FP—57965—Cloud Computing

Cloud Computing

Cloud Computing is a way for delivering services or resources on-demand.

According to the National Institute of Standards and Technology (NIST):

***Cloud computing** is a model for enabling ubiquitous(worldwide) (সর্বব্যাপী), convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction..*

This cloud model is composed of

- *five essential characteristics*
- *three service models* and
- *four deployment models*.

five essential characteristics

On Premises	Cloud
1. **Scalability**: High Cost, Low Utilities. Once scaled Up, difficult to scale down, and often leads to heavy losses in terms of infra and maintenance cost.	1. **Scalability**: Allows to pay how much used. With much easier provisions to scaling up or down.
2. Server Storage: Needs lots of storage and servers with power, maintenance	2. **Server Storage:** Offers by cloud provider, they maintain the storage, servers etc. Saving money and space.
3. Data Security: Less Security .	3. **Data Security:** Better Security. Also avoid constantly monitor and manage security protocols.
4. Data Loss: In case data Loss, the chances of data recovery may be very small.	**4. Data Loss:** Have robust DR measure to ensure faster data recovery.
5. Maintenance: Requires additional teams for H/w and S/w maintenance. This increases the cost also.	**5. Maintenance:** Maintained by the cloud provider, reducing the cost and resource allocation.

Cloud Computing refers to on-demand computer services over the internet as pay-as-you-go basis. Rather than managing files and services on local storage devices, doing the same over the internet in a cost-efficient manner.

Cloud Computing

Deployment Model

Service Model

Public Cloud

Private Cloud

Hybrid Cloud

Public :The infrastructre is available to all over the internet. Own by cloud service providers. Like a bus service.

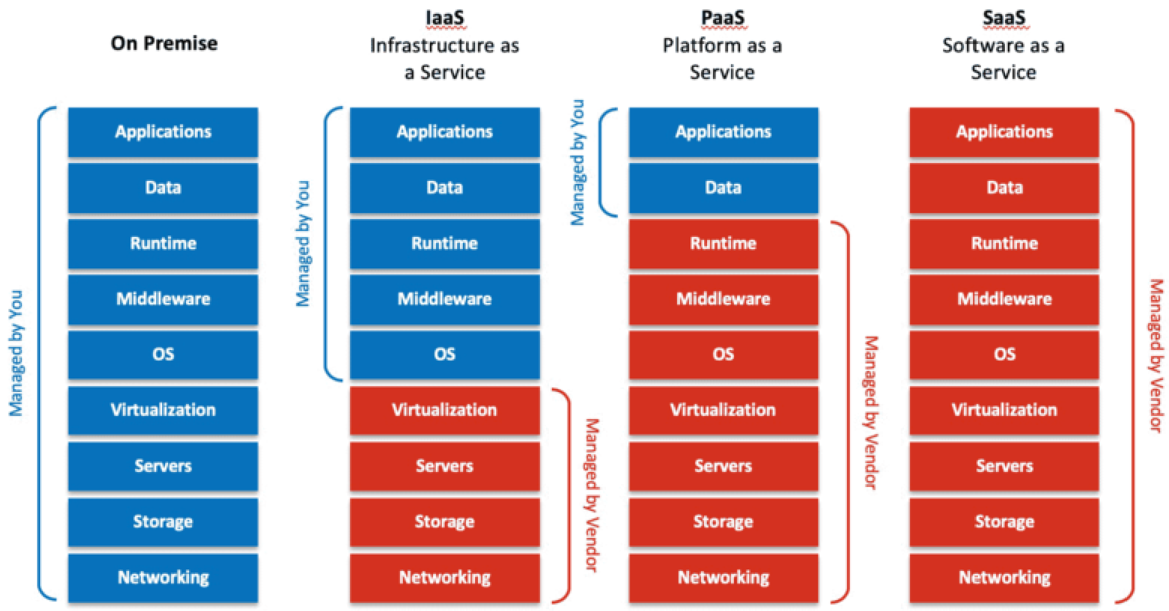
Private :The infrastructre is Exclusively available for a single organization Can be managed by the org or a 3rd party. Like own car.

Hybrid :The infrastructre is combination of public and private infra. Like hiring a cab/shuttle.

IAAS

PAAS

SAAS



On Premise	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Cloud Components

The components are broadly classified into **Frontend Components** and **Backend Components**.

Frontend Components

Clients: Clients are the devices through which the end users interact. They are divided into three broad categories: ***mobile, thin and thick clients***.

Smartphones and tablets constitute mobile clients, while computers without an internal hard drive is a thin client, and thick clients are your typical computers.

Backend Components

Datacenter: It is a server or a collection of servers.

Distributed Servers: These servers are spread across multiple locations.

Storage, security and other such infrastructures add to the backend list.

Through a network layer, cloud establishes the connection between the frontend and backend devices.

Cloud Characteristics

Core attributes of cloud computing services are:

1. Elasticity

2. On-demand

3. Provider-pooled computing resources

4. Metered service usage

5. Broad network access

On-demand

pooled computing

Elasticity

Metered service usage

Broad network

On-demand Self Service: User should be able to create services, resources, whenever wanted, Customer can select the resources whenever they wanted with a help of self-service provisioning portal. Any time access, create, update the resources using internet.

Rapid Elasticity: The most attractive features of cloud computing. When there is certain load on the servers, and it exceeds the threshold, it can increase its capacity automatically. The requests are going through a load balancing to the VMs. If the load exceeds the threshold, it creates more VMs automatically. There may be some rules, depending on the load what is the number VMs or servers needs to be created. This is called **Scaling Out (Creating new servers based on demand).** When the loads reduce, it automatically terminates the extra VMs, this is called **Scaling In.** This concept is called **Horizontal Scaling,** When Shutdown the servers and increase the memory size, increase the number of CPUs (2 core to 4 core etc.)it is called **Vertical Scaling(Increasing the computing power of a machine).**

Measured Service: Detail level of billing, like location, number of servers or size of CPUs etc.

Resource Pooling: Sharing the servers with the physical server. E.g. Like Uber Shuttle vs Single hire, which may cause the higher fare. In cloud user can create VMs, these are provisioned from physical servers. One of the physical servers will provide the memory, resources for the VM . There may be other VMs in the same physical server and those can be owned by other customers. But they are totally isolated. (**Multi Tenancy)**

Broad network access: Access to the services from anywhere, and the cloud provider must be available in various geo locations, can be accessed in any time, any network with internet and a device with a compatible browser.

Advantages of Cloud

- 24 * 7 availability and accessibility
- Scalability
- Security
- Enhanced collaboration
- Cost effective

and the list adds on.

Collaboration

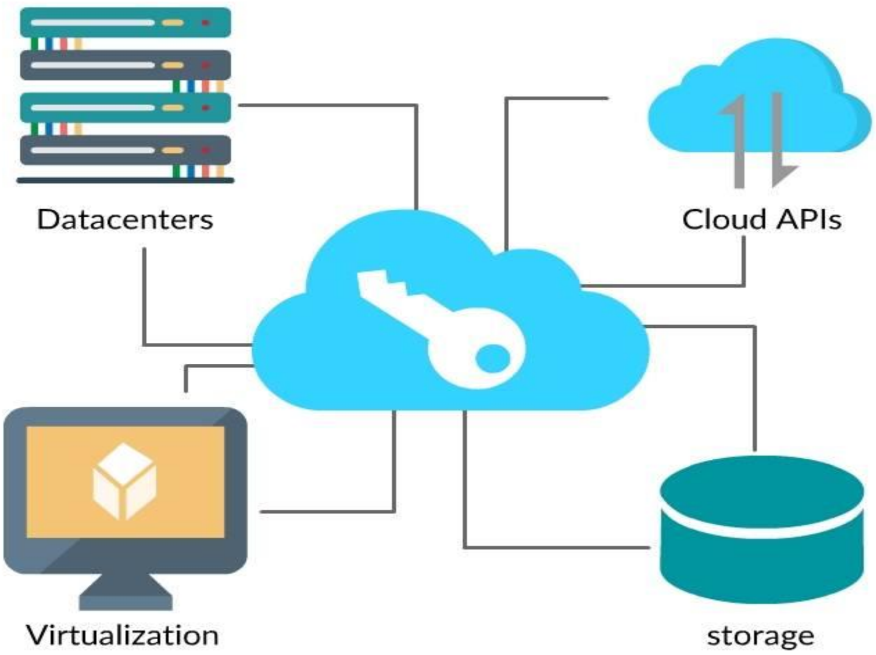
Security

Scalability

Cost effective

Availability

Key Factors



Cloud computing is enabled through these key factors.

- Cloud Datacenters
- Virtualization
- Cloud APIs
- Cloud storage

Cloud Datacenters are used for providing scalable and reliable cost-effective infrastructure.

Virtualization

Virtualization is one of the core concepts that enable cloud computing.

So, what is virtualization?

The process of creating a virtual environment in a resource, to enable execution of services without interfering with other activities done by the resource.

An ability that allows you to share the physical instance of an application or resource with multiple users.

Virtualization is achieved by **creating logically isolated resources on the physical resource**.

Few resources that can be virtualized include servers, storage, network, etc.

Features

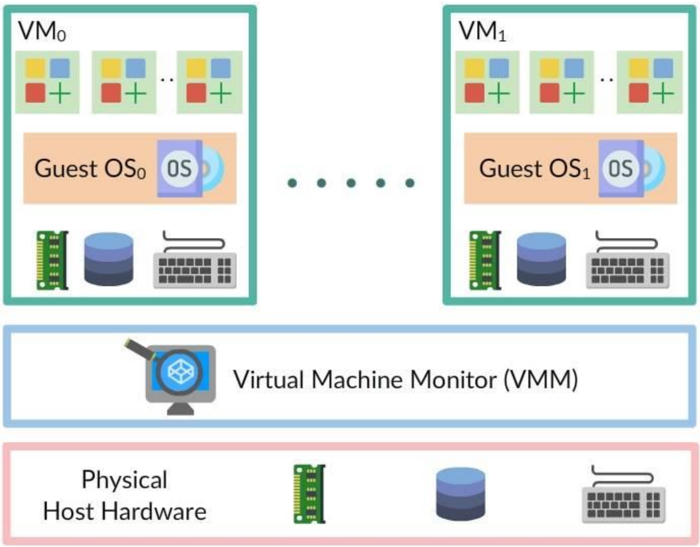
Prominent features of virtualization include:

Partitioning: You can split a resource to support many applications and hardware.

Isolation: Every virtual instance is segregated from one another as well as from the resource.

Encapsulation: You can summarize a virtual instance as a single entity to easily identify the service it offers.

How Virtualization Works?



- The interaction between the host server/machine and the virtual machine is facilitated by software called **Hypervisor** (VMM).
- Hypervisor distributes the hardware resources such as CPU, memory to the virtual environments.

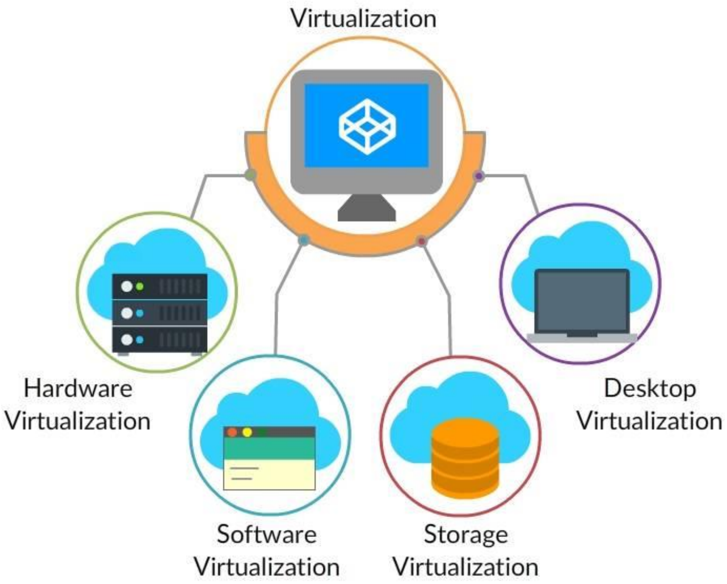
Terms to Remember

- A virtual server is a virtual machine running on a server.
- Virtual Machine Monitor (aka) Hypervisor, manages the virtual machine existing on a single host machine.
- Virtual infrastructure management component runs on top of hypervisor, it deals with allocation of resources such as providing information for provisioning virtual infrastructure, support for defining operational rules.
- Virtualization Platform is the software that runs on the physical server, used to create host VMs such as VMware vSphere, Citrix and XenServer.

Increased efficiency and multitasking

- Manageability - the ability to move, copy, and isolate VMs
- Sustainability - energy savings by the way of less hardware and electricity
- Availability - the ability to snapshot, clone, and run redundant VMs
- Security - isolation of VMs and applications

Virtualization Types



Virtualization varies depending upon the resources you deal with:

- Hardware Virtualization
- Software Virtualization
- Storage Virtualization
- Desktop Virtualization

Hardware Virtualization

***Hardware virtualization** is the abstraction of physical hardware using the hypervisor.*

Hardware virtualization or **server virtualization** is the concept where you generally create a virtual machine on top of physical hardware. The hypervisor manages the virtual environment.

Types

- Full virtualization
- Para virtualization
- Emulation virtualization

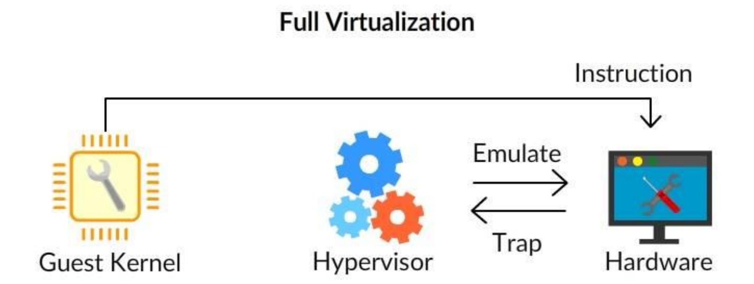
Full Virtualization

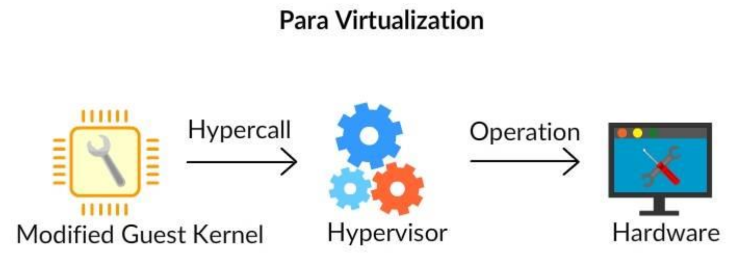
A technique in which user service requests are separated from physical hardware. The OS and the necessary software run on top of the virtual machine. The Guest OSs are unaware of virtualization.

VMware Workstation, Virtual Box, and Hyper-V are few products that support full virtualization.

Para-Virtualization

Para-Virtualization is a technique that offers a software interface to the virtual machines. This interface will be similar but not identical to the underlying hardware-software interface. It is used to execute critical tasks in the host as against the virtual host. Guest OS recognizes the presence of the hypervisor and communicates directly with it. Xen, Oracle VM for X86 are some of few examples.





Software Virtualization

Software or application virtualization encapsulates or abstracts the programs/applications from the underlying hardware on which it is executed.

- It enables applications to run in environments not suitable for the native application.
- It reduces system integration and administration costs as it helps to maintain a common software baseline across multiple computers.

Storage Virtualization

A concept where multiple physical storages are grouped to appear as single storage is known as storage virtualization.

Desktop Virtualization

A concept that stores the users desktop on a remote server allowing the user to access it from any device or any location is Desktop virtualization or client virtualization.

Cloud Service Models

Based on the organization's requirement, cloud providers offer a variety of services and resources, packaged as a service model.

The three main service models include:

1. IaaS (Infrastructure as a Service)
2. PaaS (Platform as a Service)
3. SaaS (Software as a Service)

Variations from the above-mentioned base models, such as storage as a service, security as a service, etc., keep emerging in the market.

Infrastructure as a Service (IaaS)

- Provide building blocks for cloud IT
- Provides networking, computers, data storage space
- Highest level of flexibility

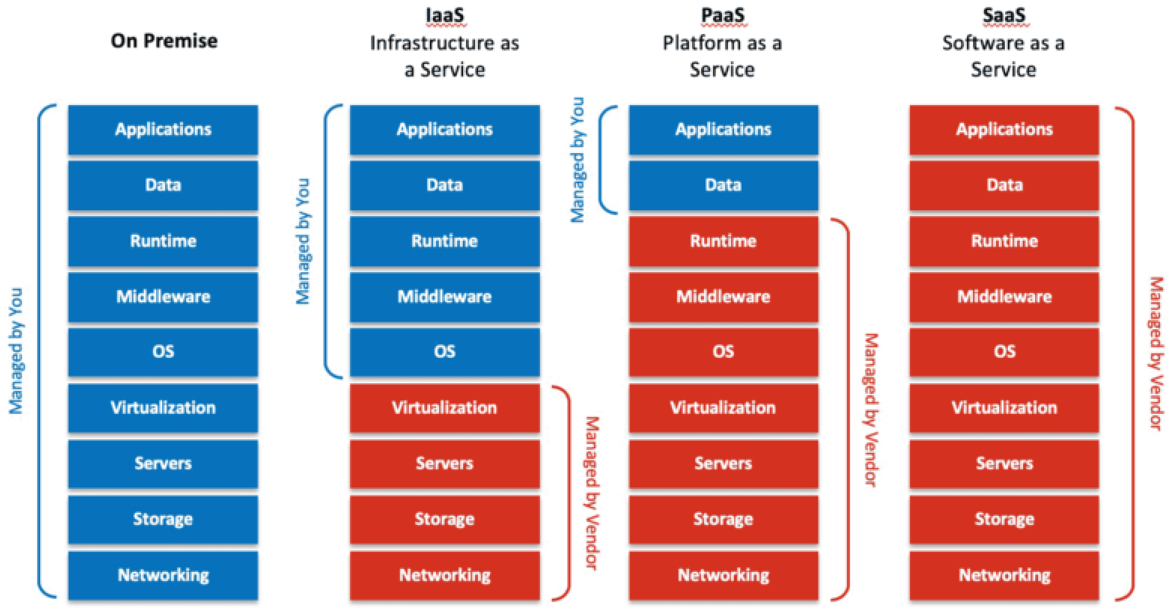
- Easy parallel with traditional on-premises IT

Platform as a Service (PaaS)

- Removes the need for your organization to manage the underlying infrastructure
- Focus on the deployment and management of your applications

Software as a Service (SaaS)

- Completed product that is run and managed by the service provider



Example of Cloud Computing Types

Infrastructure as a Service:

- Amazon EC2 (on AWS)
- GCP, Azure, Rackspace, Digital Ocean, Linode

Platform as a Service:

- Elastic Beanstalk (on AWS)
- Heroku, Google App Engine (GCP), Windows Azure (Microsoft)

Software as a Service:

- Many AWS services (ex: Rekognition for Machine Learning)
- Google Apps (Gmail), Dropbox, Zoom

Pricing of Cloud

- AWS has 3 pricing fundamentals, following the pay-as-you-go pricing model
- Compute:
  - Pay for compute time

- Storage:
    - Pay for data stored in the Cloud
- Data transfer OUT of the Cloud:
    - Data transfer IN is free
- Solves the expensive issue of traditional IT

Service Models Examples

Infrastructure as a Service (IaaS): As the name suggests, it provides computing infrastructure and other resources such as virtual-machines, block or file-based storage, load balancers, IP addresses, virtual networks etc.

Example: Azure virtual machines, Amazon EC2, Rackspace.

Platform as a Service (PaaS): As the name suggests, it provides you computing platforms which typically includes operating system, programming language execution environment, database, web server etc.

Example: AWS Elastic Beanstalk, Windows Azure, Heroku etc.

Software as a Service (SaaS): Provides on-demand software and there is no need to worry about installation and setup of the application.

Example: Microsoft office 365, salesforce.com.

IDaaS

Identity as a service (**IDaaS**) is a SaaS-based identity and access management offering.

Identity as a Service (IDaaS) is the authentication infrastructure that is hosted and managed by a third-party service provider.

Types of identities available are:

1. **Internal Users**: Internal users are part of an organization such as employees and maintenance personnel.
2. **External Users**: External users are those who are using the product or service implemented by an organization such as business partners.
3. **Consumers**: Users who use authentication mechanisms to utilize the application such as Facebook.

Core aspects of IDaaS:

1. **Identity Governance and Administration** (IGA): Provision cloud users and enable password reset functionality.
2. **Access**: User authentication, SSO, and such authorization-based integration.
3. **Intelligence**: Identity access log monitoring and reporting.

Multi-factor authentication is one such type of application such as GitHub where users need to submit multiple factors to access the data.

DaaS

Data as a service is another cloud service model which is a little bit more ambiguous than some of the other cloud service models.

- It refers to the fact that data stored in the cloud is available over the network remotely on demand, anytime of day using any type of device where data is stored on cloud service provider infrastructure.
- The data can be included of anything such as files, entire databases, photographs, videos, website data. So , it's quite ambiguous and generic in that way. Geographic location is irrelevant because when it comes to storing data in the cloud, cloud providers have the option of replicating data between their data centers around the globe, thus making the data that the user needs locally available.

DaaS examples

Let's see some specific DaaS examples, but do understand these examples can also fall under other cloud service models.

- Google Drive is the file storage solution in the cloud just like Microsoft OneDrive is. Now these types of offerings might be considered Software as a Service, but on a broader scope we referred to it as Data as a Service.
- Flickr is a popular web site on the Internet for photography where photography enthusiast can upload photographs they have taken and they can discuss the particulars related to that. And it's all stored online, hence in the cloud. So, this is considered Data as a Service.

BPaaS Additional Cloud Service Models

BPaaS (Business process as a service) is another cloud service model that is anything required for the business to function, although it may not be related to the nature of the business. For example, of a business process might include payment card processing, if you want your customers to be able to purchase our goods of services with the debit card or credit card, that payment has to be processed somewhere somehow. So, you might outsource that and have it run in the cloud.

- Business Process as a Service is considered a higher-level cloud service model that sits upon things like SaaS, PaaS, IaaS and like all cloud services, business processes that are running in the cloud are delivered remotely over the network.

CaaS

CaaS (communication as a service) *is another cloud service model that involves anything like phones, emails, messaging, video conferencing which are outsourced, handled and also responsible by cloud provider.*

- So the service would be remotely available over the network. Now in some cases when it comes to CaaS, you might still have physical hardware on premises. For example, you might have cameras for video conferencing, you might have voiceover IP telephones, physically at your site. But their configuration and how they are managed would be handled in the cloud. So voiceover IP is a good example of CaaS being hosted and being the responsibility of the cloud provider.
- Instant Messaging is another great example, we wouldn't have to have servers under our control that would allow Instant Messaging, that would be the responsibility of the cloud provider.

Note - Anything as a Service is a generic term that refers to these cloud service models.

Cloud Deployment Models

A cloud deployment model is used to represent a specific cloud environment type, differentiated based on the type of users availing the cloud models.

The four common models are -

1. Public Cloud

2. Private Cloud

3. Hybrid Cloud

4. Community Cloud

Public Cloud

Public cloud is a cloud environment owned by a third-party cloud provider that enables availability of resources such as applications, virtual machines, etc., to the general public over the internet.

Few of such providers are Amazon Web Services, Microsoft Azure.

A public cloud being a fully virtualized environment provides services in a multi-tenant fashion. Each tenant's data remains separated from other's data.

Success of a public cloud relies on a high bandwidth network connectivity enabling faster data transmission.

Salient Examples

- Cloud storage services
- Online software applications
- Cloud hosting and the list grows.

Benefits of Public Cloud

Scalability: On-demand availability of resources.

Cost Effective: Expenditure reduced due to centralized management of resources.

Reliability: Backup support enabled in case of failures.

Flexibility: Offers all services such as IaaS, PaaS, and SaaS.

Location Independent: Services are enabled to consumers anywhere and anytime.

- The most common deployment model
- Offers resources without the responsibility of ownership
- Independent consumers rent a specific space
- The cloud provider is responsible for providing services, and all management and maintenance of the underlying infrastructure, resource- consumption, and security
- Consumer needs to take steps to make sure data remains confidential
- Allows you to host client workloads and add more computing power or storage whenever it is needed, without disruption

Private Cloud

Private cloud is also recognized as an **internal cloud or corporate cloud**.

Usually built and owned within an organization and is a secured cloud-based environment accessible only for the organization.

In a private cloud:

- Administration can be done either by an internal or by an outsourced staff.
- Same organization technically plays both the roles of cloud consumer and cloud provider.

Private cloud is most ideal for the organizations which require **direct control over the environments to meet security and business compliance requirements**.

Benefits of Private Cloud

Higher Security and Privacy: Achieved using access restrictions to connections made to resources.

Legal Compliance: Can be deployed in accordance with any retention and access-control policies.

Better Control: Since private cloud can be accessed only by a single organization, that organization will configure and manage it based on their needs.

- Private clouds are controlled by a single organization.
- In a private cloud there is complete control over the infrastructure, reliability, and performance.
- You can buy or rent a private cloud
- If bought then the organization is responsible for all management and maintenance.
- If rented, the service provider will take care of the infrastructure.

Hybrid Cloud

Hybrid cloud environment is the combination of both private and public clouds.

Organizations use a Hybrid cloud to deploy private clouds for critical workloads and a public cloud to host less critical (or less sensitive) workloads.

An e-commerce website could be an ideal example. It can be hosted within a private cloud for better security, while its brochure site can be hosted within a public cloud for cost-effectiveness.

If your organization wishes to establish a hybrid cloud, it needs to ensure:

- Availability of a Public IaaS platform (such as AWS, Microsoft Azure).
- Availability of a private cloud (on-premises or through a private cloud provider).
- Ensure adequate WAN (wide area network) connectivity between the two cloud environments.

Typically, an enterprise opts for a public cloud for accessing compute instances, storage resources or other services like big data analytics and it must develop its own private cloud that is compatible with the public cloud.

- Blends private and public cloud infrastructures
- Helps organizations that are busy during particular times of the year
- Scales to demand by using the private cloud for normal workloads and a public cloud for busy periods
- Combining private and public clouds allows the ability to provide extra resources and storage capacity on demand
- Hybrid clouds allow organizations to separate sensitive data from data that is less vital

Community Cloud

A community cloud is a multi-tenant platform allowing several groups with the same purpose to work on a single platform.

- Similar to a public cloud but with access restricted to a limited set of people.
- Owned jointly by the community members or by a third-party cloud provider.
- The community members typically own the responsibility for defining and evolving the cloud environment.

Suitable for joint ventures, research organizations.

- In a community cloud, different organizations share the cloud
- The organizations will have very similar security, privacy, and performance needs
- The organizations will share the cloud's infrastructure and resources
- The community, will have similarly prescribed tools for each organization to control their users' experiences

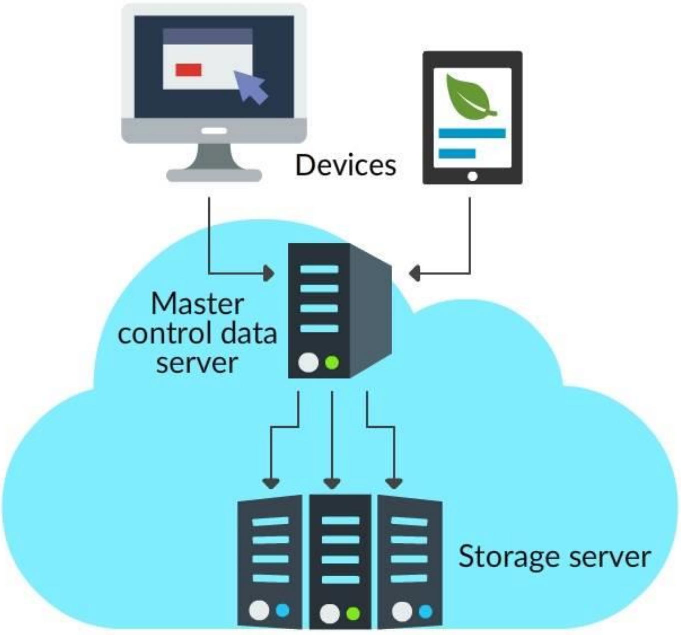
Cloud Storage and APIs

An online space that is used to store your data such as

- files
- videos
- music
- other structured/semi-structured/unstructured data,

and can be accessed by any device is known as `cloud storage`.

How Cloud Storage works



The image illustrates the way cloud storage ideally works.

1. The data from your cloud-enabled device is uploaded into the cloud through a third-party application such as Dropbox.
2. The uploaded data reaches a master control data server located in a data center owned by your cloud service provider. The master server maintains a copy of your data in various storage servers.
3. The data is stored across many machines in the cloud geographically, where you can retrieve it using APIs or web-based protocols.

Cloud Storage Security

Cloud storage providers enable security of the data by adopting various methods:

Encryption: A complex algorithm is used to encode your data, users will need the encryption key to decode the data.

Authentication: Protects access to data by enforcing users to create username and password. Multiple levels of authorization such as multi-factor authentication will be used as appropriate.

Cloud Storage Benefits

- A reliable and secure system to back up your essential files.
- Files stored in the cloud can be retrieved remotely.
- Files are accessible from anywhere.
- An affordable way of protecting important data.
- An assurance of restoration of data from any unwanted failure or data loss.
- No need to install storage equipment.
- Offers enough mobility in the workflow of a business or company.

Cloud Storage Risks

Irrespective of the many benefits, cloud storage, comes with a few notable risks as well:

1. Data security (data is vulnerable when it is transferred to and from the cloud).
2. Accessibility depends on network connectivity.
3. Cost depends on the usage.

Cloud APIs

Cloud application programming interface serves as a layer between `users, cloud services, and resources`.

It interacts with the cloud infrastructure to assist with

- Computing
- Storage and
- Network resources for requested cloud applications or services.

Cloud APIs vary according to the provided services, as follows:

- **Infrastructure as a Service (IaaS)**: Infrastructure APIs help in the provision of computing and storage resources.
- **Software as a Service (SaaS)**: SaaS APIs enable connectivity and interaction with the application layer.
- **Platform as a Service (PaaS)**: PaaS APIs provide back-end architecture, functionality for the applications.

Cloud Migration

Businesses are slowly migrating from on-premise to cloud due to **scalability, reliability, and high availability** offered by the cloud.

Do you think these are the only criteria? The answer is NO.

In this topic, you will understand **important considerations** when you plan to migrate and use the cloud for your business needs.

Cloud Migration Strategy

6 R's

Refactor or Rearchitect

Refactoring and re-architecting of applications and is usually driven by a business need to add features or for scalability. Refactoring/re-architecting often boosts agility, business continuity, and overall productivity and collaboration. However, this strategy tends to be the most expensive and is usually executed after an initial migration via one of the other approaches, like rehosting.

Replatform

Well-established organizations sometimes have a legacy system that is far too structured to move into IaaS cloud platforms. Instead of changing the core of the applications, the applications are emulated through a virtual machine so that legacy IT systems can become compatible with modern day cloud technologies. Replatforming, though sometimes costly, is a far better option for companies that cannot restructure the IT legacy systems at the time of cloud migration.

Rehost

Rehosting is a popular migration strategy also known as "lift and shift." It is a quick solution for migrating to the cloud and moves applications, software, and data to cloud with little effort. Rehosting is popular for initial migrations because it involves moving existing physical and virtual servers into an IaaS solution. The IaaS model hosts the infrastructure that is typically found on sites, such as the servers, storage, and networking hardware and offers a virtualized environment through a hypervisor layer. Rehosting may lead companies to re-architecting in the future, once a cloud-based operation is in place.

Repurchase

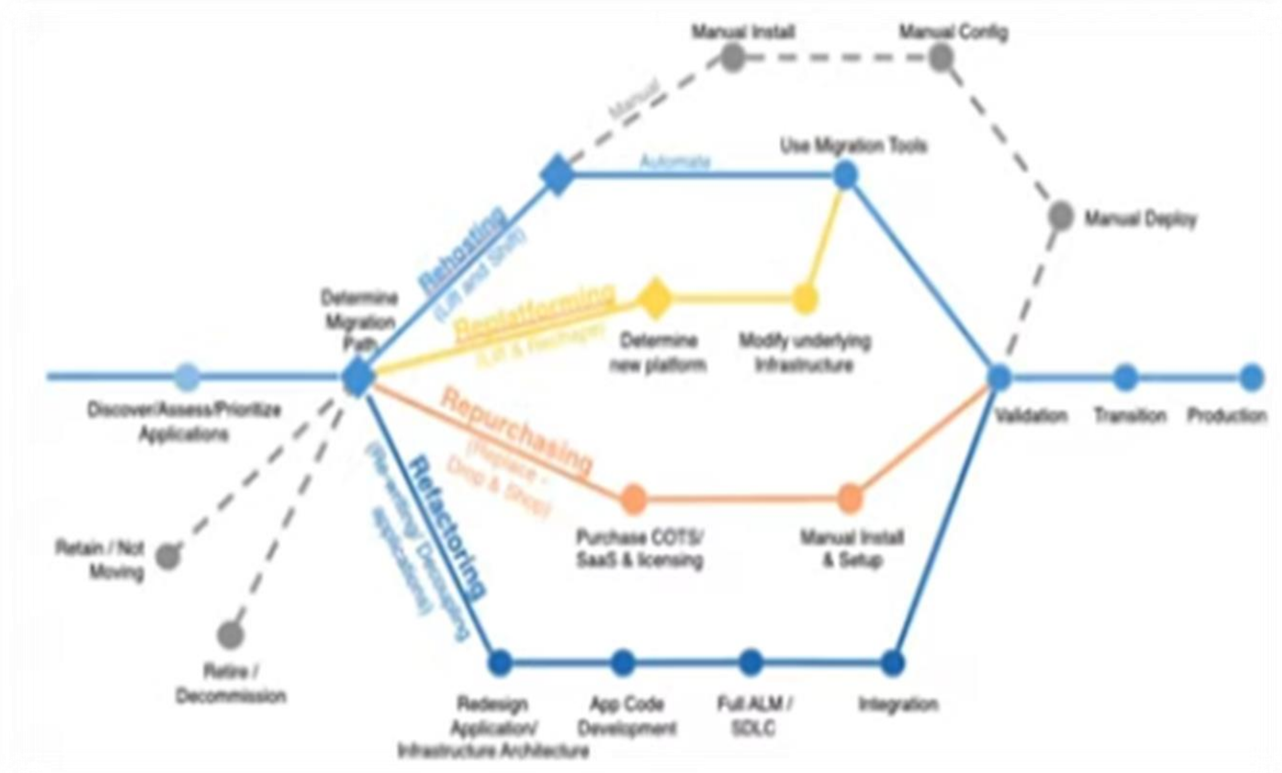
Repurchasing, when possible is an excellent and fast way to access cloud-based SaaS that is tailored to your business needs by the cloud provider. SaaS, or software as a service, takes your company's existing data and applications and articulates them in a cloud-based product to help manage operations, such as human resources (HR), customer relationship management (CRM), or content management (CMS).

Retain

Some elements of your environment may not migrate and are retained as-is. There are many reasons to maintain an in-house element, such as riding out the depreciation value or the cost of migration is too high, and your company can maintain more value using the application or service on the ground. Retaining some IT aspects on-premise is a popular chose for a hybrid cloud service.

Retire

Identifying everything in your business environment that have the potential to migrate allows you to evaluate the value of the product, service, or application. Identify all the users of each migration element and see what's being used and what is not. Determining what you can retire will also help save money on elements that should have been previously phased out of use.



Cloud Migration Benefits

Here are some common scenarios that will be benefited from cloud migration.

- If your application is experiencing increased traffic and it is difficult to meet the demand.
- When your clients need faster deployment and access to applications (cloud increases focus on development rather than infrastructure implementation).
- When it's becoming more difficult and expensive to keep up with your growing storage needs.
- Benefits start-ups (cloud computing shifts IT expenditure to a pay-as-you-go model).

Costing the Cloud

Costing is broadly categorized as:

- **CAPEX** (Capital Expense)
- **OPEX** (Operational Expense)

Given here are certain scenarios that illustrate the usage of CAPEX and OPEX:

- In traditional Internal IT Infrastructure environment where everything is set up and managed internally, high CAPEX and OPEX are incurred.

- In case of a colocation facility, where a location that hosts the infrastructure is owned or rented from a third party, high CAPEX and a slightly lower OPEX is incurred.
- Consider an environment where services are managed by outsourcing them, it incurs reduced CAPEX and increased OPEX.
- Now, if you consider a public cloud in which the infrastructure is fully outsourced, it incurs only OPEX and CAPEX is cutoff.

Cloud Cost Models

If you plan to adopt a cloud model, you need to consider reducing the operational cost as against reducing the capital expenses.

Given here are some commonly used cloud models:

Free Payment Model: Majorly used in marketing or advertising type of companies where consumers will be able to register and use the service freely. It helps the companies to market their product based on the usage metrics.

Plan Payment Model: Subscription-based usage, where users will be allowed to access the cloud for a specific period/cost.

Pay as you use: As the name suggests in this model, you will pay based on what you have used.

Applications Suitability for Cloud

Cloud computing can certainly provide a number of benefits. But when considering a move to the cloud, you'll also have to consider your applications and certain applications are better suited to cloud computing than others.

- So, you want to consider applications that are required only for a limited period, maybe your organization is going through a developmental phase that is only going to be temporary and you require some kind of software application to support that phase.
- At the end of the day, you are still relying on your internet connectivity when accessing the cloud services. So, an application that is non-critical is a little better suited to the cloud because if you do lose your internet, you lose access to the cloud and hence to that application.
- So public cloud models are a great solution for Startup companies, particularly because of the minimal initial capital outlay and the scalability that's offered.
- It may not be the ideal solution for legacy systems, mission-critical applications, or applications that handle sensitive data as there might be an increased cost in dealing with any kind of outdated technologies or proprietary hardware and software that's required to drive them. They may not be compatible with the cloud platform and again for mission-critical applications you're relying on the Internet.
- So that could be disastrous and applications handling the sensitive data has an increased risk with transferring or storing highly confidential or sensitive information in the cloud because it is no longer under your physical control. So, you always need to be aware of that.

These are some of the limitations and considerations in terms of assessing your application compatibility for a cloud type of environment.

Common Scenarios

Common scenarios where cloud computing plays a major role:

***Compute Clouds**: Enables organizations to access resources on-demand (highly scalable and inexpensive).*

***Compute Storage**: Enables organizations to maintain and secure data offsite.*

***Cloud Applications**: Organizations can deploy and host applications on a cloud to enable ease of access for the users.*

Operational Benefits

- **Reduced Cost**: Cloud computing reduces your operational and infrastructure costs considerably.
- **Increased Storage**: You can store as much as data you need on a cloud.
- **Automation**: Updates to the software and applications are taken care of automatically.
- **Flexibility**: Easy to test and deploy your applications.
- **Mobility**: Cloud is always available for you anytime and anywhere.

Shared Responsibility Model

If the IT infrastructure is managed on-premises (in their own data center), the organization is accountable for the security of those applications, infrastructure, and the data that resides.

Whereas, if the organization decides to opt for a public cloud computing model, it will need to sort out what IT security responsibilities are to be handed over to the cloud provider.

The cloud provider and the cloud user will be made responsible for different security aspects and should work together to ensure full coverage.

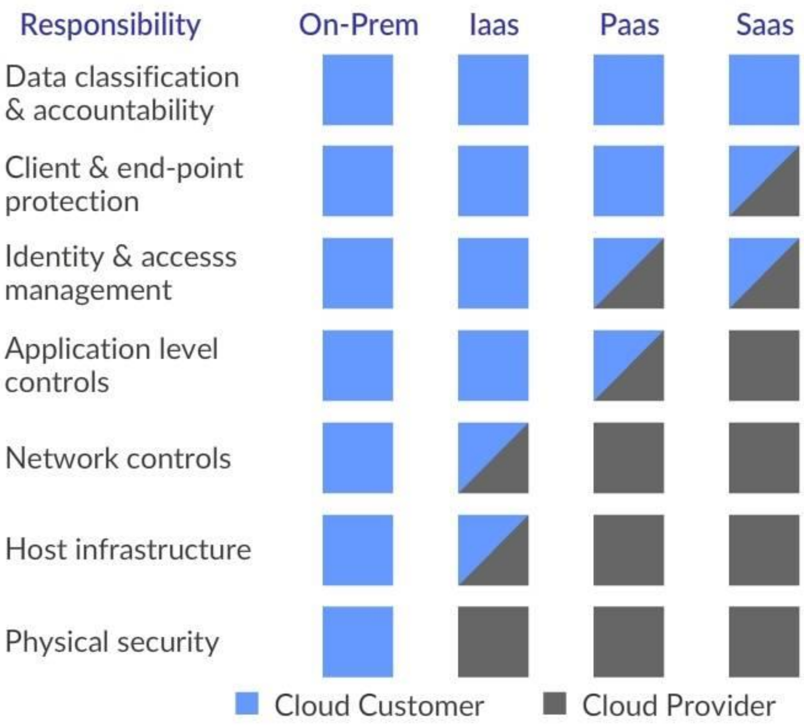
This activity is achieved by a shared responsibility model.

It is a cloud security framework that describes a cloud service provider’s security commitment and its users to ensure responsibilities.

While you move across the various cloud service models (IaaS to PaaS to SaaS), the responsibility of the cloud service providers increases and the customer's responsibilities reduces.

- In IaaS, the service provider is responsible for physical security, host infrastructure, and network controls and the rest are taken care of by the customer.
- In PaaS, the service providers are responsible for application level controls, identity management in addition to those mentioned for the IaaS model.
- In SaaS, the service provider is responsible for the whole application package.

Shared Responsibility in Microsoft



Responsibility	On-Prem	Iaas	Paas	Saas
Data classification & accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◩
Identity & accesss management	🟦	🟦	◩	◩
Application level controls	🟦	🟦	◩	⬛
Network controls	🟦	◩	⬛	⬛
Host infrastructure	🟦	◩	⬛	⬛
Physical security	🟦	⬛	⬛	⬛

🟦 Cloud Customer ⬛ Cloud Provider

The customer and service provider responsibilities differ based on the services chosen. The above picture includes the responsibilities of customers and service provider in on-premises and off-premises based on services.

Shared Responsibility Model: AWS

*AWS has devised three responsibility models for **infrastructure services, container services, and abstract services**.*

- In the infrastructure model, AWS is responsible for the security of the cloud, and any data that goes into the cloud becomes the customer's responsibility.
- In the container model, AWS takes the additional responsibility for the OS, network configuration, platform and application management.
- In the abstract model, AWS takes the whole responsibility except for the customer-side data and data encryption.

FP—55540—Azure Essentials

Introduction to azure

Azure Essentials

`Azure Essentials` is the first of the series of courses on **Azure**.

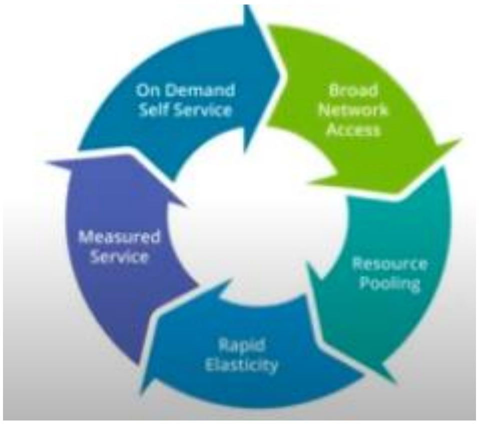
The content for this course has been taken from https://learn.microsoft.com/en-us/#/

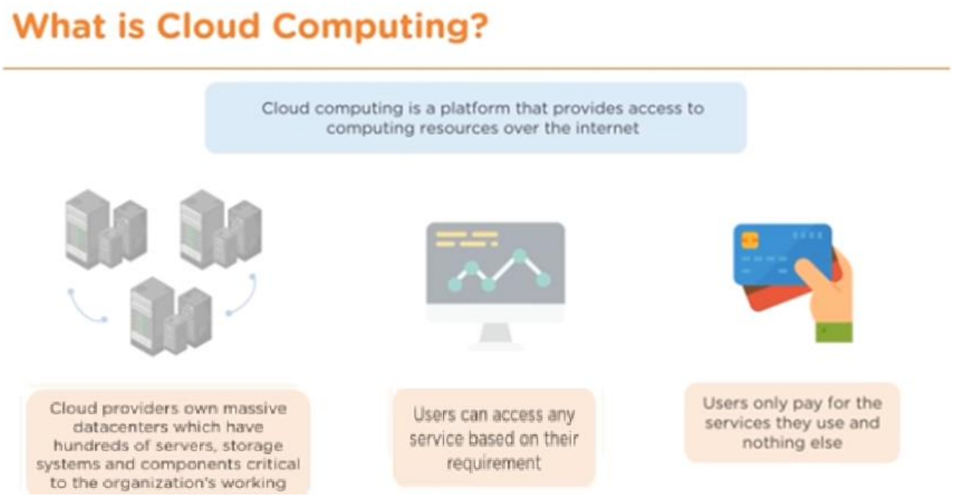
What is Microsoft Azure?

Microsoft Azure is a set of unified cloud services, which help IT professionals and developers to **build, deploy** and **manage applications** through the global network of Azure data centers.

What is Cloud Computing

Cloud Computing is the use of remote servers on the internet to Store, Manage and Process data rather than a local server or your personal computer.





What is Cloud Computing?

Cloud computing is a platform that provides access to computing resources over the internet

Cloud providers own massive datacenters which have hundreds of servers, storage systems and components critical to the organization's working

Users can access any service based on their requirement

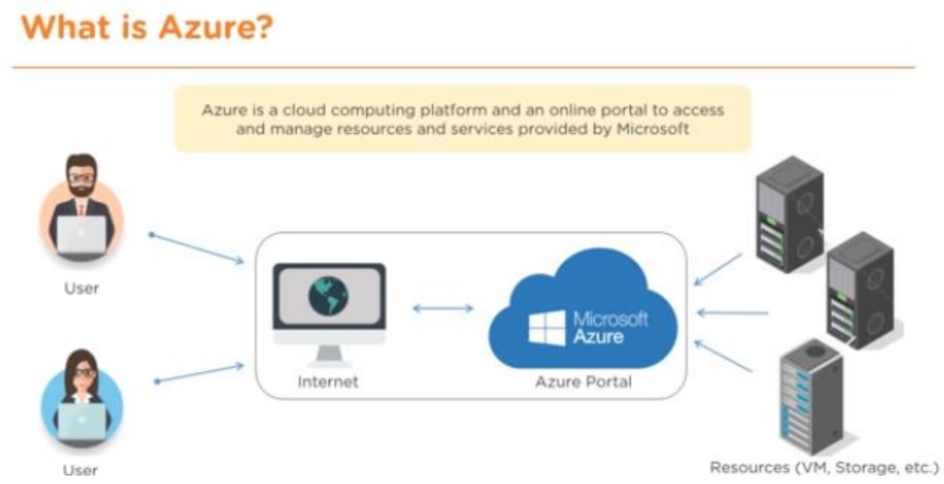
Users only pay for the services they use and nothing else

What is Azure

- Microsoft Azure is set of cloud services to help your organisation meet your business challenges.
- It's the freedom to build, manage and deploy applications on a massive, global network Microsoft Azure
- Using your favourite tools and frameworks

Azure is a cloud computing platform and an online portal that allows you to access and manage cloud services and resources provided by Microsoft

- Microsoft Azure is flexible. Resources can be computed up and down as needed
- It is highly reliable with high availability and 24x7 tech support
- It offers to pay for what you use pricing plan
- Azure supports backup and disaster recovery tools



What is Azure?

Azure is a cloud computing platform and an online portal to access and manage resources and services provided by Microsoft

User

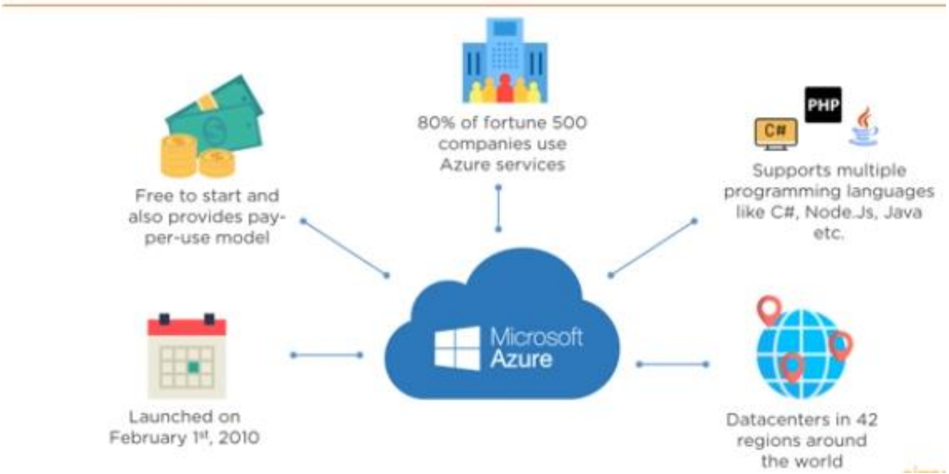
User

Internet

Microsoft Azure

Azure Portal

Resources (VM, Storage, etc.)



Free to start and also provides pay-per-use model

80% of fortune 500 companies use Azure services

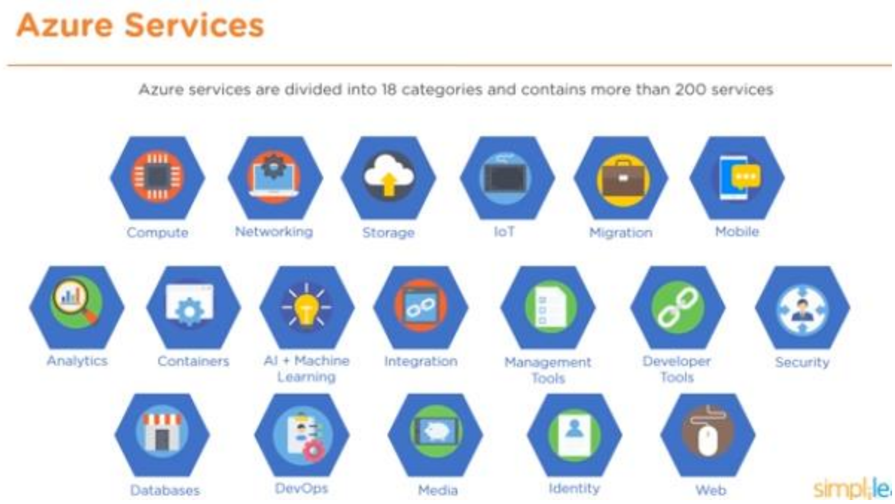
Supports multiple programming languages like C#, Node.Js, Java etc.

Launched on February 1st, 2010

Microsoft Azure

Datacenters in 42 regions around the world

Azure Cloud Services



Azure Services

Azure services are divided into 18 categories and contains more than 200 services

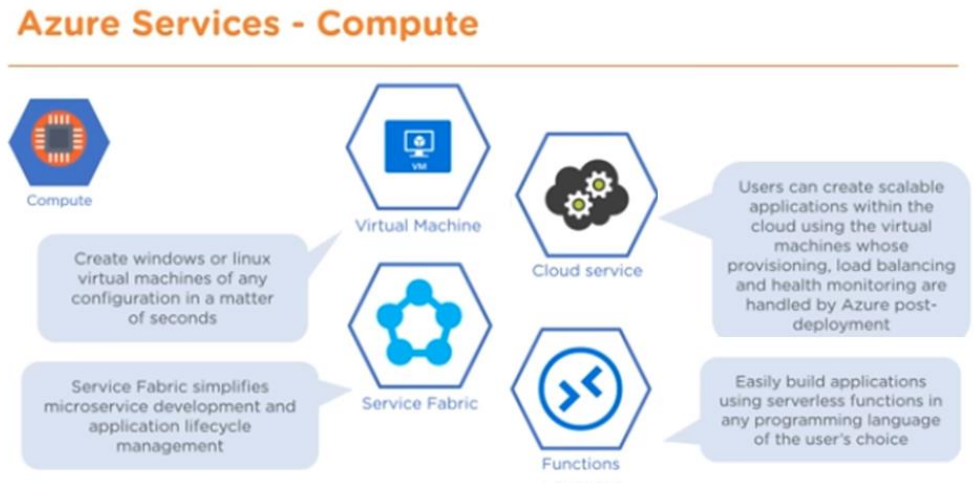
Compute, Networking, Storage, IoT, Migration, Mobile

Analytics, Containers, AI + Machine Learning, Integration, Management Tools, Developer Tools, Security

Databases, DevOps, Media, Identity, Web

simplilea

Azure Services - Compute



Azure Services - Compute

Compute

Virtual Machine

Create windows or linux virtual machines of any configuration in a matter of seconds

Service Fabric

Service Fabric simplifies microservice development and application lifecycle management

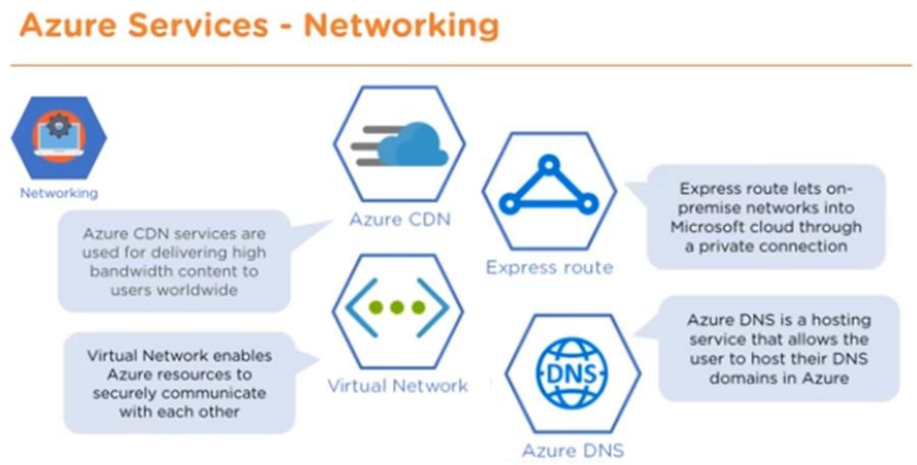
Cloud service

Users can create scalable applications within the cloud using the virtual machines whose provisioning, load balancing and health monitoring are handled by Azure post-deployment

Functions

Easily build applications using serverless functions in any programming language of the user's choice

Azure Services - Networking



Azure Services - Networking

Networking

Azure CDN

Azure CDN services are used for delivering high bandwidth content to users worldwide

Virtual Network

Virtual Network enables Azure resources to securely communicate with each other

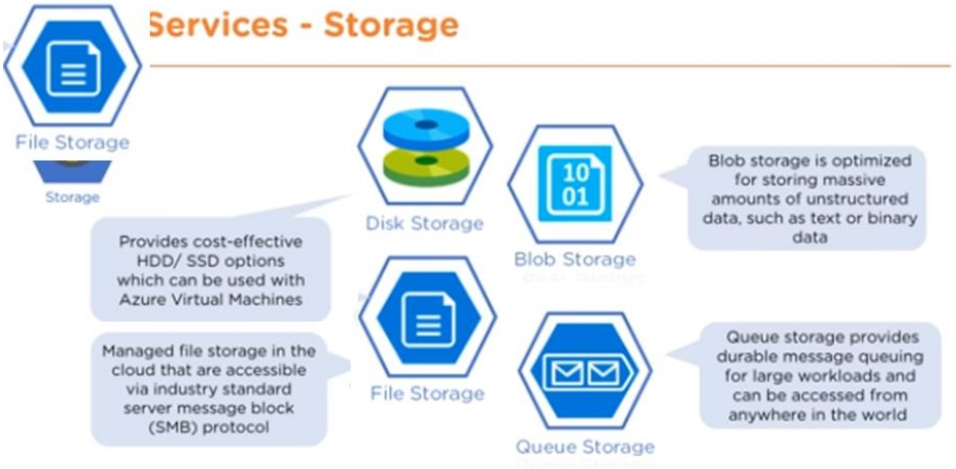
Express route

Express route lets on-premise networks into Microsoft cloud through a private connection

Azure DNS

Azure DNS is a hosting service that allows the user to host their DNS domains in Azure

Azure Services - Storage



Services - Storage

File Storage

Storage

Disk Storage

Provides cost-effective HDD/ SSD options which can be used with Azure Virtual Machines

File Storage

Managed file storage in the cloud that are accessible via industry standard server message block (SMB) protocol

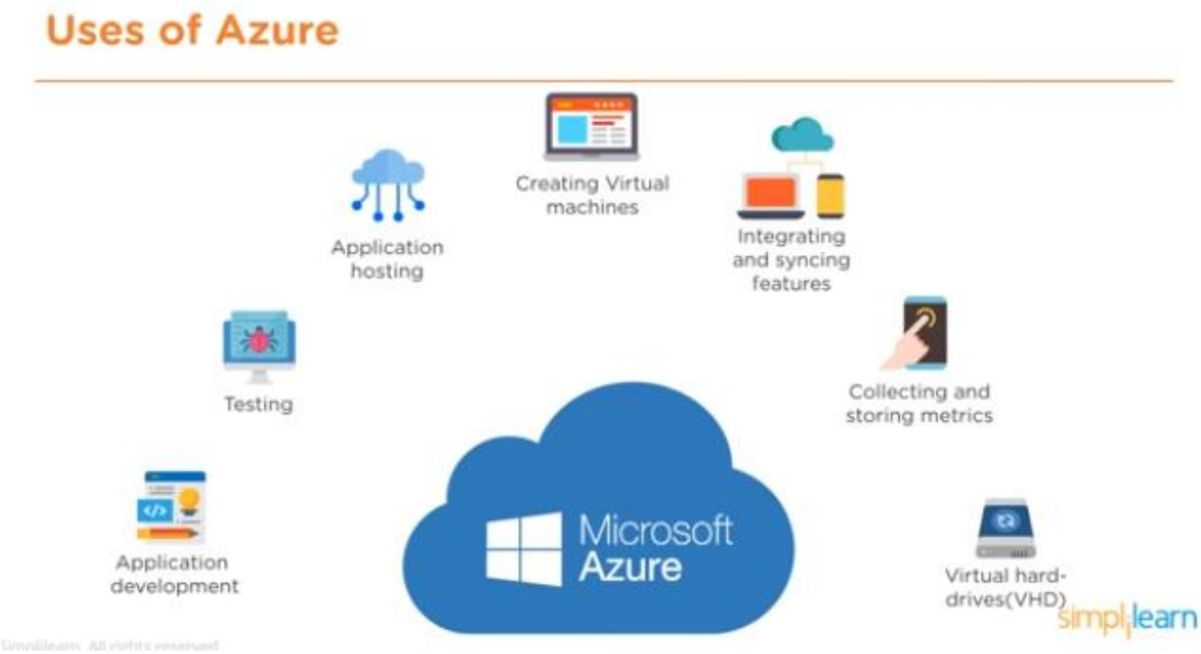
Blob Storage

Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data

Queue Storage

Queue storage provides durable message queuing for large workloads and can be accessed from anywhere in the world

Uses of Azure


Uses of Azure
Creating Virtual machines
Application hosting
Integrating and syncing features
Testing
Collecting and storing metrics
Application development
Microsoft Azure
Virtual hard-drives(VHD)
simplilearn
©Simplilearn. All rights reserved.

Overview of Azure Services

Azure provides cloud services that can be used to design and implement your customized cloud solution and infrastructure. They allow you to:

- Migrate on-premises datacentre to Azure cloud
- Deploy cloud-based applications
- Host workload in the Azure cloud
- Integrate Azure cloud services with an on-premises infrastructure

Azure cloud services can be categorized as **Compute**, **Network**, **Data and Storage**, **App Services**, etc. These are few to name and there are much more to help with **Identity and Access Management**, **Automation**, **Security**, **Availability**, etc.

Azure as IaaS (Infrastructure as a Service)

Allows the user to access, manage and monitor the data centers. Thus, giving complete control of the OS and the application platform stack to the developers.

- The virtual machine can be completely modified to meet business requirements.
- IaaS facilitates efficient design time portability. Hence an application can be migrated to Microsoft Azure without rework.
- IaaS allows a quick transition of services to cloud, which helps the vendors to offer services to their clients easily.

IaaS is perfect for the applications where complete control is required.

Azure as PaaS (Platform as a Service)

The client is provided with the **`platform to develop and deploy software`**, without having to think about hardware and infrastructure. It takes care of most of the OS, servers and networking issues.

- `PaaS is fast` with less hassle for developers; applications can go from idea to availability more quickly.
- `PaaS is cost-effective` with lower upfront investment and less admin / management work for organizations.
- `PaaS lowers risk` as platform is upto date with latest technology stack and tools for automation.

Azure as SaaS (Software as a Service)

Software as a service (SaaS) allows users to connect to and use cloud-based apps over the Internet, such as Office365.

SaaS customers use the software running on the provider's infrastructure. SaaS is also referred as **software delivered over the web.**

Advantages:

- Gained access to sophisticated enterprise applications
- Pay only for what you use
- Use free client software
- Mobilise your workforce easily
- Access app data from anywhere

Azure Datacenters

Azure is backed by a **global network of data centers** that aims to meet global customer needs, ensure high application performance and maintain availability.

Azure Management Tools

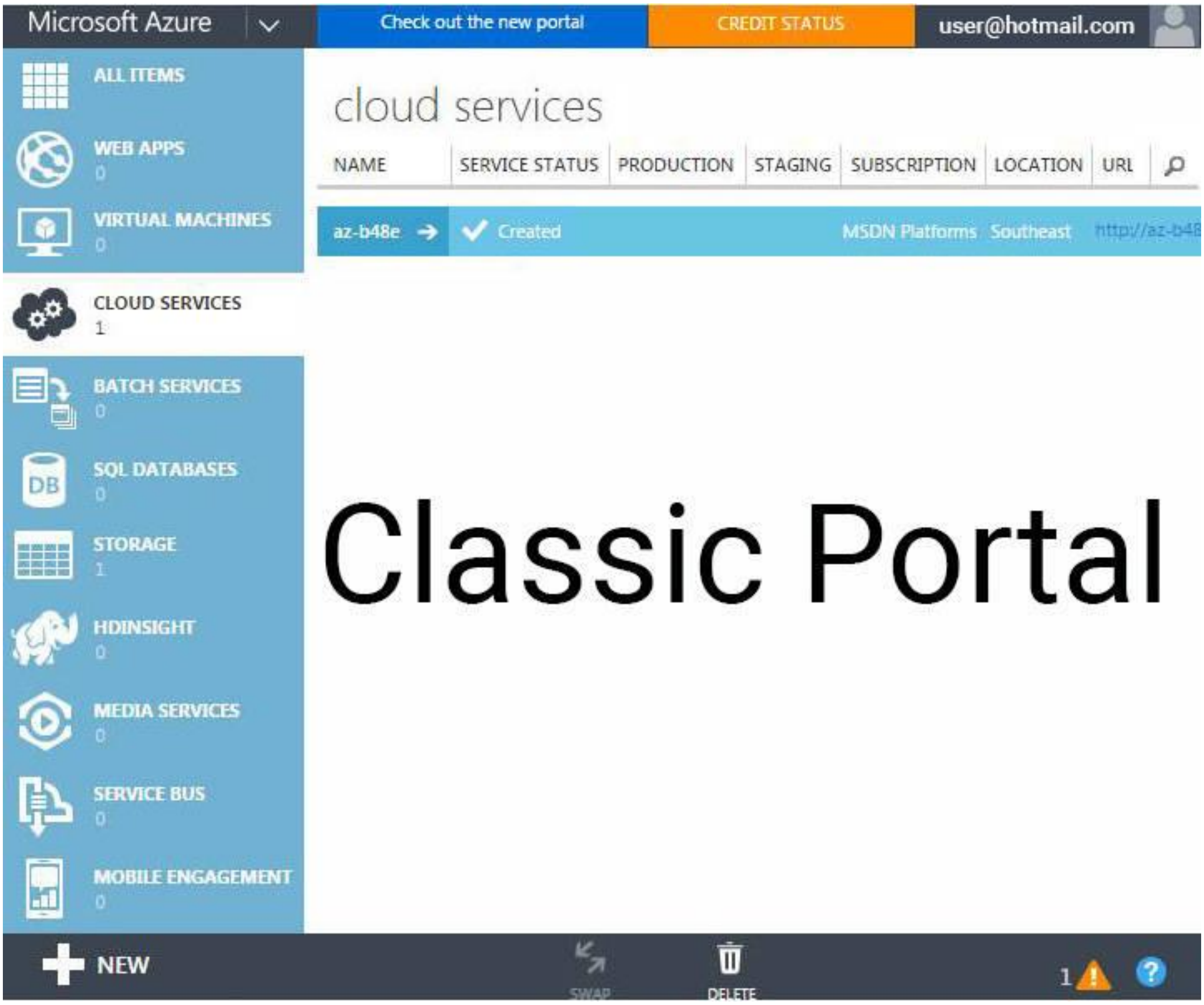
Accessing Azure

Azure can be accessed and managed through:

- Azure Classic Portal
- Azure ARM portal
- Azure Resource Manager
- Client Tools like
  - PowerShell
  - Azure CLI

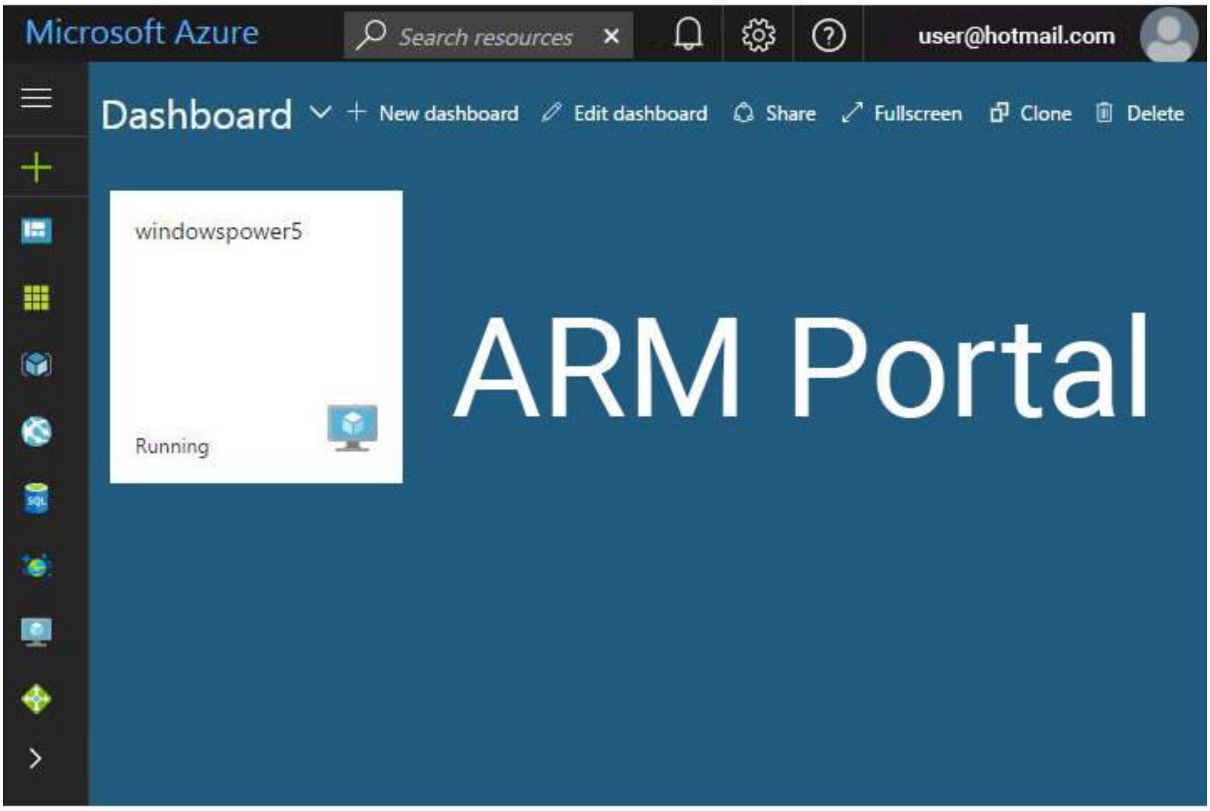
- Visual Studio with Azure SDK for .NET

Azure Classic Portal



This was the first portal in Azure that was being used before the launch of Azure Resource Manager (ARM). It was based on the **Service Management model** and provides **limited Role-Based Access Control (RBAC) support**.

Azure Resources Manager



Azure Resources manager (ARM portal) is now the default portal for Azure cloud services management. It supports new features like:

- Templates based deployments
- Role-based Access Control (RBAC)
- Customized dashboards to view key resources

https://portal.azure.com/

Client Tools

While Azure portals provide a GUI for managing your Azure subscriptions and services, in some scenarios, these portals may not offer the most optimal management capabilities.

For teams that want to **perform service management in an automated fashion** by using REST API and creating scripts for repetitive or cumbersome administrative tasks, Azure offers options like:

Azure PowerShell modules - to run scripts from Windows.

Azure command-line interface (CLI) - to run scripts on all operating systems like Windows, Linux, and macOS.

Azure PowerShell modules

PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language. Initially a Windows component only, known as Windows PowerShell, it was made open-source and cross-platform on 18 August 2016 with the introduction of PowerShell Core.

How to use PowerShell?

- Tasks are executed by **command-lets (cmdlets)**
- Each command-let contains verb which describes action that will be taken
  - **Get**-Process
  - **Join**-Path
  - **Connect**-PSSession
- All PowerShell command-lets are parametrized to ensure maximum flexibility

Azure PowerShell Overview

Azure PowerShell is a set of cmdlets designed to help with management of Azure resources directly from the PowerShell command line.

Common Scenarios

Azure PowerShell (same goes for CLI) can be used for

- **Day to day operations**
  - Automation of repetitive tasks
  - Scheduling
  - Deployments
- **DevOps**
- **Learning**
- **Achieving things that are hard otherwise**

Basics

Two Module bundles

- AzureRm (old modules; Azure resource management)
- Az (new modules; recommended)

Easy installation

- Install-Module Az -Force -AllowClobber
- Import-Module Az

Az vs. AzureRm compatibility

Az modules are natural upgrade from AzureRm modules.

If you want to use Az but have plenty of AzureRm based scripts simply run compatibility command-let.

- Running **Enable-AzureRmAlias** command-let will make
- **Get-AzureRmVm** an alias of **Get-AzVm**

Demo

Install

1. Open Windows PowerShell as administrator
2. Run Install-Module Az -Force -AllowClobber
3. Import-Module Az

4. Connect-AzAccount

    Connect(CTRL Space for intellisence)-AzAccount - (CTRL Space for intellisence)

    1. Connect-AzAccount
    2. Prompt to log into Microsoft account
       Will show the account info.
    3. Get-AzContext
       To get the current session
    4. Selecr-AZSubscription -Subscription <Subscription Name>
       To get the current subscriptions
    5. Get-AzResourceGroup
       All the resource groups
    6. Get-AzResourceGroup | Format-Table
       This is uses of pipeline, to run more than one commands.
    7. Get-AzResourceGroup | Format-List
    8. Get-AzResourceGroup | Format-Wide
    9. Get-AzResourceGroup | Export-csv
    10. Get-AzResourceGroup | out-GridView
    11. Get-AzResourceGroup | out-GridView -PassThru
    12. Get-AzResourceGroup | Select ResourceGroupName, Location
    13. Get-AzResourceGroup | Where-Object { $_.Location -eq 'NorthEurope' }
    14. Get-AzResourceGroup | Where-Object { $_.Location -eq 'NorthEurope' } | Select ResourceGroupName, Location
    15. Multiline:
        Get-AzResourceGroup | '
        >> Where-Object { $_.Location -eq 'NorthEurope' } | '
        >> Select ResourceGroupName, Location

        Create a new Resource Group
    16. New-AzResourceGroup – Name <Name> -Location <Location>
        New-AzResourceGroup – Name azDemo -Location 'North Europe'

        Create a new VM
    17. New-AzVM – ResourceGroupName < ResourceGroupName> -Location <Location> -Name <Name> -Image <OSImage>
    18. New-AzVM – ResourceGroupName azDemo -Location 'North Europe'- Name VMDemo -Image UbuntuLTS
        Will ask for authentication

        Also ,we can use PowerShell ISC, VSCode where we can get an IDE, multitab, text editor intellisence, more powerful scripts etc

Azure Network Services

Microsoft Azure Network Services offer the foundation for developing hybrid cloud solutions with the help of following essential resources.

- **Azure Virtual Network:** Isolated network within the Microsoft Azure cloud.

- **Azure Traffic Manager**: Controls how user traffic is distributed between geographies in cloud services.
- **Name Resolution Service**: For internal hostname resolution within a cloud service.
- **Azure ExpressRoute**: Extend on-premises networks into the virtual network over a dedicated private connection facilitated by a connectivity provider.
- **Application Gateway**: works at the application layer and acts as a reverse-proxy service, terminating the client connection and forwarding requests to back-end endpoints.

What is Virtual Network?

Virtual Network, also known as a **VNet** constitutes a ***logical boundary defined by a private IP address space*** that you designate. You can distribute IP address space into one or more subnets. **This makes it functionally equivalent to on-premises networks.**

VNets are similar to AWS VPC (Virtual Private Cloud), offering various networking features like the ***ability to customize inter-VM connectivity, Virtual Private Networks (VPN), access control, DNS, routing, and DHCP blocks***.

Why Virtual Network?

Azure Virtual Network allows to securely connect cloud infrastructure to your on-premises datacentre.

- Virtual Networks allow to set up a virtual lab in the cloud by enabling connectivity to on-premises resources with the help of Point-To-Site and Site-to-Site VPN connections.
- Virtual Network also acts as a DHCP server, which allows configuring a DNS server to be leased out when a virtual machine is a spin up in the cloud.

VNet Capabilities

- **Isolation** - VNets are isolated from one another. One can create ***separate VNets for development, testing, and production*** that use the same CIDR address blocks.
- **Internet Connectivity** - By default, all Azure Virtual Machines (VM) and Cloud Services role instances are connected to a VNet and have access to the Internet.
- **VNet Connectivity** - VNet to VNet gateway needs to be configured to establish a connection between VNets.
- On-premises Connectivity - VNets can be connected to on-premises networks through ***point to site, site to site***.
- Azure Resource Connectivity - Azure resources such as Cloud Services and VMs can be connected to the same VNet. These ***resources can connect to each other using*** private IP **addresses**, even if they are on separate subnets.

Azure offers default routing between subnets, VNets, and on-premises networks, thus avoiding the need to configure and manage routes.

- **Traffic Filtering** - VM and Cloud Services role instance network traffic can be filtered outbound and inbound by destination IP address and port, source IP address and port, and protocol.
- Routing - Azure allows User-defined routes and routes.
- **Load balancing and traffic direction** - Load balances traffic to servers.

VNet Components

Subnets

A subnet is a range of IP addresses in the VNet. We can divide a VNet into multiple subnets for organization and security.

Additionally, we can configure VNet routing tables and Network Security Groups (NSG) to a subnet.

IP Addresses

There are two types of IP addresses that can be assigned to an Azure resource:

Public IP Address is used for internet/public-facing communication.

Private IP Address is used for communication within a VNet, and when using VPN gateway or ExpressRoute.

Both Public and Private IP Address can be assigned through DHCP (Dynamic Host Configuration Protocol).

Dynamic IP is allocated by default to the VM from the subnet via DHCP. When VM is started/stopped, the IP may be released/renewed based on the DHCP lease.

Static IP can be allocated to a VM, which is only released when the VM is deleted.

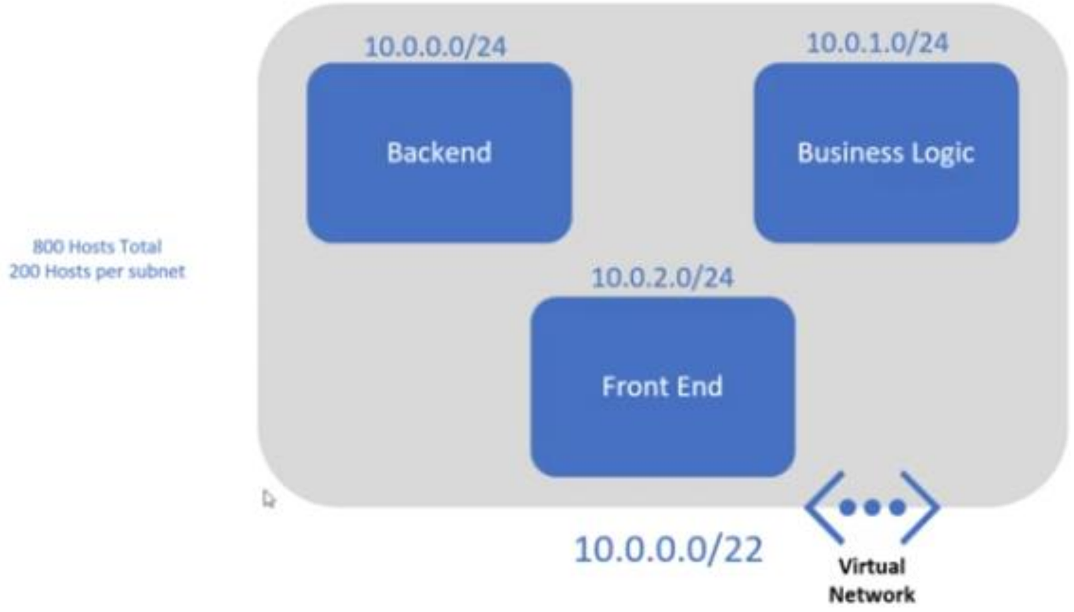
NSGs

Network Security Groups (NSGs) ***allow or deny traffic*** (through a rule base), to either a network interface or a subnet. ***By default, the outbound and inbound rules include an*** implied deny all **.**

NSGs are stateful, meaning that the TCP sequence numbers are checked in addition to checking if the connection is already established.

Creating VNs

Assume we have the following 3 tiers application



We need to create separate subnets for each tier. There needs to be 800 hosts in the VN and per subnet should have 200 hosts each. Based on these wee need to calculate address spaces and the particular address spaces provided in the image.

1. Go to Azure Portal
2. Go to Virtual Network
3. Create or Create a resource → Virtual Network→ create
4. Create a new Resource Group
5. Name for the VN
6. Location
7. Next → IP Address
8. Delete the default Azure provided IP Address. It may have more than one address spaces but never be blank.
9. 10.0.0.0/22
10. Provide at least one subnet (here 3)
11. Add
12. Then another subnet etc.
13. Next to Security - Default
14. Next to Tags→ a key-value set, to billing purpose (mainly a note)
15. Review and create.
16. Can view in Resource after creation.

We can modify the VNs or subnets later. A VN may have 255 subnets capacity. Out of which 5 (0-4) are reserved for Azure internal purpose. We may create 255 - 5 subnets.

Load balancing

Azure provides three different load balancing solutions:

- **Azure Traffic Manager**: DNS is used to direct traffic to the necessary destination. There are three destination selection methods - failover, performance or round robin.
- **Azure Load Balancer**: Performs L4 load balancing within a Virtual Network. Currently only supports round robin distribution.
- **Azure Application Gateway**: Performs L7 load balancing. Supports HTTP request based load balancing, SSL Termination, and cookie-based persistence.

DNS and Routing Tables

- `DNS name resolution` - Built-in (default) and support for custom (customer-owned) DNS.
- `Routing Tables` - Azure provides user defined routes and forced tunnelling methods.

Intersite Connectivity

Methods

There are two types of gateways.

VPN - Traffic is encrypted within the endpoints by the following modes:

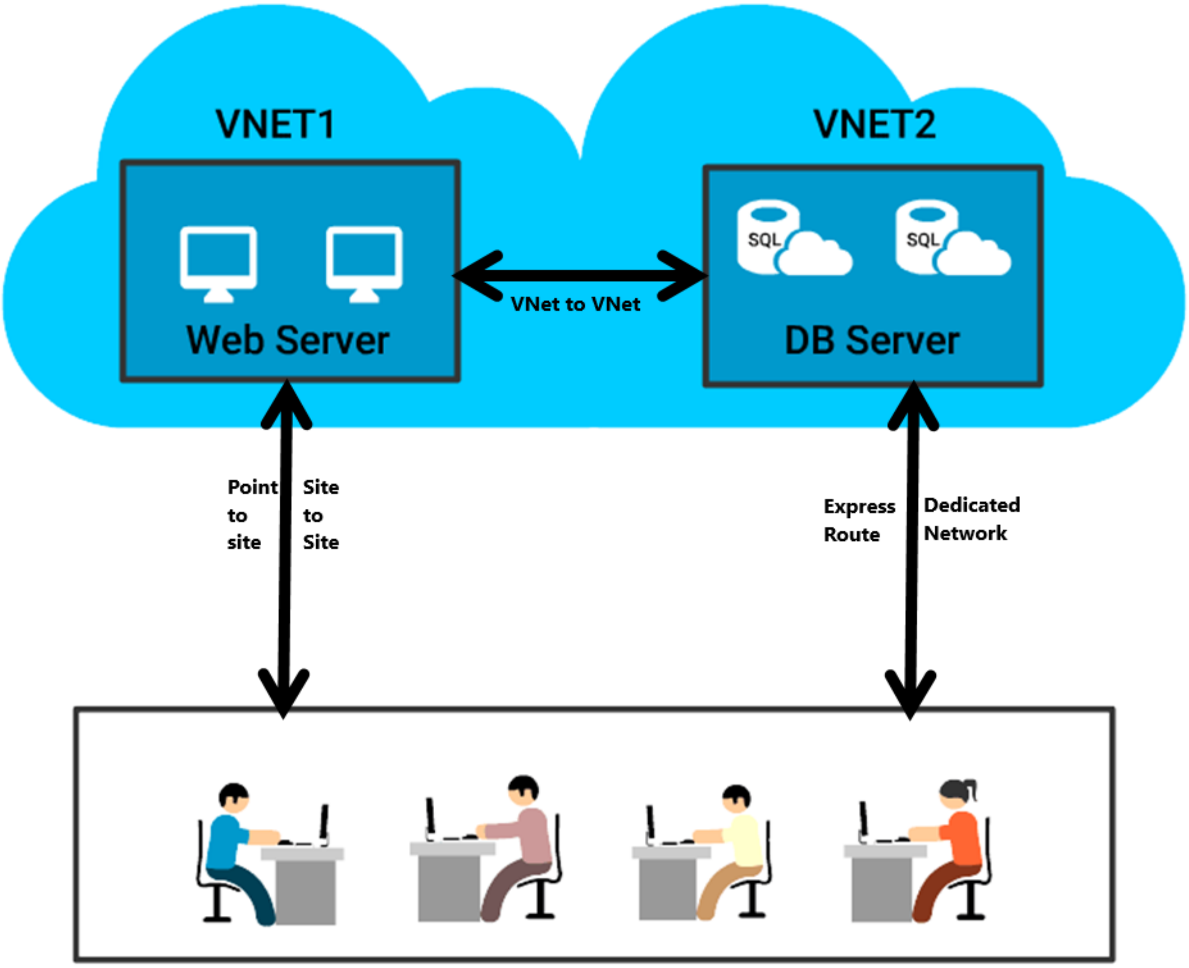
Site-to-Site - Traffic is secured using IPSEC/IKE between two VPN gateways, for example between Azure and an on-premise firewall.

Point-to-Point - Via a VPN client, a user connects to Azure, and traffic is encrypted using TLS (Transport Layer Security).

VNet-to-VNet - Traffic is secured between two Virtual Networks using IPSEC/IKE.

Express Route - It provides a dedicated peered connection into Azure.

Detailed



- **VNet to VNet Connectivity** - VPN can be used to connect two or more Azure VNets. Such connections are termed VNet-to-VNet VPNs.
- **A Point-to-Site VPN** - connects a single computer to a VNet. To create this connection, you must ***configure each on-premises computer*** that you want to use, with the resources in the VNet.
- **A Site-to-Site VPN** - connects an on-premises network and all its computers to a VNet. To create this connection, you must configure a gateway and IP routing in the on-premises network. But it is ***not necessary to configure individual on-premises computers***.
- **ExpressRoute Connectivity** - An ExpressRoute connection is a ***dedicated server*** that does not connect to the public Internet. By using ExpressRoute, you can ***increase security, reliability, and bandwidth***.

Azure Compute Services

Microsoft Azure Compute Services **offer the processing power for running cloud applications**.

The Microsoft Azure Compute Service can run many different kinds of applications. A principal goal of this platform, however, is to ***support applications that have a substantial number of simultaneous users***.

Compute Options in Azure

- **Virtual Machines** is an IaaS service that allows you to deploy and manage VMs inside a VNet.
- **App Service** is a managed service to host mobile app backends, web apps, RESTful APIs, or automated business processes.
- **Service Fabric** is known as a distributed systems platform that operates in numerous environments. Service Fabric is an orchestrator of microservices across a cluster of machines.
- **Azure Batch** is called a managed service for operating large-scale parallel and high-performance computing (HPC) applications.
- **Cloud Services** is a managed service for operating cloud applications and utilizes a PaaS hosting model.

Resource Groups

Resource groups are ***containers that are automatically created*** for VMs, DBs, and other assets that are required for your solution or only the resources that you want to manage as a group.

They provide a way to ***monitor, control access, provision and manage billing*** for collections of assets that are required to run an application.

Points to Remember

- All the ***resources in a group should share the same lifecycle*** i.e. deploy, update, and delete them together.
- If a resource (e.g. DB server), needs to exist on a different deployment cycle, it should be in another resource group.
- ***A resource can only exist in one resource group***. It can be added, moved and deleted from a resource group at any time.
- A resource group can include resources that ***reside in different regions***.
- A resource group can be used to ***control access***.
- A resource can ***interact with resources in different resource groups***. (Scenarios where two resources are related but do not share the same lifecycle).

What is Azure VM?

- Azure virtual machine is one of the wide range of services that Azure offers to create your instance Each virtual machine provides its own virtual hardware including CPUs memory, hard drives, network interfaces and other devices
- Azure Virtual Machine offers the flexibility of virtualization without buying and maintaining the physical hardware that runs it

It is a **general-purpose computing environment** that lets you create, deploy, and manage VMs running in the Microsoft Azure cloud.

Azure VM's can be used in following ways:

- **Development and test** - Azure VMs provide a fast and effortless way to create a computer with particular configurations needed to code and test an application.
- **Extended datacenter** - VMs in an Azure virtual network can easily be connected to organization's network.
- **Applications in the cloud** - since the demand for an application can fluctuate, it might create economic sense to operate it on a VM in Azure. Thus one has to pay for additional VMs only when required and shut them down when they don't.

Different Ways to Create VM

- **Azure CLI** - used to create and manage Azure resources from the command line or by using scripts.
- **Azure Portal** - provides a browser-based user interface for creating and configuring virtual machines and all related resources.
- **Azure PowerShell** - used to create and manage Azure resources from the PowerShell command line or scripts.
- **Resource Manager template** - a JSON file is used to define one or more resources to be deployed to a resource group and define the dependencies between the deployed resources. **This template can be used to deploy the resources consistently and repeatedly.**

VM Size

The VM size is determined by the workload that you want to run. The size then determines factors such as processing power, memory, and storage capacity.

Following VM sizes are available:

- **A-series**: is basic with no load balancing or auto-scaling support.
- **D-series:** offers faster CPUs and local Hyper-V host SSD (temporary disk).
- **Dv2 series:** provides largest VMs with configuration up to 448 GB of RAM and 64 data disks. CPU is 35% faster than D-series.
- **DS, DSv2, and GS series:** Support for Premium Storage (SSD for operating system and data disks).

Benefits

1. Easy development and test
2. Agility and scale
3. Enhanced performances

4. Pay as you go pricing
5. Extended Datacenter
6. Disaster Recovery

Components

Virtual Machine in Azure comes under compute services and it can be used with other services like Disks, Images, Availability Sets, Hosts and many more.

First Components is Operating Systems.

- It is one of the main components of Azure. Here, the OS creates connections to Remote Desktop Session Host.
- Few OS available for Azure Virtual Machine are - Ubuntu, RedHat, Linux, Windows Server Datacenter and CentOS
- You can also set the OS disk size in the Virtual Machine so that the memory is not wasted

Second Components is Disks.

- Azure Virtual Machines use attached virtual hard disks (VHD) for storage. There are two types of VHDs:
    - Image: It is a template for the creation of a new Azure VM
    - Disks: It is a bootable VHD that can be used as a mountable disk for a VM
- Page blobs back all the disks in Azure Storage and they inherit the benefits of blob storage
- The disks are mounted as drives on the VM

Third Components is Virtual Network.

- On a physical infrastructure, many components operate the virtual machines in a scalable and secure manner
- The components could include equipment such as separate network, load balancers, firewalls, and more
- These components are deployed in an Azure Virtual Network
- Azure Virtual Network provides many features like- Subnet, IP address, Load balancer and, Network security group

Fourth Components is Availability Sets.

- Sometimes, there is a slight chance that there could be a failure in physical servers
- If in case a failure occurs, the Azure platform will migrate the failed VM to a healthy host server to reconstitute the VM
- Hence, it is recommended to deploy at least two instances of the VM
- VMs placed in an availability set should perform an identical set of functionalities

VM Creation Demo

VM Availability

To ***ensure high availability*** of an application, Azure places VMs into a logical grouping called an ***Availability Set.***

When deployed with a service, Azure ensures that the VMs in the Availability set are arranged across Fault Domains on different Racks. In case of a maintenance event or failure of one fault domain, at least one VM keeps running.

Along with Load balancers, availability sets can provide up to 99.95% SLA for VMs.

Fault Domain

A fault domain is a set of hardware components (rack of resources like servers, power, etc.) that share a single point of failure. Web, worker and Virtual Machines are arranged in this hardware.

Azure deploys an application or service across multiple fault domains.

Update Domain

Update domain in Azure means, that all physical servers in one update domain will get host updates like firmware, drivers and OS updates at the same time.

In the Illustration UD#1 is getting updated but the user can access the content from UD#2.

It provides Web or Worker role (within rack) instances with high availability by ensuring that only one of the Instances is down for an update at one time.

VM Scaling

Scalability is known as the ability of a process, network, or system to accommodate fluctuating workload/demand.

- **Vertical scaling**, also known as scale up and scale down, **involves increasing or decreasing virtual machine (VM) sizes** in response to the workload, without creating additional VMs.
- **Horizontal scaling** also known as scaling out and in, **involves adding or removing instances of a resource**. The application continues operating without interruption as new resources are provisioned.
    - Once provisioning process is complete, the solution is deployed on the additional resources.
    - If demand drops, additional resources can be shut down cleanly and deallocated.

Azure Storage Services

Microsoft Azure Storage is a highly scalable and robust storage solution for your applications. Watch this video to get a high-level picture about the Storage Services.

- Is elastic and can scale applications on demand
- Uses auto-partitioning system that automatically load balances based on the traffic
- Accessible from any application, running on the cloud/desktop /on-premises server/mobile device
- Exposes data resources through REST APIs

Azure Storage offers four storage types.

- ***Blob Storage*** - for unstructured object data like images, videos, documents, etc.
- ***Table Storage*** - a NoSQL key attribute data store for structured datasets.
- ***Queue Storage*** - for storing a large number of messages. `(Example: Creating backlog requests to be processed asynchronously OR for passing messages between various components.)`
- ***File Storage*** - shared storage for sharing files across application components via File service REST API.

Azure Storage Account

Azure Storage account is a secure account that provides access to Azure Storage Services. There are two types of Storage Accounts.

- ***General Purpose Storage Accounts*** that give access to blobs, tables, queues, files and Azure virtual machine disks.
- ***Blob Storage Accounts***, are specialized storage accounts for unstructured data as blobs. This type of account is recommended for applications that require just the ***block or append blob storage.***

Storage Replication

Azure Storage Account offers multiple options to replicate data in a single data center / across facilities / across geographies to:

- Ensure durability
- Higher availability
- Protect data (against hardware failures or unforeseen catastrophes).

Options available:

- Locally redundant storage
- Geo-redundant storage
- Zone-redundant storage
- Read-access geo-redundant storage

StorSimple

StorSimple is a **Hybrid Cloud Storage Solution** to manage storage tasks between on-premise devices and cloud storage.

It has **physical arrays** for deployments in data centers and **virtual arrays** for smaller enterprise environments, which require network-attached storage (NAS).

Local storage gives the flexibility to retain part/entire data locally and could be useful for getting higher performance.

StorSimple is ideal for applications requiring high performance and capacity.

Azure Backup

Azure Backup is a multi-tenant Azure service to back up and store data.

- Backup all your critical applications and data using the Azure Backup Agent.
- Azure ***Backup data is encrypted*** at the source, in transit, and at rest in the Azure.
- ***Configure the retention policy*** of backups as required (for example, 30 days, 99 years).

- ***Azure Site Recovery*** delivers a seamless portal experience for taking backups and operational recovery.

Azure Database Services

Azure provides many Database services to cater to the wide range of needs of enterprises. Few them are:

- **Relational Database Services** - Azure provides SQL, MySQL, and PostgreSQL services as PaaS, making it easier to move existing workloads to Azure.
- **SQL Data Warehouse** - SQL based fully managed elastic data warehouse that can scale up and down as per demand.
- **Azure Redis Cache** - SAAS offering of Redis Cache that provides secure, dedicated cache for applications requiring low latency.

Data Lake Store

Azure Data Lake Store is known as a **Highly Scalable Apache Hadoop file system** that can be used for enterprise-wide big data analytics workloads.

Key Features:

- **Unlimited storage** and variety of data formats.
- Can **store data in native format** without the need for any transformation.
- Built for workloads requiring **massive read throughput** and analysis of large amounts of data.
- **Can be accessed from Hadoop** using the WebHDFS-compatible REST APIs.

Azure Cosmos DB

Microsoft has developed Azure Cosmos DB to ***support global distribution and horizontal scale***. It extends the idea of a ***index-free database system***.

Offers ***turnkey distribution*** by enabling seamless scaling based on user demand in any region or geography.

Support various new data types, making it flexible to ***work as a graph database or key-value database.***

Experience Low latency, owing to read and write from the nearest region.

Azure App Services

What are App Services?

App Service is a ***Platform as a Service (PaaS)*** that offers development framework to build and deploy mobile, web, logic, and API apps.

Create web and mobile apps for any platform or device. Azure runs these apps on ***fully managed virtual machines (VMs)*** , with user's choice of shared VM resources or dedicated VMs.

Also, App Services allows connecting these apps to any SaaS or enterprise system within minutes and unlock the data.

Key features and Capabilities of App Service

- Multiple languages and frameworks - supports ASP.NET, Node.js, Java, PHP, Python, etc.

- DevOps optimization - can set up continuous integration and deployment with Visual Studio Team Services, GitHub, or BitBucket.
- Global scale with high availability - can Scale up or down manually or automatically.
- Security and compliance - is ISO, SOC, and PCI compliant.
- Application templates - can choose from an extensive list of templates in the Azure Marketplace.
- Visual Studio integration - to streamline the work of creating, deploying, and debugging.

Web App Services

Web App Services help in hosting your websites and web applications. Main features include:

- Support for .NET, Java, PHP, Node.js, and Python.
- High availability with auto-patching.
- Continuous deployment with Git, TFS, GitHub.
- Azure Marketplace based solutions that simplify the development and deployment.
- Multiple Deployment slots to run two or more versions of the same app (production and dev) concurrently on the same virtual machine.
- Azure WebJobs to execute background processes.
- Hybrid connections from web apps to access on-premises resources or VMs within an Azure virtual network.

Mobile App Services

Mobile Apps is a highly scalable, globally available mobile application development platform for Enterprise Developers and System Integrators. With Mobile Apps you can:

- Build native and cross platform apps using native SDKs.
- Connect mobile apps to your enterprise on-premises or cloud resources.
- Build offline-ready apps with data sync - make your mobile workforce productive by building apps that work offline.
- Push Notifications to millions in seconds and engage your customers.

Logic App Services

Use **Logic Apps** for automating business processes and integrating systems and data across clouds without writing code. Main features of Logic Apps:

- Visually create business processes and workflows
- Deliver integration capabilities in Web, Mobile, and API Apps
- Integrate with your SaaS and enterprise applications
- Automate business processes
- Connect to on-premises data

API App Services

Azure API App Service offer a rich platform and ecosystem for ***building, consuming, and distributing APIs*** in the cloud and on-premises. Main features of this service are:

- Integrate with SaaS and enterprise applications
- Generate client proxies or APIs in language
- Automate versioning and deployment of API Apps
- Secure APIs with Single Sign-On, OAuth, and Active Directory
- Share APIs internally with organizational gallery

Azure Analytics and IOT

Azure HD Insight

Azure HD Insight is widely used to deliver ***Hadoop as a service*** ***on top of the Azure platform***. It uses the ***Hortonworks Data Platform (***HDP) Hadoop distribution.

Azure HD Insight gives open-source analytic clusters for Spark, Hive, Storm, Kafka, MapReduce, HBase, and R Server to deploy these big data technologies.

Organizations can use HD Insight to:

- Create Hadoop-powered big data solution and services
- Manage and monitor Hadoop clusters
- Analyze and report statistics on big data utilization and availability

Azure Machine Learning

Azure Machine Learning is known as a **cloud predictive analytics service** that allows quick ****creation and deployment of predictive models***.

It comes with ***ready-to-use library of algorithms***, to create models and deploy your predictive solution quickly.

Azure Machine Learning offers ***tools to model predictive analytics*** and offers a ***fully managed service*** for using predictive models as ready-to-consume web services.

Azure Stream Analytics

Azure Stream Analytics strives to **gather knowledge structures from the continuous ordered streams of data** with real-time analysis.

The streams may comprise web searches, ATM transactions, sensor readings, phone conversations, social network data, or computer network traffic.

It offers a ready-made solution for business requirement that involve handling large volumes of information and react very quickly to changes in data.

Azure Stream Analytics Usage

- **Connected devices** - Monitor and diagnose real-time data from connected devices to generate alerts, respond to events, or optimize operations.
- **Business operations** - Analyze real-time data to respond to dynamic environments to take immediate action.
- **Fraud detection** - Monitor financial transactions in real-time to detect fraudulent activity.
- **Website analytics -** Collect real-time metrics to gain instant insight into a website's usage patterns or application performance.

Event Hubs

AzureEvent Hubs is a event ingestion service and scalable data streaming platform that receives and processes numerous events per second.

Event Hubs processes and stores events, data, or telemetry created by distributed devices and software. Data transmitted to an event hub can be transformed and stored with the help of any real-time analytics provider or storage/batching adapters.

Offering publish-subscribe capability with low latency and huge scale, Event Hubs acts as the "on ramp" for Big Data!

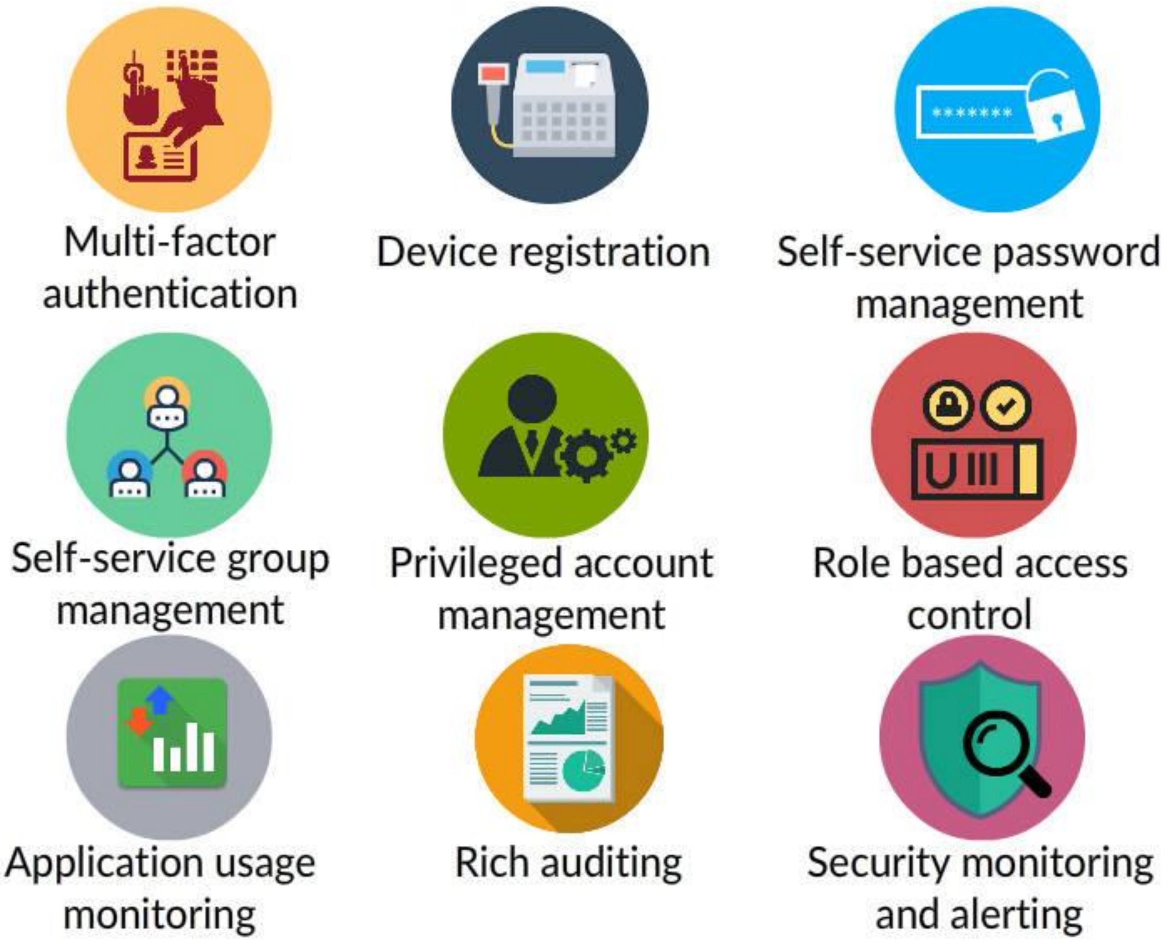
Other Azure Services

Azure Active Directory

Azure AD is known as an identity management solution that **offers access and identity services** for cloud resources. It is available as both on cloud and on-premises service. It helps to:

- Configure access to applications.
- Configure SSO to cloud-based SaaS applications.
- Manage users and groups.
- Provision users.
- Enable federation between organizations.
- Provide an identity management solution.
- Identify irregular sign-in activity.
- Multi-factor authentication.
- Extend existing on-premises AD implementations to Azure AD.

Features of Azure AD


Multi-factor authentication
Device registration
Self-service password management
Self-service group management
Privileged account management
Role based access control
Application usage monitoring
Rich auditing
Security monitoring and alerting
****
U III

Azure AD includes a `full suite of IDM capabilities` such as,

Access & Authentication

- Multi-factor authentication
- Device registration
- Role based access control

Management

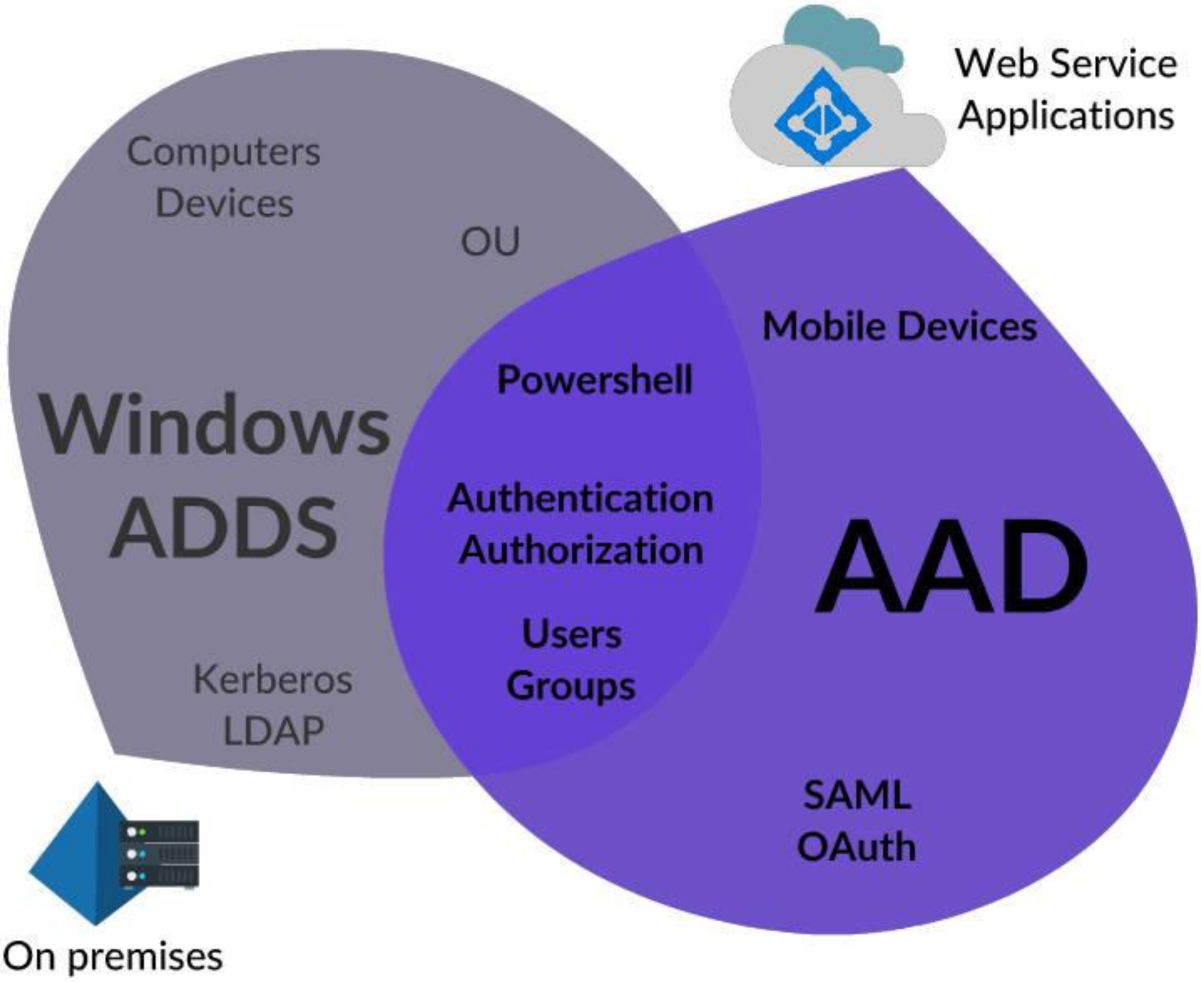
- Self-service password management
- Self-service group management
- Privileged account management

Monitoring & Auditing

- Application usage monitoring
- Rich auditing
- Security monitoring and alerting

These capabilities can help secure cloud-based applications, streamline IT processes, cut costs and also help assure corporate compliance goals are pan.

Azure AD vs ADDS



Azure AD and Windows Server Active Directory (AD) are used for Authentication. But Azure AD differs in many aspects, such as;

- It doesn't have,
    1. Active Directory forest and Trust relations
    2. Organizational Units
    3. Group Policies
- It uses Open AD connect, O-Auth, WS-federation and SAML protocols for Authentication and Authorization.

Azure AD Editions

Azure AD is available in free and paid editions such as,

- Free
- Basic
- Premium 1
- Premium 2

To know **Azure AD Pricing and Edition Comparison** visit Azure AD features & Pricing

Azure Security Center

Azure Security Center aids to ***prevent, detect, and respond to threats*** with increased visibility into and control over the security of Azure resources.

- Offers ***integrated security monitoring*** ***and*** ***policy management*** across Azure subscriptions.
- Aids in ***detecting threats*** that might otherwise go unnoticed.
- ***Works with a broad ecosystem*** of security solution.

Azure Key Vault

Azure Key Vault helps **safeguard cryptographic keys and secrets** **used by cloud applications and services**. It streamlines the key management process and enables to maintain control of keys.

By using Key Vault, you can **encrypt keys and secrets** (such as authentication keys, storage account keys, data encryption keys, etc.) by using keys that are protected by **Hardware Security Modules (HSMs).**

Developers can create keys for testing and development in minutes, and then easily migrate them to production keys.

Azure Essentials - Course Summary

Congratulations! You have come to the end of this course. By now, you must have got a good idea about various services offered by Azure for:

- Networking
- Computing
- Storage
- Database
- Analytics and IOT
- Few other important services

Azure Identity Management

Azure IDM Introduction

Welcome to the course Azure Identity Management. This course will introduce following concepts along with relevant Hands-On exercises.

- Azure Active Directory (AAD)
- Managing users and groups in (AAD)
- Azure Active Directory connect (AAD connect)
- Synchronizing an On-premise Active Directory with AAD in a hybrid scenario
- Azure AD Premium features
- Implementing Multi-Factor Authentication (MFA)
- Integrating Applications with AAD

Please note that this course has been curated using the materials/resources received through our partnership with Microsoft. Hence, you could see that the content for this course has been taken from Microsoft official sites.