

Management groups,

1. All conditions declared in the management groups will be inherited to subscriptions.
2. 10000 management groups can be supported in a single directory
3. Each management group can support 6 levels of tree depth
4. This limit doesn’t include management group level
5. Each management group and subscription can only have one parent.
6. Each management group can have many children.

Subscriptions:

1. User groups and resources created by those user accounts. For each subscription there are limits and quotas on the amount of resources you can create and use. Using subscriptions companies can manage costs and teams, projects, etc..

Resource groups:

1. Logical container where it holds software, databases, web apps, and storage accounts.

Resources:

1. Instances that you create, like virtual machines, storage or SQL databases.

Bandwidth refers data moving in and moving out, some inound transfers i.e. data coming into azure data centers are free, for outbound transfers such as data going out are charged based on zones.

1. **Azure cost management:** provides set of tools for monitoring, allocating, optimizing azure costs. You can also perform historical breakdown to check on what you spend the most on.
2. **Pricing calculator:** let’s you know prices of services,
3. **Total cost of ownership(TCO):** cost savings you can realize by migrating to azure.

Cloud computing: delivery of computing services, servers, storage, databases, networking, software, ananlytics, over the internet, enabling faster services.

VM are nothing but just like your physical systems, there are other two options i.e. **containers**, **serverless computing**.

**Containers**: containers are just like VM, but they don’t need operating system. Instead, the application and all its dependencies is packaged into a container and the standard runtime environment is used to execute the app. This allows container to start the app in few seconds, as there is no OS to boot and initialize.

**Docker** is one of the leading platforms to manage containers. Dockers are lightweight approach to application deployment because they allow different components of the application to be deployed independently into different containers.

Multiple containers can be run on single machine, and they can be run on on-primes or different cloud, without any changes and they can be exchanged between systems,

**Serverless computing**:

Lets you run code with out creating, configuring, or maintaining a server. The core idea is that your **application is broken into separate functions** **they run when triggered by some action**.

Serverless model is different from VMs and containers in which you only pay for the processing time used by each function. VMs and containers are charged while they are running – even if the application are idle. But when app is divided into certain tasks, you can test them separately, execute them separately. Launch them separately, this will be fastest when you deploy your applications.

**Cloud Concepts**:

1. **High** **availability**
2. **Scalability** – scaling up(adding additional capabilities to manage increase in demand ) and scaling out (we can add additional resource)
3. **Elasticity** – ability to automatically increase or decrease resources. Difference between elasticity and scalability is elasticity is done automatically.
4. **Agility** – ability to react quickly, cloud services can allocate and deallocate resources quickly. They are provided on demand via self-service. Huge amounts of computing services can be provided quickly in minets.
5. **Fault tolerance**: When some function is not working ability to take backup of this event.
6. **Disaster recovery**: the ability to recover from an event which has taken down a cloud service.
7. Global reach
8. Customer latency capabilities

**Business analytics tool**: tools to extract data and integrate into a repository may be to data warehousing, where it can analyze.

**Business intelligence tools**: tools that process large amount of unstructured data and helps you to retrieve meaningful insights.

**Cloud bursting**: config that setup between private cloud and public cloud. If 100% of resources occupied in private cloud overflow topic can be diverted to public cloud.

Cloud computing types:

1. SaaS – for web-based applications
2. IaaS – for internet-based access to storage and computing
3. PaaS – developers to build and host web applications.

**Database sharding**: a type of partitioning that let you divide large database into smaller databases,

**DevOps**: union of people, process and technology to enable continuous value of delivery to customers.

**Elastic computing**: ability to dynamically provision and de-provision computer processing, memory and storage resources to meet changing demands without worrying planning.

**Hybrid Cloud:** combination of public and private cloud, bound together by technology that allows data and applications to be shared between them.

**Middleware**: software that lies between **operating system** and **application running** on it. Enables **communication and data management** for distributed applications in cloud-based applications. So, for example data in one database can be accessed in another database. Examples are **web servers**, **application servers**, and **content management systems**.

**Economies of scale**: concept here is ability to reduce costs when operating at large scale compared to operating in small scale. Big companies such as Amazon, Google, Microsoft leverage benefits of economies of scale, and then pass those benefits to their customers.

Economies of scale: ability to buy at cheaper prices when you but at larger volume, when compared to buying a single user.

**Compare CapEx vs OpEx**

**CapEx (Capital Expenditure):** this is the upfront spending money in order to procure physical infrastructure and deducting that upfront money over time. This CapEx value reduces over time.

Includes below costs:

1. Server costs: buying physical server, making sure on fault tolerance, power supply, huge cost.
2. Storage costs:
3. Network costs:
4. Backup and archive costs:
5. disaster recovery costs
6. infrastructure cost
7. technical people costs

**OpEx (Operational Expenditure)**: this money you spend on services or products now.

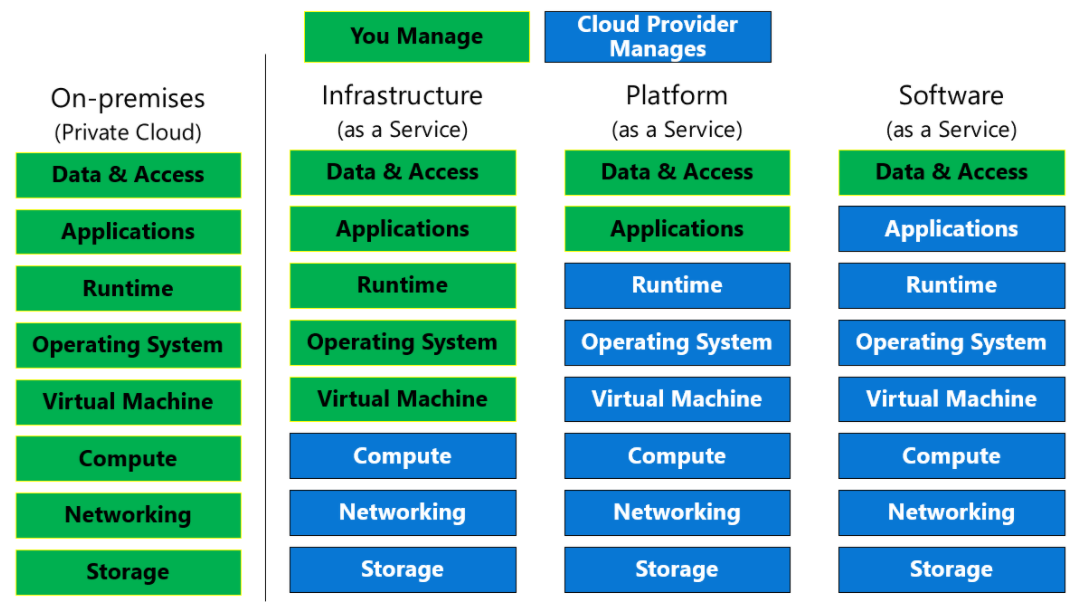
**Cloud deployment**:

Cloud deployment defines where your data is stored and how your customers interact with it.

1. public cloud:
   1. owned by the cloud services provider.
   2. **Ownership:** resources that an end user uses.
   3. **Multiple end users:** public clouds are available to multiple users.
   4. **Public access:** allows public to access desired clouds.
   5. **Availability:** most common cloud type deployment model.
   6. **Connectivity:** people use internet to connect to these clouds.
   7. **Skills:** not much technical skills are required to use resources.
2. private cloud:
   1. owned by user or organization.
   2. **Ownership**: owner and users could be possibly same.
   3. **Hardware**: owner is responsible for purchase, maintenance and management of cloud hardware.
   4. **Users**: operates only within one organization.
   5. **Connectivity**: users can use cloud using secure requests
   6. **Public access**: public access is not provided
   7. **Skills**: required technical knowledge to access private clouds.
      1. You can create your own cloud datacenter and provide self-service access to computer resources in your organization.
      2. Organizations have complete control over resources and on secutiry.
      3. Hardware must be purchased for start-up and maintenance.
      4. Private clouds are not agile as public clouds.
3. Hybrid cloud
   1. Combines both public and private clouds.
   2. You can host website in public cloud, and host a highly secure database in private cloud.

Shared responsibility model:

Shared responsibility model ensures cloud workloads run securely and in a well-managed way. Depending on the service we are using, cloud provider is responsible for few aspects, and the end user is responsible for other few aspects of workload management, and in some cases both shares responsibility.



**Infrastructure as a service (IaaS)**:

It is the most basic category of cloud computing services. With IaaS, you rent IT servers, VMs, storage, networks, operating systems, from a cloud provider pay-as-you-go-basis.

**Characteristics**:

Upfront costs: no upfront costs, users pay only what they consume.

Ownership: user is responsible for purchase, installation, configuration, management of their own software.

Cloud provider Ownership: provider is responsible for ensuring underlying cloud infrastructure.

**Migrating workloads**: IaaS are managed in similar way as on-premises infrastructure, and provide easy migration for existing applications.

**Tests and development**: Teams can quickly setup dev and test environments, they can dismantle once they are done. Environment setup is easy and fast.

**Website hosting**: running websites using IaaS is less expensive.

When using IaaS, ensuring that service is up and running is a shared responsibility. Cloud provider is responsible for ensuring cloud infrastructure is functioning correctly. Cloud customer is responsible for ensuring the service they are using configured correctly.

**Platform-as-a-serive (PaaS)**:

PaaS provides an environment for building, testing, and deploying software applications. Goal of PaaS is to create an application as quickly without having worry about underlying infrastructure.

PaaS characterizes:

1. Upfront costs: no upfront costs, pay as you use.
2. User ownership: user is responsible for development of their own applications, so user need not worry about managing server or infrastructure. This allows user to focus on application.
3. Cloud provider ownership: cloud provider is responsible for everything other than your application.

Software-as-a-service (SaaS):

SaaS is software that centrally hosted and managed for end customer. It allows users to connect to and use cloud-based apps over the internet. Examples are email, calendars.

**SaaS characteristics**:

**Upfront costs**: Users have no upfront costs, they pay subscriptions typically on monthly or annual basis.

**User ownership**: users just use application software; they are not responsible for any maintenance or management of that software.

**Cloud provider ownership**: cloud provider is responsible for provision, management, and maintenance of application software.

**Comparing Cloud services**:

**IaaS**: most flexible category of cloud services. Aims to give you complete control over the hardware that runs your application.

|  |  |  |  |
| --- | --- | --- | --- |
|  | IaaS | PaaS | SaaS |
| NoCapEx | No upfront costs | No upfront costs | No upfront costs |
| Agility | Can be made accessible quickly, and deprovisioned whenever needed | More agile than IaaS, users don’t need to configure servers running applications | Staff can provide access to latest software quickly and easiy. |
| Consumption-based model | Organizations pay only for what they use and operate under OpEx model. | Pay what you use, operate under OpEx model | Subscription model, typically monthly, yearly subscription models. |
| Skills | No deep tech skills required to deploy. Use and gain the benefits of public cloud. |  |  |
| Cloud benefits | Can leverage skills and expertise of cloud provider to ensure workloads are secure and highly available | Can leverage skills and expertise of cloud provider to ensure workloads are secure and highly available |  |
| Flexibility | IaaS the most flexible cloud service as you have control and manage the hardware |  | Users can access the same application data from anywhere. |
|  |  |  |  |

You could use Microsoft 365 on your company's computers (SaaS), and in Azure, you could host your VMs (IaaS), and use **Azure SQL Database (PaaS) to store your data**. With the cloud's flexibility, you can use any combination that provides you with the maximum result.

Azure services are divided into 4 types

1. Compete
2. Networking
3. Storage
4. Databases

All VMs are share one kind of physical hardware, shared hardware is achieved through a hypervisor.

A Hypervisor is a software used to create the virtualized environment allowing multiple VMs to be installed on same host.

Cloud deployment models:

1. Public – shared infrastructure CSDN, provisioned on demand, accessed over internet.
2. Private – infrastructure is privately hosted, managed, owned by the individual company using it.
   1. Giving more importance to and control to company’s data.
   2. Who wanted to keep secret control on company’s data, they can opt this.
   3. On-premise server.
   4. More capEx is required, to acquire hosts and datacenter.
   5. Maintenance is required,
3. Hybrid – combination of private and public
   1. Used when network link is established between private and public.
   2. Normally short-term configurations(dev-test purposes), can often be a transitional state for enterprises.

Key Cloud concepts:

1. On-demand resourcing
2. High scalability
   1. Scaling up and down: altering power and performance of an instance, perhaps one with greater CPU and memory power.
   2. Scaling in and out: adds or removes number of instances you’re using for compute instances.
3. Highly available:
4. Security

Cloud service Models:

1. IaaS
2. PaaS
3. SaaS

Use cases of Cloud Computing:

1. Migrating production services from on-primes to cloud.
2. Traffic bursting – increasing power when needed.
3. Backup/DR
4. webhosting
5. test/Dev environments
6. proof of concept
7. Big data/ Data Manipulation

How data center architecture Is reflected in Cloud:

1. Location
   1. Public cloud providers will have whole regions worldwide
2. Physical security
3. Mechanical & Electrical infrastructure
4. Network infrastructure
5. Servers
6. Storage

What is Microsoft Azure?

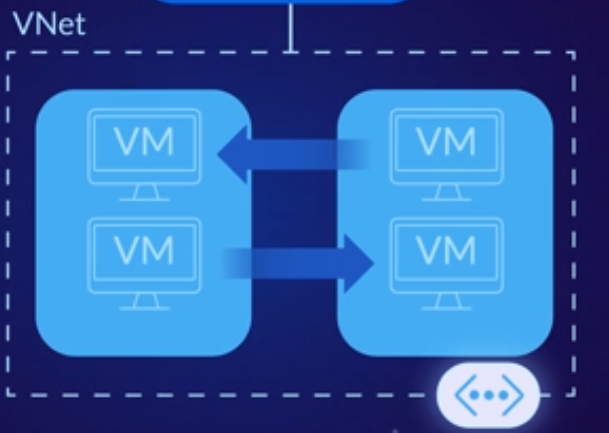
Compute

1. It provides online services, that organizes to use built, host and deliver applications.
2. Lift and shift migration – migrating on-premise application to Azure cloud platforms.
3. Azure VMs are known as IaaS.
4. Azure was providing VMs earlier, later Azure is providing **Azure App services**. Azure app services are part of **PaaS**. We can upload code instances of APP, and Azure takes care of it. If we have **mobile or web service**, we can use Azure App service instead of VMs.
5. **Azure Container Instance** self-contained software environments. Containers are similar to VMs but they dnt have Operating systems installed init. So, it is easy to deploy them, as they very light weight applications. Containers run on VMs.
6. IF we have application which uses more than one container, if our application uses more than one container then we must go with Kubernetes. In that case we must use **Azure Kubernetes service**, also known as **container orchestrator**.
7. **Azure Kubernetes service** makes it easy to deploy and manage multi container application in Kubernetes service.
8. **Azure Functions** it is Microsoft serverless offerings. **Azure functions** is kind of **Azure App service,** except that it executes individual functions rather than entire applications, and you only pay when it gets used. When we provision app service instance, it executes until we shut it down, and we pay for whole time its running. With Azure functions, better we have consumption plan, which means we pay only when a function gets used.

Storage:

1. Azure blob storage: collection of files, flat structure typically used for **unstructured** data. Different type based on frequency you use.
   1. Hot – frequently accessed files
   2. Cool – infrequently accessed file, may be once in a month. Advantage is cost is less than hot tier.
   3. Archive – Rarely accessed, we could use for backup, low storage costs, but highest retrieval costs, it also takes several hours to retrieve files from this tier.
2. **Azure file storage**: this is Hierarchal file storage, typical hierarchy structure that we use in windows. We can mount on windows
3. **Azure Data Lake storage**: Azure data Lake storage Gen 2, this is Hadoop compatible storage for use with data analytics applications.
4. **Azure SQL Database**: it is not typical SQL database,
5. **Azure DB for Open source**: all open source databases are deployed here.
   1. **Azure Database for MySQL**
   2. **Azure database for MariaDB**
   3. **Azure database for Postgre SQL**
   4. These databases are suitable for online transaction processes.
6. If we need to build Azure data warehouses, Then **Azure synapse Analytics** is the best choice.
7. If our application used by multiple users across the world, relational databases can’t scale, in such cases we would need to depend on NOSQL databases, Azure comes with **Azure Cosmos DB**, which can scale globally.
8. **Azure cache for Redis** which is typically used for caching frequently requested data.
9. But there are many options available for Azure storage sections.

Networking:

1. VMs that are connected each other are called **VNet**. VM access another instance through IP address. **Vnets** can be divided into subnets. We can define how traffic should flow between.
2. By default, all outbound traffic from a VM to the internet is allowed. If we need inbound traffic to be allowed, then we need to assign public IP address to VM.
3. If we want VMs in one Vnet should communicate VMs in another VNet, then we can connect VMs using **VNet peering**.
4. Kubernetes in can be in VNets too, along with VMs.
5. If we want to create a secure network between VNet and On-premise network, we can use either **Azure VPN** or **Azure ExpressRoute**.
   1. VPN – sends encrypted traffic over the internet.
   2. ExpressRoute – it is a dedicated connection for High speed and reliable connection between on-premise systems to cloud systems, but much expensive than VPN.

When we sign up for portal.azure.com, Microsoft azure gives you subscription account and billing account. We can have multiple subscriptions in billing account. Each subscription generates invoice, so, for each subscription will generate billing for each department in your organization.

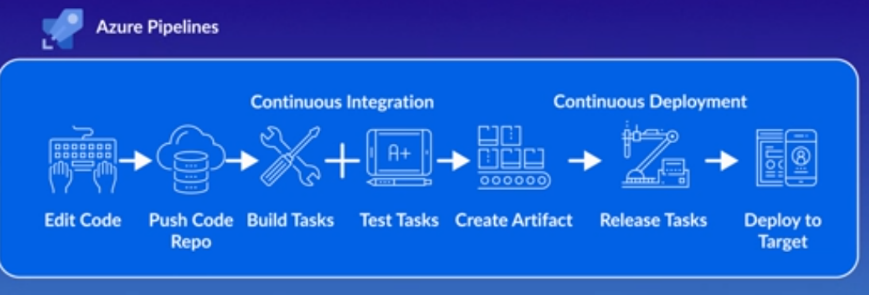
Resources in subscription are isolated, we must have multiple subscriptions for security and multiple compliance reasons.

Learned how to create a VMs, how to deploy in html project in Azure webapp.

In order to delete any up and running service, it is better to delete resource group. Whenever you deploy webapp and you use CLI commands to deploy, it will automatically create resource group for you. If you delete resource group all your instances, webapps, gets deleted which ever tagged to the resource group.

Service Category:

Microsoft provides a great tool called **Azure Migrate**. Which helps us to migrate applications from on-premise to Azure cloud.

1. It discovers on-premise applications which includes both physical and virtual servers.
2. For each server it tells you that
   1. Whether the application is ready to migrate or not?
   2. How big the azure VM will be?
   3. How much it costs?
   4. Any dependency servers that will also need to be migrated?
3. Azure also maintains **Azure active directory,** which takes care of identification. Similar tool, which is like Active directory. Many options are available to get sync in between On-premise directory to **Azure Active directory**.
4. **Azure Pipeline** helps to have continuous integration and continuous deployment. Lets you create automated workflows to continuously build, test, and deploy code.
5. **Azure CDN (Content Delivery Network)**: it helps to speed up responsiveness of our application. It caches the most frequently accessed data to in locations around the world. So, end users will retrieve it from closet point. With this it really feels like, web cloud deployed applications feel like, they are local applications.

**AZUre IoT** applications: it is a SaaS. With out writing any code.

Azure Sphere: helps to make more secured all IoT devices. It includes **certified chips**, **Azure Operating system, and Azure Cloud security.**

When you get a lot data from IoT devices, you might be interested to perform Analytics on top of this data. Microsoft provides wide varitery of Analytics tools.

1. **HD Insight** – framework to provide Hadoop, Spark, Hive and strom.
2. **Azure databrics**
3. Azure synaptic services.

**Azure cognitive services**:

1. Prebuilt artificial intelligence tools. Cognitive services helps you add AI tools to our applications, even if we don’t know anything related to Machine learning.

**Azure bot services**: framework for creating chatbots.

**Azure machine learning studio**: built machine learning without any coding.

**Azure machine learning services**: best solution when you need to implement and build your custom modified artificial intelligence tools.

**Azure Integration**: using this we can integrate all our individual applications.

**Azure Monitor**: keep track of all services what is happening. **Azure monitor Correlates events from multiple resources into centralized repository**.

Designing a Solution:

e-commerce application in Azure reference architecture.

1. Azure web app – for hosting web-based application to book tickets
2. Azure SQL database – to save all concerts.
3. Azure cognitive search – to search all concerts in your database
4. Azure Actice directlry – to save login information of your company.
5. Azure Queue storage– when we receive custom orders, we should keep them in a Queue, and process them one by one.
6. Azure function: when ever we need to process any Queue, we should have one function.
7. Once it processed the Queue, it will process the ticket and stores them as a image, it will be called as Azure Blob storage.
8. Azure text analytics: to review the concerts, how did they feel.
9. Azure cache Redis: to cache the concert information, makes search functionality but faster.
10. Azure CDN: caches the website files whenever something requested, makes faster browsing experience.
11. Azure traffic manager manages the traffic to our application
12. Azure insights: helps to understand diagnostic issues, how people are reacting with our application.

**Diff between Azure CDN and Cache Redis**: Redis stores session state and other data needs provides low latency access, CDN used to cache static content such as images, CSS or HTML

**Managing services**: building webapp is one thing, but making sure it runs on system and runs with less expensive is must.

**Azure Advsior**: helps to understand the Azure systems, not only this it also helps us understand how do we reduce the costs.

**Azure Security center**: dashboard, Azure also shows any page/application not following compliance rules, it will get displayed on security center. Also, shows how successful is my Azure subscriptions are.

**Azure Resource Manager (ARM)**: it helps you to automate creating virtual machines and delete them. ARM is template, for specific configuration, and it takes care of creating VM automatically for you. We can also export those templates as well. Also provides consistency across azure environment.

**Azure Blueprints**: which lets you automate everything in your azure environments.

1. Azure Security center : it is unified infrastructure, it improves security of not only Azure resources but also Azure data center.
2. Azure Key vault: solution to manage, keys, certificates, secrets.
   1. We can also store, tokens, passwords, and certificates too.
   2. Azure Key vault designed in such a way that, Microsoft cant see or extract company’s daa.
3. Azure f Logs:
   1. It monitors the resources you wanted to monitor.
   2. They include metrics and logs.
   3. Using logs we can perform analysis and on our resources.
4. Azure sentinel
   1. Cloud based **security information event management** provides **security analytics** and **threat intelligence** across the enterprise.
   2. Detect threat even your solution available in cloud or on-premise. Provides 30000 foot view, So, you can monitor most of the services.
   3. Actively hunts for suspects or threats.

**Storage Security**

1. Azure storage service encryption
   1. All the data available in Azure is automatically encrypted using 256-AES encryption.
   2. Encryption cannt be disabled.
2. Shared access signatures
   1. Another security features
   2. It provides a granular control how your data should be accessed.
      1. Such as what entities can user use
      2. How long those security should be applicable.
3. Storage account keys
4. Storage analytics

Database Security:

1. Azure SQL firewall Rules
   1. When Azure SQL created, Azure SQL Database firewall automatically blocks public endpoint for the server
   2. All the requests from internet should pass through SQL firewall rules.
   3. We can implement 128 server rules
2. Azure SQL Always encrypted
   1. Used to store sensitive data i.e. credit card, SSN numbers,
   2. It is available in all versions of Azure databse, starting rom 2016.
3. Azure SQL transparent data encryption
   1. Used to protest SQL databases, SQL managed instances, from malicious activities or offline activities.
   2. Real time encryption provided.
   3. We cannt encrypt logical master database.
   4. TDE has to be manually enabled for SQL database, managed instance or synapse databases.
4. Azure SQL Database Auditing
   1. Perform audition
   2. Generates audit reports makes iit easier to check anamolies.
   3. Best to enable server level blob audting and leave database level blob auditing.
5. Role based access control (or RBAC)
   1. Using RBAC, we can easily manage what users have access to Azure, what can they do with RBAC. RBAC is authorization systems, built on Azure Resource Manager.
6. Azure Active directory
   1. Identity and access management services.
   2. Using AD, we can control access to internal resources or external resources too.
7. Azure Active directory B2C
8. Azure Active directory B2B
9. Azure Active directory Domain services
   1. Replicates from AD service and can also works with AD DS.
10. Azure multi-factor Authentication
    1. Offers 2 step verifications.

Networking Security:

1. Network security Group
   1. Several network security rules will get created.
   2. All these rules comes in play when you access Azure resources.
   3. Can create rules, cant delete default rules.
2. VPN Gateway
   1. To exchange information between Azure cloud to On-prime network.
   2. When virtual gateway get created, Azure creates another 2 VMs, which are not accessible to any one or not part of VNet
3. ExpressRoute
   1. Azure cloud to On-prime via private connect instead of VPN.
   2. Layer3 connectivity
4. Firewall
   1. Included with GateWay services.
5. Application Firewall
6. DDOS protection
   1. Basic
      1. Automatically enabled
      2. Relatime mitigation
   2. Standard
      1. Protocol attacks
      2. Application layer attacks
7. Network service endpoints
   1. Extend the identity/private address of Azure virtual network.

Price and support:

1. Private businesses must have at least 500 users, and public should atleast have 250 users.

Azure Support options:

1. Developer
   1. For trail and non-production environments.
2. Standard:
   1. Reply with in 1 hour
   2. Available in 24/7 around the clock.
3. Professional direct:
   1. 24/7 available
   2. Reply with in 1 hours
   3. Trainings provided.
   4. Operational support
4. Premier
   1. Response time in 15 mins
   2. Guidance provided.
5. Microsoft developer network forums, for any questions.
6. Stackoverflow
7. Server fault
8. Azure feedback forums.
9. Azure knowledge center

**Azure SLA:**

1. Formal document, specific terms and conditions
2. Three primary services
   1. Performance targets
   2. Uptime
   3. Connectivity
3. With free basic account you wont get support, but you can use them as production. With free account, you don’t get any support as well.
4. Basic Tier of Azure comes with 99.9% SLA, but not free tier of Azure.
5. Azure previliaged identity management is multifactor authentication
6. You wanted to create a VMs in Azure and you have PowerShell script, you have Linux machine with Azure CLI installed, is this enough? No, because you need **Azure CLI** with **PowerShell** core installed in machine. If you have command prompt
7. If you have Azure cloud shell installed, above config is enough. In Azure cloud shell you can run bash and PowerShell based scripts.
8. You can run PowerShell in MacOS too.
9. **Cloudyn** is used to track cloud usage and expenditure.
10. Azure Service Bus is enterprise message broker.
11. When you make **Azure reservations** for a year or three years, costs might reduce than normal paln.
12. **Azure management groups** are for managing resources in Azure.
13. **Azure Functions** are serverless computing.
14. **Azure Logic Apps**: lets you automate and orchestrate the specified taks.
15. **Azure Application insights**: used to monitor live web application.
16. we can have Azure resources which are belongs to same resource groups but can be available in different locations.
17. When you assign certain tags to resources, resource groups can’t inherit them, but they can inherit permissions.
18. **Azure locks** to prevent accidental modification or deletion of resources in Azure.
19. When you wanted to tag some variable i.e. orgazniation you wanted to tag company name, that you would do in Azure polocies,
20. Azure Key Valut: used for security purposes and secret key management.
21. Azure SQL database comes under PaaS.
22. Company wants to move data from one region to another, So, Azure storage account automatically replicate data to another region? Yes, if you set replicate to read -access-geo-redundant storage.
23. **Microsoft trust center** can assist you company in getting compliance reports.
24. Public preview is available to all customers.
25. Data center failures
26. For any services, you must buy the appropriate support plan, it doesn’t come as part of procuring.
27. Azure CLI can be installed in windows machine and MACOs , this is not a web based tool
28. Azure virtual machine scale sets: lets you create and manage set of identical VMs. Scale sets are nothing but more VMs. Scale sets provide high availability to your applications and allow you centrally manage, configure. If ScaleSets are deployed in multiple data centers then they provide high tolerance.
29. Azure resources can access resources from other resource group too.
30. You can extend private cloud, by adding virtual servers in a public cloud. But it becomes the hybrid cloud.
31. Azure Storage is IaaS.
32. From portal.azure.com. we can launch Azure cloud shell and select bash or powershell. As this is supported in web browser, you can do it in from Ubuntu, Windows, or Mac OS.
33. PowerApps is not a part of Azure. So, you can’t use in Azure. It is a tool to create webpage layout.
34. Data copied to Azure storage account, is maintained automatically at least three copies.

The more regions your cloud vendor, provides the more flexibility or scale your application, because it is closer to your users. Also some services are available in only few regions, and few services are available across all regions. Few regions where Azure deployes, gov projects, where it has Gov US people monitors those data centers, such as Arizona, Texas etc..

Regional Pair: As it is possible to have diaster, So Azure pairs up with another region servers, with in the same geography. **All region pairs i.e. their physical servers are always at 300 miles away. Few services such as geo-redundant storage provides automatic replication to the paired device.**

**Availability sets** are a way to ensure that your application remains online, even if a high maintenance event is required.

**Availability zones**: are the physical separate locations within the region, that use availability sets to provide fault tolerance.

Do deploy your apps into availability when they are high critical applications, So, that your application will be available round the clock. Usually people deploy, their VMs, managed disks, load balancers, SQL databases into availability zones.

**Container services:**

If you wanted to run multiple instances of an application, on a single host machine, then container services are best option. Container orchestration is can start, stop, scale out an application instances as needed. They come under Azure **PaaS**

1. Container references the operating system of the host environment that runs the container.
2. Unlike virtual machine, you don’t need to manage the operating system.
3. Containers are light weight and are created to stop, start, scale out dynamically.
4. Containers respond to changes very quickly to restart, in case of crash or hardware interruption.
5. Azure support docker containers.

As more and more applications move to container services, So, it will be hard to manage your applications, with Kubernetes you can easily manage workload containers.

The task of automating, managing and interacting with large numbers of containers is known as orchestration.

We can move existing applications to containers and run them in AKS, Kubernetes.

**Azure networking**:

1. Azure networking allow you to connect cloud and on-premises infrastructure.

Azure virtual network: enables to connect Azure services such as VMs to securely communicate each other. Multiple virtual networks can be connected from different regions can be connected using virtual network peering.

**Azure load balancing**:

Load balancing provide us to scale our applications and create high availability to our services.

**Azure VPN Gateway**:

Responsible for sending encrypted traffic between azure virtual network and on-premise network or over the internet.

**Azure Application gateway**:

It is a web traffic load balancer that enables you to manage traffic to your web applications. With application gateway you can route applications from sourceIP to destination IP address and port. Also provides a firewall to secure your application.

**Azure Cosmos DB**:

Globally distributed services, enables you to elastically and independently scale across any number of Azure’s geographic regions. Schema less and highly responsive.

**Azure Database migration service**:

Supports fully managed database platform to support seamless migrations from multiple database sources to Azure platforms with minimal downtime.

**Azure IoT central**:

Is a SaaS solution to that makes it easy to connect, monitor and manage IoT assets.

1. New-AzVM is a command to create virtual machine inside Azure subscription.
2. Powershell core is a cross platform version of powershell that runs on windows, Linux or MacOS.
3. Azure CLI – cross platform command-line program that **connects Azure and executes administrative commands on Azure resources**.
4. Azure Cloud Shell: browser-based cloud shell, it provides flexibility of choosing a shell. Windows users can select powershell, linux users can opt for bash shell. When you use **Cloud shell**, you need to have **storage account created**.
5. Azure advisor: advices on high availability, security, cost and performance. It continuously look for deployed services and provide recommendations.

10/26/2020

Below is the command to run in PowerShell to create Virtual Machine

New-AzVm

-ResourceGroupName "myRGTemplate" `

-Name "myVMPS" `

-Location "West US" `

-VirtualNetworkName "myVnetPS" `

-SubnetName "mySubnetPS" `

-SecurityGroupName "myNSGPS" `

-PublicIpAddressName "myPublicIpPS"

Get-AzVM -name myVMPS -status | Format-List 🡨 command to get the status of VM

Stop-AzVM -ResourceGroupName myRGTemplate -name myVMPS

az group list 🡨 display all resource group names

az group list –output table 🡨 shows in table structured format

Azure CLI commands:

az vm create --name myVMCLI --resource-group myRGTemplate --image UbuntuLTS --location EastUS --admin-username azureuser --admin-password "Pa$$w)rd1234" 🡨 Create Virtual Machine in Azure CLI

az vm show --resource-group myRGTemplate --name myVMCLI 🡨 to show VM

az vm show --resource-group myRGTemplate --name myVMCLI –show-details –ouput table

venkatsubbarao@Azure:~$ **az vm stop --resource-group myRGTemplate --name myVMCLI**

About to power off the specified VM...

It will continue to be billed. To deallocate a VM, run: az vm deallocate.

venkatsubbarao@Azure:~$ **az vm show --resource-group myRGTemplate --name myVMCLI --show-details --output table**

Name ResourceGroup PowerState PublicIps Fqdns Location Zones

------- --------------- ------------ ------------- ------- ---------- -------

myVMCLI myRGTemplate VM stopped 52.188.17.190 eastus

**10/27/2020**

A firewall is a service that grants access based on originating IP address. We create firewall rules with set of IP address.

**Network Security Groups**:

Allow you to filter network traffic to and from Azure resources in an Azure virtual network. NSG contain security rules that enables you to filter traffic to and from resources by source and destination IP address, port and protocol.

**Application security Groups**:

Enables you to configure network security as natural extension of an application structure. ASG enables you to group similar port filtering requirements.

**Azure network security solutions**:

**Perimeter layer**

Responsible to protecting organizations from network-based attacks against resources.

**Azure security Center**

To access full site of Azure security center services you will need to upgrade to standard tier subscription.

**Azure Blueprints**:

Define a repeatable set of Azure resources that adhere to organization standards.

Azure Blueprint is different from Azure Resource Manager Templates, because with Azure resource manager templeates, after you deploy they have no active relationship with deployed resources. But with Azure blueprints, you still maintain the relationship with deployed resource, there by maintaining relationships, this way it improves auditing and tracking capabilities.

Azure monitor is something, which monitor Azure resources, and it also collects data from various sources.

**Azure Health Service**:

Provides personalized guidance when there are issues with Azure resources, helps you understand the issues, and they notify you. Also, notifies you where there is a planned outage.

Questions:

Which Azure service should you use to correlate events from multiple resources into a centralized repository?

* A. Azure Event Hubs
* B. Azure Analysis Services
* C. Azure Monitor
* D. Azure Log Analytics

You can run Azure CLI commands on PowerShell core, PowerShell core can be installed on Windows, Linux, and MacOS too.

You were given with PowerShell script to create Virtual machines; you have Linux machine with CLI installed. You csynaan’t meet this goal.

Azure firewall can limit the amount of traffic.

You have on-premise systems to communicate to the Azure virtual machines? What do you recommend? A Virtual network gateway and a gateway subnet.

MPP relational databases– synapse analytics

\*An organization that defines all international standards across all industries -ISO

\*An organization that defines the standards used by the US govt -NIST

\*An European policy that defines data privacy & protection- GDPR

\*A dedicated public cloud for federal/state agencies in the US- Azure Government

Question #90*Topic 1*

What should you use to evaluate whether your company's Azure environment meets regulatory requirements?

* A. the Knowledge Center website
* B. the Advisor blade from the Azure portal
* C. Compliance Manager from the Security Trust Portal
* D. the Security Center blade from the Azure portal

**Azure Advanced threat protection ATP** is to monitor the threats using sensors.

**Azure Active Directory Identity protection** is to enforce Azure MFA.

**Azure Trust center** is to check if Azure complies with regional requirements.

A premier support plan can only be purchased by companies that have an **Enterprise Agreement(EA)**.

Azure Virtual network interfaces are come with free of cost.

Unused user accounts don’t come with charge, So, you can keep them.

Monthly uptime percentage = (Maximum available minutes – Downtime in Minutes / maximum available miutes \*100

Using Azure All Inbound traffic is free, whereas outbound traffic is going to be charged.

Azure free account has a spending limit

Azure free account has a limit for data that can be uploaded to Azure.

Azure free account has limit of 10 web, mobile and web apps.

Transferring data between different azure regions is costly, but if you move with in the region it is same.

Azure Dev/Test Labs will minimize the administrative effort required to deploy and remove virtual machines.

Standard support plan is the lowest cost option to receive 24x7 access to support engineers by phone.

15. to achieve hybrid cloud, company must always migrate from private cloud model. 🡪 no

17. Virtual Machine Scale sets, allows us to create, manage identical VMs.

23. Azure resources, can only access other resources in the same resource group.

37. **Which Azure service should you use to correlate events from multiple resources into a centralized repository? Event Hub**

**You can delegate permissions to several virtual machines, then that virtual machine should be in same resource group.**

**To what should an application connect to retrieve security tokens? Azure AD**

**Azure Activity log** is used to view which user turned off VM in last 14 days.

Azure firewall/NSG doesn’t encrypt all the network traffic sent from Azure to internet.

**Monitor threats** using Azure sensors Azure **advanced threats protection**.

**Enforce Azure MFA** based on **Azure AD identity protection**.

From Azure health,

1. Administrator can view health of all services deployed.
2. Azure administrator can create rule to be altered if Azure fails.

Azure services in public preview are not subjected with SLA.

Azure fabric services:

1. Number of node types in cluster
2. Properties for each node.

Azure Complaince manager is the place to track company’s standards and regulations.

Azure free account has spending limit.

Azure free account has a limit for the amount of data that can be uploaded to Azure.

Companies can increase the SLA guaranteed uptime by adding azure resources to **multiple regions**. its not if they buy multiple subscriptions.

If you need different payment for each your department, you need to use different subscriptions.

Architectural review 🡪 premier plan.

**Lowest possible cost** is basic plan.

If single data center fails, two or more regions 🡪 No. if in question two or more availability zones 🡪 yes

Public IP address costs money, so, you should remove.

Control the ports on the internet can use to access virtual machines 🡪 NSG.

Limit the type of connections from web servers to database servers 🡪 NSG

Azure storage accounts: IaaS

When ever any VM wants to access Internet via http, you should modify **NSG and firewall**.

To what should an application connect to retrieve security tokens? **Azure Active Directory**

Company’s regulatory and standards 🡪 **compliance manager**

COSMOS DB comes under PaaS.

Better to have **multiple subscriptions** when each department managed by different administrator.

Company’s regional requirements 🡪 **Trust center**

Azure firewall/NSG don’t encrypt data, but it blocks or allow traffic based on IP address.

**Azure monitor** can monitor performance of on-premise systems too, also sends triggers/alerts.