# Manage identity and access

## Resources and an Identity provider


As a user you need to access an application.

As a user we are first asked to perform the act of authentication.

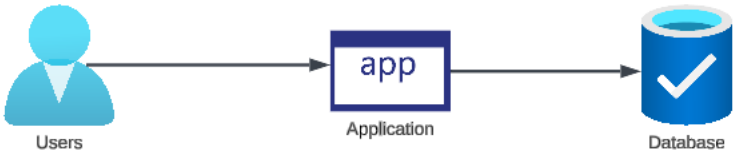
Here we might provide a user name and password. This allows the application to verify our identity.


The application would need to maintain a data store of identities. The application would compare the user name and password with the identity information stored in the database.

Here the application need to maintain the database when it comes to storing user identities.

The next step after authentication is authorization. Here the user needs to have permissions to access a resource.

Let's say that the application provides online courses. And now the user wants to access a course. Here the course is a resource. Does the user have access to the course? Has the user paid for the course and hence can they access the course?



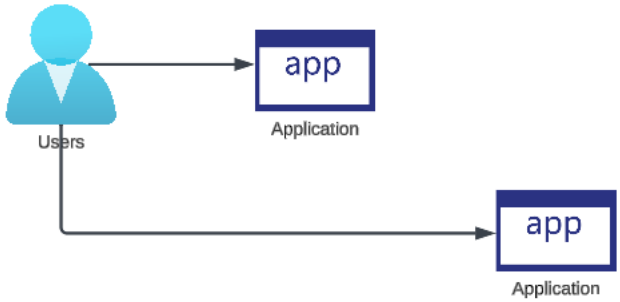

Here again the application would need to have a data store in place to store the permission information. From there the application can determine if the user has the required access or not.

Nowdays applications can make use of external identity providers for authentication and authorization.

This reduces the burden for applications to maintain a data store of credential information.

And there is so much more that an Identify provider can provide in terms of functionality.


The user can be requested for an additional authentication method in addition to the user name and password - This is known as Multi-Factor Authentication.




**An identity provider can perform Single-Sign on. Here the user logs into one application. That same credentials can then be passed onto logging into another application.**

**Identity providers can also provide reporting and auditing - See who has logged in, what resources were accessed.**

# Using Azure as a cloud platform

**Azure as a cloud platform.**

app

Application

**Let's say that a company wants to host a set of applications.**

**Buy physical servers**

**Buy storage**

**Setup a network**

**All of this costs money, there is an initial investment that the company needs to undertake.**

Large companies will normally setup data centers. These centers contain a number of servers, storage devices, racks, cooling devices etc.

All of this is an investment from the company.

With a cloud platform such as Azure, we can don't need to have an initial investment on resources.


We can host applications on a service known as the Virtual Machine service.

This is a compute service that allows you to host virtual machines on the Azure cloud network.

Here we only pay for the running cost of the machine. There is no initial investment to be made.

Azure provides more than 200 services across the board that can be used for hosting applications.

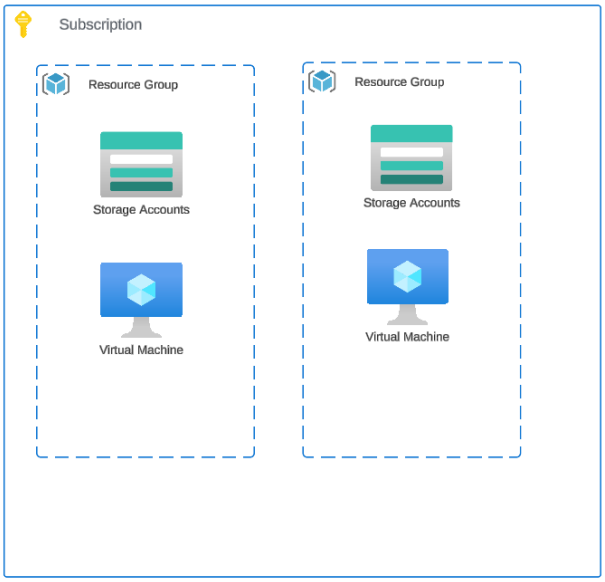
## Important basic concepts with Azure

We need to understand the basic concepts when it comes to deploying resources on Azure. Because that's what need to secure.

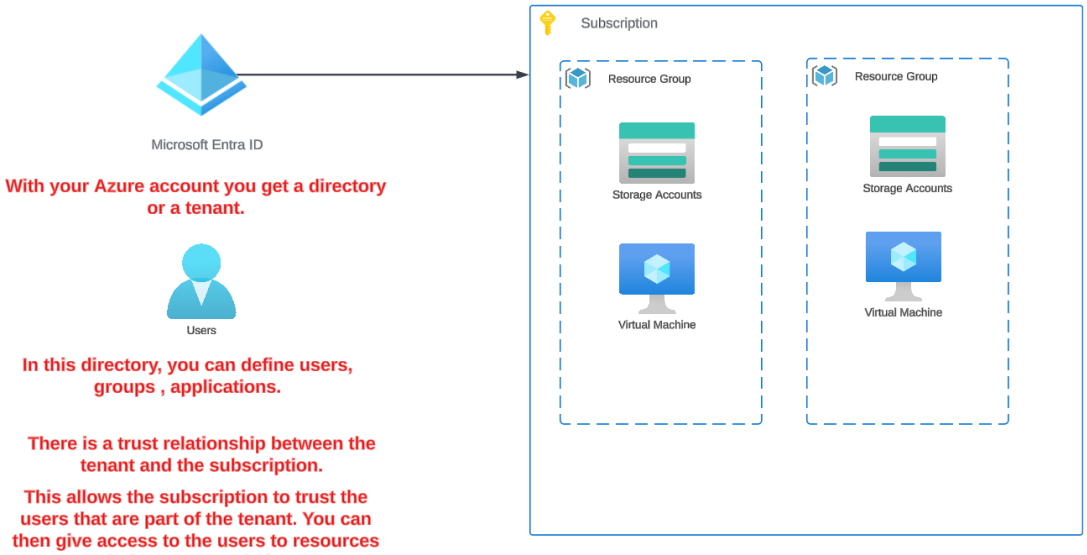
When we create an Azure account, we get a subscription. This is used for billing purposes.

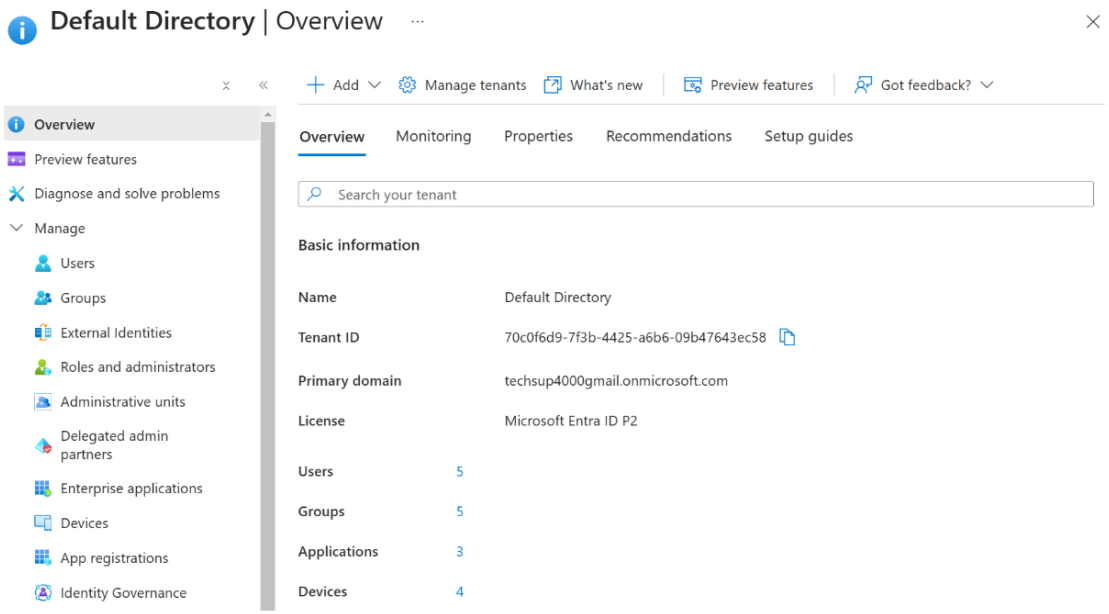
Resource groups are used to group resources together. Its a logical grouping of resources.

We can then deploy resources on Azure based on services that Azure provides.

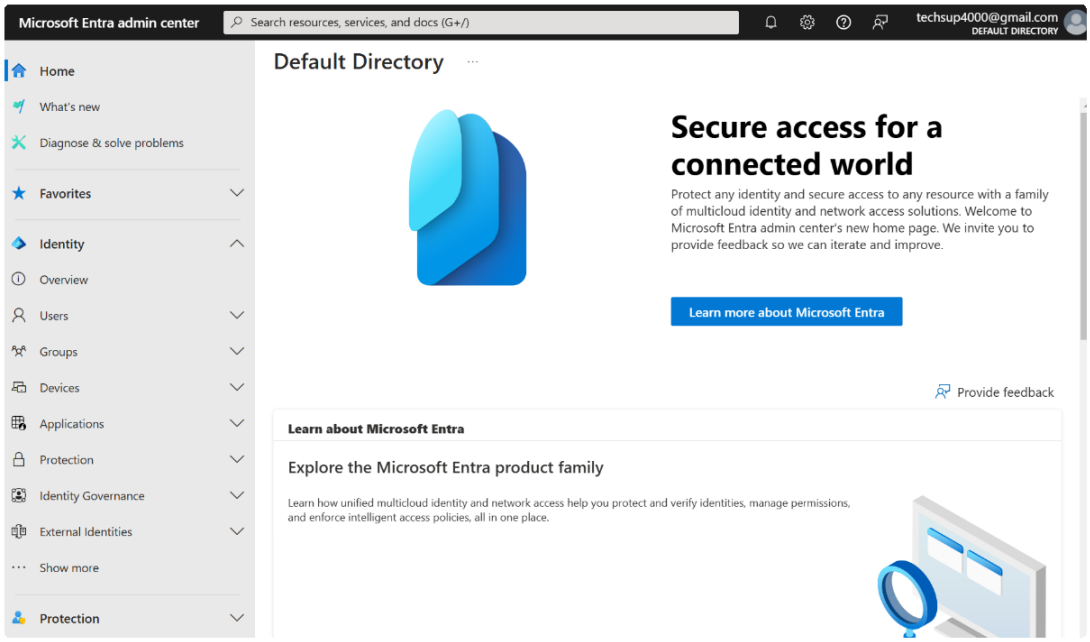


# Microsoft Entra ID - The big picture

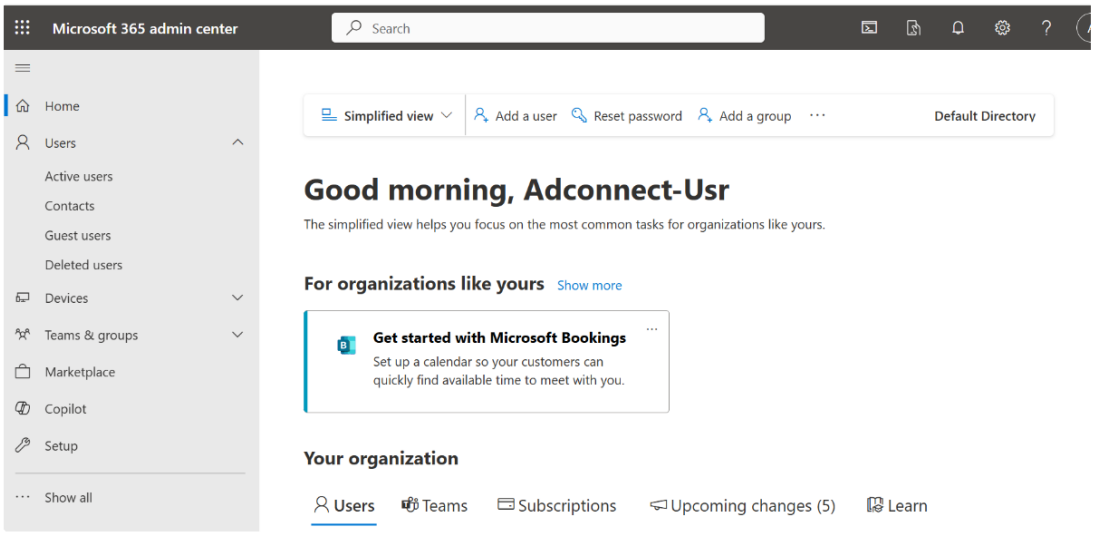


Now we can access Microsoft Entra ID in Azure.




We can also use Microsoft Entra Admin center to access Microsoft Entra ID.
Microsoft Entra is a suite of identity-based services.




We can also manage the users , groups from Microsoft 365 Admin center.

Remember that Microsoft Entra ID is the identity provider for many services.
But no matter which User interface you use, in the end you work with the same backend service that works with your tenant/directory.

# Lab - Creating a group in Microsoft Entra ID

## Let's start working with Azure resources


**This is a compute service that allows you to host virtual machines on the Azure cloud network.**

**What is involved in the deployment of a virtual machine.**


What is the size of virtual machine - number of vCPU's, RAM

What is the number and size of the disks you want allocated for the virtual machine.

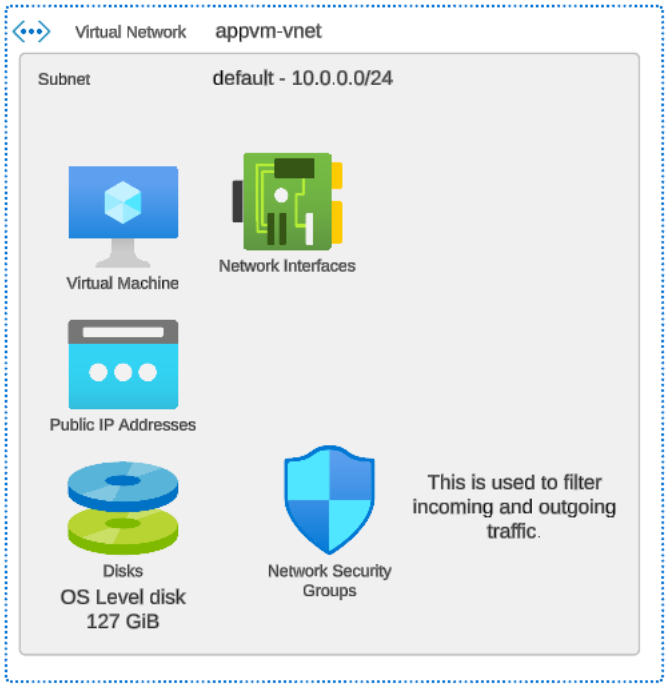

What is the underlying operating system - Ubuntu, Windows Server.

The network details for the virtual machine.

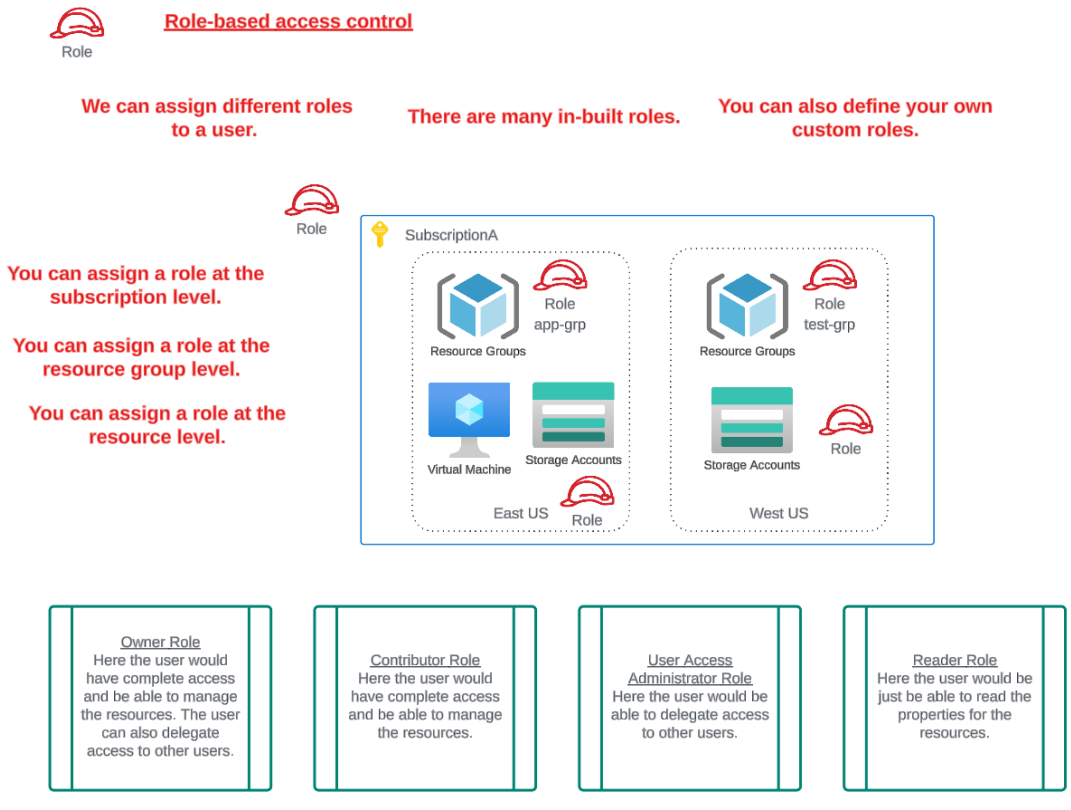
**Azure Marketplace - This has in-built templates that you can choose from. For example , there is a template for Ubuntu Server 22.04. If you choose this template for your machine, it will create for you a virtual machine based on that operating system.**

**You can choose a virtual machine size - This will allocate the required hardware resources for your machine.**

**Apart from the virtual machine itself, there are other resources created on the Azure platform to complement the Azure virtual machine.**

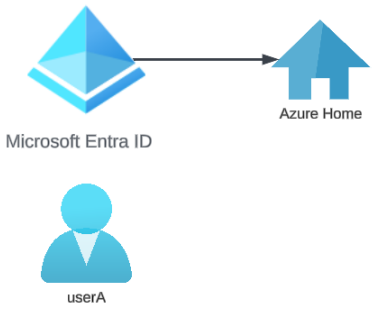


# So what is Role-based access control




| Owner Role | Contributor Role | User Access Administrator Role | Reader Role |
|---|---|---|---|
| Here the user would have complete access and be able to manage the resources. The user can also delegate access to other users. | Here the user would have complete access and be able to manage the resources. | Here the user would be able to delegate access to other users. | Here the user would be just be able to read the properties for the resources. |

# Lab - Role-based assignments - Resource level



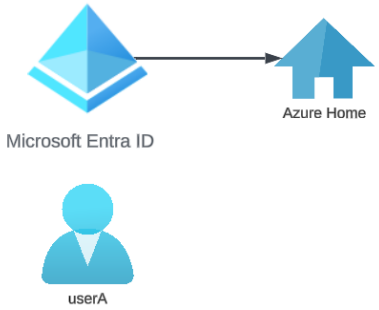




**Let's give UserA the reader role to the Azure virtual machine.**


**We will notice that we cannot see the other aspects of the virtual machine such as the virtual network etc.**

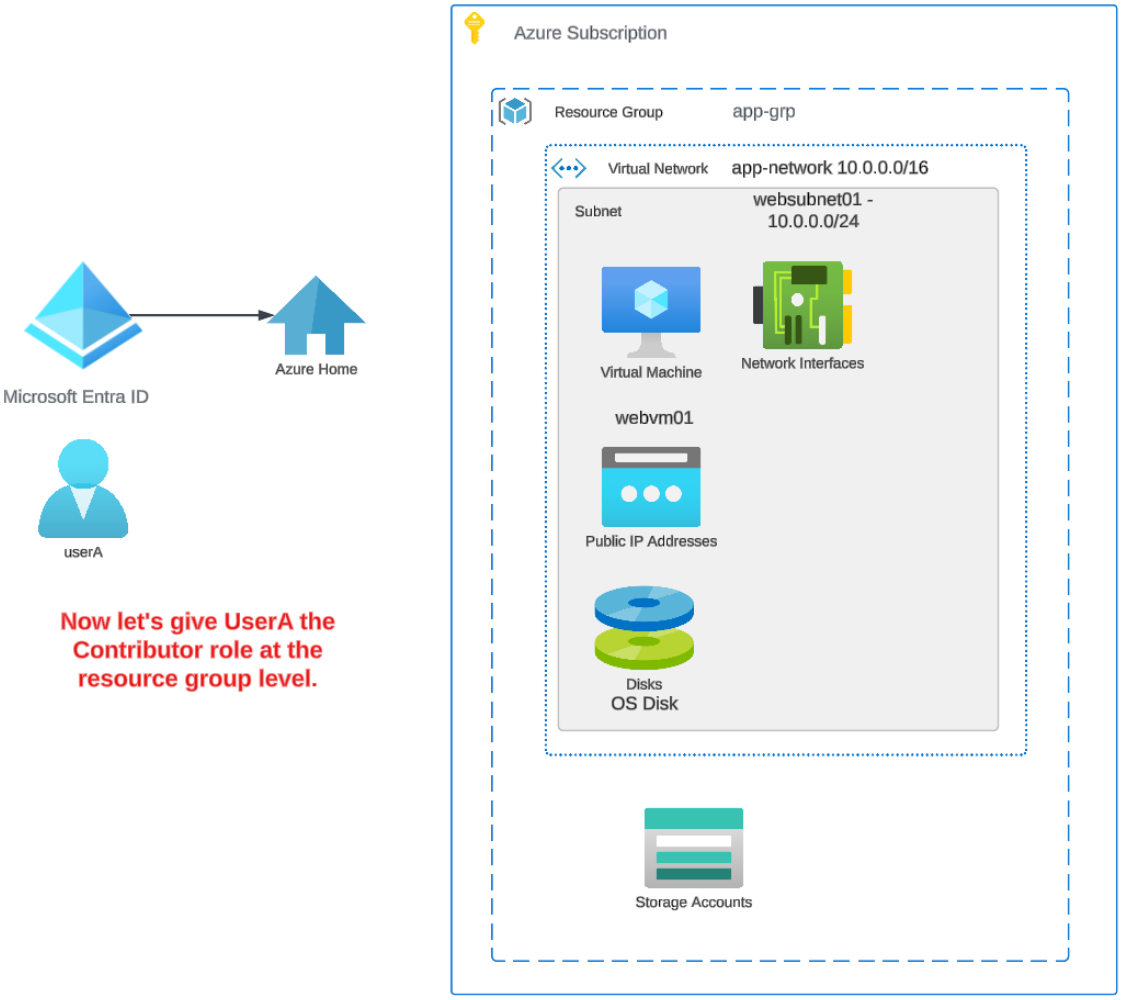
# Lab - Role-based assignments - Resource group level




**Now let's give UserA the Reader role at the resource group level.**


**Well now we can view the other resources but can be stop the virtual machine?**

# Lab - Role-based assignments - Contributor Role

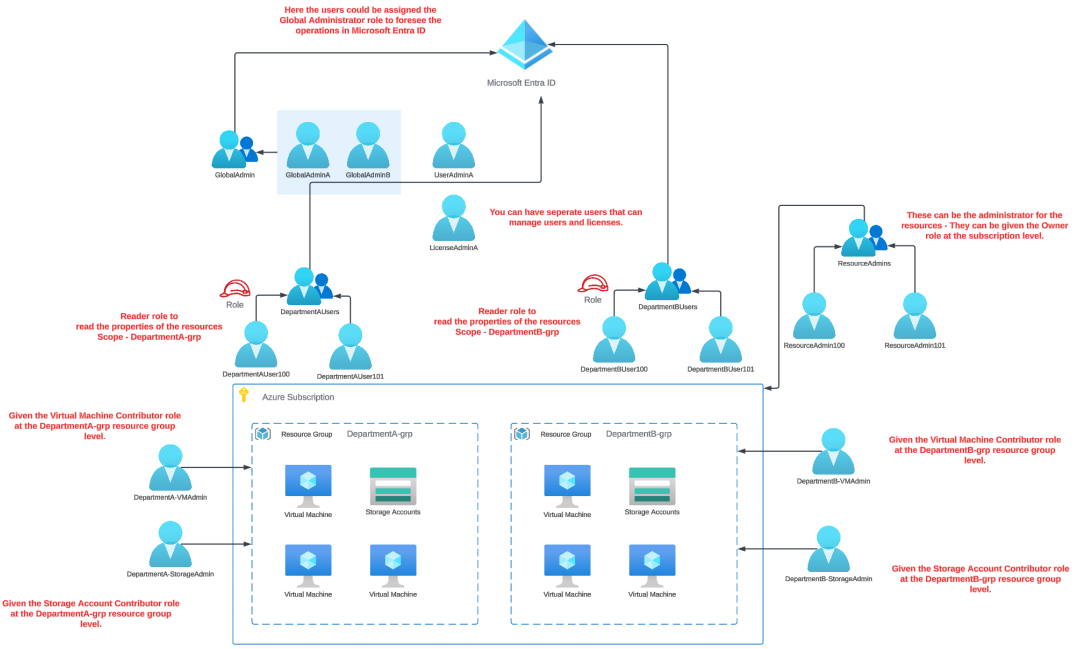



**Now let's give UserA the Contributor role at the resource group level.**

**So now we can stop the virtual machine.**

**Can we create a new resource in the resource group such as an Azure Storage Account.**

# Understanding the entire landscape till now

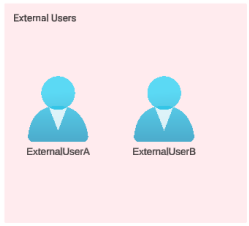


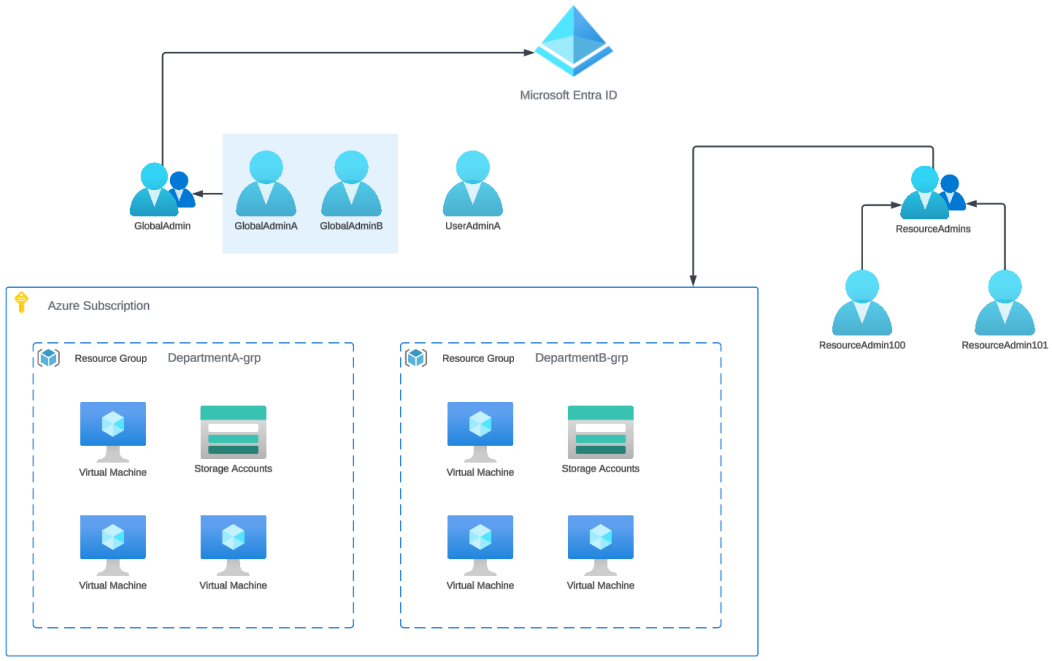

# Lab - Inviting an external user

You might have external users. These users are part of another organization. They belong with to another Microsoft Entra ID tenant or another identity provider.

They might need access to your Azure resources for a brief period of time.

Instead of recreating the users in your own tenant (which can lead to increased maintenance), you can instead intite them as guest users.



# Microsoft Entra ID Licenses

## Microsoft Entra ID Licensing

- **Microsoft Entra ID Free.** Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.
- **Microsoft Entra ID P1.** In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic membership groups, self-service group management, Microsoft Identity Manager, and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
- **Microsoft Entra ID P2.** In addition to the Free and P1 features, P2 also offers Microsoft Entra ID Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.

Reference - https://learn.microsoft.com/en-us/entra/fundamentals/whatis

## Steps that we need to follow

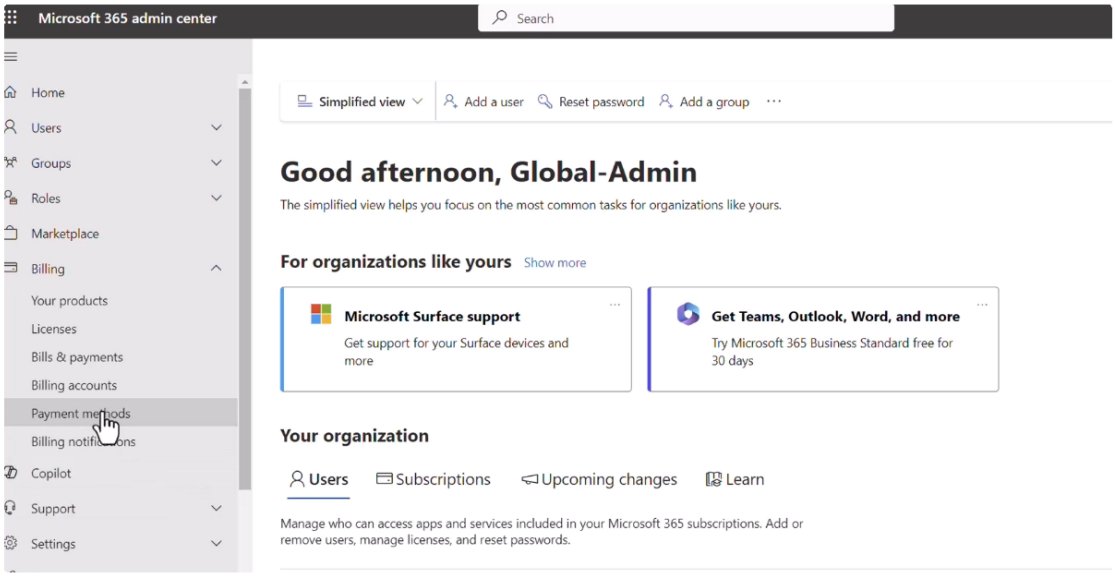
Microsoft Entra ID

**We first need to create a new user - We will assign the global administrator role to the user.**

Users

We will then log in as the user in Azure and change the password as part of the normal process for a new user.

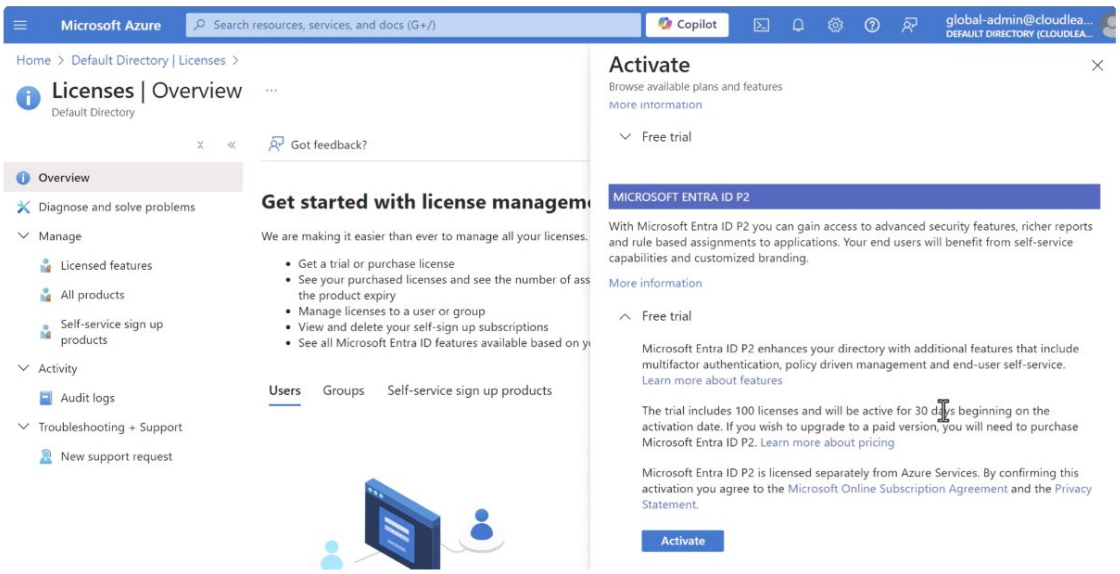
Then we need to log onto Microsoft 365 Admin center



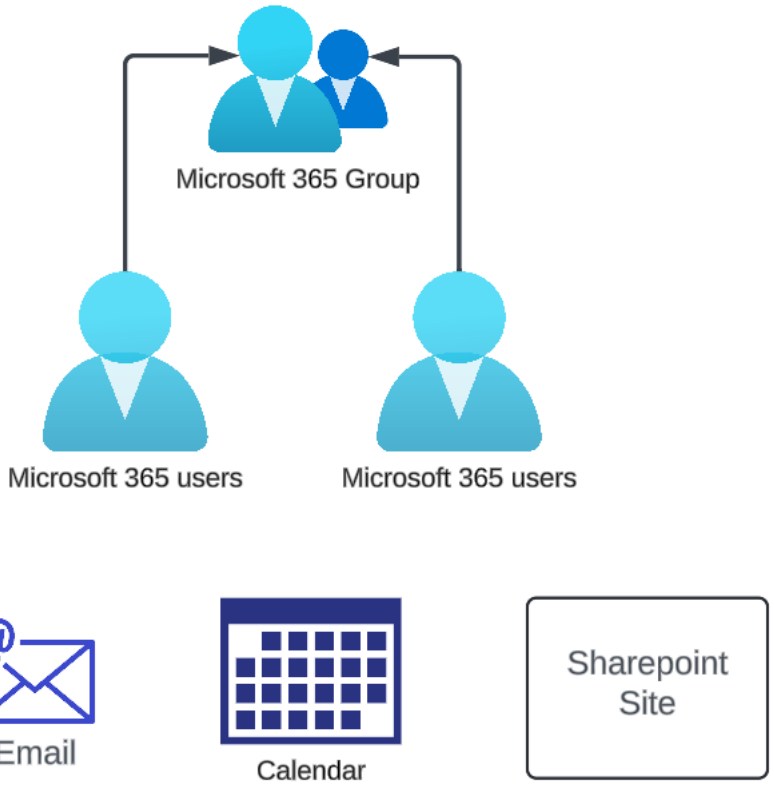

We need to add a valid payment method - Please note that the trial licenses don't incur a charge.

Then your billing account needs to have a valid address.

Then in Azure, we can subscribe for free trial licences for Entra ID P2 - 1 month.



## Microsoft 365 Groups




**Here users are given access to a shared email address, a shared calendar and a shared sharepoint site. Its used for collaboration.**

**Dynamic rules can be set for Microsoft 365 user-based groups.**

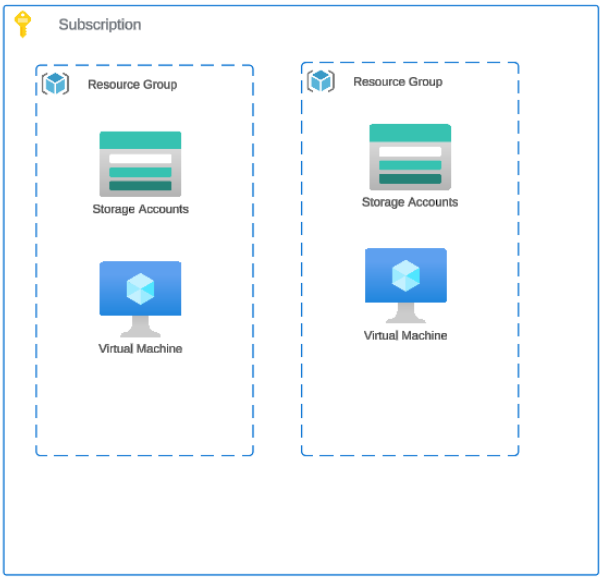
**You cannot add a Microsoft 365 group to a security group.**

# Microsoft Entra ID - Application Registration



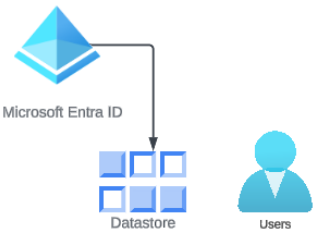

**If your application needs to interact with Azure-based resources, you can define an application object in Microsoft Entra ID.**

**When you register an application in Microsoft Entra ID, you get an application object and a service principal.**




**The application object can be used across all tenants, but the service principal associated with the object can only be used in the default tenant.**

**Objective - Use a tool known as POSTMAN to get the details of all users in our tenant.**



In the end , we can think of Microsoft Entra ID as a data store of information for our users, groups etc.

We now want to retrieve the details of users that are defined in our tenant.


Now how we can fetch our data. Well most platforms provide an API - Application Programming Interface. We can make calls to the API to retrieve the data.

Step 1 : Let's define an application object that will represent our POSTMAN tool.


Step 2: Next we need to give permissions to the Application Object.

Configured permissions

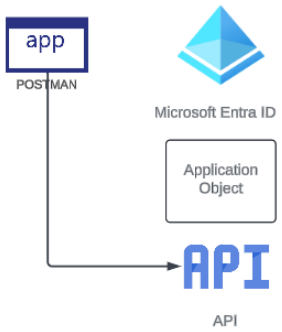
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for Default Directory

| API / Permissions name | Type | Description | Admin consent req... | Status |
|---|---|---|---|---|
| Microsoft Graph (1) | | | | ••• |
| User.Read.All | Application | Read all users' full profiles | Yes | Granted for Default Dire... ••• |

**Now this is not RBAC and this is not Microsoft Entra ID Roles.**

**Yes, we can assign role-based access control to the service principal associated with the Application Object. But we are not doing this here.**




**This is because our application does not need permission to a resource , so we dont need RBAC. Also our application does not need any role in Microsoft Entra ID.**

**Our application wants to call the in-built Graph API by Microsoft , which is like another application set of resources. Hence here we need to add permissions to our application object.**

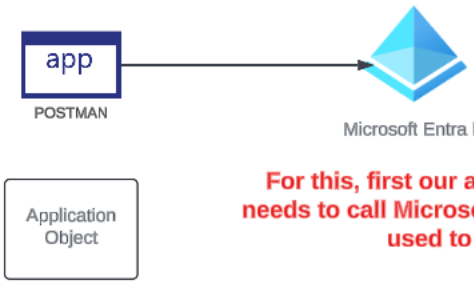
**Now why Application Permissions?**

**And why grant admin consent?**

**Step 3 : Obtain an access token**

**We need to authorize our POSTMAN tool first to ensure that it can access user information in Microsoft Entra ID.**

**For this ,we use OAuth which is a commonly used standard for authorization.**




**For this, first our application (POSTMAN) needs to call Microsoft Entra ID which can be used to get a token.**

**We can call the OAuth endpoint and get the access token accordingly.**

**Step 4 : Use the access token to get the user information via the use of the Graph API.**

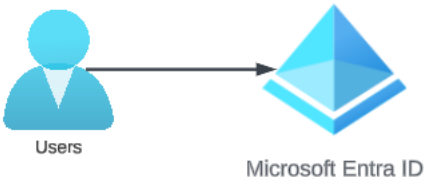
# Microsoft Entra ID - Enterprise Applications


**So we can register application objects in Microsoft Entra ID to represent our appications.**

**But we can also make use of Enterprise applications in Microsoft Entra ID.**

**The Microsoft Entra Gallery has support for applications from other vendors as well.**


**Online storage for files.**




**You can have a user defined in Microsoft Entra ID**


**Then that same user can use the same credentials via single-sign on to log into let's say another application - Dropbox**

**Microsoft has established the facility for Microsoft Entra ID to also be used as the identity provider for other software-as-a-service applications as well.**

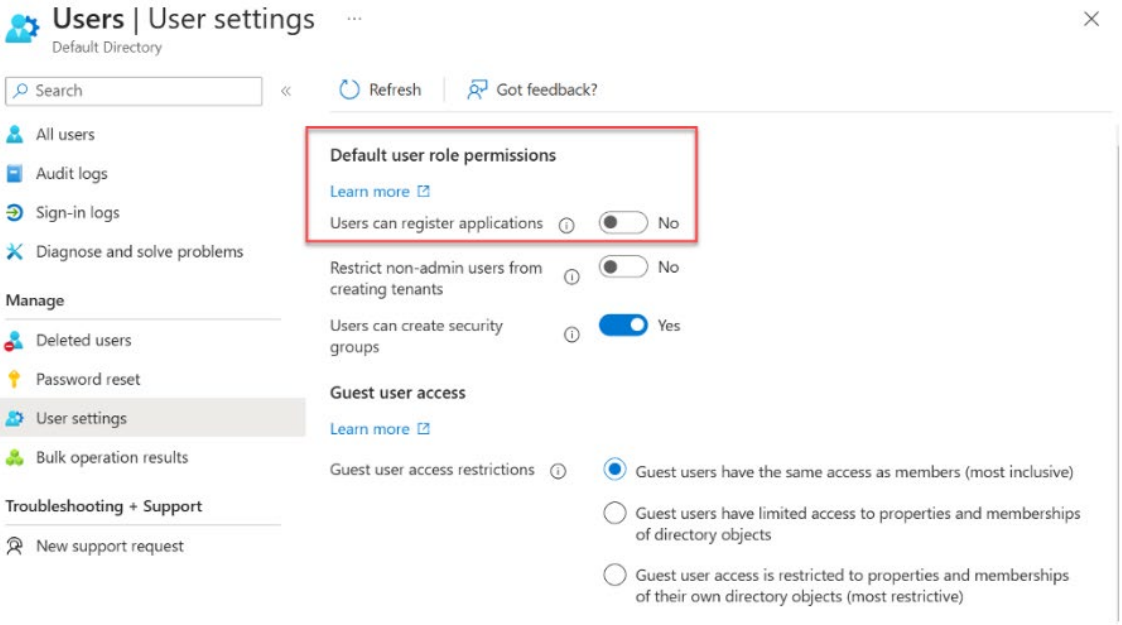
# Managing applications in Entra ID

Microsoft Entra ID

Enterprise Application

**Whenever a user registers an application, they become the owner of the application.**

**This allows them to control the user assignment, configurations such as single-sign on etc.**




**To limit users so that by default they cannot register applications.**

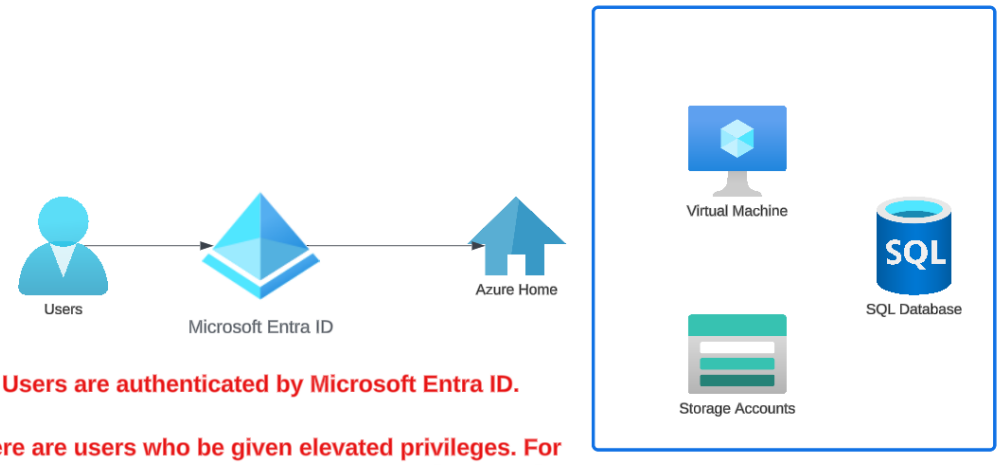
**When you disable default access, you can provide access via the use of Microsoft Entra ID roles**

**Application Developer - Here the user can register applications.**

**Application Administrator - Here users can create and manage all aspects when it comes to enterprise applications, application registrations and application proxy settings.**

**Cloud Application Administrator - All aspects of the Application Administrator , except having the capability to manage Application Proxy.**

# Multi-Factor Authentication




**Users are authenticated by Microsoft Entra ID.**

**There are users who be given elevated privileges. For such users, you want to have extra security when it comes to authentication.**

**With Microsoft Entra ID, you can make use of Multi-Factor Authentication. This is the process where a user will be prompted for an additional form of identification during the authentication process.**

**There are various other forms of additional security methods that are available such as**

1. **Microsoft Authenticator App**
2. **Windows Hello for Business**
3. **FIDO2 Security keys**
4. **SMS**
5. **Voice call**

# Passwordless authentication

Microsoft Entra ID

Users

**When users log in, we enter a user name and a password. We can also be asked to perform Multi-Factor authentication.**

**But we can also use passwordless-authentication options that are secure in nature.**

**Windows Hello for Business**

**Here first a user can use their biometric or PIN number to log onto a Windows machine.**

**After the login is completed, an exchange happens between the machine and Microsoft Entra ID that helps to authenticate the user.**

**Windows Authenticator App**

**This is an app that can run on iOS and Android devices. Here the App can be used as a secure mechanism to log into via Microsoft Entra ID.**

**Apart from this we also have FIDO2 security keys and Certificate-based authentication.**

# What is Microsoft Entra ID Protection

**Microsoft Entra ID Protection**


**You can define multiple users as part of your Microsoft Entra ID tenant.**

**These users can have different permissions - These can be RBAC or roles defined in Microsoft Entra ID.**

**We have be known of the fact of malicious users who will try to gain access to our infrastructure.**

**All they need is one gateway into your tenant and they will claw their way to gaining more access to your resources.**

**We can prevent major breaches by first of all only giving privileges to users that are required, least privilege.**

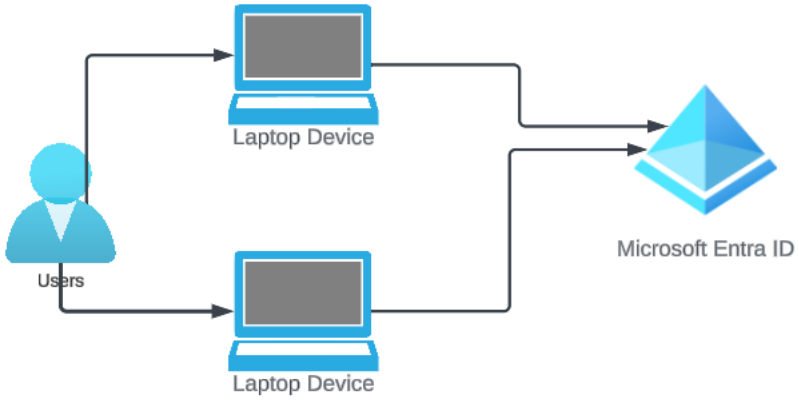
**But at the same time we need to protect our identities. We can achieve this with Microsoft Entra ID protection.**

**Microsoft can detect potential problems with users and their sign-in's based on data collected from the past and using Machine learning algorithms.**


**Microsoft has typically millions of sign-ins on their various platforms. They collect these signals and maintain information on signals that lead to potential breaches when it comes to user sign-ins.**

## An example of a signal

### Atypical travel




**A user is signing in from devices in different locations. This is not normal for a user. Microsoft might detect this as a risk when it comes to the sign-in process.**

**The risk is then categorized into levels - High, Medium and Low. High means that Microsoft is confident that the account has been comprimised.**

the account has been comprimised.

# Required roles

ID Protection requires users be assigned one or more of the following roles in order to access.

Expand table

| Role | Can do | Can't do |
|---|---|---|
| Security Administrator | Full access to ID Protection | Reset password for a user |
| Security Operator | View all ID Protection reports and Overview<br><br>Dismiss user risk, confirm safe sign-in, confirm compromise | Configure or change policies<br><br>Reset password for a user<br><br>Configure alerts |
| Security Reader | View all ID Protection reports and Overview | Configure or change policies<br><br>Reset password for a user<br><br>Configure alerts<br><br>Give feedback on detections |
| Global Reader | Read-only access to ID Protection | |
| User Administrator | Reset user passwords | |

| Capability | Details | Microsoft Entra ID Free / Microsoft 365 Apps | Microsoft Entra ID P1 | Microsoft Entra ID P2 |
|---|---|---|---|---|
| Risk policies | Sign-in and user risk policies (via ID Protection or Conditional Access) | No | No | Yes |
| Security reports | Overview | No | No | Yes |
| Security reports | Risky users | Limited Information. Only users with medium and high risk are shown. No details drawer or risk history. | Limited Information. Only users with medium and high risk are shown. No details drawer or risk history. | Full access |
| Security reports | Risky sign-ins | Limited Information. No risk detail or risk level is shown. | Limited Information. No risk detail or risk level is shown. | Full access |
| Security reports | Risk detections | No | Limited Information. No details drawer. | Full access |
| Notifications | Users at risk detected alerts | No | No | Yes |
| Notifications | Weekly digest | No | No | Yes |
| MFA registration policy | | No | No | Yes |

Reference - https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

## What are Access Reviews

Imagine we have this entire landscaped and this is nothing when compared with large organizations.

We have users that are assigned to groups. Groups can be given roles or RBAC permissions.

Users can also be given access to applications.

Well what happens when the user changes their department or leaves the company. They should no longer have the required access.

But how can we guarantee that the access is revoked. Well we can create and conduct access reviews.

| Access rights of users | Reviewers can be | Review created in | Reviewer experience |
|---|---|---|---|
| Security group members<br>Office group members | Specified reviewers<br>Group owners<br>Self-review | access reviews<br>Microsoft Entra groups | Access panel |
| Assigned to a connected app | Specified reviewers<br>Self-review | access reviews<br>Microsoft Entra enterprise apps | Access panel |
| Microsoft Entra role | Specified reviewers<br>Self-review | PIM | Microsoft Entra admin center |
| Azure resource role | Specified reviewers<br>Self-review | PIM | Microsoft Entra admin center |
| Access package assignments | Specified reviewers<br>Group members<br>Self-review | entitlement management | Access panel |

# License requirements

This feature requires Microsoft Entra ID Governance or Microsoft Entra Suite subscriptions, for your organization's users. Some capabilities, within this feature, may operate with a Microsoft Entra ID P2 subscription. For more information, see the articles of each capability for more details. To find the right license for your requirements, see Microsoft Entra ID Governance licensing fundamentals.

Reference - https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

# What is Privileged Identity Management

Microsoft Entra ID

**Here you can provide just-time privileged access to Microsoft Entra ID and Azure resources. Hence no need to provide access beforehand.**

**Maybe a User needs to register an application. But it may only be for a particular project.**

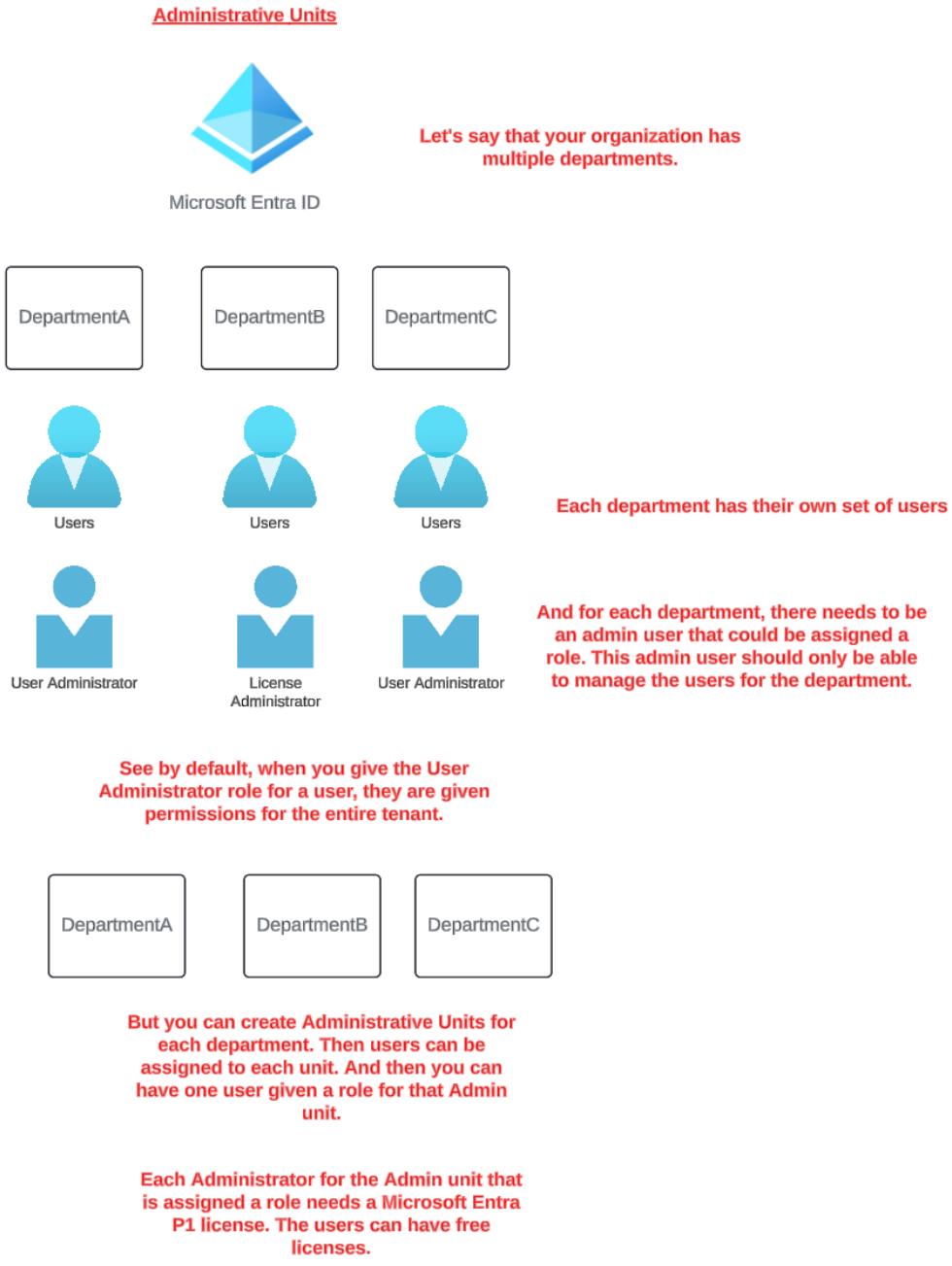
**It may not be required when the user id is created, but needed at a later on stage. Well then there is no need to assign a role like the Application Developer role when the user id is created.**

**Instead the user can request for the role whenever it is required.**

**You can also configure aspects such as time-bound access , approval to activate privileged roles.**

**In terms of licensing, we need to have either Microsoft Entra ID P2 or Microsoft Entra ID Governance.**

# Administrative Units



You can also add a group to an administrative unit. But the administrator of the admin unit can only manage the name and members of the group. The administrator cannot manage the members themselves. To manage the members , they need to be added as users of the Administrative unit.

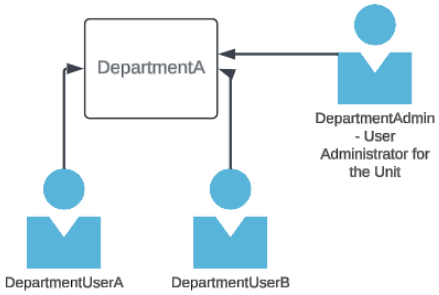
Let's implement the following


Create an administrative Unit


Give the User Administrator role within the Admin unit to a user named DepartmentAdmin

Then let's add two users to the Admin unit. And one user at the tenant level.


Have a user at the tenant level.

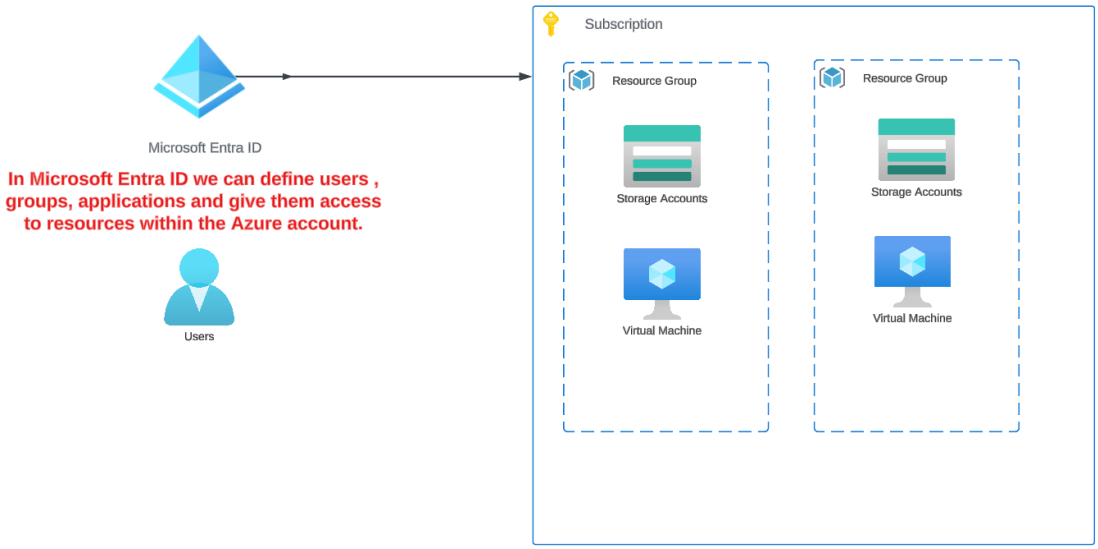

Then log in as the DepartmentAdmin User

As DepartmentAdmin can we create a new user at the tenant level? - No

As DepartmentAdmin can we reset the password for DepartmentUserA? - Yes

As DepartmentAdmin can we reset the password for UserA? - No

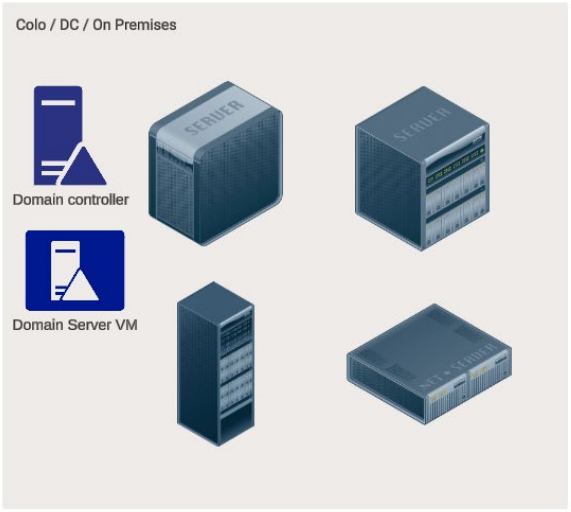
# Having a hybrid setup




But existing companies might be having their own data centers with their own servers and applications.

When it comes to identity management, they might be using their own identity-based software.

One example is using Microsoft Active Directory.




Microsoft Active Directory has services such as Active Directory Domain Services. This is used to store information about objects on a network.

It stores information about user accounts and devices on the network.

You would install the Active Directory domain services on a Windows Server machine. This is a role that is available on Windows Server.

You can then host a domain and maintain information about users and devices on the network within that domain.

Now we are going to see how we can sync identities defined in Microsoft Active Directory with Microsoft Entra ID.

## Our implementation on a hybrid setup

Microsoft Entra ID

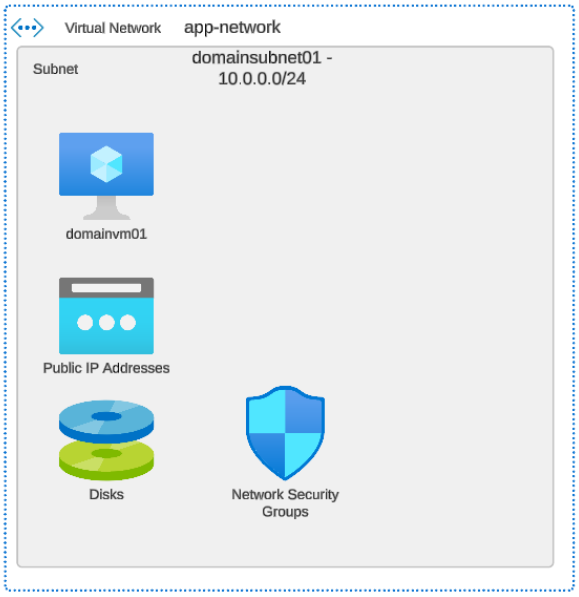
Step 1 : Register a custom domain in Microsoft Entra ID.

We need to have a matching domain for users defined in an on-premises setup.

Then we need to setup a user with the custom domain name as a Global Administrator or a Hybrid Identity Administrator.

Step 2 : Let's use Azure services to simulate an on-premises network

Setting up Microsoft Active Directory Domain Services

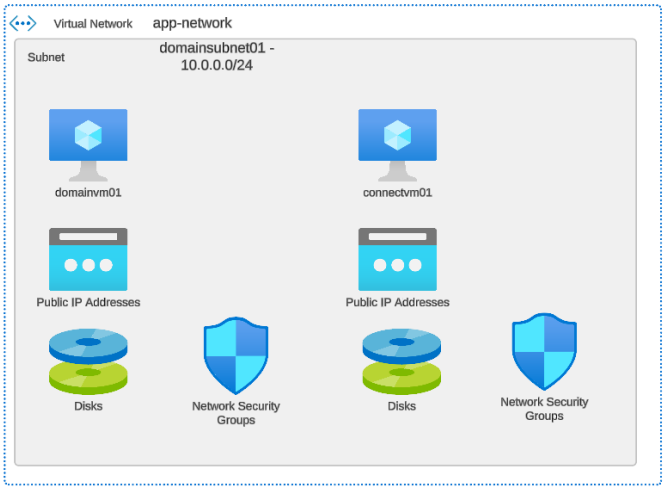



1. We will create a virtual machine based on Windows Server 2022.

2. We will install the role of Active Directory Domain services and have a domain in place.

3. We need to change the settings of the virtual network so that it uses our Windows Server when it comes to DNS.

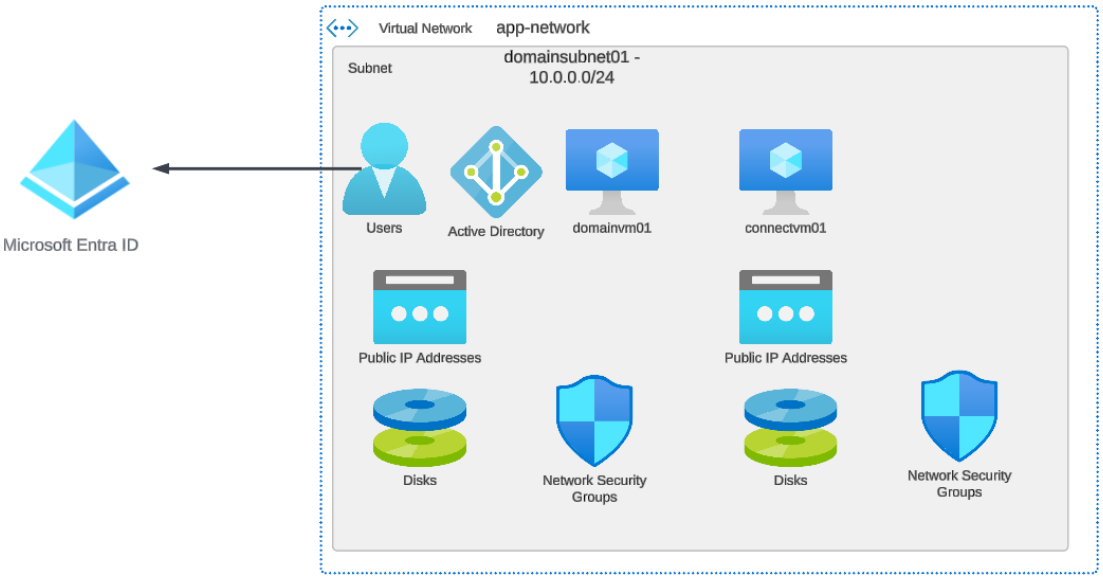
**Step 3 : We need to setup Microsoft Entra Connect. This needs to be setup on a Microsoft Windows Server. This is used to sync the identities from the on-premises identity server to Microsoft Entra ID.**




**The connectvm machine needs to be added as part of the domain.**

**When configuring Microsoft Entra Connect we need to use a user which is a domain administrator defined in the Active Directory domain.**

# Pass through authentication




**So now our users are syncrhonized onto Microsoft Entra ID via the use of Microsoft Entra Connect.**

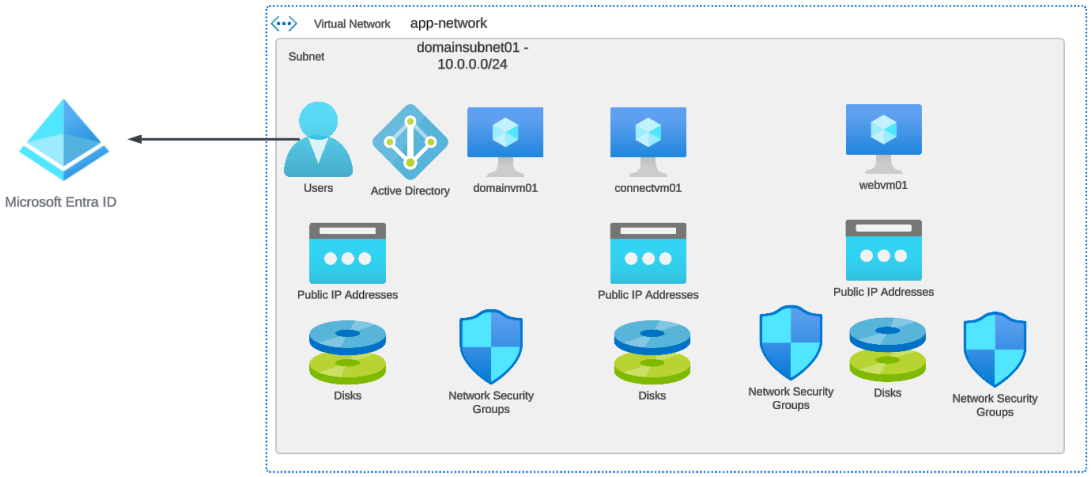
**By default , password hash synchronization is configured. Here a hash of a hash of the users password configured on-premise is stored in Microsoft Entra ID.**

**Hence here the user can use the same user name and password for cloud services as well.**

**But there is another configuration option - Pass-through authentication. Here a password validation is conducted on the on-premises active directory server before the user can log onto the cloud services.**

**Here the password validation does not happen on the cloud. Also you can enforce constraints that are available in Microsoft Active Directory like password policies etc.**

# Application Proxy




**Let's say that you have an internal web application that needs to be accessed from the Internet.**

**And this is without the need of exposing the application infrastructure to the Internet.**

**There are ways that you can achieve this - Using reverse proxy's , Using VPN connections.**

**But we can make use of Application Proxy. This gives you remote access to your on-premises web applications.**

**Step 1 : Deploy a new Windows Server to our infrastructure. Install Internet Information Services so that it behaves as a web server. This will serve as our on-premise web application.**

**Step 2: Next we will disassociate the Public IP address from the webvm01 machine.**

**Key Points - In order to setup an on-premises application onto Microsoft Entra ID , we need the following**

1. **A Microsoft Entra ID P1 or P2 subscription**
2. **An application administrator account**
3. **Users Synchronized from on-premises to Microsoft Entra ID**

# Secure networking

## Understanding the Azure virtual network


**This is an isolated network on the cloud.**

**This is similar to having a network in an on-premises data center.**

**You can host resources such an Azure virtual machines in an Azure virtual network. These resources can securely communicate with each other.**

**A virtual network is scoped to a particular region and subscription.**

## Understanding Network Security Groups

## Network Security Groups

This is used to filter network traffic between Azure resources in an Azure virtual network.

Here you create Inbound and Outbound rules to allow or deny traffic.

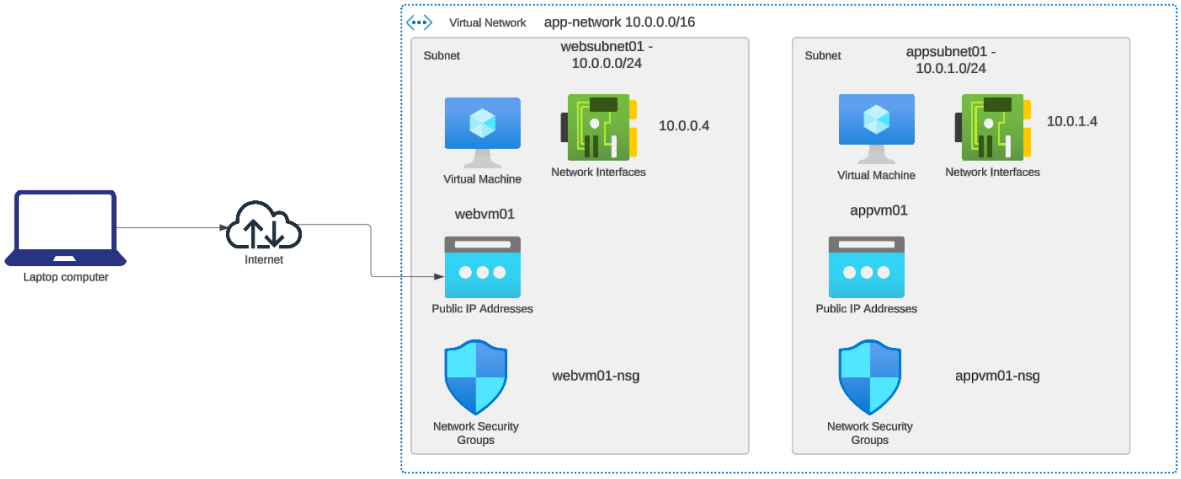
## Rules

1. Name of the rule
2. Priority - Rules are processed in the order of priority
3. Source or destination - IP address, Service Tag , Application Security Group.
4. Protocol - TCP, UDP, ICMP etc.
5. Port Range
6. Action - Allow or Deny

## Default Rules

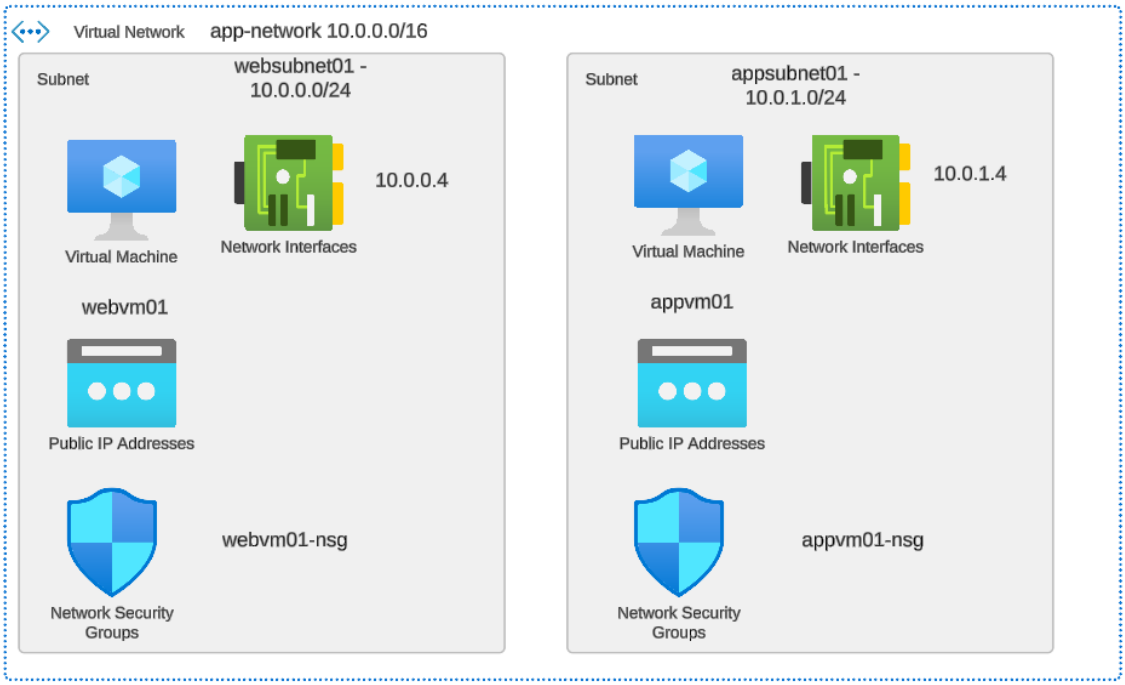
| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| **Inbound Security Rules** | | | | | | |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowAzureLoadBalanc··· | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | DenyAllInBound | Any | Any | Any | Any | Deny |
| **Outbound Security Rules** | | | | | | |
| 65000 | AllowVnetOutBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowInternetOutBound | Any | Any | Any | Internet | Allow |
| 65500 | DenyAllOutBound | Any | Any | Any | Any | Deny |

# Lab - Network Security Groups - Access to other machines




Let's deploy another Linux-based virtual machine to another subnet in the same virtual network.

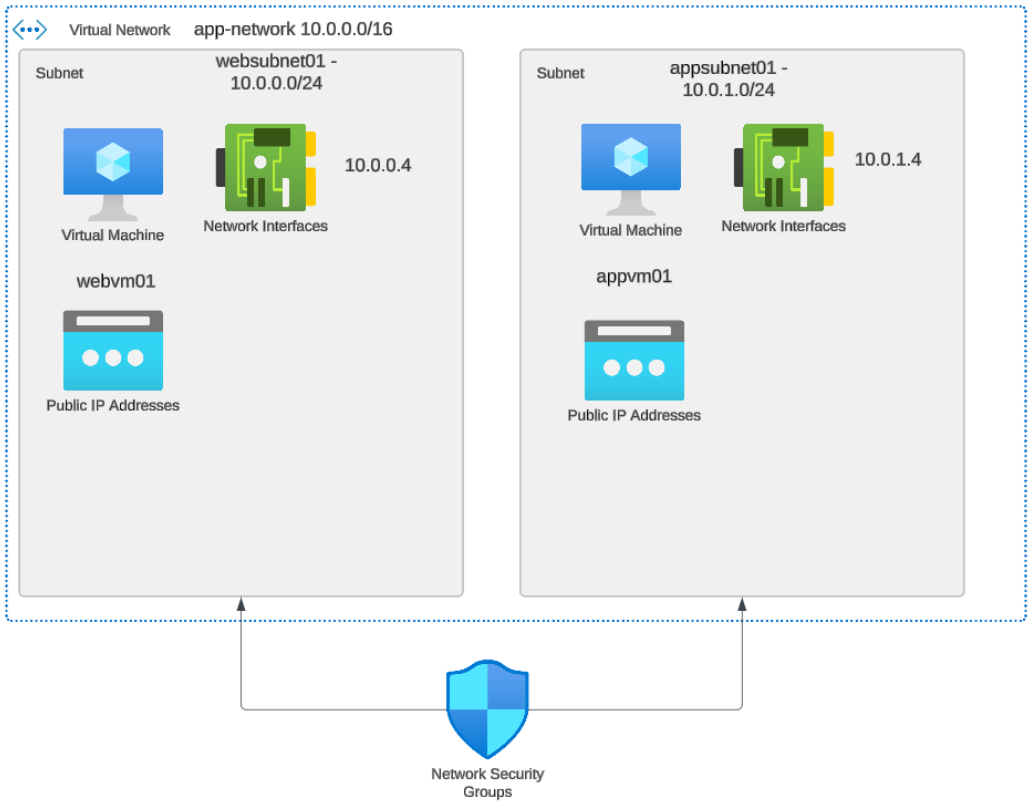
# Lab - Network Security Groups – Subnets




**We can also define Network Security Groups at the subnet level.**

**We can create a new network security group and associate that NSG with both subnets.**

**We can detach the NSG's at the network interface level.**



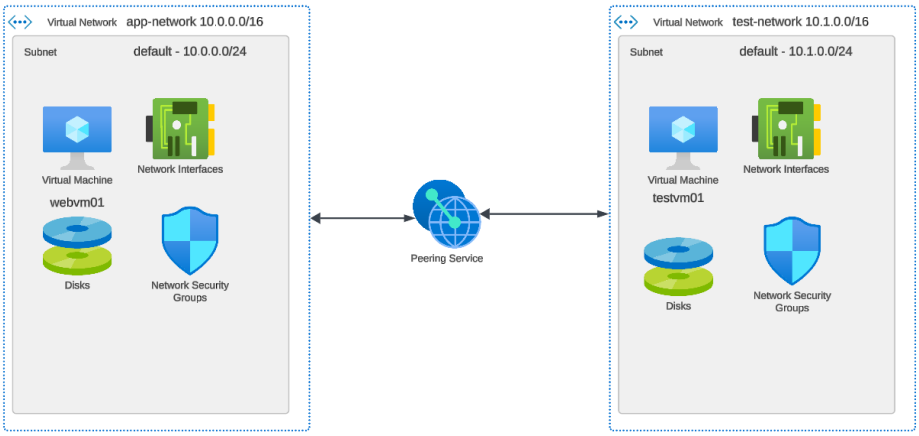

## Application Security Groups – Setup

**These helps to group virtual machines together.**

Application
Security Groups

**Then instead of allowing connections to individual machines in NSG's, we can allow access to Application Security Groups.**

# Virtual Network Peering



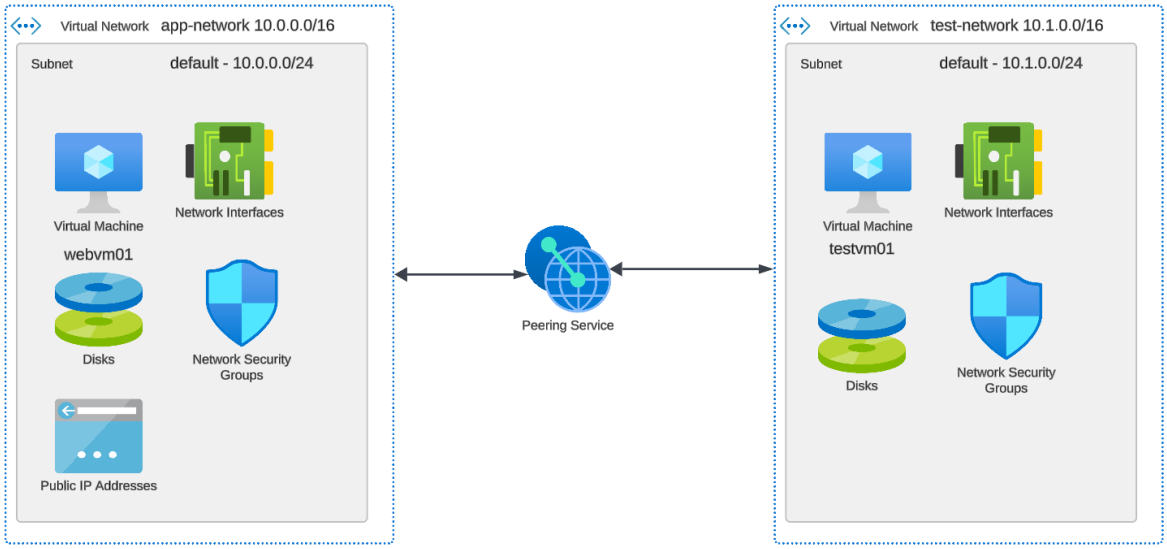

**This services allows you to connect virtual networks together.**

**The traffic across the virtual machines uses the Microsoft backbone network.**

**When peering virtual networks together, they cannot have overlapping CIDR blocks.**

**You can connect Azure virtual networks in the same region or across regions.**

# Lab - Virtual Network Peering




**We will deploy another virtual machine in another virtual network.**

**Can we reach the web server running on webvm01 from testvm01 without virtual network peering?**

**Then let's establish a virtual network peering connection.**

# User Defined Routes

By default there are system routes in place which ensures the traffic is routed correctly across subnets in a virtual network.

But let's say that your company has a virtual machine that is hosting a virtual appliance - Firewall.

And all traffic in the virtual network needs to be routed through the virtual appliance.

We can define a user-defined route that makes sure all traffic is routed through the firewall appliance device.


# Lab - User Defined Routes

Let's say that all traffic needs to be routed via a new virtual machine named centralvm01.

Let's create that new machine first.

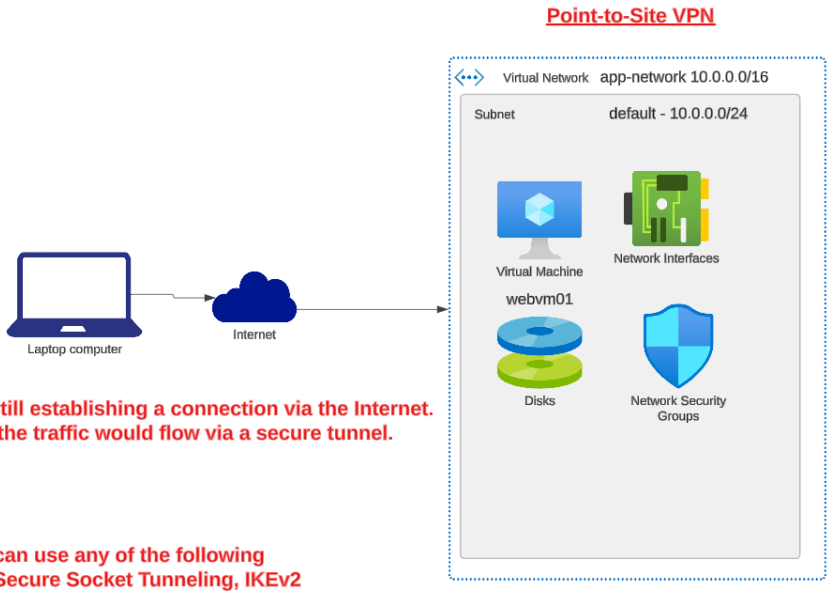
Then we will create a new route table.

Then create a route that routes all traffic for websubnet01 via centralvm01.

We then need to associate the route table with appsubnet01

In order to route requests we now need to implement 2 aspects
Enable IP forwarding on the network interface for centralvm01 and at the OS level.

# Point to Site VPN Connection




We are still establishing a connection via the Internet. But the traffic would flow via a secure tunnel.

The secure tunnel can use any of the following protocols - OpenVPN, Secure Socket Tunneling, IKEv2

The client computers that connect via the VPN connection need to authenticate - This can be done via a Certificate, Microsoft Entra ID or usage of RADIUS and Active Directory Domain Server.

This allows you to create a secure connection to an Azure virtual network from a client computer.

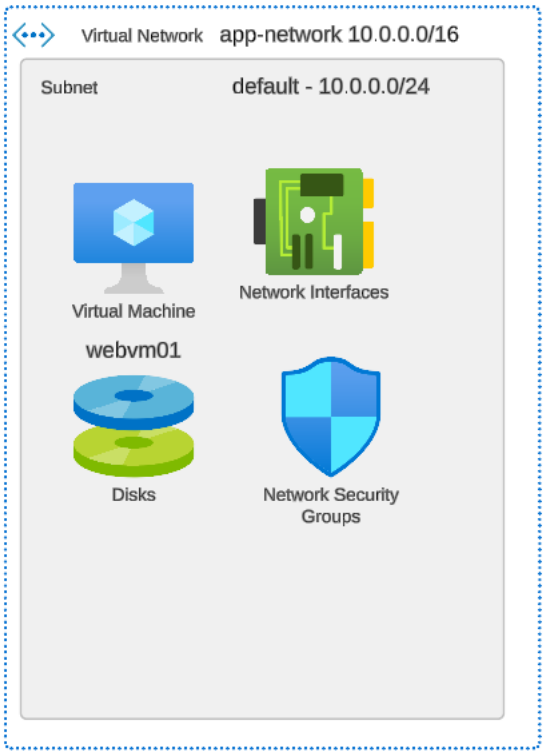
Here there is no need for the virtual machine hosting the application to have a Public IP address.

This is ideal when you have a few clients that need to connect to applications hosted in Azure virtual networks from their home computers.

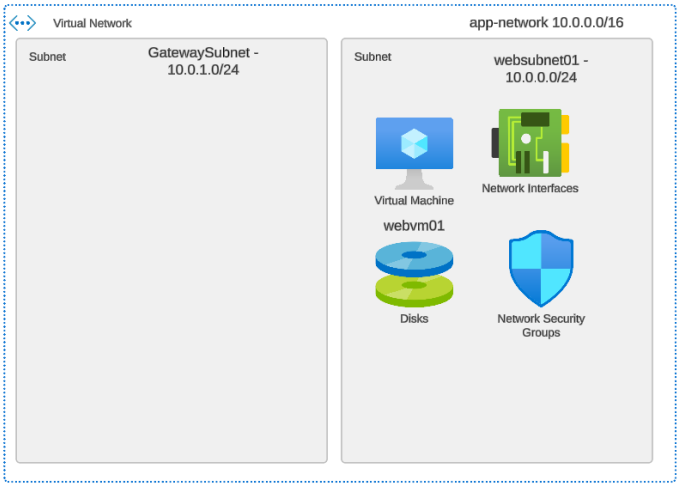
# Lab - Point-to-Site VPN

**Point-to-Site VPN**

**Step 1 : Let's have a Windows Server in place that is hosting Internet Information Services. We will make sure that the server does not have a public IP address.**

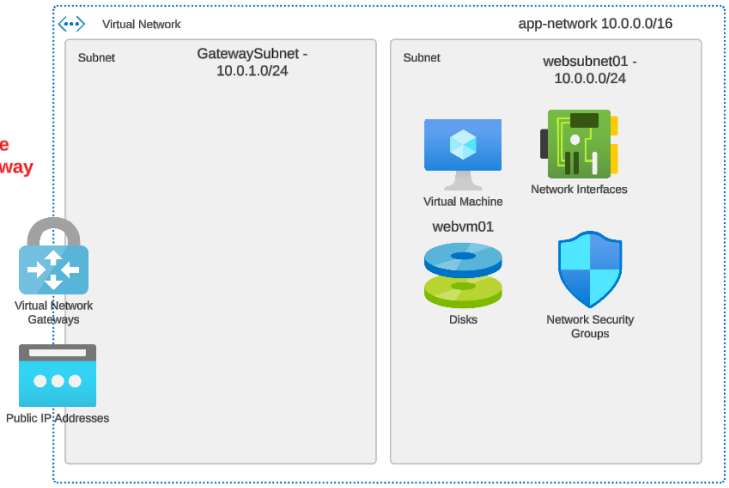



**Step 2: We need to create a gateway subnet with the name of GatewaySubnet. This subnet would host the required resources for the VPN gateway that will be deployed later on.**




**Step 3 : Deploy the VPN gateway. This is used to establish VPN connections from clients.**

**The VPN gateway needs a public IP address. The connections are established through the VPN gateway via the use of the Public IP address.**




## Create virtual network gateway

Subscription * : Azure subscription 1

Resource group : app-grp (derived from virtual network's resource group)

**Instance details**

Name * : network-gateway

Region * : North Europe

Deploy to an Azure Extended Zone

Gateway type * : VPN / ExpressRoute

SKU * : VpnGw2

Generation : Generation2

Virtual network * : app-network

Create virtual network

Subnet : GatewaySubnet (10.0.1.0/24)

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

**Public IP address**

Public IP address * : Create new / Use existing

Public IP address name * : gateway-ip

Public IP address SKU : Standard

Assignment : Dynamic / Static

Enable active-active mode * : Enabled / Disabled

Configure BGP * : Enabled / Disabled

**Authentication Information (Preview)**

Enable Key Vault Access : Enabled / Disabled

**Choosing the least cost option when it comes to a Generation 2 VPN gateway.**

**VPN Gateways**

Setting up a virtual network is free of charge. However, we do charge for the VPN gateway that connects to on-premises and other virtual networks in Azure. This charge is based on the amount of time that gateway is provisioned and available.

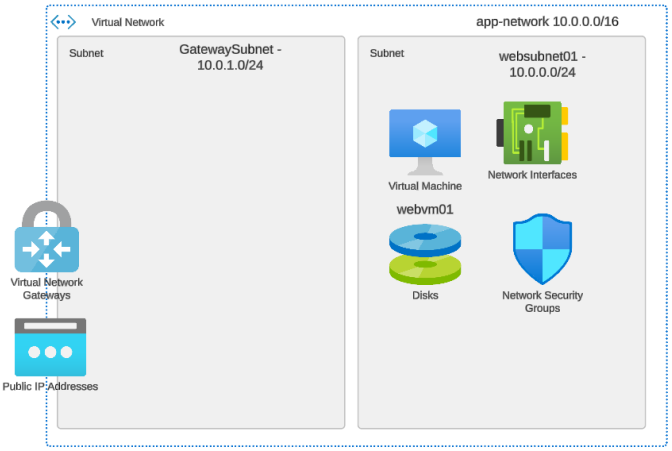
| VPN Gateway Type | Price | Bandwidth | S2S Tunnels | P2S Tunnels |
|---|---|---|---|---|
| Basic | $0.04/hour | 100 Mbps | Max 10<br>1-10: Included | Max 128<br>1-128: Included |
| VpnGw1 | $0.19/hour | 650 Mbps | Max 30<br>1-10: Included<br>11-30: $0.015/hour per tunnel | Max 250<br>1-128: Included<br>129-250: $0.01/hour per connection |
| VpnGw2 | $0.49/hour | 1 Gbps | Max 30<br>1-10: Included<br>11-30: $0.015/hour per tunnel | Max 500<br>1-128: Included<br>129-500: $0.01/hour per connection |
| VpnGw3 | $1.25/hour | 1.25 Gbps | Max 30<br>1-10: Included<br>11-30: $0.015/hour per tunnel | Max 1,000<br>1-128: Included<br>129-1,000: $0.01/hour per connection |
| VpnGw4 | $2.10/hour | 5 Gbps | Max 100<br>1-10: Included<br>11-100: $0.015/hour per tunnel | Max 5,000<br>1-128: Included<br>129-5,000: $0.01/hour per connection |
| VpnGw5 | $3.65/hour | 10 Gbps | Max 100<br>1-10: Included<br>11-100: $0.015/hour per tunnel | Max 10,000<br>1-128: Included<br>129-10,000: $0.01/hour per connection |

**Step 4 : Generate certificates for authentication. Clients need to use this certificate to authenticate while creating the VPN connection.**

**For a company you would normally generate certificates from a trusted authority.**


**You first generate a root certificate.**


**The public key of the root certificate is then uploaded to Azure to the VPN gateway. This allows the gateway to trust the clients.**

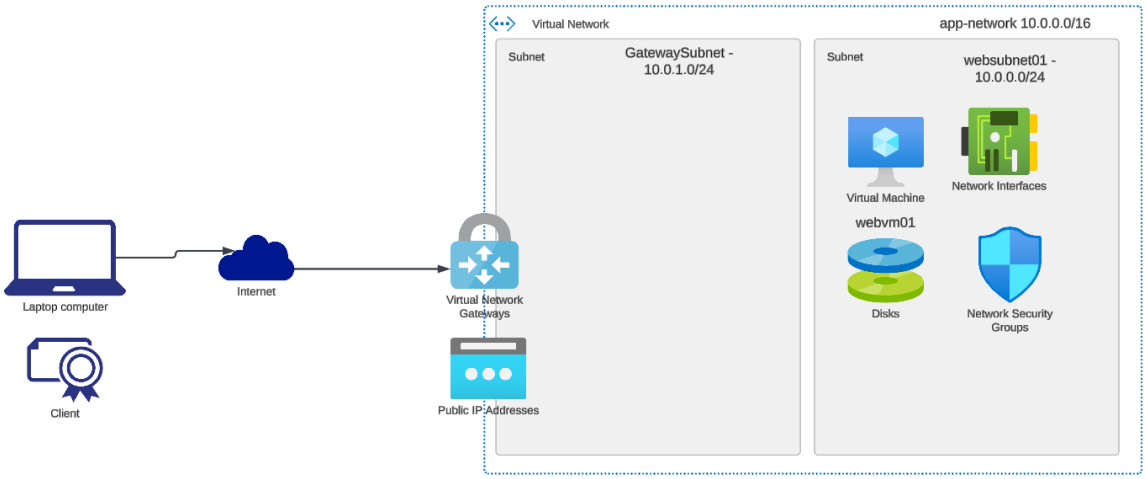




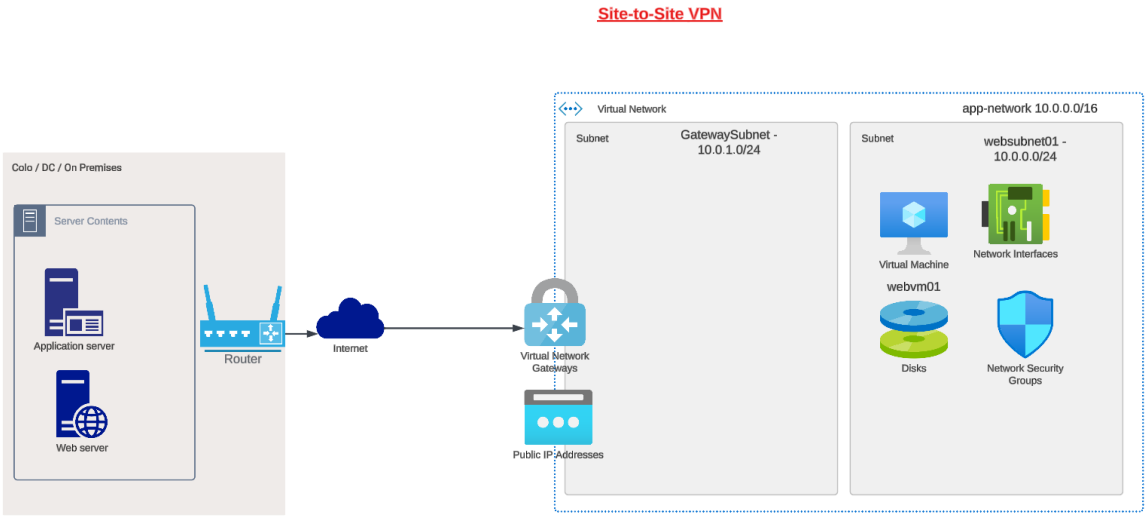
**Then you generate the client certificate from each root certificate.**


**This certificate needs to be installed on each client computer that needs to connect via the VPN gateway.**

**Step 5 : Download and install the VPN client from the VPN Gateway. The client can then establish a VPN connection.**



# Site-to-Site VPN Connection



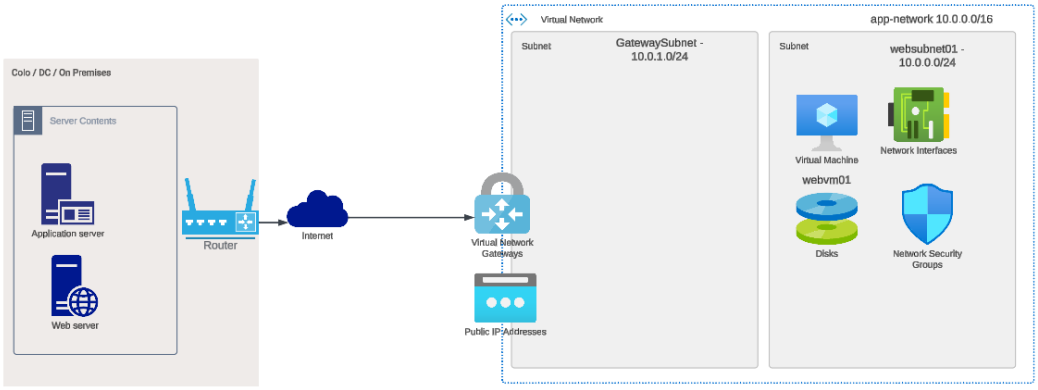

**This is used to securely connect an on-premises network onto an Azure virtual network.**

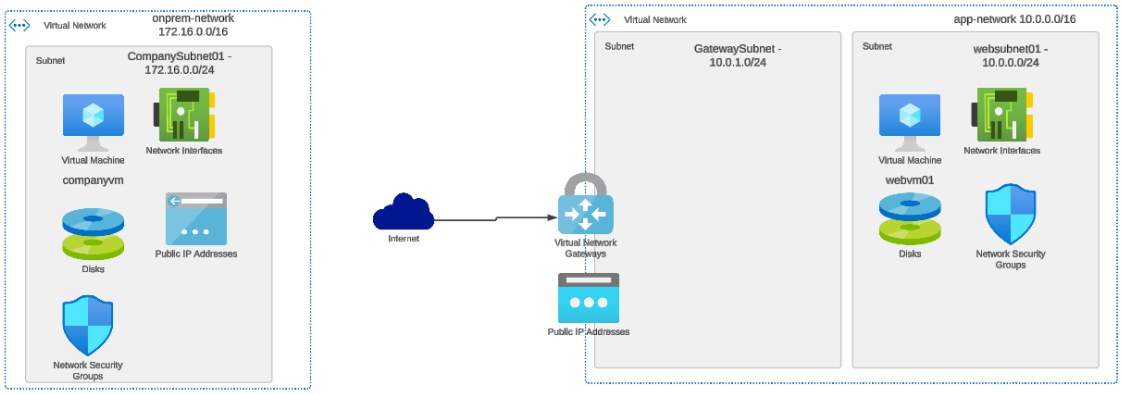
**Here the connection is established via a secure IPsec/IKE VPN tunnel.**

**Here the on-premises network needs to have a router with a Public routable IP address.**

# Lab - Site-to-Site VPN

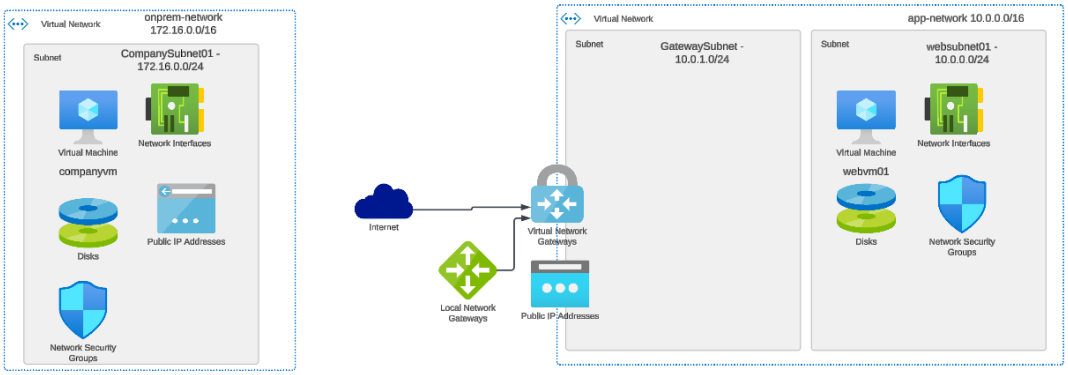
**Step 1: We will need to simulate our on-premises network.**

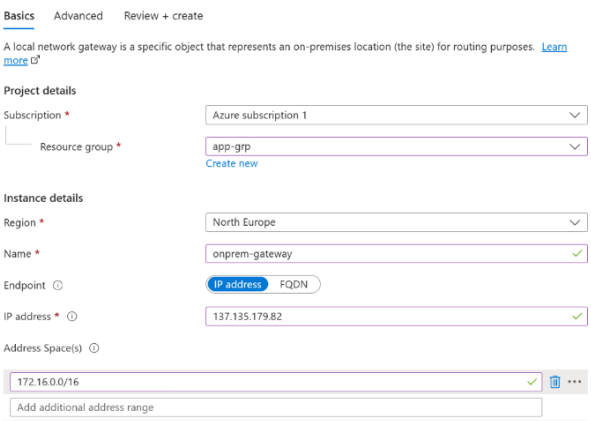



**We will deploy an Azure virtual machine based on Windows Server 2022 in another virtual network.**

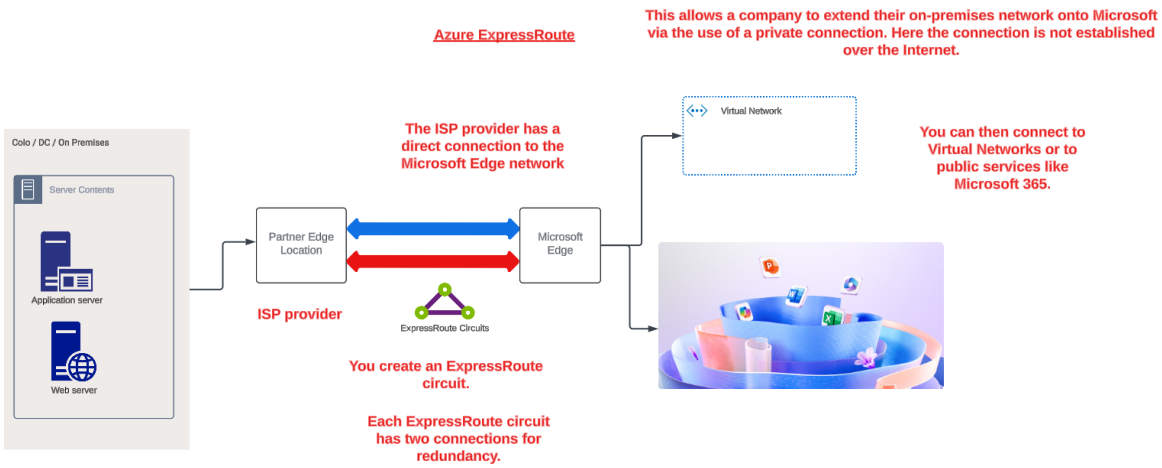
**Step 2 : Deploy a local network gateway - This is just an object that is used to represent your on-premises setup. It provides info to the VPN gateway on routing requests to your onprem network.**




**Step 3 : We need to deploy a routing service on our companyvm server. This will help route requests via the Site to Site VPN connection.**

# Azure ExpressRoute

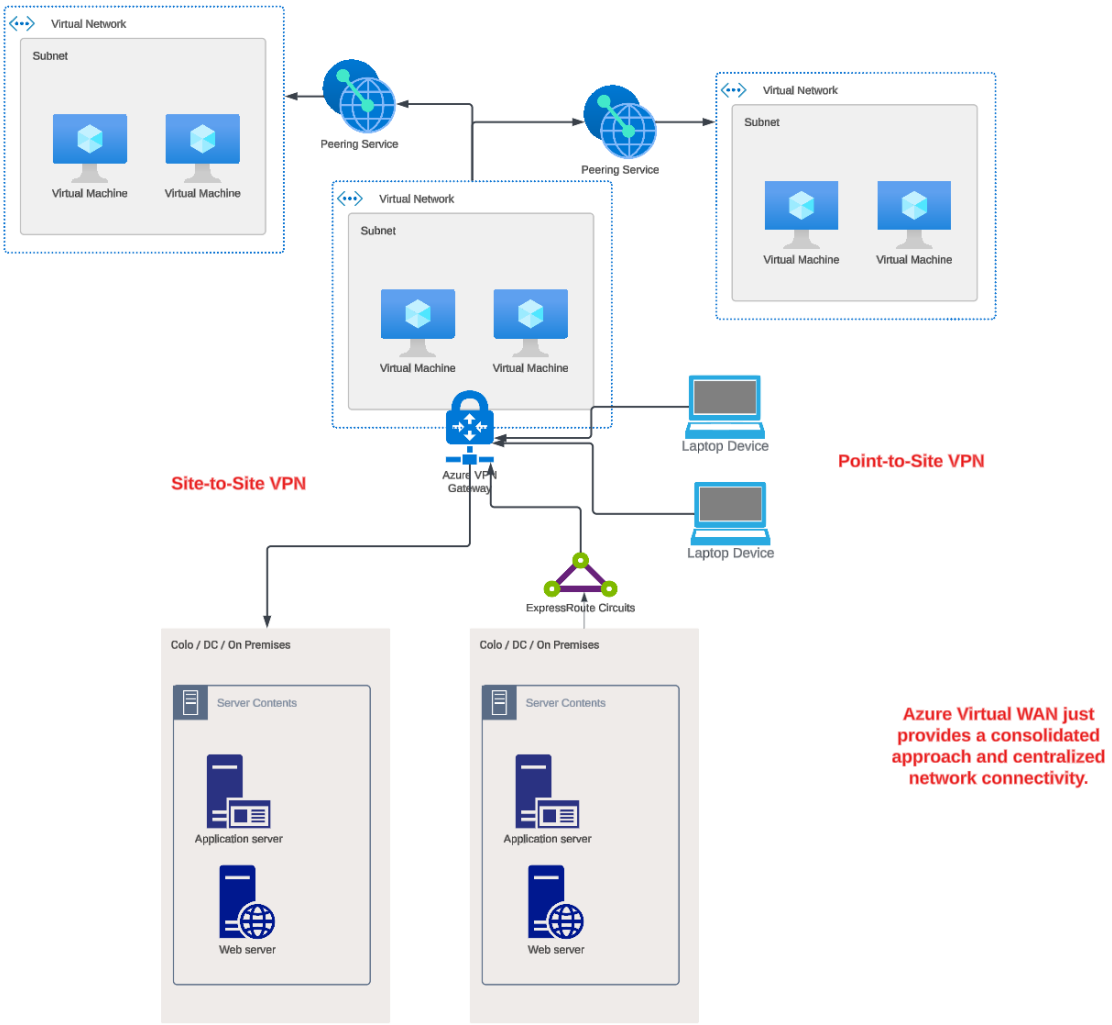


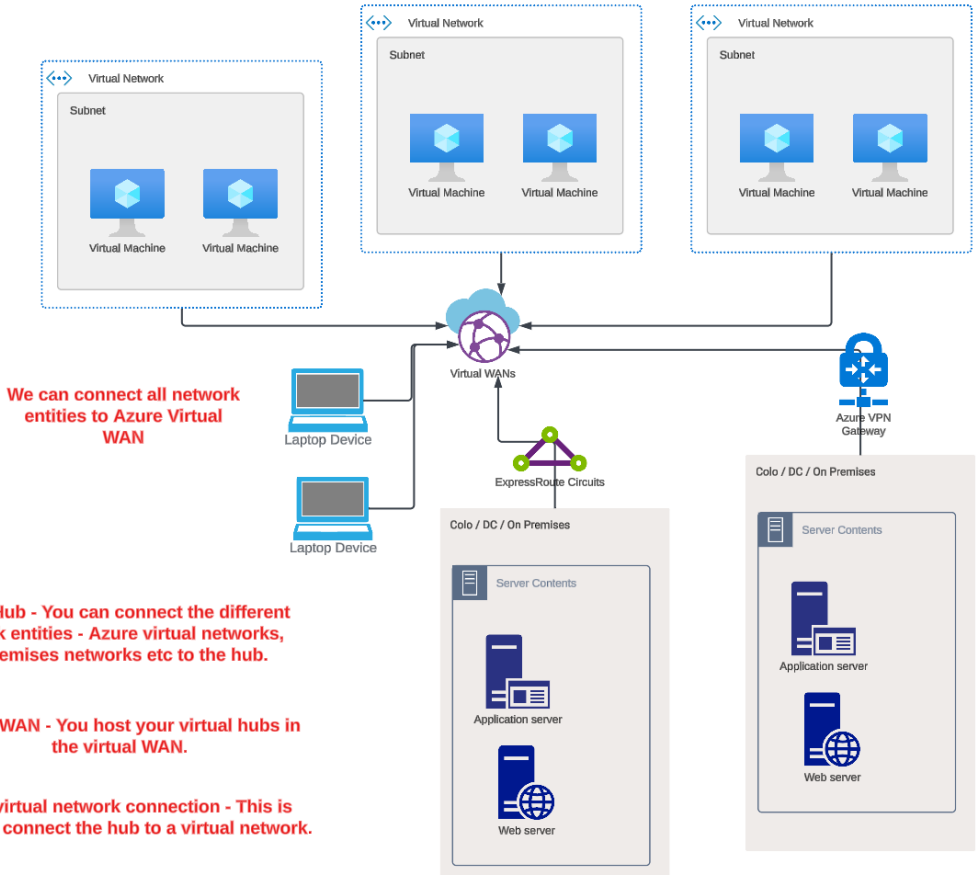

**The ExpressRoute circuit is a logical connection between on-premises and Microsoft cloud services.**

**Once you have an ExpressRoute circuit in place, you can then create Azure private peering connections to virtual machines and services using private IP addresses.**

**You can also create Microsoft peering connections to public services like Microsoft 365.**

# Azure Virtual WAN






## Virtual WAN types

There are two types of virtual WANs: Basic and Standard. The following table shows the available configurations for each type.

Expand table

| Virtual WAN type | Hub type | Available configurations |
|---|---|---|
| Basic | Basic | Site-to-site VPN only |
| Standard | Standard | ExpressRoute<br>User VPN (P2S)<br>VPN (site-to-site)<br>Inter-hub and VNet-to-VNet transiting through the virtual hub<br>Azure Firewall<br>NVA in a virtual WAN |

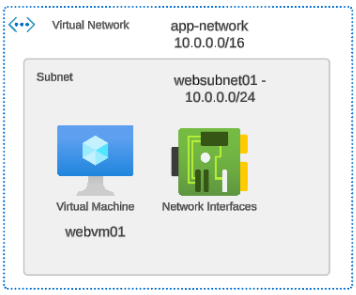
Reference - https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

# Lab - Virtual WAN

### Azure Virtual WAN Pricing

| Type | Price | Unit |
|---|---|---|
| Standard Virtual WAN Hub | $0.25/hour | 1 per Deployment Hour |
| Standard Virtual WAN Hub with Route maps or a Firewall Manager Policy for 3rd Party Integrations | $0.40/hour | 1 per Deployment Hour |
| Standard Virtual WAN Hub Data Processing | $0.02/GB | Per GB |
| VPN S2S Scale Unit[1] | $0.361/hour | 500 Mbps per Scale Unit, per Deployment Hour |
| VPN S2S Connection Unit[2] | $0.05/hour | 1 per Connection Unit per Deployment Hour |
| VPN P2S Scale Unit | $0.361/hour | 500 Mbps per Scale Unit, per Deployment Hour |
| VPN P2S Connection Unit | $0.013/hour | 1 per Connection Unit per Deployment Hour |
| ExpressRoute Scale Unit[3] | $0.42/hour | 2 Gbps per Scale Unit, per Deployment Hour |
| ExpressRoute Connection Unit | $0.05/hour | 1 per Connection Unit per Deployment Hour |
| NVA Infrastructure Unit | $0.25/hour | 500 Mbps per Unit, per Deployment Hour |
| Firewall NVA Data Processing (Load Balancer Related Charges) | $0.005/GB | Per GB |
| Routing Infrastructure Unit[4] | $0.10/hour | 1 Unit Per Deployment Hour |

Reference - https://azure.microsoft.com/en-us/pricing/details/virtual-wan/

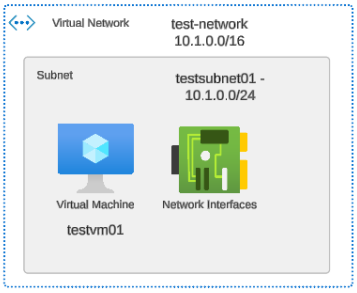

**Windows Server with Internet Information Services.**

**We will create a virtual WAN resource.**

**Then create a virtual WAN hub.**

**Create virtual network connections between the hub and the virtual network.**

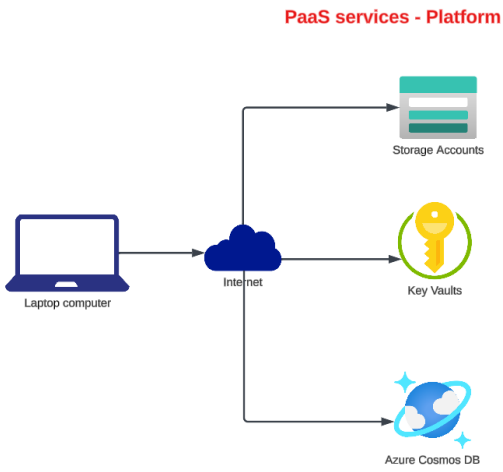
**Create a Point-to-Site VPN connection.**



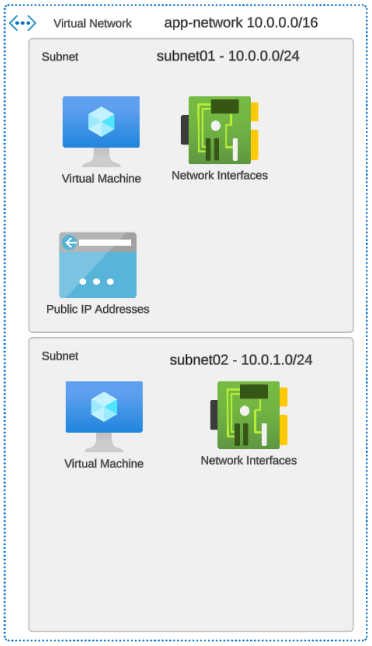

**Ubuntu Server**

**We will have two virtual networks in place. Ideally we would want to peer the networks together.**

# Securing access to PaaS services




We normally access these services via the Internet because they are public services.

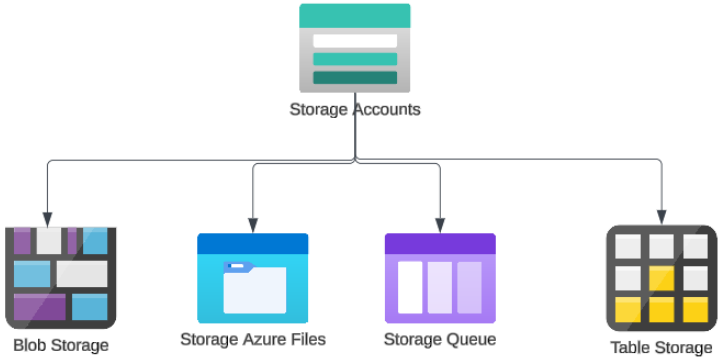



But we might have applications hosted on virtual machines that need to have private access to these services.

They don't want the requests to these services to traverse the Internet.

# What are Azure Storage Accounts

**Azure Storage Accounts - This is storage on the Azure cloud for your blob objects, files, queues and tables.**

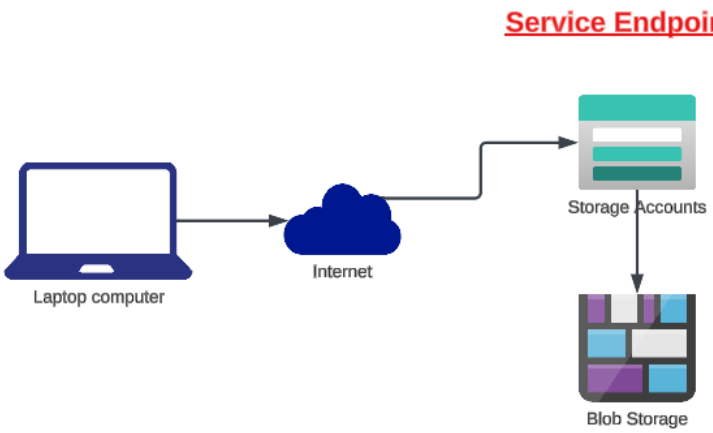



**Azure Storage Accounts provides 4 services.**


**This is used for storing a large amount of unstructured data. Suitable for storing images, documents, video and audio files.**


**The video and audio files could be stored in an Azure storage account.**

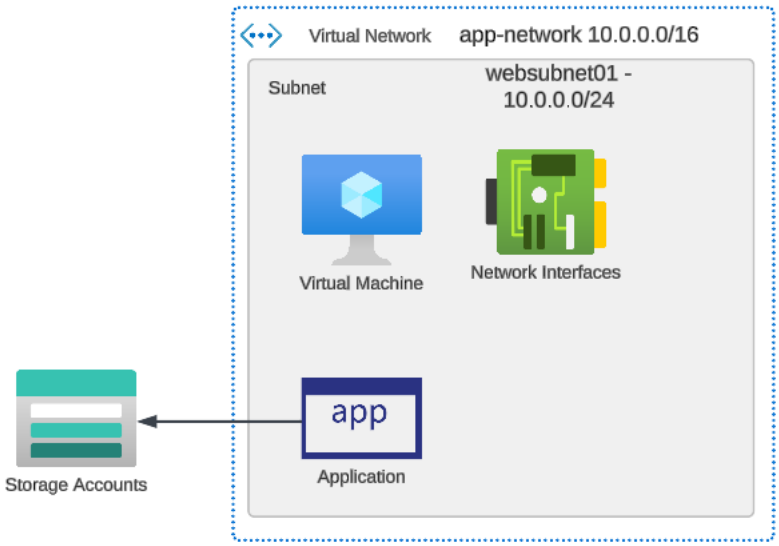
# Service Endpoints




The Azure Storage account service is a public service that is accessible over the Internet.

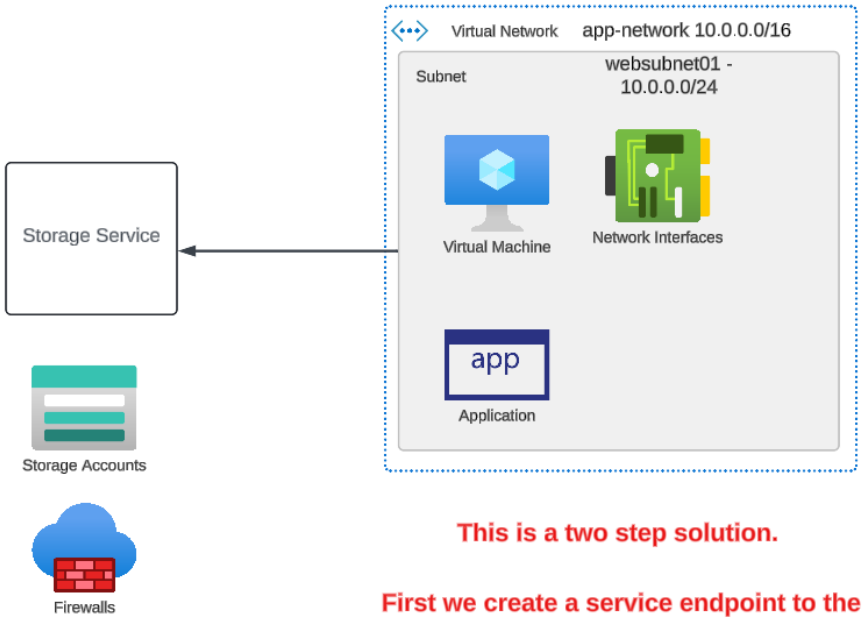
That means requests to the Azure storage account need to traverse over the Internet.

But let's say from a security perspective, you have an application that needs to privately access the storage account. Maybe the storage accounts stores sensitive information.




**Let's say that you have an application setup on an Azure virtual machine and you want to have secure and private access to the Azure storage account.**

**For this we can make use of service endpoints. With the help of service endpoints traffic to public services travels via the Microsoft Backbone network.**




**This is a two step solution.**

**First we create a service endpoint to the Microsoft.Storage service.**

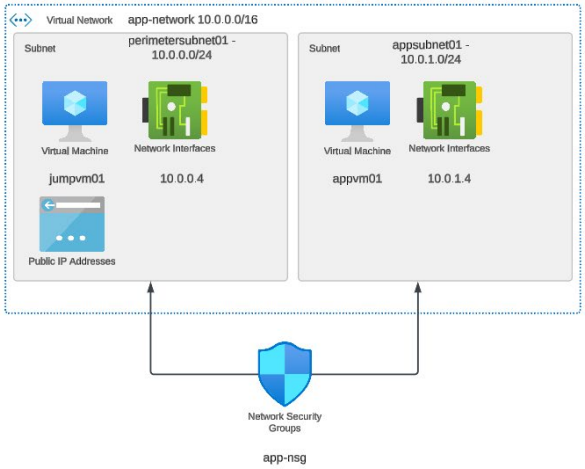
**Then from the Azure storage account, we use the firewall feature to only allow traffic from the subnet via the service endpoint.**

**The service endpoint itself does not block traffic from the Internet to the storage account. It's still is a public service.**

**At this point in time there is no additional charge for using a service endpoint.**

# Lab - Service Endpoints

We will create the following setup where we have a server that will act as a jump server. This would be public facing. We can then use this machine to log onto our internal virtual machines.

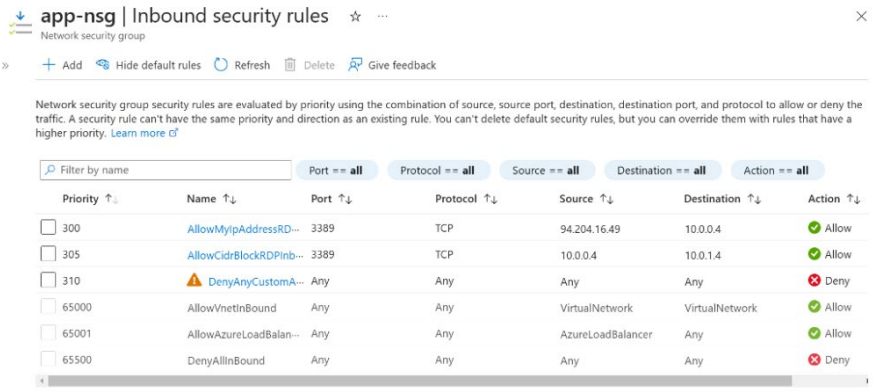


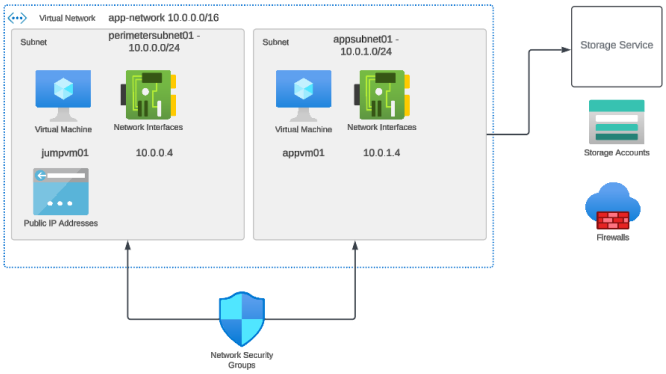


We will try to access an Azure Storage account from appvm01.

We will install Azure Storage Explorer on appvm01.

You will see that the virtual machine can still access the Azure storage account. This because currently Azure allows outbound access to the Internet from Virtual machines.

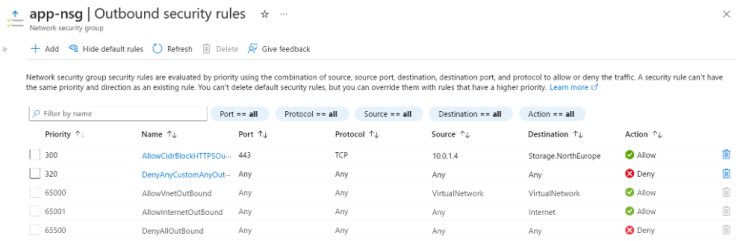





1. **Let's add a service endpoint to the storage service.**

2. **Then from the Firewall setting, let's only allow connections from our IP address and the subnet appsubnet01.**

**3. We can also modify the NSG for outbound traffic so that it is only allowed to the Azure storage service in the North Europe location.**



## What is Azure Cosmos DB


**Azure Cosmos DB is a fully managed NoSQL, relational and vector database.**

**You get fast access to your data.**

**Different API's**

NoSQL

**Data is stored in document format.**

**You can query for items using Structured Query Language (SQL)**

MongoDB

**Here documents are stored in BSON**

PostgreSQL

**Managed open source relational database with better performance.**

Apache Cassandra

**Here data is stored in a column-oriented schema.**

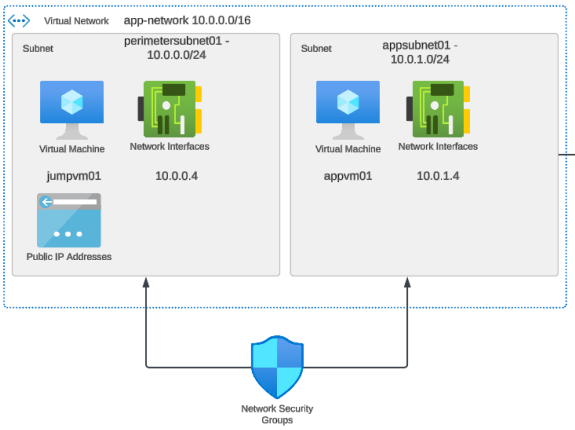
Gremlin

**This allows you to store graph-based databases.**

Table

**Store data in the form of key/value pairs.**

## Lab - Azure Cosmos DB - Service Endpoints

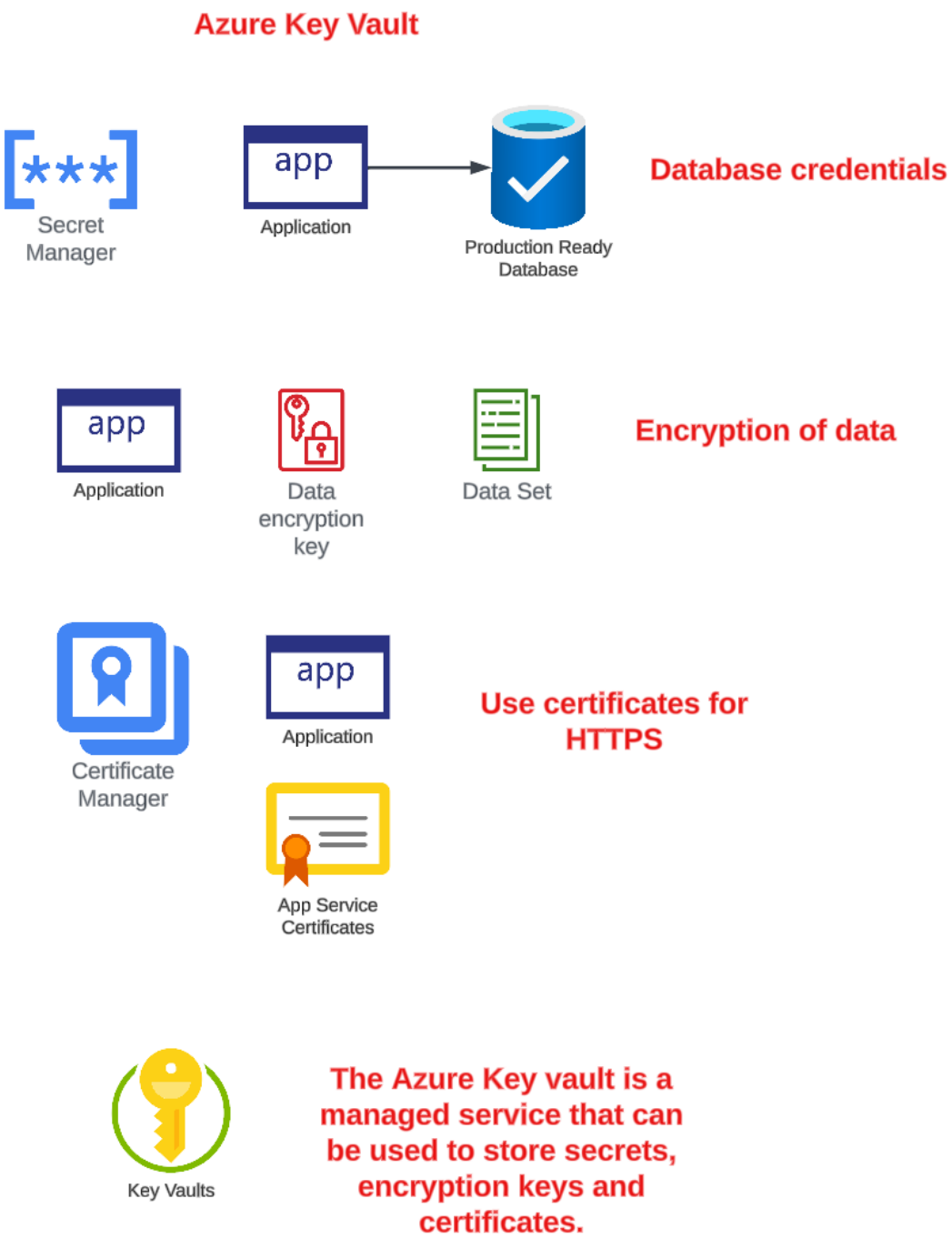




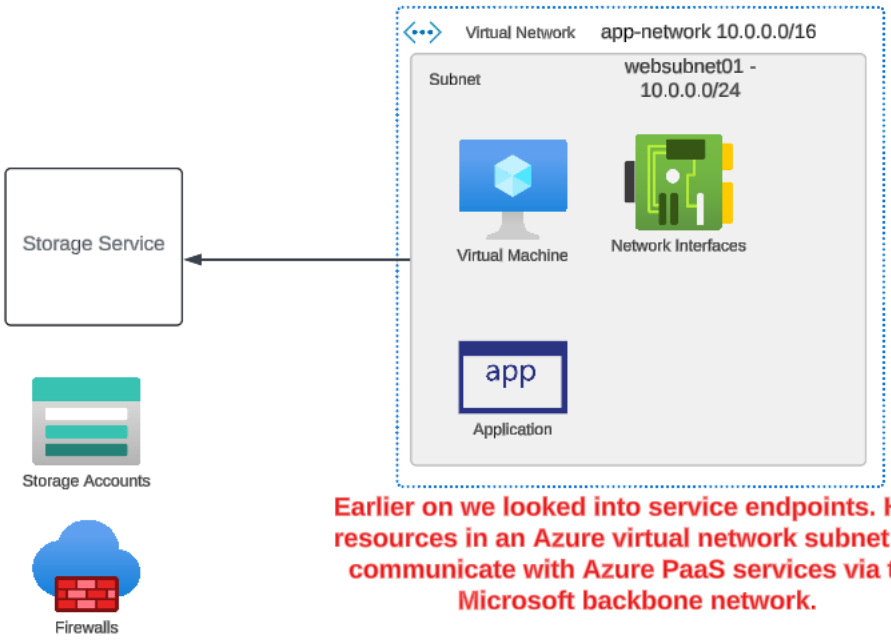
1. Let's add a service endpoint to the Azure Cosmos DB service.

2. Then from the Firewall setting, let's only allow connections from our IP address and the subnet appsubnet01.

## The Azure Key Vault service



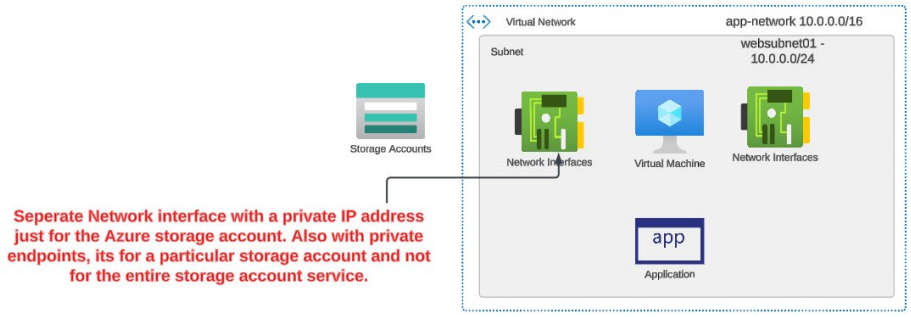
# Azure Private Endpoints




**Earlier on we looked into service endpoints. Here resources in an Azure virtual network subnet can communicate with Azure PaaS services via the Microsoft backbone network.**

**Azure private endpoints takes a step further for private communication between PaaS services and your virtual network.**

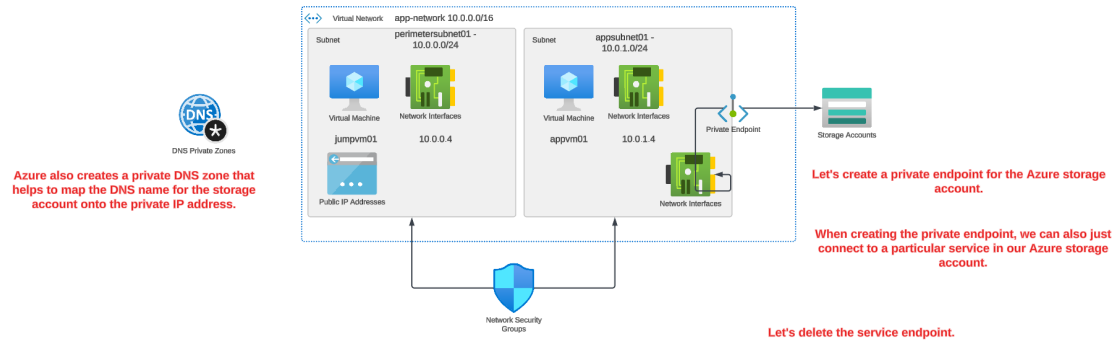
**Here this service creates a seperate network interface for your Azure PaaS service. It's like bringing your service into your virtual network. This is powered by Azure Private Link.**




| | |
|---|---|
| Private Link Service | No charge for private link service |
| Private Endpoint | $0.01 per hour |
| Inbound Data Processed | 0-1 PB - $0.01 per GB<br>1-5 PB - $0.006 per GB<br>5+ PB - $0.004 per GB |
| Outbound Data Processed | 0-1 PB - $0.01 per GB<br>1-5 PB - $0.006 per GB<br>5+ PB - $0.004 per GB |

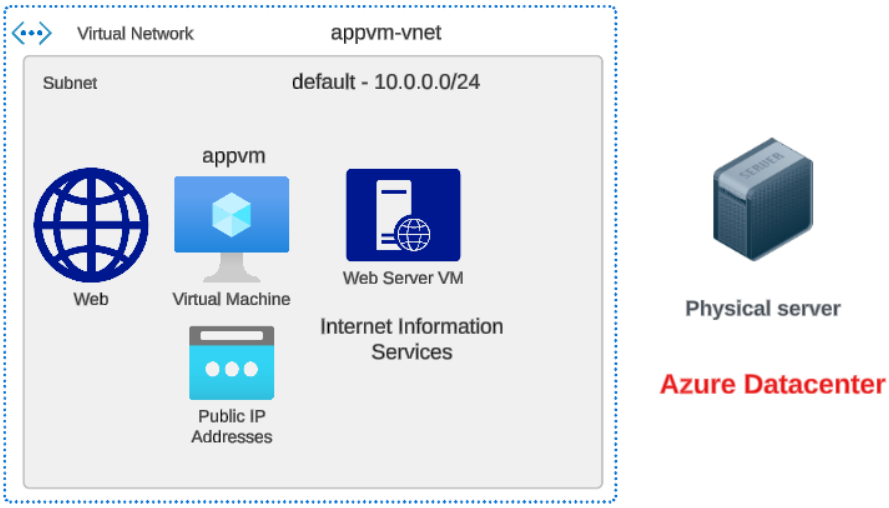
Reference - https://azure.microsoft.com/en-us/pricing/details/private-link/

# Lab - Azure Private Endpoints

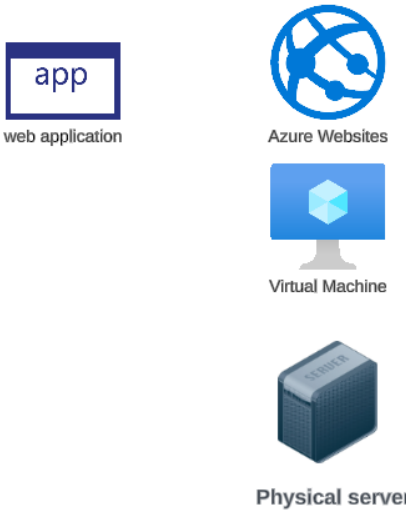


# What are Azure Web Apps

**Now we can host web applications on Azure virtual machines.**




**Azure Web App Service**




**This is a managed service. Here the virtual machine and physical infrastructure is managed for you.**

**There is support for web applications based on .NET, Java, Node.js, PHP, Python.**

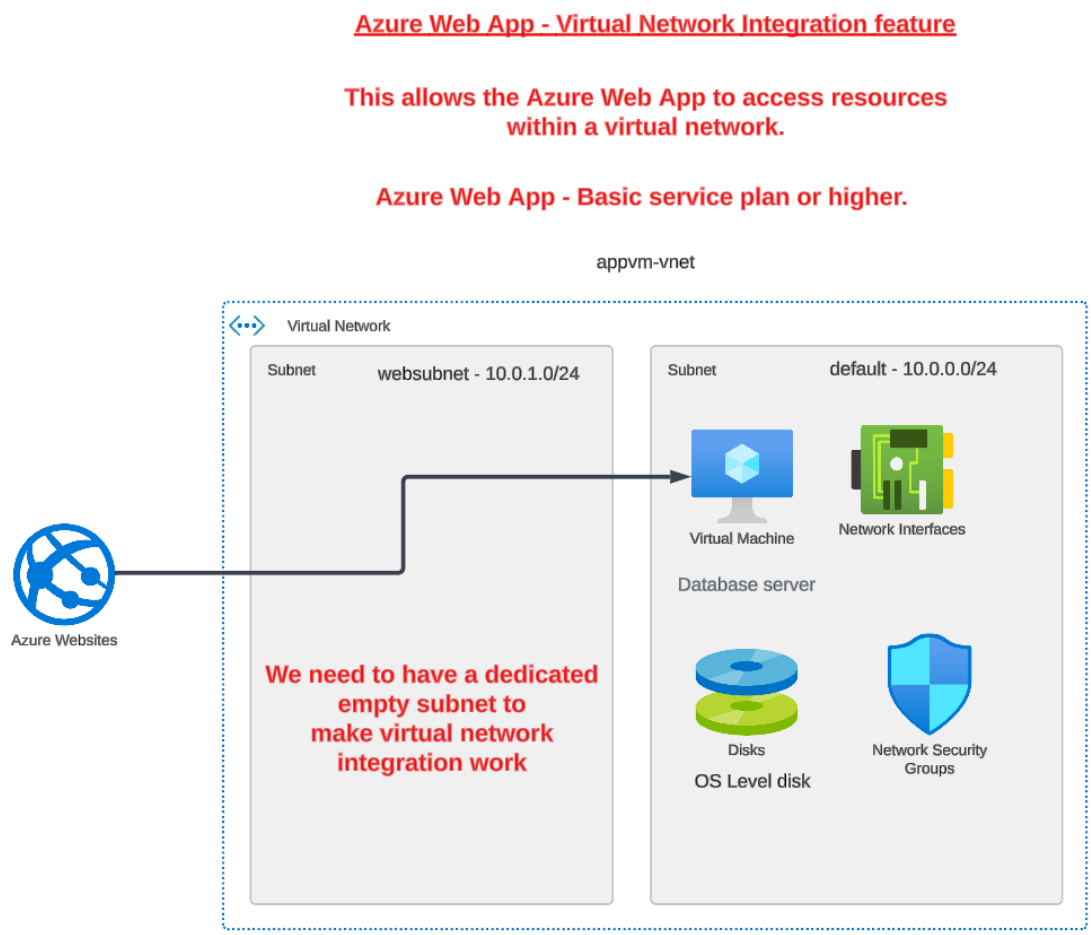
**Here the patching of the framework and the operating system is managed by the service.**

**You also get other features such as High Availability.**

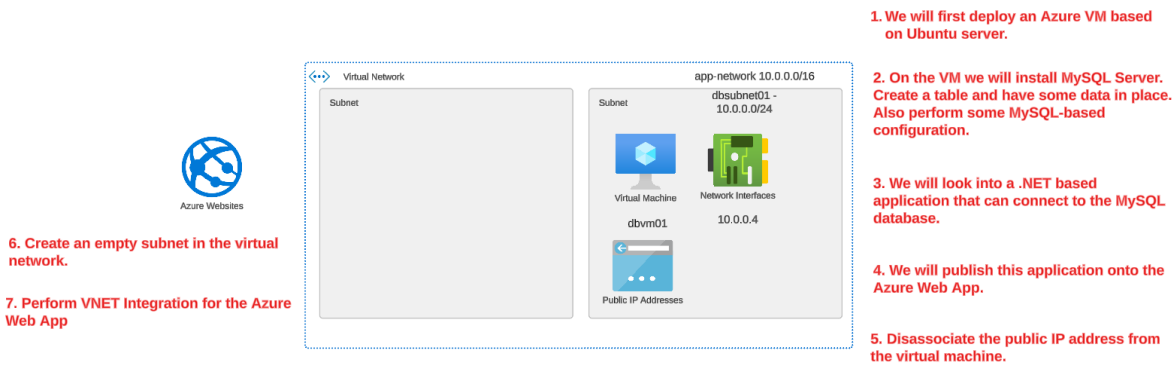
**If you have a web application that fits the framework and you don't want to manage the virtual machines, then you can opt for the Azure Web App service.**

**But if you need to host a custom application that needs to be installed, then you would probably need to use the Azure virtual machine service.**

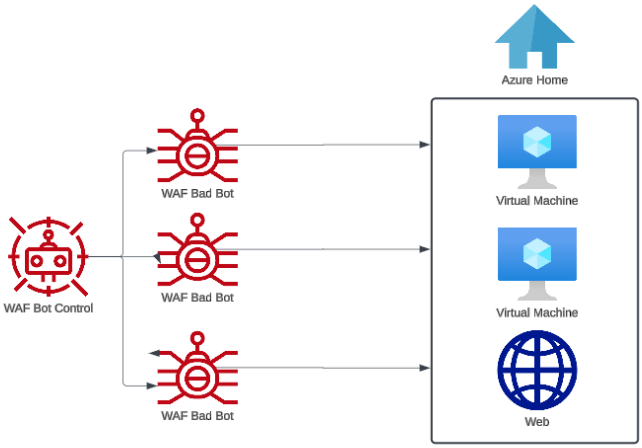
# Azure Web App - Virtual Network Integration




# Azure Web App - Virtual Network Integration - Implementation Overview



# Azure DDoS protection




A company has a web application residing on infrastructure on Azure.

The web application is an Internet-based application. Since its exposed to the Internet, it is also prone to attacks from the Internet.

One such attack is a DDoS attack - A distributed denial of service attack.


DDoS - Network Protection - This includes protection for a set of public IP resources.

DDoS - IP Protection - This is for an individual public IP resource.

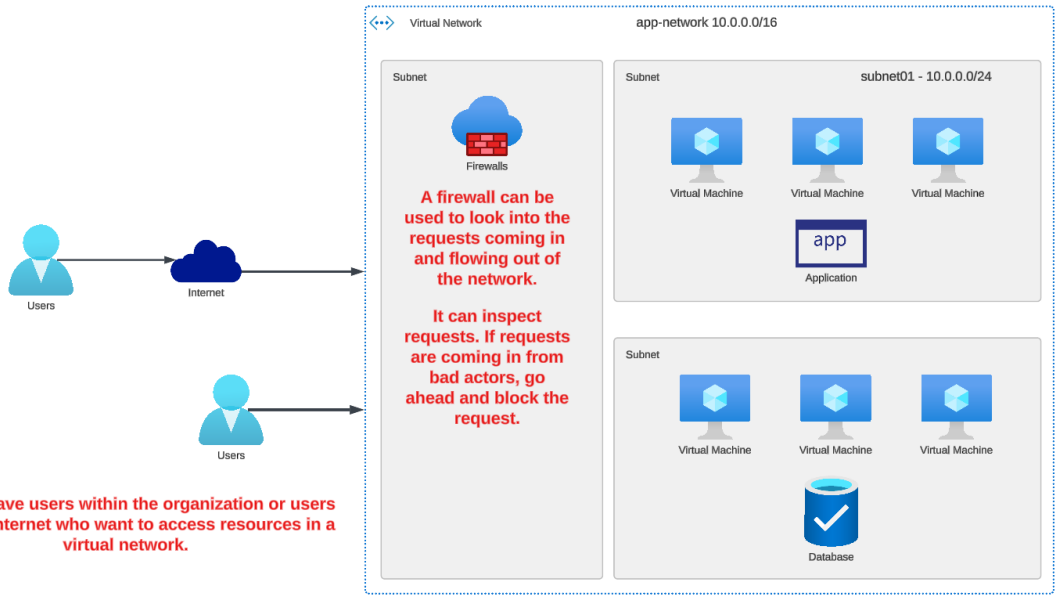
Features

1. The application traffic is monitored 24*7 to check for any sort of attacks.
2. You get real time metrics when an attack takes place.
3. You get access to a Rapid Response team.

# What is the Azure Firewall service

We have looked at Network Security Groups that can be used to filter the incoming and outgoing traffic.

But normally organizations want to have a full fledged firewall appliance for protecting their resources in networks.

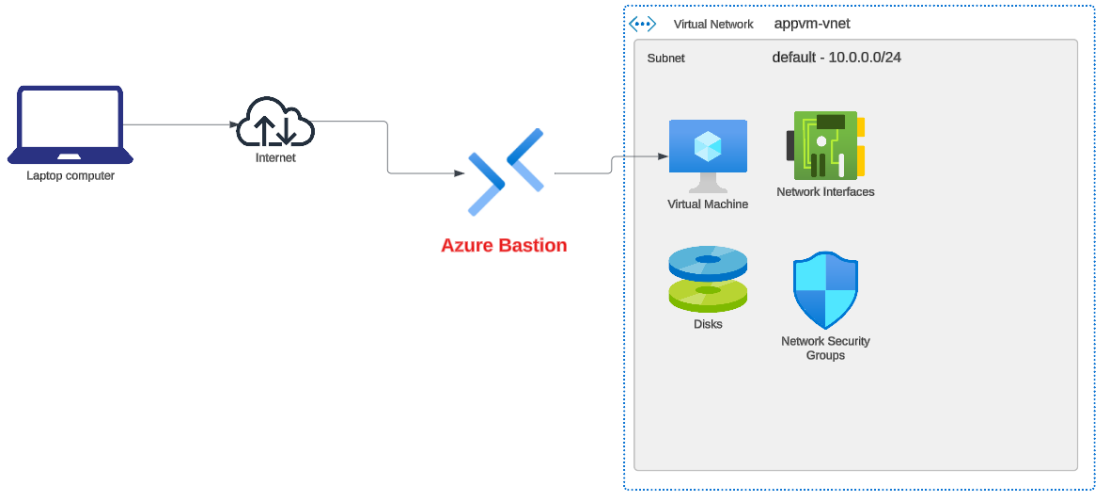



A firewall can be used to look into the requests coming in and flowing out of the network.

It can inspect requests. If requests are coming in from bad actors, go ahead and block the request.

You can have users within the organization or users from the Internet who want to access resources in a virtual network.

# What is the Azure Bastion Service




**This is a fully managed service that provides secure connections to virtual machines without the need of machines needing to have a Public IP address.**

**You can establish RDP and SSH connections to virtual machines from the Azure Portal.**

## Different SKU's available

| Feature | Developer SKU | Basic SKU | Standard SKU | Premium SKU |
|---|---|---|---|---|
| Connect to target VMs in same virtual network | Yes | Yes | Yes | Yes |
| Connect to target VMs in peered virtual networks | No | Yes | Yes | Yes |
| Support for concurrent connections | No | Yes | Yes | Yes |
| Access Linux VM Private Keys in Azure Key Vault (AKV) | No | Yes | Yes | Yes |
| Connect to Linux VM using SSH | Yes | Yes | Yes | Yes |
| Connect to Windows VM using RDP | Yes | Yes | Yes | Yes |
| Connect to Linux VM using RDP | No | No | Yes | Yes |
| Connect to Windows VM using SSH | No | No | Yes | Yes |
| Specify custom inbound port | No | No | Yes | Yes |
| Connect to VMs using Azure CLI | No | No | Yes | Yes |
| Host scaling | No | No | Yes | Yes |

| | Price[2] |
|---|---|
| Azure Bastion Developer | Free |
| Azure Bastion Basic | $0.19 per hour |
| Azure Bastion Standard | $0.29 per hour |
| Additional Standard Instance[1] | $0.14 per hour |
| Azure Bastion Premium | $0.45 per hour |
| Additional Premium Instance[1] | $0.22 per hour |

Reference - https://azure.microsoft.com/en-us/pricing/details/azure-bastion/

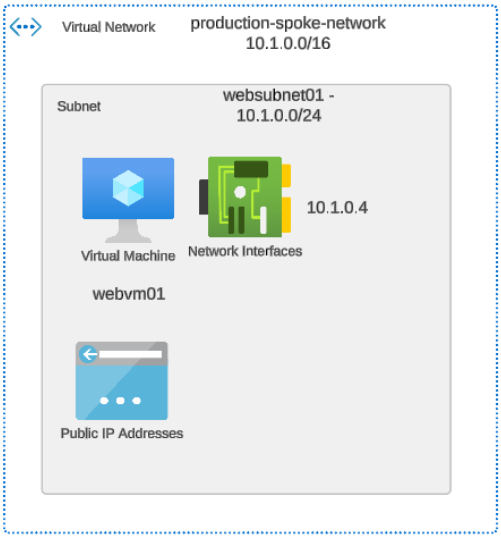
# Lab - Azure Firewall

**Azure Firewall setup**

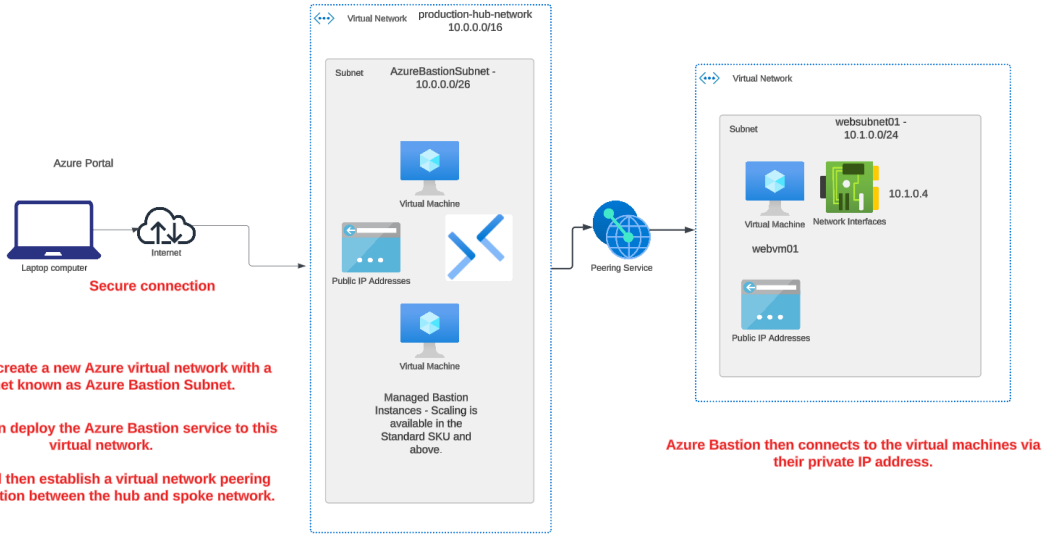
First let's deploy an Azure virtual machine based on Ubuntu server.

Let's not have an NSG and not have a Public IP address for the machine.

Note that we are creating a virtual network that is part of a hub-spoke design.




**Azure Bastion Setup**




Now let's create a new Azure virtual network with a subnet known as Azure Bastion Subnet.

We will then deploy the Azure Bastion service to this virtual network.

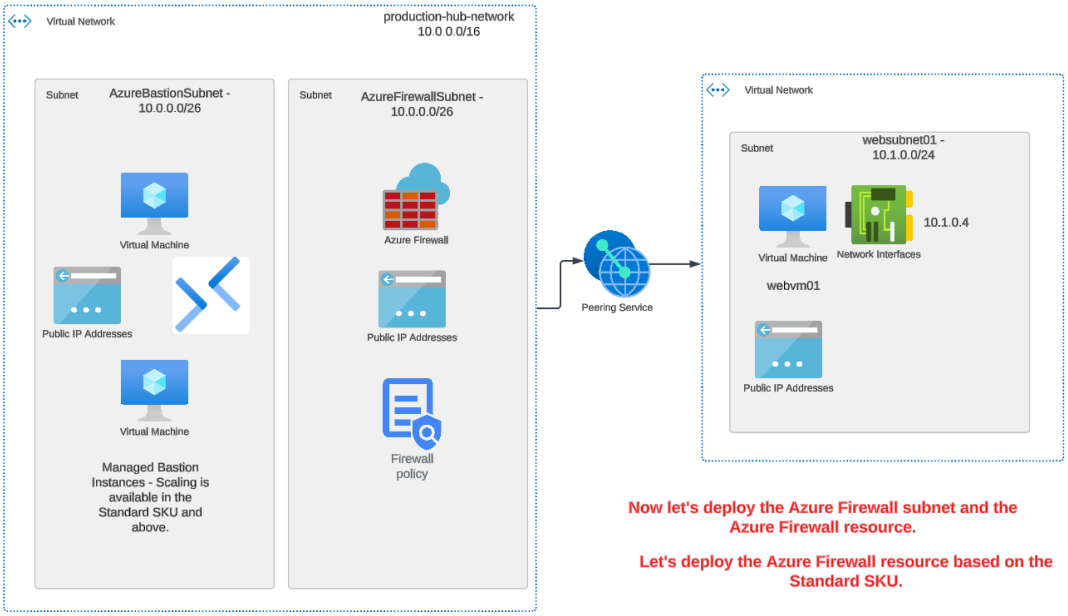
We will then establish a virtual network peering connection between the hub and spoke network.

Azure Bastion then connects to the virtual machines via their private IP address.

Then using the Azure Bastion service, we will log into the virtual machine and install a web server.

Note:- From the webvm01 machine we can still access the Internet.

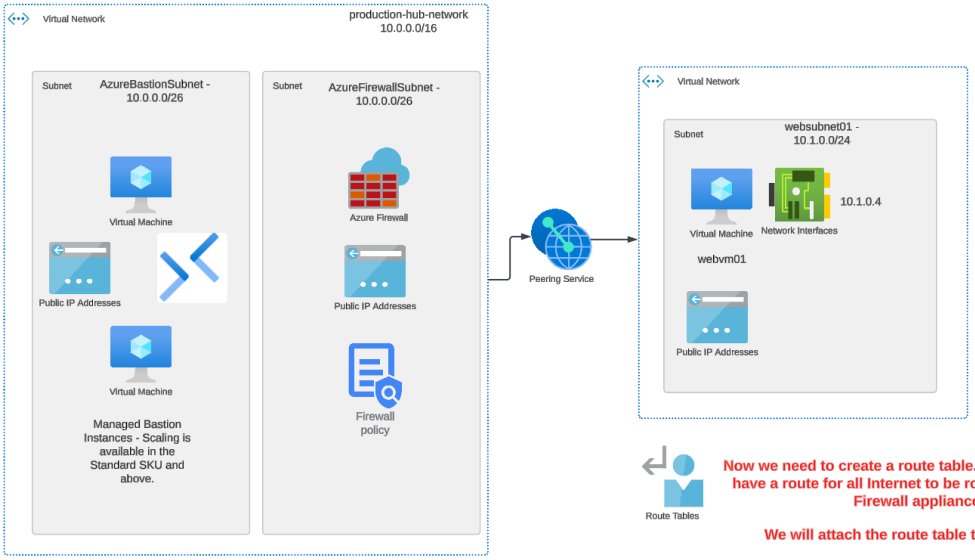
**Azure Firewall Deployment**




Now let's deploy the Azure Firewall subnet and the Azure Firewall resource.

Let's deploy the Azure Firewall resource based on the Standard SKU.

**Route traffic via Azure Firewall**




Now we need to create a route table. This table needs to have a route for all Internet to be routed via the Azure Firewall appliance.

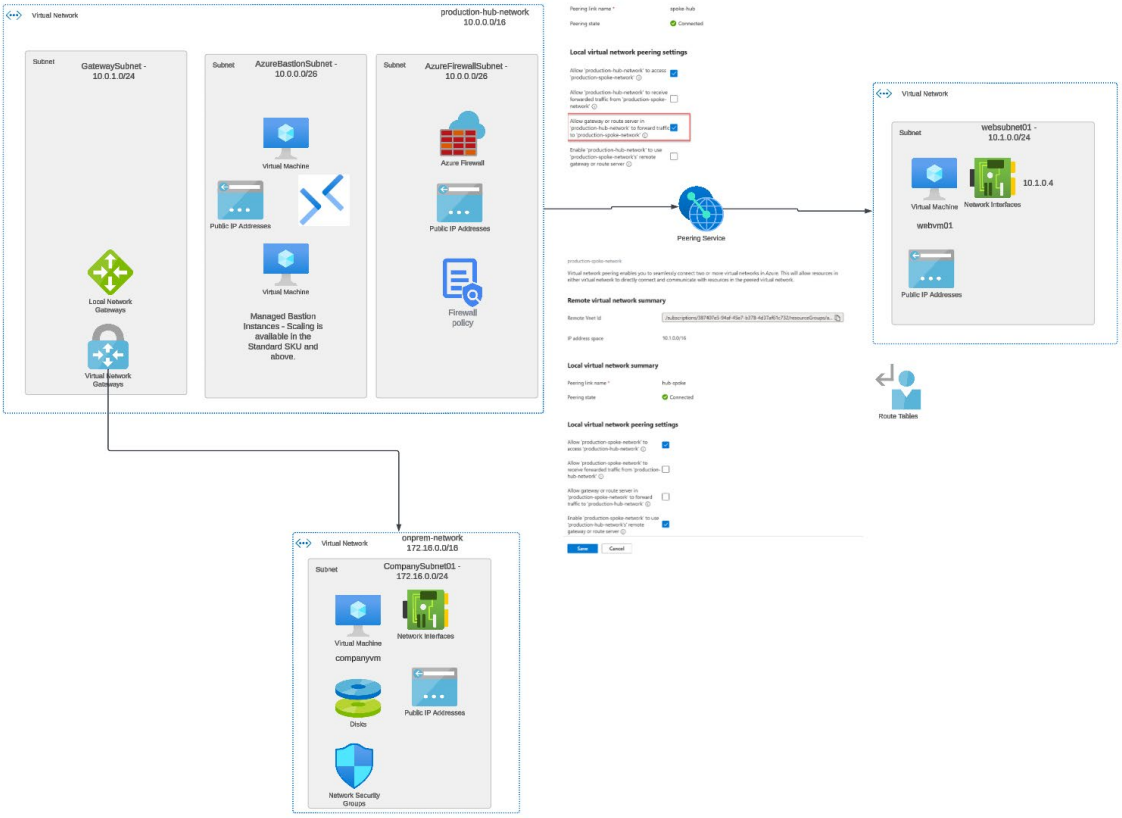
We will attach the route table to websubnet01.

As soon as you do this, outbound requests to the Internet will not be allowed from the webvm01 machine.

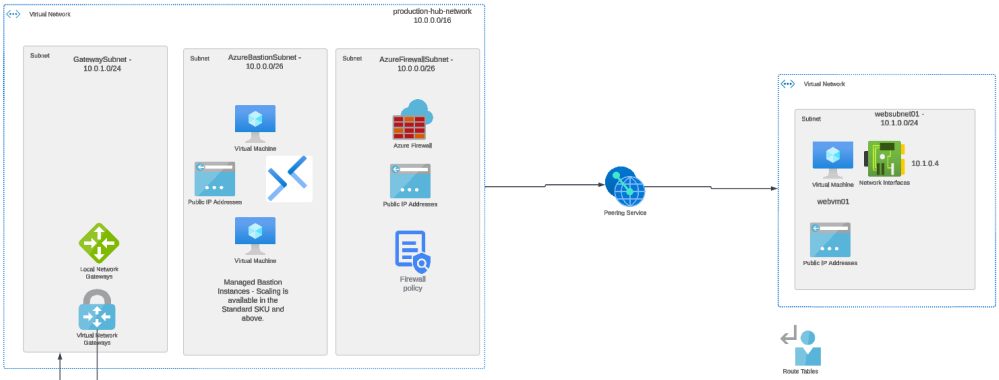
# Hub Spoke Architecture

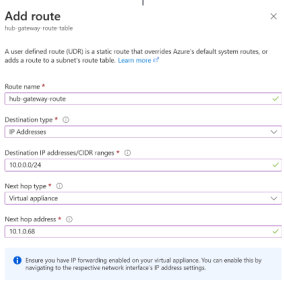
We can also connect our on-premises networks via Site-to-Site VPN connections.

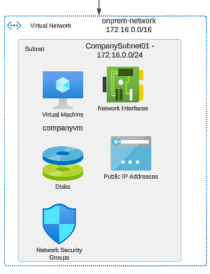
Step 1 : Update the virtual network peering connections



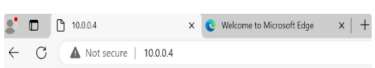

Step 2 : Create a new route table so that the hub gateway subnet can route requests via the Firewall appliance. This is for requests that need to be routed to the spoke network.



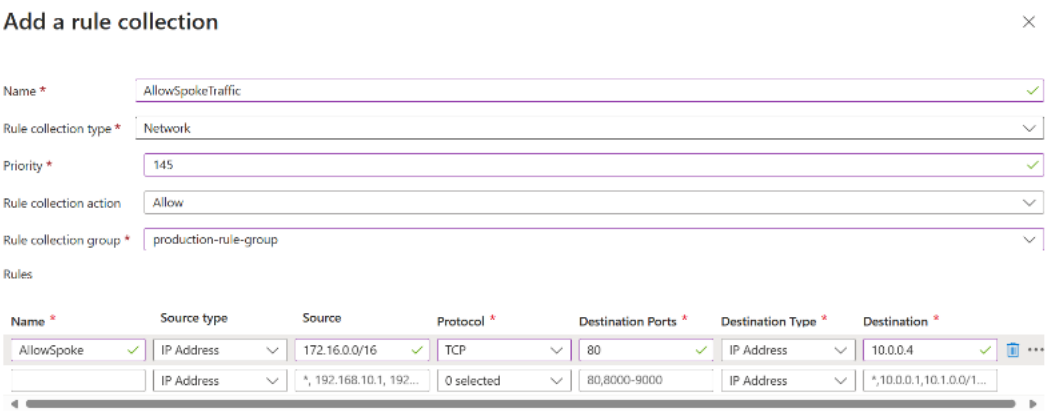




But then we will receive an error



We need to add a network rule

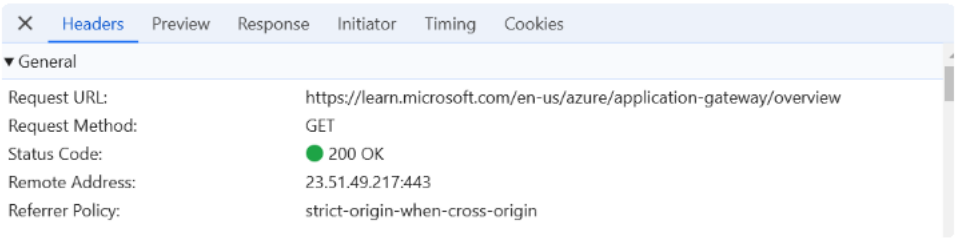



## Azure Application Gateway

**Azure Application Gateway**

**The Azure Application Gateway is a Layer 7 load balancer. Here the routing decisions can also be made based on the details of the HTTP request.**

**When you make a request for a URL, there are a lot of attributes associated with the HTTP request.**



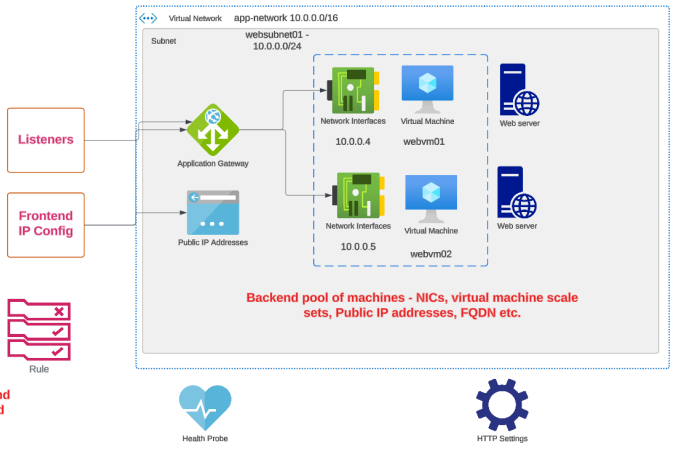

**The Azure Application Gateway can parse the HTTP request and route the request accordingly.**

The different components

The Listener listens for incoming client connections. Listeners are based on the protocol, port, hostname and IP address.

The Application Gateway has a Frontend IP address. All client requests are routed to the frontend ip configuration.

You can have a Public or Private IP address attached to the Front End IP configuration.




The rules are used to route requests to the backend targets. This is based on the listener, the backend server pool and the HTTP settings.



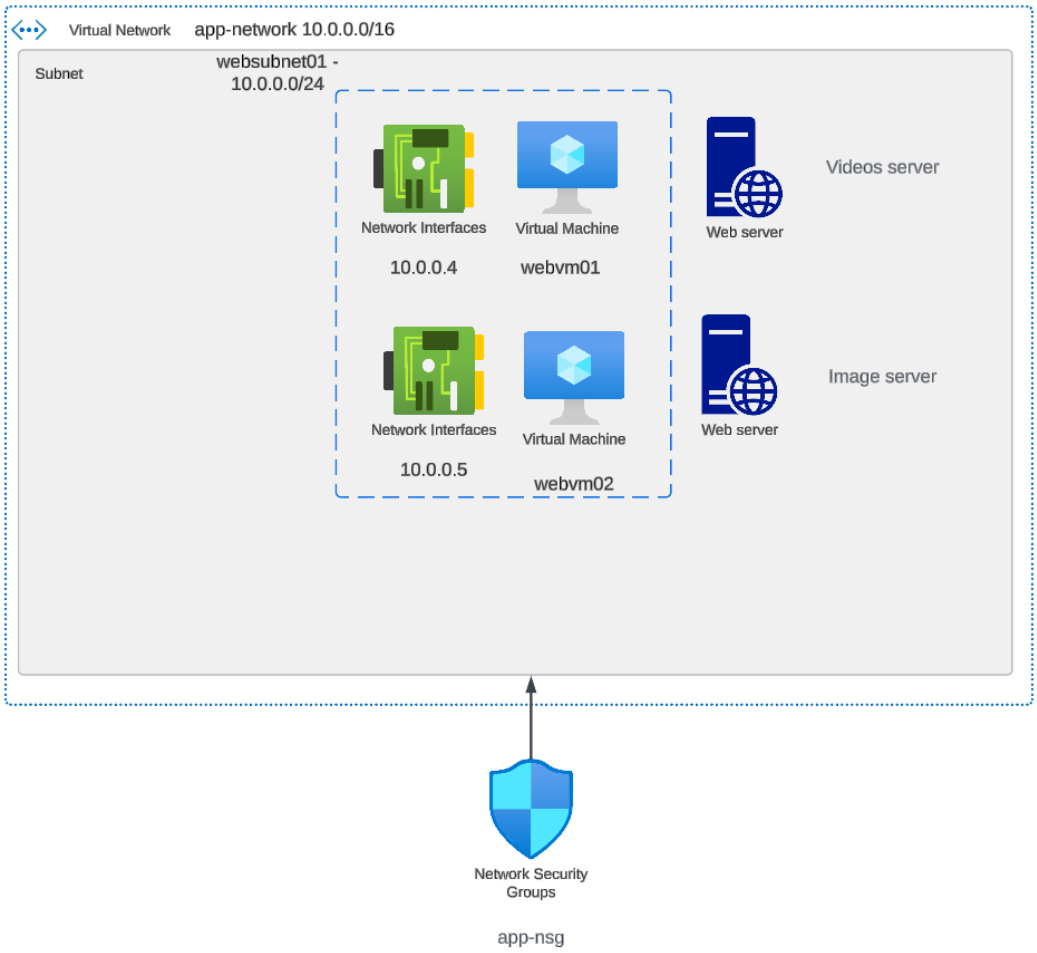

The Health Probe can be used to monitor the health of the backend resources.




Here you have settings such as the port number, protocol and encryption.

# Lab - Azure Application Gateway - URL Routing

## Azure Application Gateway Setup




**First let's define machines based on Ubuntu Linux that will become target resources in the backend pool for the Azure Application Gateway.**

**The machines will initially have a public IP address to install the web server. Later on we can disassociate the Public IP addresses.**

**The machines will have NGINX and html pages in place.**

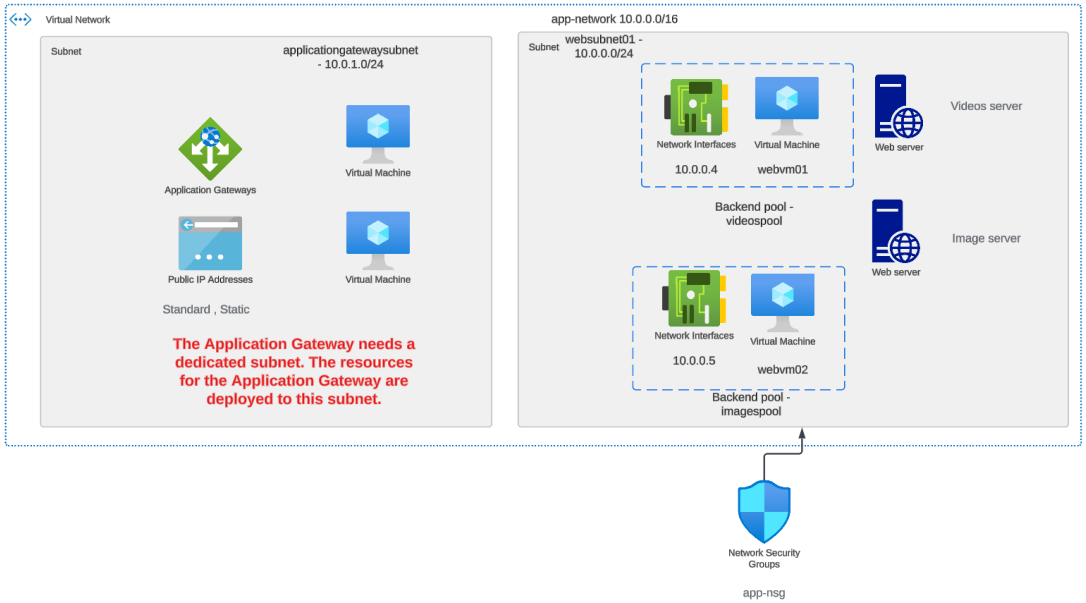
**We will have a Network Security Group attached to the subnet.**

## Azure Application Gateway Implementation

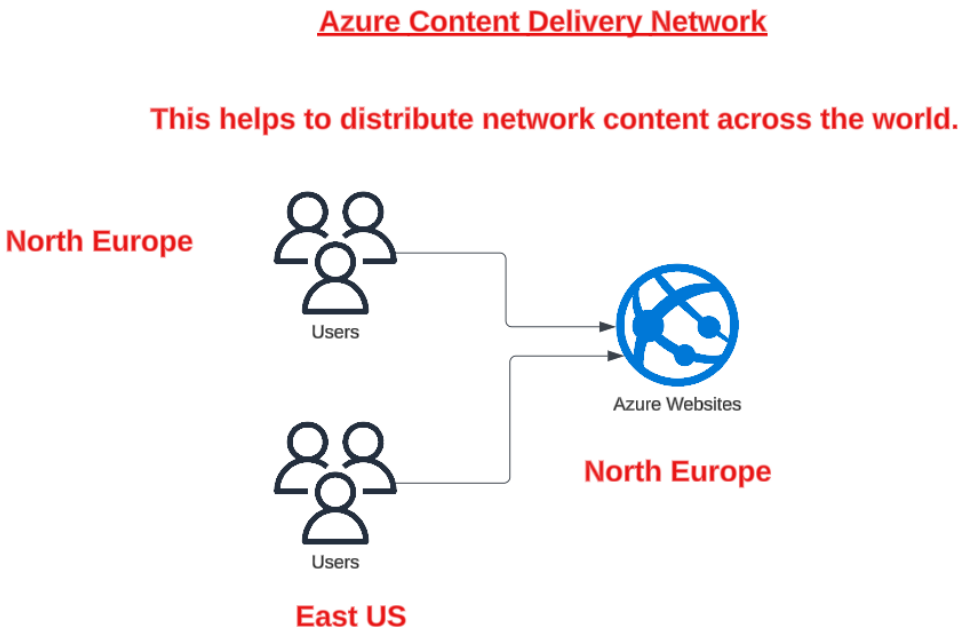
**We want to base the routing of requests based on the URL.**

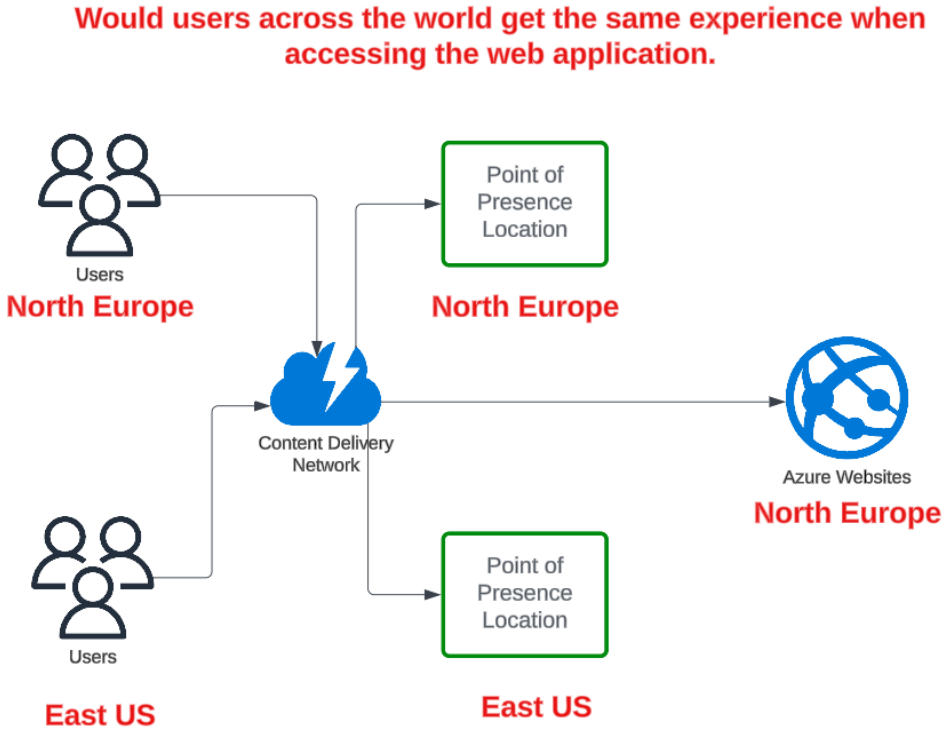
**If the URL contains /videos then the request needs to be directed to the backend pool that contains the videos server.**

**If the URL contains /images then the request needs to be directed to the backend pool that contains the images server.**



## Azure Content Delivery Network



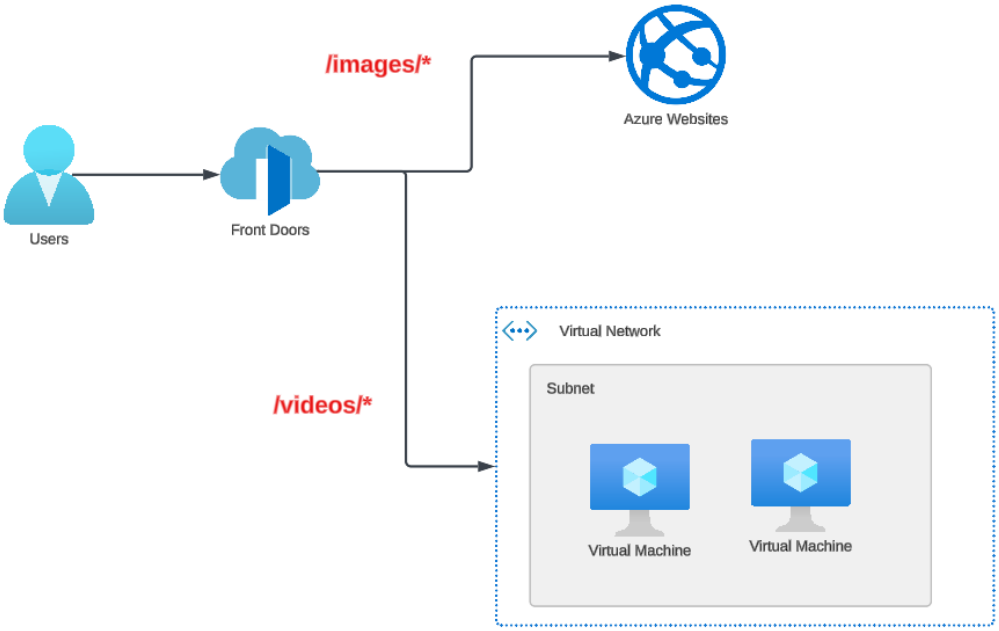

## Azure Front Door

This helps to deliver content to users with low latency and greater scale.

Its just an enhanced version when it comes to a CDN service.

Here content can be delivered efficiently via the use of point of presence locations across the world.

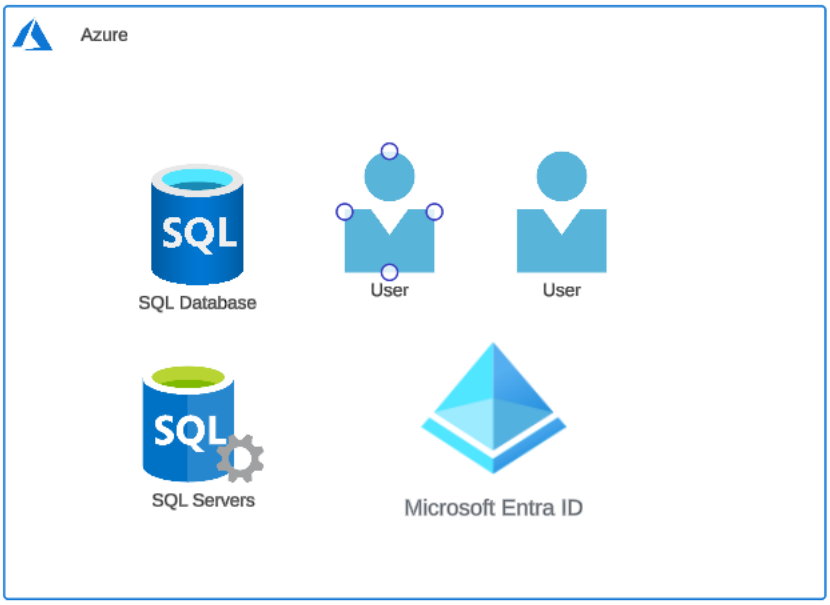
There are different features available with the Azure Front Door service. For example we can route requests based on domains and URL paths.




Caching is also available so that frequent responses can be taken from the cache instead of being processed from the origin server.

# Secure compute, storage, and databases

## Lab - Microsoft Entra database authentication




**Normally when we want users to access the data in the Azure SQL database, we create SQL users based on SQL Logins. We then give access to the SQL database users to objects in the database system.**

**But if we already have users defined in Microsoft Entra ID , we can enable Microsoft Entra database authentication and give the users access accordingly.**

**Let's first define two users in Microsoft Entra ID - dbadmin and dbusr**

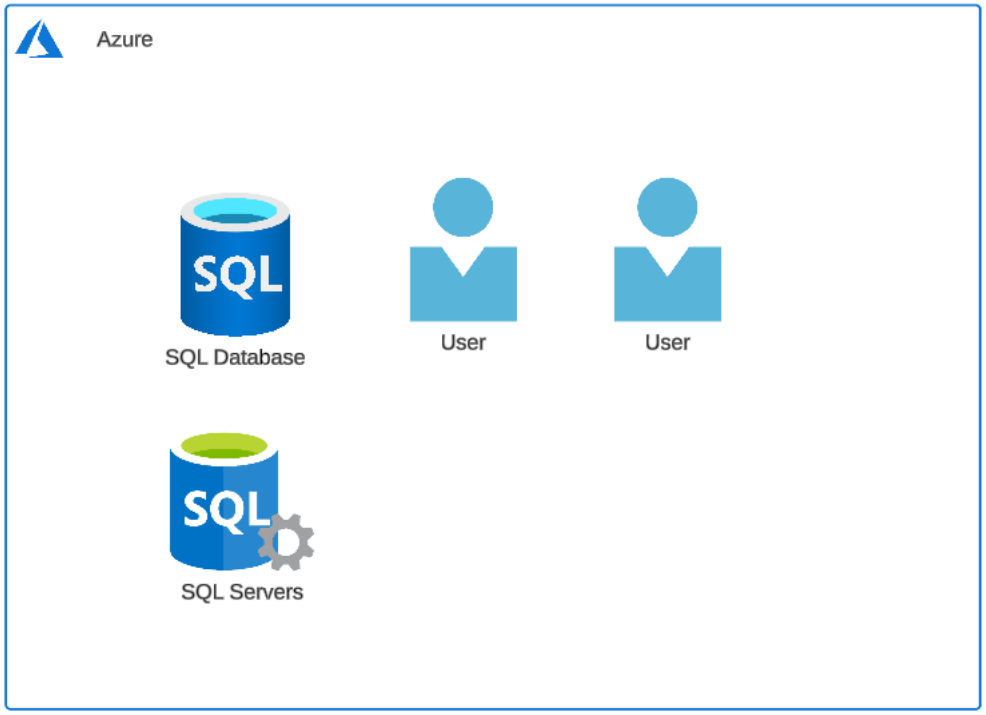
**For the Azure SQL database server, we can then set the Microsoft Entra admin as dbadmin.**

**Let's install Azure Data Studio on our laptop. We can use this free tool to log onto the Azure SQL database.**

**Let's connect to the Azure SQL database via the dbadmin user details.**

**Now let's add a new SQL user based on the dbusr login details in Microsoft Entra ID and give access to the database objects.**

# Lab - Enable Database auditing



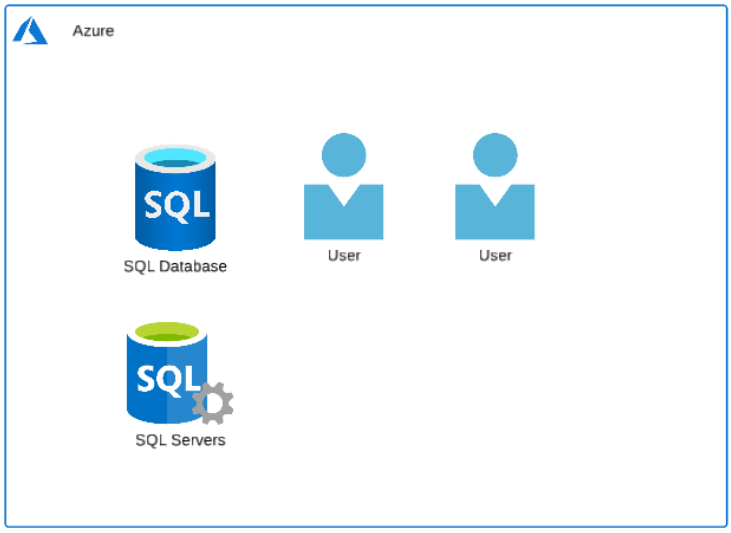

**We can enable Azure SQL database auditing - This can be used for regulatory compliance. You can get more insights into the database activity.**

**You can set the auditing at the database or the server level.**

**The database audit logs can be sent onto an Azure storage account, a Log Analytics workspace or Azure Event Hub. When configuring an Azure Storage account via the Azure portal , the database server and the storage account need to be in the same region.**

# Azure SQL Database Always Encrypted


**Storage of encryption key**




**You can enable the Always Encrypted feature when it comes to the Azure SQL database.**

**This helps to safeguard sensitive information such as credit card numbers and other sensitive information.**

**Here you need to make use of Encryption keys. There are two keys.**
**Column encryption key - This is used to encrypt the data in the column.**
**Column master key - This is the key-protecting key for the column encryption key.**

**The column master key can be stored in an Azure Key vault or a Windows Certificate Store.**

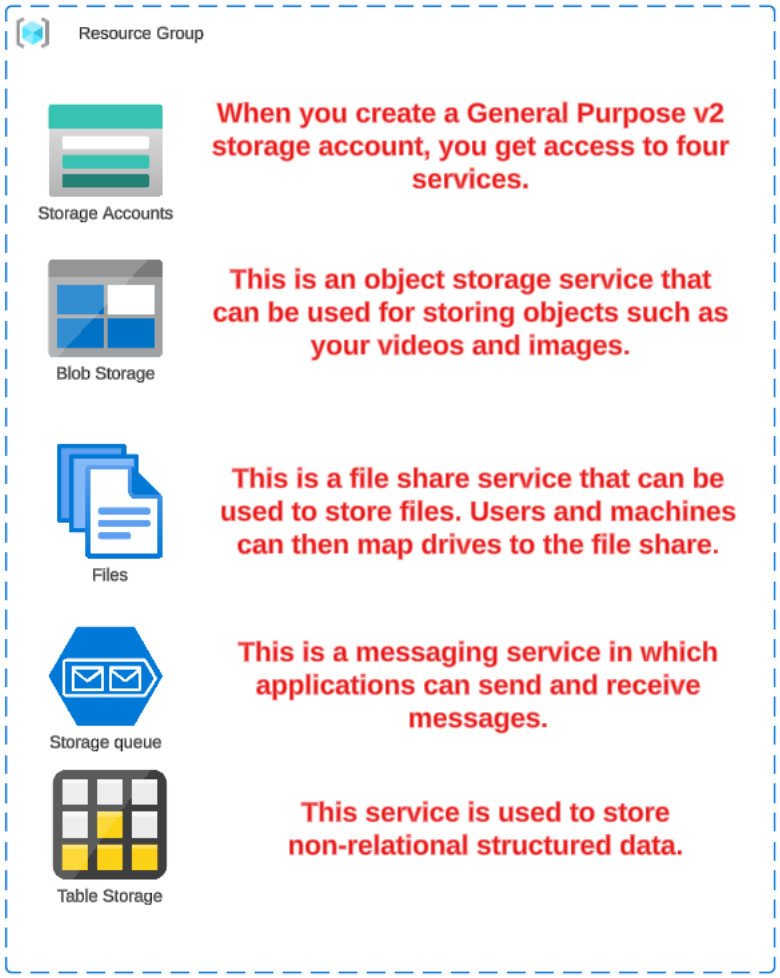
**You can use two types of encryption**

**Deterministic Encryption - Here the same encrypted value is always generated for the given plaintext value.**

**Randomized Encryption - Here the different encypted values are generated. But it doesn't support searching, grouping, indexing and joining on encrypted columns.**

**We need to use SQL Server Management Studio to enable the Always Encrypted feature.**

# Securing access to Azure Storage Accounts




**We will focus on how to securely access the data in a storage account for the various services.**

## Authorization to the Azure Blob service




**We can enable anonynous access for a container.**
**This will allow any user to access the data in the container.**


**Using Access Keys - This is like a secret or password that allows you to access all of the services and all data in an Azure Storage account.**

## Using the Shared Access Signature

**Here we can grant limited access to our data in the Azure Storage Account - Here we can grant permissions service wise, give permissions for different actions, provide a start and end expiry time.**

**We can create a Shared access signature at the blob level, the container level and the Storage account level.**

# Lab - Shared Access Signature - Blob Service - Permissions example





Allowed services ⓘ

☑ Blob ☐ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☑ Service ☑ Container ☐ Object

Allowed permissions ⓘ

☑ Read ☐ Write ☐ Delete ☑ List ☐ Add ☐ Create ☐ Update ☐ Process ☐ Immutable storage ☐ Permanent delete

Blob versioning permissions ⓘ

☐ Enables deletion of versions

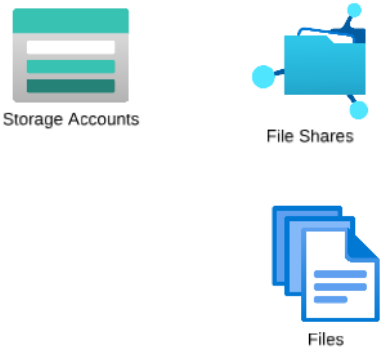
Allowed blob index permissions ⓘ

☐ Read/Write ☐ Filter

**What would be the result of using the above Shared Access Signature?**

**We should be able to list the containers and list the objects in the container, but we will not be able to read an object in the container.**

# Lab - Shared Access Signature - File Service - Permissions example




**What would be the result of using the above Shared Access Signature?**

Allowed services ⓘ

☐ Blob ☑ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☑ Service ☑ Container ☐ Object

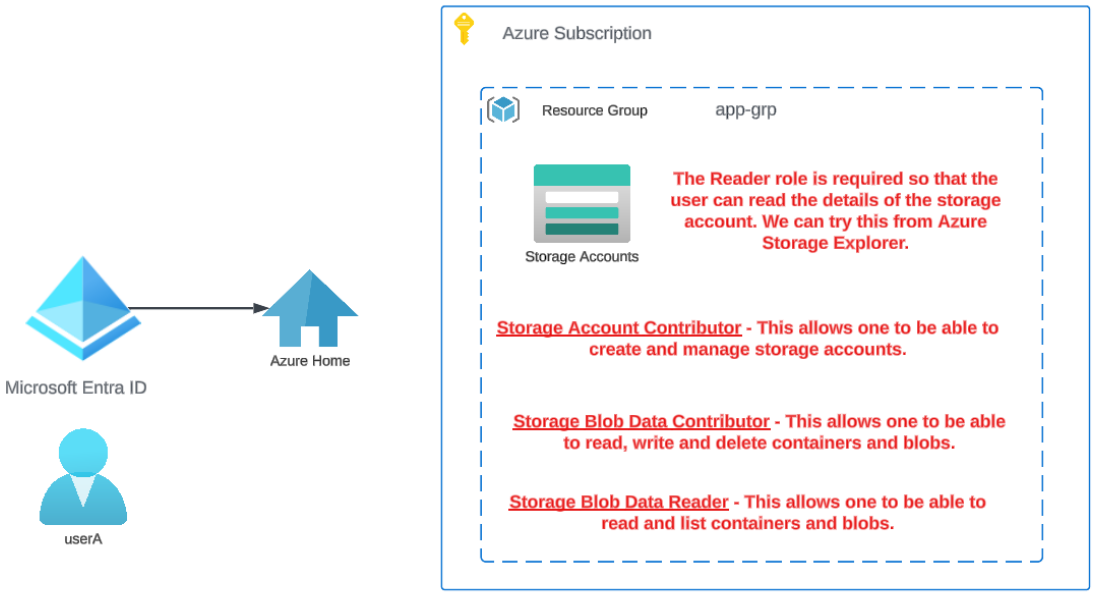
Allowed permissions ⓘ

☑ Read ☐ Write ☐ Delete ☑ List ☐ Add ☐ Create ☐ Update ☐ Process

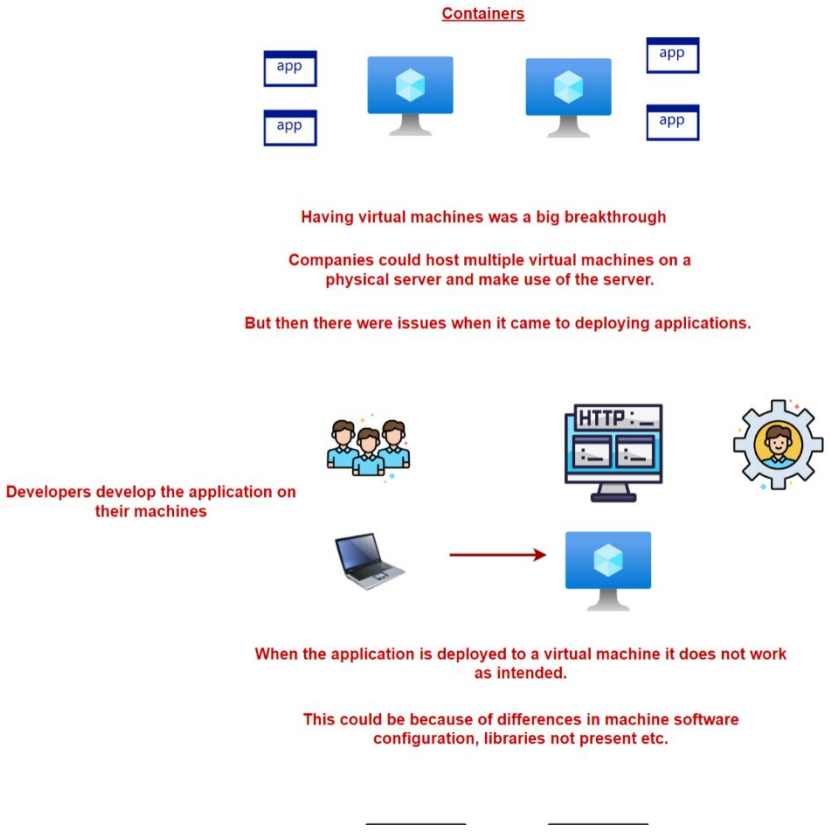
☐ Immutable storage ☐ Permanent delete

**Again we can access the file share and list the files in the file share. But we can't access each individual file.**

# Lab - Role assignments for Azure Storage Accounts - Blob service




# Understanding the container landscape




You have 2 applications on the same machine.

One application update requires a library/component to be installed.

This causes the other application to stop working.

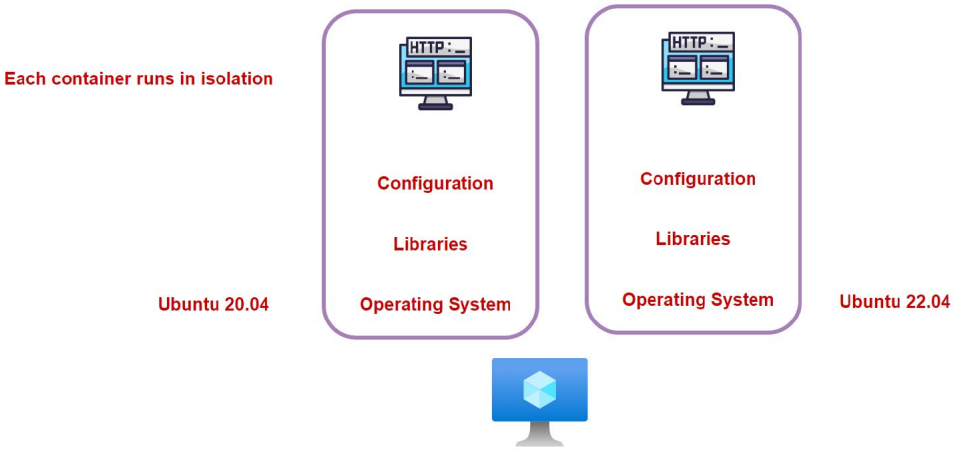
## Welcome to containers

This is a unit of software that packages up all the code and dependencies that are required for the application to run.

## CONTAINER ARCHITECTURE

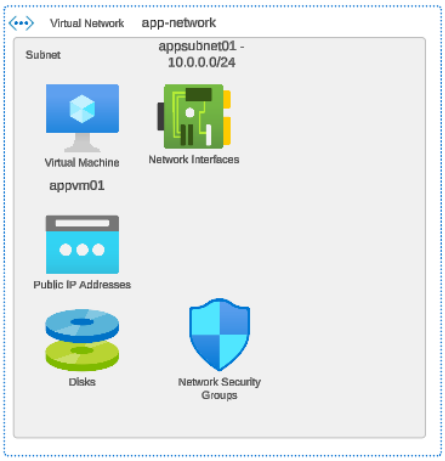
The underlying container will have a light-weight operating system, the application, libraries etc.

Each container runs in isolation



# Lab - Deploying Docker on a virtual machine

We will first deploy a Linux-based virtual machine.

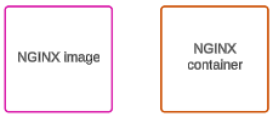




If you wanted to host a web application , we would first need to install a Web server and then host our web application.

For example, we can install the NGINX web server.

But we will run NGINX via the use of Docker containers.




We will then run the NGINX web server in a Docker-based container.

The container is run by first downloading the NGINX image from an online repository known as Docker Hub.


We will first install the Docker tool set on the virtual machine.

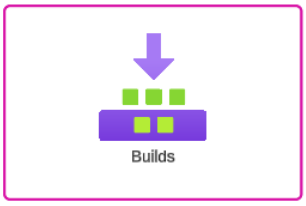
# Lab - Azure Container Registry

There are readymade images available on Docker Hub.

You can use these images to run containers.

But let's say we want to run our own application within a container.






We can take our code, create a build and use Docker to first create an image that would contain our application.

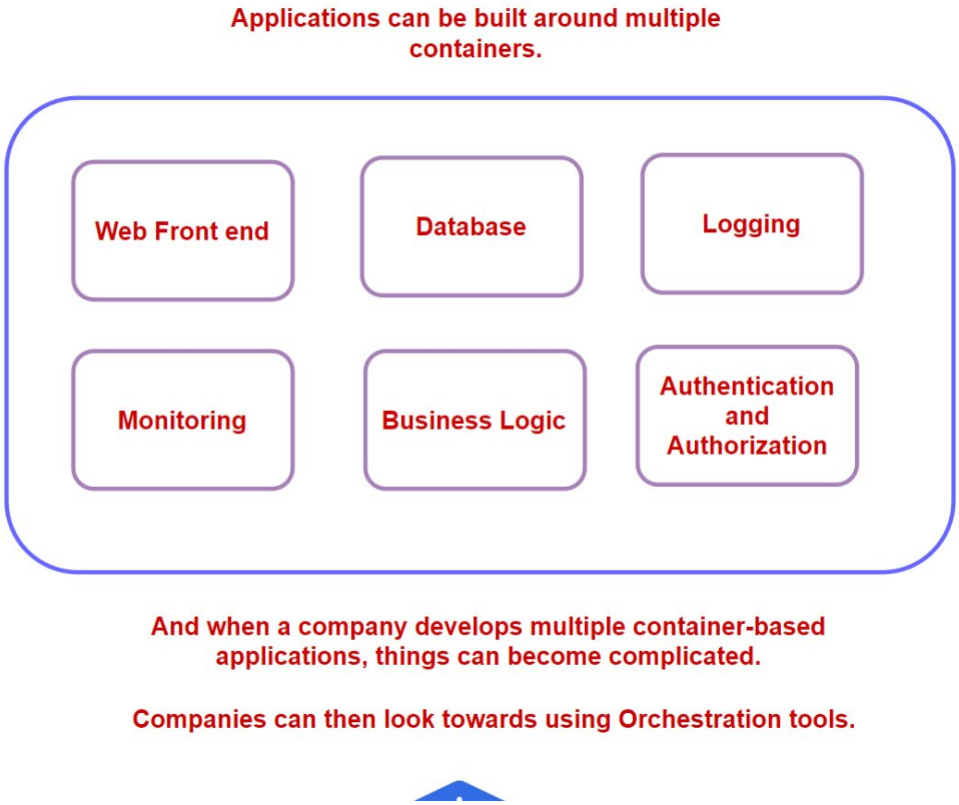

We can then run a container out of the image and hence run our application.


We need a place to store our newly created application image. We can store it in Docker Hub. Or use an Azure service known as Azure Container Registry. This is a private registry that can be used for storing your Docker-based images.

What are we going to do

1. Have an application in place
2. Containerize the application into a Docker image using the Docker toolset - This will be done on the Linux machine where we have Docker installed.
3. Publish the Docker image to the Azure Container Registry.

# Lab - Using Azure Kubernetes



Companies can then look towards using Orchestration tools.

A popular tool when it comes to container-orchestration is Kubernetes.

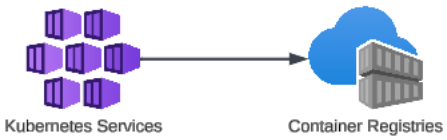
It's an open source platform that is used for managing your containerized workloads and services.

## Features provided

1. It can restart containers if they fail
2. You can load balance traffic across your containers.
3. You can dictate the state of the services that need to run.
4. You can mount different storage systems when it comes to persistence of data.
5. You can scale up your services whenever required.

We will build a new Kubernetes cluster.

We will build a new Kubernetes cluster.

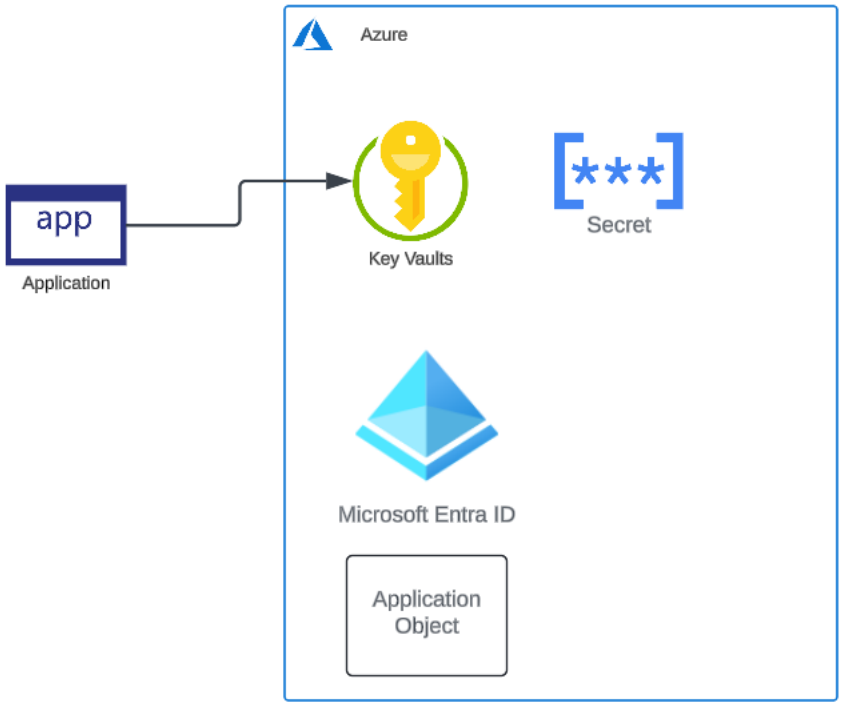



We will deploy our application as a container onto the Kubernetes cluster. Here the cluster will take the Docker image available in the Azure Container registry.

In order for the Kubernetes service to authorize itself with the Azure Container Registry, Azure will create a managed identity for the Kubernetes cluster and assign the AcrPull role to the identity.

## Manage security operations

## Using an application to access secrets




**Let's see how a simple application can be used to access the secrets in the key vault.**

**Note that we can now define an application object in Microsoft Entra ID to represent our application.**

**And then we can give access to the application object to the secrets in the key vault.**

# Lab - Azure Key Vault soft delete

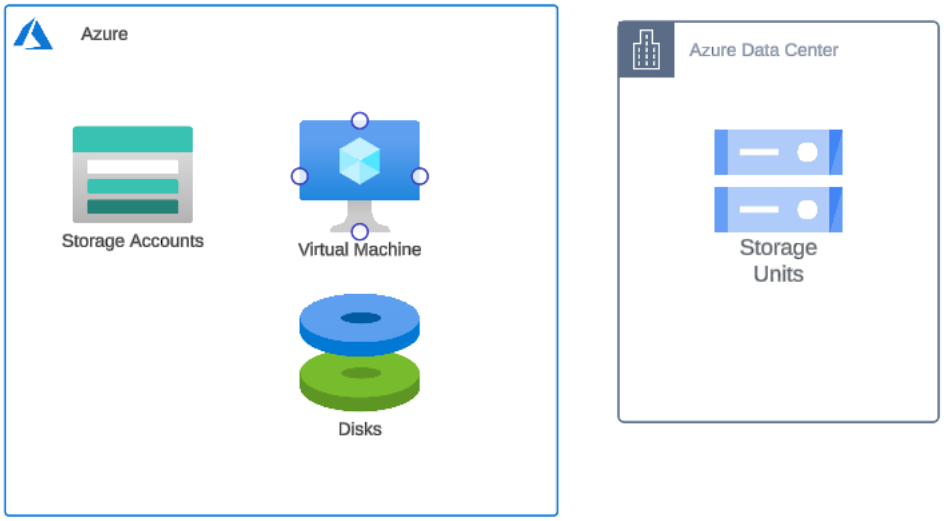

**This feature allows you to recover the deleted vaults or the deleted key vault objects - keys, secrets , certificates.**

**You can configure the recovery time - between 7 - 90 days.**

**In order to permanently delete a secret, you need to perform 2 steps - delete the object. This puts the object in a soft-deleted state. Then purge the object in the soft deleted state.**

**When purge protection is enabled, you cannot permanently delete a vault or an object until the retention period has passed.**

## Encryption at rest




**When we store data using Azure storage accounts or on disks attached to an Azure virtual machine, we need to understand in the end that the data is physically stored on disks located on storage units in Azure data centers.**

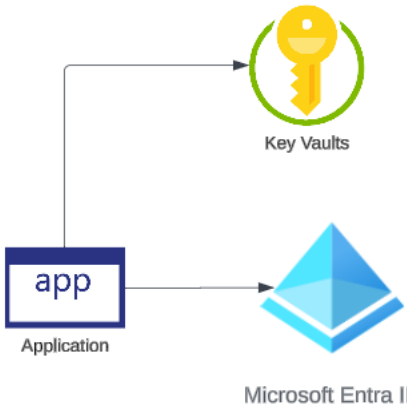
**Micrrosoft does have a lot of security protocols and features to protect the data. But as a customer we are also responsible for the data we store on Azure-based services.**

**Azure offers to encrypt data at rest, when the data is finally stored on the physical disks in the Azure data center.**

**When creating Azure storage accounts, the data is also encrypted using Microsoft Managed keys. We can also use keys defined in the Azure Key vault service.**

**There are also different layers of encryption available when it comes to disks attached to an Azure virtual machine.**

# Managed Service Identity

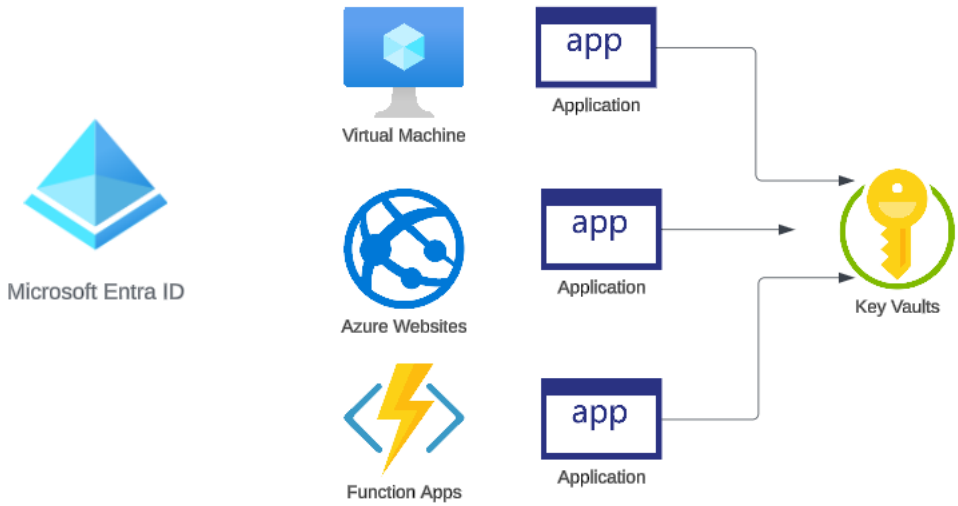



**Application uses an Application Object to access an Azure Key**

**The application with the help of the in-built classes would get the required access tokens to access the Key vault**

**Even though we now make use of RBAC, we still need to embed the credentials of the Application Object in our code.**

**You can make use of Managed Identities. This gives a way for applications to authenticate to Azure resources without the need of embedding credentials.**




**Your application could be hosted on a service that supports managed identities.**

**The managed identity for the resource can be registered in Microsoft Entra ID. This would create a service principal for that resource.**

**You can then provide RBAC access for that service principal onto the resource. And in your code you don't embed any sort of credentials.**

**We will look into an example of having an application hosted on a Virtual Machine that is accessing the blob service.**

# What is the Azure Policy service

**Azure Policy**

**Helps to govern your resources. You can define rules that resources need to comply by.**

Virtual Machine

**Let's say a company only wants Virtual Machines to be constrained to a particular region.**

**Or machines need to be of a certain SKU.**

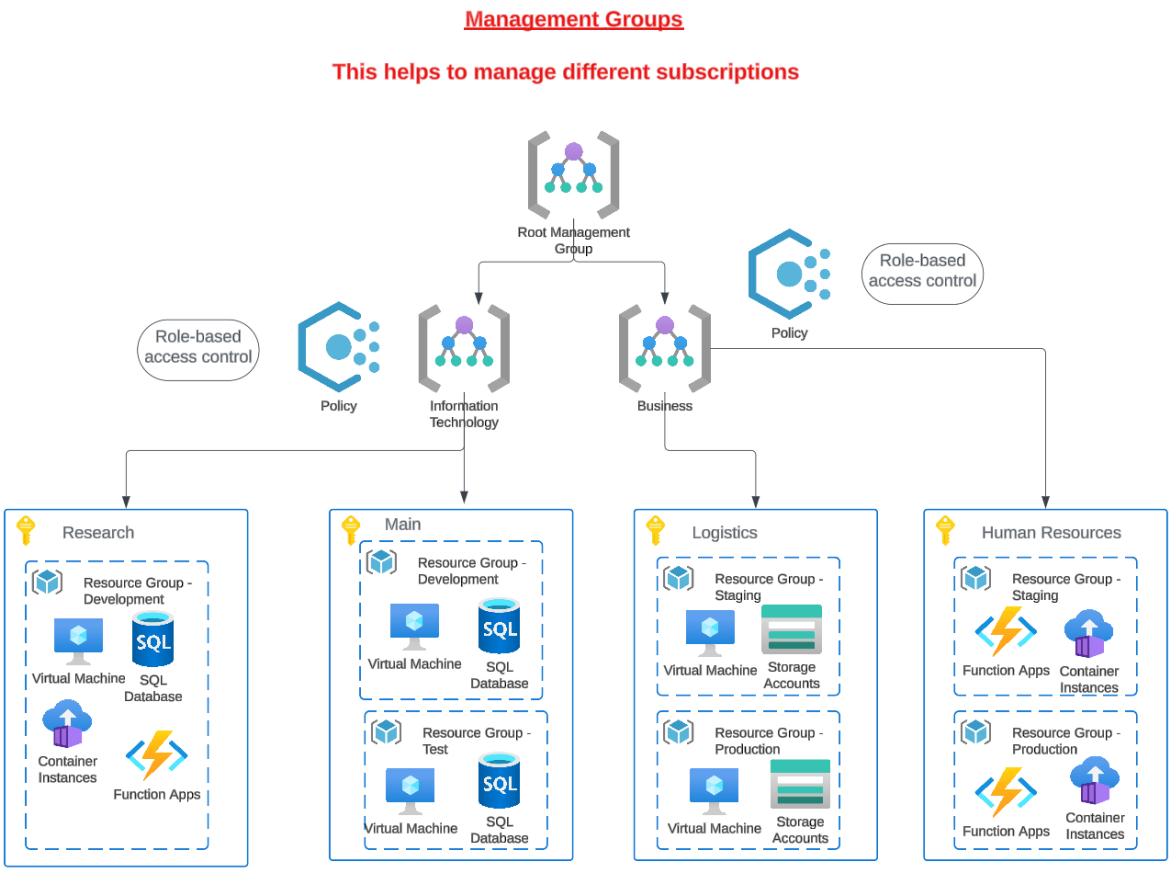
Policy

**You can use in-built policies for this**

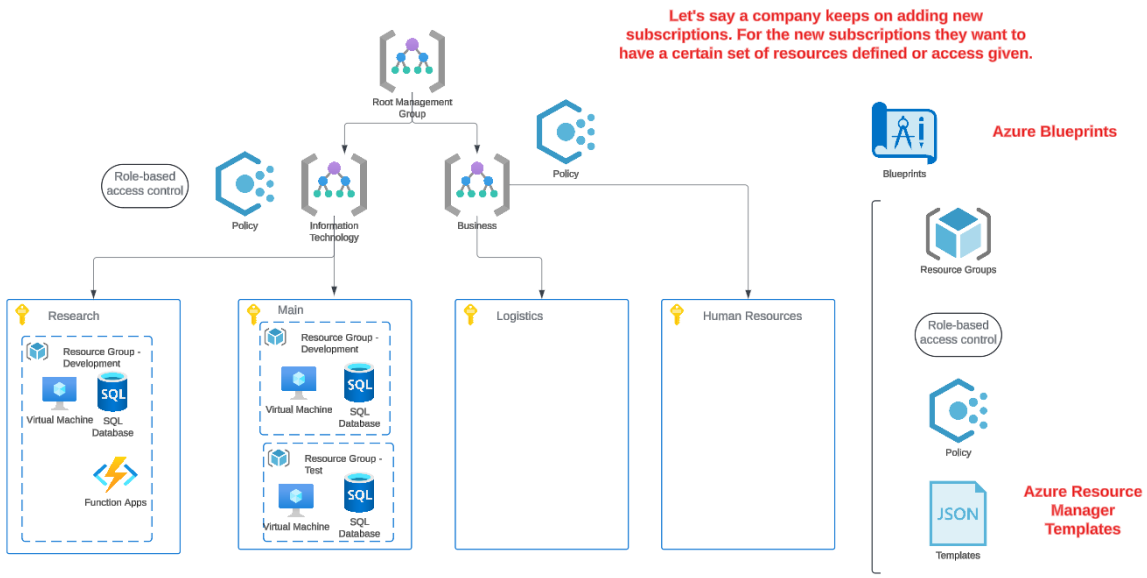
**You can also define your own policies.**

**You can also define an initiative which is a list of policies.**

# Management Groups



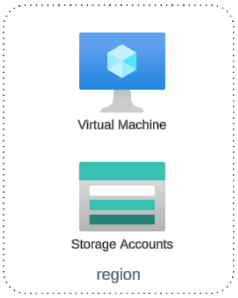

# Azure Blueprints

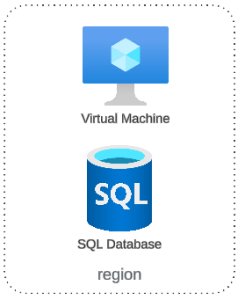


# What is the Azure Monitor Service

This service allows you to collect data for your resources in Azure and your on-premises resources as well.


You can analyze and work on the analyzed data.





You can look at the metrics collected for various resources

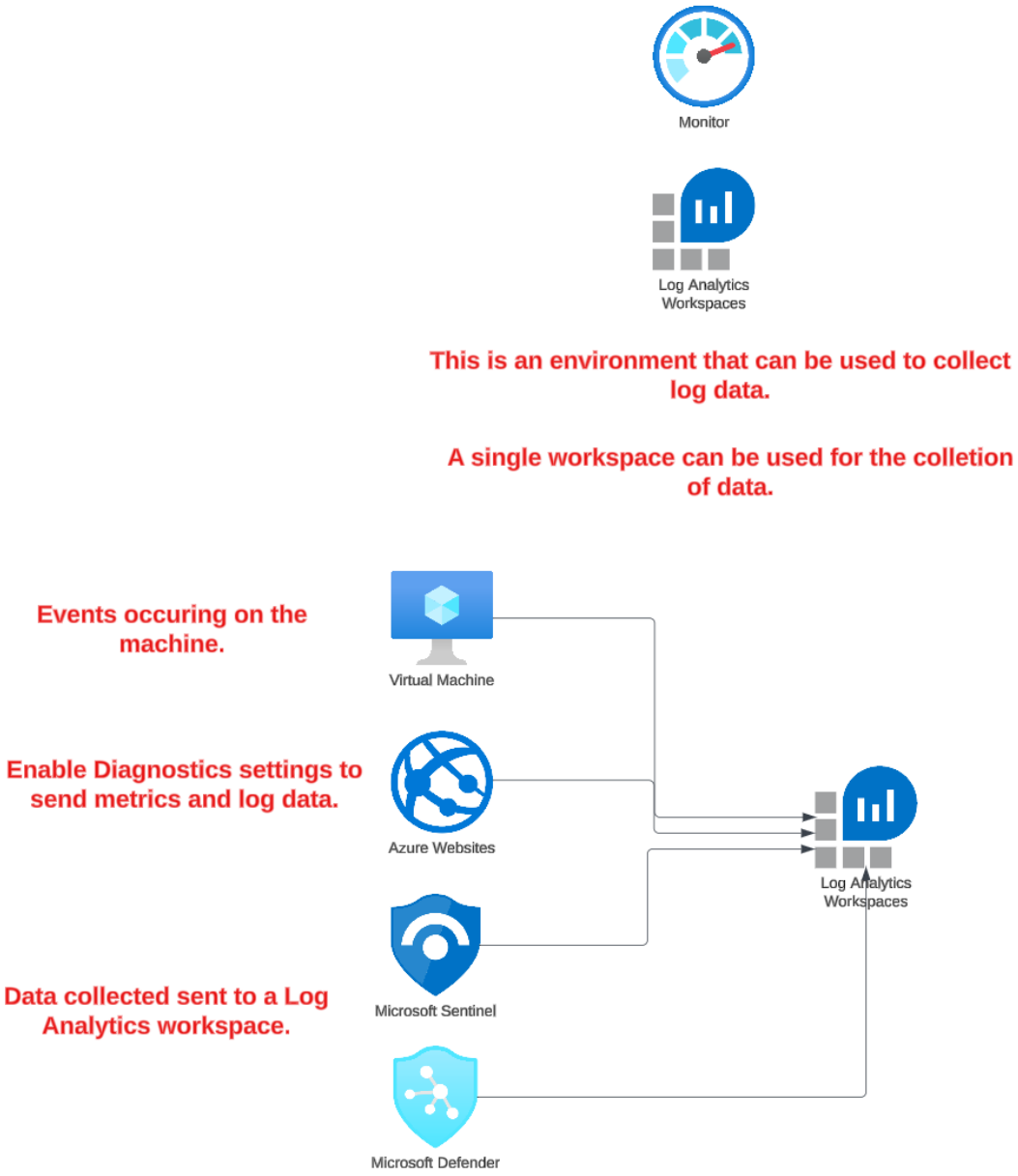

Alerts can be generated if metrics for resources go beyond a particular threshold.


You can also collect logs for various resources.

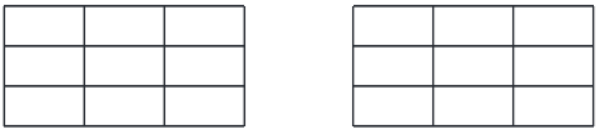

You can get insights when it comes to resources such as Virtual Machines


You can get reports and even Visualize the data.

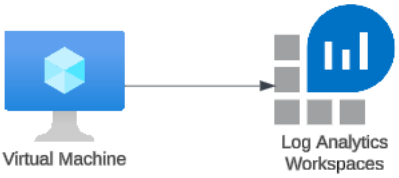
# What is a Log Analytics Workspace




Within the Log Analytics workspace, the data is collected into tables that have rows of data.



You are charged for the data that is ingested into the workspace and for how long you plan to retain the data.




You can have multiple virtual machines that send data to a Log Analytics workspace.

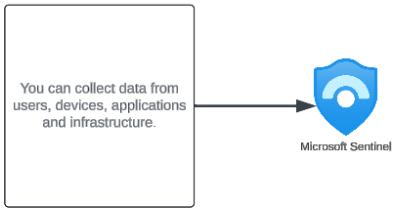
For collecting data from Azure virtual machines , we need to define a data collection rule.

In the rule, we can define the source when it comes to what is the data we need to collect. And then define where to deliver the content to.

## What is Microsoft Sentinel

**Microsoft Sentinel - This is a scalable , cloud-native security information and event management system (SIEM).**

**It also provides security orchestration, automation and response (SOAR)**



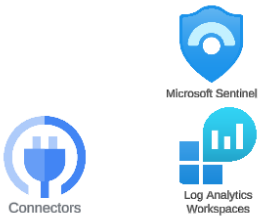

**Microsoft Sentinel can then be used to analyze the ingested data and detect and investigate threats.**

**Microsoft Sentinel also has inbuilt threat intelligence that helps to detect malicious activities.**

**You can use workbooks for interactive visual reports.**

**We can collect data via the use of data connectors.**

**These connectors can connect to Azure services or even to other SaaS providers.**




**In order to collect data, we need to have a Log Analytics workspace. We can then use data connectors to stream the data onto the Log Analytics workspace.**

**The Microsoft Sentinel service will sit on top of the Log Analytics workspace.**




In order to collect data, we need to have a Log Analytics workspace. We can then use data connectors to stream the data onto the Log Analytics workspace.

The Microsoft Sentinel service will sit on top of the Log Analytics workspace.

There are different RBAC roles to manage Microsoft Sentinel

Microsoft Sentinel Reader - Here one can view data, incidents and workbooks.

Microsoft Sentinel Responder - Here one can also manage incidents.

Microsoft Sentinel Contributor - Here one can also install and update solutions from content hub and create resources like workbooks, analytic rules.

Microsoft Sentinel Playbook operator - Here one can list , view and manually run playbooks.

Microsoft Sentinel Automation Contributor - Here one add playbooks to automation rules.

Pricing - You pay based on the data analyzed and the data stored in the Log Analytics workspace.

**There are some data sources that are free**

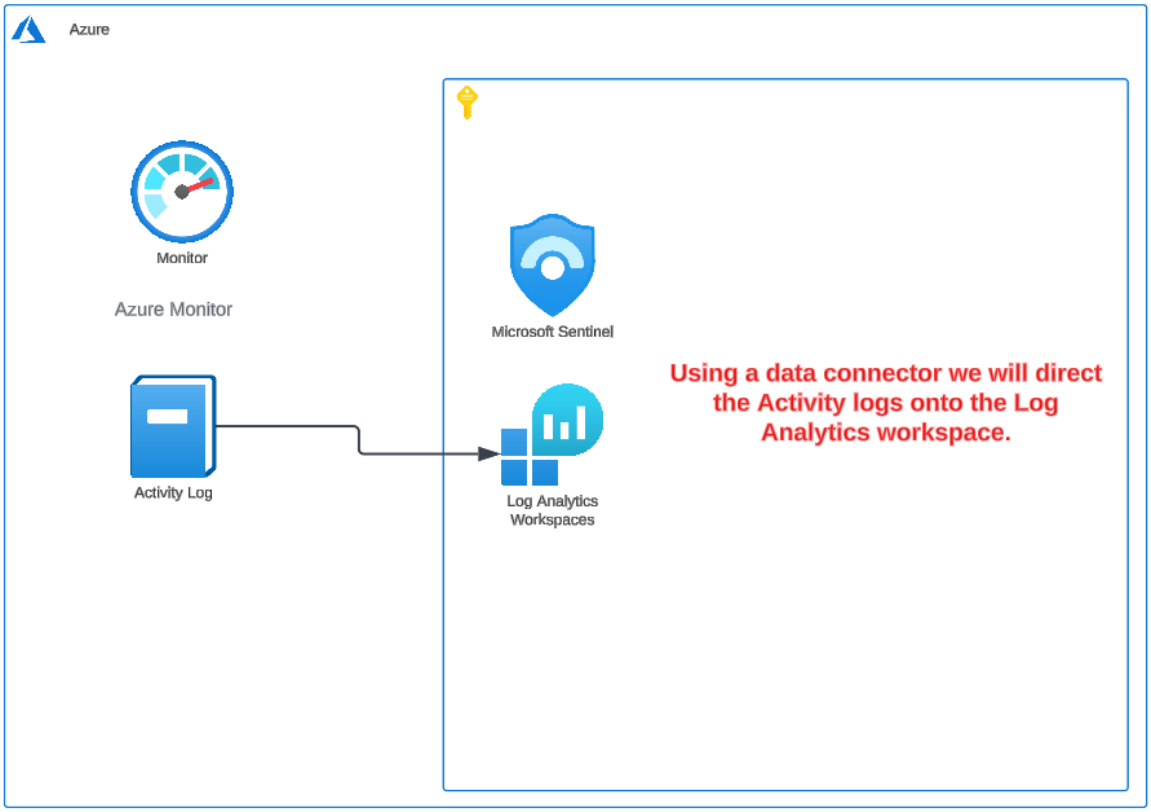
# Free data sources

The following data sources are free with Microsoft Sentinel:

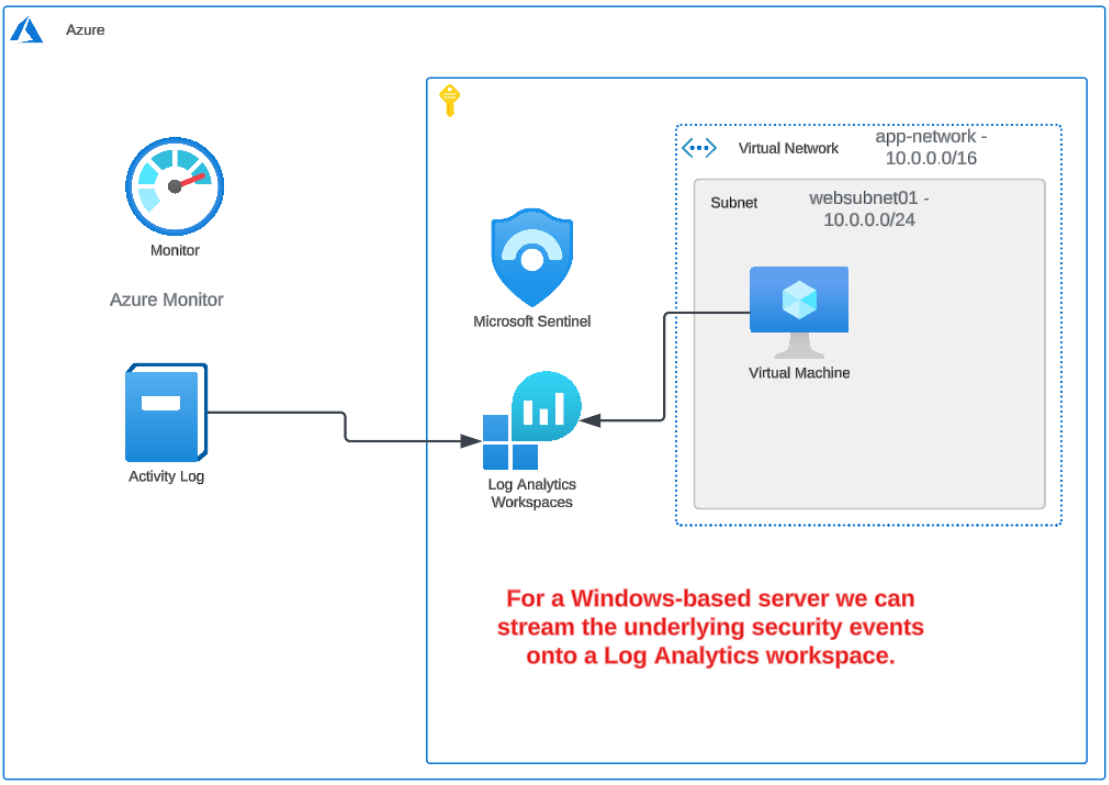
- Azure Activity Logs
- Microsoft Sentinel Health
- Office 365 Audit Logs, including all SharePoint activity, Exchange admin activity, and Teams
- Security alerts, including alerts from the following sources:
  - Microsoft Defender XDR
  - Microsoft Defender for Cloud
  - Microsoft Defender for Office 365
  - Microsoft Defender for Identity
  - Microsoft Defender for Cloud Apps
  - Microsoft Defender for Endpoint
- Alerts from the following sources:
  - Microsoft Defender for Cloud
  - Microsoft Defender for Cloud Apps

Reference - https://learn.microsoft.com/en-us/azure/sentinel/billing?tabs=simplified%2Ccommitment-tiers#free-data-sources

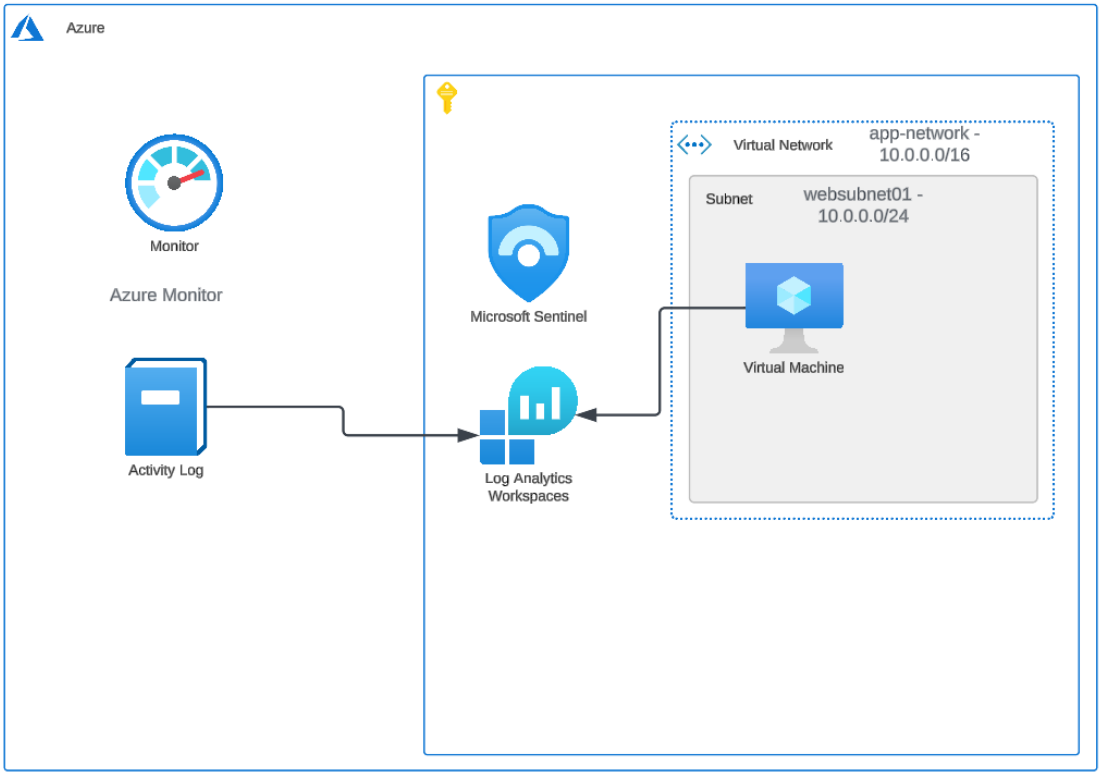
## Lab - Microsoft Sentinel - Azure Activity Connector




## Lab - Microsoft Sentinel - Windows Security Events Connector




## Microsoft Sentinel – Playbooks




**You can use playbooks to automate the response to security threats discovered by Microsoft Sentinel.**

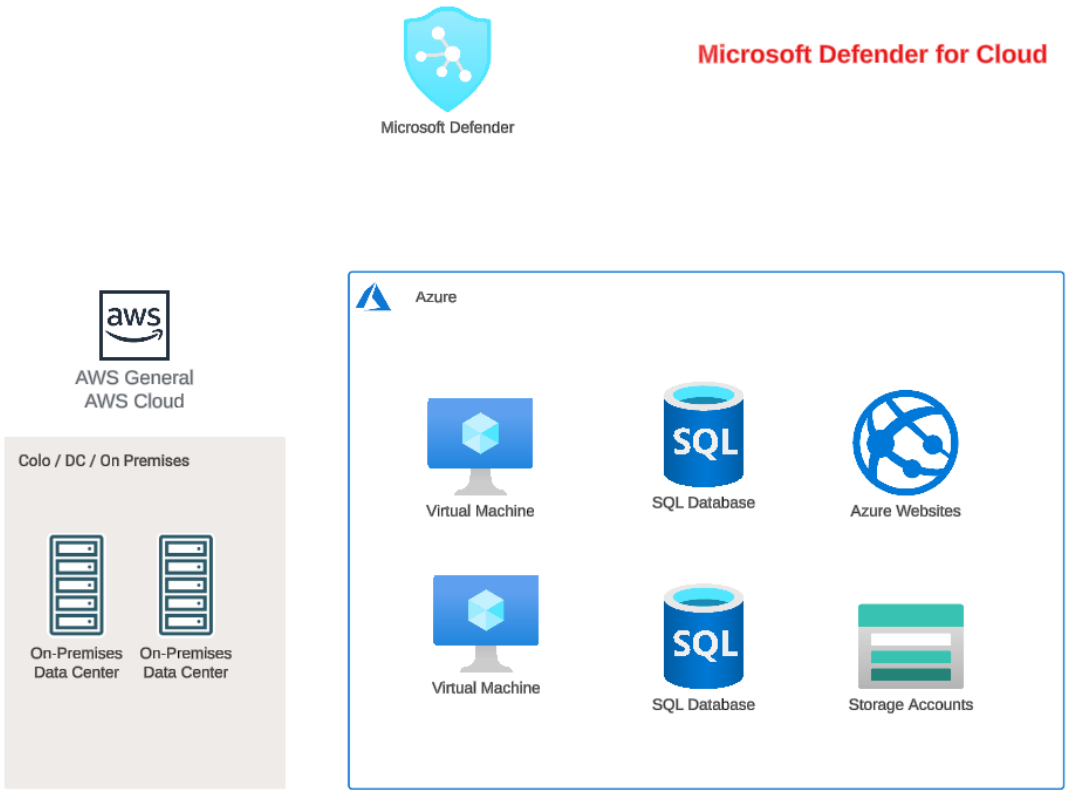
**For example, if a user account in Microsoft Entra ID has been compromised based on the Sign-in logs, then you can use a playbook to disable the account.**

**Of if a machine has been compromised, you could run a playbook that could isolate the Azure virtual machine.**


**For this we can define a workflow of the steps that need to be followed in the response via the use of an Azure Logic App.**

**The Microsoft Sentinel service account needs the Microsoft Sentinel Automation Contributor role for the resource group that contains the Azure Logic App.**

# What is Microsoft Defender for Cloud



This service helps to protect your application workloads.

You have workload protection for servers, databases , storage, containers.

Protection is available for other cloud platforms and even for your on-premise workloads.

You can implement a centralized Azure policy - There is one based on the Microsoft cloud security benchmark. This contains security principles based on guidelines for Azure and other cloud platforms.

Based on the security posture of your resources, you get a secure score.

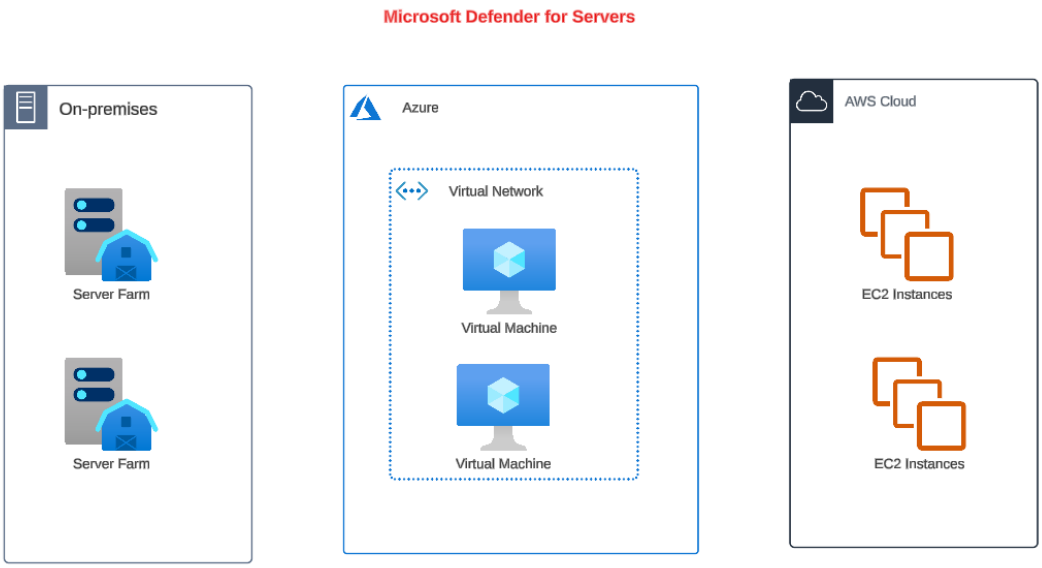
You can try Defender for Cloud for free for 30 days.

You need to enable Microsoft Defender for Cloud for your subscription.

Once you enable this, you get

1. Foundational Cloud Security Posture Management
2. Recommendations
3. Workbooks
4. Secure score
5. Regulatory compliance with Microsoft cloud security benchmark.

# Microsoft Defender for Servers



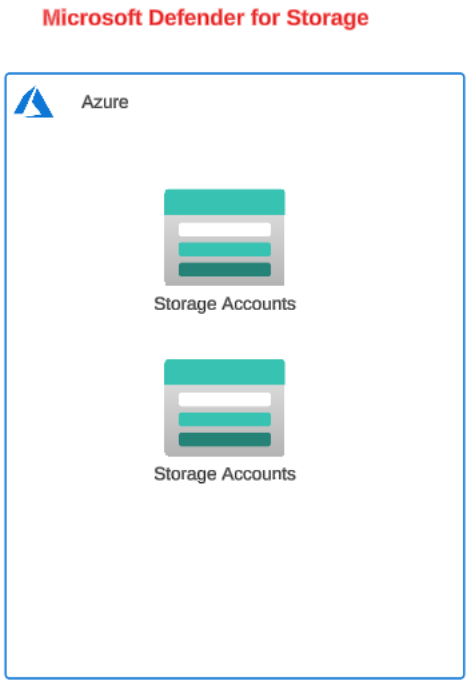

Here you get threat detection and advanced defenses for your Windows and Linux-based machines. These machines can in Azure, Amazon Web Services, Google Cloud platform or even your on-premises environments.

With the Microsoft Defender plans, we get security baselines, OS level assessments, vulnerability assessments, file integrity monitoring etc.

When we enable Defender for servers , the Defender for Endpoint extension is enabled for existing and new servers. This adds the capability of vulnerability management capabilities, threat analysis, endpoint threat detection.

Vulnerability Management - Here you can discover vulnerabilituies and misconfigurations in near real time. There is support for Windows and Linux-based machines.

## Microsoft Defender for Storage

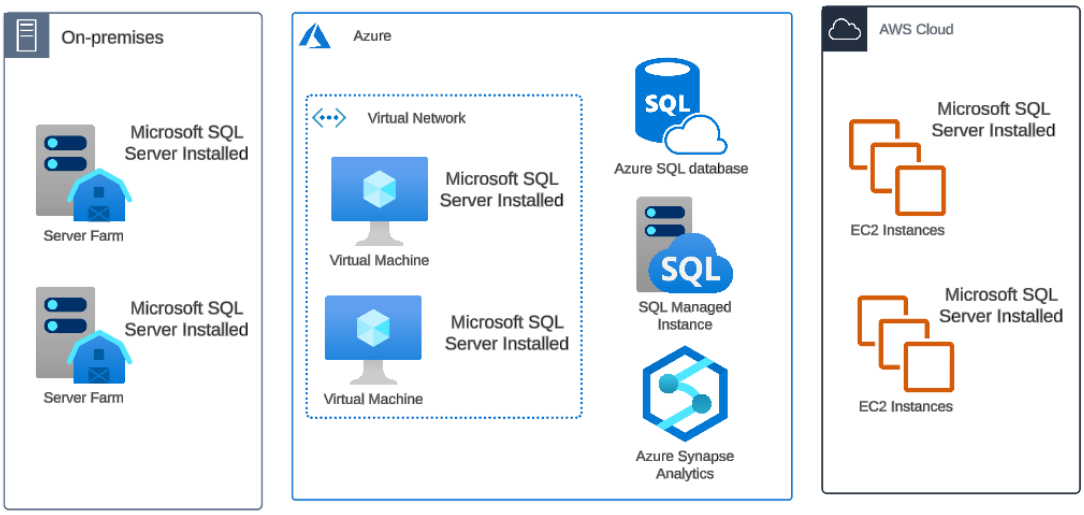



**This service helps to detect threats when it comes to Azure Storage accounts.**

**It can detect malicious file uploads, sensitive data exfiltration and data corruption.**

## Microsoft Defender for SQL

**Microsoft Defender for SQL**




**Here you get protection for Azure SQL databases, Azure SQL Managed Instance, Azure Synapse Analytics, SQL Servers hosted on Azure , on-premises and other cloud platforms.**

**You get vulnerability assessments to detect vulnerabilities.**

**You get Advanced Threat Protection that detects potential harmful activities. You can get immediate security alerts if such activities are detected.**