Microsoft Certified Azure Administrator

Exam AZ-104
Microsoft Certified Azure Administrator Associate

Microsoft Azure

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

Index

Azure Portal

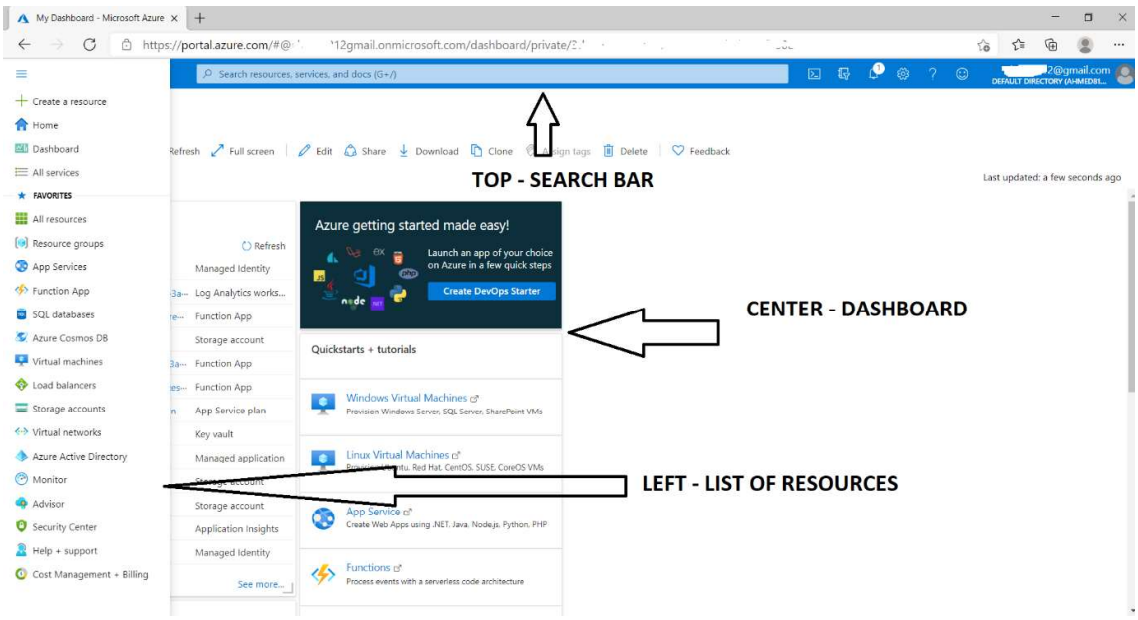
Azure provides 3 administration tools to choose from

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

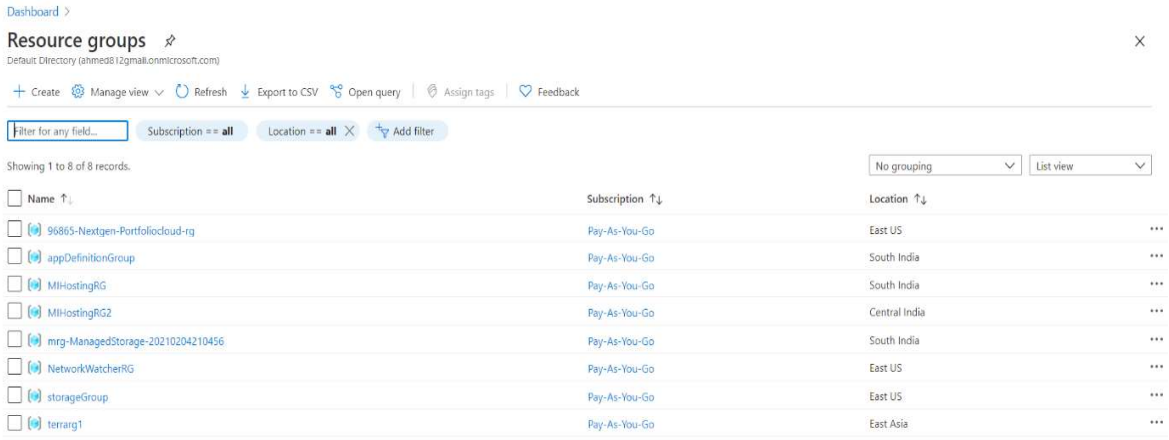
- We can use the **Azure GUI portal website (portal.azure.com)** to create, configure, and alter our Azure subscription resources.
- We can locate the resource needed and execute any changes. We have wizards and tooltips to guide through various administrative tasks.
- Please note that we cannot use 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.

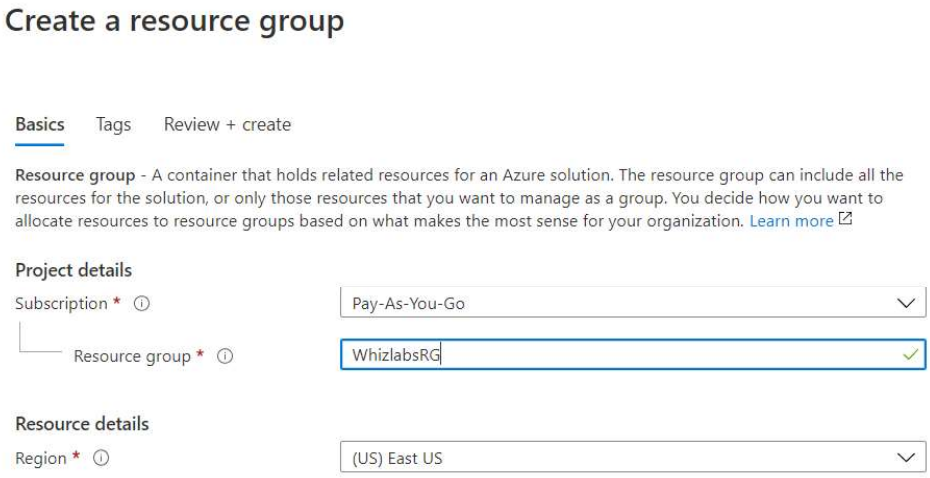
1. **Left** — A list of resources and services to create and manage your Azure environment.
2. **Center** — A dashboard that you can tailor to meet your (Public or Private dashboards) needs.
3. **Top** — A search bar to quickly find resources and services, a notification icon, access to a web-based command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



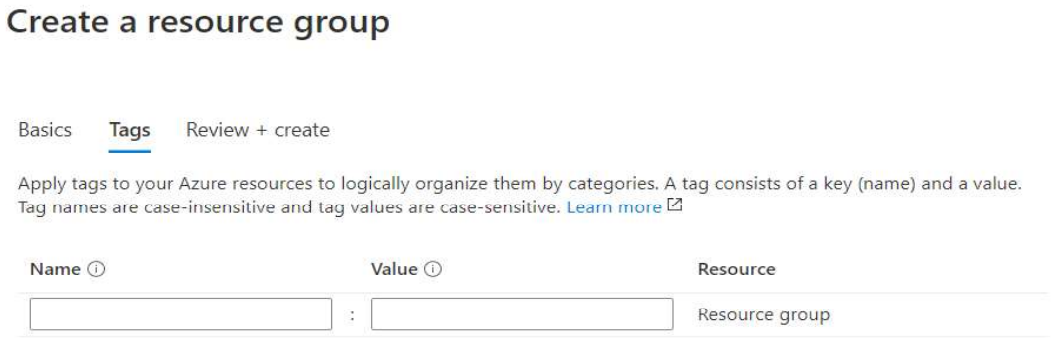
- Let's try to create a resource and see how to use the Portal. For example, let us create a resource group called demystify.
- Click on the Burger menu on the left top and select Resource group and click on it. You will get a new Panel.



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

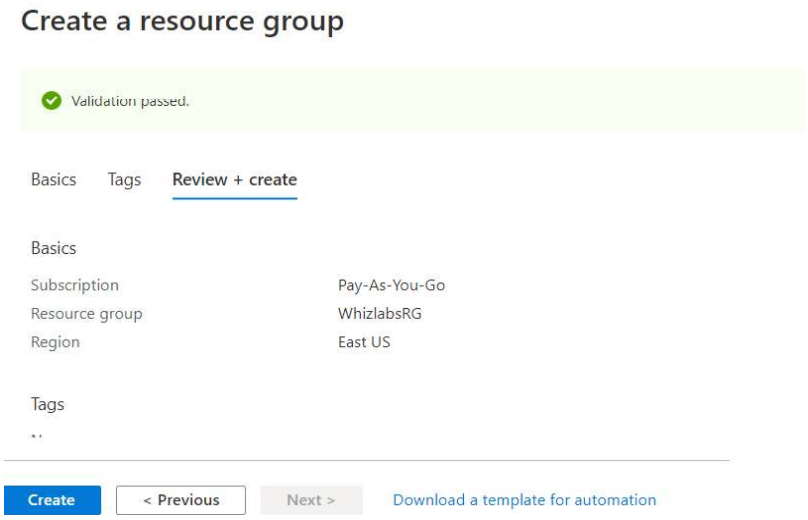


- Click Next, and you will get a new panel to add Tags. Tags are helpful for accounting and segregation but not mandatory.

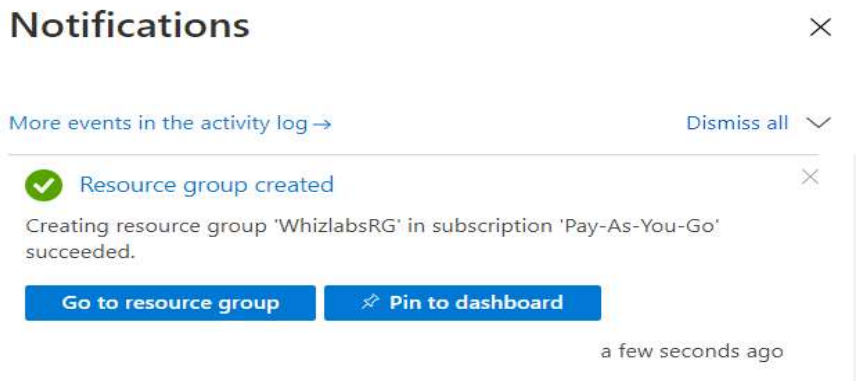


- Click NEXT, and at this point, Azure will validate all the options chosen.
- If there is any error, it will put a red dot on the tab where the error occurred, and you will need to go back to the tab and fix it before proceeding.
- If validation passed, you would see the Validation passed with a green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

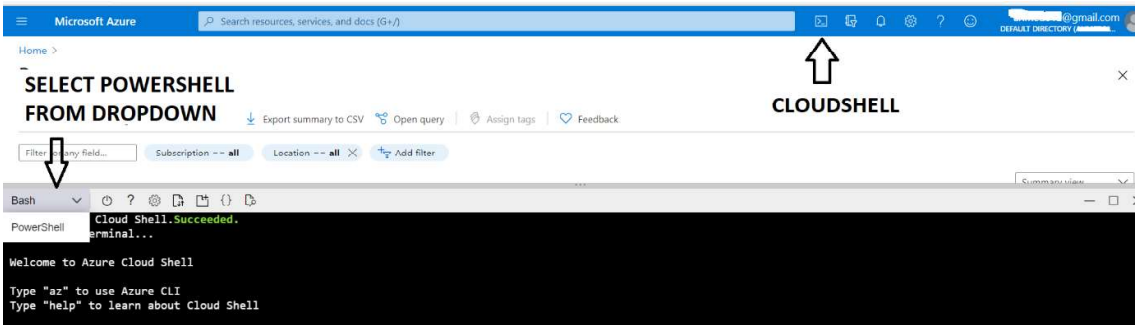
Azure provides three administration tools to choose from

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.

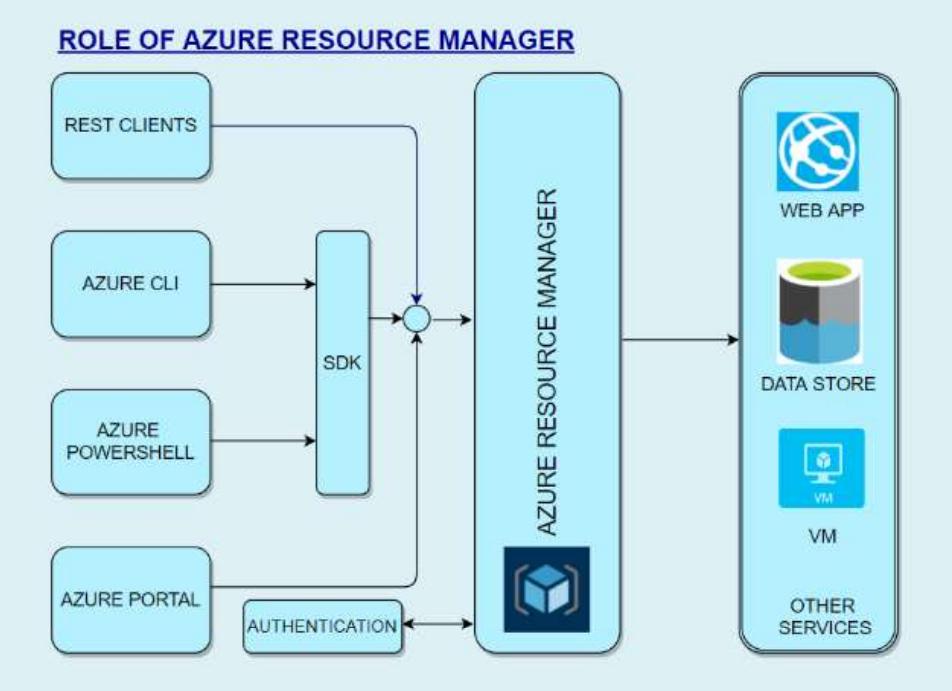
Working with Powershell:

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:

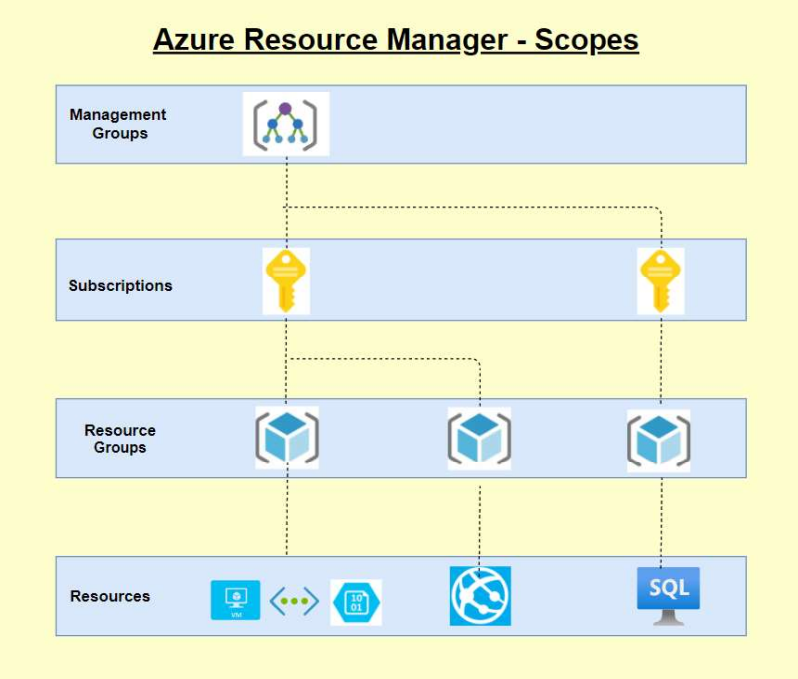
- Declarative templates so we don't have to worry about the current state.
- Allows group deployments
- Define dependencies so the correct order of deployment is done.
- Apply tags to organize resources logically
- Allows for redeployment and have confidence that same results will be achieved
- Applies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

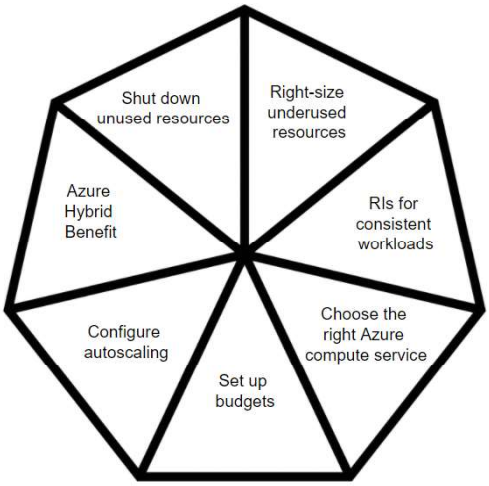
- **Azure Pricing Calculator**
- **Cost Management Center**
- **Migration planning – Estimation, Workload, and right-sizing**
- **Billing Data API & Advisor**
- **DB & Cosmos DB Capacity calculator**

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.

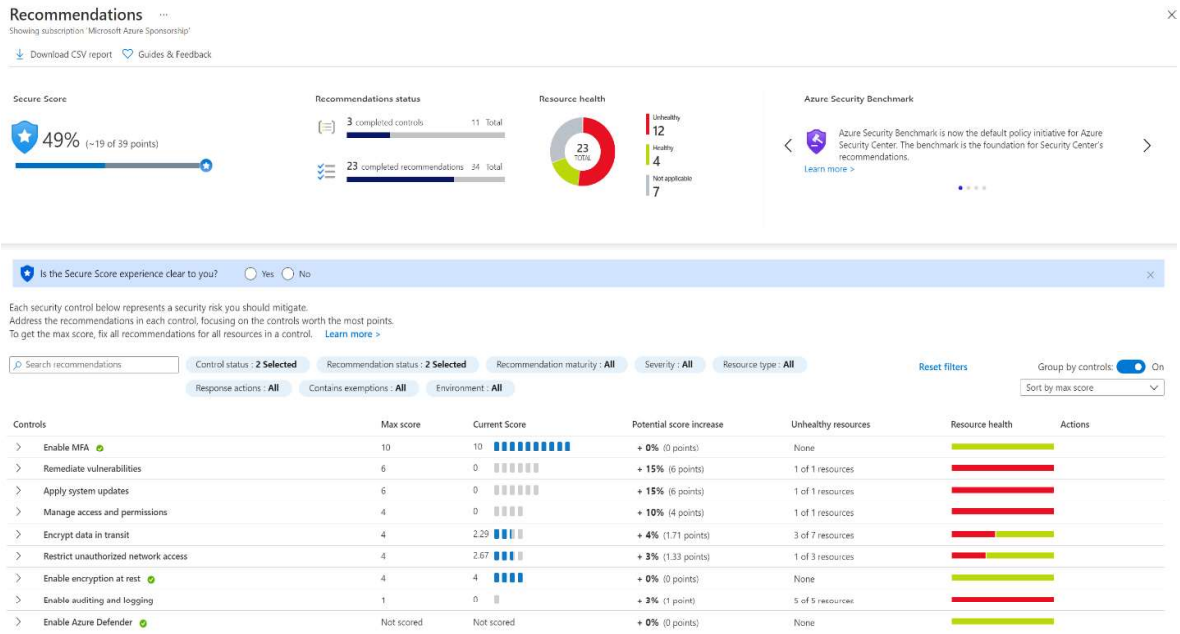
Key Pointers:

- 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.

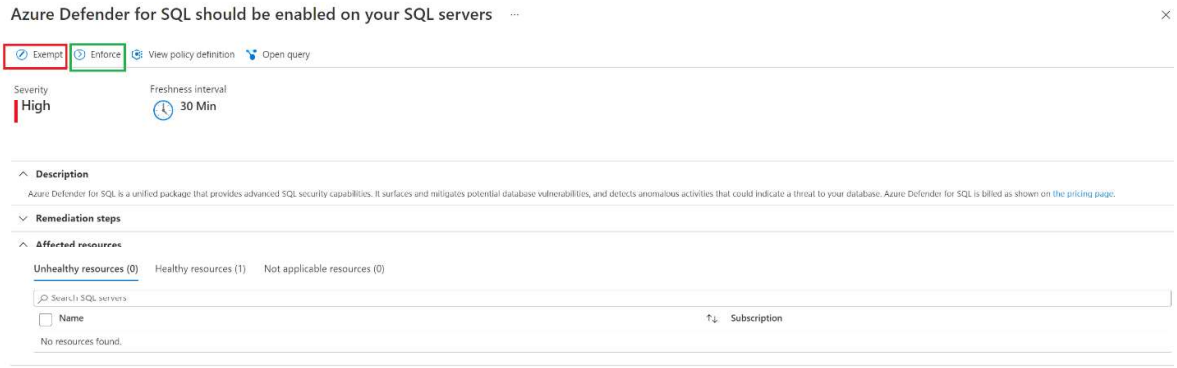
Environment assessment:

- 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.

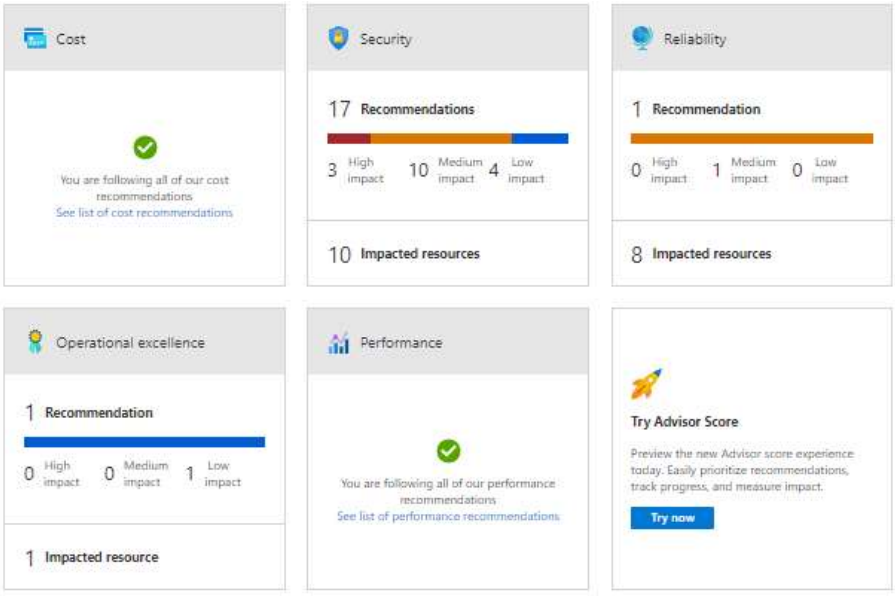
FEATURES	AZURE SECURITY CENTER FREE TIER	AZURE DEFENDER
Continuous assessment and security recommendations	✔	✔
Azure secure score	✔	✔
Just in time VM Access	- -	✔
Adaptive application controls and network hardening	- -	✔
Regulatory Compliance Dashboard (Preview)	- -	✔
Threat protection for Azure VMs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

Azure Advisor

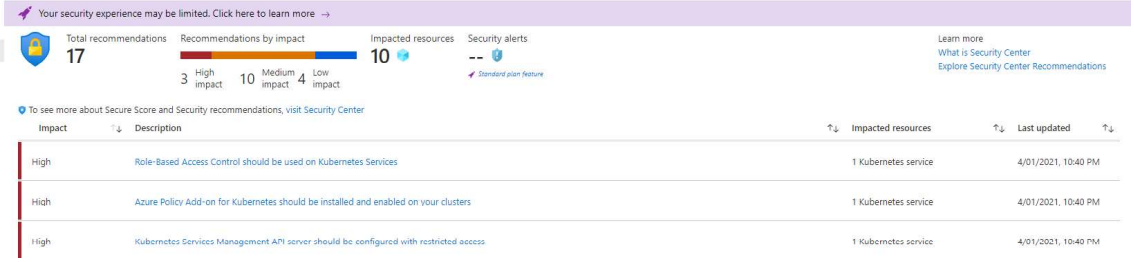
Azure has 5 pillars called the Azure well-architected framework which provides best practices to help build and deliver great solutions.

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.

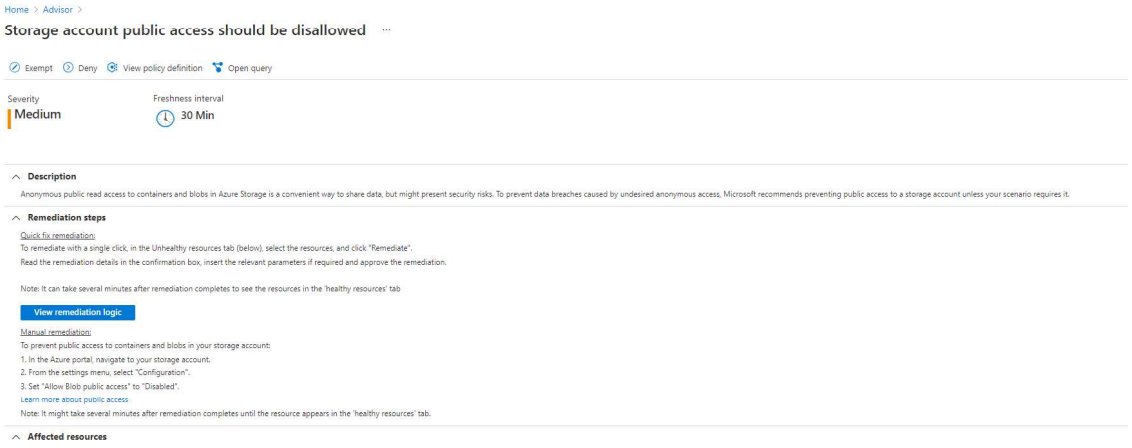
- On each of the 5 pillars, we will be given recommendations to optimize. Please see below.



- 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

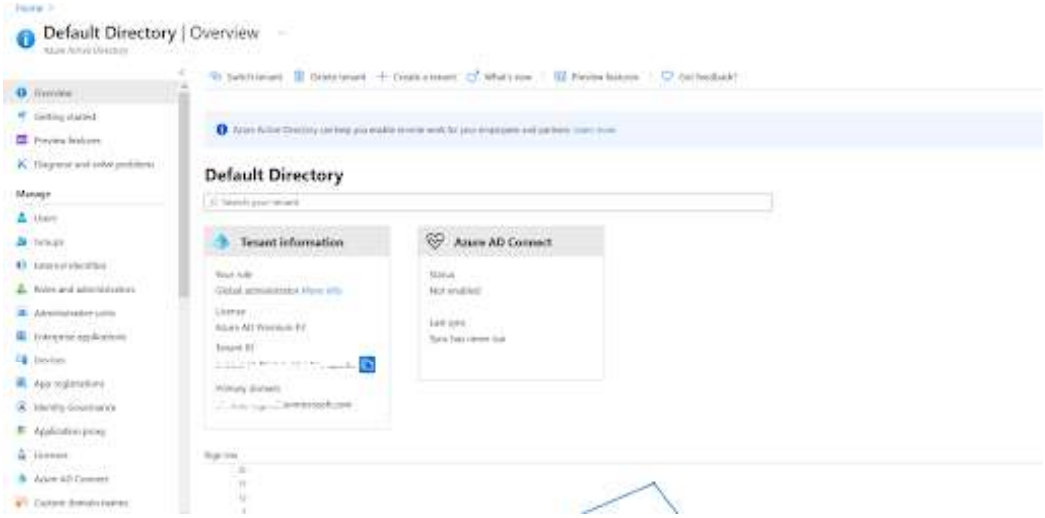
Azure AD Connect

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.

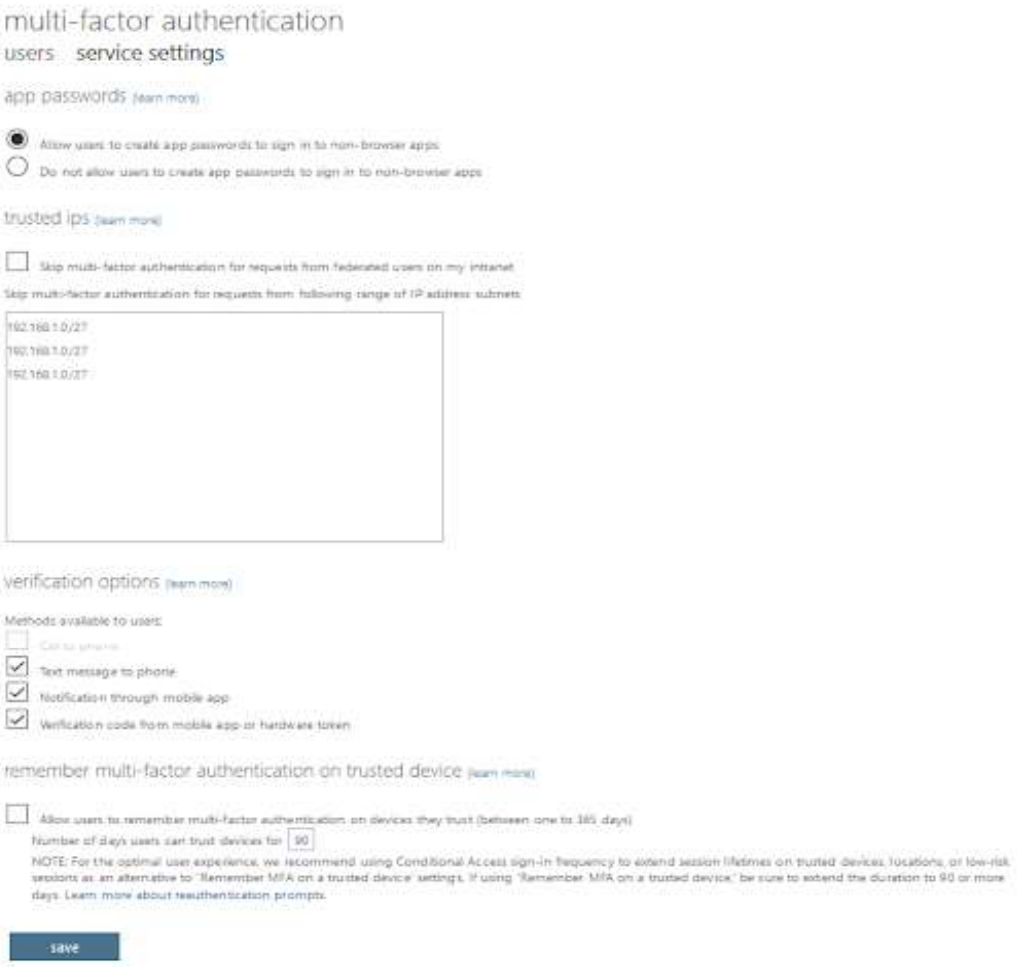
License Management – We can perform license Management here. We can track all acquired licenses and assigned licenses and make sure we don't overuse and pay heavy penalties

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"
}
```

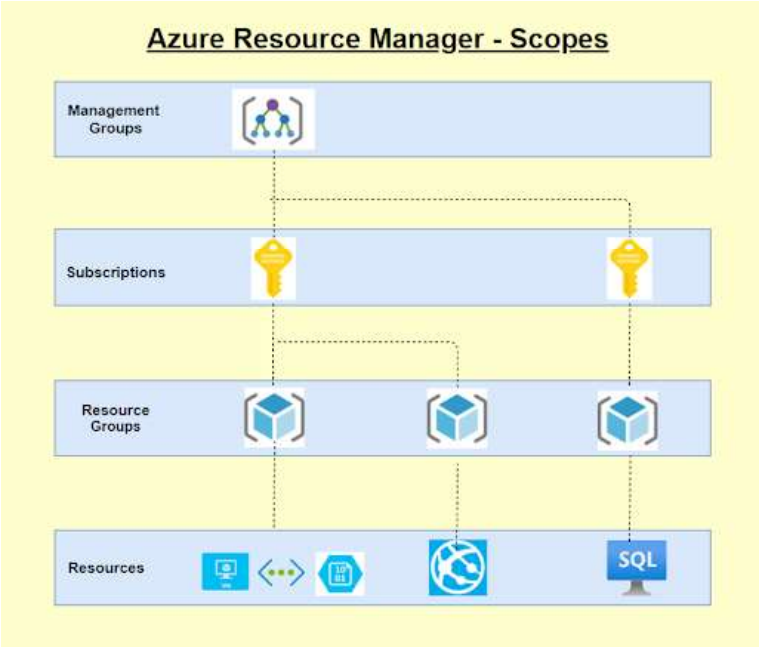
3. Scope

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:

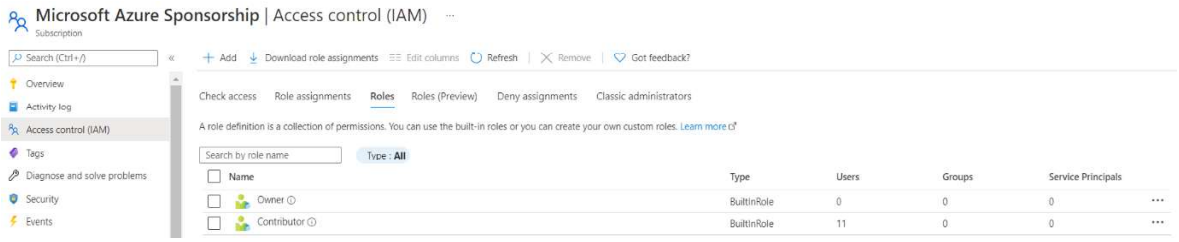
a. **Management group**
b. **Subscription**
c. **Resource group**
d. **Resource**

- 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

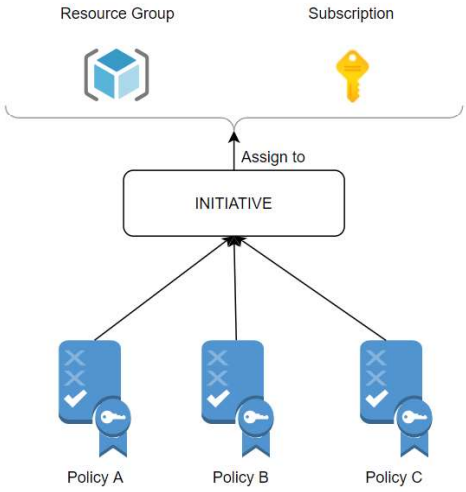
Earlier RBAC had only allowed, but now it can be denied assignments also. If there is a deny assignment, the user will be blocked from doing the action. Deny assignments take precedence over role assignments where a given user has both allow and deny but deny will be the end action.

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.

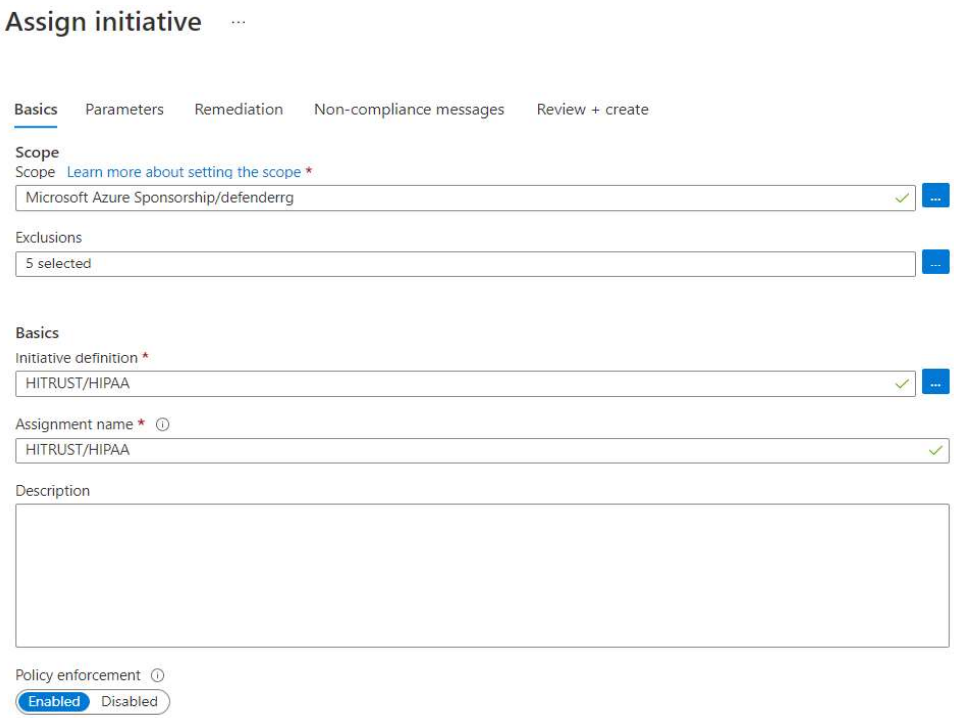
Step 2: Policy Initiative

- 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.

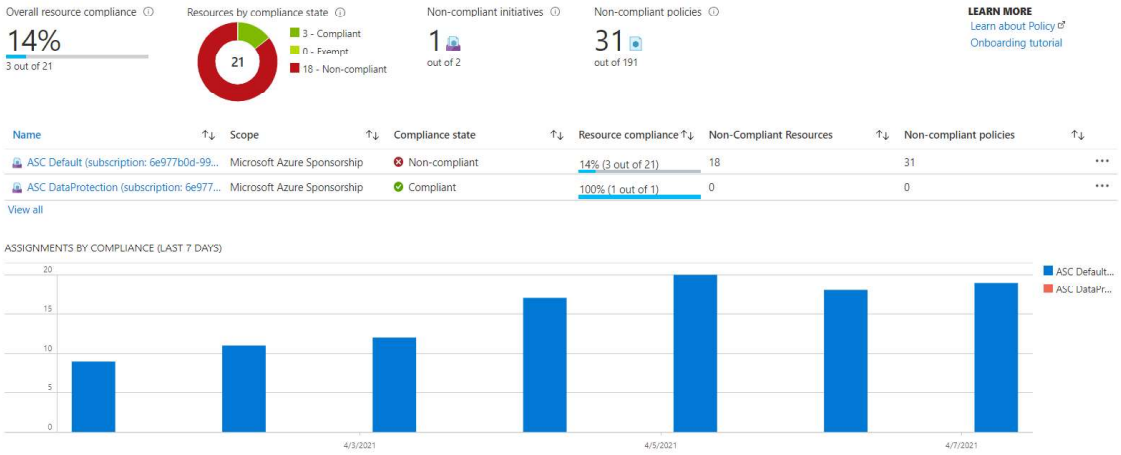
- Here we also select the scope. We can assign to an entire subscription or resource groups within a subscription.
- Also, we could exclude resources. Let's say we selected subscription 1 but we want to exclude one Resource group. Then we use the exclusions. In the example below, 5 resources are excluded 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.

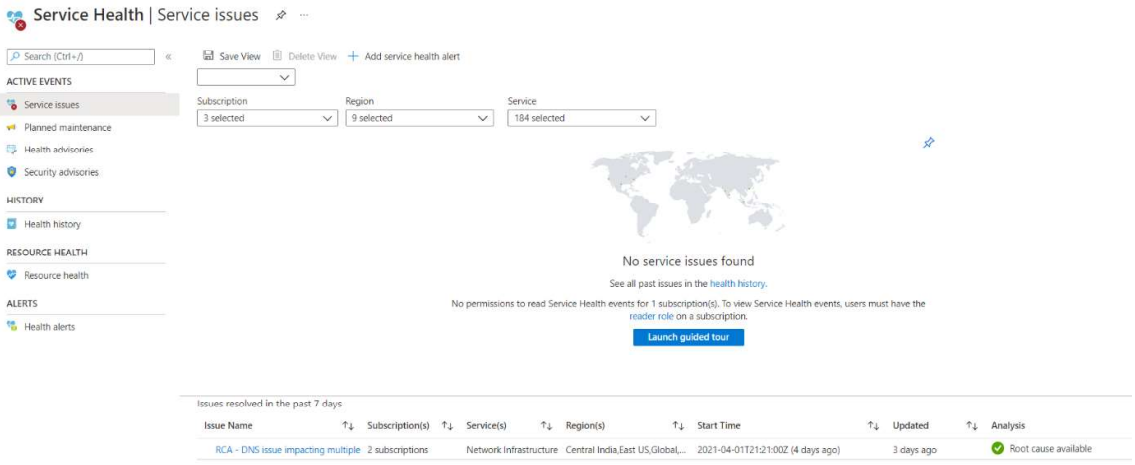
Azure Service Health

- 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:

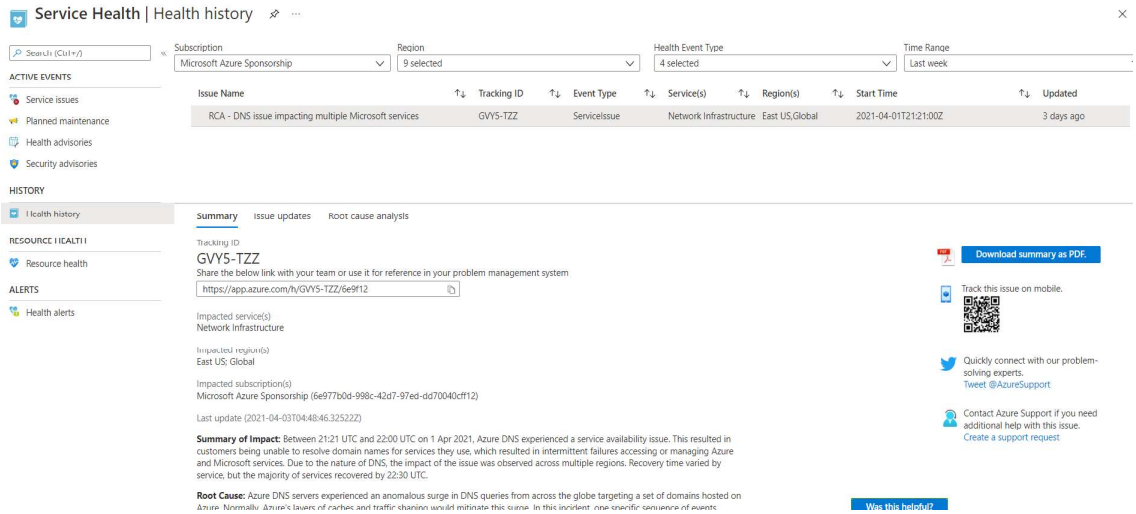
Service Issues

- 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.



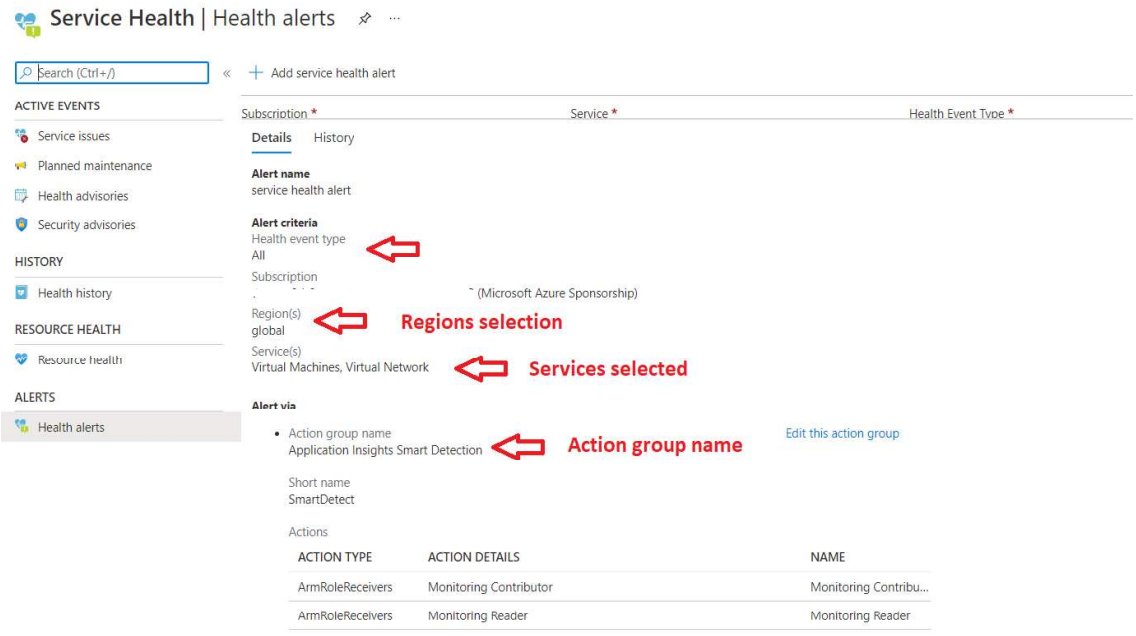
Health History

- 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.

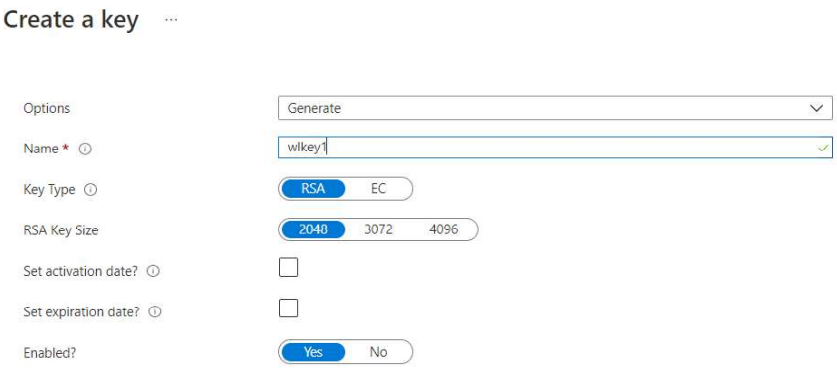
Azure Key Vault is a **PaaS platform in Azure. It** is integrated into Azure Active Directory. We can store secrets, Keys, and certifications and have multiple versions stored. We have audit logs as a feature. Azure Key vault is **FIPS 140-2** compliant.

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

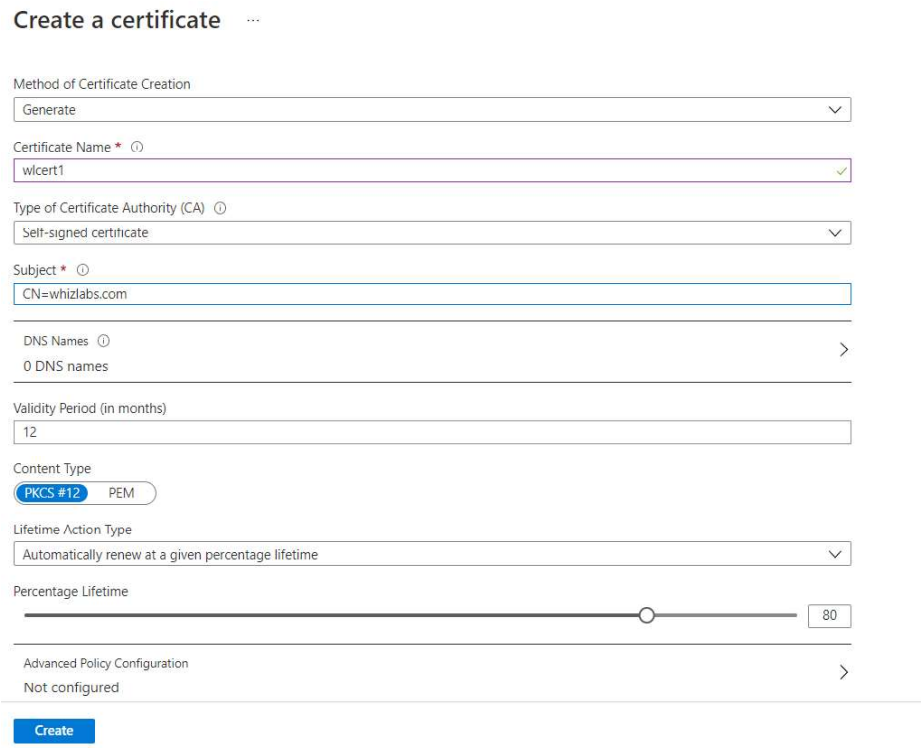
Keys

- 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.



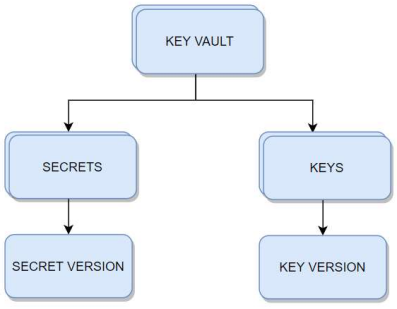
Audit

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.



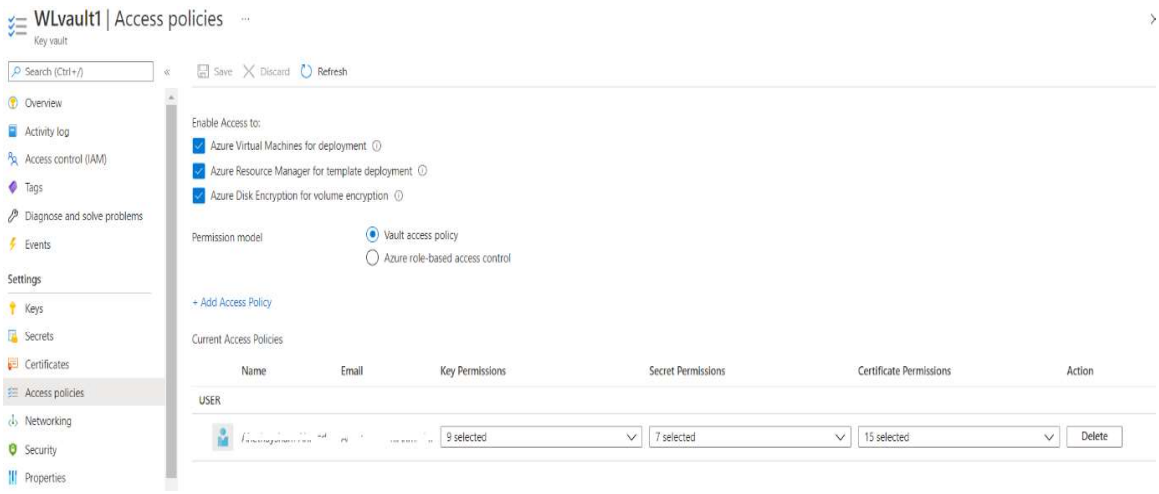
Access Policy

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

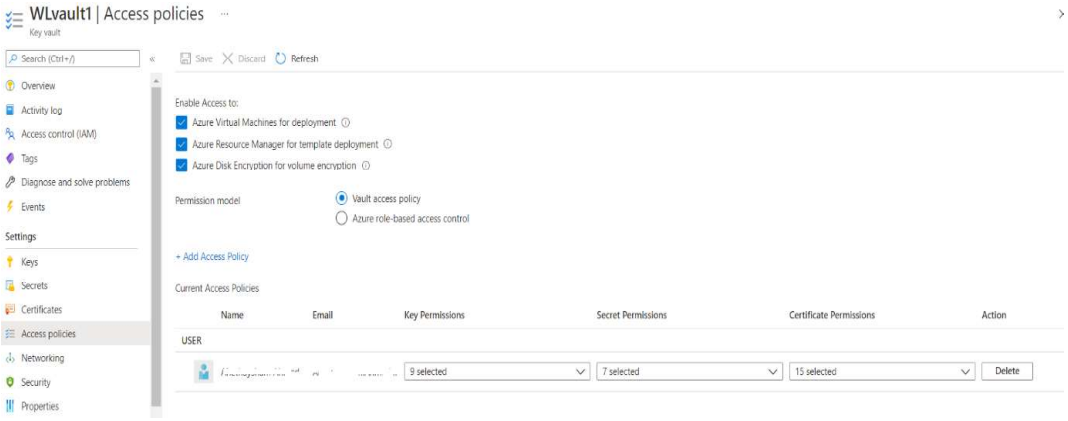
iv. This is controlled by RBAC only

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.

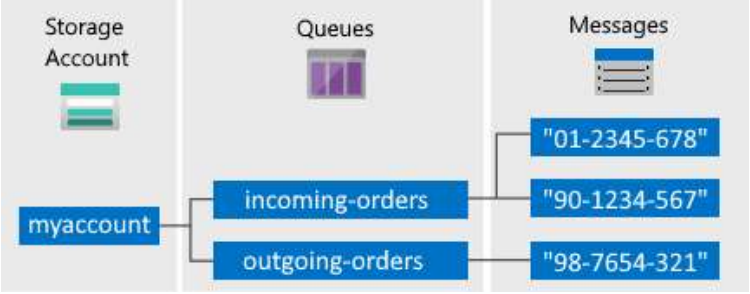
Azure Queue Storage

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.

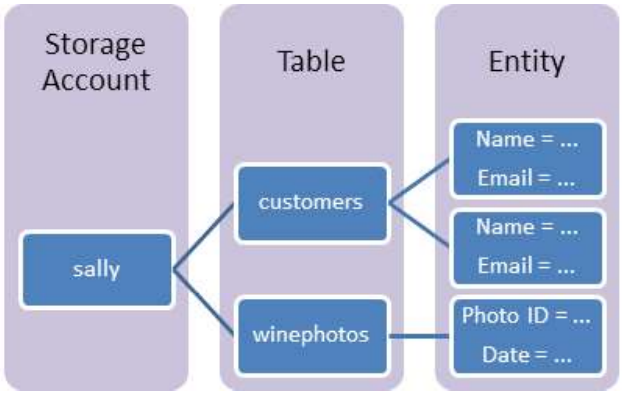


Table Storage architecture

- **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

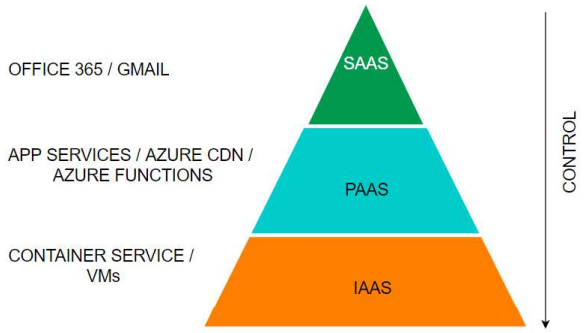
- **What are the retrieval options?**
  - There are two options.
    - *Standard Priority (Default)* – up to 15 hours
    - *High Priority (Max 10 GB)* – less than 1 hour

- **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
   ```

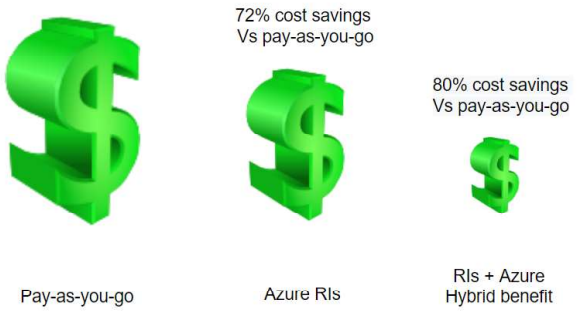
   Else you need to deallocate the VM, which will allow you to use any size. You need to deallocate, resize and start a VM.

   ```
   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%)

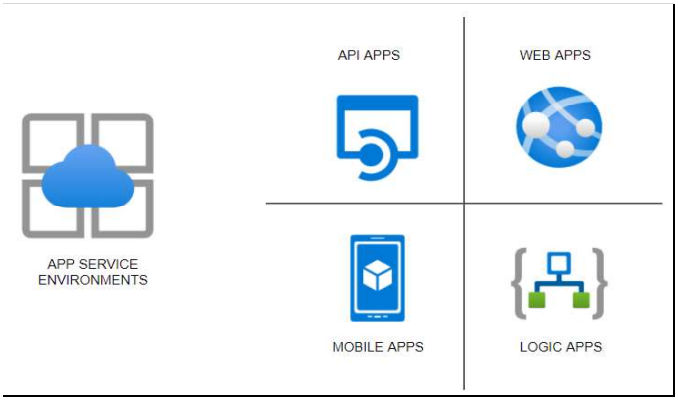
FAQs

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