**Azure Fundamentals**

This document is all about learning the details of Azure platform and cloud computing. This will help us to understand more aspects about Azure such as:-

1. Learn cloud concepts like Cost effective, Scalable, Elastic, Available Globally, Reliable or Fault tolerance, Current, Secure.
2. Benefits of cloud computing and how it saves time and money.
3. Understand basic strategies for transitioning to Azure cloud.
4. Understand the services provided by Azure like compute, network, storage and security.

Real life example -> Cloud computing can be compared to the way in which we use electricity. We only pay for what we use. While switching on a light bulb, then we are paying only for the amount of electricity we use and we do not have to bother about all the other aspects of how electricity is being generated, transported, stored etc.

**Cloud Computing** -> Cloud computing is the process of renting resources from a cloud provider. The major cloud providers are Microsoft, Amazon and Google. All these cloud providers provide a variety of cloud services. The core functionality of the main services of different cloud providers would remain the same. For example, while buying a PC we would buy an 8 gb ram and latest processor for smooth working, but if our work load increases then we would have to constantly spend money and update the PC components. Cloud provides us the flexibility to buy what we only need and once the need is over we can return the same and we only have to pay for what we use.

Major cloud providers -> Microsoft, Amazon, Google.

Cloud service categories -> IaaS, PaaS, SaaS

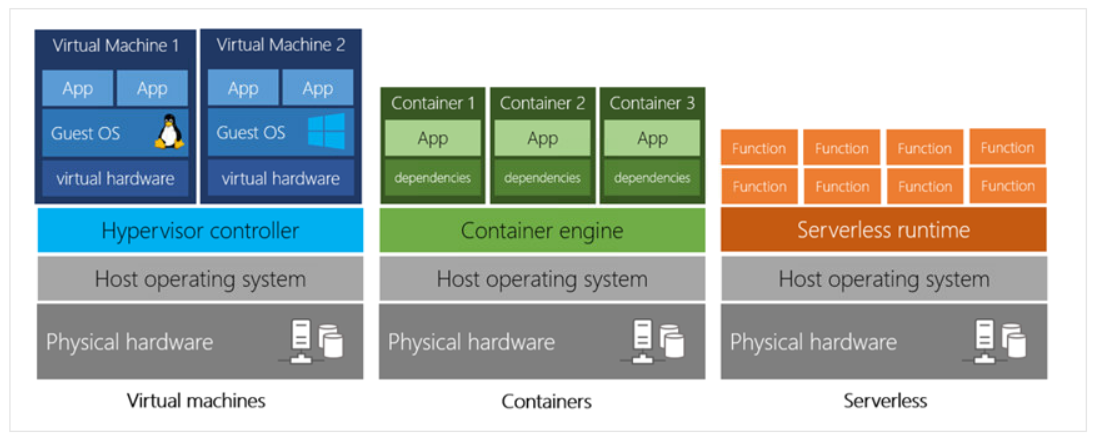
Major cloud services -> Compute power, Storage, Network, Security, Analysis.

“Lift and Shift”-> When a company gradually moves from existing process to cloud

Azure Datacentres -> Availability zones

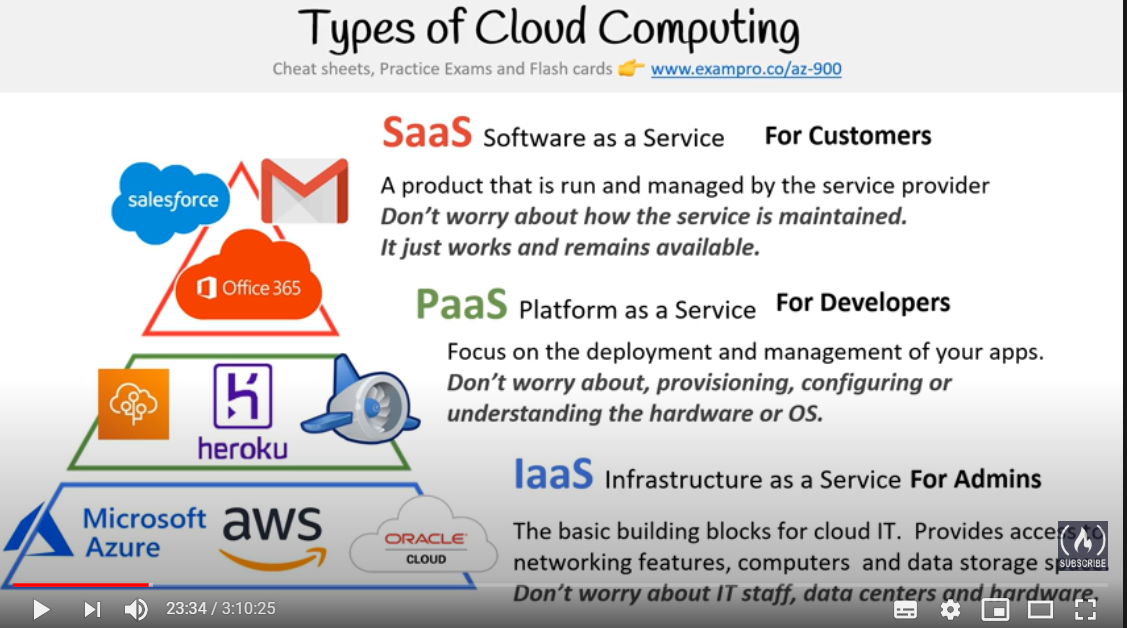
**Cloud Services**

1. **Compute Power** -> Nowadays most of the applications are hosted on cloud and hence when we access them online we are indirectly always sending requests and receiving responses from the cloud. This is possible when those applications we access are hosted on cloud servers using compute power. There are 3 major ways of using compute power based on the requirement of the user or organization :- Virtual machines, Containers, Serverless computing.
2. VM -> When priority is more for having more control on the operations then the adequate option is VM. VM is a system which is hosted on a remote server in any of the data centres hosted by the cloud provider. VM would have its own operating system and can be used as a virtual computer.
3. Containers -> Containers can be used when the requirement is more for fast usage and scalability. Docker containers are the prime example for the same, where multiple containers can be hosted on a single machine and all of them would be independent of each other. Each container would have its own application which can be installed from the images of the same. These containers can be moved from one system to the other based on availability as well.
4. Serverless computing -> Used when priority is for processing speed. Here the application is broken down into small functions and for each specific task a function is triggered to perform the task. In serverless computing the user have to pay for the processing time taken by the function whereas while using VM and containers the user has to pay all the time when they are up and running.



1. **Storage** -> Another important service provided by cloud providers. Nowadays while using an android phone we can see that while taking a picture it gets automatically stored in google photos, which is the cloud. Similarly we use storage services offered by the cloud daily in our lives. If the data to be stored is simple in nature then can be stored on cloud disks, while trying to store complex data then databases comes into picture.

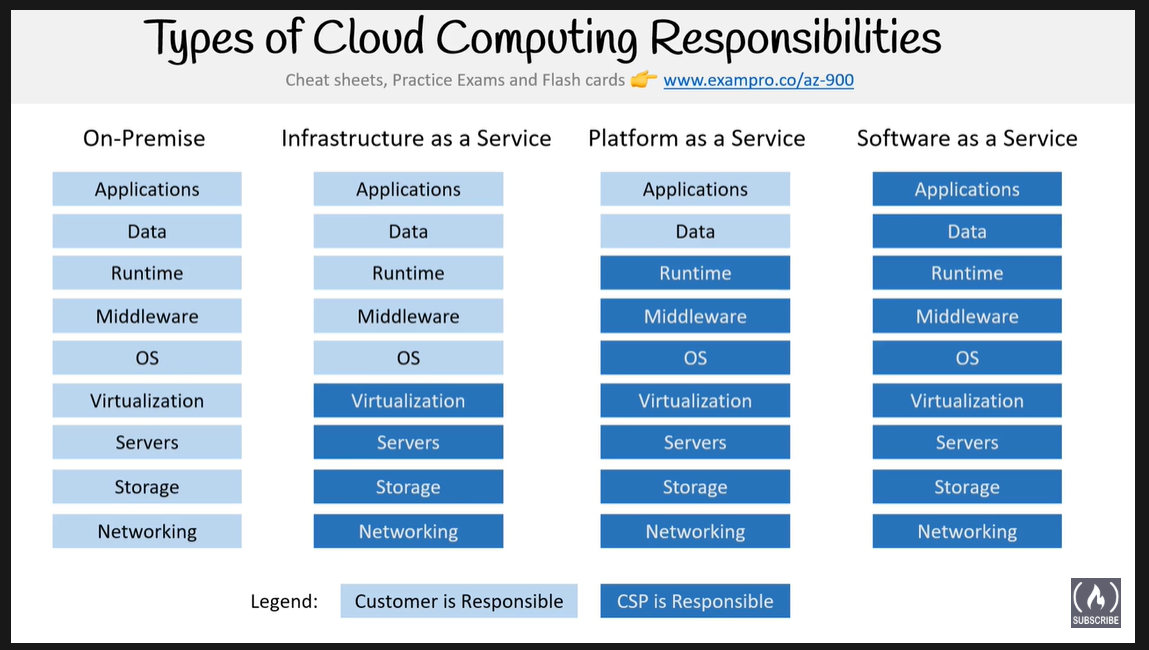
**Azure provide more than 100 services which are broadly classified into 3 types**

1. **IaaS (Infrastructure as a Service)** -> Compute power, Storage, Networking, Databases.
2. **PaaS (Platform as a Service)** -> Provides a platform which can be used by developers to develop their applications. This saves lot of time for the developers as they don’t have to bother on the configuration part. Ex : Heroku, Windows Azure, AWS Elastic Beanstalk.
3. **SaaS (Software as a Service)** -> Softwares which are run by Cloud service provider which we use daily such as Gmail, Office 365 etc 

**Benefits of Cloud computing**

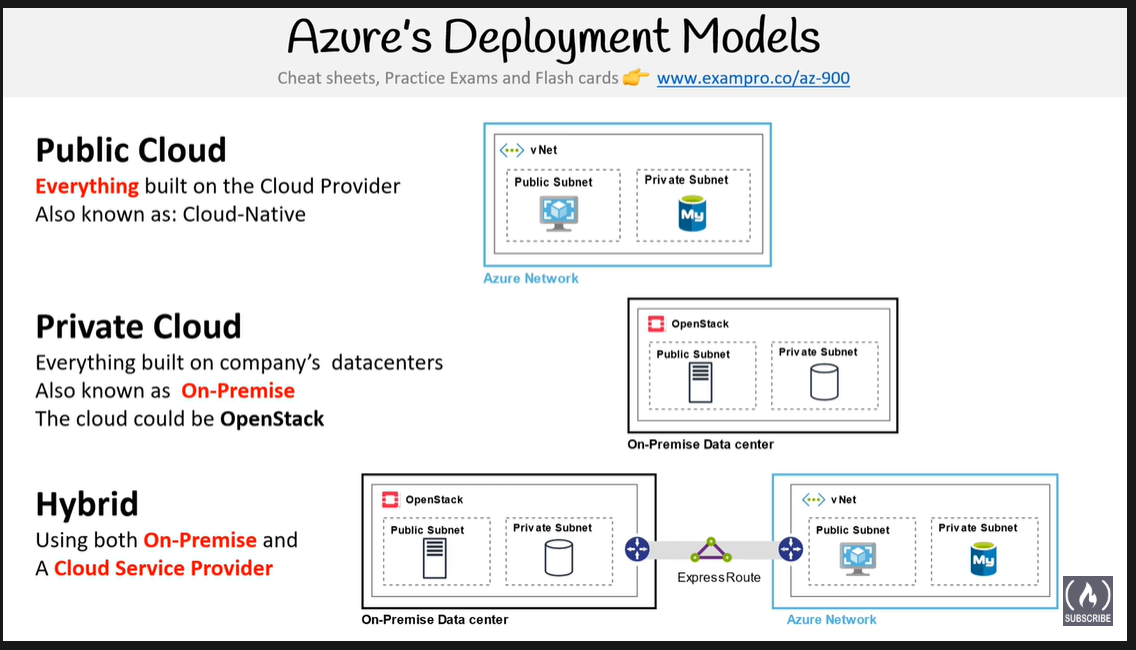
1. Cost Effective 🡪 Cloud computing is quite cost effective as you have to pay only what you use and not for the overall infrastructure. Company’s using cloud computing can pay for what resources that they need for specific time and then later give back the resources and not pay for it.
2. Scalable 🡪 Scalability is an important benefit, cloud providers helps users to scale up or scale down the resources to their wish. There are 2 types of scalability
3. Vertical Scaling – Here more resources are secured from cloud to increase the capability of the server
4. Horizontal Scaling – Here more servers are resourced from the cloud so that they will equally be able to distribute the workload and work efficiently
5. Reliable 🡪Cloud computing is heavily reliable as all the data and resources stored in cloud are always properly backed up and also redundant resources are present. Hence even when there is loss in data then cloud provider would be able to utilize the redundant or backup option hence reducing the changes of risk or failure. This is also called fault tolerance.
6. Available 🡪 The datacentres are present today at almost all parts of the world. Users can opt the data to be at a nearest datacentre for reducing the response time or can opt to distribute the resources to multiple datacentres catering to their specific needs.
7. Elastic 🡪 Cloud computing can also automatically determine if the application on the cloud has sudden spike of usage and cater to it by providing additional resources without the user intervention so that on heavy load the application will not go down.
8. Current 🡪 Cloud providers gives users the advantage of only to bother about development and deployment of the application. All hardware and software updates would be taken up properly by cloud provider in a timely manner.
9. Secure 🡪 The cloud providers provide a lot of physical protection to their datacentres by having walls, increased security, cameras etc. Also only authorized personnel will be allowed inside each department in the datacentres. Proper software protection will also be present to protect the resources.

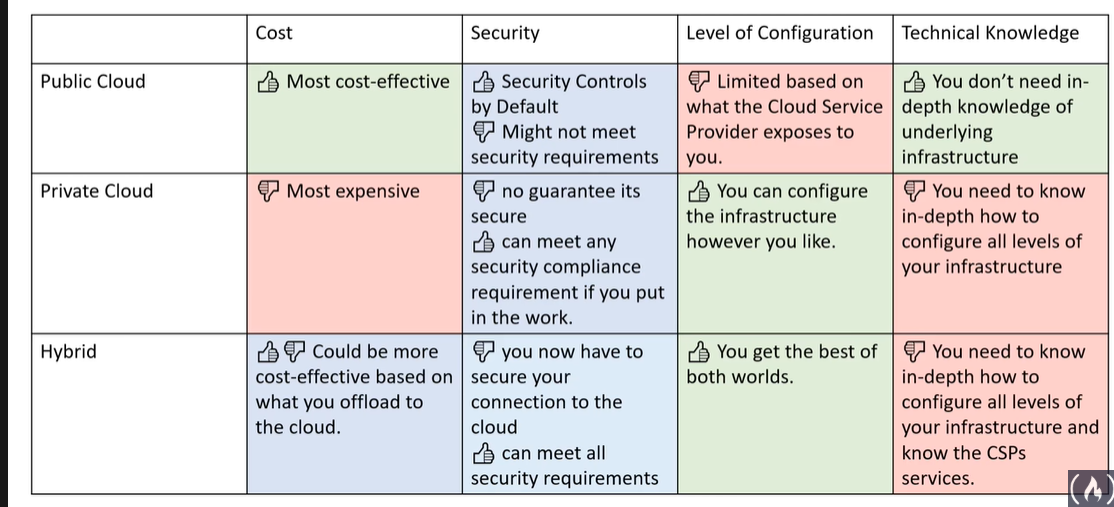
**Responsibilities in Cloud Computing**

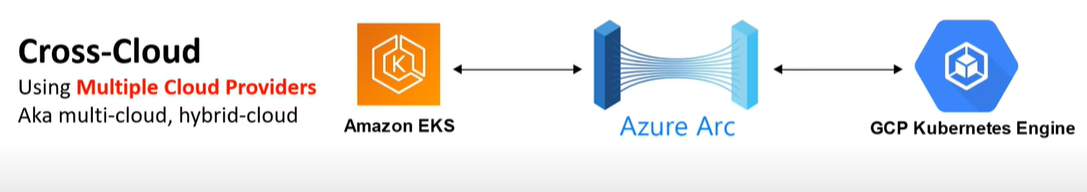


**Cloud Deployment Models**

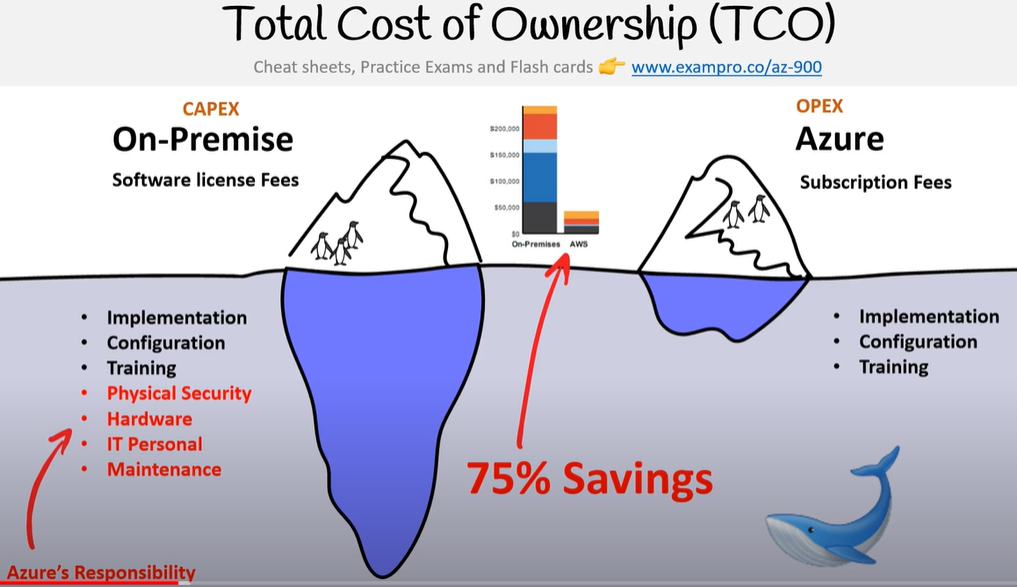
1. Public Cloud -> Everything on the cloud provider
2. Private Cloud -> Everything on company’s datacentre using cloud mimicking tool such as Openstack
3. Hybrid Cloud -> Combination of public and private
4. Cross Cloud -> Used by large organizations to interact between cloud services of diff cloud providers



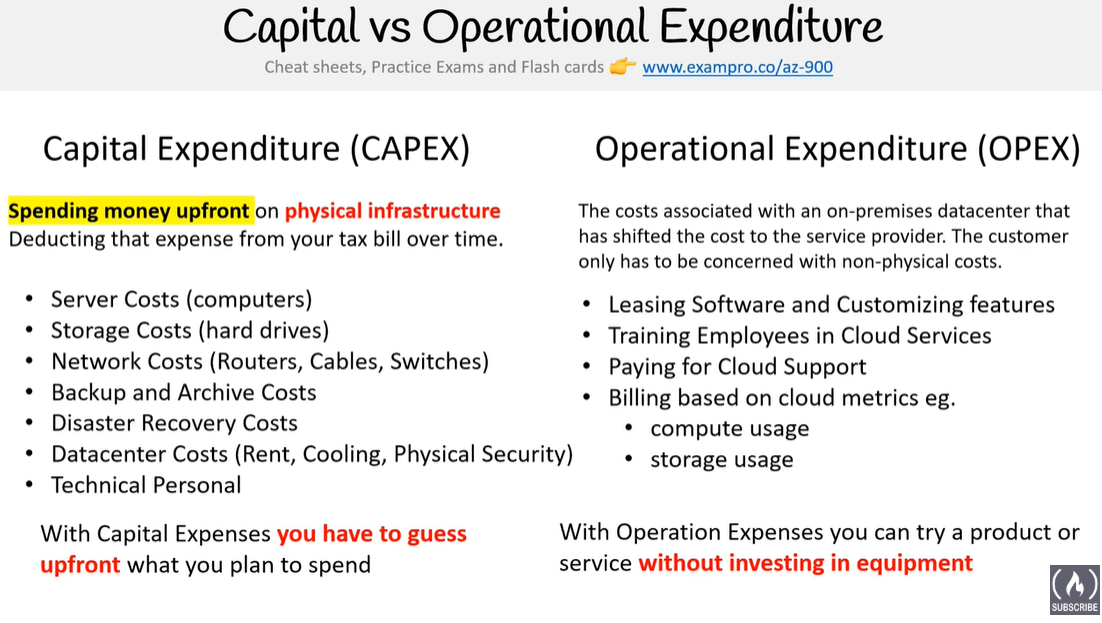


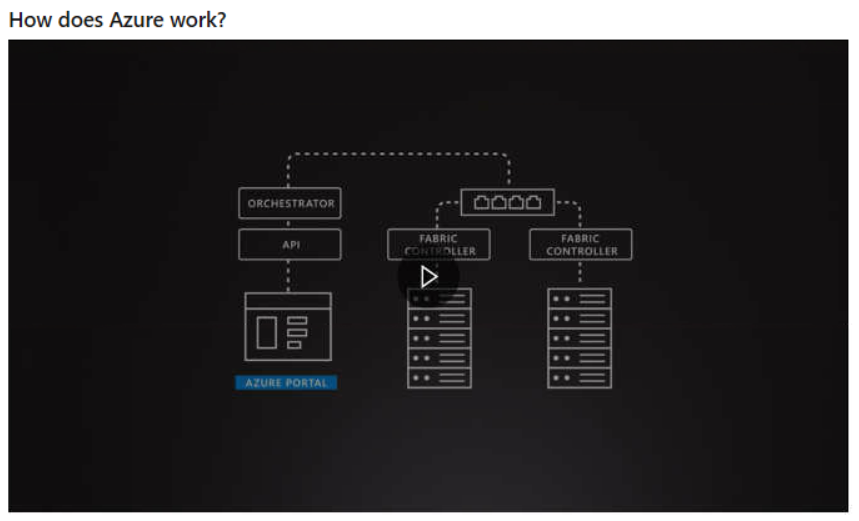
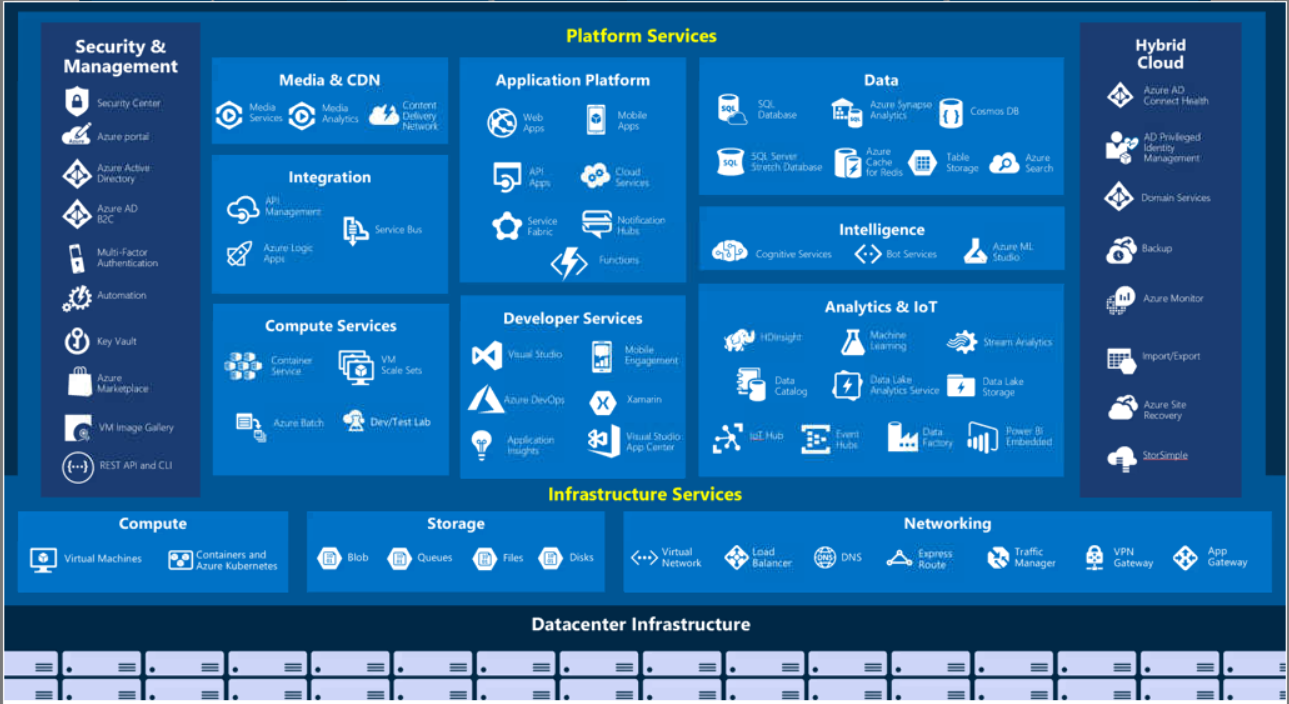


**TCO (Total Cost of Ownership)**

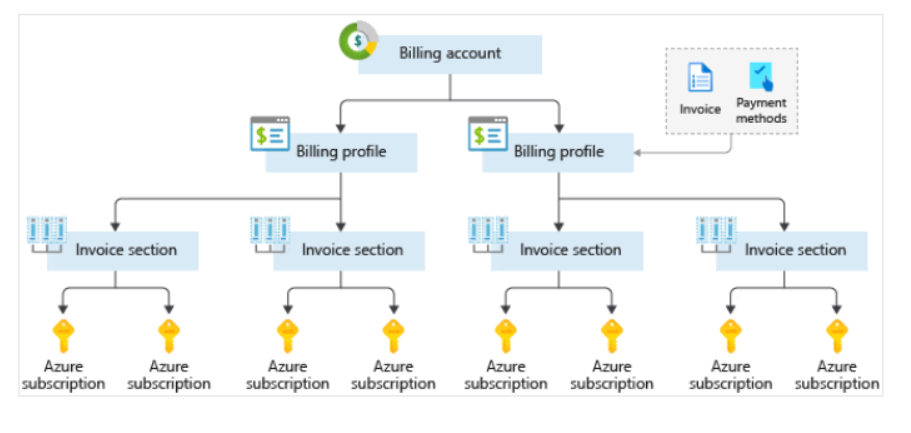
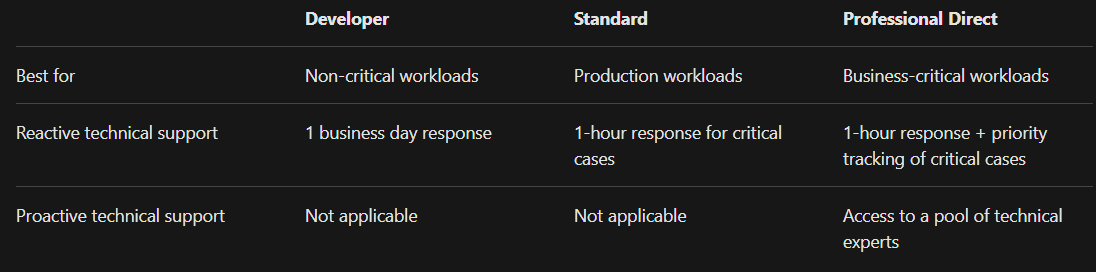
It is basically a comparison between On-premise and Cloud Services. Always the On-Premise resources cost would be considerably high when compared to Cloud service.

CAPEX vs OPEX



**Azure Billings and Support**

1. Azure Subscription 
2. Azure free support
3. Azure support plans (Developer, Standard, Professional Direct) 

**Azure Compliance offerings**

1. **CJIS – Criminal Justice Information Services**

Any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy

1. Cloud Security Alliance (CSA) Star Certification

 involves a rigorous independent third-party assessment of a cloud provider's security posture

1. GDPR – General Data Protection Regulation

GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyse data tied to EU residents. The GDPR applies no matter where you are located.

1. EU Model Clauses

Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU

1. UK Government G-Cloud

is a cloud computing certification for services used by government entities in the United Kingdom

1. HIPAA – Health Insurance Portability and Accountability Act

 HIPAA is a US federal law that regulates patient Protected Health Information

1. ISO (International Standards Organization) and IEC (International Electrotechnical Commission) 27018

covering the processing of personal information by cloud service providers.

1. MTCS Singapore (Multi-tier Cloud Security)

certification across all three service classifications: (IaaS),(PaaS),(SaaS).

1. SOC (Service Organization Controls) 1,2 and 3

Microsoft-covered cloud services are audited at least annually against the SOC report framework by independent third-party auditors

1. NIST CSF (National Institute of Standards and Technology Security CyberSecurity Framework)

NIST CSF is a voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks

**Azure architecture and service guarantees**

1. Azure regions
2. Azure special regions
3. Azure geographies
4. Availability zones
5. Region Pairs
6. SLA characteristics (Performance targets, Uptime and connectivity guarantees, Service credits)
7. Composite SLA
8. Application SLA

**Managing services with Azure portal**

1. **Azure portal, Azure Powershell, Azure CLI, Azure Cloud Shell, Azure mobile app**

|  |
| --- |
| Azure Cloud shell is a containerized shell running on the Azure portal. The Azure Cloud shell gives us the option to select either Bash or Powershell base containers.  Azure CLI can be used on Windows, Linux and Mac.  Azure Powershell is based on Windows.  Powershell core can be used on Windows, Linux and Mac. |

1. **Azure Advisor**

Is an Azure service that gives recommendations regarding the high availability, security, performance, operational excellence and cost.

**Azure Compute**

1. Azure Virtual Machines (when to use VM’s)
2. Scaling VM in Azure (Availability sets, VM Scale Sets, Azure Batch)
3. Availability sets (Update domain, Fault domain)
4. VM Scale Sets
5. Azure Batch
6. Containers (when to use containers over VM)
7. Azure Container Instances (ACI) and Azure Kubernetes Service (AKS)
8. Migrating apps to Containers (role of Azure Container Registry and Azure Active Directory)
9. Azure App Service (PaaS) – Web apps, Mobile Apps backend, API apps.
10. Serverless Computing (Abstraction of Servers, Event driven, Micro billing)
11. Azure Functions
12. Azure Logic Apps
13. **Azure Virtual Machines (when to use VM’s)**

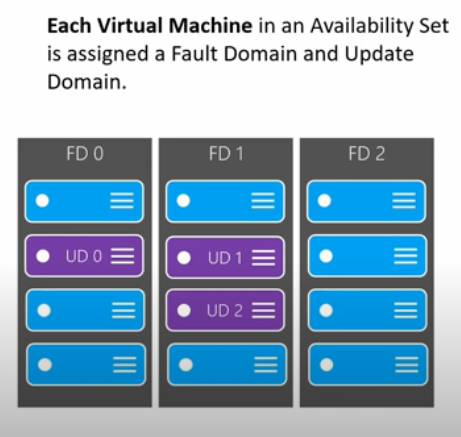
Azure VM’s are primarily used while using the ‘Lift and Shift’ principle.

1. **Scaling VM in Azure (Availability sets, VM Scale Sets, Azure Batch)**

Three ways in which we can increase the performance and capacity of VM’s.

1. **Availability sets (Update domain, Fault domain)**

In Azure there are 2 types of maintenance that can occur – planned and unplanned. To successfully manage planned maintenance we use **Update** domain and for unplanned maintenance we use **Fault** domains.

In the above image the three blocks represent the 3 racks in a datacentre.

**Availability set** – is a logical grouping of VM’s into update and fault domains to avoid planned and unplanned maintenance.

**1 Availability set = up to 3 Fault domains + 5 update domains (can be increased to 20)**

**Fault domain** – the VM’s are placed in separate racks to avoid a common source of failure such as power or network failure (which are unplanned occurrences).

**Update domain** – the VM’s are placed as separate to avoid any planned maintenance downtime.

1. **VM Scale Sets**

Can be used to implement the Scalability and Elasticity benefits. By using VM Scale sets, the user can have multiple VM’s with identical specs and a load balancer that evenly distributes the traffic. It can also increase and decrease the capacity automatically based on the demand.

1. **Azure Batch**

Provides the capability to scale to thousands of VM’s to manage heavy tasks.

1. **Containers (when to use containers over VM)**

Containers are faster than VM’s. Another advantage is when we have to run same applications on multiple OS it can be easily achieved using containers.

**VM’s virtualize the hardware, whereas Containers virtualize the OS.**

1. **Azure Container Instances (ACI) and Azure Kubernetes Service (AKS)**

ACI is used when the need is for containers and AKS is used when there are multiple containers and they need to be orchestrated.

1. **Migrating apps to Containers (role of Azure Container Registry and Azure Active Directory)**

Azure Container Registry is used for storing the container images.

Azure Active Directory is Azures identity management service.

1. **Azure App Service (PaaS) – Web apps, Mobile Apps backend, API apps.**

Used to build and run web, mobile backend and API applications.

1. **Serverless Computing (Abstraction of Servers, Event driven, Micro billing)**

These listed below are the main features of Serverless computing

1. **Abstraction of Servers** -> The servers on which the Serverless computing services run are hidden from the user.
2. **Event driven** -> usually system which use Serverless computing services are ones which are event driven. Which means that an event can trigger a specific set of code or workflow to get executed.
3. **Micro billing** -> is the feature which elaborates that while using Serverless computing services we are only paying for the time the functions or code is executed.
4. **Azure Functions**

One of the services that Azure provides for Serverless computing. Azure Functions execute the **code**. It is mostly stateless that means each function is run on separate instance.

1. **Azure Logic Apps**

Is an Azure Serverless computing service that executes a **workflow**. It is mostly having a state which means that the second iteration would run on the same instance used by the primary iteration.

**Azure Data Storage**

Azure also has the capability of storing up to 32 TB of data in its virtual disks

Azure Blob storage has the ability to store up to 8 TB of data for virtual machines.

1. Types of Data (Structured vs Semi-structured vs Unstructured)
2. Azure SQL Database, Azure Cosmos DB, Azure Blob Storage, Azure File Storage, Azure Queue Storage, Azure Disk Storage, Azure Data Lake Storage, Azure Synapse Analytics
3. Storage Tiers
4. Storage encryptions – Azure Storage Service Encryption (SSE) and Client-side encryption.
5. **Types of Data (Structured vs Semi-structured vs Unstructured)**

**Structured Data** is also called relational data, this is the kind of data that adheres to specific schema. Usually stored on tables such as SQL DB’s. Examples of relational data are data from sensors or financial data.

**Semi-Structured Data** is also called non-relational data and are stored in NoSQL databases.

**Unstructured Data** are the type of data that doesn’t have a specific structure such as large video files, JSON files, PDF doc

1. **Storage Services in Azure**
2. **Azure Cosmos DB (PaaS)** -> unstructured NoSQL DB that is widely distributed worldwide which results in fast access and retrieve speeds.
3. **Azure SQL Database (PaaS)** ->structured relational database. (Azure DB Migration Service can be used to migrate on-premise SQL database to Azure SQL Database).
4. **Azure Data Lake Storage (PaaS)** -> Data Lake storage is primarily used for storing data that can be later used for Analytics purpose.
5. **Azure Synapse Analytics (PaaS)** -> structured relational database. Azure Synapse Analytics service is the new name for Azure SQL Datawarehouse. This service can be quite handy for parallel processing of large volumes of data. It is also able to easily communicate with Analytics services in Azure as Azure Data Lake Storage does.
6. **Azure Blob Storage (IaaS)** -> unstructured storage. Blob storage is primarily used for storing large volumes of data such as video files, binary data etc. It can be used to store about 8TB of data for VM’s.
7. **Azure File Storage (IaaS)** -> File storage is primarily used for sharing data between one service to another. It used SMB protocol.
8. **Azure Queue Storage (IaaS)** -> Can be used to store messages.
9. **Azure Disk Storage (IaaS)** -> Normal disk storages like SSD or HDD for VM’s. Mostly helpful in ‘Lift and Shift’ scenarios.
10. **Storage Tiers**

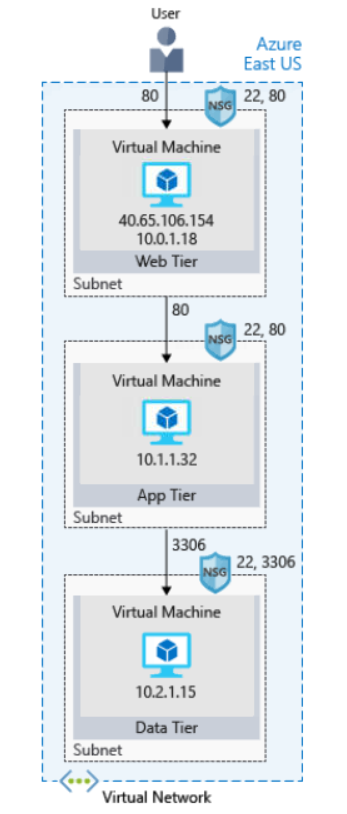
Helps in classifying the data based on how frequently they are accessed. There are 3 types of storage tiers.

1. **Hot storage tier** -> frequently accessed data
2. **Cool storage tier** -> infrequently accessed and stored for 30 days.
3. **Archive storage tier** -> rarely accessed and stored for 180 days.

**Azure Networking**

1. Loosely coupled architecture (N-tier architecture – Web tier, application tier, data tier)
2. Azure Virtual Network
3. Network Security Group (NSG)
4. Load Balancer - Availability and Resiliency
5. Azure Load Balancer
6. Azure Application Gateway
7. Content Delivery Network (CDN)
8. Domain Name System (DNS)
9. Azure Traffic Manager and Network Latency
10. Load Balancer vs Traffic Manager
11. **Loosely coupled architecture (N-tier architecture – Web tier, application tier, data tier)**

In this architecture the whole system is divided into different components, which results in improved performance and easy scalability. An example of loosely coupled architecture is the N-tier architecture wherein an application will be divided into Web tier, Application tier and Data tier. The user will always interact with the Web tier layer.



1. **Azure Virtual Network**

Azure Virtual network is an isolated network that helps azure services to securely communicate with each other. Azure Virtual Network can further have Subnets which can provide secure access to individual components as shown in the above image. Azure VPN Gateway can be used to connect an Azure service to an outside server. Azure Virtual Networks are also specific to a region.

1. **Network Security Group (NSG)**

NSG is something which is similar to a firewall, which can be used to allow or deny the inbound traffic

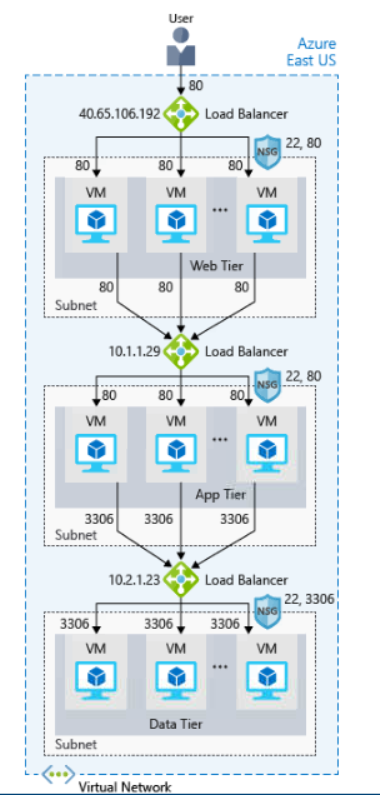
1. **Load Balancer - Availability and Resiliency**

An important benefit of Azure is to make the service up and running without any or much downtime. The load balancer plays a vital role in distributing the traffic to each systems in a pool. Load balancer works only if the VM’s in the pool are having the same configurations.

Availability – refers to how long a service is up and running

Resiliency – ability for system to stay up during abnormal conditions

1. **Azure Load Balancer**

Is provided by Azure to make the services highly available and resilient. Azure Load Balancer also removed the additional headache of maintaining the software and hardware while using on-premise load balancers, here Azure takes care of all the maintenance. 

1. **Azure Application Gateway**

This is also a load balancer, which is used when all the traffic is http. Azure Application Gateway is a load balancer whichi is designed for web applications.

1. **Content Delivery Network (CDN)**

The CDN is a set of distributed servers that can be used to effectively deliver content to the users with minimum latency.

1. **Domain Name System (DNS)**

DNS is the naming system for ip addresses. Azure DNS is a service that can be used to map the ip addresses to a specific name

Ex : 193.168.1.3 ip address getting mapped to [www.costco.co.in](http://www.costco.co.in)

1. **Azure Traffic Manager and Network Latency**

Latency can be defined as the time taken for a request to reach a particular server. The farther the server, the greater the latency. Azure Traffic manager comes into picture here to reduce the network latency. Azure Traffic manager would reroute the traffic to the nearest DNS server.

1. **Load Balancer vs Traffic Manager**

Load balancer would reroute the traffic to other similar VM’s in the pool if it finds that a specific VM is down.

Traffic Manager works at the DNS level and would reroute the traffic to nearby endpoint if it finds that a specific endpoint is down.

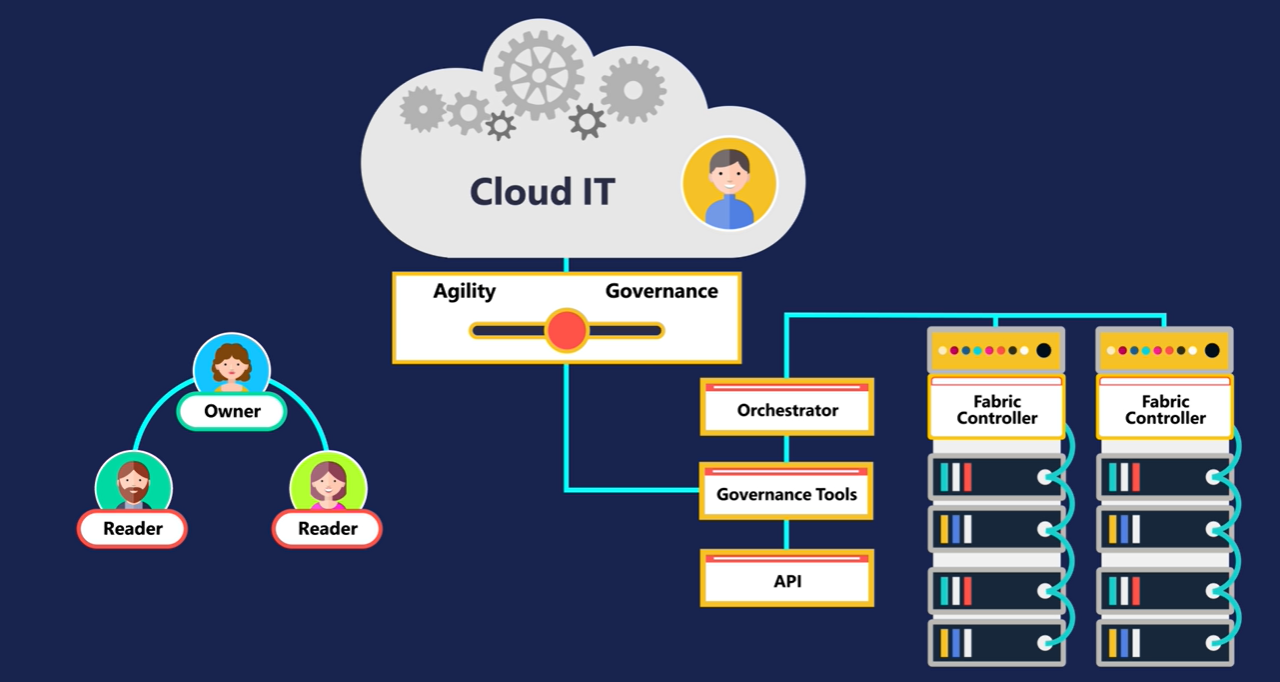
Load balancer works primarily to increase availability and resilience.

Traffic manager works primarily to decrease the latency and improve resilience.

**Azure Governance**

1. Azure Governance
2. Management groups
3. Azure Policy
4. Initiatives
5. Azure Blueprints
6. Microsoft Privacy Statement vs Microsoft Trust Center vs Service Trust Portal vs Compliance Manager
7. Azure Monitor
8. Azure Service Health
9. **Azure Governance**

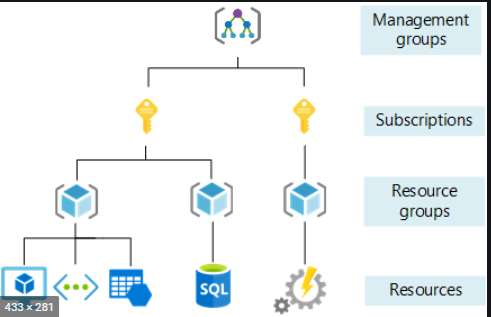
After moving from on-premise to cloud, there are chances that users would overuse Azure resources and create a significant dent in Organizations cost management. Azure governance relates to set of rules that needs to be implemented for user role and resource usage so that cost is successfully managed.

There are number of governance tools that implements user and resource control in Azure. 

1. **Management Groups**

This is the highest level of implementing Governance in Azure. Management groups are collection of subscriptions and can be used to enforce high level rules for RBAC, policies, initiatives, blueprints, resource groups.

Whatever rules are applied to the management groups by default will be applicable to all the lower layers.



Once a management groups is created, it would automatically come under a root management group which is created in Azure Active directory.

Any Azure AD user can create a management group.

1. **Azure Policy**

Is an Azure service that establish a set of rules that can be implemented to control the utilization of the resources and for the organization to work by adhering to compliance.

Azure Policy will constantly audit the existing resources, new resources and resources to which changes has been added.

Azure policy mainly consist of three categories – policy definitions, policy assignment and policy results

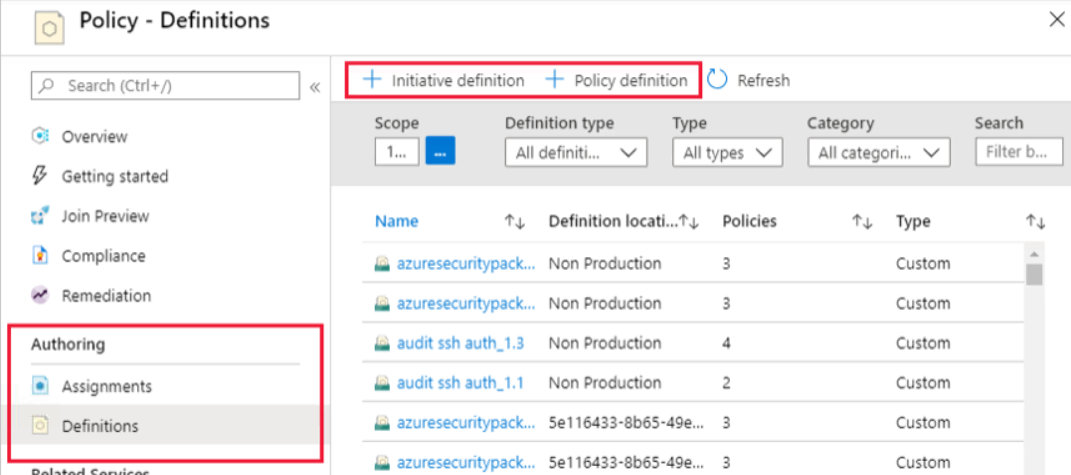
Policy definition – is the list of roles that needs to be followed (allowed locations, allowed resource type, allowed storage account, allowed VM, not allowed resource types).

Policy assignment – is the process of assigning the policy to a resource group, subscription, management group.

* Policy definition is always stored as a JSON file.

1. **Initiatives**

Initiatives helps to group multiple policies into one. This can be quite handy when there are multiple policies being forced. Initiatives also have definition and assignment part.

Initiatives can be created under the Authoring section

1. **Azure Blueprints**

When there are multiple policies, roles and resource templates that needs to be implemented then configuring and managing the same becomes a tedious process. Azure Blueprint is a one point solution for these problems. Azure blueprint is an azure service that can contain:-

1. Policy assignment
2. Roles assignment
3. Resource groups
4. Azure resource manager templates

Main categories of Azure Blueprint are blueprint definition and blueprint assignment

Azure Blueprint vs Azure Resource Manager templates

The key difference between blueprint and ARM templates is that ARM templates are not stored on the cloud, they are stored either locally or in a source control tool such as GIT. But blueprint is stored in Azure itself.

1. **Microsoft Privacy Statement** vs **Microsoft Trust Center** vs **Service Trust Portal** vs **Compliance Manager**

**Microsoft Privacy Statement** -> gives details about what personal data Microsoft processes, how is it processed and for what purpose it is processed

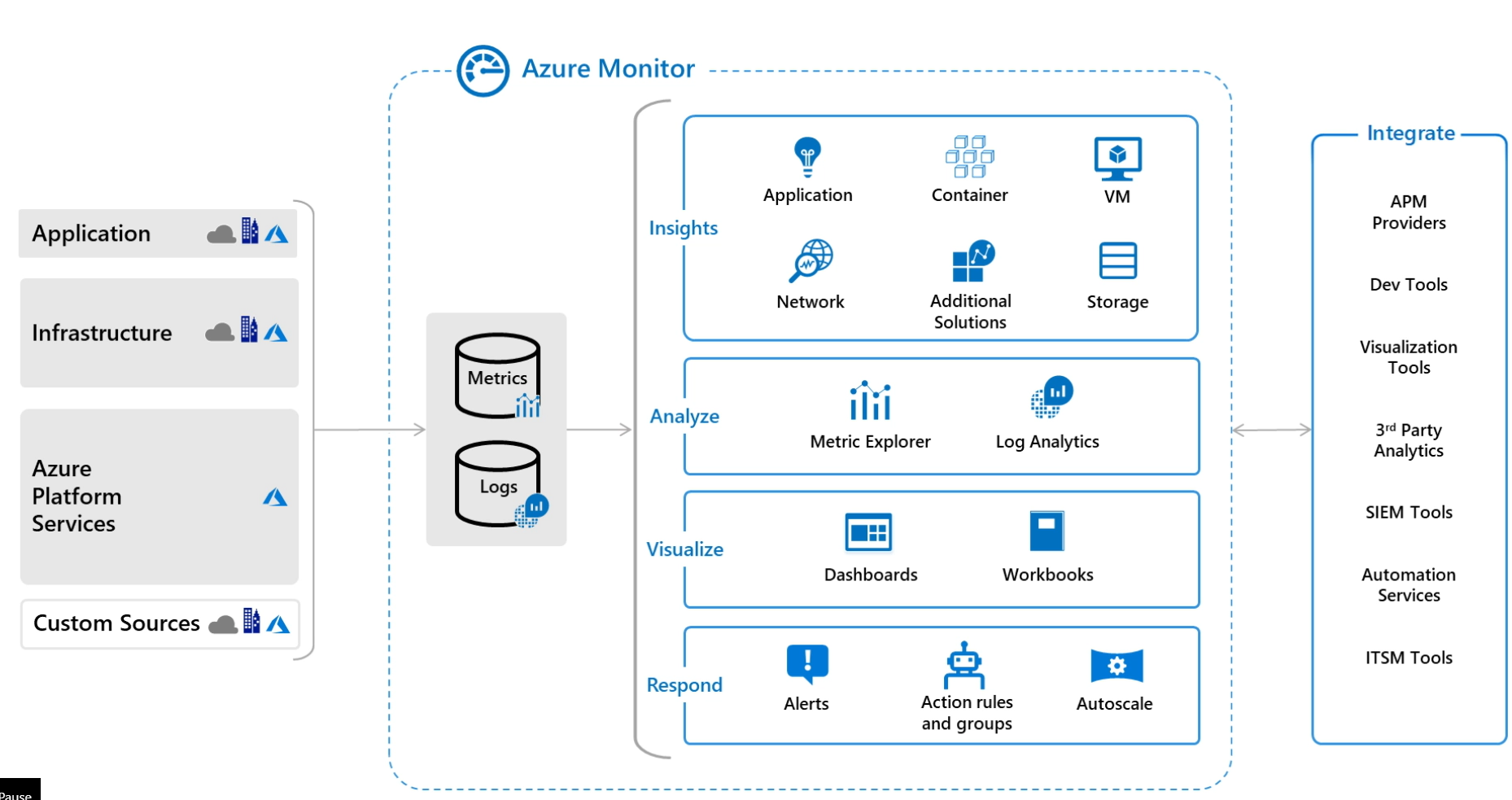
**Microsoft Trust Center** -> gives details about how Microsoft implements security, compliance, privacy etc in all Microsoft cloud products and services

**Service Trust Portal** -> this portal has the Compliance manager service and where Microsoft publishes the audit results and the compliance related information (ISO, HIPAA, GDPR etc)

**Compliance Manager** -> is risk assessment Dashboard within the Service Trust portal that helps to track the compliance aspects of Microsoft services and cloud based applications.

1. **Azure Monitor**

Is an Azure service which maximizes the availability and performance of the application by collecting telemetry data from the services and storing them as **Metrics** and **Logs**.



Application Insights, Monitor for VM’s and Monitor for Containers – will monitor and diagnose the data.

Analyse the obtained Metrics and Logs using Metrics Analytics and Log Analytics.

Visualize the metrics and logs collecting using dashboards

Respond to any issues using alerts, actions and auto scaling.

The data collected using Metrics Explorer and Log Analytics can also be deeply diagnosed with further tools.

1. **Azure Service Health**

Is an azure service that can be used to monitor the health of the resources and is having three main components.

**Azure Status** -> gives comprehensive details about the service outages and health of all the services across all the regions

**Azure Service Health** -> gives the health details of the services and the regions that the user is currently using. It also has capability to send alerts.

**Azure Resource Health** -> gives the health details of the individual resources that the user is using.

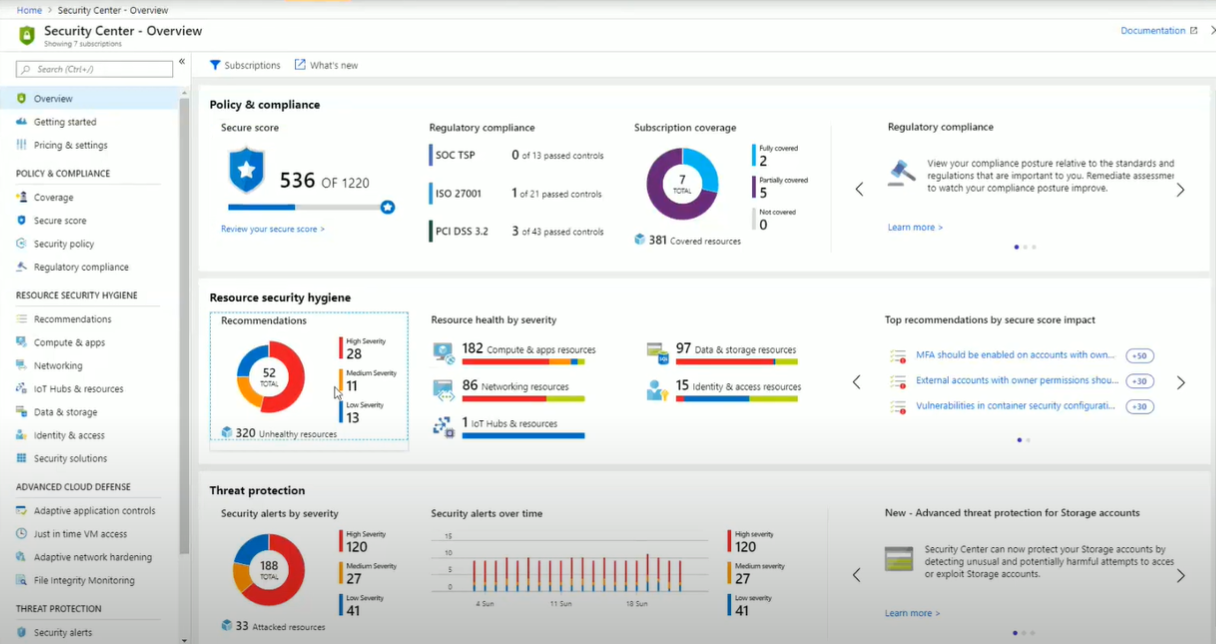
**Azure Security**

1. Azure Security Center
2. Authentication vs Authorization
3. Azure Active Directory
4. Encryption
5. Encryption in Azure
6. Azure Certificates
7. Azure Firewall, Azure Application Gateway
8. Azure DDoS protection
9. NSG, VPN, Azure ExpressRoute
10. Azure Information Protection (AIP)
11. Azure Advanced Threat Protection (ATP)
12. Security is a shared Responsibility
13. **Azure Security Center**

Security is regarded as shared responsibility of the user and the cloud provider. Azure Security Center is an Azure service which can be used to monitor the security aspects of cloud services as well as on-premise services which are used by the organization.

Security Center is having 2 pricing tier – **Free** and **Standard tier**, wherein the Free tier will cover will continue to monitor the services and suggest the recommendations that needs to be taken up.

To upgrade from **Free** -> **Standard** tier the user must have either of the following roles: Subscription contributor, Subscription owner or Security admin



Security Center has functionalities to setup **security policy, providing recommendations, alerts and also advanced cloud defence mechanisms such as ‘Just in time VM access’**.

Security policy -> wherein we enable the data collection for monitoring all the resources in the hybrid cloud framework

Recommendations -> will help to analyse and view the impacts which are there on the services and also the applications to be installed to resolve the issues.

Alerts -> uses the advanced Microsoft security concepts to categorize the different types of attacks happening and suggest remedial steps and various advanced defence tools.

Just in time VM access is one such advanced security tool to combat the threats.

1. **Authentication vs Authorization**

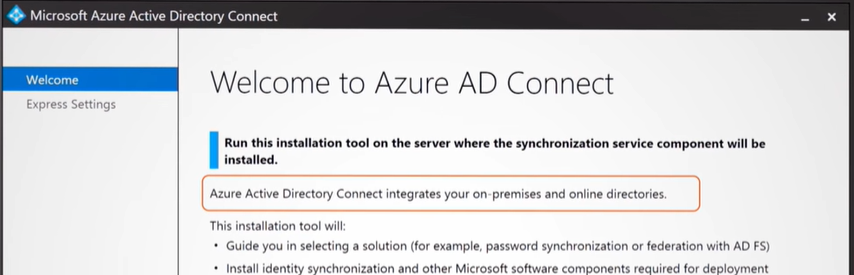
Identity management is the primary source of security nowadays as the number of devices through which a person can use a service has increased exponentially (like mobile apps, web, cloud etc.)

**Authorization** -> is the process of giving appropriate role based access for the users to access the application.

**Authentication** -> is the process of providing access for user into the service or application by validating the credentials as well as providing higher degree of security through features like multi factor authentication

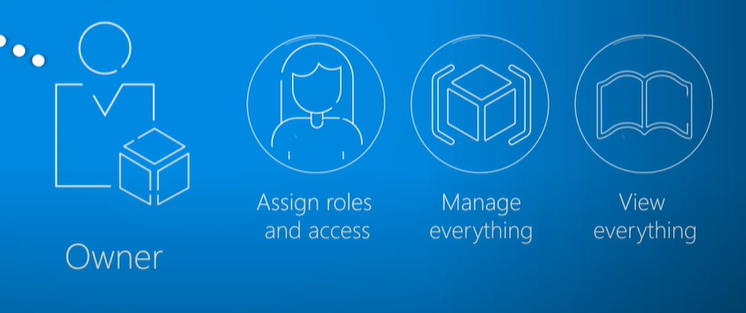
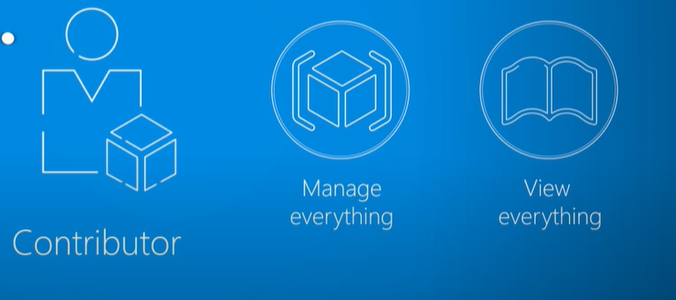
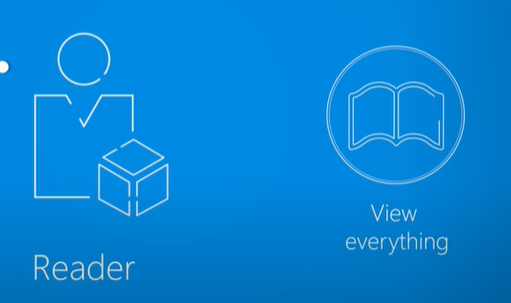
1. **Azure Active Directory**

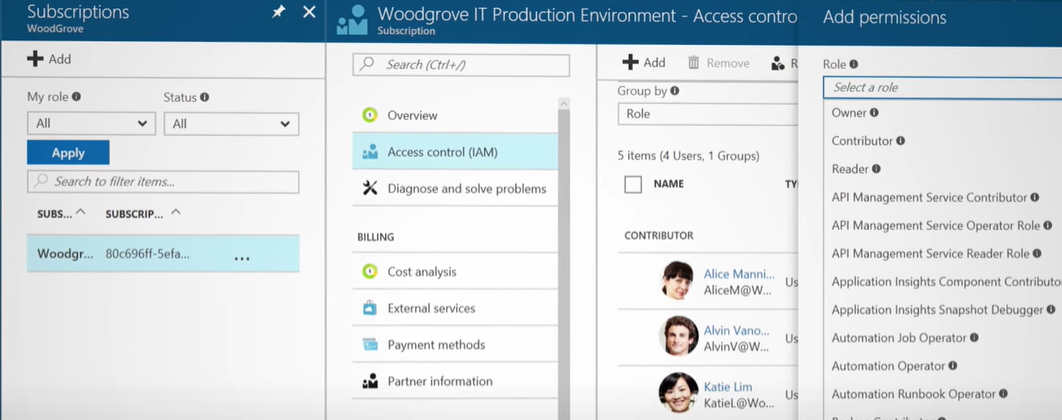
Is and Azure service that is used for identity management for services on the cloud or on-premises. Azure Active Directory can be easily integrated with on-premise AD as well using Azure AD Connect.



Azure AD provides a number of efficient services for identity management :

1. **Authorization**
2. **Multifactor Authentication**
3. **Single-Sign-On login**
4. **Application Management and Device management**
5. **B2C identity services**
6. **B2B identity services**
7. **Providing identity to services** – service principal and managed identities. Service Principal relates to providing authentication coupled with roles for the service. Managed Identities can be created for Azure services in Azure AD and Azure would take care of identity of the service.
8. **RBAC (Role based access control)** – RBAC generally has 3 built in roles (**Owner, Contributor, Reader**). With RBAC we can also create custom roles.



RBAC is a core service which is free of cost.

1. **Azure Privileged Identity Management (Azure PIM)** – provides a higher level of identity management in Azure AD. This is done by using advanced identity management methods like ‘Just in time’, ‘Time bound’, ‘MFA’ etc.
2. **Encryption**

Is the process of making the data in an unreadable format so that security is not compromised.

**Symmetric Encryption** -> The same key is used to encrypt and decrypt the data.

**Asymmetric Encryption** -> There would be two keys public key and private key. Anyone of the key would be able to encrypt the data. But to decrypt the data we would need both the keys.

**Encryption at rest** -> is the encryption that needs to be established when the data is at rest. For example when the data is stored in disks or databases, then it should be encrypted and stored.

**Encryption in transit** -> is the encryption that needs to be established when the data is moving from one system to another system. One of the ways to establish encryption while data is moving is using VPN.

1. **Encryption in Azure**

Encryption can be implemented in Azure using a number of different methods.

1. **Azure Storage Service Encryption** -> used to encrypt the data at rest in Azure blob, disk, queue, file storages and decrypt the data before being accessed.
2. **Azure Disk Encryption** -> used to encrypt the Virtual machines be it windows or linux. Azure Disk Encryption is directly linked with Azure Key Vault which stores the encryption keys and secrets.
3. **Transparent Data Encryption** -> used to encrypt the databases and datawarehouses.
4. **Azure Key Vault** -> There are a number of different encryptions happening in Azure services and all of them have multiple keys, secrets or certificates. It is utmost priority that these doesn’t end up in wrong hands. Azure Key Vault is a service that is capable of storing the keys, secrets and certificates.
5. **Azure Certificates**

**Service certificates** -> are the certificates that is used by the service to securely communicate with other services

**Management certificates** -> are the certificates that are used for deployment models such as Visual Studio, Azure SDK etc.

1. **Azure Firewall, Azure Application Gateway**

Azure Firewall can be used to block unwanted requests coming into the application by allowing access to only the trusted IP addresses.

Azure Application Gateway is a load balancer that has the WAF(Web Application Firewall) and can block unwanted HTTP traffic.

1. **Azure DDoS protection**

Denial of Service attack is a common attack that can occur when the attacker gets access to one of the public IP of the application and then flood the application by sending high volumes of requests and thus flooding the application and reducing the availability of the application.

Azure DDoS Protection is a one stop solution to protect against all sorts of DDoS attacks.

Azure DDoS Protection is accessible from all the Azure regions.

Azure DDoS Protection comes in 2 plans – Basic and Standard.

Once Azure DDoS Protection Standard plan is enabled then the same plan can be applied to all the subscriptions under the tenant.

Azure DDoS Protection plans sends the data directly to Azure Monitor and Azure Security Center.

Azure DDoS Protection standard plan would cover the additional cost incurred by the customer while facing a DDoS attack.

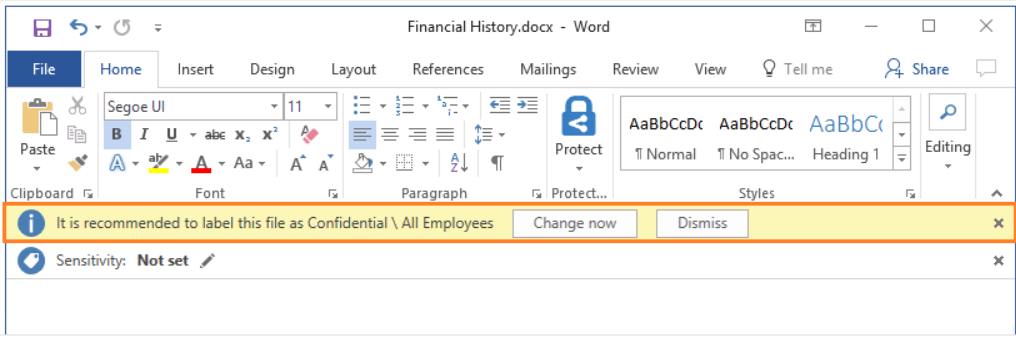
1. **NSG, VPN, Azure ExpressRoute**

**Network Security group** can control the traffic flowing from one subnet to another subnet.

**VPN** can be used to control the traffic and provide security while transferring data from Cloud services to On-premise services and vice-versa.

**Azure ExpressRoute** – used to establish effective and secure private communication between On-Premise system and cloud services.

1. **Azure Information Protection (AIP)**

Is an Azure service which can be used to assign labels to protect the shared emails and documents. 

1. **Azure Advanced Threat Protection (ATP)**

The ATP portal can be used to monitor and respond to suspicious activities. ATP sensors which are deployed on domain controllers send the data to the ATP portal.

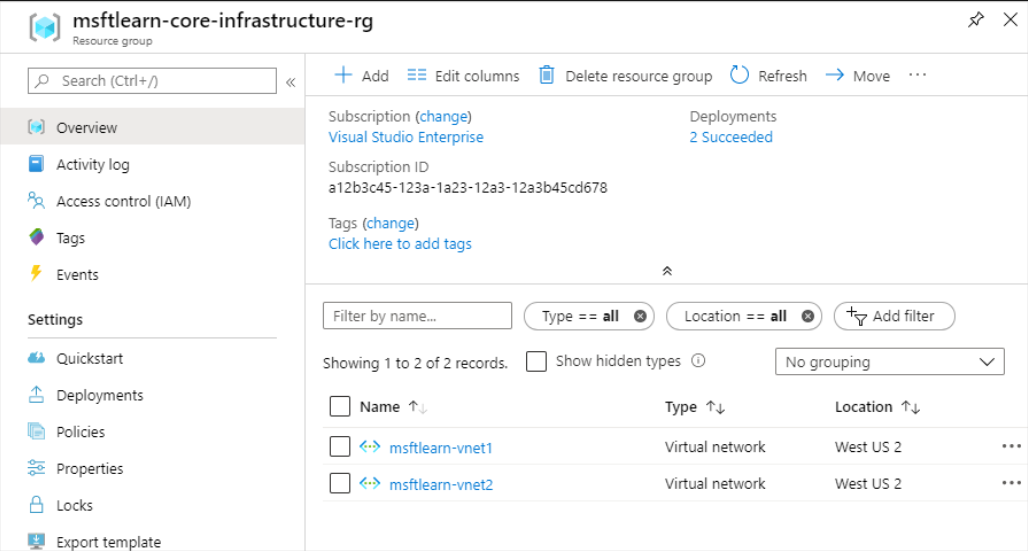
To access the ATP portal user must have **Azure AD Security group access**.

**Azure Resource Management**

1. Resource Groups
2. Using Tags
3. Using Policies
4. Using RBAC
5. Using Resource Locks
6. **Resource Groups**

Resource Groups are fundamental components in Azure. It can be considered as a logical container which holds resources in Azure such as VM’s, Databases, Networks etc.

* Resource group needs to be created inside the subscription to hold the resources.
* Each resource can be part of only one Resource group.
* Resources can be moved from one Resource group to another.
* Not all resources can be moved from one Resource group to another.
* If Resource group is deleted then all the resources inside it will also be deleted.
* Resource groups cannot be nested.
* Resources can be grouped logically (all compute resources in one group, all DB resources in another group likewise)
* Resources can be grouped based on their lifecycle (Prod, dev, staging)
* Authorization can also be added to resource groups using RBAC.
* Policies can be applied to resource groups which will be inherited by all resources inside it by default.
* Resource groups can be created using Azure portal, Azure Powershell, CLI etc



1. **Using Tags**

Tags are name/value pairs that can be used to classify the resources and resource groups.

* A resource can have up to 50 tags.
* The name field can accept 128 characters for Storage resources.
* The name field can accept 512 characters for all other resources.
* The value field can accept 256 characters for all resources.
* Tags if applied to Resource groups aren’t applied to the resources under it.

Benefits of tagging

* Tags can be used to organize resources for billing purpose.
* Tags can be helpful in easily monitoring and tracking down impacted resources
* Tags can be helpful in automation. For example we can give tag as shutdown:6PM and create a policy to shutdown all resources with the same tag easily.

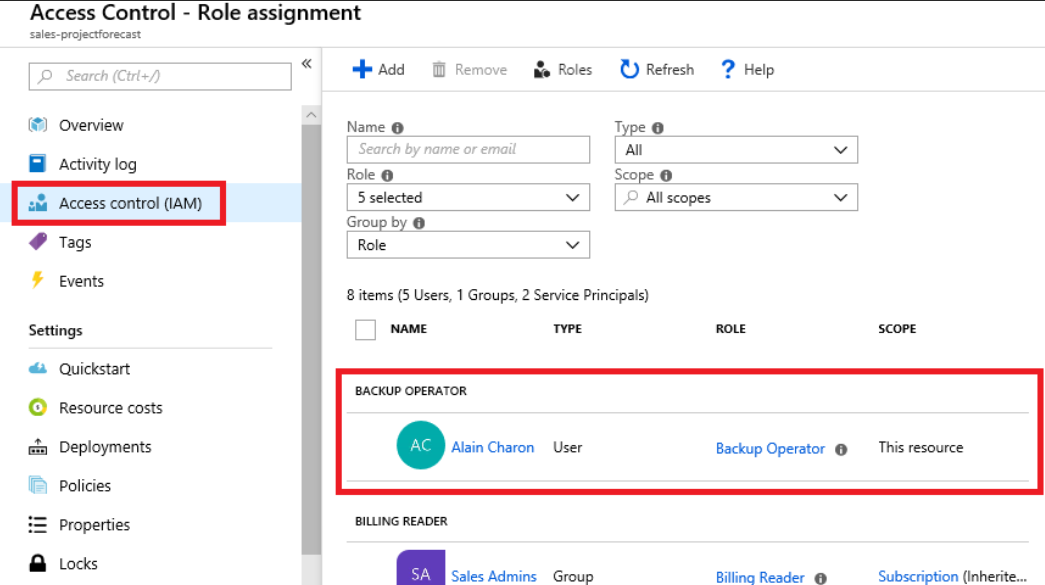
1. **Using Policies**

Azure policy is a service that can be used to apply a specific rule. It can be applied to subscription, resources and resource groups. Policy definition and Policy assignment are main parts of the policy.

Once a policy is assigned to specific resource group, then all the resources under that resource group inherit the policy.

1. **Using RBAC**

Role based access control is an important feature of the Azure Active Directory which allows control over users using the resources.

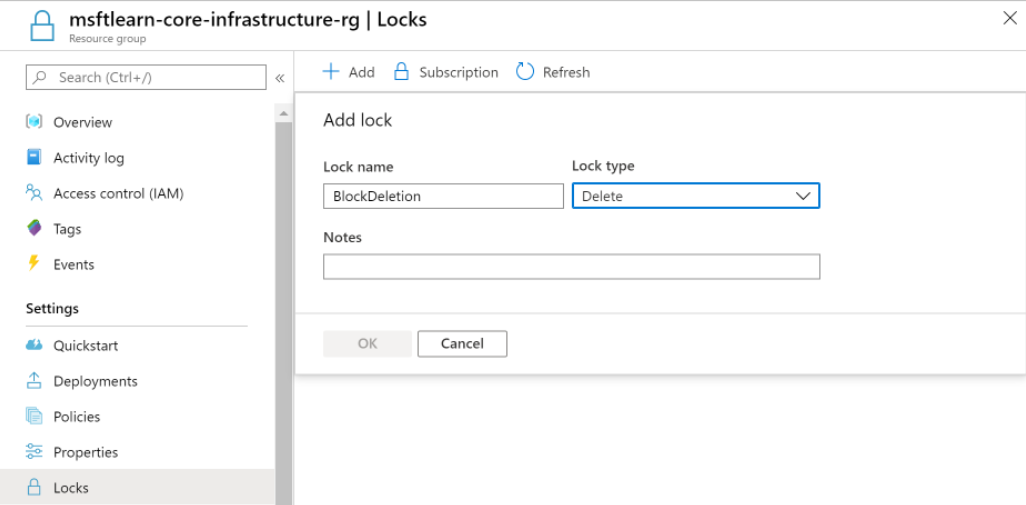
RBAC can be effectively used in resource management and can be applied to subscription, resources and resource groups, which gets inherited by the lower layers. 

1. **Using Resource Locks**

Resource locks are another important feature that can be used to prevent the accidental deletion of valuable resources. Locks has 2 setup options – **Delete and Read-Only**

**Delete** states that the resource or resource group cannot be deleted without removing the lock

**Read-Only** states that the resource or resource group doesn’t allow write operations.

Resource locks can be applied to subscriptions, resource group and resources and are inherited by the lower layers. 

**Azure Cost and Optimization Methods**

1. Pricing in Azure
2. Factors affecting Cost
3. Azure Pricing Calculator
4. Azure Advisor
5. Azure Cost Management
6. Azure TCO calculator
7. Save on Infrastructure Cost
8. Save on Licensing Cost
9. **Pricing in Azure**

Cost is always related to Performance in Azure. Performance is an important factor for organizations while moving onto Cloud. But it is also important to keep the costs low.

In Azure the pricing varies from resource to resource and also it dependents on the number of external factors and configurations of the resource.

While using a resource, there are number of meters that Azure uses to understand the usage statistics and finally during month end, come up with the billing.

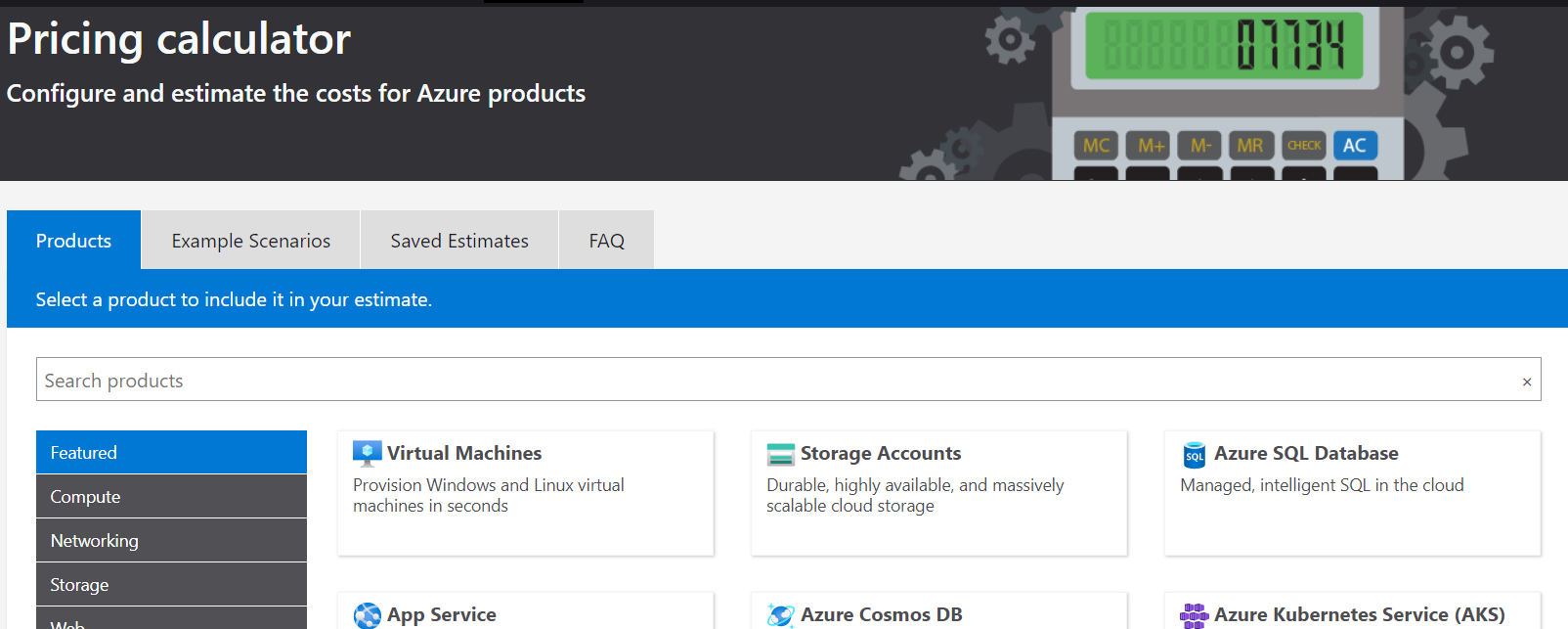
1. **Factors affecting Cost**

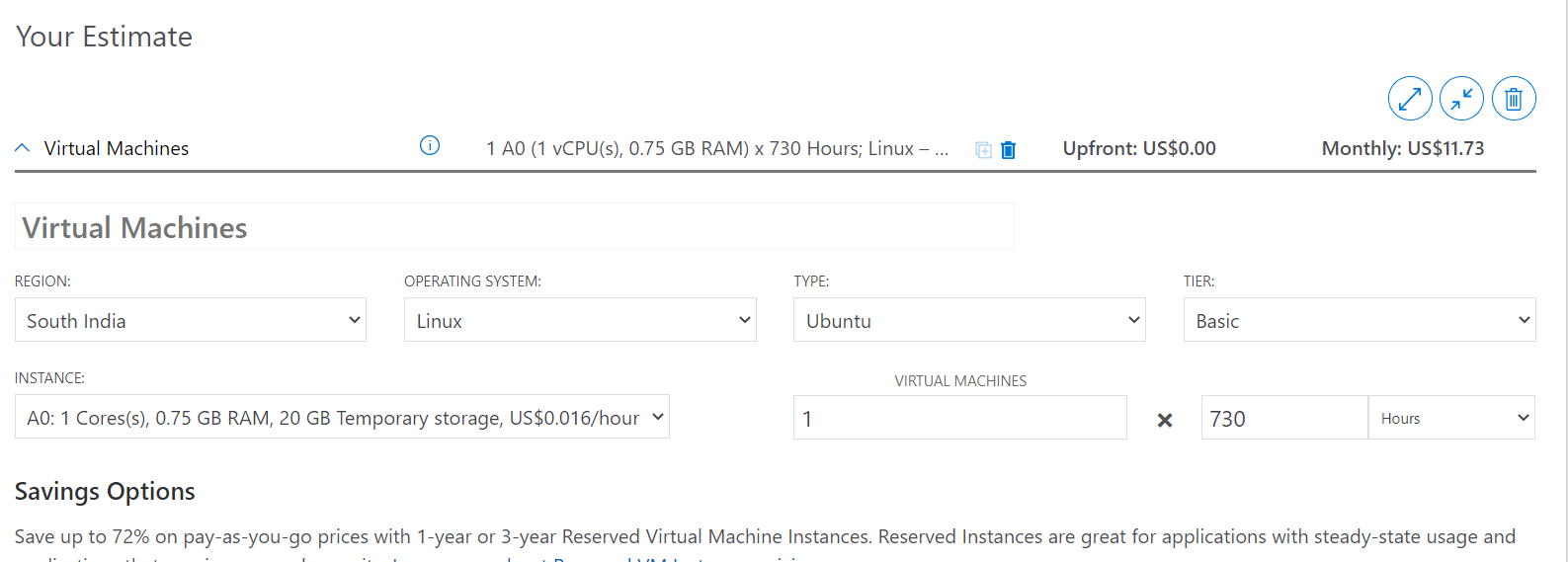
Below are the main factors that affect cost

1. **Resource type** -> each resource type has a different cost from others.
2. **Services** -> billing is different for Azure inbuilt services and services in Azure marketplace
3. **Location**
4. **Billing zones** -> the data flowing into the datacentre is free of cost (5 GB per month) whereas the cost of data flowing out of the datacentres depend on billing zone.
5. **Azure Pricing Calculator**

Can be used by organizations who are planning to move into Azure. Azure Pricing calculator website gives the flexibility to configure resources as per our wish and get to know about the monthly billing cost of the total solution that is being planned to move to Azure from on-premise.

The calculated estimate can be shared as an excel file or as a url.



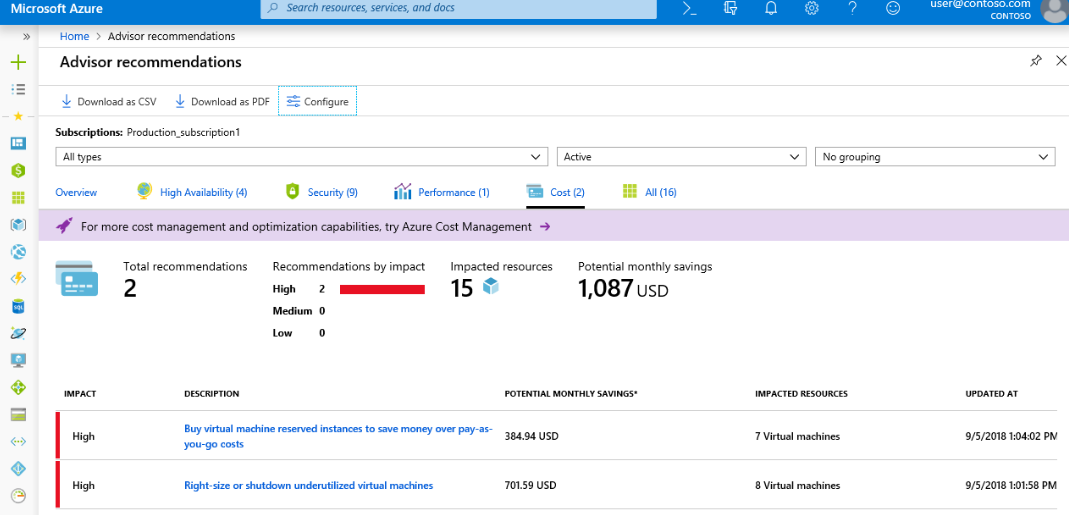


1. **Azure Advisor**

Is a free service provided by Azure which can be used to get the recommendations about the cost, performance, security, reliability and operational expenses.

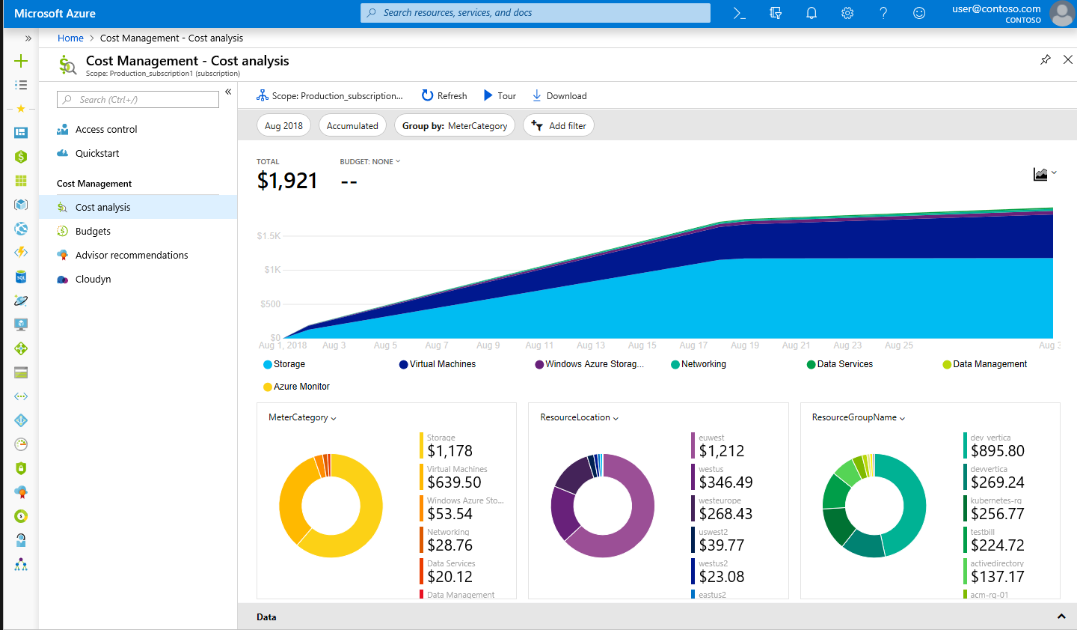
When Pricing calculator is used to determine the cost before moving onto the cloud, Azure Advisor provides comprehensive recommendations on how the cost can be reduced for the existing resources that are being used.

|  |
| --- |
| Azure advisor provides mainly 3 types of cost recommendations :-   1. Deleting unprovisioned ExpressRoute services 2. Buy reserved instances over Pay-as-you-go 3. Right-size or shutdown underutilized VM’s |



1. **Azure Cost Management**

Is a free service which is provided by Azure which gives in depth details about the cost management of the existing Azure resources.



1. **Azure TCO calculator**

TCO refers to the total cost of ownership. On-premise is marked as CAPEX and Cloud is marked as OPEX. CAPEX and OPEX varies in the additional capital expenditure which is present in CAPEX like Physical security, Hardware, Maintenance etc.

TCO calculator helps organizations moving from On-premise to Cloud to understand how much cost they are saving. In TCO Calculator, **the first step** is to define the resources based on four resource categories

1. **Servers**
2. **Database**
3. **Storage**
4. **Network**

**The second step** is to list out the additional CAPEX expenses as Assumptions and in **the third page**, TCO calculator will calculate the difference between On-Premise and Cloud.

1. **Save on Infrastructure Cost**

Above we have seen different types of methods to save costs. There are also other alternate ways to save the cost in cloud

1. **Use Azure Credits** -> Credits are awarded with Free usage which helps to utilize Azure resources without additional payment. There are also credits provided by Azure which are coupled with certain software like Visual Studio.
2. **Use Spending Limits** -> Spending limits can come quite handy which would result in saving unseen usage expenses. Once spending limits has been set, there would be reminder from Azure while the credit amount is getting over.
3. **Use Reserved Instances** -> If fixed resources are being used by and organization then the organization can save around 70 to 80% cost while switching from pay-as-you-go to Reserved Instances.
4. **Choose low-cost regions and locations**
5. **Right-size underutilized VM’s** -> is the process of reducing the capacity of VM’s which are not being utilized to their full potential. Azure Advisor and Cost Management provides recommendations for the same.
6. **Deallocate VM’s in off hours** -> if the VM’s are used only during office hours then cost can be saved by Deallocating them by the end of the day. Auto-shutdown feature of VM’s can be utilized to achieve this.
7. **Delete unused VM’s**
8. **Migrate to PaaS or SaaS from IaaS**
9. **Save on Licensing Cost**

Licensing cost is another important part in cloud where the cost can be saved. This can be done by different ways. Below are some of the ways by which existing licenses can be reused

1. **Azure Hybrid Benefit for Windows Server**
2. **Azure Hybrid Benefit for SQL Server**
3. **Azure Enterprise Dev/Test and Azure Pay-As-You-Go Dev/Test**
4. **BYOL in Azure Marketplace**