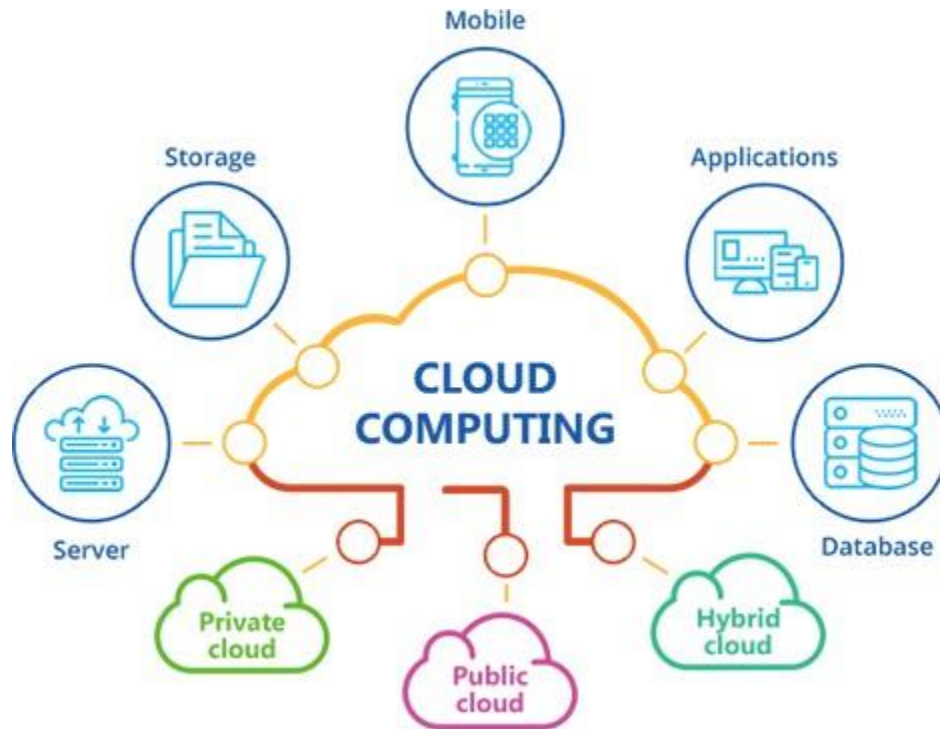B.Sai Krishna/Rakesh Sharma(Azure Team)

what is cloudcomputing

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the use


Azure Cloud Computing

Microsoft Azure, formerly known as Windows Azure, is Microsoft's public cloud computing platform. It provides a range of cloud services, including those for compute, analytics, storage and networking.

At its core, Azure is a public cloud computing platform—it is Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) that can be used for services such as analytics, virtual computing, storage, networking, and much more. It can be used to **replace** or supplement your on-premise servers.

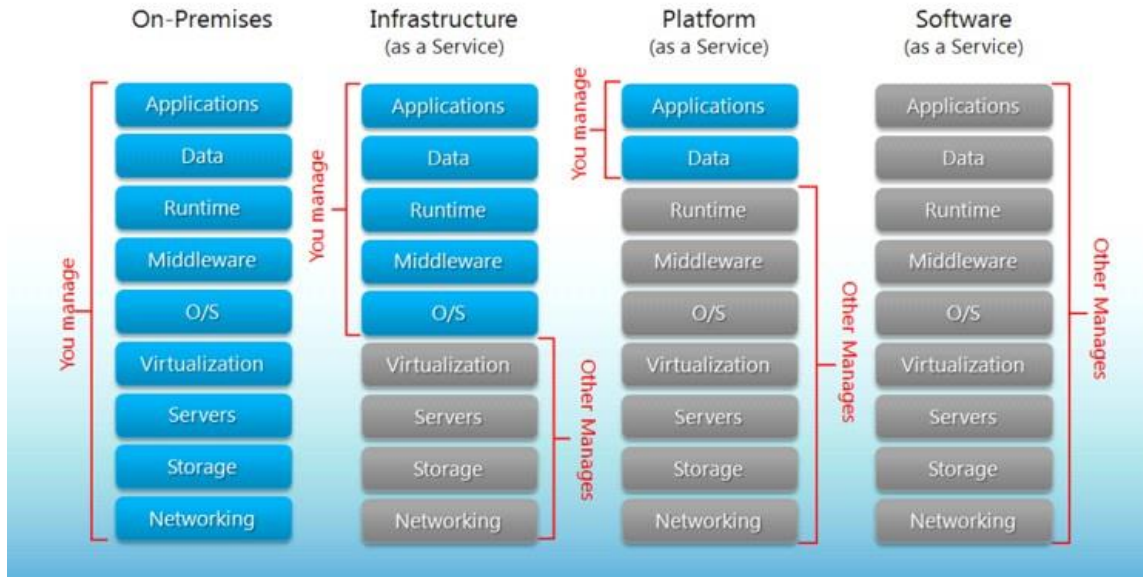To meet the business requirements and also some third party tools using Azure Cloud.
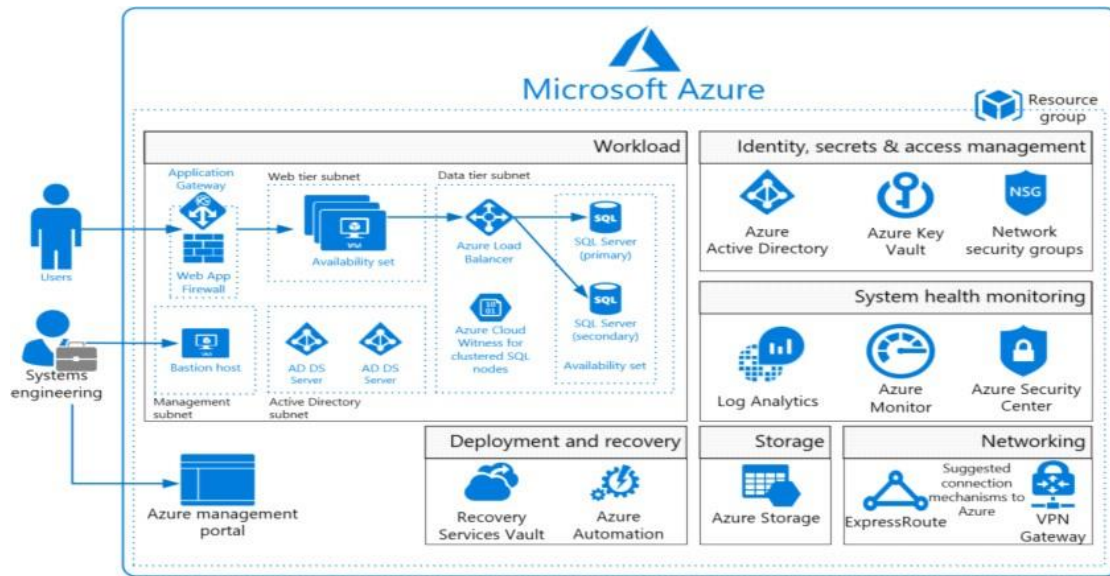
Azure Architecture
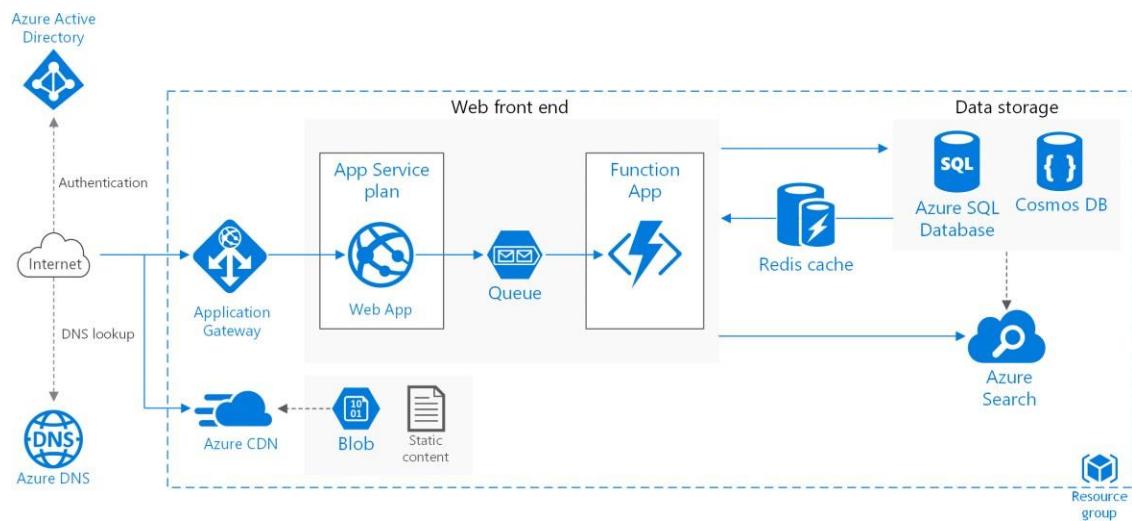
Azure Cloud Services

i.IAAS [Infrastructure As A Service]

ii.PAAS [Platform As A Service]

iii.SAAS [Software As A Service]

Separation of Responsibilities

(The Above image can easily explain why we need cloud)

Azure Cloud Deployment

i. Public Cloud: The infrastructure is owned by your cloud provider and the server that you are using could be a multi-tenant system.

ii. Private Cloud: The infrastructure is owned by you or your cloud provider gives you that service exclusively. For eg: Hosting your website on your servers, or hosting your website with the cloud provider on a dedicated server.

iii. Hybrid Cloud: When you use both Public Cloud, Private Cloud together, it is called Hybrid Cloud. For Example: Using your in-house servers for confidential data, and the public cloud for hosting your company's public facing website. This type of setup would be a hybrid cloud.

Cloud Deployment Models
(c) 2018 David Maiolo
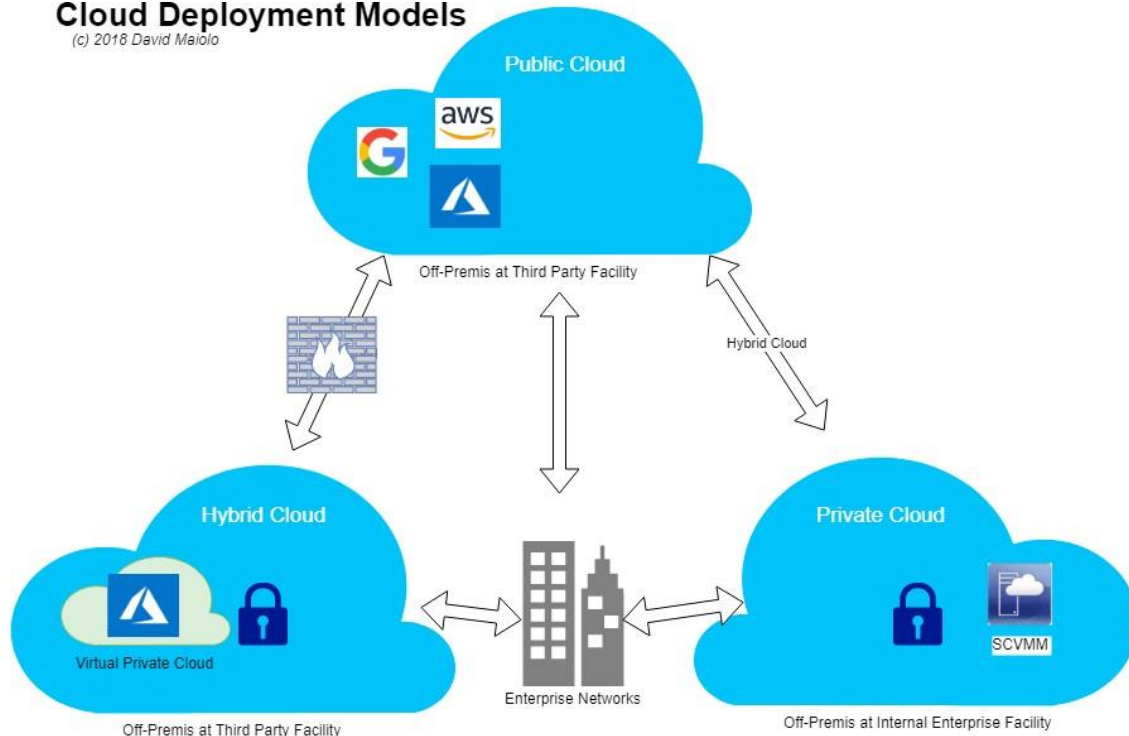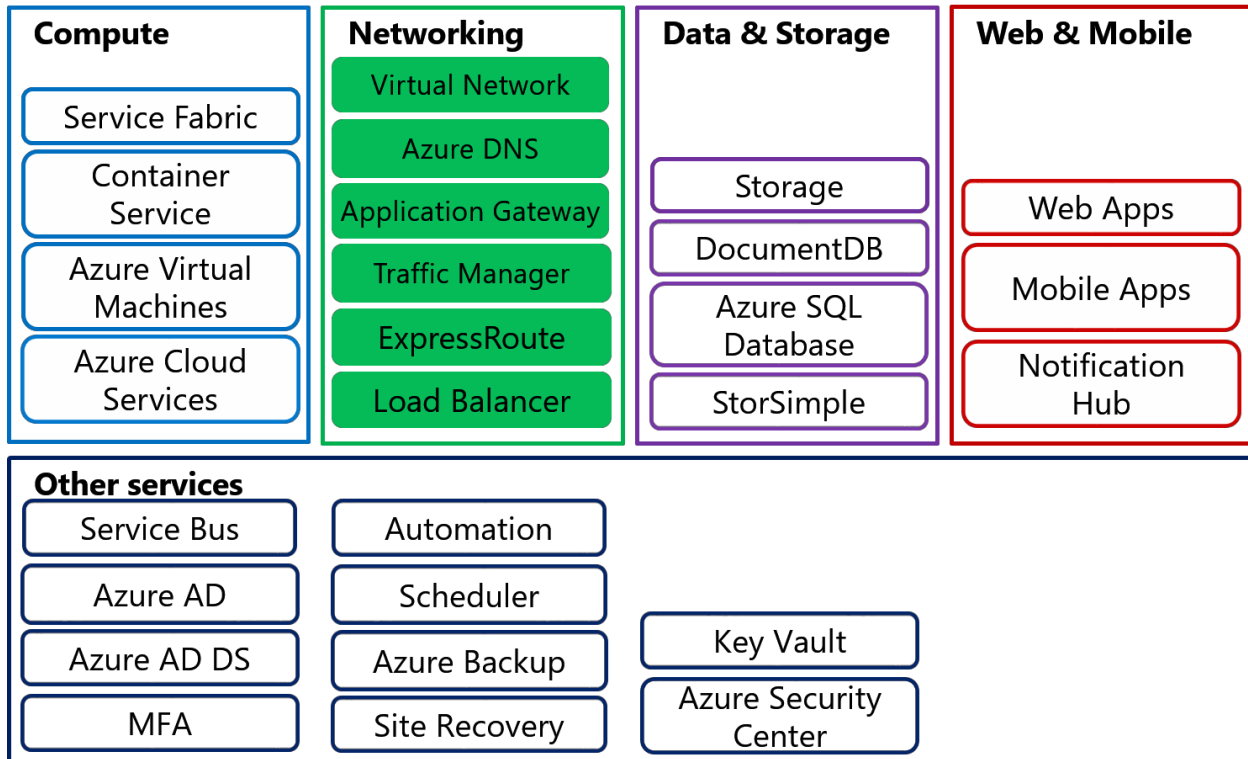
Components of Windows Azure OS

Azure OS is that part of Azure platform which runs applications and stores data. Windows Azure OS contains five services.

a. Compute

b. Storage

c. Virtual Network

d. CDN

e. Fabric Controller

Compute Service runs applications. Simply speaking, Compute is your applications hosting environment. Compute service offers three execution models and they are:

Compute	Networking	Data & Storage	Web & Mobile
Service Fabric	Virtual Network		
Container Service	Azure DNS	Storage	Web Apps
Azure Virtual Machines	Application Gateway	DocumentDB	Mobile Apps
	Traffic Manager	Azure SQL Database	
Azure Cloud Services	ExpressRoute		Notification Hub
	Load Balancer	StorSimple	

Other services

Service Bus	Automation	
Azure AD	Scheduler	
Azure AD DS	Azure Backup	Key Vault
MFA	Site Recovery	Azure Security Center

Virtual Machines

Virtual Machines execution model is used when a user wants to use only the Cloud infrastructure.

Web Sites

Websites execution model is used when a user wants to move an existing application or run a web application in a managed environment.

Cloud Services

Cloud Services execution model is used when a user wants to develop and run a multi-tier application or highly-scalable applications.

SQL Database

SQL Database is the relational storage service Azure offers to store relational data in the cloud. It is like a SQL server database on cloud. Note that SQL Database is available as a service. SQL Database contains all common features of the SQL server such as tables, primary keys, stored procedures and functions, user-defined functions. Not only that, it also manages transactions and concurrency. The important point here is applications can access SQL Database using different data access technologies like EF and ADO.NET and WCF Data Services. (just like sql server)

Virtual networks

Azure Virtual Network is a fundamental component that acts as an organization's network in Azure. Organizations can use virtual networks to connect resources. Virtual networks in Microsoft Azure are network overlays that you can use to configure and control connectivity between Azure resources such as VMs and load balancers.

IP addresses

VMs, Azure load balancers, and application gateways in a single virtual network require unique IP addresses in the same way as clients in an on-premises subnet do. This enables these resources to communicate with each other. There are two types of IP addresses that are used in a virtual network:

Private IP addresses. A private IP address is allocated to a VM dynamically or statically from the defined scope of IP addresses in the virtual network. This address is used by VMs in the virtual network to communicate with other VMs in the same virtual network connected VNets/networks through a gateway/ExpressRoute connection.

Public IP addresses. Public IP addresses allow Azure resources to communicate with external clients, and are assigned directly at the virtual network interface card of the VM or to the load balancer.

Subnets

You can further divide your network by using subnets for logical and security isolation of Azure resources. Each subnet contains a range of IP addresses that fall within the virtual network address space.

Network interface card

VMs communicate with other VMs and other resources on the network by using virtual network interface cards (NICs). Virtual NICs configure VMs with private and optional public IP address. VMs can have more than one NIC for different network configurations.

DNS

The Domain Name System (DNS) enables clients to resolve user-friendly fully qualified domain names (FQDNs), such as to IP addresses. Azure provides a DNS system to support many name resolution scenarios. However, in some cases, such as hybrid connection you might need to configure an external DNS system to provide name resolution for virtual machines on a virtual network.

Azure load balancer and internal load balancer

To increase availability and scalability, you can create two or more VMs that publish the same application. For example, if three VMs host the same website, you might want to distribute incoming traffic between them and ensure that if one VM fails, traffic is distributed automatically to the other two. You can use an Azure load balancer to enable this traffic distribution between VMs. In this configuration, a single endpoint is shared between multiple VMs. The Azure load balancer automatically distributes requests across those VMs as the requests arrive at the endpoint. You can use two types of Azure load balancers:

Internal load balancer. The internal load balancer enables you to load balance traffic between VMs in the same cloud service (for classic model), or between VMs and a virtual network with a regional scope, where the input IP address of the load balancer is a private IP address.

Internet-facing load balancer. The internet-facing load balancer enables you to load balance incoming Internet traffic to VMs.

Application gateway

Application gateways provide load-balanced solutions for network traffic that is based on the HTTP protocol. They use routing rules as application-level policies that can offload Secure Sockets Layer (SSL) processing from load-balanced VMs. In addition, you can use application gateways for a cookie-based session affinity scenario.

Traffic Manager

Microsoft Azure Traffic Manager is another load-balancing solution that is included within Azure. You can use Traffic Manager to load balance between endpoints that are located in different Azure regions, at hosted providers, or in on-premises datacenters. These endpoints can include Azure VMs and Azure websites. You can configure this load-balancing service to support priority or to ensure that users connect to an endpoint that is close to their physical location for faster response.

Network security groups

You can use network security groups to provide network isolation for Azure resources by defining rules that can allow or deny specific traffic to individual VMs or subnets. This enables you to design your Azure virtual network to provide a network experience that is similar to an on-premises network. You can achieve the same functionality in your Azure virtual network as you would in the on-premises networks, such as perimeter networks (also known as DMZ or demilitarized zone).

User Defined Routes

User Defined Routes (UDR) control network traffic by defining routes that specify the next hop of the traffic flow. You can assign User Defined Routes to virtual network subnets.

Forced tunneling

With forced tunneling you can redirect internet bound traffic back to the company's on-premises infrastructure. Forced tunneling is commonly used in scenario where organizations want to implement packet inspection or corporate audit.

Regional virtual networks

Azure Virtual Network is bound to Azure subscriptions and it is not possible for multiple subscriptions to use the same Azure virtual network. If you need to provide communications between different Azure subscriptions, you need to create separate Azure virtual networks in each subscription and then use site-to-site virtual network connections or the Microsoft Azure service ExpressRoute, to connect them. All new virtual networks are regional virtual networks. This means that they can span a complete Azure region or datacenter. This differs from the legacy implementation of virtual networks in Azure, which were restricted to a single affinity group, allowing you to co-locate virtual networks, storage accounts, and services in the physical proximity to each other within the same area of a single datacenter. If you have older virtual networks in your subscription, these could be tied to an affinity group. However, over time, you need to migrate all virtual networks to regional virtual networks and remove their ties to specific affinity groups.

Cross-premises network connectivity

Virtual networks in Microsoft Azure also enable you to extend your on-premises networks to the cloud. To extend your on-premises network, you can create a virtual private network (VPN) between your on-premises computers or networks and an Azure virtual network. Alternatively, you can use ExpressRoute to provide a connection to an Azure virtual network that does not cross the Internet. Using these two methods, you can enable on-premises users to access Azure services as if they were physically located on-premises in your own datacenter.

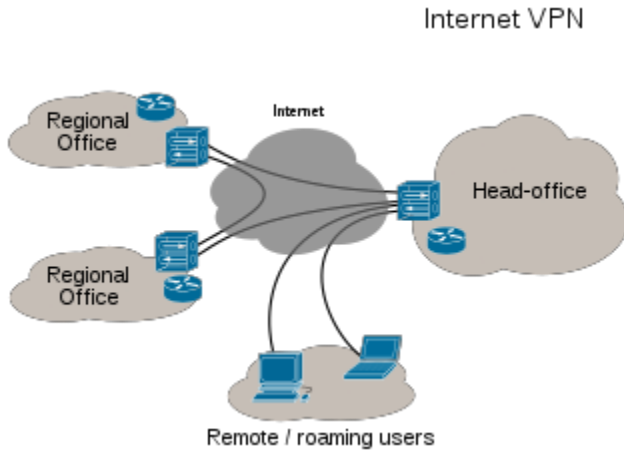To connect to an Azure virtual network from an on-premises network, you can use:
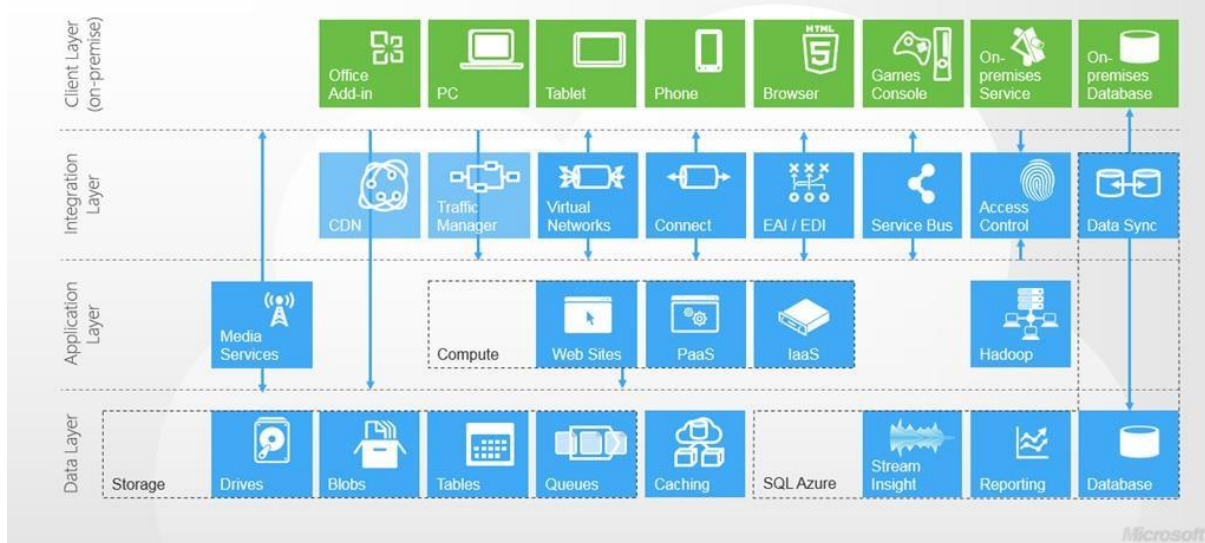
A point-to-site VPN

A site-to-site VPN

ExpressRoute

VNet-to-VNet VPN

Internet VPN

For Reference:

Azure Pricing:

There are two ways to purchase Azure Stack:

1. Purchase Azure Stack services via your own EA

2. Purchase Azure Stack services from a service provider

Links:

https://acloud.guru/learn/intro-to-azure

https://azure.microsoft.com/en-in/overview/what-is-azure/

https://www.geeksforgeeks.org/introduction-microsoft-azure-cloud-computing-service/

https://www.simplilearn.com/cloud-computing/microsoft-azure-fundamentals-training

https://www.edureka.co/microsoft-azure-training

Videos:

https://acloud.guru/learn/intro-to-azure

https://www.udemy.com/azure-introduction-i/

https://www.youtube.com/watch?v=0bPJPiX89K0