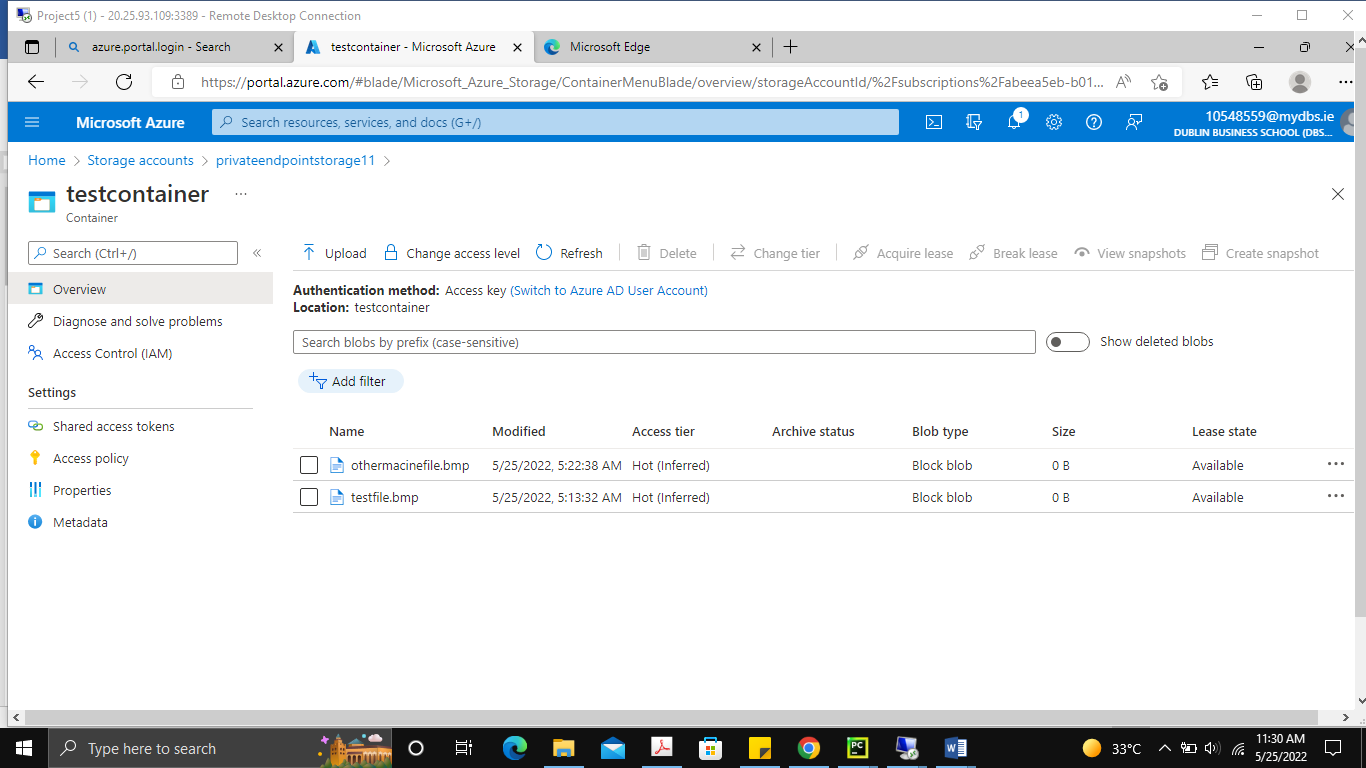
1. Successfully created a virtual machine and we can use for file sharing.



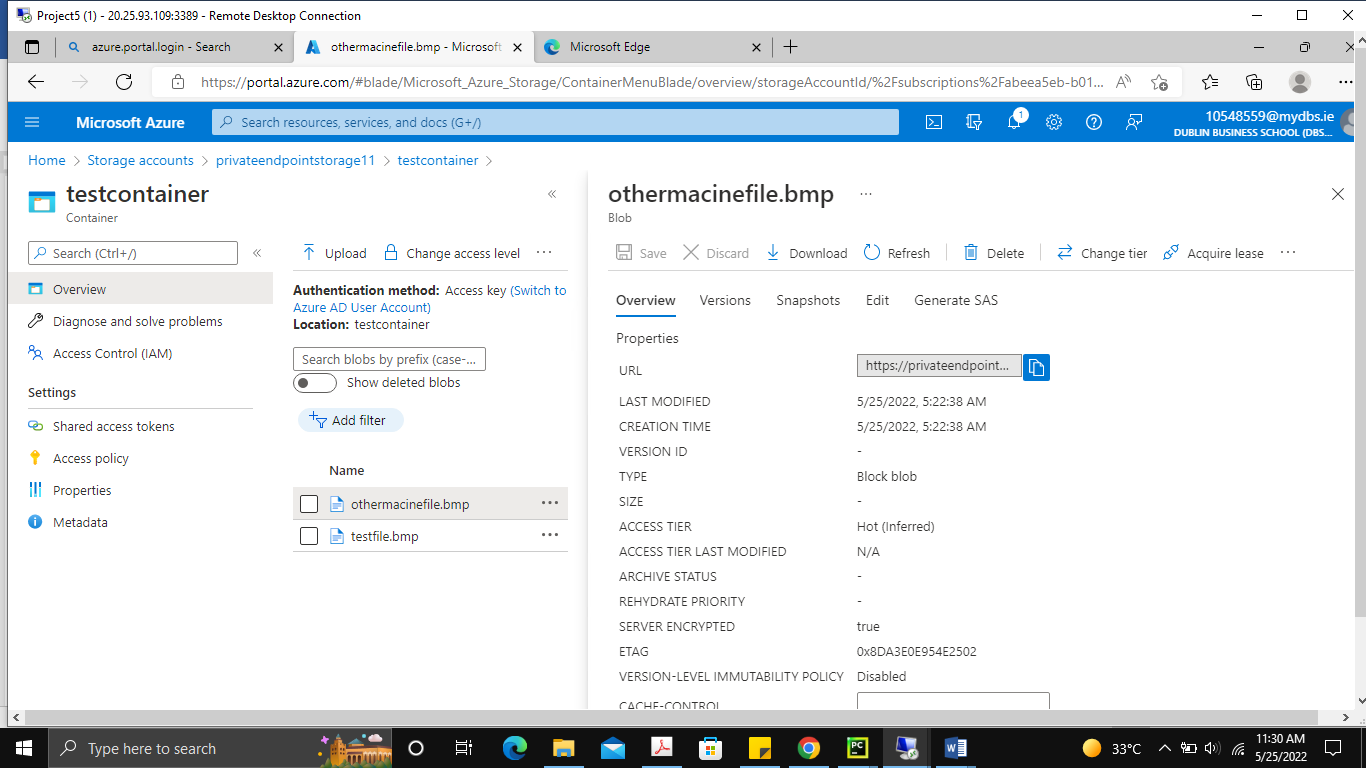
1. The machine is on a private network where traffic passes from the vnet private endpoint. Now check the domain name traffic is passing from the private endpoint



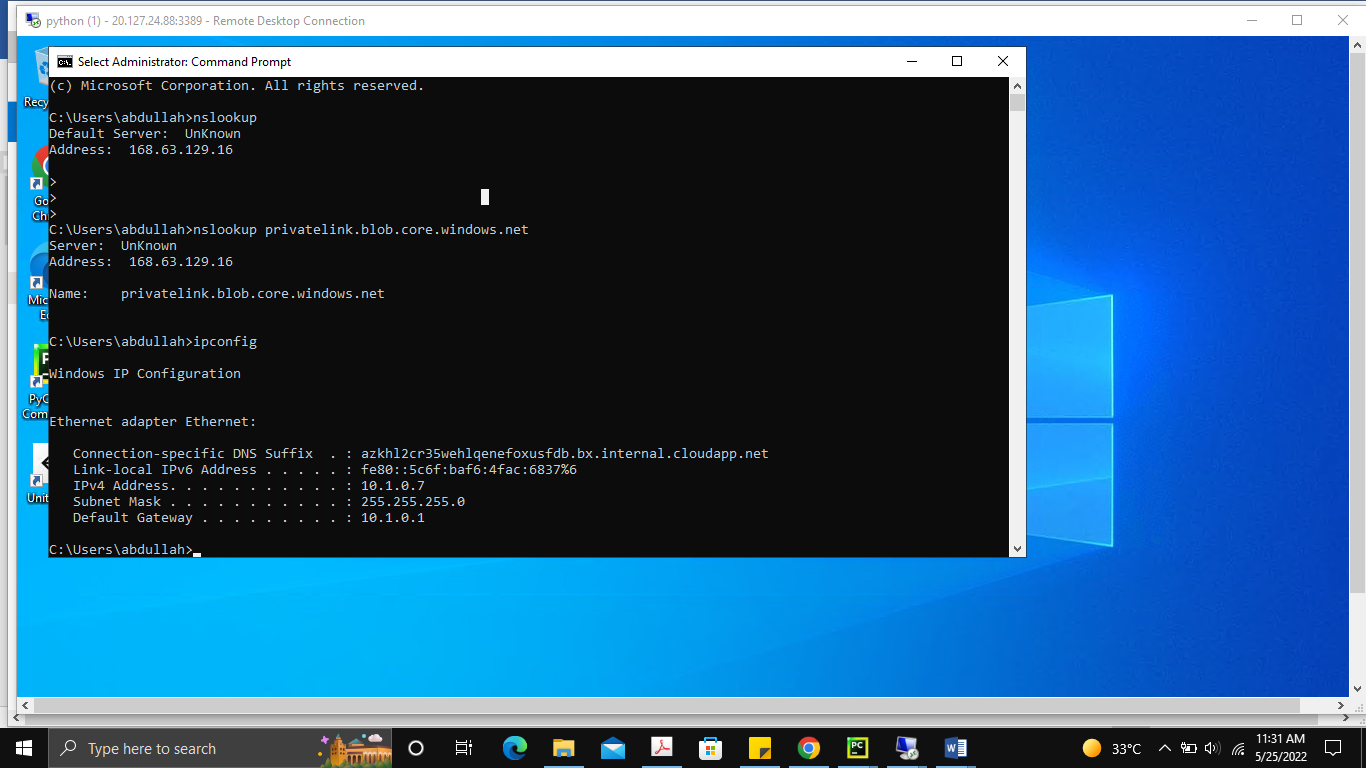
1. The container is now accessible on the project5 vm machine. Machine traffic goes to a private network and we are able to share a file via container which is only accessible via a remote endpoint machine. We can see the file which is uploaded and download the file from each other machine



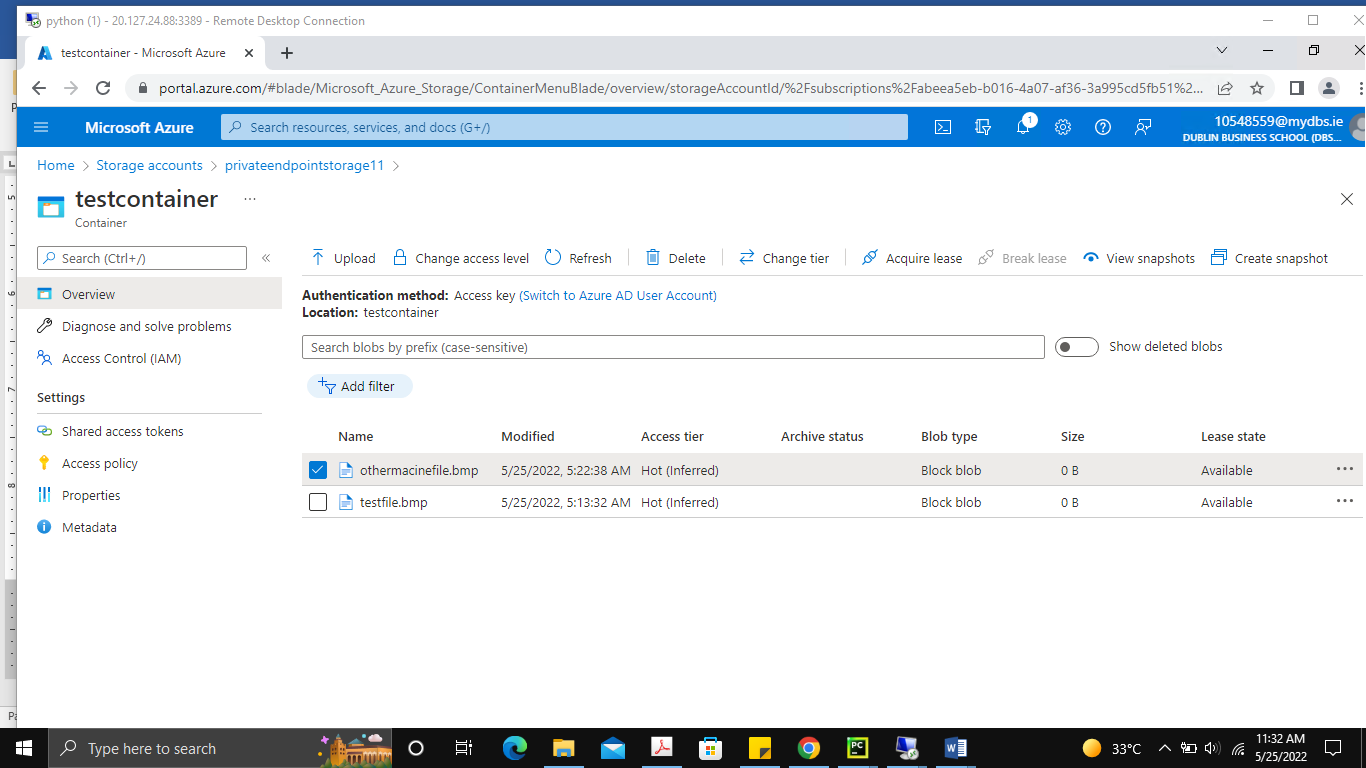
1. We upload a file whose name is *othermachinefile.bmp* file uploaded successfully and we can download and edit the file from another private end machine



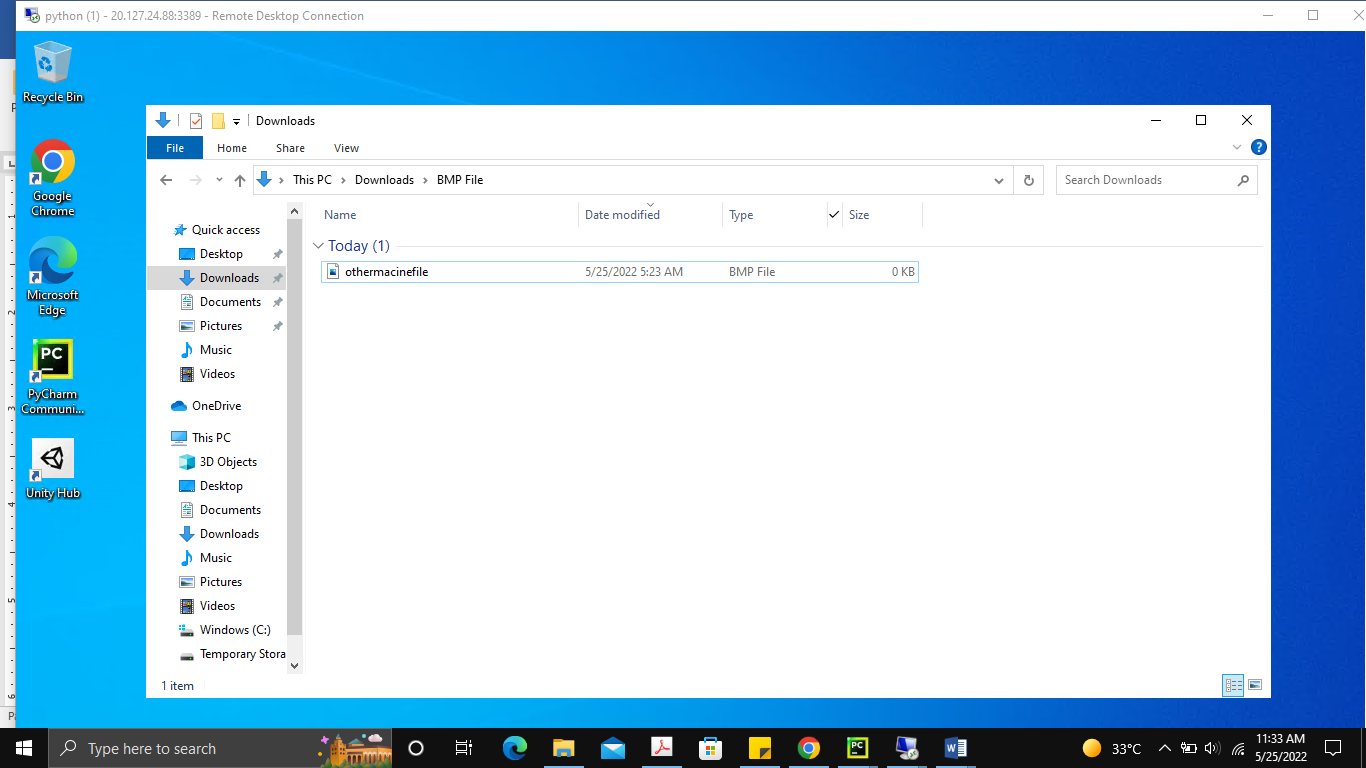
1. Now, we will create a second machine and the traffic of this machine will go to private network. We can check by applying a command *nsloopup* and address our dns private zone which is (privatelink.blob.core.windows.net) and we can see that the traffic is successfully passed.



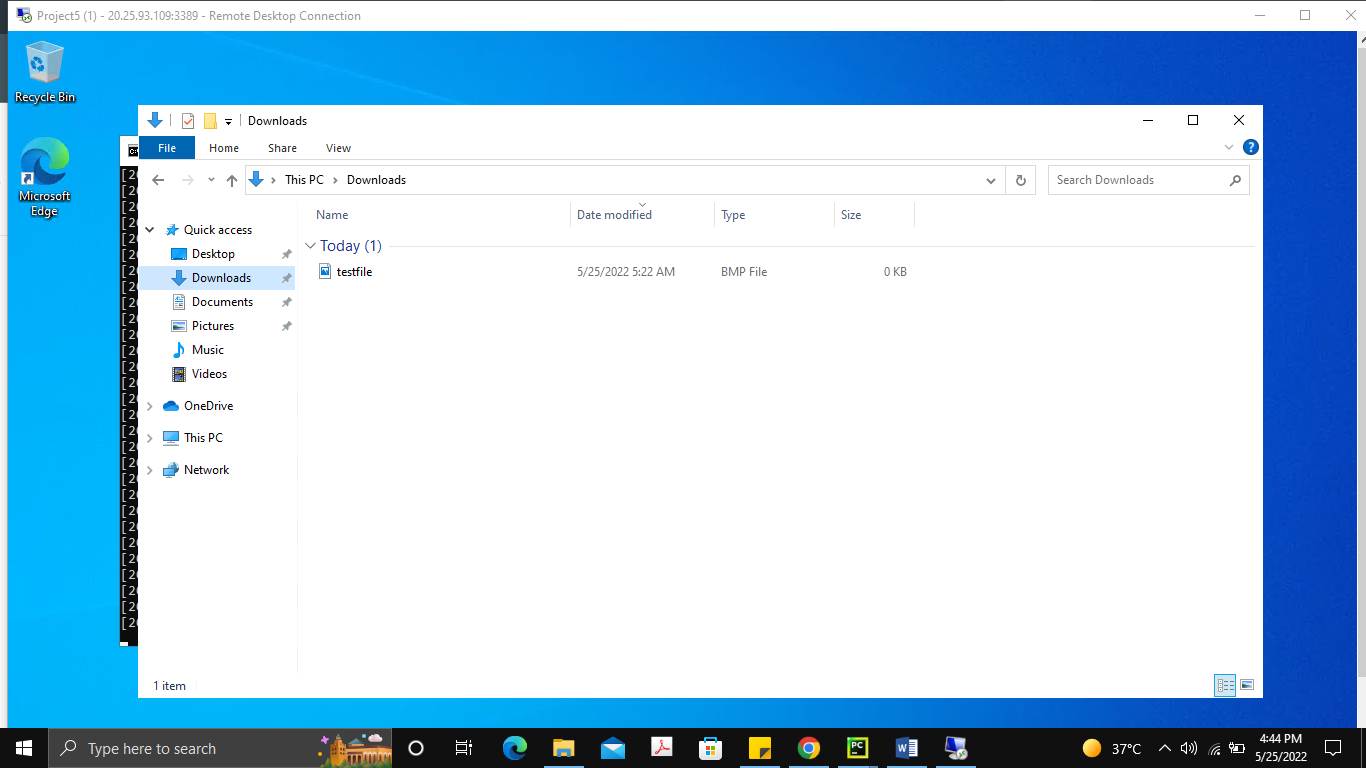
1. File is also uploaded successfully in our private end point container. We can see file name is *testfile.bmp,* we can edit, delete, and download a file easily.



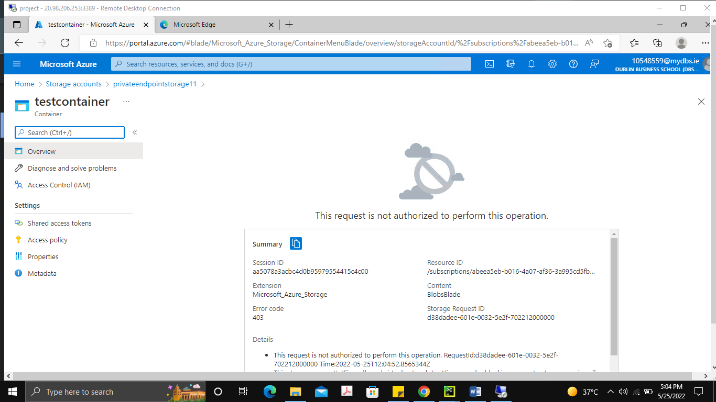
1. File is download on first machine and we can see that file and share where we want.



1. File is download on second machine and we can see file and share where we want.



# Now check whether the container is accessible or not after the creation of a new virtual machine. We can check this is not accessible from this machine and hence our enhanced storage security risk management is established.



**Feature work**

In this project we are fixing storage account problems, for example, we have a company that has a file storage server and this server is connected to many networks. If we are connected to a network, then we can switch from one network to another network easily. For example, my system is connected to a single network which is 192.168.3.0 (the public network of the company) and the private network of that company is 10.70.0.1 now i can easily switch between these two networks both have their firewalls but both are connected to a single router. In this way, a person who is not a part of the admin can easily access file storage servers and can retrieve important information. So, to fix this problem we switch from non-cloud to cloud and use the private endpoint zone

You can also use Private DNS zones if you have a route to the internet on azure. Some of your internal networks can route to the internet from another point (for example from on-premises datacenter), it does not matter. When having a full name resolution on Azure services one can have the same benefits. When a private endpoint is created we can have an automatic DNS record created on the Private DNS zone and it works.

You have your own DNS Servers in this case that are a Windows Server Active Directory integrated DNS which will be used for name resolving. Install DNS servers also to the cloud to get the name resolving working. Your DNS traffic is not routed to the internet (and Private DNS Zone) from Azure without some server that acts as DNS relay in vnet. Create a conditional forwarder to on-premises DNS for your public DNS-zones (privatelink.blob.core.windows.net) and point those towards your Azure VM which is a DNS relay in cloud when you have a relay server. Put forwarders also for the Azure DNS server to point Azure’s public DNS services in (IP **ANY** ). For example you can use couple of domain controllers in cloud to act as a DNS relay.

The DNS request which is asked from Azure DNS Services must be routed from Azure Virtual Network or else it won’t be allowed to Azure Private DNS zones. I suggest for the lower latencies that you should use for forwarder your ISP provided DNS in on-premises DNS servers and Azure public DNS service in Azure based DNS servers. You should ensure that when any VM tries reaching Azure DNS service 168.63.129.16 (from on-premises) traffic **should be routed**from Azure Virtual Network by the DNS relay. This can be done using route table in Azure, on-premises firewall or anything that is being used as routing device in on-premises.

**Conclusion**

The dns framework of the internet works similar as telephone directory, deals between names and phone numbers. Dns servers deal with the interpretation of domain names and their corresponding ips addresses, controls resolution of ip addresses and their domain names when we type domain in browser.

Finally, we can share a file using azure dns and a private endpoint since azure file shares support industry-standard *server message block (smb) protocol and the network file system (nfs)* protocols, you can seamlessly replace your on-premises file shares with azure file shares without fear of application compatibility issues. Private link gives a safe method for relocating jobs to azure. Insurance against information spillage: a private endpoint is planned for a case of a paas asset rather than the whole assistance.

Private endpoints seem fantastic, and we've been hoping for this functionality from microsoft azure for years to block our paas services from being exposed on the internet.

The most challenging element of the implementation was explaining to security personnel that we had a public fqdn that would respond to private ip addresses.

Azure infrastructure has evolved into private endpoints. You should carefully examine if your firm requires upfront configuration work and continuing service payment for use. For example, if you need to limit all internet traffic to service while allowing on-premises traffic to access it, or if you need to safeguard particular sub-resources in your virtual network, azure now has private endpoints.

**The chosen cipher used in the *domain name system (dns)* is explained below**.

Acl access control list

Ad authenticated data

Arp address resolution protocol

Api application programming interface

Ca certificate authority

Css cascading style sheets

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

Fqdn fully qualified domain name

Html hypertext markup language

Ip internet protocol

Isp internet service provider

It information technology

Itl information technology laboratory

Ict information and communications technology

Ivn identical virtual network

Lan local area network

Mac message authentication code

Md message digest

Mx mail exchanger

Nist national institute of standards and technology

Nic network interface card

Nsec3 hashed next secure

Ntp network time protocol

Nsg network security group

Os operating system

Otp one time password

Pki public key infrastructure

Pe personal endpoint

Sql structured query language

Sas shared admittance signature

Smb server message block

Tcp transference control protocol

# References

|  |  |
| --- | --- |
| [1] | R. E. A. R. Bush, "clarifications to the dns specification," *clarifications to the dns specification,* p. 125, 1997. |
| [2] | P. Mockapetris, "domain names - concepts and facilities," *domain names - concepts and facilities,* november 1987. |
| [3] | D. Barr, "common dns operational and configuration errors," *common dns operational and configuration errors,* p. 20, feb 1996. |
| [4] | A. A. R. Austin, "threat analysis of the domain name system (dns)," *threat analysis of the domain name system (dns),* p. 20, august 2004. |
| [5] | P. Mockapetris, "domain names - implementation and specification," *domain names - implementation and specification,* p. 25, november 1987. |
| [6] | J. D. A. F. Neves, "preventing use of recursive nameservers in reflector attacks," *preventing use of recursive nameservers in reflector attacks,* p. 30, october 2008. |
| [7] | S. Farhat, "https://buildwindows.wordpress.com/," 2020. [online]. Available: https://buildwindows.wordpress.com/about/. |
| [8] | T. Redkar, "windows azure platform," *tony guidici,* 2011. |