**Virtual Machines**

Let's go through some important points when it comes the topics discussed in this section

**1. Choosing the size for the virtual machine** - Remember that the size of the virtual machine plays an important role in both the cost and performance you get for your virtual machine.

If you are looking at the Free services provided by Azure - <https://azure.microsoft.com/en-us/free/>

Here you get 750 hours of compute ONLY free per month ONLY for the **B1S VM Size**

So if you look at the sizes for Azure virtual machines, this corresponds to just getting 1 vCPU and 1GiB of RAM which is quite less to hosting a workload on the server. Hence please keep this in mind. If you need better performance, you will have to choose a virtual machine size that is outside the boundaries of the Free service.

**2. Costing for a virtual machine**- Remember that costing for a virtual virtual machine depends on several factors, such as time as it runs for, the region used for hosting the virtual machine, the underlying operating system.

If you don't need the virtual machine running for a certain duration of time, you can always go ahead and stop the virtual machine. This will ensure you don't get charged for the compute cost of the virtual machine.

To ensure you don't get charged for the compute costs for the virtual machine, the virtual machine must be in the Stopped (deallocated) state.

Also keep a note that you will still be charged for other aspects of the virtual machine ( such as the disks attached to the virtual machine) , even if the virtual machine is stopped.

**Availability Sets**

When you host your virtual machines in Azure, you sometimes need to cater to the following

1. An unplanned event wherein the underlying infrastructure fails unexpectedly. The failures could be attributed to network failures , local disk failures or even rack failures.
2. Planned maintenance events , wherein Microsoft needs to make planned updates to the underlying physical environment. In such cases , a reboot might be required on your virtual machine.

You can increase the availability of your application by making use of availability sets. Each virtual machine that is assigned to the availability set is assigned a separate fault and update domain.

**Fault domains** are used to define the group of virtual machines that share a common source and network switch. You can have up to 3 fault domains.

**Update domains** are used to group virtual machines and physical hardware that can be rebooted at the same time. You can have up to 20 update domains.

If you deploy two or more virtual machines in an Availability set, you will get a guarantee of virtual machine connectivity to at least one virtual machine 99.95% of the time.

**Availability Zones**

1. This features help provides better availability for your application by protecting them from datacenter failures.

2. Each Availability zone is a unique physical location in an Azure region.

3. Each zone comprises of one or more data centers that has independent power, cooling, and networking

4. Hence the physical separation of the Availability Zones helps protect applications against data center failures

5. Using Availability Zones, you can be guaranteed an availability of 99.99% for your virtual machines. You need to ensure that you have 2 or more virtual machines running across multiple availability zones

An interesting fact - Does it cost more to use an Availability Zone. Well no, you don't get charged separately for the use of Availability Zones.

Below is an excerpt from the Microsoft documentation

Reference - <https://docs.microsoft.com/en-us/azure/availability-zones/az-overview>

**Azure Virtual Network**

The Azure Virtual Network service is used to define an isolated network in Azure. The virtual network can then be used to host your resources such as Azure virtual machines.

The Azure virtual network gets assigned an address space which you specify when you create an Azure virtual network

You can then add subnets to your Azure virtual network. This helps divide your network into more logical segments.

An example is shown below of having multiple subnets. You could have one subnet named SubnetA in the virtual network to host your Web servers and another subnet to host the Database servers.

When you create a virtual machine in a virtual network, the virtual machine gets a Private IP address from the address space of the subnet is it launched in.

**Network Security Groups**

These are used to filter network traffic to and from Azure resources in an Azure virtual network.

A network security group is attached to the network interface attached to the virtual machine.

* A network security group consists of Inbound rules that are used to control the traffic inbound into a virtual machine
* By default all traffic into a virtual machine is DENIED.
* You have explicitly add rules to allow traffic into a virtual machine
* There are also outbound rules to control the traffic flowing out of the virtual machine. By default all traffic outbound onto the Internet is allowed.

**Virtual Network Peering**

* Virtual Network Peering is used to connect two Azure virtual networks together via the backbone network.
* Azure supports connecting two virtual networks located in the same region or networks located across regions.
* Once you enable virtual network peering between two virtual networks, the virtual machines can then communicate via their private IP addresses across the peering connection.
* You can also peer virtual networks that are located across different subscriptions.
* The virtual networks can't have overlapping CIDR blocks.

**Point-to-Site VPN Connection**

A Point-to-Site VPN connection is used to establish a secure connection between multiple client machines and an Azure virtual network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario

Image reference -<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

To implement a Point to Site VPN connection, you need to create a VPN Gateway in Azure.

**Site-to-Site VPN Connection**

A Site-to-Site VPN connection is used to establish a secure connection between an on-premise network and an Azure network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario

Image reference - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

* On the on-premise side, you need to have a VPN device that can route traffic via the Internet onto the VPN gateway in Azure. The VPN device can be a hardware device like a Cisco router or a software device ( e.g Windows Server 2016 running Routing and Remote services). The VPN device needs to have a publically routable IP address.
* The subnets in your on-premise network must not overlap with the subnets in your Azure virtual network
* The Site-to-Site VPN connection uses an IPSec tunnel to encrypt the traffic.
* The VPN gateway resource you create in Azure is used to route encrypted traffic between your on-premise data center and your Azure virtual network.

**Azure Storage Accounts**

Types of storage accounts

* **General-purpose v2 accounts**– This is recommended for most scenarios. This storage account type provides the blob, file , queue and table service.
* **General-purpose v1 accounts**– This also provides the blob, file , queue and table service, but is the older version of this account type.
* **BlockBlobStorage accounts**– This is specifically when you want premium performance for storing block or append blobs.
* **FileStorage accounts**– This is specifically when you want premium performance for file-only storage.
* **BlobStorage accounts**– This is a legacy storage account. Use General-purpose v2 account as much as possible.

The most common type of storage account is the General Purpose v2 storage account.

Use case scenarios for the different services in a General Purpose v2 storage account

**Blob service**

* This is object storage for the cloud.
* Here you can store massive amounts of unstructured data on the cloud.
* This is highly recommended when you want to store images, documents, video and audio files.
* Within the blob service, you create a container that is used to store the blob objects.

There are three different types of blobs

**Block blobs** – This is used for storing text and binary data.

**Append blobs** – This is ideal for logging data.

**Page blobs** – This is used to store virtual hard disk files for Azure virtual machines.

To use the Blob service you have to first create a container and then upload the blobs or objects into the container.

When you upload an object or blob to the service, each bob gets a unique URL which you can access if you are assigned the right permissions

**File service**- Use this service if you need to store files that need to be accessed by machines using the SMB (Server Message Block) protocol

In the File service, you can first go ahead and create a file share.

You can then mount this file share from different machines. You can't mount drives with the Blob service.

**Table service** - Use this if you want to store NoSQL data or table like data.

It's easy and simple to create a table and add data from the Azure portal itself.

**Queue service** - Use this if you want to exchange messages between components of your application

**Azure Storage Accounts - Replication**

There are different replication techniques available to make your data highly available.

The different replication techniques available

1. *Locally-redundant storage (LRS)*- Here data is replicated synchronously three times within a physical location in the primary region.
2. *Zone-redundant storage (ZRS)*- Here data is replicated synchronously across three Azure availability zones in the primary region. This is good when you want to have data present even in the event of a data center failure.
3. *Geo-redundant storage (GRS)*- Here data is replicated synchronously three times in the primary region, then replicated asynchronously to the secondary region.
4. *Read access Geo-redundant storage (RA-GRS)*- Here data is replicated synchronously three times in the primary region, then replicated asynchronously to the secondary region. Here the data in the secondary region is also available for read-only purposes.

**Azure Storage Accounts - Access tiers**

Access tiers help you optimize the storage costs and access costs for your data. The different access tiers are

**1. Hot**– This is optimized for storing data that is accessed frequently. This can be set at the account level.

**2. Cool**– This is optimized for storing data that is infrequently accessed and stored for at least 30 days. This can be set at the account level.

**Note:- For the Cool Access tier , the storage costs are lower than the Hot tier. But the access costs are higher than the Hot access tier.**

**3. Archive tier** - This is optimized for storing data that is rarely accessed and stored for at least 180 days. This can be set only at the blob level.

**Note:- When a blob is in the archive tier, you can’t access the blob. You have to rehydrate the blob first before it can be accessed.**

**Also the storage costs are the least when it comes to the Archive access tier. But the access costs are the highest.**

**Azure SQL Database (Platform as a service)**

This is a service that allows you to create a managed Microsoft SQL Server database on the cloud. The advantages of using this service

1. You don't have to manage the underlying infrastructure. This is managed by Azure.
2. You have a variety of purchasing options
3. You have automated backups. This reduces the burden of managing backups.
4. It gives you a service level agreement of 99.99%

If you need to have more control over the database engine, then consider installing the SQL Server engine on an Azure virtual machine.

**Azure Synapse Analytics**

This was formerly known as Azure SQL Data warehouse.

This service is used for enterprise data warehousing and Big Data Analytics

When you want to perform analysis on a large data set , consider using this service.

Below is a snapshot from the Microsoft documentation on where this tool fits in the picture of Big Data

**Azure Cosmos DB**

This is a data store that companies can opt for , when they want to get low latency access to their data and they want high availability for their data.

It is a multi-model database. This means you can choose from a variety of options when it comes to what type of data you want to store in the account.

**High Availability**

This refers to technologies that can be used to minimize IT disruptions by ensuring applications and infrastructure is made fault-tolerant.

Let's say that you had the following architecture for your application. Your application is hosted on a single virtual machine.

What happens if the virtual machine goes down for any reason, your application would not be available.

To make your application more redundant and more tolerant to failures, why not host your application on a collection of servers

Here even if one machine were to go down , you would still have the other one available. This makes your application more tolerant to infrastructure level failures.

You can also increase the availability for your virtual machines by distributing them across **Availability Zones** or **Availability Sets**.

**Disaster Recovery**

This refers to the concept of minimizing IT disruptions by recovering them to another data center that could be located hundreds to miles away from the original data center hosting your application.

The following architecture diagram is an example of implementing disaster recovery

Here your application is running on virtual machines in the West US region. Here the users are accessing your application.

At the same time, you might have the application hosted in another region (East US). The application might be in a shutdown state. This is only meant to be running if the primary region goes down for any reason.

Not lets say there is a disaster in the West US region and all the data centers go down.

To minimize any disruption to your users , the requests to the application could now be redirected to the application in the East US region. So now you would start the application here and make sure all requests are routed to the secondary region.

**Elasticity**

Elasticity refers to the concept of how flexible your architecture can scale based on demand.

For virtual machines , you can increase or decrease the size of the virtual machine at any point in time.

**Cloud Service Model**

The different cloud service models

**Infrastructure as a service (IaaS)**

* An example is the Azure virtual machine service.
* Here you don’t need to manage the underlying infrastructure.
* The physical servers and storage is managed for you.
* This helps remove the capital expense and reduces ongoing cost.
* The Virtual Machine also has an SLA. To achieve that SLA for any on-premise server would require a lot of work.
* Infrastructure cloud services also allow you to scale based on demand.

**Platform as a service**

* An example is the Azure SQL Database service or the Azure Web App service.
* Here you don’t need to manage the infrastructure or even the underlying operating system and platform components.
* You can just start hosting your data or your web application.
* Reduces development time.
* You can use an array of database technologies available in the case of Azure.
* All of these services use a Pay-as-you-go model.

**Software as a service**

* An example is Microsoft Office 365.
* Here you don’t need to manage the infrastructure or even the underlying operating system, platform components or even the software.
* Here you just start directly using the software.
* You can access your application data from anywhere.
* You don’t have the headache of managing anything.

**Cloud Models**

**Public Cloud**

* These are services that are offered over the public internet.
* It’s available to anybody who wants to use them. Users then pay based on service they use.
* Here all the servers and storage is managed by the cloud provider

**Advantages of the Public Cloud**

* No need for a capital investment – You normally don’t pay any money upfront to use a cloud service. Most of the services are based on a pay-as-you-go model.
* You don’t need to manage the underlying physical infrastructure. Hence on-going maintenance costs are also reduced.
* Cloud providers such as Azure have data centers located at different regions across the world.
* You can quickly provision resources on the cloud. It allows you to get up and running in no time.

**Private Cloud**

* These are set of services that are normally only used by users of a business or organization.
* The private cloud could be hosted either on the company’s on-premise environment. Or it could be provided by a third-party service provider.

**Advantages of the Private Cloud**

* The business has complete control over the environment.
* They can implement their own security protocols at every layer to secure the environment.
* The data held in the environment is in complete control by the business.

**Hybrid Cloud**

* This is a combination of both the public and private cloud.
* It allows data and applications to be shared across both cloud environments.

**Advantages of the Hybrid Cloud**

* Businesses can still leverage their existing on-premise environment. This is important if they have already made a substantial investment in getting their environment in place.
* They can keep data which needs to be secured by their standards in their on-premise environment.
* They can extend their infrastructure to the cloud without making a further investment.
* They can move workloads to the cloud gradually.

**Azure App Service**

* This is an HTTP-based service that allows you to host web applications, REST API's and mobile back ends. You can develop a program in programming languages such as .NET, .NET Core, Java, Ruby, Node.js, PHP and Python.
* Here you don't need to manage the underlying infrastructure. It allows you to focus on code development.
* Each App service needs to be associated with an App Service Plan.
* Each App service plan has an associated cost per month and also has specific features based on the plan you choose.

**Virtual Machine Scale Sets**

* This service allows you to create and manage a group of identical load balanced virtual machines.
* Here the number of Virtual Machine instances in the scale set can scale based on demand
* This is the best service if you want to add scalability to your application

**Azure Load Balancer**

The Azure Load balancer is used to distribute incoming network traffic to a backend group of servers.

This service helps increase the availability of your entire application architecture

Here the Load Balancer would take the incoming requests from the users and direct the requests to virtual machines running in an Azure virtual network.

If you have a web application running on the backend virtual machines, the requests would be distributed across the virtual machines by the Azure Load Balancer.

**Other tools to access Azure resources**

You can use other tools to access and work with Azure resources

* You can use PowerShell which can work on Windows, macOS and Linux
* You can use the Azure command line interface which can work on Windows, macOS and Linux
* You can use Azure cloud shell from the browser, which can then work on any operating system which has browser support

**Azure Functions**

* This service allows you to run small pieces of code as functions.
* Here you just develop and upload the code to an Azure Function.
* You only get billed for the amount of time the code is run.
* You can use a variety of programming languages in Azure Functions.
* C#, Java , JavaScript, PowerShell and Python.
* You can use libraries by using NuGet and NPM packages.

**Pricing plans available for Azure Functions**

**Consumption Plan**– Here you only pay for the time the code runs.

**App Service Plan** – If you already have an App Service plan that runs a web application, you can reuse the same plan to run Azure Functions. This would save on cost if you already have an App Service Plan in place.

**Premium Plan** – Here you get a number of pre-warmed instances that are always online and ready to run your functions. The plan also automatically adds more compute when required.

You can also invoke your functions via various triggers

**Azure Logic Apps**

This is a cloud service that helps you schedule, automate and orchestrate tasks , business processes and workflows.

**How it works**

* You first design a workflow in Azure Logic Apps
* Each workflow starts with a trigger.
* The trigger is fired via a specific event
* When the trigger is fired , the Logic App engine creates a logic app instance that runs the workflow.

**Connectors for Azure Logic Apps**

* These connectors provide easy access to event, data and actions that are sent from external applications, services , systems or platforms.
* You have built-in connectors that can connect to Azure services such as Azure functions, Azure API Apps etc.
* You have Managed connectors that can connect to platforms such as Office 365, Microsoft Dynamics.

**Azure Traffic Manager**

The Azure Traffic Manager service is a DNS-based traffic load balancer that distributes traffic across services that are distributed across different Azure regions.

The Traffic Manager service is used to direct client requests to the most appropriate service endpoint that is based on a traffic-routing method and the health of the endpoints.

The different traffic routing methods available for the Azure Traffic Manager are

* Priority – Route traffic to another endpoint in case the primary fails.
* Weighted – Route traffic to different endpoints based on weight.
* Performance - you want end users to use the "closest" endpoint in terms of the lowest network latency.
* Geographic - geographic location their DNS query originates from.
* Multivalue – Here different endpoints are sent to the client. The client then selects the endpoint to send the request to.
* Subnet – This maps a set of end-user IP address ranges to a specific endpoint within a Traffic Manager profile.

Below is an example of the Priority routing method that can be used with the Azure Traffic Manager service

Here we are assuming that a company has similar web applications , both are running using the Azure Web App service. One web application is running in the East US Region and the other is running in the West US Region.

1. Here we create a Traffic Manager profile and create two endpoints. Each endpoint points to each Azure Web app respectively. We assign a priority of 1 to the service endpoint attached to the Azure Web App running in the East US region and  a priority of 2 to the other service endpoint.

1. Here users would make requests to the Traffic Manager service.

2. The requests could be initially be directed to an Azure Web App located in the East US region , since there is a priority of 1 to the service endpoint attached to this endpoint.

3. Now let's say there is an issue with the web application running in the East US region, Azure Traffic Manager would then understand that there is an issue with the web application running in this region.

It would then start redirecting user requests to the second endpoint which has the Priority of 2.

Hence over here you are adding a higher availability to your architecture by ensuring that user requests are always adhered to by redirecting requests if the primary service fails for any reason.

If you use the Weighted Routing method , you can actually load balance requests across multiple service endpoints

Over here , users requests would be directed or load balanced across both web applications running in different regions.

In the Performance routing method as shown below, users will be directed based on the least latency of an endpoint.

And then we have the Geographic routing method wherein users would be directed to an endpoint based on their geographic location

**Monitoring in Azure**

For all monitoring aspects you can head over to Azure Monitor.

1. You can use the Metrics section to view the entire metrics for your Azure resources

2. You can use the Activity Log feature to look at all the control plane activities. So if someone has shutdown a virtual machine, you would be able to see who shutdown the virtual machine in the Activity Logs.

3. You can also view any service related issues in the Service health module of Azure Monitor

4. You can also create a service health alert in Azure Service Health

5. You can also direct logs from various resources such as Azure virtual machines onto the Logs section. Here you have to create a Log Analytics workspace to store the logs

**Azure Kuberntes**

**What is Kubernetes?**

* This is an open-source platform that is used to managing containerized workloads.
* Kubernetes is able to provide a DNS name to your container.
* If there is a high load on your containers , Kubernetes can load balance and distribute network traffic.
* Kubernetes can also restart containers that fail.
* It can be used to replace or kill containers.
* It also helps to store and manage sensitive information such as passwords, OAuth tokens and ssh keys

**What is Azure Kubernetes?**

* Fully managed Kubernetes service on Azure.
* Makes it easy to deploy and manage containerized applications.
* It helps to remove the burden of managing the underlying infrastructure for the Kubernetes deployment.

**Azure Content Delivery Network**

This is an ideal service to use for your web applications. If you need content to be distributed to users across the world for your web sites , then its ideal to use the Azure Content Delivery Network Service

* Here the users are directed on various Edge servers by the Content Delivery Network service.
* The Edge servers will get the content from your web site and also cache frequently accessed content.
* The Edge servers are located across the world , so it gives all users a seamless experience when it comes to accessing your web site.

**Azure Advisor**

Use this tool to get various recommendations on aspects such as Cost, Security and High Availability.

#### ****Application Insights****

**Points on this service**

* Application Performance Management service for web developers.
* You can use this tool to monitor your applications.
* It can help developers detect anomalies in the application.
* It can help diagnose issues.
* It can also help understand how users use your application.
* It also helps you improve performance and usability of your application.

**How does it work**

* You install a small instrumentation package within your application.
* You can see the statistics of your application locally in Visual Studio as you run your application.
* You can also use the Application Insights resource in Azure to monitor your application.

**What are the different aspects monitored by Application Insights**

* Request rates, the response times and failure rates – This is done at the page level.
* Exception recorded by your application.
* Page views and their load performance as reported from the user’s browser.
* User and session counts.
* Performance counters of the underlying Windows or Linux Machines.
* Diagnostic trace logs from your application.
* Any custom events or metrics that the developer writes themselves in the code.

#### ****Azure Cognitive services****

Azure Cognitive Services are API’s , SDK’s and services available for helping developers building intelligent applications.

Here the developer does not need to have any AI or data science skills.

There are many services available for developers to make use of

**Computer Vision**– This helps developers process images and return information. You just supply the image, and the service can help identify the image.

* This service can detect objects, help provide categories for the image.
* It can also detect color , faces , help describe an image.
* It can also extract text from images.
* It can also help moderate content in images.

**Face API**– This can be used to detect, recognize and analyze human faces in images.

* It can also help find similar faces from a set of images.
* It can also help identify a detected face against a database of people.

**Speech services**

* You can use the Speech-to-Text service to translate speech to text.
* You can also generate synthesized speech from text using Text-to-Speech.

#### ****Azure Machine Learning****

* Machine learning is the process that enables computers to use existing data to forecast future behaviors , outcomes and trends.
* Here the computers don’t need to be programmed on how to learn.
* Azure Machine Learning gives you a cloud-based environment for preparing data, train the data, testing, deploying and managing machine learning models.
* You get a visual interface which can be used to drag and drop modules to build experiments and deploy models.
* **Machine Learning Studio** – This is a drag-and-drop visual workspace which you can use to build, test and deploy machine learning solutions without the need of writing any sort of code.
* This tool has prebuilt and preconfigured machine learning algorithms.

#### ****Azure HDInsight****

* This is a cloud distribution of Hadoop based components.
* Azure HDInsight allows you to process large amounts of data.
* You can use HDInsight for a variety of big data processing scenarios such as Data warehousing , Batch processing and for Data science as well.
* You can create different types of clusters – Apache Hadoop, Apache Spark, Apache Hbase.
* HDInsight also supports a host of programming languages such as Java, Python, .Net and Go.

#### ****Azure DevOps****

* This is a complete set of tools that can be used to help teams to plan work, collaborate on code development and build and deploy applications.
* Azure DevOps have the following services in place
* **Azure Repos**– This allows you to host Git repositories or use Team Foundation Version Control.
* **Azure Pipelines**– This provides build and release services for continuous integration and release.
* **Azure Boards**– This helps to plan and track work items.
* **Azure Test Plans**– This provides tools for testing of applications.
* **Azure Artifacts**– This allows teams to share Maven, npm and NuGet packages from public and private sources.

#### ****Azure DevTest Labs****

* This service allows developers to efficiently self-manage virtual machines and PaaS resources without the need to wait for approvals.
* The DevTest Labs can be used to create labs consisting of pre-configured bases or Azure Resource Manager templates.
* With DevTest Labs, you can quickly provision Windows and Linux based environment through the use of reusable templates and artifacts.
* You can easily create load testing environments and create environments for training and demos.
* This service also helps in optimizing costs through the following features
* Here you can set an auto-shutdown and auto-start schedules for virtual machines.
* You can set policies on the number of virtual machines users can create.
* You can set policies on the size of the virtual machine.
* You can track costs.

**Azure Active Directory**

This is your identity system in Azure. Here you can define users and groups and provide them permissions to your resources.

Here you can also define external users who can have access to resources in Azure.

**Multi-Factor Authentication**

You can also enable Multi-Factor authentication for users. Here users need to use an additional mechanism in addition to the user name and password to log into Azure.

You can also make use of **Conditional Access policies** to create conditions to allow or deny users to log into Azure.

**Other security related aspects**

**GDPR (General Data Protection Regulation)**

* This is a set of rules that helps EU citizens have more control over their personal data
* Under this compliance schema, organizations have to ensure that personal data is gathered legally and under strict conditions.
* Also organizations have to manage the data in such a way that it is protected from misuse or exploitation.

**ISO (International Organization for Standardization)**

* This is an international body that is responsible for setting international standards.
* This is an independent, non-government organization.
* It consists of members from around 160+ member countries.

**NIST (National Institute of Standards and Technology)**

* This is an organization which looks at U.S. innovation.
* They do this by looking at measurement of science, standards and technology.

**Azure Blueprints**

* This is a service that allows you to define a repeatable set of Azure resources.
* The definition of the Azure resources can adhere to an organization’s standards, patterns and requirements.
* Using blueprints , you can orchestrate the deployment of resources such as role assignments, policy assignments, Azure resource manager templates and resource groups.
* Some differences between Azure blueprints and resource manager templates
* You can use blueprints to upgrade several subscriptions at once .
* The relationship between the blueprint definition and the blueprint assignment is reserved.

**Azure Security Center**

* This is an infrastructure security management system.
* You can use this tool to improve the security of your Azure based resources and on-premise resources as well.
* Azure Security Center has in-built support for services such as Azure virtual machines , Function Apps, Azure SQL Server databases.
* You can also allow Azure Security Center to give recommendations on what to do for on-premise Windows and Linux servers.
* On these servers, you need to ensure you install the Microsoft Monitoring agent.
* This service also helps detect and prevent threats at an Infrastructure layer

**Azure AD Identity Protection**

* This is a service that can help detect suspicious actions related to user identities
* This helps add more security to the sign-ins to your Azure AD Account.
* This service can help detect the following

1. Users with leaked credentials
2. Sign-ins from anonymous IP addresses
3. Sign-ins from infected devices
4. Sign-ins from IP addresses with suspicious activity
5. Sign-ins from unfamiliar locations
6. Impossible travel to atypical locations

**Azure AD Privileged Identity Management**

* This is a service that can help manage, control and monitor access to important resources in your organization.
* With this service, you can provide just-in-time privileged access to Azure AD and Azure resources.
* Provide time-bound access to resources using start and end dates.
* Enforce multi-factor authentication to activate any role.
* Get notifications when privileged roles are activated.
* Conduct access reviews to ensure users still require the roles.

#### ****Azure Firewall****

* This is a managed, cloud-based network security service that can be used to protect your network resources.
* It has features such as Threat intelligence – This can filter incoming requests and alert or deny traffic from/to malicious IP addresses and domains.
* The firewall itself has built-in high availability.
* It can scale automatically based on network traffic flows.

Here you can ensure that all traffic from machines in an Azure virtual network flows via the Azure Firewall service.

#### ****Azure DDoS protection****

* This service helps protect against Distributed denial of service attacks.
* This is probably the biggest security concern for companies when they expose their applications to the Internet.
* You have 2 plans for Azure DDoS protection.

**Basic** – This is automatically enabled. This continuously monitors traffic in real time and looks at mitigation of common network-level attacks.

**Standard** – This is a paid plan. But you get many benefits

–Here you can get real time attack metrics and diagnostic logs via Azure Monitor

–You can get help from DDoS Experts during a live attack

#### ****Azure Information protection****

* This is a solution that can help an organization classify and protect its documents and email by applying labels.
* The labels can be applied automatically by administrators through the use of rules and conditions.
* The labels can use visual markers on documents to tell the user the classification of the document

#### ****Azure Advanced Threat Protection****

* This is a cloud-based security tool that can be used to identify, detect and investigate advanced threats, compromised identities.
* This service can be used to protect identities and credentials stored in Active Directory.
* When monitoring your on-premise Active Directory domain controllers, you need to install an Azure ATP sensor on the domain controller.
* It can be used to identify and investigate suspicious user activities and advanced attacks.

#### ****Azure Key Vault****

* Helps you perform Secrets management – Here you can securely store your tokens, passwords , certificates , API keys and other secrets
* You can use this service to create encryption keys. You can then use these encryptions keys to encrypt your data.
* You can also easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates
* All of the secrets and keys are safeguarded by Azure, using industry-standard algorithms, key lengths, and hardware security modules (HSMs).
* You can also monitor all the key vault activity by enabling logging. The logs can be sent to an Azure storage account, to an event hub or to Azure Monitor logs.

#### ****Azure Policies****

* This service can be used to create, assign and manage policies.
* You can use these policies to ensure that resources in your Azure account remain compliant with corporate standards and service level agreements.
* You can use in-built policies or even define your own policies

#### ****Role-based access control****

* This can be used to assign access to resources in Azure.
* For example if you wanted to give access to a user to manage virtual machines in your subscription, you can use role based access control

Roles can be accessed at different scopes - Subscription, Resource groups and resources

Reference - <https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>

#### ****Microsoft Privacy statement****

To understand the data that gets collected from Microsoft when you use their products, you can refer to the Microsoft Privacy statement

<https://privacy.microsoft.com/en-us/privacystatement>

#### ****Azure services lifecycle****

* Remember that Azure keeps on updating their services from time to time. They will add new features of even deploy newer services from time to time.

Refer to the link for all updates to Azure services - <https://azure.microsoft.com/en-us/updates/>

* For services in public preview , you can actually view them from the Azure portal itself. These services are available for review for all customers.
* Note that it is not advisable to deploy resources based on these services to your production environment because there would  be no SLA attached to these services.
* You can view services in private preview - Here you need to request Microsoft to preview these services.
* Also keep a note that any services that go out of support , Microsoft will give you at least 12 months of prior notification

You can view these terms via the following link

<https://support.microsoft.com/en-us/help/30881>

#### ****Azure support plans****

This is very important from the exam perspective

This is very important from an exam perspective.

Please refer to the following link to see all of the support plan options

<https://azure.microsoft.com/en-us/support/plans/>

#### ****Azure Service Level Agreement****

Azure normally gives around 99.9% SLA for most of their services

An example for the SLA for Active Directory is given below

Please go to the following link to view the SLA for the various Azure services

<https://azure.microsoft.com/en-us/support/legal/sla/summary/>

#### ****Azure Total Cost of Ownership****

To get an idea of the possible total expenses for moving your resources to Azure, you can make use of the Azure Total Cost of

Ownership calculator

Use the following link to work with the TCO calculator - <https://azure.microsoft.com/en-us/pricing/tco/calculator/>