Microsoft Certified Azure Administrator

Exam AZ-104
Microsoft Certified Azure Administrator Associate

Microsoft Azure

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

Index

Azure Portal

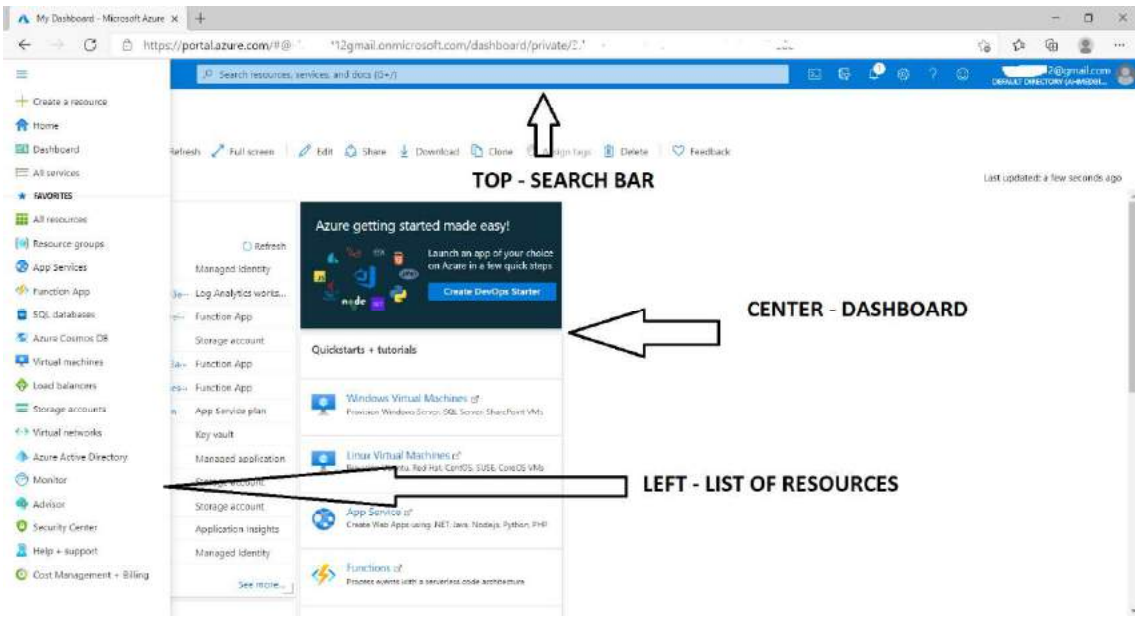
Azure provides 3 administration tools to choose from

1. The Azure Portal
2. The Azure CLI
3. Azure PowerShell

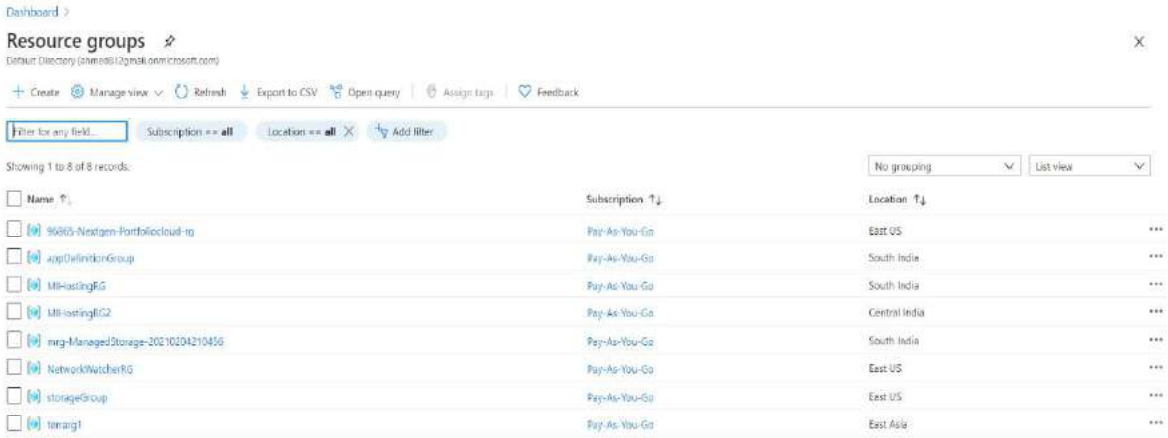
- We can use the **Azure GUI portal website (portal.azure.com)** to create, configure, and alter our Azure subscription resources.
- We can locate the resource needed and execute any changes. We have wizards and tooltips to guide through various administrative tasks.
- Please note that we cannot use the portal to perform repetitive tasks like creating 12 VMs etc.
- We need to use other tools to avoid errors, and it will also be a time-consuming process to do on the portal.

The Azure portal can be divided into 3 sections.

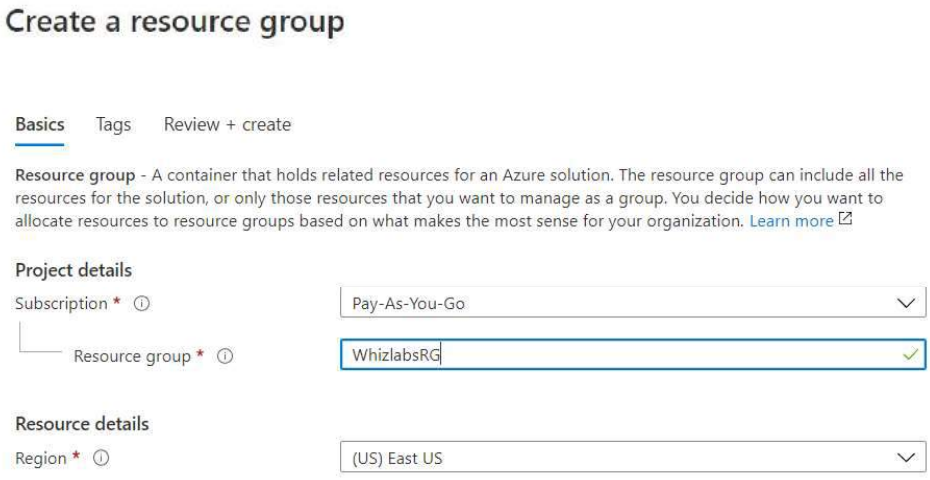
1. **Left** — A list of resources and services to create and manage your Azure environment.
2. **Center** — A dashboard that you can tailor to meet your (Public or Private dashboards) needs.
3. **Top** — A search bar to quickly find resources and services, a notification icon, access to a web-based command line, and more.



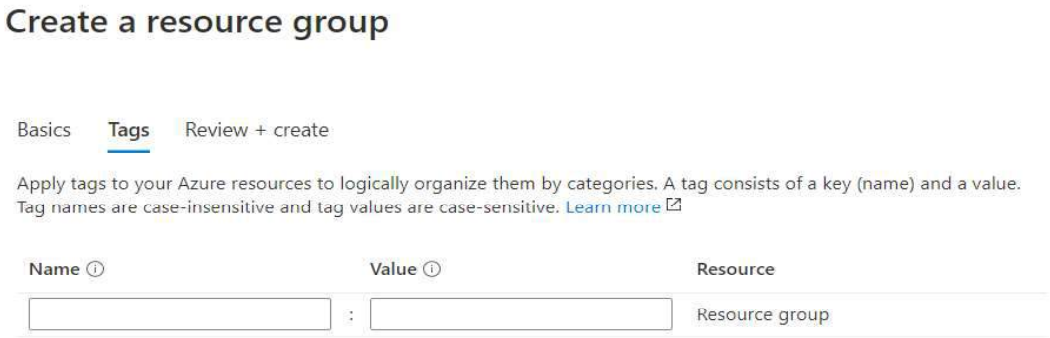
- Let's try to create a resource and see how to use the Portal. For example, let us create a resource group called demystify.
- Click on the Burger menu on the left top and select Resource group and click on it. You will get a new Panel.



- Click on the **+Create** icon. On the new Panel, add the name of the resource group and choose the desired location.

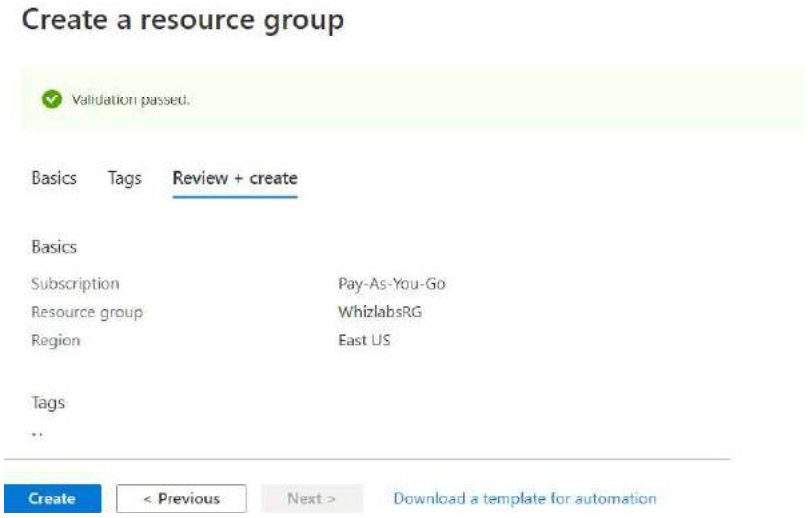


- Click Next, and you will get a new panel to add Tags. Tags are helpful for accounting and segregation but not mandatory.

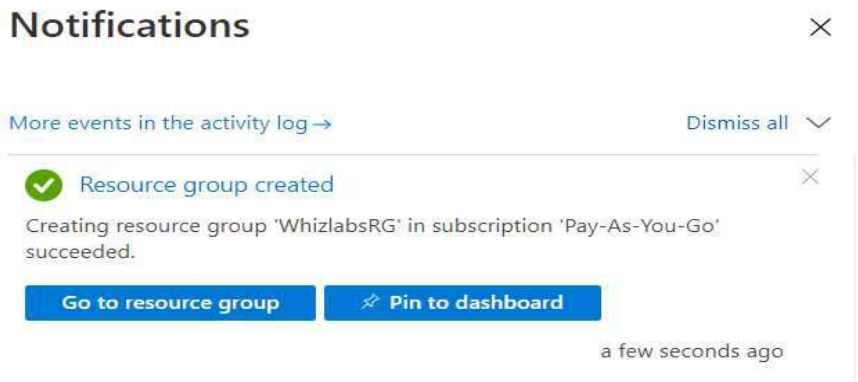


- Click NEXT, and at this point, Azure will validate all the options chosen.
- If there is any error, it will put a red dot on the tab where the error occurred, and you will need to go back to the tab and fix it before proceeding.
- If validation passed, you would see the Validation passed with a green tick message. At this point, you can click CREATE, and the resource will be created.

- You can also click on “Download a template for automation” and download the template and save it to the library additionally for future use.



- You will get a notification when the resource is created. You can also click the bell icon on Top Right to view the notification.



- If we go back to the Resource Groups, we can see this new resource group. This is a simple example of the usage of the Portal. We can use the portal for lots of activities.

We can use the Azure Portal for

- Creating/ Modifying/ Deleting resources
- Billing and accounting
- Help and Support – Contact Microsoft
- Online Help
- Health and Service Dashboards
- Security Center
- Access AAD and create applications
- Azure Monitor
- Access Documentation
- Azure Marketplace for third party products and solutions
- Access Cloudshell (On top right)

Azure CLI

Azure provides 3 administration tools to choose from

1. The Azure Portal
2. The Azure CLI
3. Azure Powershell

- Azure CLI is a cross-platform command-line program to connect and execute administrative commands on Azure resources.
- **Sample command:** `az VM create --resource-group WLRG --name WLVM1 --image UbuntuLTS`
- Azure CLI can be accessed inside a browser via Cloud Shell or with a local install on any OS like Windows/Linux or MacOS and Docker. It can also work with multiple clouds.

Let's see an example.

First, we invoke the MSI installer either in the command line or by downloading. Here is the command line below:

```
Invoke-WebRequest -Uri https://aka.ms/installazurecliwindows -OutFile .\AzureCLI.msi; Start-Process msiexec.exe -Wait -ArgumentList '/I AzureCLI.msi /quiet'; rm .\AzureCLI.msi
```

Then we sign in with the login command

```
az login
```

A new browser page will open (https://aka.ms/devicelogin), and we enter the authorization code displayed on the terminal.

Some of the common commands are as follows:

Sl No	Azure CLI command group	Resource Type
1	az group	Resource group
2	az keyvault	Key Vault
3	az SQL server	SQL databases
4	az storage account	Storage accounts
5	az vm	Virtual machines
6	az webapp	Web applications

Let's take Storage accounts as an example and work with Azure CLI

Step 1:

Create a resource group for Storage accounts

```
az group create --name StorageRG --location westus
```

Step 2:

Create a Storage account

```
az storage account create --name WLblobSA123 --resource-group
storageRG --location westus

--sku Standard_RAGRS --kind StorageV2
```

Step 3:

Finally delete to clean up the test

```
az storage account delete --name WLblobSA123--resource-group
storageRG
```

Azure Powershell

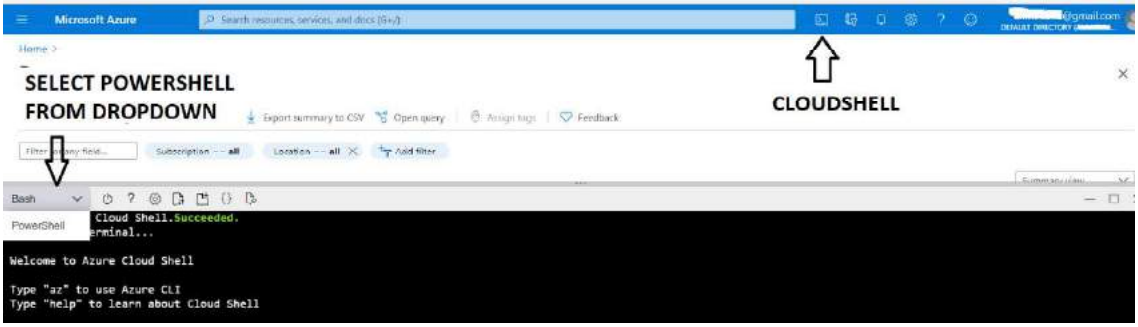
Azure provides three administration tools to choose from

1. The Azure Portal
2. The Azure CLI
3. Azure Powershell

- Azure PowerShell is a module that allows us to connect to Azure subscriptions and manage resources.
- Azure Powershell uses AzureRM command modules, and it has now added Az command modules as well.
- If we used the *New-AzureRmVM* command to create a VM via the AzureRM Module, we would change to the *New-AzVM* command to create a VM via the Az Modules.

How to use Powershell in Azure Portal?

- First, click on the cloud shell icon on the top right. If you are doing this for the first time, you will be prompted to create a Storage account to host the cloud shell files.
- You can accept a default storage account and file names or choose your own.
- By default, Cloudshell launches in **BASH MODE**.
- You need to choose Powershell from the dropdown and you will be prompted for a confirmation.



- Once you hit on the confirm button, you will get the Powershell command line to execute Powershell commands.

How to use Powershell in your local installation?

- Windows OS comes with Powershell installed. You can select Windows Powershell and hit enter once the Powershell window is launched; type az login.
- A new browser will be launched to select an already logged-in session or log in to a new session.
- After getting a successfully logged-in message, you can close the browser and go back to your Powershell screen and continue working with Powershell commands.

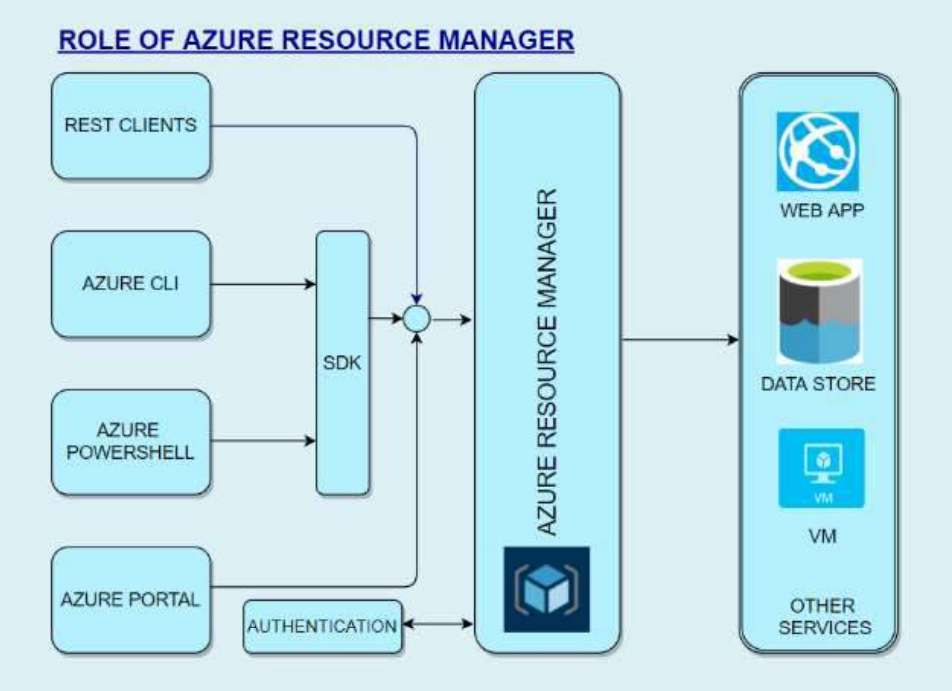
Working with Powershell:

For example: To create VM, we launch Powershell either inside a browser or by installing locally on any OS and then run the **New-AzVM** command that creates a virtual machine in our subscription as follows:

```
New-AzVm -ResourceGroupName "WLRG" -Name "WLVM1" -Image "UbuntuLTS" ...
```

Azure Resource Manager

- Azure Resource Manager provides a management layer to ***create, update, and delete*** resources in your Azure account.
- We use management features, like access ***control, locks, and tags, to secure and organize your resources after deployment.***
- When a user sends a request from any of the tools, APIs, SDKs, the Resource Manager receives the request and **authenticates/authorizes** it.
- Then it sends to azure services to take action. Since it acts as a central point, it leads to consistent results.



Benefits of Resource Manager:

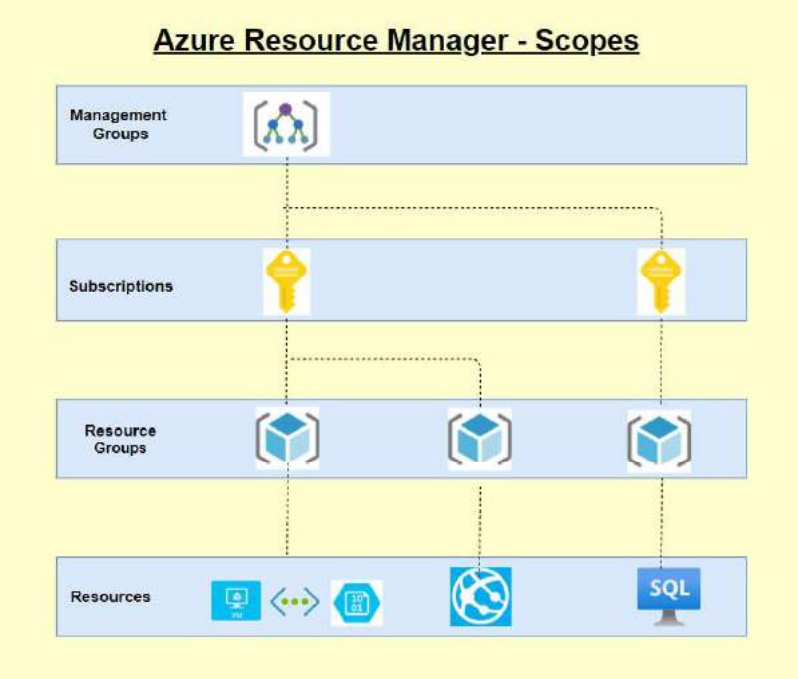
- Declarative templates so we don't have to worry about the current state.
- Allows group deployments
- Define dependencies so the correct order of deployment is done.
- Apply tags to organize resources logically
- Allows for redeployment and have confidence that same results will be achieved
- Applies access-control via RBAC natively.

Scopes

When we deploy, they are done at 4 levels.

1. **Management Groups** – At this level, we can combine multiple subscriptions to apply changes at an Organizational level. We can connect Organizations with a hierarchy where there is one management group at the root level. This is called Nesting.

2. **Subscriptions** – Subscription is a logical container used to provision resources. We will be billed at the subscription level. We can have multiple subscriptions.
3. **Resource Groups** – We can create multiple resources in a resource group. We can logically group resources at a resource group level. We can delete an entire resource group, and all resources will be deleted within the resource group. We can even move a whole resource group with all objects within it.
4. **Resource** – This is the lowest manageable item in Azure resource. Examples of Azure resources are *Virtual machines, storage accounts, web apps, databases, virtual networks, and tags. Resource groups, subscriptions, management groups are also examples of resources.*



Azure Pricing

Azure is one of the market leaders in Cloud services and has some of SQL and Windows's best pricing. It can leverage several features to save costs, and Azure provides several tools that can help calculate costs and cost-effectively plan our infrastructure and service.

Some of the available tools are:

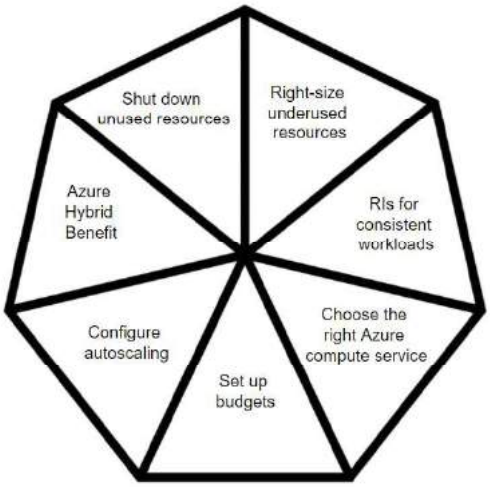
- **Azure Pricing Calculator**
- **Cost Management Center**
- **Migration planning – Estimation, Workload, and right-sizing**
- **Billing Data API & Advisor**
- **DB & Cosmos DB Capacity calculator**

Some of the features that we can leverage to save costs are as follows:

- **Azure Hybrid Benefit –** We can use our existing SQL and Windows licenses to save on costs.
- **Spot Virtual machines** - This feature allows us to take advantage of the unused CPU at a significantly lower cost at almost 90% savings.
- **Reservations** - We can commit to 1-year or 3-year and choose to pay upfront or monthly to buy RIs.
- **Azure Dev/test pricing** – For development environments, we can get special discounted rates

Ways to optimize Cost

Please see the self-explanatory chart below for ways to optimize cost



FAQs:

- Are there any other ways to save costs?
  - **EA – Enterprise Agreements** – With this, we can get good pricing offers from Azure.
  - **Price Match with AWS** – This might not be known to all, but we can ask MS to do a price match.

Azure Security Center

Introduction:

In today's world, Security has been a biggest concern for any application hosted/built in either on-premises or cloud and it is the foremost duty of a developer to prevent unwanted access to applications and prevent all other security issues. So security in the cloud is foremost important and it should also provide accurate and timely information about security.

Azure Security Center:

The Azure Security Center in Azure Cloud is a unified infrastructure security management system that can be used to strengthen the overall data security and provide advanced threat protection across various workloads such as Azure cloud or other cloud providers or even on-premises.

When an application is being moved to Azure IaaS, the customer has more responsibility on securing the data when compared to moving to PaaS. So the security center offers various tools that can be used to harden the network and secure the various cloud services.

The security center can be used to address the 3 major security challenges:

- **Strengthen the environment:** The security center assesses the whole azure environment and all the resources deployed and it understands the security status of the same. By doing so, it provides detailed security related information.
- **Protect against modern threats:** Today we have various threats that can easily take over the application. So a security center can be used to provide various threat prevention recommendations by assessing the deployed workloads and also provides timely security alerts.
- **Secure the environment faster:** Since the security center is natively built in azure cloud, it can be used to quickly secure the cloud environment and also protect against various threats.

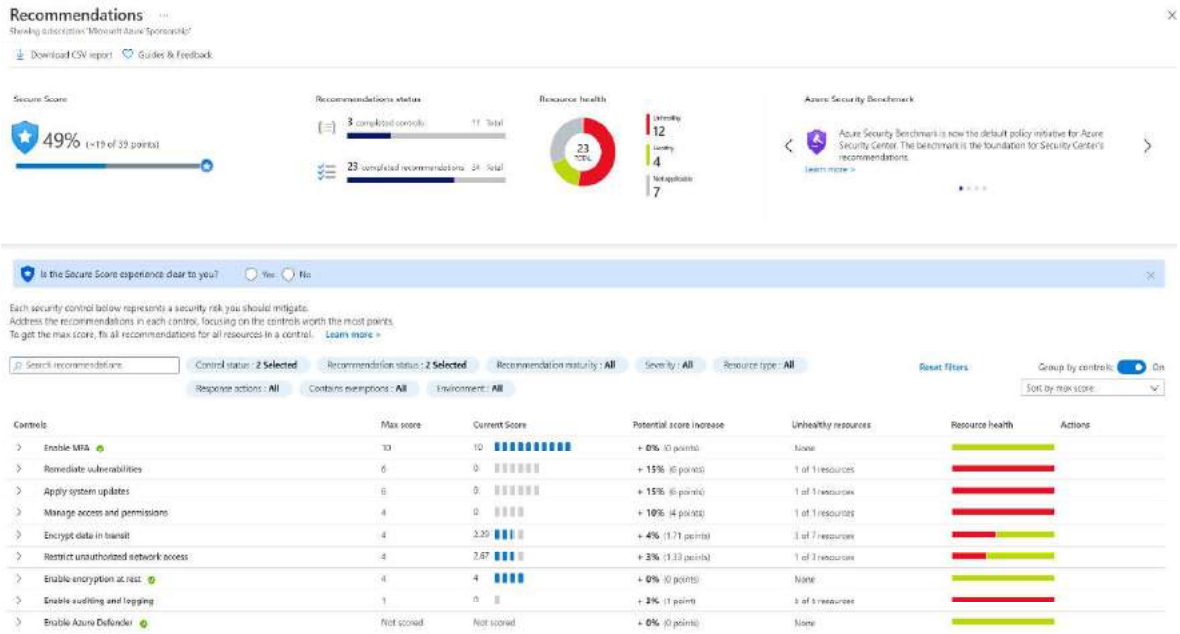
Key Pointers:

- Since the Security center is natively part of Azure, various PaaS services SQL Database and storage accounts can automatically be monitored by the security center without making any additional deployment.
- Also the security center can be used to protect not only azure services but also applications deployed in other cloud providers or even in on-premises.
- To perform these, a log analytics agent needs to be installed in the external application.
- The Azure VMs are auto-provisioned in the security center when they are deployed and do not require any additional installations.

- The log analytics agent installed in the external system and azure will be collecting various information and the same will be processed in the security engine to provide detailed recommendations and actions to secure the data and the workload.
- It is also very important that these recommendations should be considered and necessary actions should be taken. By doing so, the environment can be highly secured and malicious activities can be prevented.

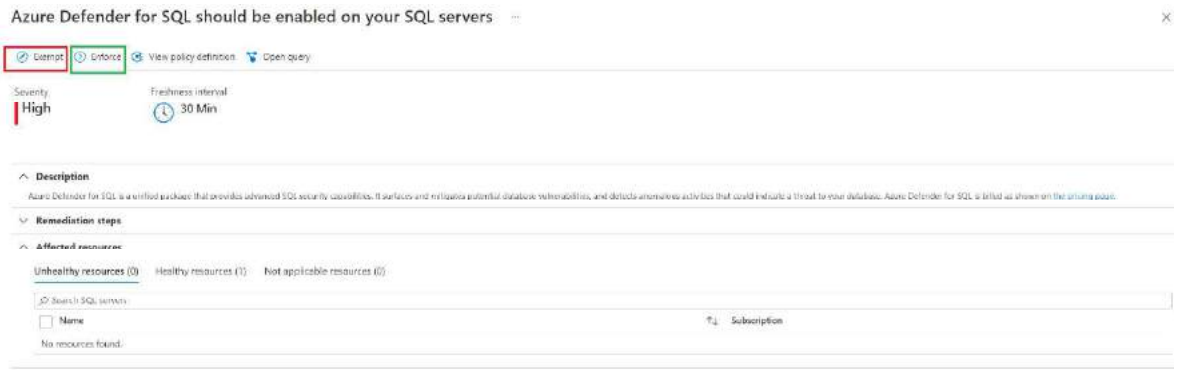
Environment assessment:

- The security center continuously monitors all the resources deployed in the cloud and provides various recommendations to secure it.
- Based on the recommendations, it also displays the necessary action to be taken to secure the resources.
- Also based on the analysis, it provides a security score which as per recommendation should be 100%. Below is the image of the security center portal.



- The details here are filtered based on a subscription in which it displays the security posture of various resources in the subscription.
- The red bar on the right denotes that the particular security recommendation "**Remediate vulnerabilities**" was not implemented and some resources may be affected due to this.
- If a recommendation is clicked, it displays further more information about the recommendations, severity of it and total number of affected resources.
- Also it is the ***user's/Administrator's*** choice whether to perform or skip a particular security center's recommendation.
- It is not mandatory to perform all the recommendations and Microsoft does not produce any discounts/credits if the security score is kept 100%.

- If a user chooses to skip a recommendation, he/she can go inside the recommendation and give “Exempt” to overcome this recommendation.
- It is also possible to enforce a particular recommendation and by doing so, it will be creating a template deployment which will make sure to use the “**DeployIfNotExist**” policy and create the resource with this security recommendation.



All these recommendations and security alerts provided by the security center provides a great insight of what all security threats may occur to the resources and how to prevent it well before-hand.

Cost of Azure Security Center:

The azure security center itself is a free service but to have more features other than providing recommendations and actions, a paid service called the azure defender is available and it can be used to extract below additional details.

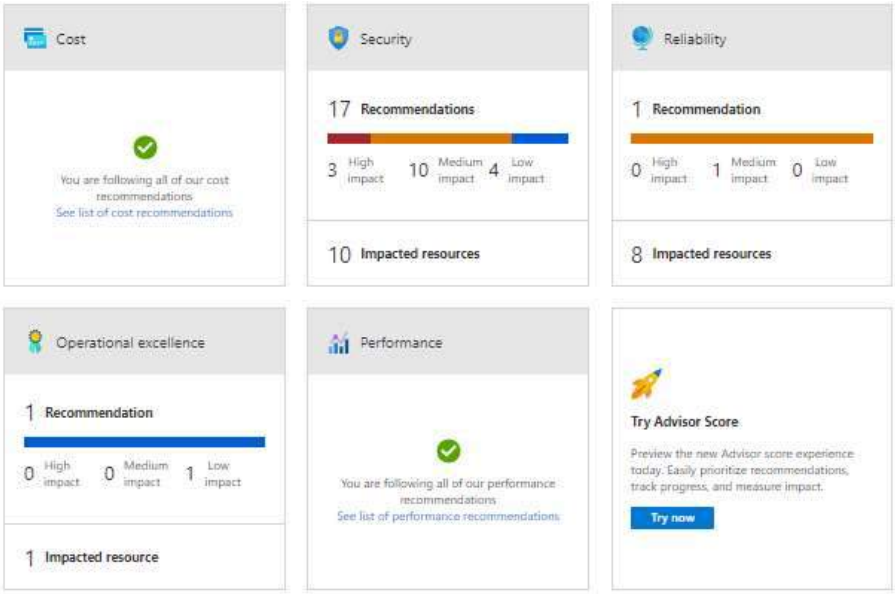
FEATURES	AZURE SECURITY CENTER FREE TIER	AZURE DEFENDER
Continuous assessment and security recommendations	✔	✔
Azure secure score	✔	✔
Just in time VM Access	- -	✔
Adaptive application controls and network hardening	- -	✔
Regulatory Compliance Dashboard (Preview)	- -	✔
Threat protection for Azure VMs and non-Azure servers (including Server EDR)	- -	✔
Threat protection for PaaS services	- -	✔
Microsoft Defender for Endpoint (servers)	- -	✔

Azure Advisor

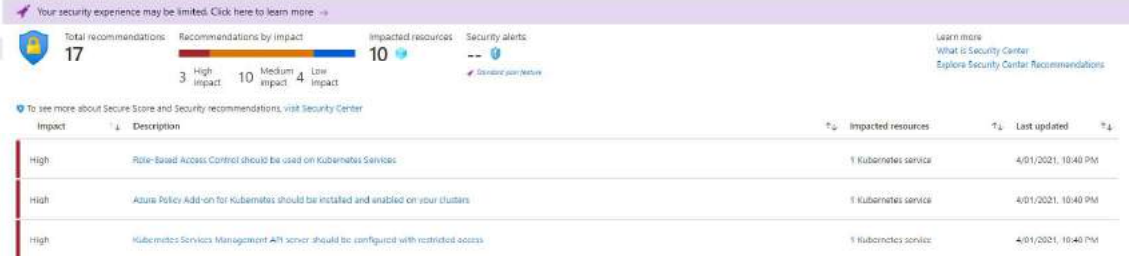
Azure has 5 pillars called the Azure well-architected framework which provides best practices to help build and deliver great solutions.

To enable customers to follow these best practices and optimize the cloud deployments, Azure has a free tool called Azure advisor. Azure advisor analyses the configurations and usage logs and offers recommendations which are customized and can be executed.

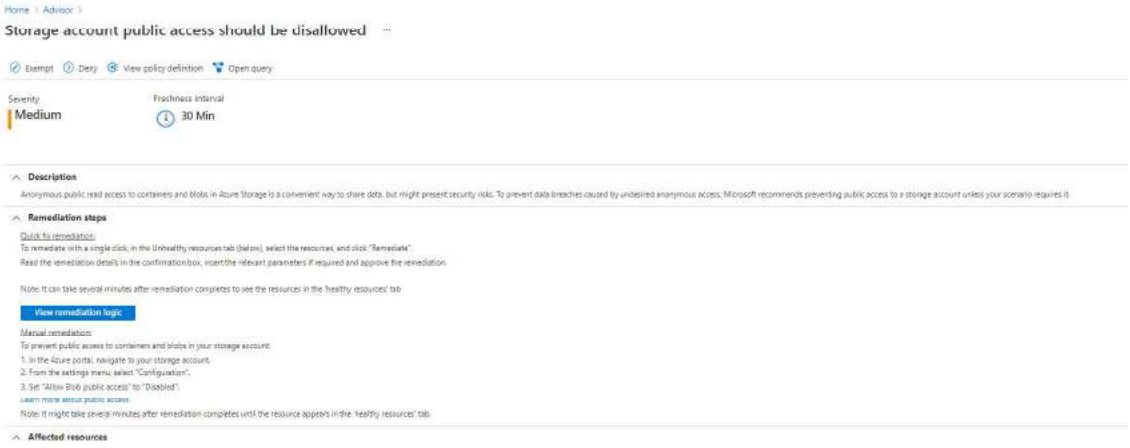
- On each of the 5 pillars, we will be given recommendations to optimize. Please see below.



- If we click on each of these recommendations, we can see what the recommendations are.



- If we further click on each of the line items, we will give the list of resources that are not compliant and will provide manual and in some cases remediation action which can be deployed directly.



- You can also note from the above that these recommendations are setup with the help of Azure policies.
- We can see the Policy definition and we can exempt the policy itself from being flagged as non-compliant.
- We can enable the deny action also in which case the resource will be prevented from being created.
- Here we have the policy which is audit and hence the resource is created and marked as non-compliant.

Sample remediation code:

```
{
  "properties": {
    "allowBlobPublicAccess": false
  }
}
```

We can download these recommendations as a CSV or PDF file.

Azure Advisor also has 2 features in preview. One feature is alerts which are yet to be generally available (GA). The other feature is the Advisor score which gives us on a percentage basis if we are following best practices.

Azure Active Directory

Microsoft introduced **Active Directory** in the year 2000 which to this day is one of the best products from its stable.

Any Enterprise with Windows servers would be running the Domain Controllers in a ***Domain/Tree/Forest*** organization setup with multiple DCs playing different roles **(*called FSMO – Flexible single master operation)*** and in multiple locations for load balancing and reducing latency and increasing fault tolerance.

Before this, Microsoft had NT4 where there was a single ***PDC (Primary Domain Controller)*** backed by a ***BDC (Backup Domain Controller)*** to provide Enterprise Identity Management.

Windows 2000 and beyond uses the Active Directory and it uses **LDAP** (***Lightweight directory access Protocol)/Kerberos*** for authentication. Here all resources like computers, printers, etc are all considered objects.

This concept changed with Azure Directory which like most cloud service providers also uses REST API in the background.

Any service invoked on the Azure cloud is with REST APIs and this is the foundation for ***AAD (Azure Active Directory)***. Therefore, AD on the client premises and AAD on the cloud will not work seamlessly.

Let's look deeper and compare the two and in that process understand AAD better.

- **Communication** – As discussed, AD uses LDAP and AAD uses REST API
- **Authentication** – Cloud based protocols for AD/ AAD uses Kerberos and NTLM
- **Access Setup** – AD uses Admin/data owners and AAD organizes users into groups
- **Network Organization** – AD uses Forest/Domain/Tree/Organizational Unit (OU) whereas AAD uses users and groups
- **Desktops** – AD uses GPO (group policy object) and AAD can use Microsoft intune to join desktops

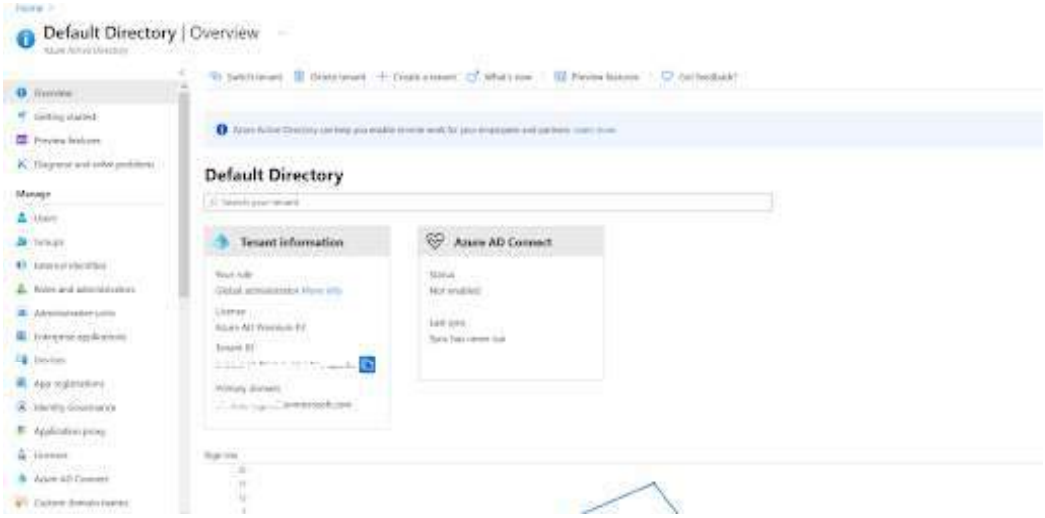
Azure AD Connect

In situations where we want to enable a hybrid environment where we have both AD on-premises and AAD on Azure cloud, we need to use Azure AD connect which syncs data between the two directories.

AD connect will allow us to synchronize user accounts and passwords. There are several methods of synchronization.

- **Hash Synchronization** – Here only a hash of the password is stored on cloud
- **Pass-through authentication (PTA)** – Here the authentication is forwarded to the on-premises server
- **Federation** – Federation services provides authentication across several external identities in addition to providing on prem access

AD Features



Default Domain – The default domain is based on our email id. If our email id is demystify@gmail.com. Then our domain name will be demystifygmail.onmicrosoft.com. It is a combination of user and domain and then addition of .onmicrosoft.com.

Usernames – Any user name we create will have the suffix of our domain name

Custom domain name – If we want to use our own company name, then we should create a custom domain (for example demystify.com) and then we can create a user smith@demystify.com

App registrations – We can register our applications here and grant access to the application/users.

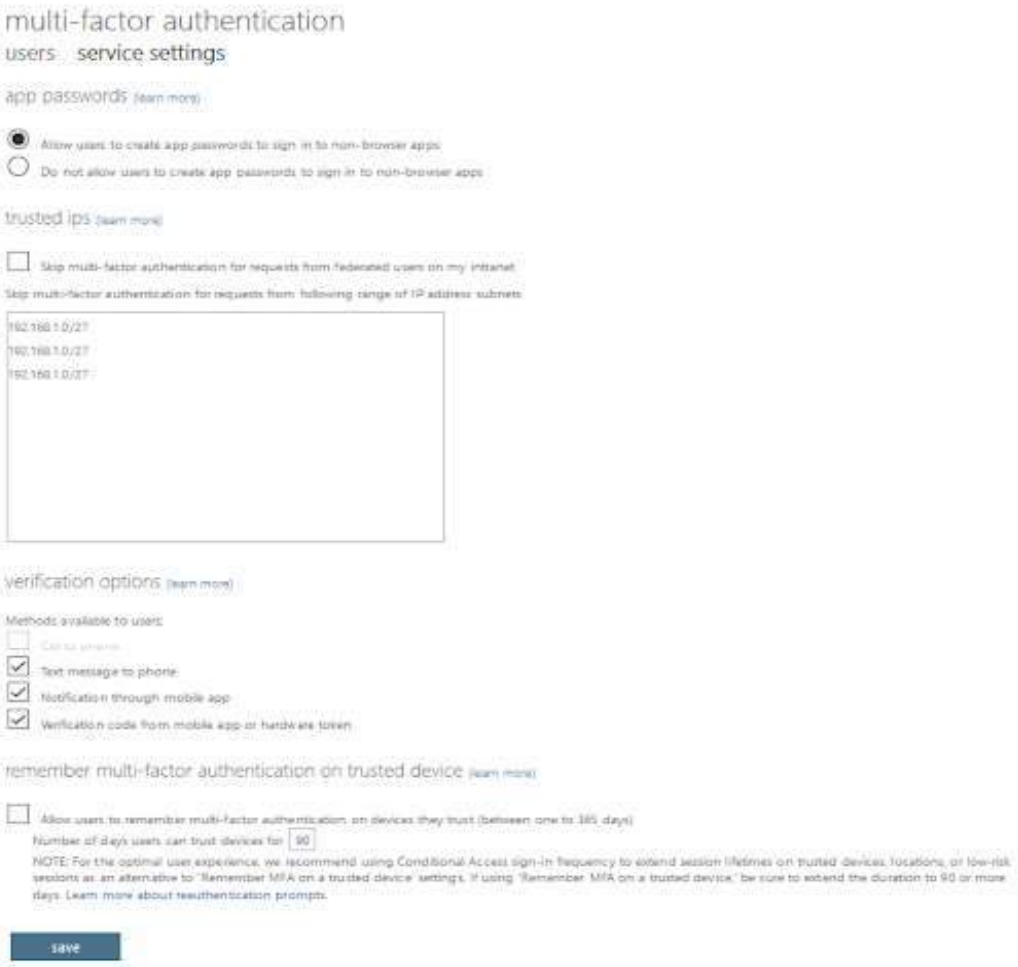
License Management – We can perform license Management here. We can track all acquired licenses and assigned licenses and make sure we don't overuse and pay heavy penalties

Enterprise applications – we can see all the enterprise applications and assign them to our users. When a user logs in, he/she can see only the applications assigned to them.

Security – This is one of the key areas. Under security, we can see the following

- **Azure AD Conditional Access –**We can add conditional access policies like restricting users from logging in from outside office network or even outside country
- **Azure AD Identity Protection –**We can assign user risk / sign-in risk and the system will dynamically assess risk and react like unusual geography of login
- **Azure Security Center**
- **Identity Secure Score –** We are given a security score which tells us our overall security posture

- **Named locations –** If we readily identify safe locations like cities where headquarters and branch offices are located, we can create named locations and allow these under conditional access policies.
- **Authentication methods –** We can enable additional authentication methods like FIDO2 Security Key/ Microsoft Authenticator
- **Multi Factor Authentication (MFA) –** We can configure MFA and add multi-factored authentication. Please note that this setting is outside of the azure portal and a link will take out to the GUI. Sample screen looks like this.



Azure Role-Based Access Control (Azure RBAC)

- The policy of any organization is to follow the principles of least privileges. One must not be given access beyond what is necessary to perform a role in the organization.
- The principles apply for cloud resources also. Let's take the example of a VM operator. His role dictates that he must be able to **start/stop/restart/create/delete** VMs.
- So, we use Azure **RBAC** to grant just that access. In our case, we will grant the operator the RBAC role of VM contributor.
- Azure **RBAC** is an authorization system. It uses Azure Resource Manager behind the scenes. Azure RBAC provides fine-grained control of access to Azure resources at various levels.
- The Policies can be applied with a boundary like being able to do so in a set of resource groups called scope.

Let's see some examples where we use Azure RBAC:

- Grant access DBA group to manage databases in 2 resource groups.
- A user can manage all resources in a resource group like VM, web apps, storage account, Vnet/Subnets.
- Grant one application to access to create resources.

How Azure RBAC works

We assign Azure roles to make RBAC work. A role assignment consists of three elements: security principal, role definition, and scope.

1. Security principal

A *security principal* is an object that could represent a user or a group or a service principal or managed identity and requests access to Azure resources. We can grant access to any of these entities.

2. Role definition

A *role definition* is a collection of permissions and is called a *role*. A role definition will list the operations that can be performed. It could be something like read, write, and delete. We could grant access at a high level like owner, or even more specific roles like the VM operator where the access is limited to VM operations only.

Azure has *built-in roles* that you can use. For example, we have a contributor role where we can create all objects but we cannot grant. If we want to grant access to only certain resources, we will create a custom-defined role.

As you can see below, we can apply policies against the data stored within the scope's resources. For example, the secret within a key will be data, and we can dictate whether the data can be read or not.

ROLE DEFINITION

```
"permissions": [
    {
      "actions": [
        "Microsoft.Authorization/*/read",
        "Microsoft.Insights/alertRules/*",
        "Microsoft.Resources/deployments/*",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Support/*",
        "Microsoft.KeyVault/checkNameAvailability/read",
        "Microsoft.KeyVault/deletedVaults/read",
        "Microsoft.KeyVault/locations/*/read",
        "Microsoft.KeyVault/vaults/*/read",
        "Microsoft.KeyVault/operations/read"
      ],
      "notActions": [],
      "dataActions": [
        "Microsoft.KeyVault/vaults/*"
      ],
      "notDataActions": []
    }
  ],
  "roleName": "Key Vault Administrator",
  "roleType": "BuiltInRole",      =========> Builtin or CustomRole
  "type": "Microsoft.Authorization/roleDefinitions"
}
```

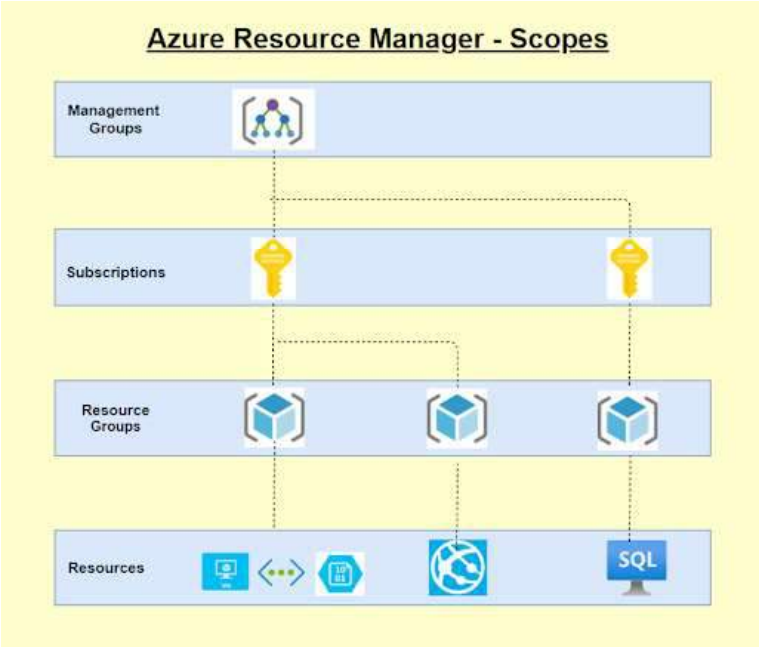
3. Scope

The scope is the set of resources to which we apply the access to. Let's say that we grant a VM operator role to a person, but we don't want that person to be able to stop VMs in production, then we apply the scope to non-production subscription or resource group only.

A scope can be applied at the four levels:

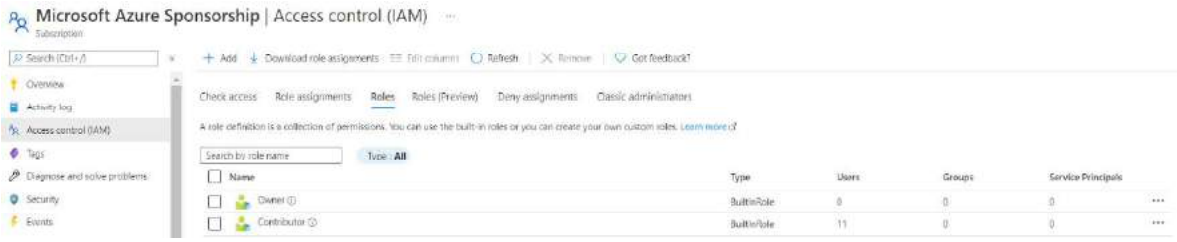
a. **Management group**
b. **Subscription**
c. **Resource group**
d. **Resource**

- Scopes follow a hierarchical structure, and they follow a parent-child relationship.
- Scopes applied at a higher level are inherited by the resources below it.
- For example, a policy with a scope of Management groups will be inherited by all subscriptions under it.
- Likewise, a policy scoped at the RG level will be inherited by all resources under it.



4. Role assignments

We assign the role to the user or group. When we assign the role, the user gets the privileges. And we simply remove the role assignment when we want to revoke the access. Under IAM, for every resource, we can see the roles under the roles tab.



5. Deny assignments

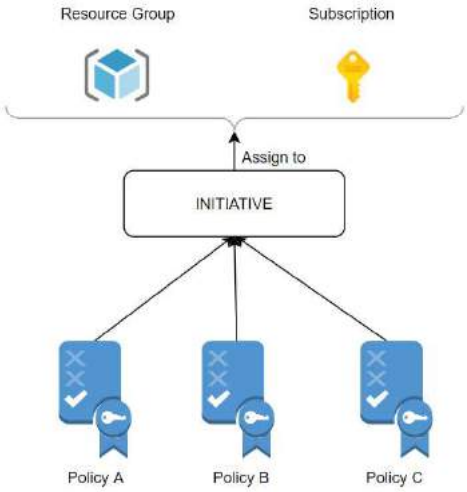
Earlier RBAC had only allowed, but now it can be denied assignments also. If there is a deny assignment, the user will be blocked from doing the action. Deny assignments take precedence over role assignments where a given user has both allow and deny but deny will be the end action.

6. License requirements

RBAC feature is free and included with our Azure subscription.

Azure Policy

- Every organization has a set of standards which are set up. Some of these could be best practices for smooth functioning or cost optimization.
- Others could be mandatory compliance adhering to Government laws and/or governing bodies like **ISO** or **HIPAA**.
- Azure Policy is a free service in Azure that we could use to define, assign, and manage standards for resources.
- Let's say that **GDPR** policy mandates that data should not leave the country. T
- Then we can create a policy that could prevent or just mark as non-compliant if data were stored outside the country.
- Once such a policy is set, it would even point to such previously created resources which are non-compliant.
- With quite a few built-in policies under categories such as *Storage, Networking, Compute, Security Center, and Monitoring,* it is very convenient to select the policy that suits us and use them simply.



Here are the steps to using Azure Policy

Step 1: Policy Definition

- First, we create a policy definition.
- We could also use existing definitions.
- We could take multiple policies and create a policy definition.

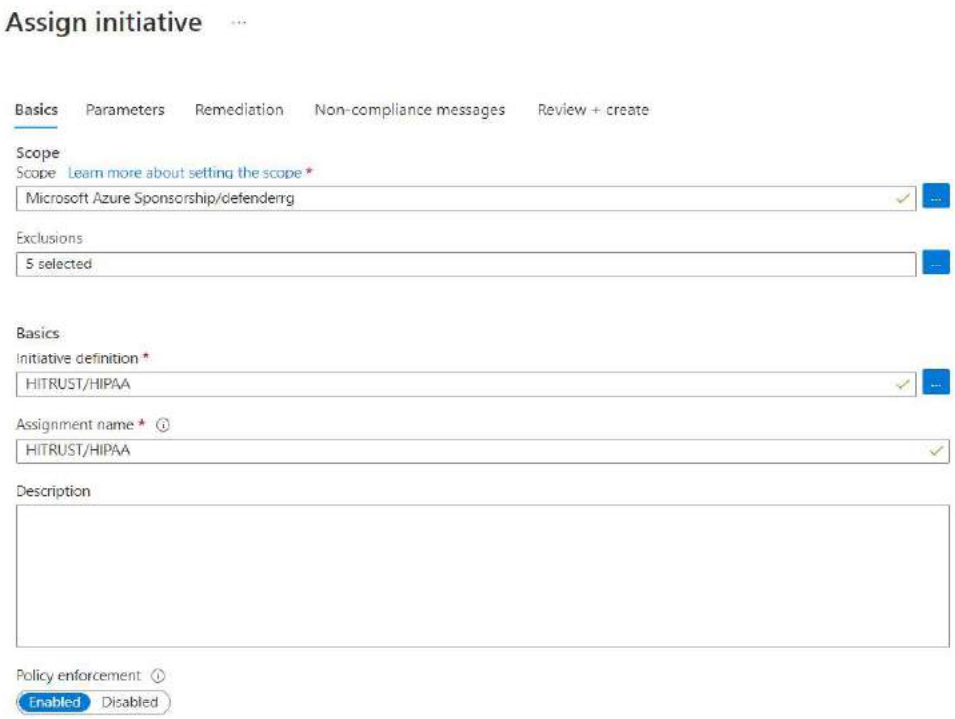
Step 2: Policy Initiative

- Once the policy definition is done, we need to create the initiative definition.
- We can select any number of policies we need and create a group to add the policies.
- We can initiative parameters and policy parameters
- We then create the initiative definition

Step 3: Assign Policy/Initiative

- We could either assign a policy or an initiative. It is better to assign initiative as we could assign multiple policies.

- Here we also select the scope. We can assign to an entire subscription or resource groups within a subscription.
- Also, we could exclude resources. Let's say we selected subscription 1 but we want to exclude one Resource group. Then we use the exclusions. In the example below, 5 resources are excluded from the above-selected resource group.
- We select the initiative definition. In our case below, we selected HITRUST/HIPAA, and this initiative will have lots of policies as per the regulatory compliance for the HIPAA act.
- If we planned to enable it at a later time, we could mark the policy as disabled.



Common use cases for Azure Policy

- **Implementing Governance**
- **Regulatory compliance like GDPR/HIPAA/PCI DSS**
- **Security**
- **Cost**
- **Management**

All Azure Policy data and objects are encrypted at rest.
Once set up, we can see the non-compliant policies, and we will be able to remediate.

How are policies evaluated

The following are the times or events that cause a resource to be evaluated:

- During the standard compliance evaluation cycle, which occurs once every 24 hours.
- A policy or initiative is newly assigned to a scope.
- A resource is created, updated, or deleted in a scope with a policy assignment.
- A policy or initiative already assigned to a scope is updated.

Some built-in Policies available

In Azure Policy, we get several built-in policies that are available by default. For example:

- **Allowed Locations** (Deny): We can allow only certain locations like the USA if the company operates in the USA.
- **Not allowed resource types** (Deny): If a particular resource type like CosmosDB is not allowed, then we cannot create the same.

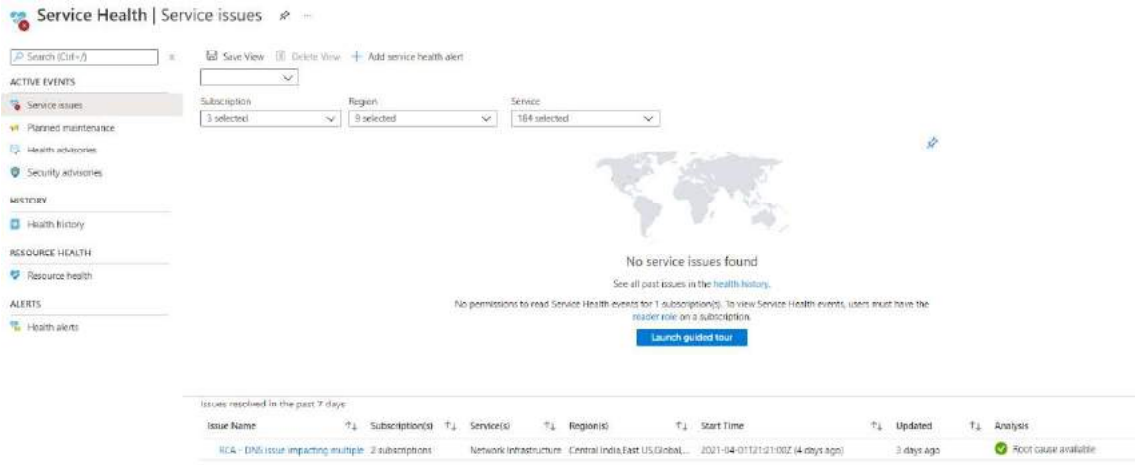
Azure Service Health

- Azure Service heath is a personalized dashboard that shows the service issues that affect you.
- It is able to dynamically do this to all the regions that we have resources in and all the resources that we have allocated for our subscriptions.
- We could even configure and add/remove regions or services or simply add all of them.
- The other features of Service health include cloud alerts that can notify us of any active issues or upcoming maintenance configured by us.
- Once we subscribe to an issue, we will get details and updates and we will get incident RCA.
- With Service Health, we get guidance and support during service incidents.

Here are some details:

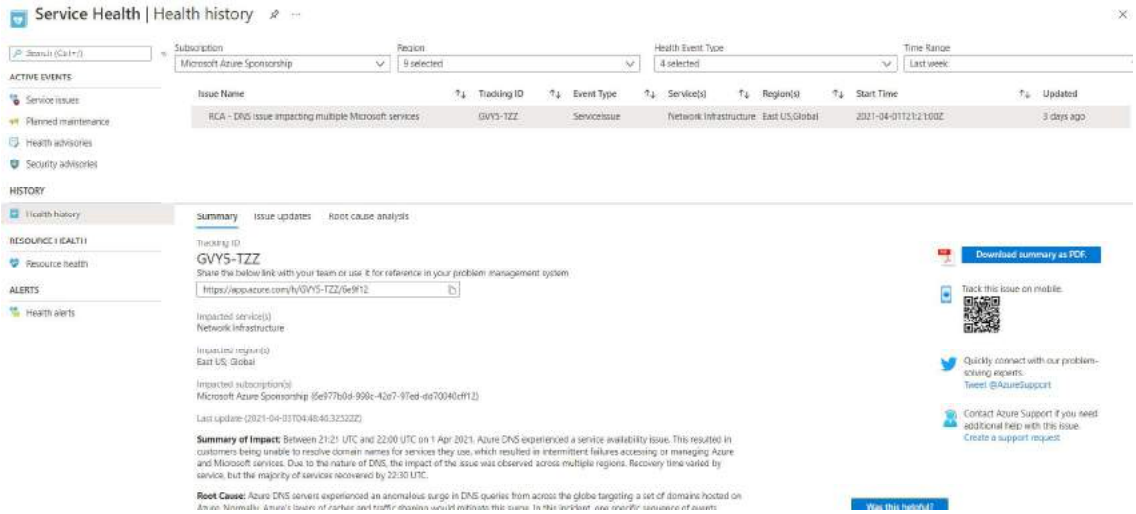
Service Issues

- This panel shows us any current issues that are on-going for the **regions/resources** where our resources exist.
- You can see that 3 subscriptions are selected with 9 regions and 184 services.
- You can also see the past incident at the bottom that has been resolved.
- We can get complete details and also download the RCA (Root Cause Analysis) for the issue.



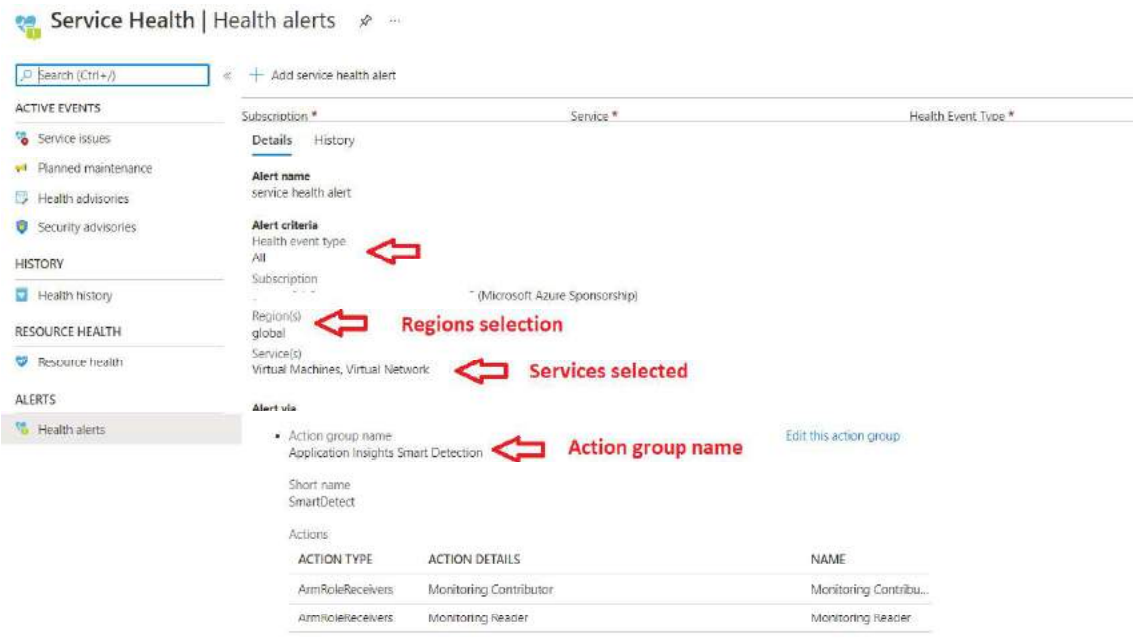
Health History

- We can see the health history and we can get details like Summary/ Issue updates/RCA.



Health Alerts

- We can set health alerts to be notified for the services we choose and for the regions which are of interest to us.
- Here we have selected to be alerted via the Action group when there are issues with VMs and VNets for all regions.
- Once set up, we will get an email when any issue occurs. We could also select the type of event. In this case, we have selected all events.



FAQs

1. **What are the permissions needed to view Service Health?**
   To view Service Health events, users must have the reader role on a subscription.

2. **How does Azure Service Health compare with Azure Status page?**
    - We use Azure status page for a global view of the health of all Azure services.
    - It serves as a quick reference for incidents with widespread impact. You can access this page at https://status.azure.com.
    - Service Health keeps us informed of the health of our environment with a personalized view of the status of our Azure services.
    - It provides us richer features including alerting and RCAs.

3. **What is the difference between Resource Health and Service Health?**
   Service Health provides information about the health of individual cloud resources, such as VMs etc. Service Health provides a personalized view of the status of our Azure services and regions

4. **If a service is down, should we contact Microsoft?**
   We need to check Service Health first to see if there is a known incident affecting us. If there are any outages reported also, we need to monitor for updates. If there is no issue listed, we need to create a support ticket.

5. **What is the cost for Azure Service Health?**
   Service Health is available at no additional cost.

6. **What are the SLAs for Azure service health?**
   Since Service Health is a free service, it does not have an SLA.

Azure Key Vault

Best practices dictate that we never hard-code sensitive information like password-strings etc., in our code. If we do so and store the code in Github, the information could be leaked and misused. Even the connection strings like urls for databases or even IP addresses or our servers must be protected.

Azure has a secret store called Azure Key Vault, which stores our secrets and passwords. One could never be able to read the secret but will be able to use it with the right set of permissions.

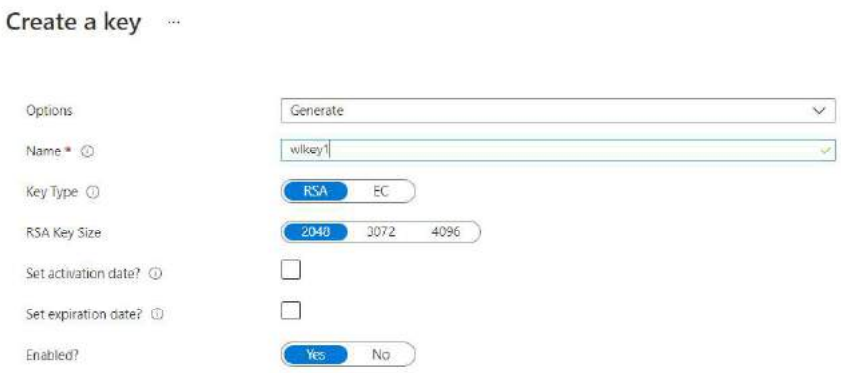
Azure Key Vault is a **PaaS platform in Azure. It** is integrated into Azure Active Directory. We can store secrets, Keys, and certifications and have multiple versions stored. We have audit logs as a feature. Azure Key vault is **FIPS 140-2** compliant.

Secrets

- We can store up to 25kb in size.
- We can store plain text passwords, connection strings, JSON, XML, and more.
- We can have an activation date and expiry date.
- We can create as enabled or not if we don't have immediate use etc

Keys

- A Key is typically asymmetric in the **PKI (Private Key Infrastructure)**. Here we have a public key and a private key. The public key is known to all, and anybody can use it to encrypt the data. But the private key is known only to the owner, and only the private key can decrypt the data.
- Azure will generate the private and public keys, but the private keys will never be disclosed.
- We could also use symmetric keys for storage and SQL data, and in this case, the symmetric key would be wrapped with an asymmetric key making it secure.
- The key type could be **RSA/EC** and **2/3/4 kb** in size.
- We can have an activation date and expiry date.
- We can create as enabled or not if we don't have immediate use etc.



Certificates

- We could either generate our keys or import keys.
- Keys could either be self-signed or use a CA (Certification Authority) like Digicert or GlobalSign, etc.
- We can have validity between 1 month to 10 years.

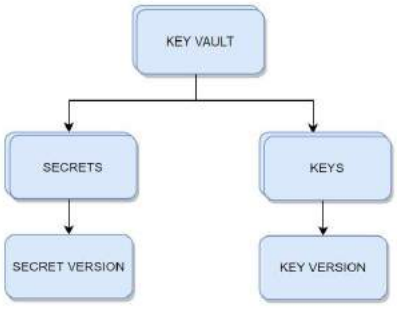
Audit

Since all activity takes place within the Azure Key vault, we can audit all types of usage. We can see who is using and type of activity.

Versioning

It is always recommended to keep changing the secrets. This will help protect in case the secrets were leaked to limit the damage. To do this, we can create a new version. Also, we need to automate the process so that we don't forget to do it.

Azure Key Vault has a **unique versioning engine.** We can rotate secrets and keys, and new versions are created. When we have used an older version of the key to encrypt, we will be able to point to the older version and decrypt the data.



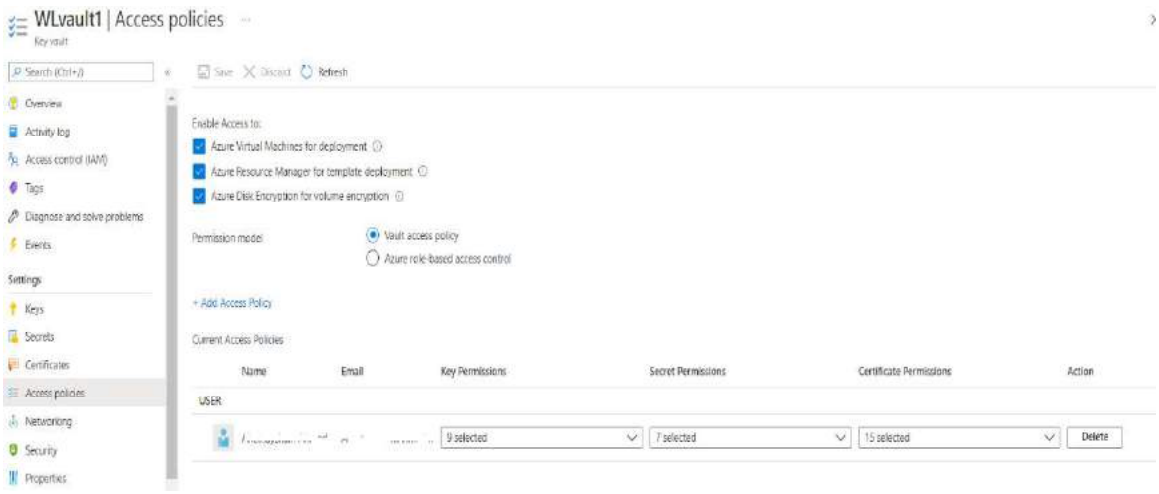
Access Policy

We can set access policies at the key vault level and more granularly at the **Key/Secret** and Certificate level.

We can enable access to:

- Azure Virtual Machines for deployment
- Azure Resource Manager for template deployment
- Azure Disk Encryption for volume encryption

The above will allow the usage of the key vault for the VMs/ disk and other deployments to be attached automatically.



Also, we can have access granted via the key vault policy or via RBAC.

FAQs

1) **We want to have a different set of access for different secrets to the same individual. How do we achieve it?**
   Create another key vault and grant access.

2) **Is Key Vault regional or global?**
   Though Key Vault is global, use key vault in the region where your data resides to reduce latency.

3) **When do we choose the access policy and when to choose RBAC?**
   There are two Access planes – one is the Management plane, and the other is the Data plane.
   a. **Management Plane**
      i. This ties to the key vault level
      ii. Operations are create/update/delete of Key vaults/ access policies / tags etc
      iii. They don't involve with what's inside the key vault, i.e., the actual content

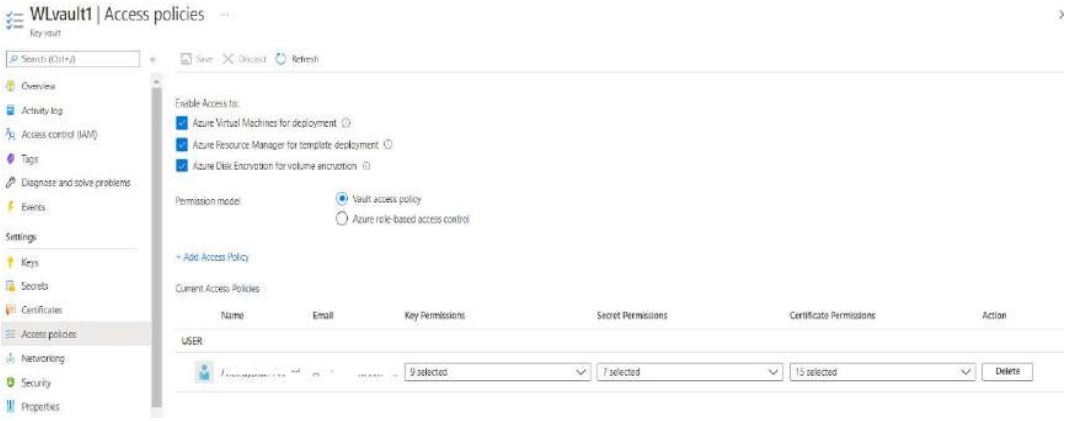
iv. This is controlled by RBAC only

b. Data Plane

i. This deals with secrets/Keys/Certificates
ii. Example for Keys - encrypt, decrypt, list, delete, backup, etc
iii. Example for Certificates - get, list, create, import, update, delete, recover
iv. Example for Secrets - get, list, set, delete, recover, backup, restore, purge
v. This can be controlled by either RBAC or Key Vault access policy

4) My RBAC roles for Key vault management are not working. What could be the problem?

a. Please see the permission model below is selected for Vault access Policy and not Azure RBAC. Please change to RBAC and retry.



5) Please list RBAC roles for key vault Management?

a. Key Vault Administrator
b. Key Vault Certificates Officer
c. Key Vault Crypto Officer
d. Key Vault Crypto Service Encryption User
e. Key Vault Crypto User
f. Key Vault Reader
g. Key Vault Secrets Officer

Azure BLOB

Azure Storage has 5 types:

Azure Blob storage	*Used to store Binary/Text data*
Azure File storage	File Shares
Azure Disk Storage	Persistent data storage
Azure Queue storage	Messaging Store and Queuing
Azure Table storage	NoSQL Datastore

Blob Storage:

- Scalable
- Use REST API, CLI, ARM template to create a storage account
- Blob is typically a file, can be image, file, video
- Common scenarios – backup/restore, upload large files, logging
- It can be used for DR purposes
- The newest version of ADLS (Azure Data Lake Storage) is built on top of Blob Storage called ADLS Gen2
- Endpoint for Blobs is https://*.blob.core.windows.net
- For a blob, the base URI includes the name of the account (myaccount), the name of the container(mycontainer), and the name of the blob(myblob). Here name will as follows:
    - https://myaccount.blob.core.windows.net/mycontainer/myblob
- You can use Storage Explorer to view/upload/copy files

Limits:

- No limits to the number of objects
- Max size of a single object in a container is about 5TB

Blob types

- Block Blob – Large objects that are broken and each block is uploaded in parallel. It is optimal for Streaming
- Append Blobs – We use these where we keep updating and appending to the files. For example, logging.
- Page Blob – Stores the VHD VM disks. Max size is 8TB

Access levels

- **Private (no anonymous access)** – This is the default. A valid token is needed to access data.

- **Blob (anonymous read access for blobs only)** – Globally accessible with reading access
- **Container (anonymous read access for containers and blobs)** – All blobs in the container can be read and listed. Access is at the container level, and hence it is for container level, and every blob can be read.

Access Tiers

- There are 3 access tiers – **Hot/Cool and Archive**.
- As you move from Archive to hot, the pricing will go up, and as you move from Hot to Archive, the cost of accessing will go up.
- You need to decide based on how often you access and balance between storage cost and access cost.
- **Cool** – Use this for more than 30 days but less than 180 days
- **Archive** – This is for anything accessed for more than 180 days. Please note that it will take several hours to access the data.
- To recall, you need to "rehydrate" the blob by changing the access tier to Hot or Cool. This can also be set at blob level only, whereas COOL/HOT is at the account level.

Zone Replication

Storage can be replicated for availability. Here are the options:

- **Locally redundant storage (LRS)** – 3 copies stored in a single Datacenter. Single point of failure if the data center is unavailable. Cheapest option.
- **Zone-redundant storage (ZRS)** – 3 copies in 3 zones in the primary region. Also recommended to replicate to the secondary region.
- **Geo-redundant storage (GRS)** – Here, the secondary copies are stored in another region, which protects us against a region-wide outage. Basically, it is LRS plus an additional copy in a secondary region. The primary copy process is Synchronous, while it is asynchronous for secondary.
- **Read-access geo-redundant storage (RA-GRS)** – Compared with GRS, the secondary copy will also be available only for READ access.
- **Geo-zone-redundant storage (GZRS)** – Here, it is the same as LRS except that the secondary copy will be in a zone in another region, which is the twin region of our primary region. Basically, it is ZRS plus a single copy in the secondary region. The primary copy process is Synchronous, while it is asynchronous for secondary.
- **Read-access geo-zone-redundant storage (RA-GZRS)** – Same as GZRS, except that you will be able to read data from your secondary region also. *(If it is not RA, then we need to remember that data is available but not readable until Microsoft fails over to the secondary region in case of a regional failure or if we manually failover)*

	LRS	ZRS	GRS	RA-GRS	GZRS	RA-GZRS
Node	✓	✓	✓	✓	✓	✓
Datacenter/zone	×	✓	✓	✓	✓	✓
Region	×	×	✓	✓	✓	✓
Read-access	×	×	×	✓	×	✓
SLA	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%
Durability	11 9's	12 9's	16 9's	16 9's	16 9's	16 9's

Lifecycle Management

- You can use lifecycle management to move your data from one access tier to another.
- For example, you can move from Hot to Cool after 30 days and then from Cool to Archive after 180 days and then delete after 1 year.

Soft Delete

- If you enable this feature, the blob will not be deleted but will be marked for deletion.
- You specify the number of days, like 90, and after 90 days, the blobs will be deleted.
- This protects against malicious or accidental deletion.
- Please note that you will pay for the 90 days of storage.

Built-in Roles for Blob storage

Role	Access
Storage Blob Data Contributor	Read, write, and delete Azure Storage containers and blobs.
Storage Blob Data Owner	Provides full access to Azure Storage blob containers and data operations
Storage Blob Data Reader	Read and list Azure Storage containers and blobs.
Storage Blob Delegator	Get a user delegation key, which can then be used to create a shared access signature for a container or blob that is signed with Azure AD credentials.

Azure Storage Firewalls and Virtual Networks

- We can have a layered security model and specify the IP addresses from which access will be allowed.
- Also, we can specify Vnets/subnets from where access will be allowed.
- *Time-bound access – SAS Signatures*
- A Storage account key gives complete access to your data.

- If there is a need to provide access for a short/limited period, we can create a **SAS Signature** with a start and end time, and the data can be accessed during that window only.
- We can specify allowed *services/service types/permissions (Read/Write/List etc)/Start and expiry date/time/ Allowed IP address range*

Use Case Scenarios:

- *A Company wants to store more than 5TB of data. The cost must be minimized – Solution – Azure Blob Storage using Import/Export Service.*

- *A Company wants to use Azure Storage. The Data has various usage tiers. Tier 1 – Used regularly and needed immediately in the first 30 days, Tier 2 – Not used after 30 days, Tier 3 – Not used after 180 days, and Tier 4 – Can be deleted after 1 year. – Solution – Implement Lifecycle Management*

- *A Company plans to move 500MB of data to Azure Blob. What is the best Method – Solution – Download Storage Explorer (or use Storage explorer on the portal) with SAS and transfer data*

- *When creating a storage account, what tiers can we choose – Hot, Cool, Archive. Answer – Hot and Cool only. Archive Tier is at Blob level only.*

- *You want to protect your storage account against accidental deletion. What do you do? Solution – Enable Soft Delete*

- *With Soft delete enabled, a file is deleted. 2 snapshots are also deleted. What can be recovered? Answer – The snapshots and file can be restored.*

Azure File Storage

File Storage:

- It is one of the 4 storage solution offerings by Azure.
- One of the best use cases is the offering of fully managed file shares.
    - The file share is accessible over **Server Message Block (SMB)** protocol or **Network file system (NDS)** protocol.
    - Can mount Azure file shares either on Cloud or on-premises.
    - SMB file shares are accessible from Windows, Linux, and MacOS, whereas NFS file shares are accessible over Linux or MacOS clients.
- The file share concept can be extended to caching on Windows Servers with Azure file Sync. This allows for fast access closer to the location it is being used.

Use Cases:

- The Company has headquarters in New York and a branch office in California. Users in California are seeing latency accessing the data which is created in New York.
    - **Solution** – Use Azure File Sync, which will cache the data closer to the California location.
- The Company wants to migrate its application. The application has data residing on file shares mounted.
    - **Solution** – Use Azure files for Lift and Shift scenarios. Create a file share and mount it as a drive, and the application can be migrated and will point to this file share mounted as a drive.
- One of the clients wants high availability and has had an issue with file servers being down often.
    - **Solution** - Use File shares. If a server crashes, place a new Server, and it will automatically get the data from the cloud with Azure File Sync setup

FAQs

- **What ports does file share use?**
    - SMB protocol uses 445
    - NFS protocol uses 2049

- **How do we back up Azure file shares?**
    - Please take snapshots.

- **What versions of SMB are there, and what to choose?**
    - SMB 2.0 and SMB 3.0 are mostly used
    - SMB 3.0 is the preferred version since it provides encrypted access.
    - If a client does not support SMB 3.0, downgrade to SMB 2.0

- **Can I use Import/Export Service with Azure files?**
    - You can import into Azure files, but you cannot export from Azure files. With Blobs, you can import and export.
- **There is a requirement to use Azure files for IO intensive workloads like hosting Databases and HPC. Is this possible?**

    - Yes, please use Premium file shares as they are stored on SSD. Please note that replication has to do with the LRS only.

- **Is the storage unlimited, or are there limitations?**
    - Azure files work with Quotas. When you create a file share, you need to specify a quota like 100GB. You can alter if needed.

Tips

- **Can I use SAS to map a drive?**
    - It is possible to map a drive with SAS.

- **Can we provide share level permissions? What are inbuilt roles?**
    - *Storage File Data SMB Share Reader* – Allows READ access
    - *Storage File Data SMB Share Contributor* – Allows read, write, delete access
    - *Storage File Data SMB Share Elevated Contributor* - Allows read, write, delete, and modify Windows ACLs.

Azure Disk Storage

- VMs in Azure use two types of disks. One is an operating system disk, and the other is a temporary disk.
- The operating system with and without customization is stored as an image and loaded when the VM is built.
- Both the image and the operating system disk are virtual hard disks and are stored in a Storage account.
- The temporary disk will be stored as part of the hardware itself to provide faster access.
- The virtual hard disks use .vhd files and are stored as page blobs. Please see the blob types below:

Blob types

- **Block Blob** – Large objects that are broken and each block is uploaded in parallel. Optimal for Streaming
- **Append Blobs** – We use these where we keep updating and appending to the files. For example, logging.
- **Page Blob** – Stores the VHD VM disks. Max size is 8TB

We can also specify additional disks to store application data etc. These are called data disks. Azure offers different kinds of disks broadly classified as Managed and Unmanaged storage.

Unmanaged Disks

- This is the traditional type of disk. Here we create the storage account and specify the storage account when we use the disk.

- If we have too many disks, then there will be contention, and VMs will throttle, which will impact the performance.

Managed Disks

- This is the latest and recommended type to allocate. If we have unmanaged disks, Azure gives us the option to migrate to managed disks.
- We don't need to specify a storage account or manage the storage account. Azure takes care of management, including scalability. We just need to give the size and performance tier.
- These are the types of managed disks.
    - **Standard HDD** – These are standard magnetic drives and are the cheapest. We can offer Recovery services to replicate locally or be geo-redundant
    - **Standard SDD** – These are more consistent and reliable, and suitable for web servers.

- **Premium SSD** – These are backed by solid-state drives and deliver high performance, low latency, and useful workloads that are I/O intensive, like production and performance-sensitive ones.
- **Ultra disk** – This is the latest type, which has a max iops of 160K. But these can be used as data disks only and not OS disks.

Azure Backup Service

- Azure provides an Azure backup service to perform backups.
- We need to install an extension and need to specify the frequency.
- The snapshot will be taken for the OS disk as well as the **data .disk**
- The snapshot taken here is different from the image. The disk is prepared to create an image, and no activity is allowed, and sysprep is done.
- Here, we allow the system to run in snapshotting, and we take either application-consistent snapshots or file consistent snapshots. These snapshots are moved into recovery service vaults.
- We can set up a recovery service vault to replicate to another region.
  For example, we are in the US East, and we replicate to the US West, which protects from entire East US failure.

FAQs

- **A company has SAP Hana and other top tier databases like SQL and Oracle. What is the recommended disk type?**
  - Please use Ultra disks for data disks. Use Premium SSD for OS disk.
- **A company has a disk requirement of more than 32TB. What are the available options?**
  - Please use Ultra disks or use mirroring with striping.
- **A company wants more than 50,000 IOPS but does not want to use Ultra disks. What can be done?**
  - Please use mirroring with striping. If one disk has 20K iops and you do striping with 2 disks, you will get 40K iops, and with 3 disks, you will get 60K IOPS
- **Will the disk be deleted when we delete a VM?**
  - No, you need to delete disks explicitly.
- **I had allocated 100 GB, but now I want to add 100 GB more. Can I do that on my existing machine?**
  - Yes, deallocate VM and update disk.
- **Can we cache data?**
  - Yes, disk caching can be set to NONE or READ ONLY or READ/WRITE. For log disks, use READ ONLY.
- **Can Multiple VMs read the disk on a given VM?**
  - Yes, we can enable disk sharing.

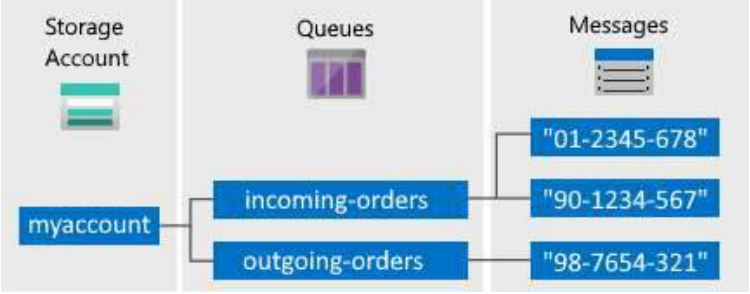
Azure Queue Storage

Queue Storage:

- This component of Azure storage is for messaging store and queuing.
- Simple and cheap
- The preferred workload of more than 80GB when compared to the Service Bus queue.
- Can Scale and message node failure will not affect Service since other nodes will process.
- Can add more worker nodes if there is a burst

The architecture of Queue storage

- We create a storage account.
- Within the storage account, we create Queues.
- For example, we create 2 queues, one incoming order and one outgoing payment.
- There will be messages which we will store under the queues.
- These messages will be read at least once and processed by the applications.



- **URL format:** Queues are addressable using the following URL format:
  http://<storage account>.queue.core.windows.net/<queue>
- The following URL addresses a queue in the diagram:
  http://myaccount.queue.core.windows.net/incoming-orders

Use Cases

- Provides a decoupling architecture. This allows for asynchronous communication.
- Let's take an example of a Purchase system integrated with a Shipping system.
- In the traditional model, both the purchase and shipping system is integrated.
- When a customer places an order, the purchase system sends the order to Shipping, and it has to get an acknowledgment.
- If there are too many orders and the shipping system does not acknowledge, it will break the system.
- In asynchronous communication, we decouple, and the purchase system does not wait for an acknowledgment.
- It will send a message, and the shipping system might check for the message queue every 5-10 minutes and process the orders. Here we use the Azure queue storage.

FAQs

- **Can we have ordering like FIFO for messages?**
  - No

- **Does Queue storage support transactions?**
  - No. Each message is independent. If 20 of 30 messages are read, and the operation fails, this is not an all-or-nothing situation to have a transaction concept to rollback 20 and process from the beginning.

- **Does Queue Storage push messages?**
  - No, it would help if you fetched the messages.

- **Can we lock messages for exclusive access?**
  - Yes, you need to acquire a lease during which period you have exclusive access.

- **What is the lease duration?**
  - 30 seconds default lease duration
  - 7 days max for lease duration
  - Can be renewed
  - The level is a message

- **Can we use batches for processing?**
  - Yes

- **Does Queue storage provide dead lettering?**
  - No

- **What are the limits?**
  - Max queue size – 500GB
  - Max message size – 64KB
  - Max number of queues – no limit

Azure Table Storage

Table Storage:

- This component of Azure storage can be used as a **NoSQL** Datastore.
- It stores data in a key-value pair. We have a partition key and a row key. These are default columns. We can add columns as needed.
- We can query or insert data using Storage Explorer.

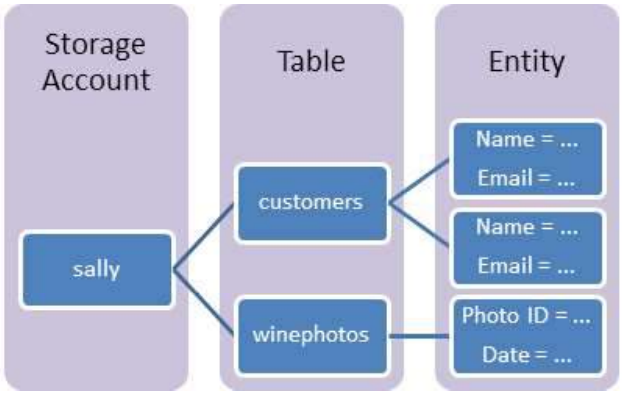


Table Storage architecture

- **URL format** for Azure Table Storage accounts: **http://<storage account>.table.core.windows.net/<table>**
- In the Storage account, we create an account (Sally)
- Under the account (Sally), we create a table (customers)
- Under the table (customers), we insert rows called Entities.
- Entities contain properties that are a key-value pair.
- Therefore Storage *Account -> Table -> Entities -> Properties*

Use Case

- Use Table storage for storing semi-structured data
- Use this for creating an app that needs a flexible data schema.

FAQs

- **How much can we store?**
  - We can store Petabytes of data.
- **Is availability a concern?**
  - With GRS, data is replicated 3 times within a region and another 3 times in an additional region. So it is highly available.
- **What is Cosmos DB table API?**
  - Cosmos has several APIs like Mongo/SQL/Gremlin, and one of the supported APIs is Table API. Both Azure Table storage and Cosmos DB table API have the same data model and support the same operations like query insert via SDK. Using the Cosmos DB table API will increase the performance like single-digit ms latency, scalability, global distribution, etc.

Azure Archive Storage

Archive Storage:

- Use Azure archive storage for rarely accessed data.
- Lowest priced storage tier
- Automatic encryption of data
- Seamless integration with Hot and cool storage tiers
- Secure data transfer with HTTPS.
- Minimum **180** days storage requirement – If we move before that, we pay early deletion fees for the number of days falling short.

Use Cases

- **Archival**
  - Healthcare and other regulations like SOX (financial records etc.) require that information be stored for multi-year periods. This provides long term compliant storage.
- **Long term Backup Retention**
  - There might be a requirement to store Database, server, desktop data for multi-years. This provides long-term storage freeing up local disk space.
- **Magnetic tape replacement**
  - If your organization has a VTL (Virtual tape library), you can move the least accessed data to archive storage.
- Other use cases are Security/Public safety data and other digital media content retention.

FAQs

- **What types of storage can be stored in Archive Storage?**
  - Only Blob storage

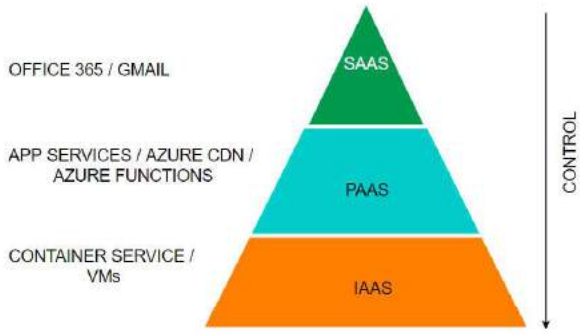
- **What are the retrieval options?**
  - There are two options.
    - *Standard Priority (Default)* – up to 15 hours
    - *High Priority (Max 10 GB)* – less than 1 hour

- **What are the fees associated with Archive Storage?**
  - The fess is as follows:
    - Data Retrieval – Standard – 1.3220$/GB
    - Data Retrieval – High Priority – 6.6097$/GB
    - Write Operation – 6.6097$/10000
    - List/Create container operation – 3.3049$/10000
    - Read Operation – Standard – 330.4813$/10000
    - Read Operation – High Priority – 3304$/10000

Azure Virtual Machines

There are 3 major delivery models when it comes to Cloud services. They are:

1. **SAAS – Software as a Service**
2. **PAAS – Platform as a Service**
3. **IAAS - Infrastructure as a Service**



- Azure Virtual Machines are part of the **IAAS** offering from Azure.
- As customers, we are responsible for managing the virtual machine, and just the hardware will be provided to us by the cloud provider. We can *start, stop and delete* the virtual machine.
- If we find that the capacity is insufficient or too high, we can change to a different machine type. We can install any software as we like.
- Also, please note that this is the most expensive of the three offerings.
- We can create **Windows or Linux VMs**, and there are multiple locations throughout the world where resources can run from.
- When we create a VM, we need to attach a virtual hard disk, and the location that we specify is where the hard disks are stored.

Here is the SLA table:

Sl No.	VM	Disk	SLA
1	2 or more VMs across 2 or more AZs		99.99% at least 1 VM
2	2 or more VMs in a same Availability set		99.95% at least 1 VM
3	Single VM	Premium or Ultra disk for all disks	99.9%
4	Single VM	Standard SSD	99.5%
5	Single VM	Standard HDD	95%

Please see below details for VM types:

Sl No	Type	Sizes	Short Description	Best for
1	GP (General Purpose)	B, Dsv, Dasv, Dav, Av2, DC, Dsv	Balanced CPU to memory	Testing/ Dev, small DB, low traffic servers
2	Compute Optimized	F, Fs, Fsv2	High CPU to memory	Medium traffic servers, batch processes, app servers
3	Memory-Optimized	Esv, Ev, Eav, Mv2, M, DSv2 , Dv2	High memory to CPU ratio	RDBMS servers
4	Storage Optimized	Lsv2	High disk throughput and IO	Big data/ DB warehousing/ Large DB
5	GPU	NC, NCv2, ND, NV	Specialized VMs for heavy graphics	Model training with deep learning
6	HPC (High-performance Compute)	HB, HBv2, HC, H	Fastest and most powerful CPU	Real-time processing

FAQs

1. **How do I resize a VM?**
   You can first run the list-vm-resize-options and see available sizes. If you find the size, you can run the resize command

   ```
   az vm resize --resource-group WLRG --name WLVM1 --size Standard_DS3_v2
   ```

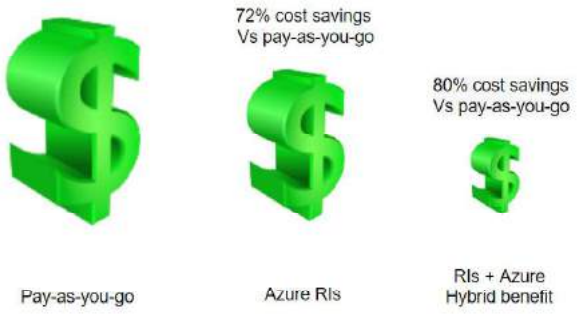
   Else you need to deallocate the VM, which will allow you to use any size. You need to deallocate, resize and start a VM.

   ```
   az vm deallocate --resource-group WLRG --name WLVM1
   ```

   ```
   az vm resize --resource-group WLRG --name WLVM1 --size Standard_DS3_v2
   ```

   ```
   az vm start --resource-group WLRG --name WLVM1
   ```
2. **What are Azure Dedicated hosts?**
   We usually shared the physical hardware with other tenants. If we want exclusively to use the physical server, then we can choose dedicated hosts.
3. **What are Azure Spot instances?**
   This feature allows us to take advantage of the unused CPU at a significantly lower cost at almost 90% savings. If there are workloads that can tolerate disruption and can be restarted, then we can choose this option. If there is another bidder who bids more than our price, we will be vacated on 30 seconds' notice. So we need to be prepared with proper scripts to save the data or any other process from exiting gracefully.

4. **How can we save costs on VMs other than Spot instances?**
   There are two other ways we can save on costs.–



5. **Reserved Instances** – We can commit to 1-year or 3-year and choose to pay upfront or monthly to buy RIs. We have the flexibility to change size if needed.
6. **Azure Hybrid Benefit** – If you have a license already, you can use the license on Azure and get this benefit.
7. **What are Azure Images?**
   If there is a custom image that we want every VM to have when created, we can choose to create a standard VM and sysprep and then create an image. We can then use this image to create VMs.
8. **How can we make VMs highly available?**
   We had discussed in the excel above with SLAs. We can use multiple machines either in availability or in more than 1 availability zone. In addition to this, we can use Azure VMSS (Virtual machine scale sets). VMSS is automatically created from a central configuration using a standard template. More VMs will be added during peak and will be brought down when the demand goes down based on our auto-scaling options.
9. **How can we back up VMs?**
   We have 3 options:
   a. **Azure Backup** – We can create recovery vaults and configure Azure Backup to back up our VMs
   b. **ASR (Azure Site Recovery)** – Here, our VMs are replicated to another region, and our entire production region fails; we can failover to the backup areas with the click of a button
   c. **Managed Snapshots** – If we have managed disks, we can take a snapshot of our disks, a read-only copy. We leveraged this feature for quick backups in dev and test environments.
10. **How can we monitor VMs?**
    Under Monitoring tabs, we have metrics to see various parameters. We can also set alerts. We can also Log analytics by enabling the Logs option in Monitoring. We need to create a log analytics workspace.

Azure App Service

Azure App Service allows us to run applications on the cloud. Here are some features:

- HTTP based Service for hosting web applications, REST APIs, and mobile backends.
- Supports .NET, .NET Core, Java, Ruby, Node.js, PHP, Python
- Run and Scale on Windows/Linux

App Services run under an app service plan. An app service plan is the logical abstraction that represents one or more VMs that runs the app service. It consists of compute resources like CPU, memory and disk space. We pay for app service plans and not the app service.

Also, we can have more than one app service running inside an app service plan. The number of app services that can run inside an app service plan depends on the app service plan. Also, the amount of resources like CPU, RAM and disk space depends on the app service plan.

Plan	Compute type	Custom Domain	Scaling	Workload	Space	Backup / Restore	No of Apps (max)
Free	Shared	No	No		Nil	No	10
Shared	Shared	Yes	Yes	Dev	1GB	No	100
Basic	Dedicated	Yes	Yes	Dev/Test	10GB	No	Unlimited
Premium	Dedicated	Yes	Yes	Prod	250GB	Yes	Unlimited
Isolated	Isolated	Yes	Yes	Prod	1TB	Yes	Unlimited

Let's look at some features of App services:

Deployment Slots	This concept is used for zero downtime deployments. There will be a production slot and a Staging slot. New version of the Production deployment will be done in the Staging slot. Either all at once deployment or in stages(canary) will be done.
Deployment Center	This allows for Continuous integration/ Continuous deployment (CI / CD)
Custom Domains	By default, the website will be xxxx.azurewebsites.net. We can buy a domain in your company name and use that name.
SSL Settings	You can certificates and ensure encrypted data transmission between client and Server
Scale up (App Service Plan)	You can increase the size of your VM if you need more resources

Scale out (App Service Plan)	You can also increase the number of instances. You can either do this manually with a slider or set up rules/schedule to scale automatically on schedule or CPU usage (like >70%)

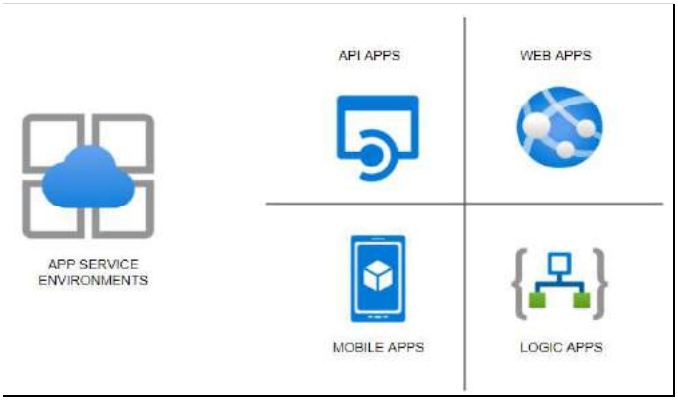
FAQs

1. **How does app service plan work?**
   App service plan is supported by Service Fabric. Service fabric replaces instances if an existing one fails. Also, it adds instances if there is a requirement.

2. **What are the types of App Services?**

   There are 4 types of services as follows:

Sl no	Type	Purpose
1	*Web App (previously Azure Websites)*	Hosting websites and web applications
2	*API App*	Used for hosting the RESTful APIs
3	*Logic App*	Used for business process automation, system integration and sharing data across clouds
4	*Mobile App (previously delivered by Azure Mobile services)*	Used for hosting mobile app back ends



App Service

- HTTP based Service for hosting web applications, REST APIs, and mobile backends.
- Supports .NET, .NET Core, Java, Ruby, Node.js, PHP, Python
- Run and Scale on Windows/Linux

Features

- **PAAS** – Patches/OS Maintenance done by Azure
- Support for Containerization and Docker
- Serverless

- **Deployments Slots** – Swap application content in Prod and avoid downtimes 
- Grouped under App Service plans with following tiers

Plan	Compute type	Custom Domain	Scaling	Workload	Space	Backup/ Restore 	Others
Free	Shared	No 	No		Nil	No	
Shared	Shared	Yes	Yes	Dev	1GB	No	
Basic	Dedicated	Yes	Yes	Dev/Test	10GB 	No	
Premium	Dedicated	Yes	Yes	Prod	250GB	Yes	
Isolated	Isolated	Yes	Yes	Prod	1TB	Yes	Private Endpoints

App Service types

1. **Webapps** – Websites/Online Apps
2. **Webapps for Containers** – Containerization
3. **API apps** – backend data

Can add – Vnet Integration / Hybrid Connections /Security, but these are not asked in the exams.

Tips

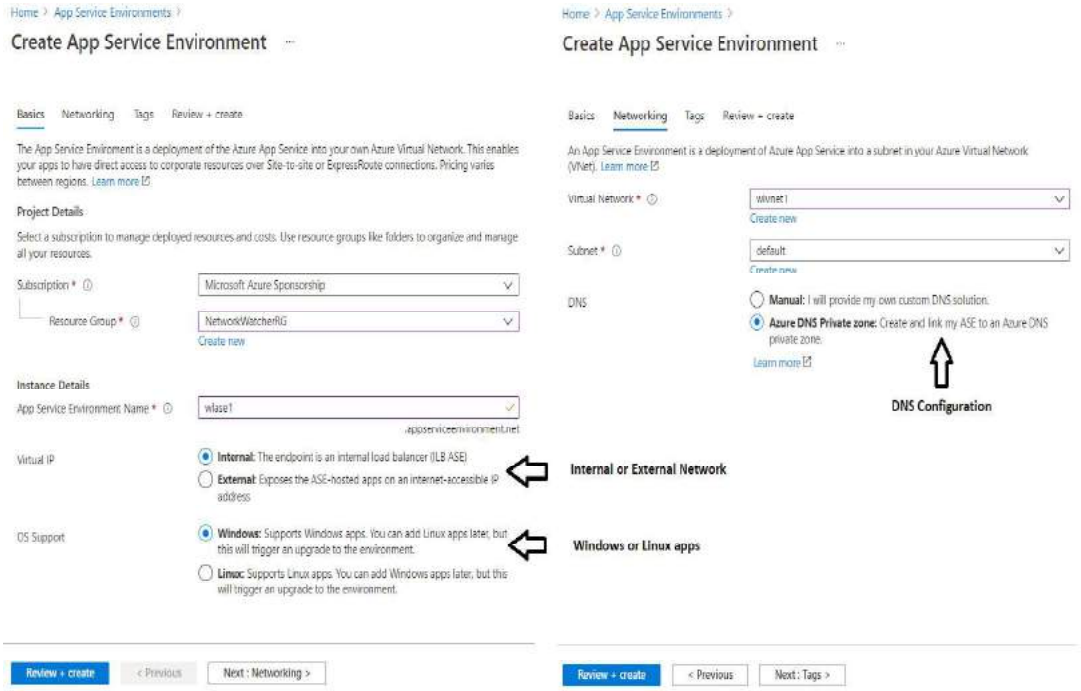
- When you move an App service from one RG to another, the App Service plan doesn't change.
- Destination RG cannot contain App Service resources like Web app or App Service plan.
- **.Net** Core application can be deployed on Windows or Linux OS
- **ASP .Net** app CANNOT be deployed on Linux OS. Only Windows OS
- Multiple Web Apps can be hosted on a single App Service plan.
- Web App and App Service plans must exist in the same region.

Application Service Environments

- There are 3 components for hosting *web apps/ Docker containers/ Mobile apps* and functions. There are app service plans which host the app services.
- When we host the regular app services, the apps are directly exposed to the internet, and the resources are shared.
- Some organizations prefer to host the services in the internal network, and security features like firewalls and security groups could be applied to protect the apps.
- For such scenarios, there is a feature called the **Azure App Service Environment**, which provides a fully isolated and dedicated environment for securely running App Service apps at a high scale.
- **App Service environments (ASEs)** provide very high scaling with isolation and secure network access with high memory utilization.
- We can create multiple ASEs within a single Azure region or across multiple Azure regions, making it ideal for horizontally scaling stateless application tiers when we have high **requests per second** (**RPS**) workloads.
  There are three types of workloads available when choosing the workload tier. They are *Dev/test, Production, and Isolated.*
- Of these, the isolated offering provides the ASE environments which host applications within the client's VNets. As stated, we have fine-grained control over inbound and outbound application network traffic.
- While the other category of app services has a fixed suffix of azurewebsties.net, we can create our own domain name.
- Also, ASEs come with powerful computers, which is twice as powerful as the regular app service plans. They also come with **1TB** Storage as compared to **50GB** of space for the regular ones.
- We can host up to 100 instances which are sufficient to host a miniature web service hub. We can expect the service to cost us about **250-300$** per month, which is very cheap for the services being provided.

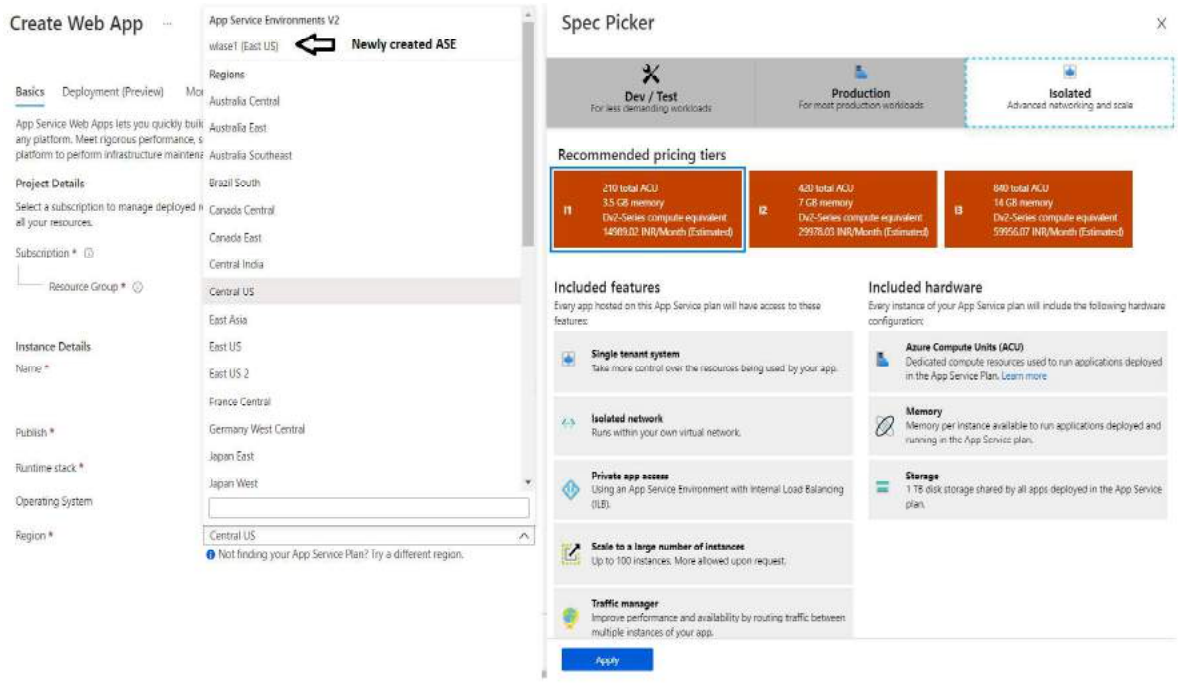
Steps to creating App Service Environment

- In the first screen, we select if the service is public-facing or internal
- Then we select whether we are hosting Windows-based or Linux-based OS.
- On the second screen, we select the Vnet where we want to host the service. *(Since services are being created in our private infrastructure, it takes much longer time to create)*
- Then we can DNS resolution. We can create our own private zone and use that name. This is not possible when choosing the other app service plans.



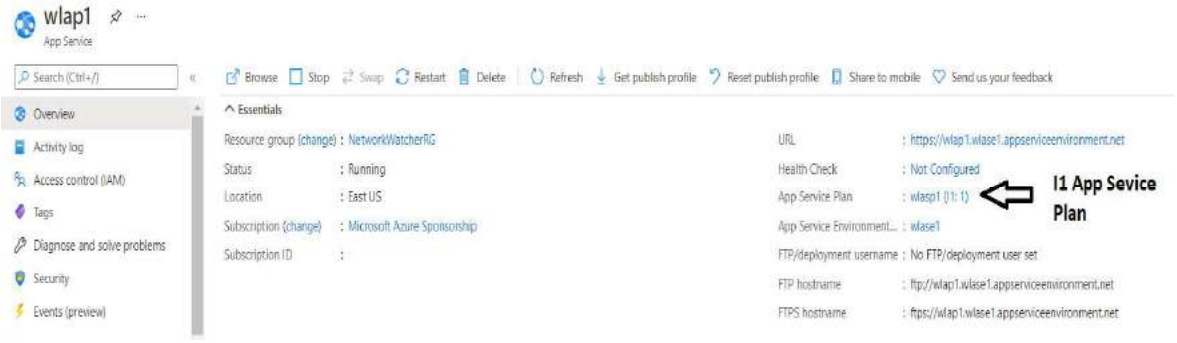
Steps to creating Web Apps under ASE

- Please note that the process is similar except that we drop down the region and select the ASE which we just created.
- Also, the below screen shows various features under ASE and pricing under each of the pricing tiers I1 and I2, and I3.



Note: *The Private link vnetLink (wlase1.appserviceenvironment.net/vnetLink) is also created below. You can go to the Resource group and click on "Show hidden types" to see this resource.*

Note: *Please see the App Service plan as I1:1 in the screenshot below to identify the isolated service plan.*



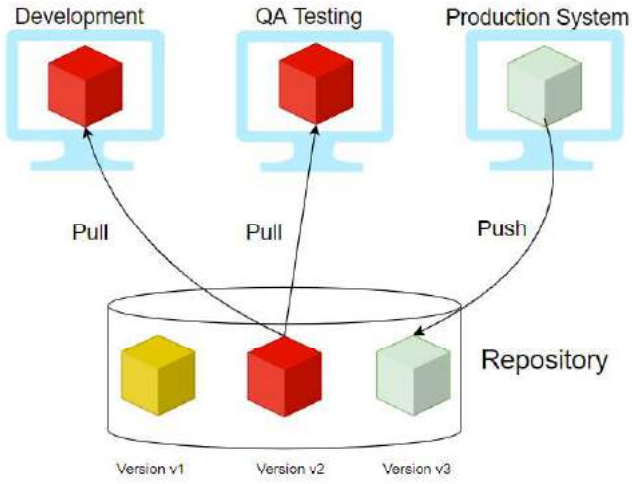
Azure Container Registry

What is a Container Registry?

A Container Registry is a central repository to store and distribute container images. A container image includes all the data needed to start a container - **for example**, the operating system, libraries, runtime environments, and the application itself.

We first build an image, and then we push the image to the repository. When needed, we pull the image into the target environment. With versioning as a feature, we have multiple versions of the container, and the different versions like the stable version would be used for Production.

Versions being tested would be in non-production regions. In the example below, v2 is a stable version, and the developer makes changes and creates v3. Once v3 is tested, it would be then pulled into Production.



Providers

Few providers provide the container registry services, and they are:

- **Docker Hub**
- **Azure ACR (Azure Container Registry)**
- **AWS ECR (Elastic Container Registry)**
- **Github Container Registry**
- **Google Container Registry**

	Amazon ECR	Docker Hub	GitHub Container Registry	Azure Container Registry (ACR)
Public Repository	No	YES	YES	No
Private Repository	Yes	YES	YES	Yes

Pricing (Public Repository)		$0	$0	$0
Pricing (Private Repository)	$	$$$	$$	
	Storage: $0.10 per GB, Data Transfer: $0.09 per GB	>= $7 per user/month	Storage: $0.25 per per GB, Outgoing Data Transfer: $0.50 per GB	Storage: $0.09 per GB
Authentication	AWS IAM	Password or Access Token	Personal Access Token (PAT)	PAT
MFA for Image Push/Pull	Yes	NO	NO	NO
SLA Availability	99.9%	N/A	N/A	99.9%
General Available	YES	YES	Beta	YES
Immutable Images	YES	NO	NO	YES
Image Scanning	YES	YES (paid plans only)	NO	YES
Regions	Choose between one of 25 regions worldwide	Not Known	Not Known	33 regions
Rate Limits	Pull: 1,000 per second, Push: 10 per second	Pull: 100/200 (Free Plan), unlimited (Paid Plan)	n/a	Pull: 1,000 per second, Push: 100 per second

ACR Service Tiers

ACR is available in 3 service tiers, also called SKUs.

1. **Basic** – Cost Optimized for developers
2. **Standard** – All features of Basic plus increased storage and image throughput. For Production
3. **Premium** – highest amount of storage and concurrent operations. It also includes geo-replication, content trust, and private link

ACR Roles

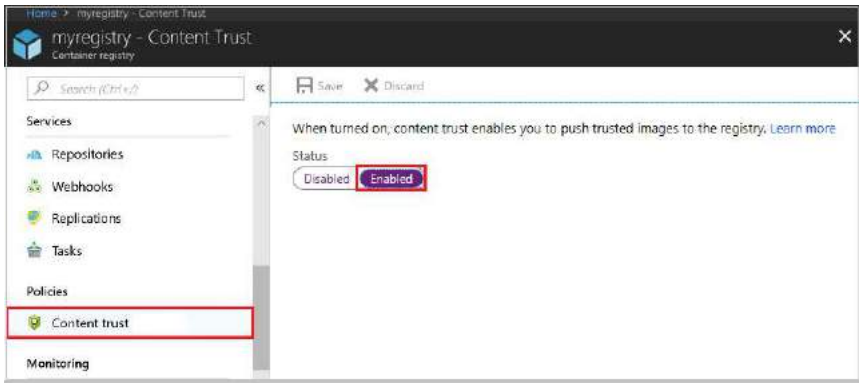
Role/Permission	Create/Delete ACR	Push	Pull	Signature Signing
Owner	X	X	X	
Contributor	X	X	X	
Reader			X	
AcrPush		X	X	
AcrPull			X	
AcrImageSigner				X

FAQs

1. **Can we change Service tiers?** –
   Yes

2. **What is geo-replication?**
   With this feature, a replica of the ACR will be created for DR purposes and local use.

3. **How can we secure the images in ACR?**
   There is a concept called CONTENT TRUST. With this, images will be signed with certificates. To enable this feature, enable registry content trust. It is available under **Policies -> Content Trust -> Enabled and then save.**



Azure Container Instance (ACI)

- Containerization is the buzzword today. Instead of spinning Physical servers and installing all the dependencies, and installing the application, we can create a container containing all the required dependencies.
- We then package and create an image and deploy it into a container.
- **Docker** is one of the platforms where we can run these containers in the Open source world. Azure has two solutions. One of those is the ACI.
- ACI is a great solution in scenarios where we need to run isolated containers. Examples are simple applications, task automation, and build jobs.
- The drawback of ACI is that it cannot be used for full orchestration like multiple containers, auto-scaling, and coordinated application upgrades. Please consider AKS for such scenarios, which is the other offering from Azure.
- In simple terms, for Production, use **AKS (Azure Kubernetes Service)**, and for simple and isolated containers, use ACI.
- One of the other best use cases for ACI is where we have production issues, and we need to troubleshoot AKS, ACI comes to our rescue where we deploy the trouble-making container in ACI and try to debug.

Advantages of ACI

- *Fast Startup times*
- *Container access*
- *Custom Sizes*
- *Persistent Storage* – We do this by mounting Azure file shares.
- *Virtual Network deployment* – When deployed in a Vnet, ACI can securely communicate with other resources in the Vnet.

FAQs

1. **What are probes in ACI?**
    - You can configure the liveness probe. We check the liveness probe to see if the container is healthy. If the container is not healthy, we need to restart. There are common scenarios when containers run for a long time.
    - You can configure the readiness probe. Here we might have a scenario where the container (maybe DB for the backend) is just coming up. We run the readiness probe and send requests to the container only if the probe succeeds.

2. **How can we monitor ACI?**
   We use Azure Monitor. Here are the available metrics at this time.
    - CPU Usage measured in millicuries (One millicore is 1/1000th of a CPU core)
    - Memory Usage in bytes
    - Network bytes received per second.
    - Network bytes transmitted per second

3. **What are container groups?**
    - Similar to AKS for orchestration, we can use container groups to combine and manage containers. They get scheduled on the same host machine.
    - The concept is similar to pods in Kubernetes. The use case for this is in scenarios where we want to divide a single functional task into a smaller number of container images. An example is a front-end container and a back-end container.
    - The front end might serve a web application, with the back end running a service to retrieve data.

Azure Kubernetes Service (AKS)

What is Containerization?

- In the traditional computing system, we had to install an Operating system and install all dependencies for an application to work. Only a single OS could be installed.
- Then came Virtualization where we could install multiple OS by introducing another layer between the hardware and the OS and this was called Virtualization. So only physical machines appeared as multiple systems.
- Then came a lightweight alternative to virtualization, which was called Containerization. This removed the drawback of having a full machine, and this had only the necessary components.
- Containers will encapsulate an application with its operating system. This would contain all the dependencies that were needed for an application to run. So we take the container and run it on any operating system, and it will run.
- Some of the containerization options are Docker, which is the most popular and sometimes equated to containers. But there are others like **LXC/LXD, ContainerD, Rocket**.

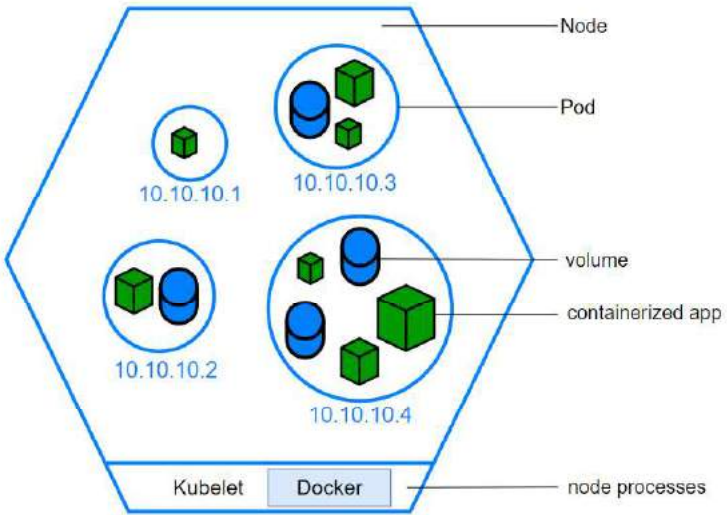
Orchestration

- Orchestration is the system that is used to manage the deployment of containers. We use Orchestrators as tools to achieve this. Some of the performed activities are automating the maintenance of those applications, replacing failed containers automatically, and managing the rollout of updates and reconfigurations of those containers during their lifecycle.
- The popular tools are *Docker Swarm by Docker, Nomad by Hashicorp, Flocker, and Kubernetes.*
- Kubernetes, also stylized as K8s, is an open-source container orchestration system. It is used for automating computer application deployment, scaling, and management. It was originally designed by Google and influenced by Google's Borg System and is now maintained by the Cloud Native Computing Foundation. It is a cluster management software for Docker containers mainly but supports others also.

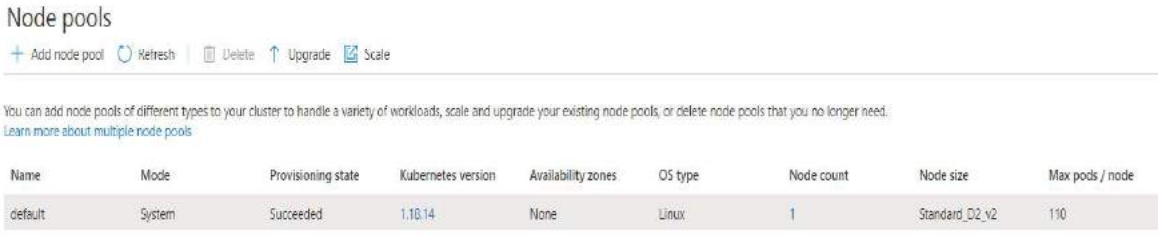
AKS

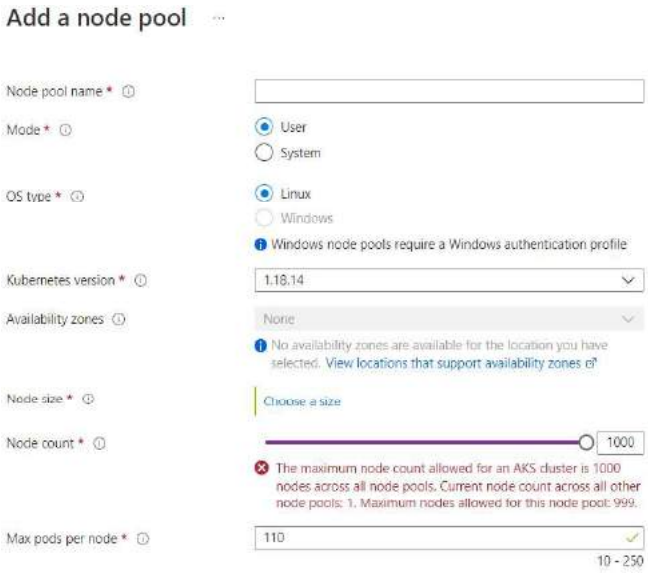
Kubernetes has become very popular, and many cloud service providers offer a Kubernetes-based platform or infrastructure as a *PaaS or IaaS offering. Google has GKE (Google Kubernetes Engine), AWS has EKS (Elastic Kubernetes Service), and Azure has AKS (Azure Kubernetes Service)*

Components of AKS



1. **The Cluster**
   - The Cluster contains 2 components
     - Control Plane – this consists of kube-apiserver, etcd, kube-scheduler and kube-controller-manager
     - Nodes that run the applications
2. **Persistent Volumes**
   - Since the nodes are added and removed on-demand and the storage associated with it is temporary, we need to create storage outside of the cluster. Hence we create persistent volumes.
3. **Node**
   - We create Node pools in Kubernetes (as shown below). Here we choose a VM size, and that will be the unit size of the nodes within the pool.
   - We can add node pools as needed. The first node pool created is the **system node** pool which hosts critical system pods like coreDNS and tunnel front.
   - We then add user node pools for application support and create different pools based on the application requirements.
   - Pods will be created within the nodes, and the max pod setting is configured at the node pool level.





4. Containers

- We store our code that is going to be run inside containers. There are readily available pre-built containers stored in container repositories or we can create our own containers.
- One or more programs can be run from the containers

5. Pods

- Nodes create Pods, and kubernetes use Pods to run instances. Usually, only one container is run within a pod, but multiple containers could run in a pod if there was a requirement from the application.
- We scale based on pods. When we can scale, we simply use pod replicas. A new pod will be spun up in another node, and we now have an additional pod. Same way, we can remove the pods to scale down.

6. Deployments

- We don't launch pods directly. Instead, we create deployments.
- A deployment will state how many replicas should run and the system manages that.

Sample Deployment yaml file

```
apiVersion : apps/v1
kind: Deployment
metadata:
  name: wl-app
spec:
  replicas: 1
  selector:
    matchLabels:
      app: wl-app
  template:
    metadata:
      labels:
        app: wl-app
    spec:
      containers:
        - name: wl-app
          image: wl66293099.azurecr.io/wl-app
          ports:
          - containerPort: 3000
```

7. Ingress

- By default, Kubernetes provides isolation between pods and the outside world. If you want to communicate with the service running in the pods, you need to open the communication. This is called Ingress.
- You can achieve this communication in several ways. The most common ways are Ingress controller or a load balancer. Please see the sample service.yaml file which creates an external load balancer. We get the IP of this service and connect.

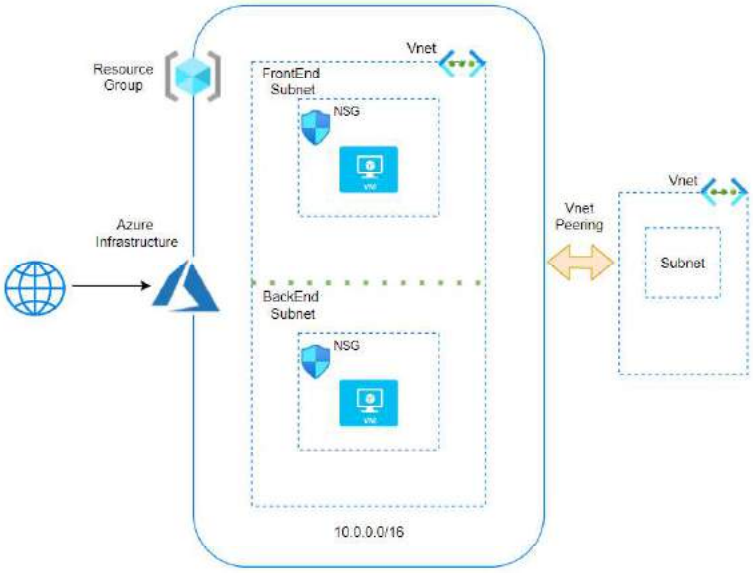
```
apiVersion: v1
kind: Service
metadata:
    service.beta.kubernetes.io
    name: wl-app
spec:
    type: LoadBalancer
    ports:
    - port: 3000
    selector:
        app: wl-app
```

Azure Virtual Network

A **Vnet** is the fundamental building block for a private network in Azure. Vnets allow azure resources like VMs to communicate securely to each other, to the internet and on-premises networks. A **Vnet** is the representation of our own network in the cloud. We can logically isolate resources within our Vnet.

Benefits of Vnet

- **Isolation** – As discussed, the components of a Vnet are isolated. We can connect to other Vnets or On Premises with Vnet Peering or VPN or Express route
- Access to the public network
- Access to VMs within the Vnet
- **Name resolution** – We can resolve to other components in the Vnet and address them
- **Security** – We can secure the components at various levels in the Vnet
- Connectivity



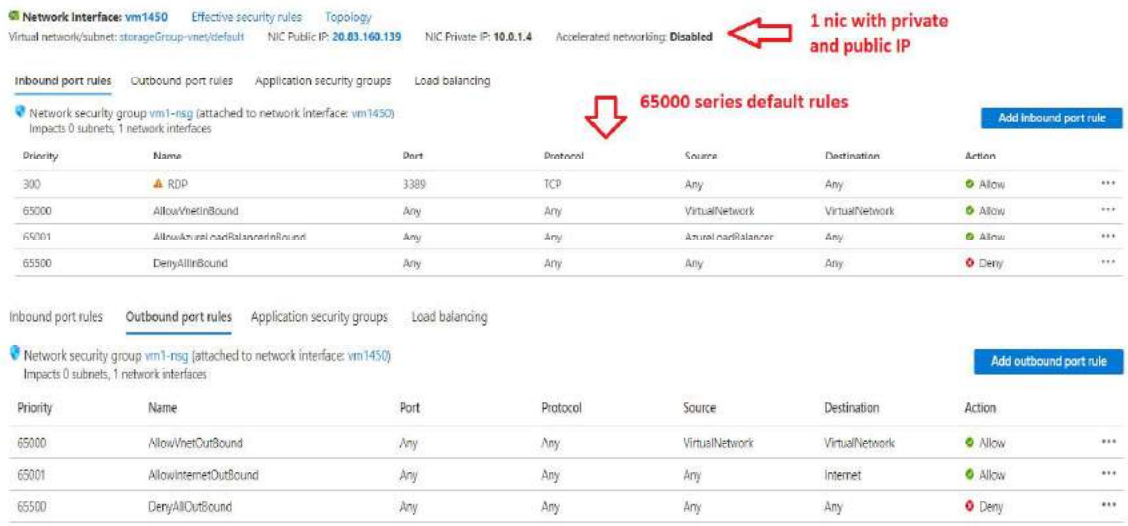
Components of Vnets

- **IP addresses**
  - **Public and private IP addresses**
    - The Vnets are configured with a range of IP addresses. The Notation is in CIDR.
    - By default, Private IP addresses are assigned to the resources with which communication takes place between the resources
    - Optionally, Public IP address can be assigned to the resources
    - Please note that we will pay for Public IPs if they are not assigned. This is to conserve Public Ips

- **Subnets**
  - A Subnet is a subcomponent of Vnet. All resources must exist in a subnet. A default subnet is created when a Vnet is created.
  - Access can be restricted at a subnet level also
  - Let's say we have 2 tiers in an application called Front end and Back end. We can create 2 subnets and configure access in such a way that internet traffic will flow to the front end subnet and from there to the back end subnet.

- **NIC - Network interface card**
  - A NIC is the networking component which allows traffic flow. A single NIC will contain the public and private address.

- **NSG - Network security group**
  - These are the rules that are assigned to allow traffic to flow. The NSG can be assigned at a NIC level or a subnet level. It is recommended to apply at any one level only.
  - If there is no NSG, then traffic will be allowed in and out
  - We set inbound and outbound rules
  - **Priority** – All rules are assigned a priority and the lowest number is taken first. If rule 100 says allow and 101 says deny, then the result is allow.
  - **Default Security rules** – There are 6 default rules that can neither be removed or modified.



FAQs

1) **What is Vnet Peering?**

   Vnet Peering allows two Vnets either in the same region *(Default Vnet Peering) or Globally (Global Vnet Peering)*

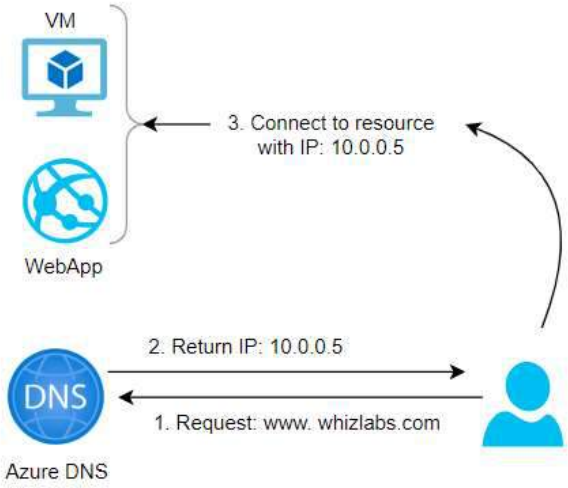
2) **What are the pre-checks for Vnet Peering?**
    a. Peering is non-transitive. If Vnet A is peered with Vnet B and Vnet B with peered with Vnet C then it does not mean that Vnet A and Vnet C are connected
    b. The Address ranges cannot overlap between the Vnets
    c. When peered, adding or deleting address range is disabled. If we need to add address range, we need to delete the peering and add the address range and then add peering again.

Azure DNS

What is DNS?

Think of the phone directory that is used at home. It is difficult to remember a string of numbers and hence the phone directory will list the phone numbers with names of persons/businesses.

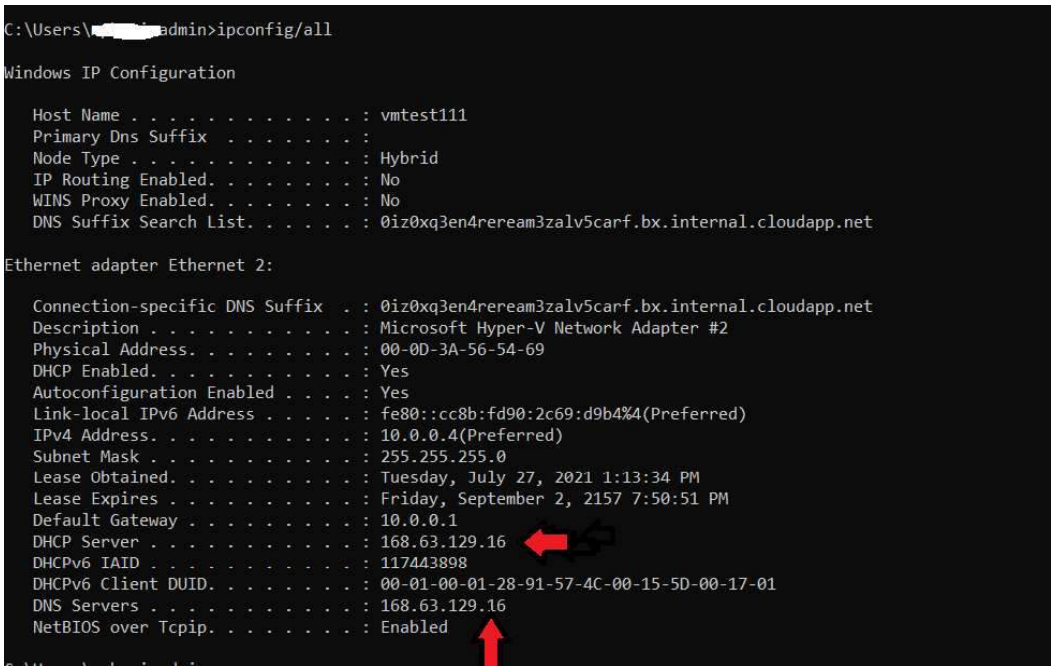
- Coming back to the IT world, computers communicate with IP addresses. The DNS (Domain naming system) is a friendly name given to the computer.
- For example, a web server has an IP address of **53.102.94.86.** Instead of using the IP Address, we assign a host name as web1. In a domain, the **FQDN (Fully qualified domain name) will be web1.demystify.com.**
- This is facilitated by DNS Servers which are setup in a hierarchy. At the top most level, we have the ROOT and under the root, we have the top level domains (TLD) examples of which are **.ORG, .COM, .NET, .IN etc.,**
- In addition to this, we have domain registrars where we purchase a domain name.
- Examples are **Godaddy, Namecheap and Amazon too via Route53**. When a user tries to connect to a server demystify.com, the DNS resolves this to the IP address by going to the **ROOT** and then to the **.COM server.**



- DNS works with a concept of Zones. We can set up Private or Public zones. Public zones are used when we want the internet to be able to resolve our names.
- However when we want to enable internal communication, we create private zones.
- Please note that zones can also be configured with a "**Split-horizon**" view which allows a private and public DNS zone to share a name.

FAQ

1) **What is IP 168.63.129.16?**
   This is actually called a Wire Server and has an IP address of 168.63.129.16. and it facilitates communication between Azure resources. It also serves as a DNS and DHCP server by default. Please ensure that this IP is not blocked.



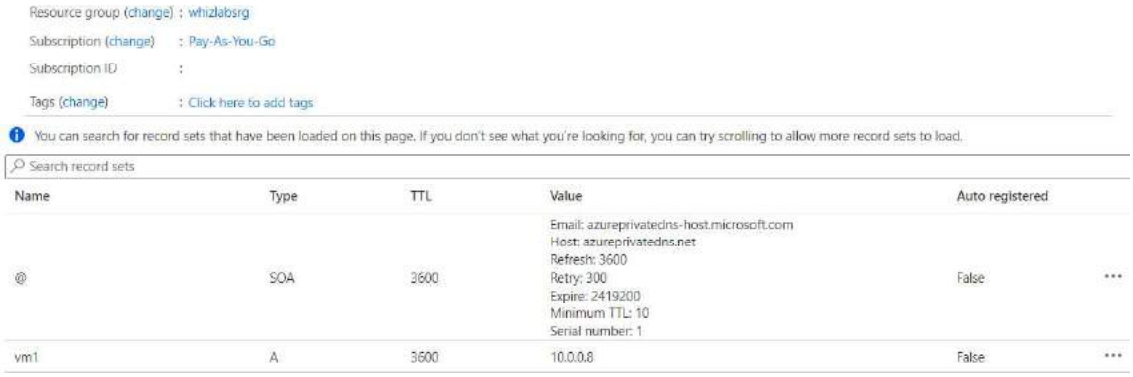
Connection-specific DNS Suffix . : lhlv032okq5e3g5zezobyk5bwf.bx.internal.cloudapp.net

Description . . . . . : Microsoft Hyper-V Network Adapter #2
Physical Address. . . . . : 00-0D-3A-8E-15-4C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7dbd:c33b:1ab:8e7f%7(Preferred)
IPv4 Address. . . . . : 10.0.1.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, March 13, 2021 7:06:42 PM
Lease Expires . . . . . : Wednesday, April 20, 2157 9:38:31 AM
Default Gateway . . . . . : 10.0.1.1
*DHCP Server . . . . . : **168.63.129.16***
DHCPv6 IAID . . . . . : 117443898
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-DE-C5-9A-00-15-5D-00-04-01
*DNS Servers . . . . . : **168.63.129.16***
NetBIOS over Tcpip. . . . . : Enabled

2) **Can I buy my domain from Azure?**
   No, Azure is not a domain registrar. You need to buy from a domain registrar and you can create a zone in azure and add the records for DNS resolution.
3) **How do we configure VMs to use private zones?**
   We can configure auto registration and for Vnet that we link with the Virtual Network Link on the DNS Zone, the DNS registration will be done automatically when the VM is created.

4) **How do I use my custom website?**

We need to create a public zone and add an alias record. Once verified with the registrar, we can start using our custom name.



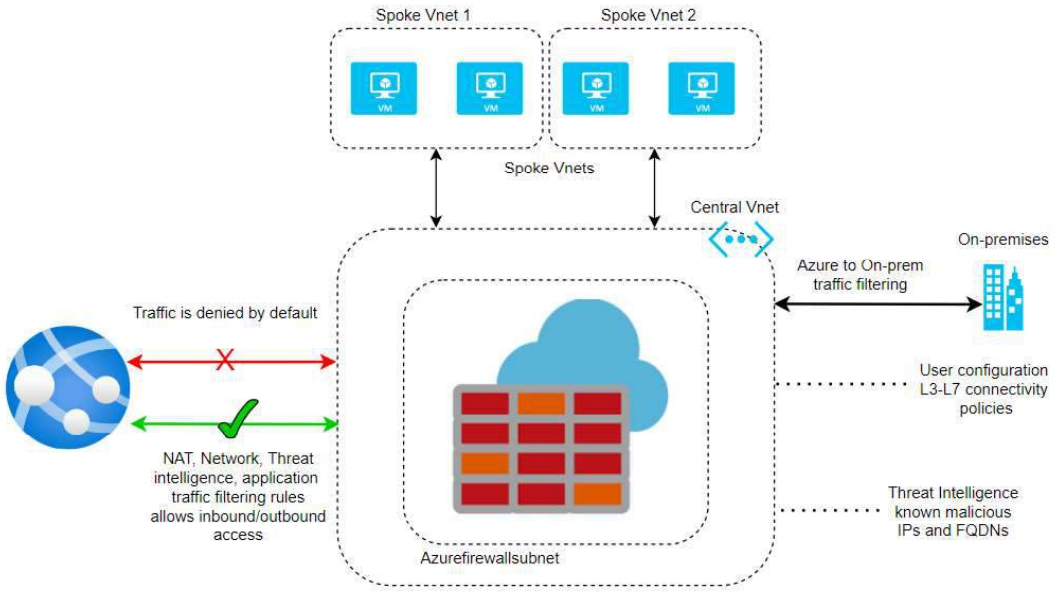
Azure Firewall

What is a Firewall?

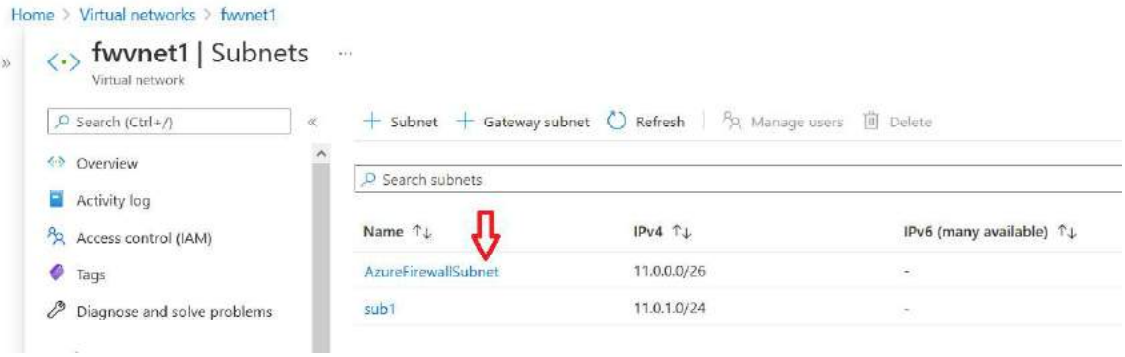
A Firewall is a security device for the network that monitors both incoming and outgoing traffic. Based on a set of security rules, it will either allow or deny the traffic. It acts as a barrier between our network and traffic from external sources like the internet. The objective is to block malicious traffic which include hackers and viruses.

Azure Firewall

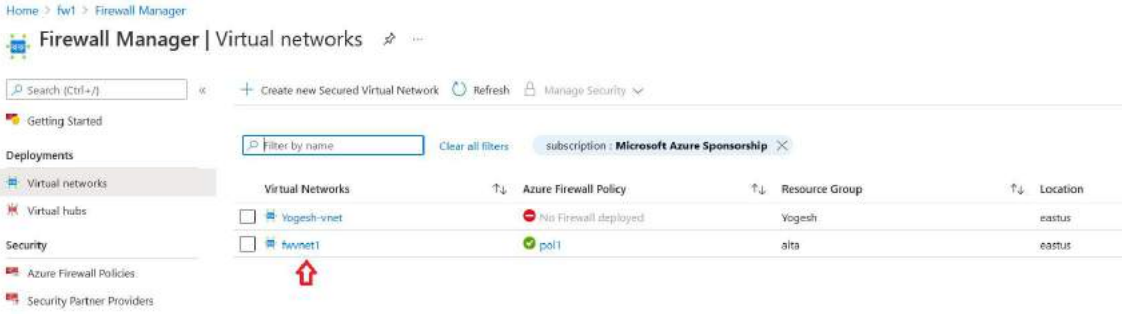
- Azure Firewall is a **network virtual appliance (NVA)** which is a managed network security device on the cloud.
- The function is to protect our network resources on the cloud. There are two types of firewalls and they are classified as either Stateful or Stateless. Let's say that you allow a certain incoming traffic *(say port 80).*
- When the same traffic returns, it is automatically allowed if it is stateless. On the other hand, Stateful traffic will need a specific rule for the outgoing traffic also, else the traffic will be blocked.
- Azure Firewall is a fully stateful firewall. So, we need to allow both incoming as well as outgoing traffic.
- Azure Firewall has built-in high availability and is highly scalable. We can create, enforce, and log application and network connectivity policies across subscriptions and virtual networks from a central location called **Firewall Manager.**
- We need to set up a static public IP address for the virtual network resources allowing outside firewalls to identify traffic originating from the virtual network. It is fully integrated with **Azure Monitor** for logging and analytics.
- A typical setup for the firewall is done via a hub and spoke model where the Vnet which hosts the firewall will act as a hub and the other Vnets will act as a spoke.
- The On premises and Internet is also connected to **Azure Firewall.** In this way, all traffic will enter via the firewall and the rules setup via the policies will then allow or deny the traffic.
- Please note the subnet that hosts the firewall must be named as Azurefirewallsubnet else it will not function



- Please see below the subnet created for the Azure firewall named as **AzureFirewallSubnet.**



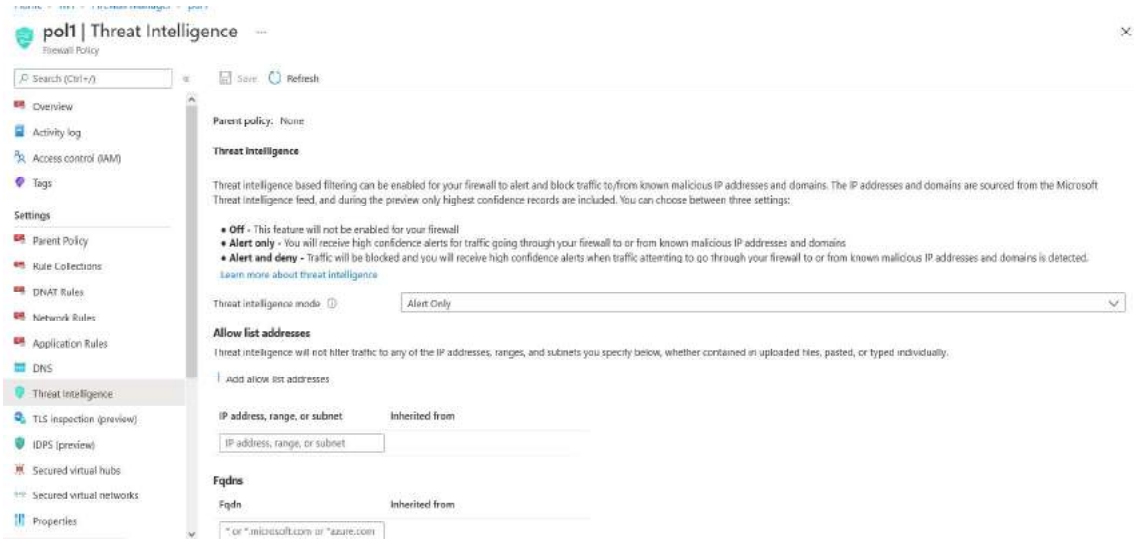
- As discussed, the rules are set up in a central location using the Firewall Manager. You can see the pol1 being assigned to **fwvnet1 Virtual Networks**. We can assign the same policy to other networks and it is easier to manage centrally.



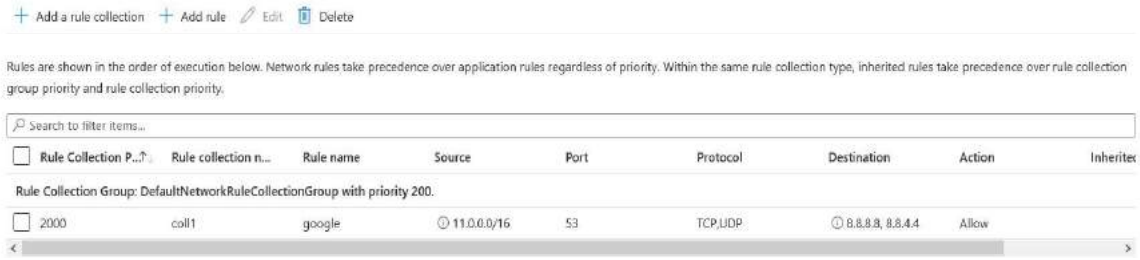
- A Policy consists of rule collections which in turn contains individual rules. Here we specify if the rule is to allow or deny.

- We assign a priority from **0 to 65535** and the lowest number takes the priority while processing the rules.
- We could place the rule collection within a group called the rule collection group. Also, the rule is available as a tab called Network rules on the main panel.
- We specify the source type as either an IP address or IP Group. We can give a range of IP addresses for Source and Destination. We can give ***** to indicate all.
- We can specify Protocol and Port numbers. In the example below, we have given Google a DNS server with IP of **8.8.8.8** and port of **53** which will allow DNS resolution.

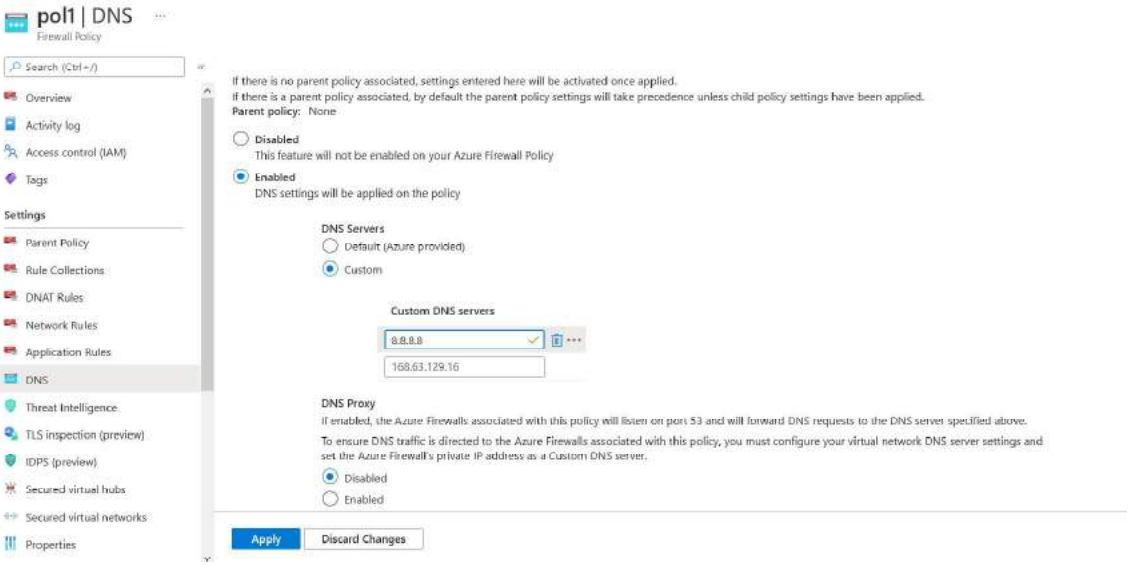
- We can optionally enable intelligence-based filtering called Threat Intelligence and the mode can be set to OFF/Alert only or Alert and deny. Microsoft threat intelligence feed provides a list of IP addresses and domains and these recorded are included as rules to allow or deny



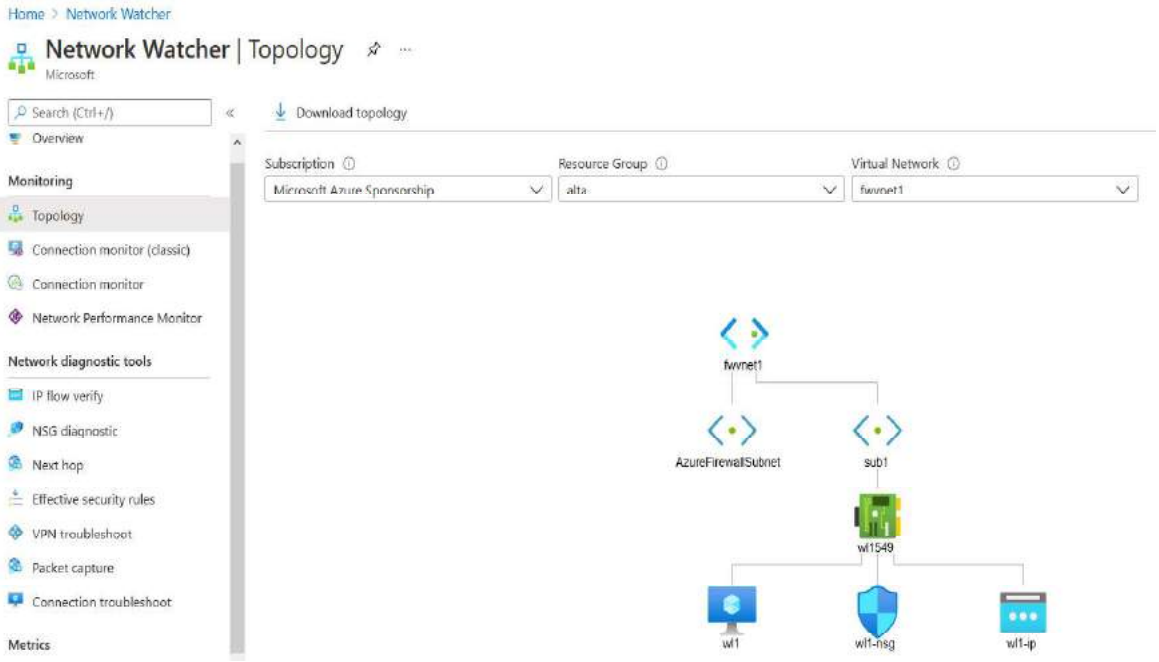
This is the Network Rule tab which lists the rules.



We can also set up DNS servers for DNS resolution on the DNS tab.

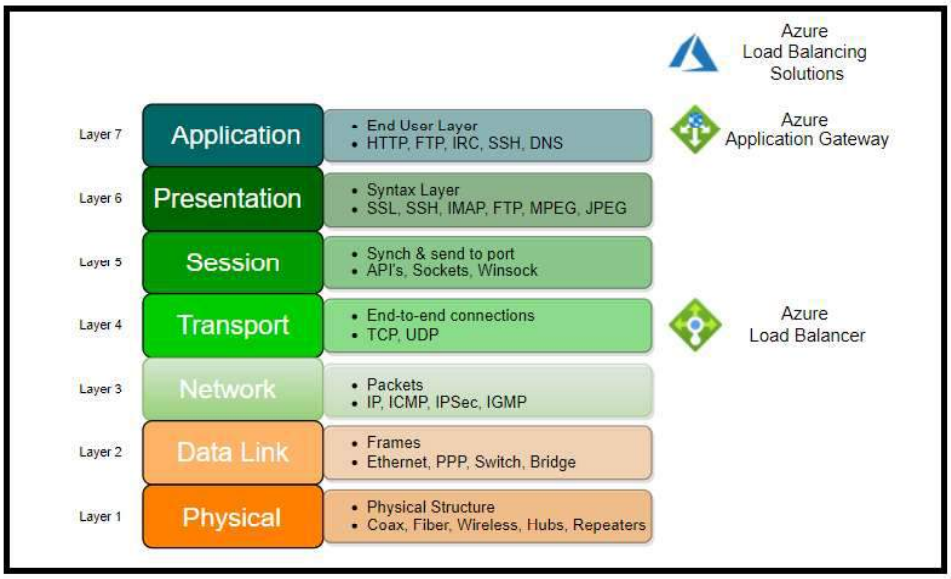


Finally, we can see the topology of the Vnet and the firewall subnet on the Network watcher blade under the Topology tab.

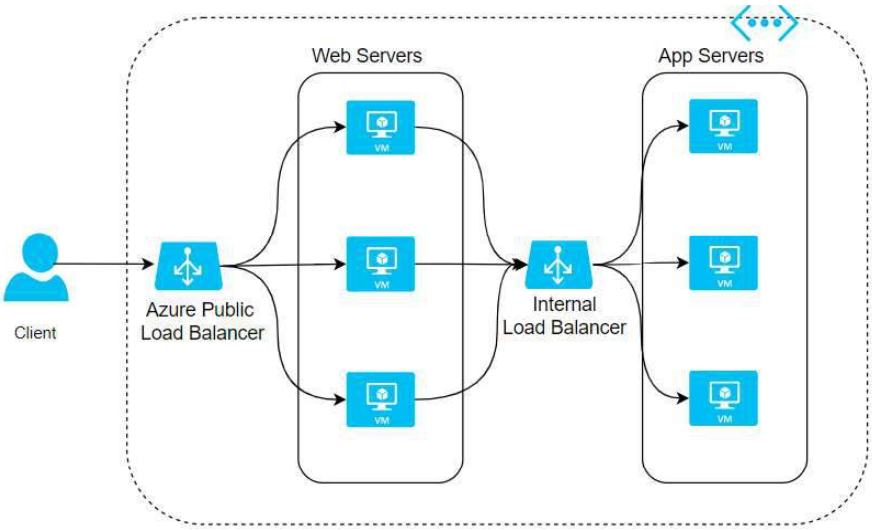


Azure Load Balancer

- Azure provides load balancing at **Layer 7** which is the application layer via Azure Application Gateway. This is typically http traffic.



- Azure also provides load balancing at Layer 4 which is a transport layer consisting of **TCP and UDP** protocols. This is the Azure Load Balancer.
- We could use the Azure Load balancer for both public facing as well as internal application. The load balancer is set up with a backend pool which distributes traffic to a set of VMs or VM Scale sets.



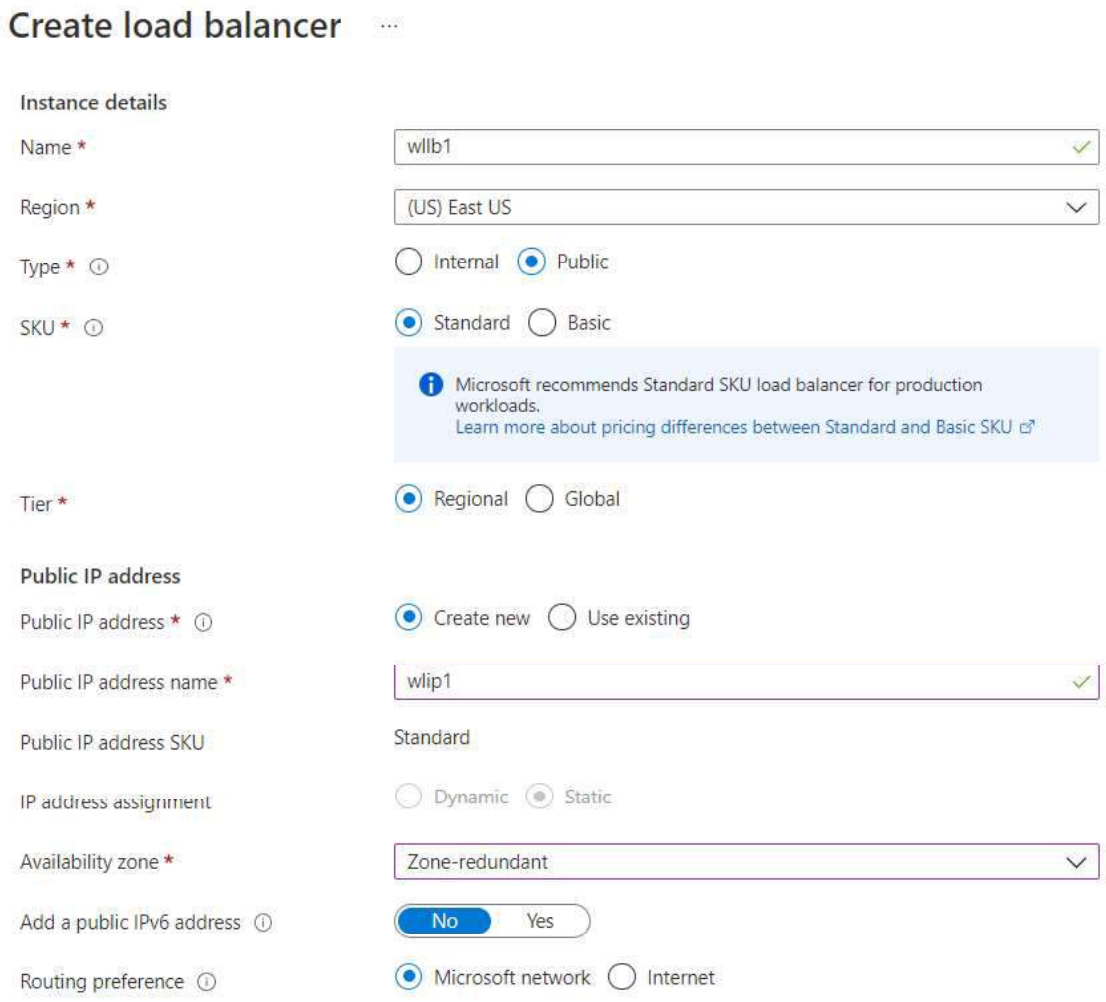
Here are the steps to create a load balancer:

Step 1: Create Load Balancer

We create a load balancer with the following options:

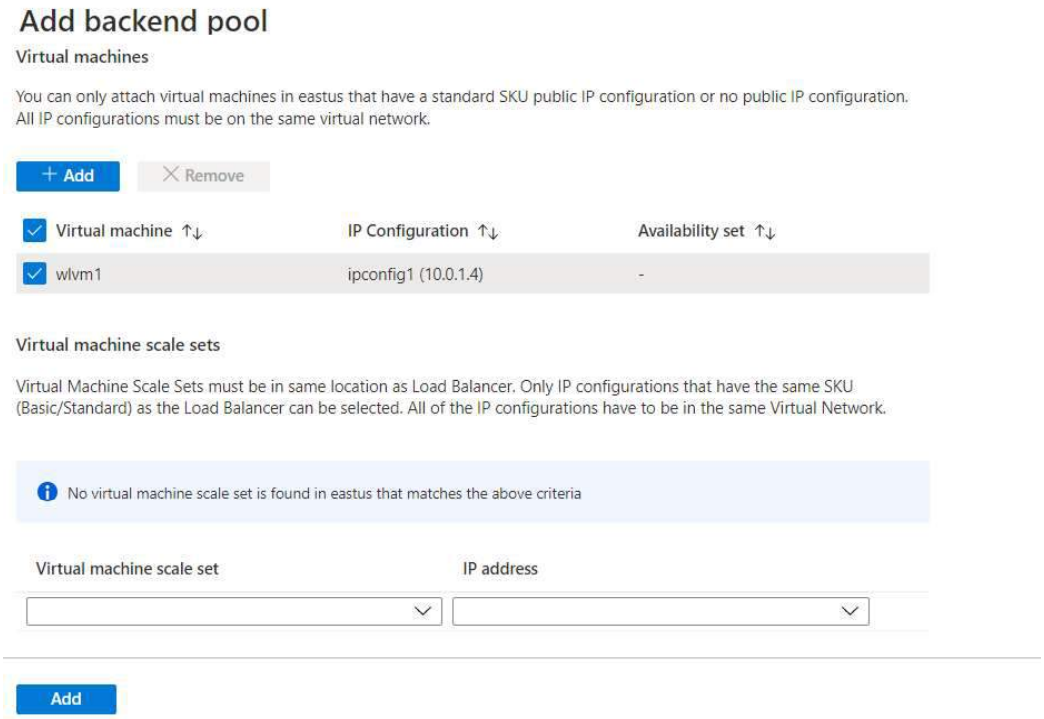
- Name for the load balancer

- Internal or Public load balancing
- SKU type could be Standard or Basic. Since Basic does not have an SLA, Standard SKU type is recommended for Production workload which has SLA of **99.99%.** *Standard SKU* comes with many more additional / better features than Basic SKU like https.
- **Regional or Global** – This is a new feature and is available for Public Load balancers



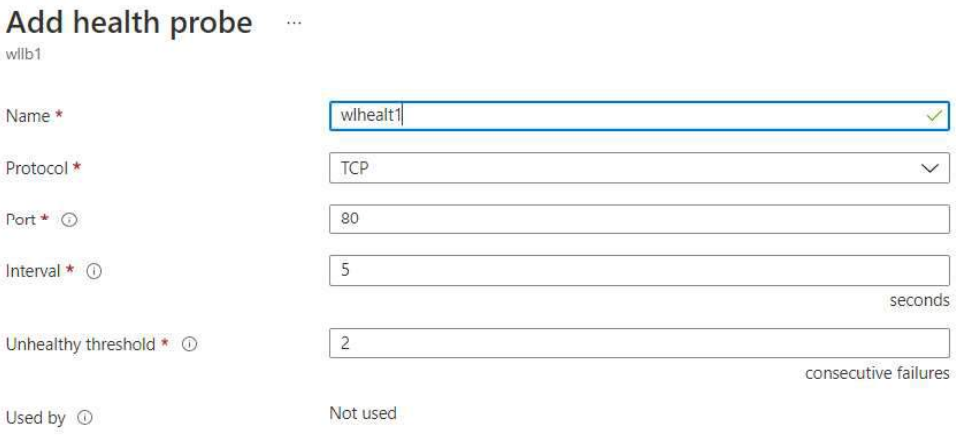
Step 2: Create Backend pool

- We create a backend pool where we attach VMs or VMSS
- VMs/ VMSS have to be in the same location.
- We could add multiple backend pools



Step 3: Add Health Probe

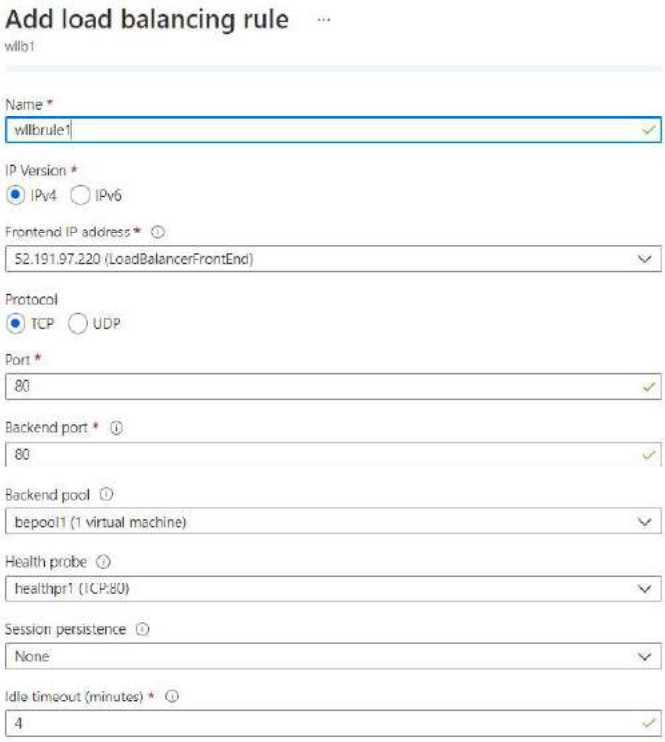
- We need to add a health probe
- We can configure **TCP/HTTP/HTTPS** as protocol
- We add a port number
- We add an interval and unhealthy threshold which is the interval for checking where the probe passes a health check. The unhealthy threshold is the number of times a probe is allowed to fail consecutively after which the instance will be marked as unhealthy and traffic routing will be stopped.



Step 4: Add Load Balancing rule

- We create a load balancing rule
- We specify frontend IP address and Protocol (TCP or UDP) and Port
- We specify the Backend port and pool

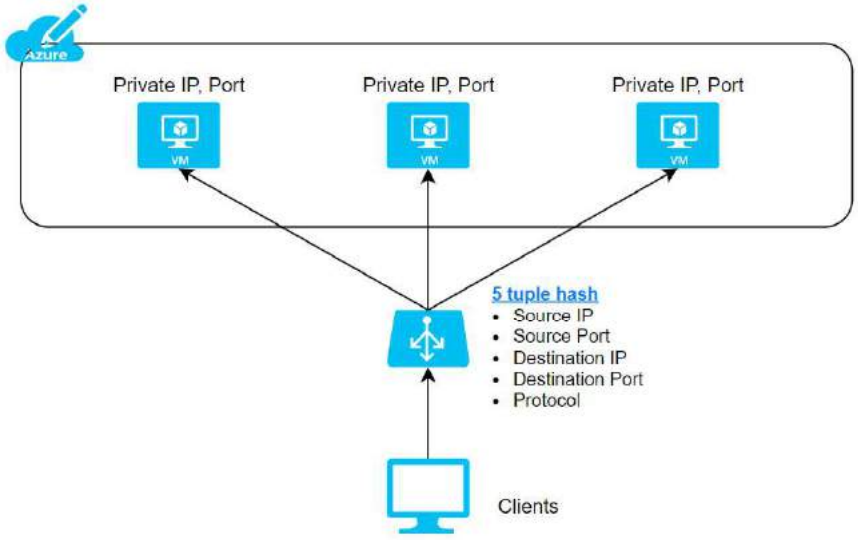
- We specify health probe
- We can also specify session persistence. If this option is enabled, the traffic will be routed to the same VM.



Azure Load Balancer can also be configured to use as follows to map traffic to the available servers:

- **2 tuple (Source IP, Destination IP)**
- **3 tuple (Source IP, Destination IP, Protocol)**
- **5 tuple (Source IP, Source Port, Destination IP, Destination Port, Protocol)**

Please see how the traffic is routed based on the 5 tuples.



Azure Application Gateway

One of the main benefits of the Cloud is elasticity on-demand.

In a traditional datacenter, if there is a peak load requirement of 100 cores from 10-11 am when users login, the machines will always need to have the capacity of 100 cores.

However, in the cloud environment, we will have a single VM with 50 cores at all times and add another VM with 50 cores between 10-11 AM alone. This has reduced consumption by almost 50%.

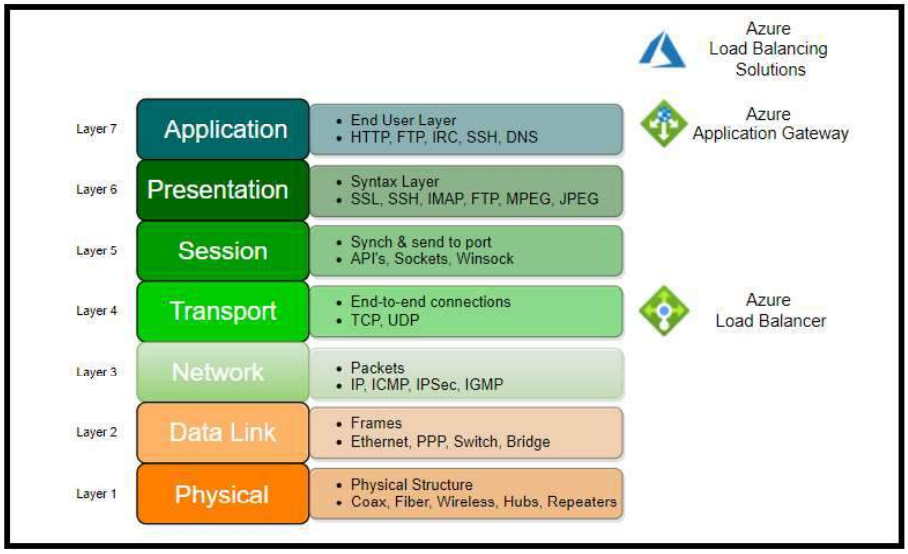
But how do we now distribute the load between the two VMs?

The solution is Load Balancing.

Load balancing can be done at 2 layers in the OSI model. One is at Layer 4 where we will use the Azure load balancer. Here a combination of source and target ip and TCP/UDP Protocol will be used to achieve routing.

The other routing type is at Layer 7, which is the Azure Application gateway. Here the application gateway uses a front-end IP address which is resolved from FQDN via DNS. It has an optional WAF (Web application firewall).

OSI LAYER and the load balancing options within Azure

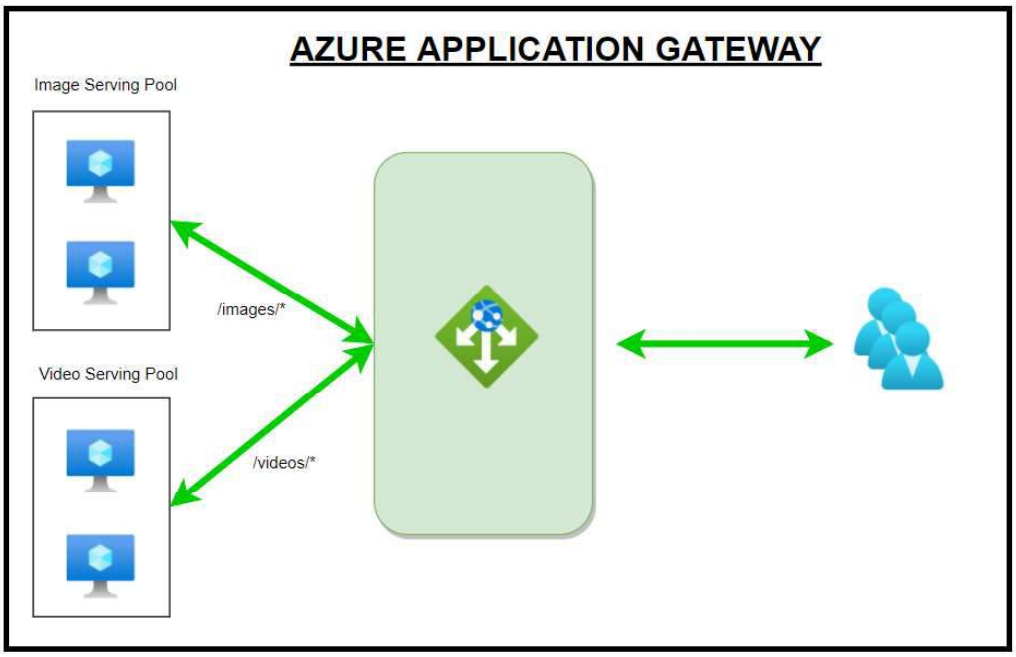


How does the Application gateway work?

Step 1: User sends a request to a website with **FQDN (fully qualified domain name)** – for example, https://demystify.com/videos. The query will be sent to a DNS server, and it will return the IP address.

Step 2: The application gateway will be configured with a listener, a logical entity checking for connection requests. The listener is configured with a front-end IP address, protocol, and port number for connection requests.

Step 3: The application gateway also has a backend Pool/s. The backend pools could be VMs or **VMSS (VM Scale Sets)** or external servers, or Azure App servers. Based on routing rules set up, the traffic will be routed to the appropriate backend servers.



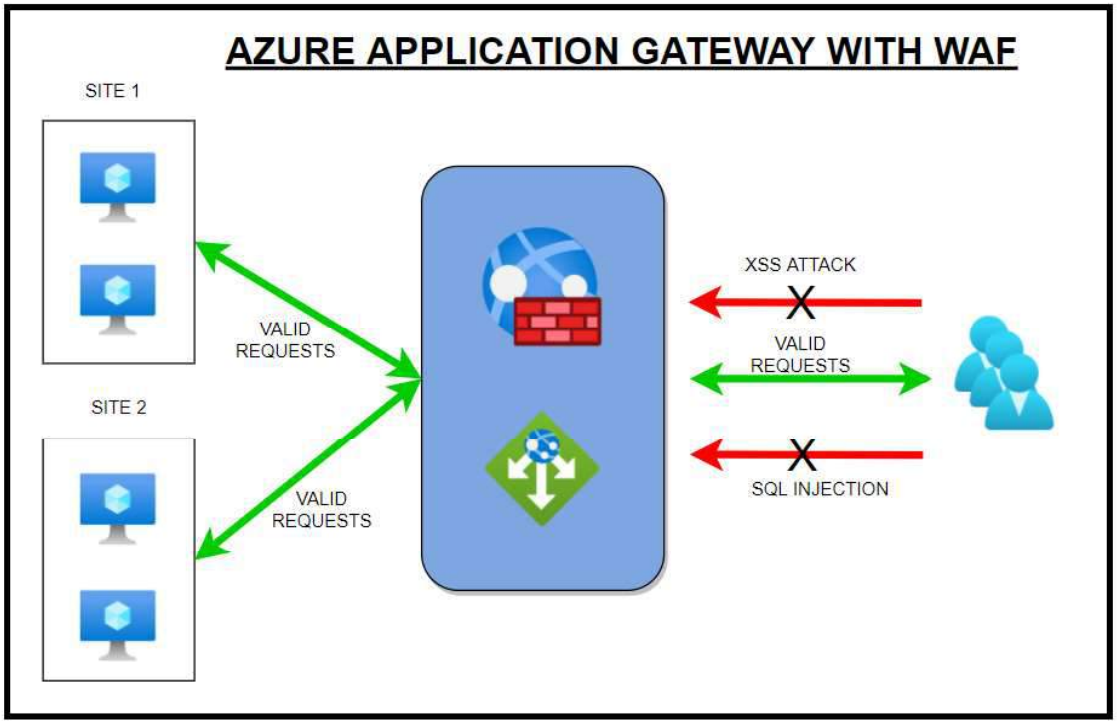
In the above example, you can see the routing rules being processed with url based routing. So when the users type the url https://demystify.com/videos, the gateway sees the videos in the url and sends the traffic to the Video Serving Pool.

Application Gateway with WAF

There is an optional feature WAF that can be additionally added to the application gateway. WAF is based on **Core Rule Set (CRS).**

We need to set up a WAF Policy that has rules. There are two types of rules. One is Managed rule sets which Azure preconfigures. The other is custom rules. Some of the features of WAF are

- Some of the features that WAF provides are preventing SQL injection**/ XSS/ http** protocol violations.
- It also protects against crawlers and scanners. We also can allow or block traffic coming in from certain countries/regions in preview, and it is called **Geo-filter traffic.**
- WAF can be set up in two modes which are Detection or Prevention.
- When WAF is added, the traffic will be evaluated before Step 3 above against the WAF rules.
- If violating traffic is found in Detection mode, the warning will be issued, and traffic continues to flow. In Prevention mode, the traffic will be blocked.


AZURE APPLICATION GATEWAY WITH WAF
SITE 1
SITE 2
VALID
REQUESTS
VALID
REQUESTS
XSS ATTACK
VALID
REQUESTS
SQL INJECTION

Azure Traffic Manager

Azure provides the following services for Delivery.

- *CDN*
- *Front Door*
- *Traffic Manager*
- *Application Gateway*
- *Load Balancer*

While Load Balancers and Application Gateways operate at **Layer 4 and 7,** Traffic Manager operates at a DNS level.

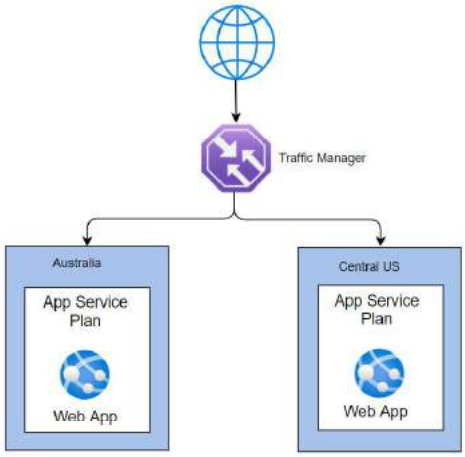
This service will distribute traffic to *public-facing azure services at a global level.* The public endpoints provided are having high availability and quick response.

We can use Traffic Manager to route traffic to regional application gateways at a global level, which could have a load balancer setup for multiple VMs at a database tier utilizing all the services.

Here are some more scenarios:
Application Gateway - to load balance between your servers in a region at the application layer.

Front Door - optimize the global routing of your web traffic and optimize top-tier end-user performance and reliability through quick global failover.

Load Balancer - Network Layer Load Balancing



How does a Traffic Manager work?

The Traffic Manager uses DNS for resolution. It uses this to find the name server. Then it locates the endpoints (which are not disabled) and routes the traffic based on the routing methods specified.

Routing Methods:

Here are the routing methods which we can configure:

Routing Method	Scenario
Priority	*When we have several endpoints, and we want to use one location preferentially, we can use this method having a primary service endpoint for all traffic.* *We can configure one or several multiple backup endpoints in case the primary is unavailable.*
Weighted	*When we want to split and route traffic to different locations, we should use this method. We have to set weights to accomplish this.* *Let's say we want to route traffic equally, we set the weight of 1 and 1 to both the endpoints* *If we give weights of 1 and 2, then the ratio will be 33:66 and one-third of traffic will go to the first endpoint, and two-thirds of traffic will go to the second endpoint.*
Performance	*Let's say that we have 3 locations like Las Vegas, Houston, and Jersey City on 3 sides of the country. We would like end-users to use the "closest" endpoint for the lowest network latency.* *For example, users in New York should connect to Jersey City, which is the closest location. Then we should select this routing method for the lowest latency by choosing the closest endpoint.*
Geographic	*Let's say that there is a requirement that data from a country (Saudi Arabia) has a mandate that data should not cross borders with sovereignty laws.* *We can use this method to direct users to specific endpoints based on where their DNS queries originate from geographically.* *So if a user from this country tried to access it, he would be routed to the servers in his country only.*
Multivalue	*If there multiple servers and we wanted to select multiple servers to select any of the available servers, we can select MultiValue.* *When a query is received for this profile, all healthy endpoints are returned. We can limit the servers returned by setting a max value.*
Subnet	*Use this method to map sets of end-user IP address ranges to a specific endpoint. When a request is received, the endpoint returned will be mapped for that request's source IP address.*

FAQs

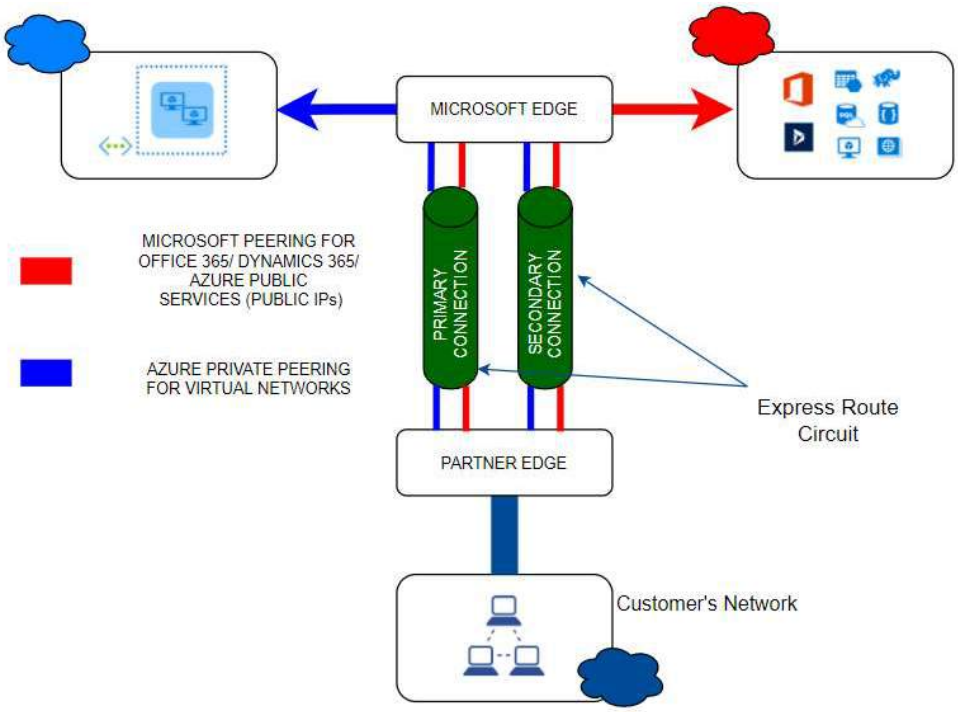
1. **What is the name of the website that will be created when we configure Traffic Manager?**
   Azure will always use azurewebsites.net as a suffix. We cannot change it

2. So how do we use our website like demystify.com?
   You need to create an alias in your DNS zone and point to the Traffic Manager.

Azure Express Route

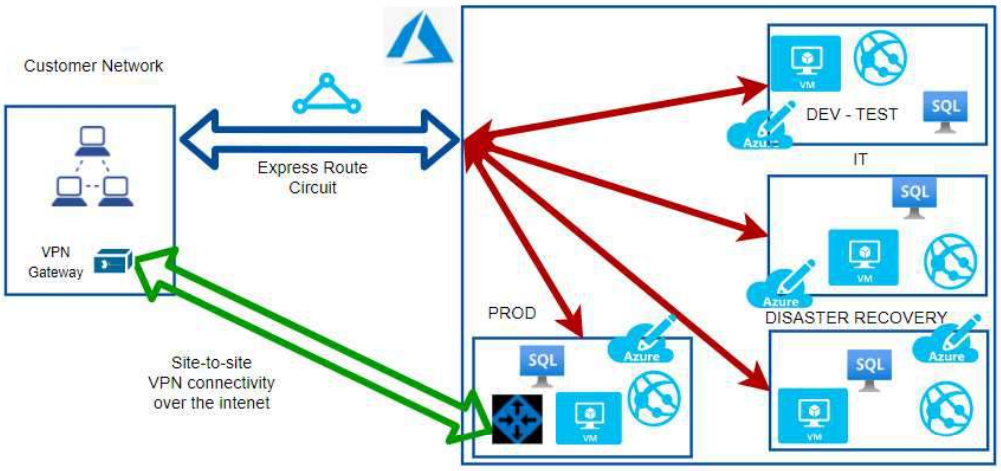
Connectivity to Azure

- There are several ways to connect to Azure. Broadly classifying them, we could either use the internet or have a direct connection.
- While connecting via the internet, we need to use a VPN to connect our infrastructure on premises with the cloud using a **VPN** gateway which encrypts our traffic by creating a tunnel.
- We could choose either a client-to-site VPN which is only one client system connected to the **cloud or site-to-site** VPN where we connect two sites.
- This setup depends on the public internet and we must secure and could have reliability issues.
- Hence it is better to use a dedicated connection between our infrastructure and the cloud with an **Express Route connectivity.**
- We need to locate a connectivity provider. There are several choices available based on location.
- For example, in India, we have *BSNL/AIRTEL/SIFY and in the USA, we have AT&T/ SPRINT/ VERIZON and many more.*



- Express Route connectivity allows us to connect to 2 Microsoft cloud services – **Microsoft Azure Services as well as Microsoft 365 services.**
- Also, we can see from the above diagram that there is an active-active redundant pair of cross connections setup for high availability. We can add further redundancy by adding up to 16 Express route connections.

- Express route has the following bandwidths to choose from based on our requirements:
- **50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps**
- If we have multiple subscriptions, we can connect all of them to a single Express route connection.
- You can have upto 10 Vnet connections on a standard Express route connection and upto 100 for Premium connection. However please note that all connections will share the same bandwidth.



We could even have a site-to-site VPN for adding redundancy. If there were issues with the Express route, we can failover to the S-2-S VPN.

FAQs

1) **If I have a 100 Mbps circuit, what is ingress and egress capacity?**
   You will have an incoming capacity of 100 Mbps and outgoing capacity of 100 Mbps.
   What is the routing protocol?
   Express route uses BGP (Border gateway protocol)
2) **What happens if there is any maintenance?**
   There won't be any impact. Express route uses an active-active setup and only the circuit will be maintained at a given time.
3) **So where does the connection land on the Azure cloud?**
   We connect to one of the Vnets in a subscription. We can connect upto 10 Vnets in each of the 10 subscriptions max. We need to go for Premium if we would like to add more.
4) **How do we plan for Disaster recovery?**
   Microsoft recommends 2 Express connectivity to avoid a single point of failure. We could also set up a Site-to-site VPN instead of a second circuit.

Azure VPN Gateway

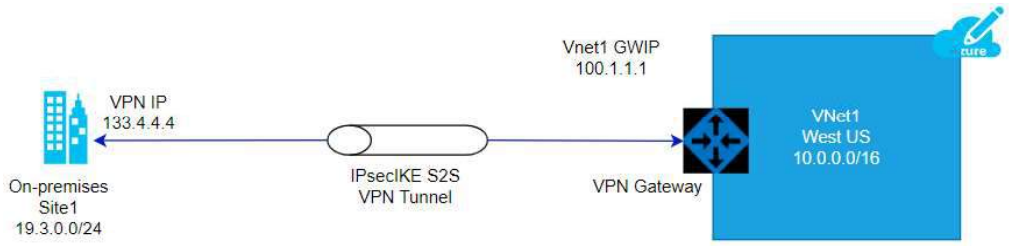
This is one of the methods that allows inter-site connectivity. Express route is the preferred connection as it has higher bandwidth and is in active-active mode. Smaller enterprises can choose VPN gateways or one could use VPN Gateway as a backup to Express route connectivity.

The VPN gateways are set up over the Public internet. Hence the traffic needs to be encrypted. **IPSEC** is used as the tunnelling protocol which creates a secure tunnel through which the data travels. Even if the traffic is intercepted, it cannot be decrypted.

VPN Gateways types

- **Site-to-Site VPN Gateways**
  - Here the On-premises will be a site and Azure VPN will be another site. We can connect multiple VNets.
- **Point to Site VPN gateways**
  - Here we connect a single client machine from on-premises to the Azure VNet.
  - We can use the same connection on multiple clients by exporting the configuration from the existing client.
- **Internal Gateway between Azure networks**
  - This is a special use case where we want to encrypt traffic between Azure Vnets.

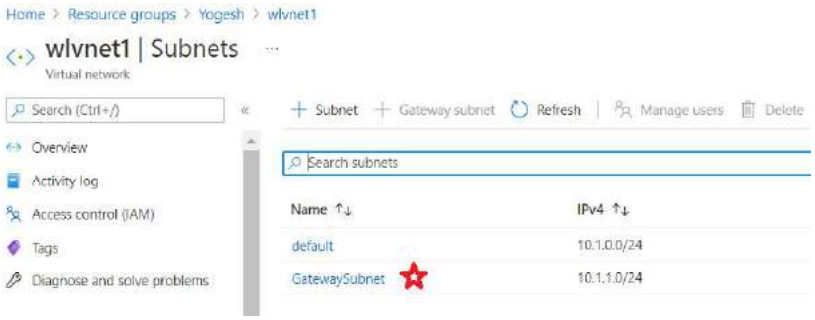
VPN Gateway Architecture



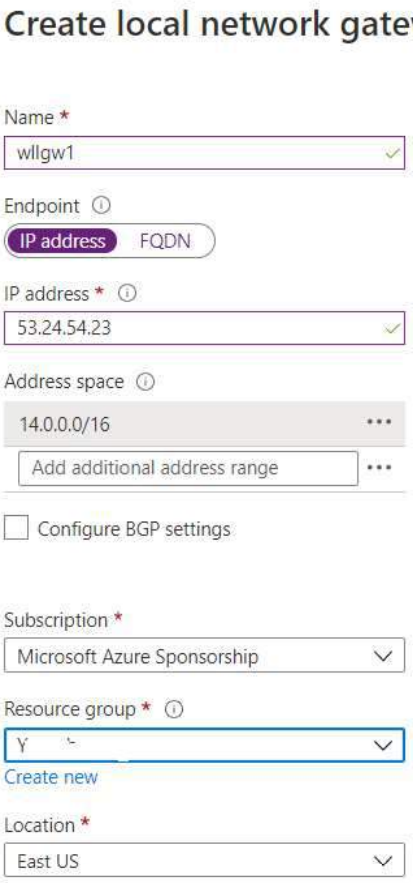
Steps to establish VPN Gateway

1. **GatewaySubnet**
   a. We need to create a subnet with the name "**gatewaysubnet**" for the setup
   b. If we are creating a Vnet, this subnet gets created automatically.

Please see the diagram below which shows the gateway subnet. This was created implicitly when the wlvnet1 was created as part of the Vnet gateway creation.



2. **Local Network Gateway**
    a. We need to obtain a Public IP address from the on-premises admin team and use that as the endpoint.
    b. See the IP address given as **53.24.54.23**. This is the ip address of the router on-premises

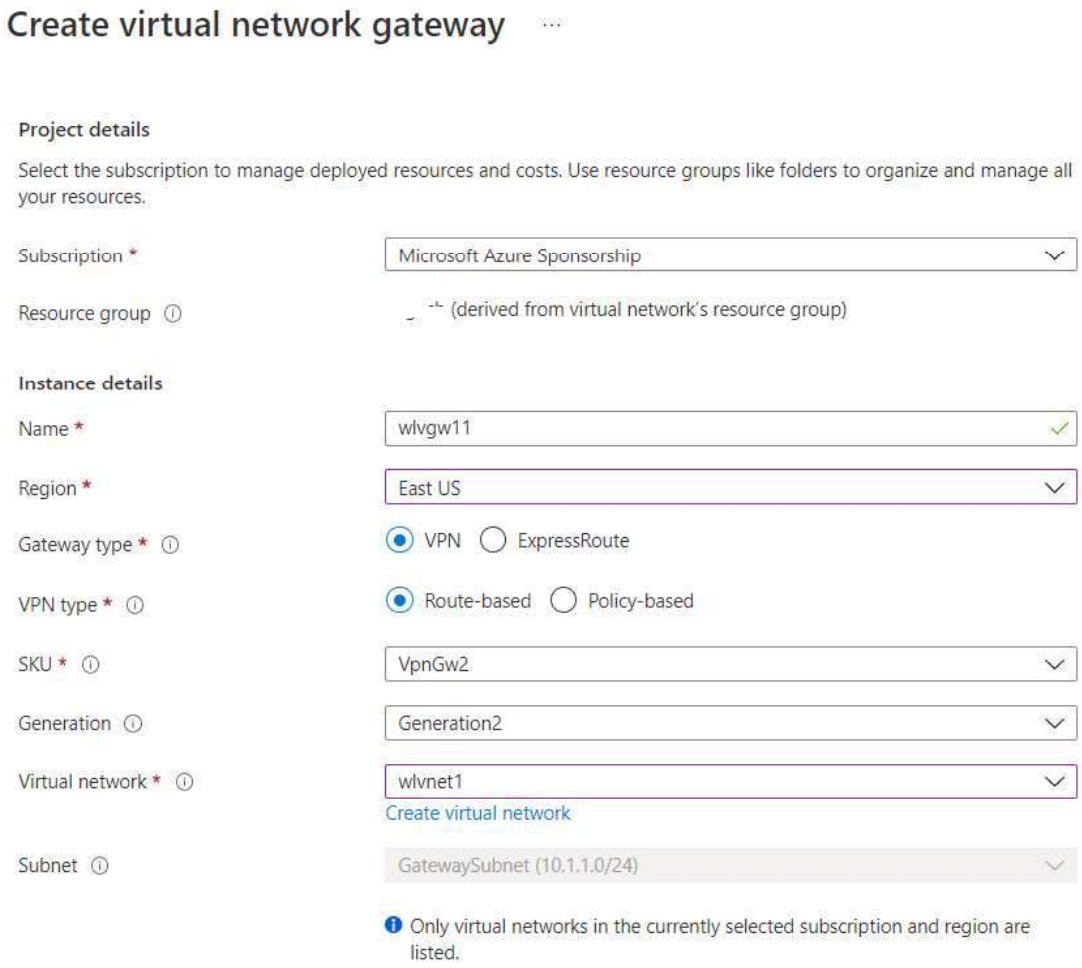


3. **Virtual Network Gateway**
    a. We need to create the virtual network gateway with the following inputs
        i. Gateway type – in our case, we are going to use VPN
        ii. Vpn type – could be either Route-based or Policy-based. Please note that we cannot change the type once it is created.

We need to delete the gateway and recreate it to make the change. Policy based is the most common type

iii. **SKU** – There are several SKUs. Please note that Basic is considered legacy and not recommended.

iv. **Subnet** – As mentioned, the name should be GatewaySubnet.



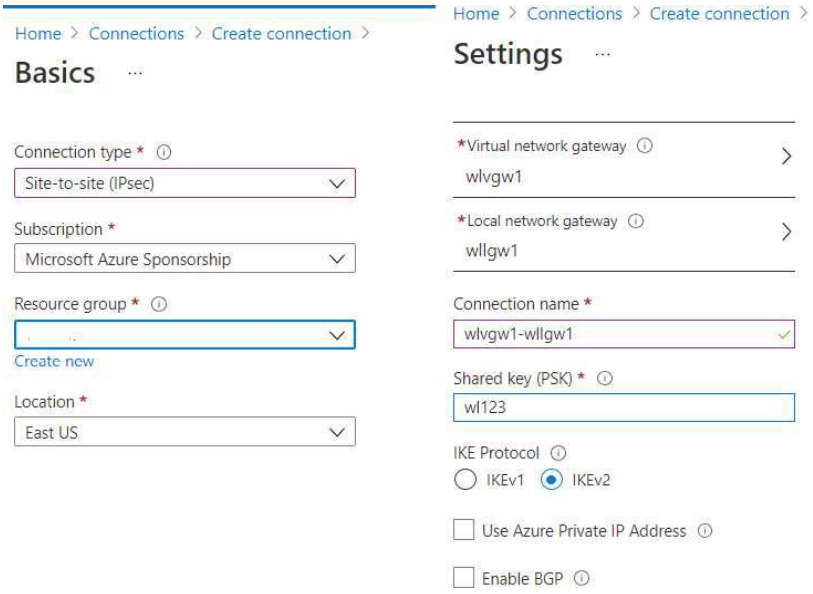
4. **Connection**

a. Once the prerequisites are fulfilled with the creation of Gateway Subnet, Local Network Gateway and the Virtual Network Gateway, we can create connection as follows

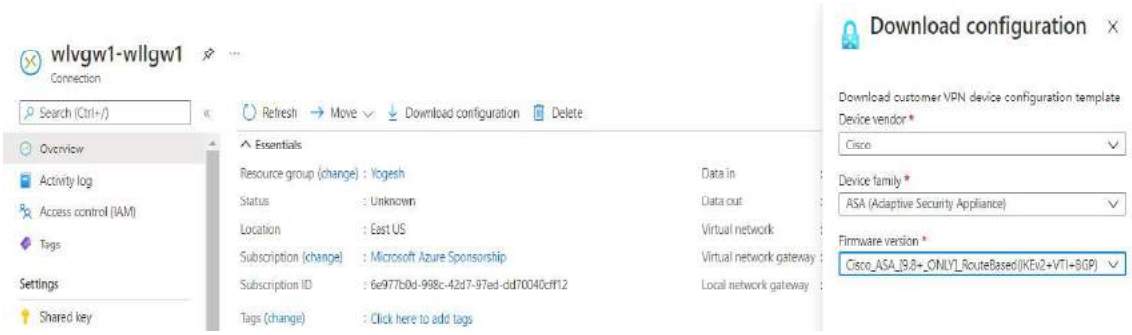
i. **Connection type** – the options are Vnet-to-Vnet, Express Route or Site-to-Site. In our case, we choose Site-to-site which uses the IPsec tunnelling protocol by default.

ii. **Bidirectional Connectivity** – Connections are usually unidirectional. We can select bidirectional to choose 2-way communication

iii. **Shared Key(PSK)** - We need to create a password here and need to share this with the on-premises admin to configure from their side.

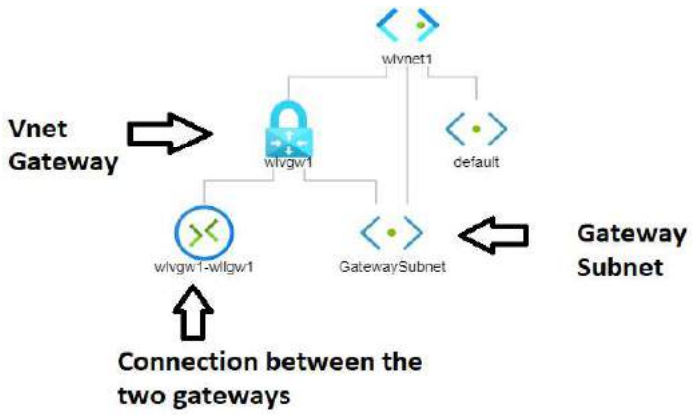


5. **On-premises setup**
    a. Once the setup is complete, we can download the configuration to be shared to the on-premises admin.
    b. We need to get the router model and select the same from the dropdown list and download the configuration and share with the admin along with the shared key.



Topology

We can check for the topology from the network watcher – topology blade.



Azure CDN

What is a CDN?

CDN stands for **Content Delivery network**. It is an architecture of distributed network of servers that can efficiently deliver web content to users.

CDNs will cache the content on edge servers in the POP (point of presence) locations keeping the content closer to the users thereby minimizing latency. This is made possible by using the existing network infrastructure of the CDN provider.

Let's say that a company demystify has a headquarters in NY, USA and branches in CA, USA and Bangalore, India.

The Servers are located in NY and we have a user logging in from Bangalore, India. The data needs to traverse the network and this will cause latency.

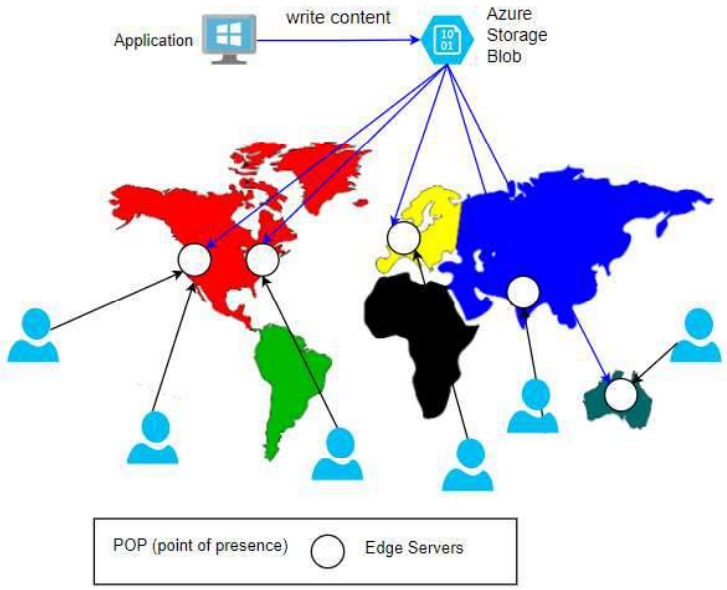
The solution here is to use CDN and use the Bangalore location to cache the data. Now, the user will be able to retrieve the data from Bangalore.

Please note that the data is not stored permanently on the edge location. This is to ensure that data does not go stale and it is current.

So we may set a cache interval of 24 hours and every day, the data will be retrieved from the Origin Server (NY, USA) and cached on the edge locations.

Also, if the data is not available (first time accessing) or if the cache has been marked as invalid, the data will be fetched from Server and sent to the user and cached on the edge location.

The next time, the request will be fulfilled by the edge server. This also reduces the load on the Origin server.



FAQs:

1) **How long is the data cached on the edge Server?**
   The TTL (time to live) by default is 7 days. This can be configured as per the application requirements. Once TTL expires, the cache will be marked as invalid.

2) **What type of azure servers can serve as Origin Servers to get source data?**
   Azure Web App, Azure Cloud Service, Azure Storage account, or any public web server.

3) **What are the CDN products available?**
   Azure has its own product. Besides that, it has tied up with Akamai and Verizon. Here are the offerings:

   a. **Azure CDN Standard from Microsoft**
   b. **Azure CDN Standard from Akamai**
   c. **Azure CDN Standard from Verizon**
   d. **Azure CDN Premium from Verizon.**

Please note that not all products might be available at all locations. You will need to check the product availability for your location.

4) **What are some of the additional features?**
   a. **Dynamic site acceleration(DSA)**
   b. **Video streaming optimization**
   c. **Customizable, rules based content delivery engine**
   d. **HTTPS support with CDN endpoint**
   e. **Compression encodings**

5) **Who are the market leaders for CDN? - PFB**

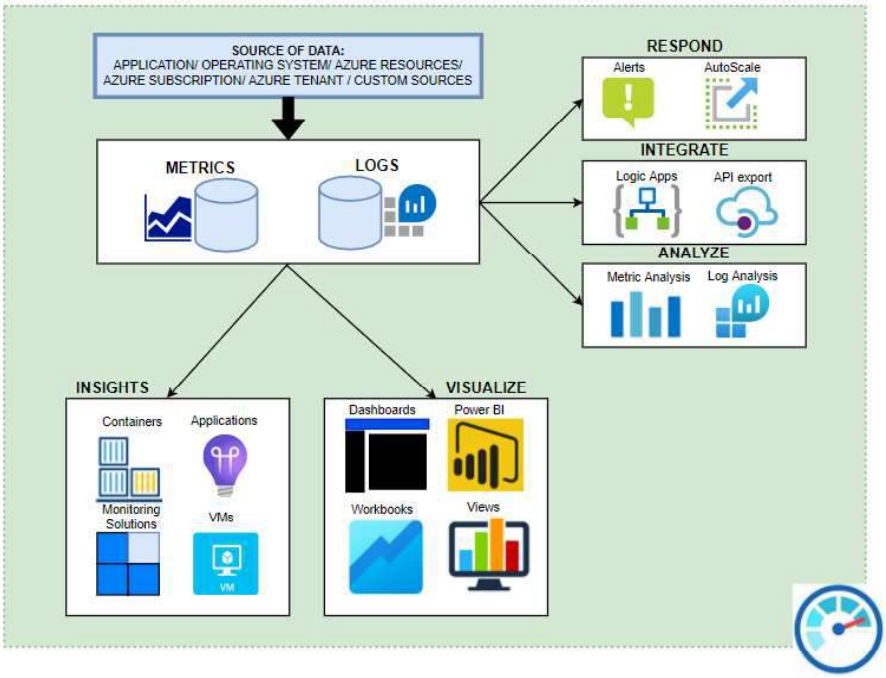
Top Competitors	Market Share	# Websites
jQuery CDN	38.60%	19,13,841.00
CloudFront	24.57%	12,18,186.00
BootstrapCDN	8.88%	4,40,178.00
Amazon S	37.79%	3,86,324.00
Vimeo CDN	5.71%	2,82,933.00
CDN JS	4.16%	2,06,402.00
OSS CDN	3.59%	1,78,093.00
CloudFlare	2.56%	1,27,104.00
Microsoft Ajax CDN	1.97%	97,471.00
Akamai	1.67%	82,949.00
MaxCDN	0.49%	24,381.00

Azure Monitor

- Azure Monitor is a free service that helps increase performance and availability. We could collect telemetry data from Azure as well as on-premises.
- We could collect the metrics and logs from our resources like VMs. We could even collect more detailed logs by enabling guest diagnostics and collect OS level information.
- We can also integrate additionally with **SIEM and ITSM** tools. We could also send data via event hubs or other services.
- Metrics are available at each resource level or they can be collectively seen at the Azure Monitor. This way Monitor acts as a central location for all our monitoring needs like Metrics, logs, alerts and activity logs.
- We also have a section on Insights where we can see more intelligent information for various resources like *Applications, VMs, Storage Accounts, Containers, Networks, SQL (Preview), CosmosDB, KeyVault, Azure Cache for Redis.*
- We could also see a map of our application and understand how the different components work together.

At a high level, we do the following:

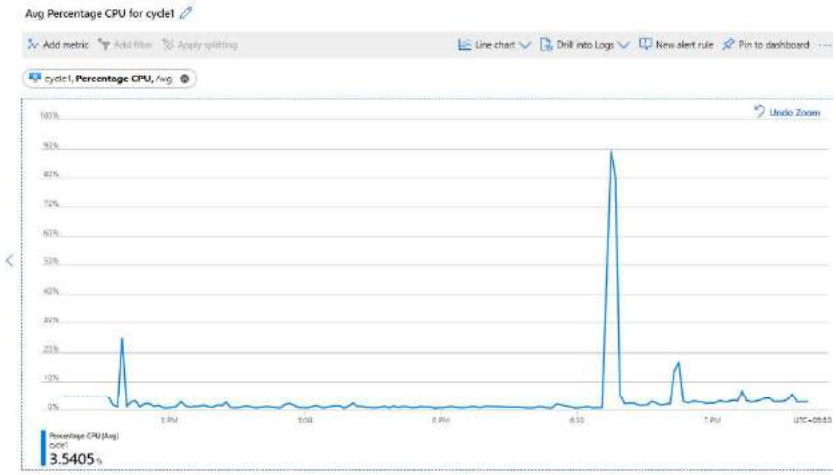
1. **Monitor & Visualize Metrics**
2. **Query & Analyze Logs**
3. **Setup Alert & Actions**



Here are some of the components which make up the Azure Monitor

1) **Inputs** –
    a. **Logs** – these are the logs generated by various resources like VMs/ Databases etc.,

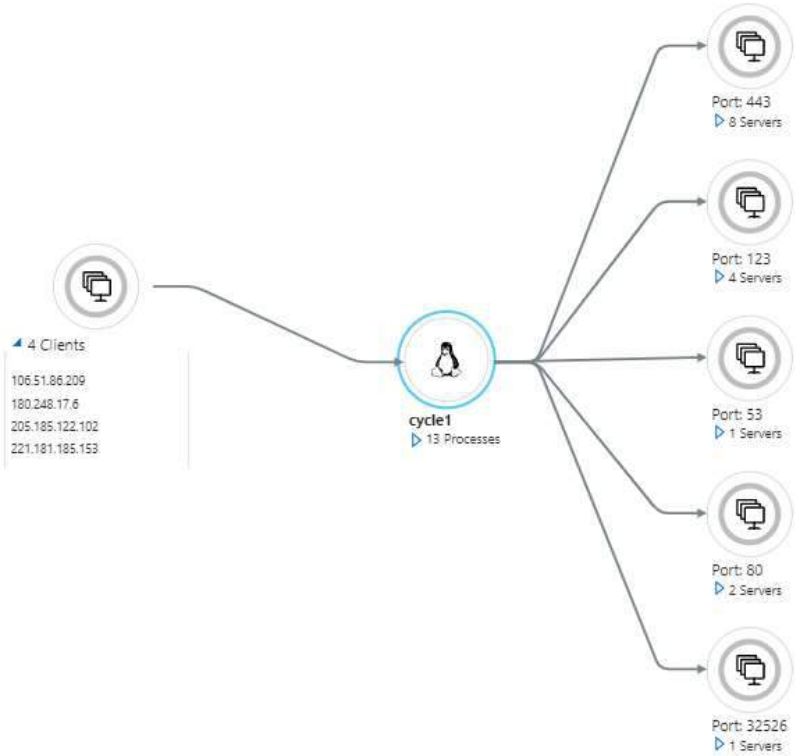
b. **Metrics** – Metrics provides numbers like *CPU percentage, Network data in/out* which helps us understand performance.
The metrics are stored in a time series DB which helps understand real time scenarios. With metrics, we can set triggers to scale the resources up and down. Please see a metric chart below on CPU percentage usage:



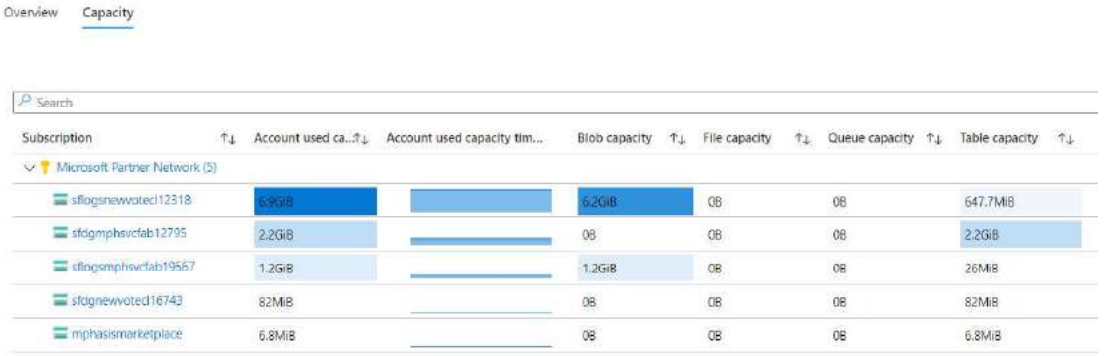
2) Insights

a. With Insights, we can get a deeper view into the resources. We could see a map of the resources and get an overall view. Please see below some insights:

APPLICATION MAP:



STORAGE OVERVIEW



KEYVAULT INSIGHTS

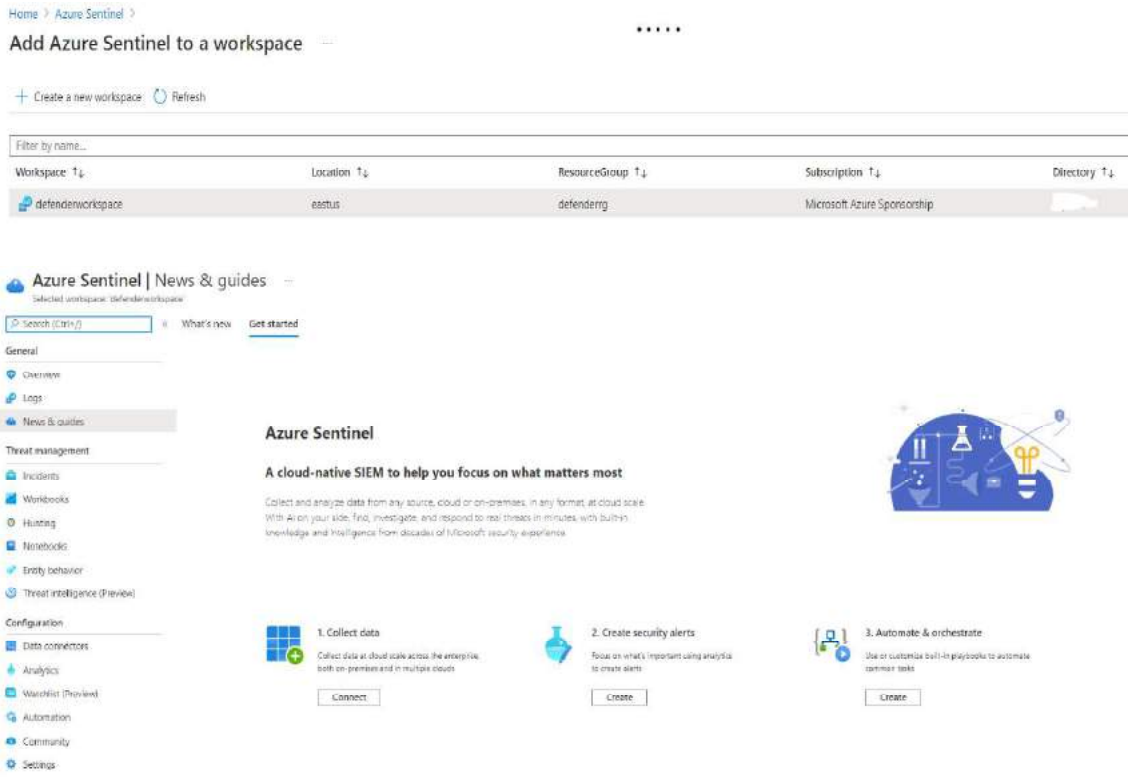
3) **Analyze**
    a. **Log Analytics** – We can work with log data from multiple sources with log analytics. We can perform complex queries with *KQL (Kusto Query Language)*. We can analyse and act on that data.
    b. **Metric Analysis**
4) **Visualize**
    a. **Metrics explorer** – interactively work with metric data with metric explorer
    b. **Workbooks** – We can use a combination of text, metrics, log queries and parameters into interactive reports. There are several built-in workbooks available for use.
    c. **Dashboards** – We can add metric graphs and queries output and create dashboards
5) **Respond**
    a. **Alerts** - When there is any issue, then we will get alerts proactively and we can automatically run *functions, runbooks, webhooks or logic apps.*
    b. **AutoScale** – With the metric as inputs, we can set up the system to scale up or down automatically.

Azure Sentinel

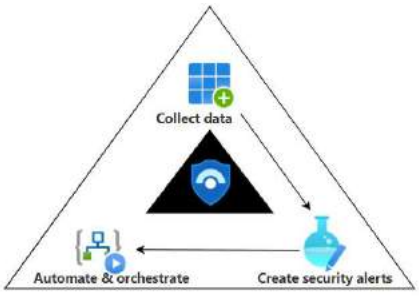
Azure Security Centre provides us with basic visibility and Analytics but Azure Sentinel goes beyond this and provides complete cybersecurity whereby it is able to provide **visibility/ analytics and Hunting/ Incidents** and finally responding to the incidents with automation.

Initiating Sentinel

- To initiate the Sentinel service, we need to create or connect **Log Analytic Workspaces**. Once done, you will see the Sentinel Panel.



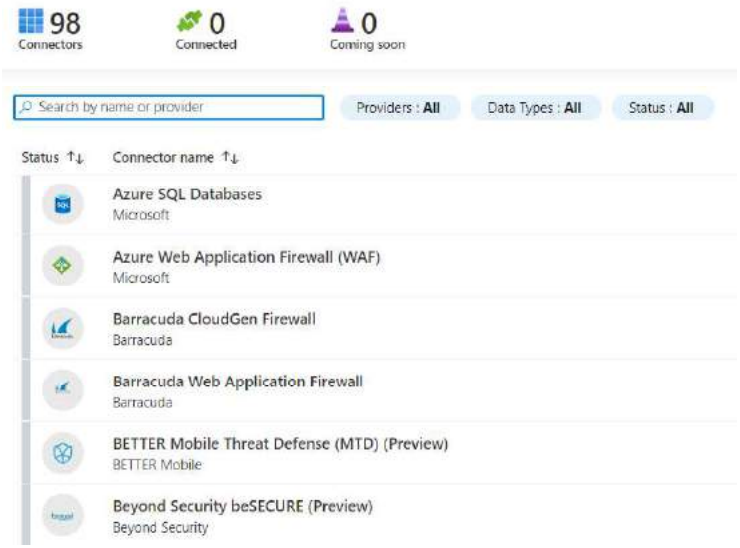
Here are the phases of Azure Sentinel:



1. Collect data

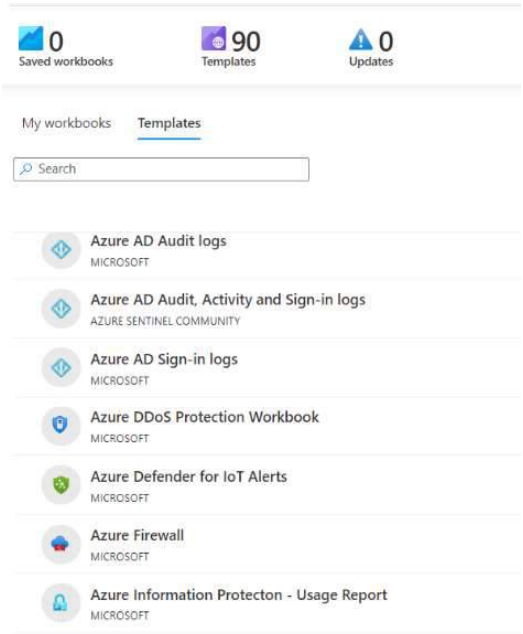
a. Azure Sentinel can collect data at cloud scale across the enterprise, both on-premises and in multiple clouds.

b. There are **98** data connectors available as of today like **Azure/ AWS** etc and we can connect to these sources and receive the data. **Examples** of Azure data are *azure sign-in activity from Azure AD.*

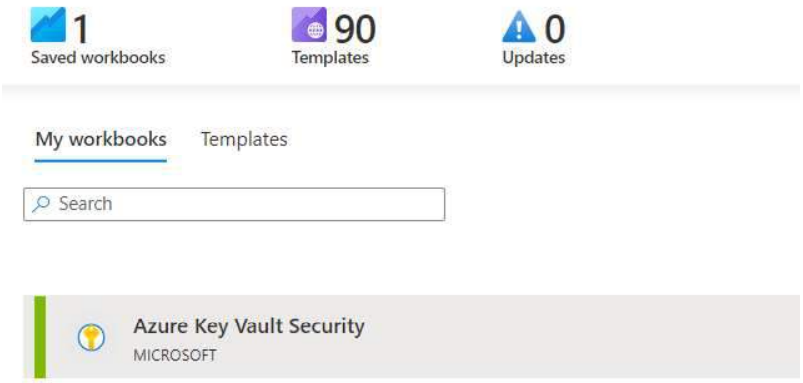


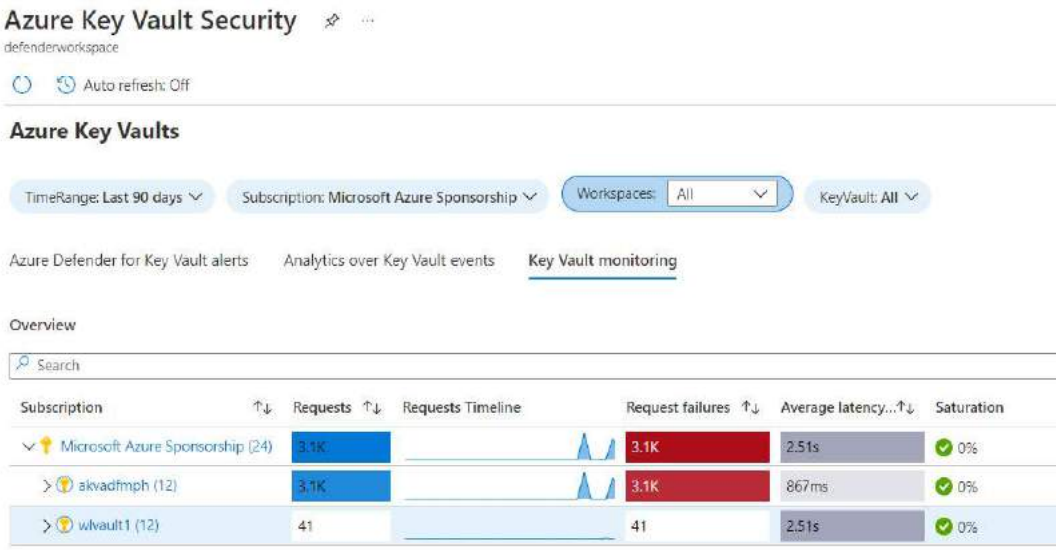
2. **Create Alerts**
   a. Once the data is collected, we can run queries against the data. We focus on what is important using the analytics and create suitable alerts.
   b. There are prebuilt workbooks available which can be selected and used to get insights.

Workbooks selection



- We need to select the template and save it and we will be able to get the details.





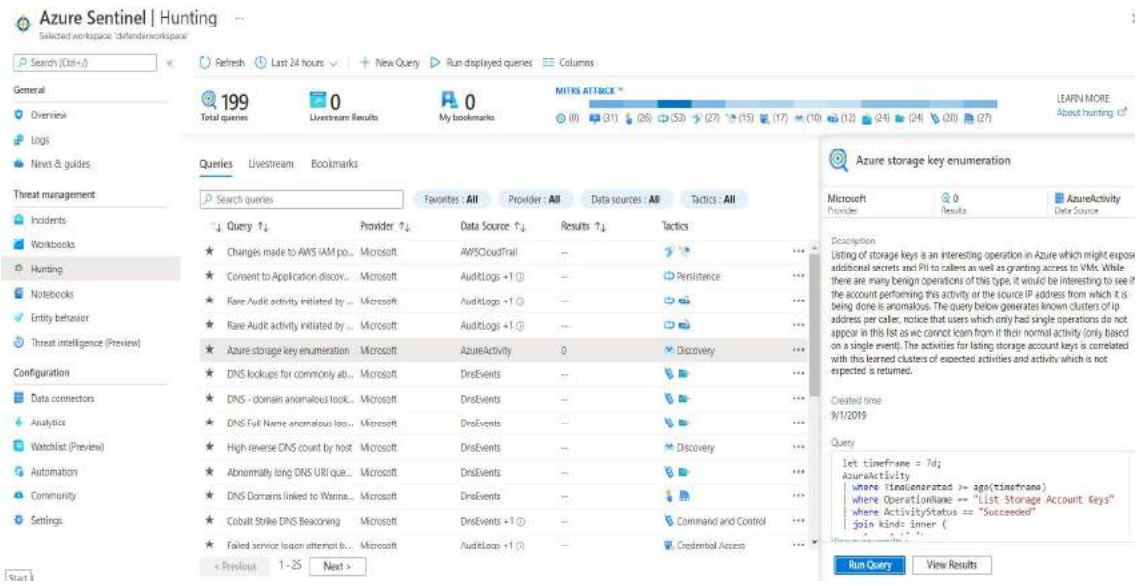
3. Automate and Orchestrate

- **a.** We build automation rules which will automate incident configuration. We could trigger playbooks to handle security alerts.
- **b.** We create rules which will trigger the playbooks to be run automatically based on the conditions

Hunting Feature

Azure Sentinel has the hunting feature where we could go further and search for various activities like listing of storage keys or high **DNS queries** etc.,

This will help us identify attacks targeted and we could go and proactively block the malicious activity.



Sentinel Community

There is a sentinel community where we can get different types of resources like *Workbooks, Analytics rules, Hunting queries, and Playbooks.*

Azure Sentinel pricing

Billing is based on the volume of data ingested for analysis. Azure Sentinel offers a flexible and predictable pricing model and we could pay either with **Capacity Reservations or Pay-as-you-Go**.

With Capacity Reservations, we can get as much as **60%** less as compared to Pay-as-you-Go.

Advanced Threat Protection

Azure has a product called Azure defender for SQL which is a unified package for advanced SQL security capabilities. This is designed for the database offerings viz., *Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics*.

Some of the functionality of the tools include

- **Discovering and Classification of sensitive data**
- **Identifying and mitigating potential database vulnerabilities**
- **Detection of anomalous activities that could be a potential threat**

The tool does 2 major activities. One is *Vulnerability assessment and the other is Advanced Threat Protection.*

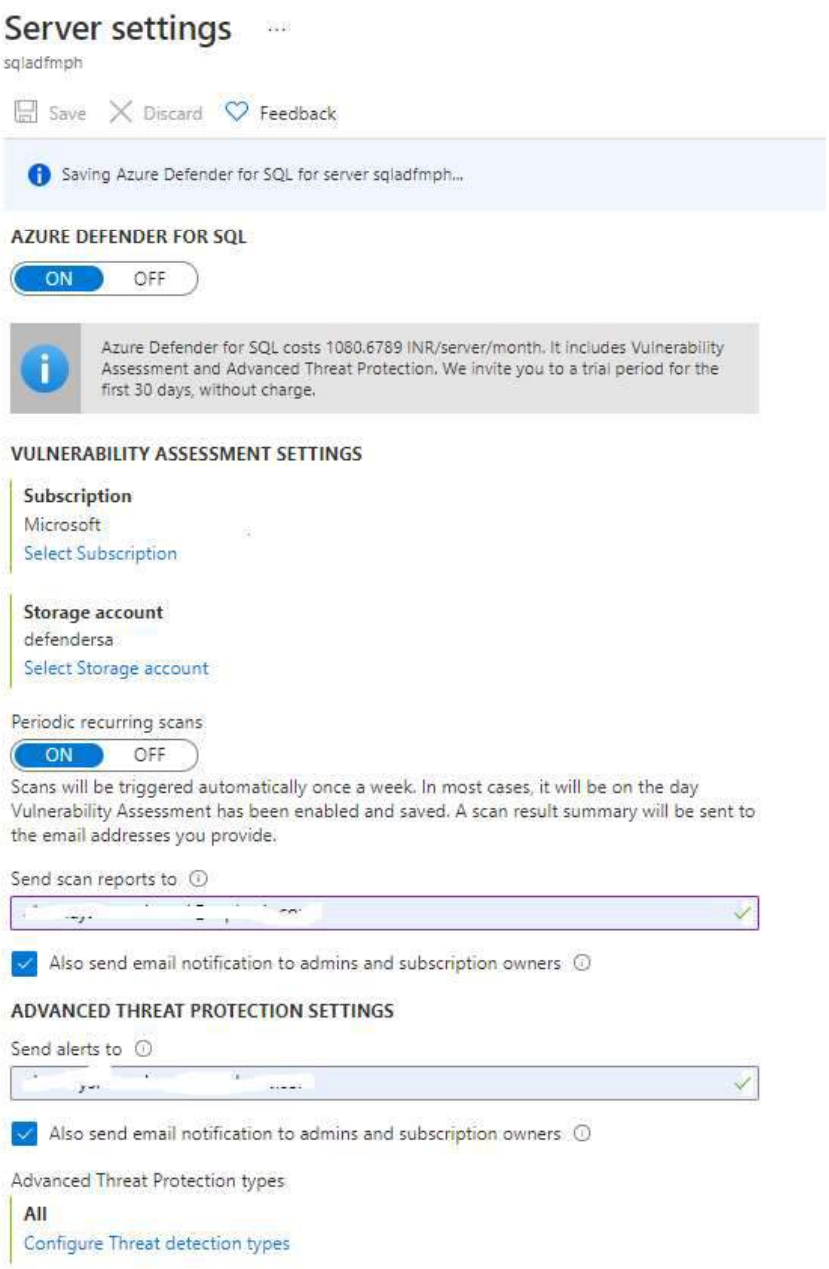
Under ATP, the following features are available:

- **Detect anomalous activities**
  - Unusual/potentially harmful attempts to access or exploit your database.
- **Continuous monitoring of database for suspicious activities**
- **Immediate security alerts on**
  - Potential vulnerabilities
  - SQL injection attacks
  - Anomalous database access patterns.
- **Recommend action on how to investigate and mitigate the threat.**

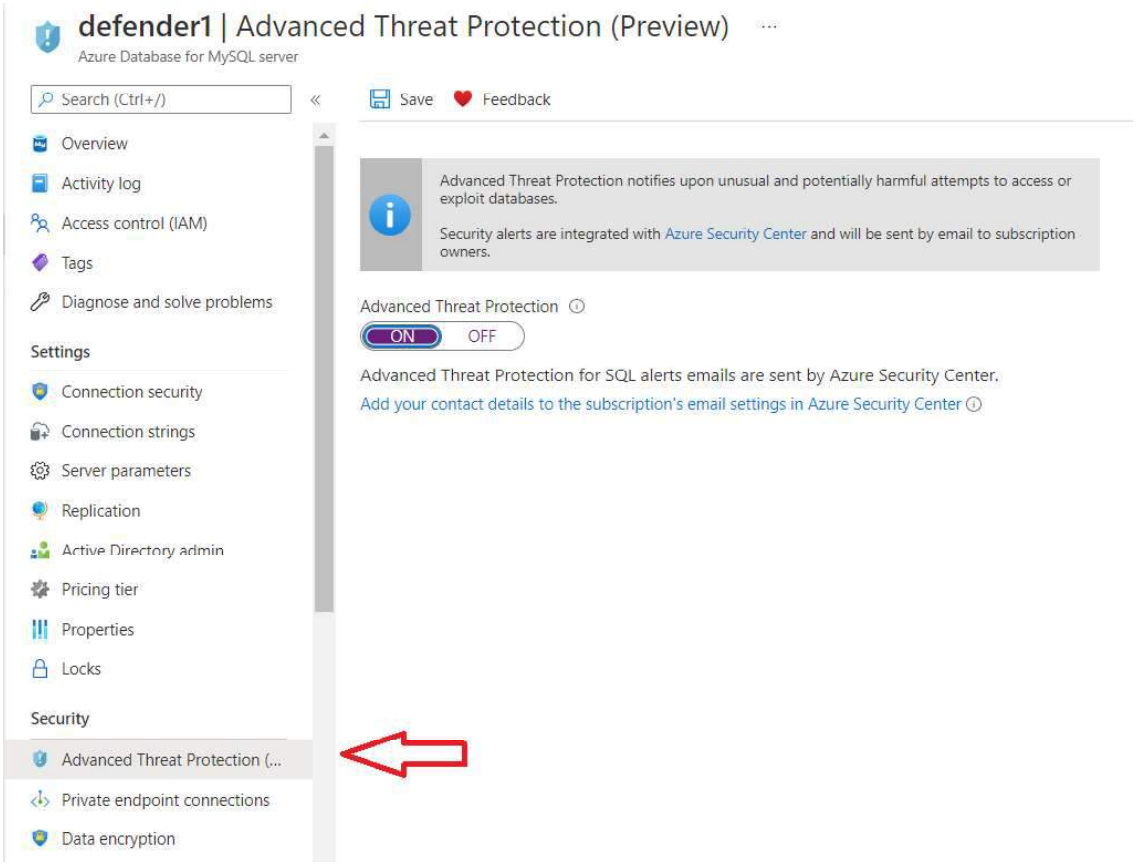
How to Enable ATP:

- We can enable/disable different type of alerts under ATP

Under Security settings of the SQL server, we can enable ATP.



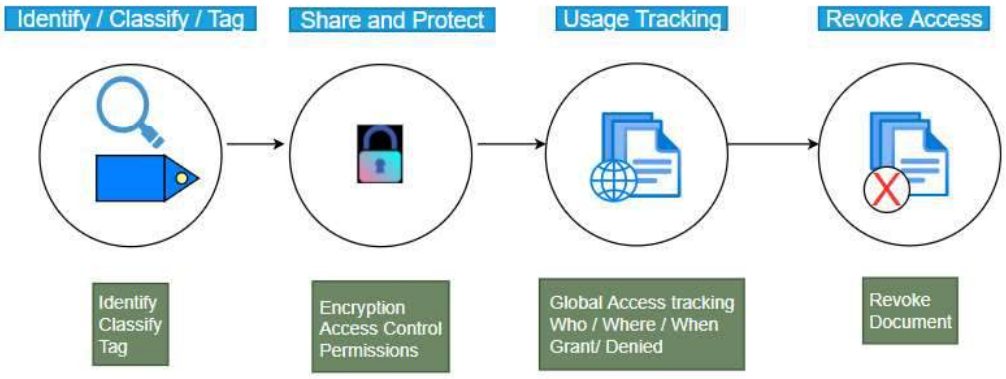
- We can see the ATP alerts in the Security Center as it is integrated with it.
- The MYSQL Database server can be configured under Security Option.


defender1 | Advanced Threat Protection (Preview)
Azure Database for MySQL server
Search (Ctrl+/)
Save
Feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Connection security
Connection strings
Server parameters
Replication
Active Directory admin
Pricing tier
Properties
Locks
Security
Advanced Threat Protection (...
Private endpoint connections
Data encryption
Advanced Threat Protection notifies upon unusual and potentially harmful attempts to access or exploit databases.
Security alerts are integrated with Azure Security Center and will be sent by email to subscription owners.
Advanced Threat Protection
ON
OFF
Advanced Threat Protection for SQL alerts emails are sent by Azure Security Center.
Add your contact details to the subscription's email settings in Azure Security Center

Azure Information Protection

AIP helps us classify and protect our documents based on the sensitivity of the data. AIP is based on **Azure Rights Management (RMS)** which is a cloud based protection technology.

We can look at the lifecycle of data below:



Lifecycle of data

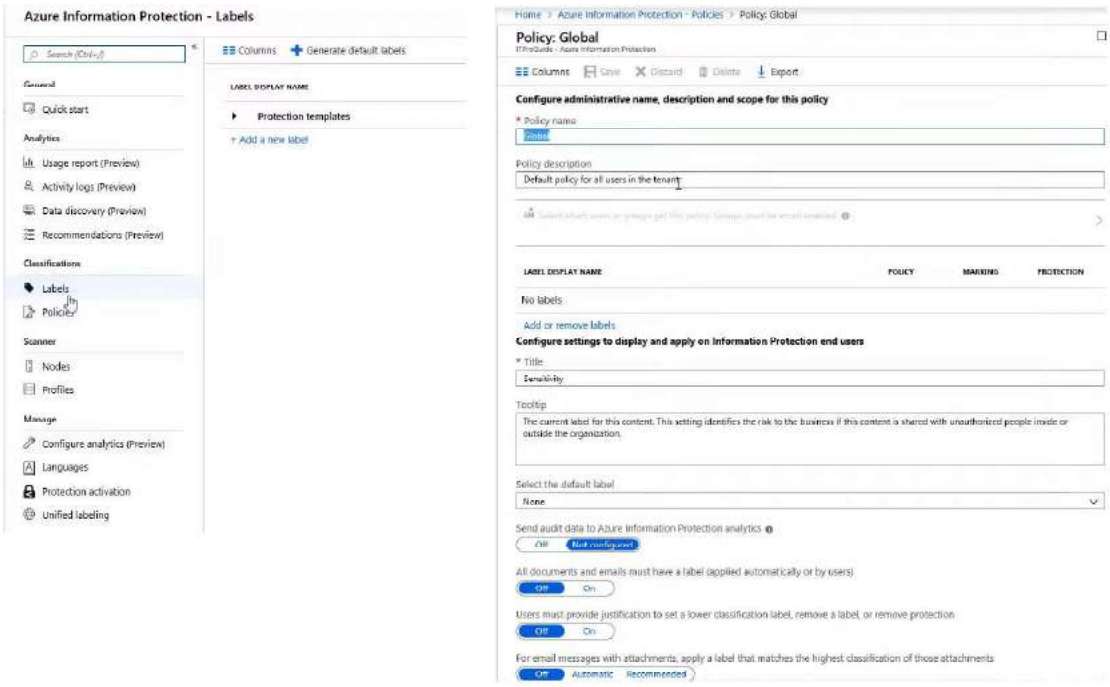
1) **Identify/Classify/Tag**
    a. In this phase, we identify the data that needs to be protected. There are two types of data in an organization. *Structured and unstructured*.
    b. Data that resides in a database can be classified as structured. Data that resides on the servers and user systems can be classified as unstructured. We identify the unstructured data
    c. Then we classify the data. Simple classification could be Public data which is *non-personal and non-confidential.* Likewise we could have confidential data.
    d. Then we need to tag the data

2) **Share and Protect**
    a. Once the data is classified and tagged, we encrypt the data. We could either use cloud key or we could use our own keys
    b. Then we grant or revoke access to the data. We could grant *viewing/ editing* permissions to different groups as needed

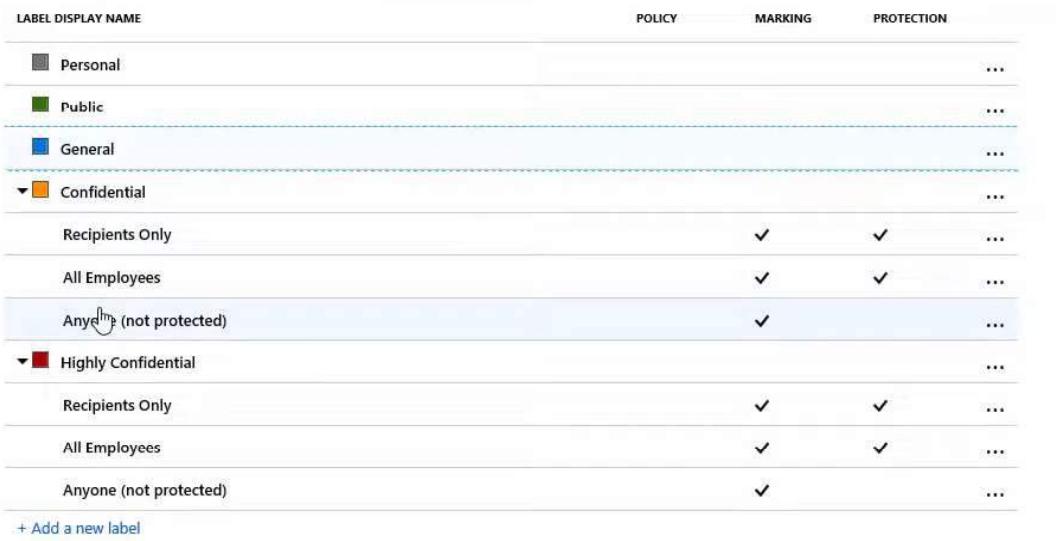
3) **Usage tracking**
    a. With RMS, we could track the usage of data
    b. We can see who accessed the data from which location and when
    c. We can grant or deny access

4) **Revoke access**
    a. Once we revoke the access to the data, the users who had access before cannot access the same data going forward.

- Below diagram shows the Labels and also the Global Policy.



- The Labels are available as default as seen below. We can create custom labels if needed to suit our needs.



AIP lifecycle:

Here are the practical steps to the same

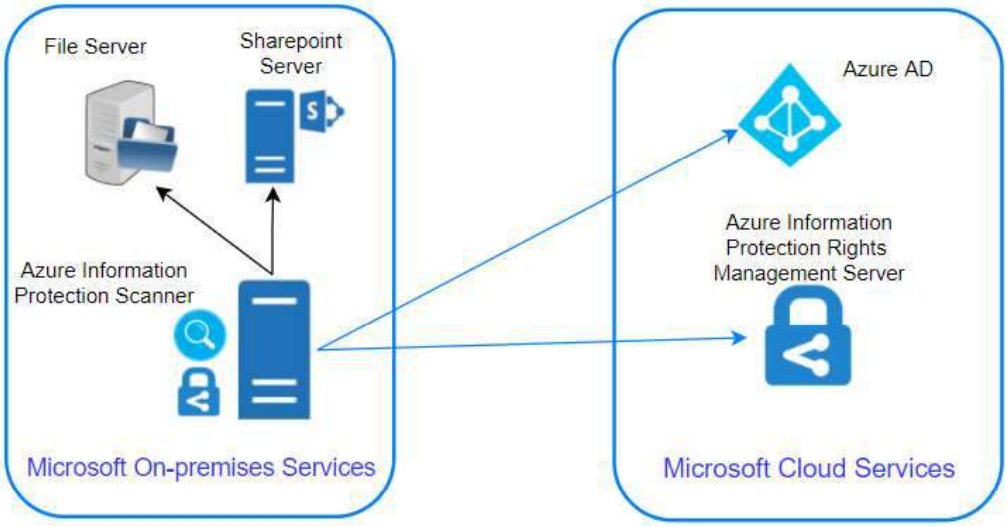
1) **Subscribe AIP** – We need to have suitable licenses like *AD Premium P1/P2*. There are other enterprise licenses also like E5.
2) **Azure AD** – We need to integrate with our AD

3) **AIP Label and Policy** – We need to create labels and then add them to our Policies. There is a global policy available by default. We can further customize or add our own Policy.
4) **Install AIP client** – We need to install AIP client on all servers that we want to manage
5) **Create custom label** – We create custom labels if needed
6) **Revoke Access** – We review and revoke access ending the life of the data managed

AIP Scanner

For On-premises setup, we need to install AIP Scanner which does the following:

1) **Discover**
2) **Protect**
3) **Classify**
4) **On-prem repository** – Any folder/drive like c: etc is considered as a repository



Requirements for AIP Scanner – Windows Server and SQL server

Steps for setting up AIP scanner

1) **Create Profile**
   - Settings like manual / automatic scan
   - Policy enforcement
   - Add Repositories like c:/, f:/docs
2) **Install SQL server**
3) **Run Powershell command and setup AIP Scanner**
   - `Install-AIPScanner -Sqlinstance "instance name" -Profile "profile-name"`
4) **Setup Access token**

Azure DDoS Protection

What are DoS and DDoS?

DoS stands for **denial of service** and **DDoS** stands for **distributed denial of service**.

Scenario:

*Let's say that you have a web server serving web traffic and you are a medium enterprise handling **1000** requests per second. If any malicious entity sends **100,000** requests per second, your server will be busy trying to respond to the 100K requests and unable to serve the regular customers. This is called **Flooding**.*

*Often the load will be so heavy that it will cause the server/machine to crash. This is called **denial of service** where customers are denied service by rendering the server unusable.*

*Imagine the same **100K** requests coming from multiple servers where malicious entities do a coordinated attack with multiple servers. This is called **distributed denial of service** where multiple servers hit a given target to bring it down. We have seen attacks feeding as much as **800 Gbps** which can bring the biggest servers down.*

Azure DDoS

It provides protection against DoS attacks with always-on monitoring and automatic network mitigation.

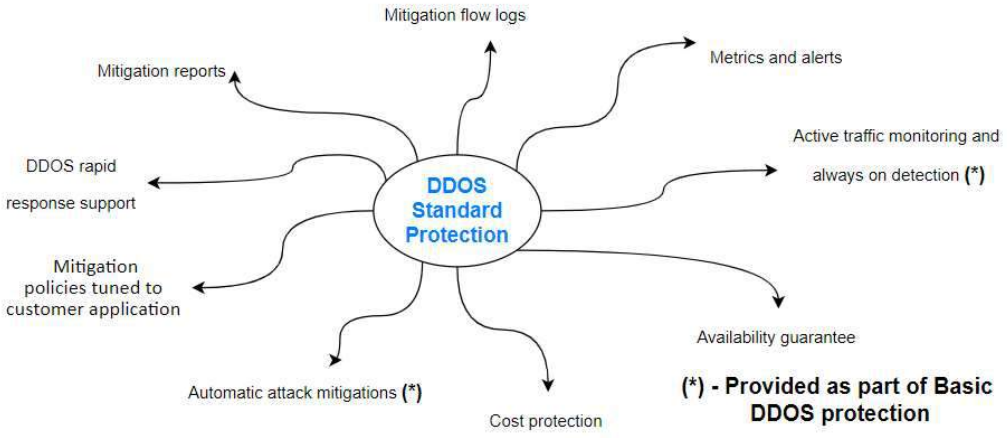
There are two levels of Service – One is **BASIC** and the other is **STANDARD**. Basic plan is free and enabled by default. After all, Azure needs to protects its resources 😊

Basic plan, like the name says, provides only basic services *(always-on monitoring and automatic network mitigation).*

Standard protection provides multiple features. This could cost you as much as **3000$** to protect about 100 resources like

- *Azure firewall, App Gateway/WAF*
- *VMs, AKS*
- *SQL, CosmosDB, Storage, App Services etc.*
- *Vnet*
- So, let's say that a **DoS/DDoS** attack occurs. The Cloud is resilient usually due to the elasticity and if you have good autoscaling, then the cloud resources will keep scaling up like VM spinning up, App Service scaling up etc.
- As a result, you will have a lot of traffic and you must be aware that while ingress traffic is not charged, consumers pay for egress traffic.
- So you will land with a huge compute bill and egress data charges.
- If we had the DDoS standard protection plan, we would be issued credit for the excessive charges if the plan failed to protect us.

Here's the list of services provided.



Some of the features of DDoS Standard protection are:

- **DDoS Rapid response** – We can engage the **DDRT** (DDoS Rapid Response Team) for attack investigation and analysis
- **Cost Guarantee** – As discussed, we will be issued a service credit for the application scale out and excess data transfer
- **Attack alerting/Metrics** - Alerts can be configured to be notified at the start/stop and logging will be done and metrics provided.
- **Extensive Mitigation Scale** – This works at a global scale and is highly scalable and can mitigate over 60 types of attacks.
- **Multi-layered protection** – It can protect at different layers (layer 3/4/7)
- **Adaptive tuning** –Let's say there is unusual traffic from an IP and it is determined as anomalous by the DDoS cognitive services, ddos protection will automatically deny traffic from the IP and block it.

In addition, we can have our own monitoring to alert when a DDoS attack occurs.

We can set up this rule in Azure Monitor to notify us that ddos mitigation has started. We can set up an action group and take actions like notifications, isolating the resource for forensics etc.,

```
AzureDiagnostics
| where Category == "DDoSProtectionNotifications"
| where type_s == "MitigationStarted"
```