REVIEW NOTES FOR:

AZ-900: MICROSOFT AZURE FUNDAMENTALS

Microsoft Learning:

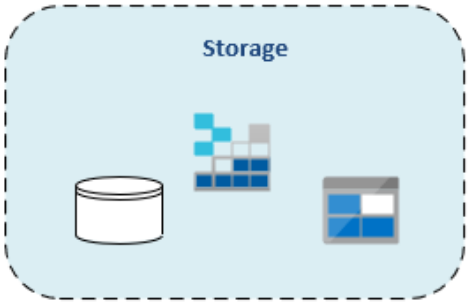
https://docs.microsoft.com/en-us/learn/paths/az-900-describe-cloud-concepts/

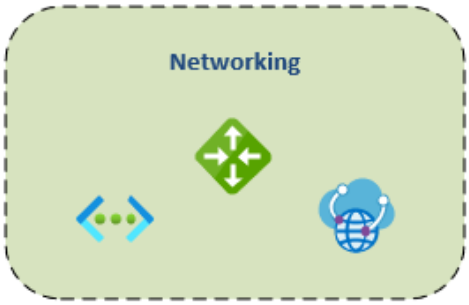
Notes prepared by Nimbasys referencing Microsoft resources

Describe Cloud Concepts

Core Azure Architectural Components

- Cloud computing is a delivery model for services. There many services in Azure, but perhaps the four main services in Azure include storage, compute, networking, and analytics.





Cloud Benefits

https://docs.microsoft.com/learn/modules/principles-cloud-computing/3-benefits-of-cloud-computing

Cloud Advantages

1. High availability – minimize downtime.
   - Example: SLA. 99.99% for Azure AD
   - Does not mean infinite availability
   - **Fault tolerance** – zero down-time of services provided by Azure
   - Additional resources can kick in to ensure availability

2. Scalability

   As demand increases, you can meet the demand in Azure by
   - Vertically – increase capacity (size) UP
   - Horizontally – increasing instances (Scale Sets – VMSS) OUT

3. Elasticity – focus more on apps. Apps are "serverless" in the sense that you don't worry about the server, but they run on a server behind the scenes.
   - Ideal benefit for seasonal; based on user consumption models
   - (Black Friday)

4. Agility – ability to rapidly develop, deploy, test apps and solutions. As an example, you can allocate and provision resources for a server in minutes. Allocate/deallocate quickly.

5. Geo-distribution – making services available to clients where the clients are (CDN)

6. Disaster Recovery – backups, data replication, geo-redundant.
   - Cost associated with each solution
   - Time to recovery and recovery point metrics
   - Downtime

Cloud services is a consumption-based Model, meaning you pay for what you use

Capital Expenditure (CapEx) = up-front costs, often depreciated over time. Value reduces over time. Cost of acquiring resources.

Operational Expenditure (OpEx) = spending money on services as they are incurred. Consumption-based costs. On-going cost of running resources.

Examples include:

- Functions - per execution, per second, or some combo
- Virtual machines – pay for when the vm's are using compute and storage.

Categories of Cloud Serivices

Cloud Service Models

https://docs.microsoft.com/en-us/learn/modules/fundamental-azure-concepts/categories-of-cloud-services

- Infrastructure as a Service (IaaS) – provides servers, storage and networking as a service
  - No ownership of hardware
  - Includes VMs/servers, networks, etc

- Platform as a Service (PaaS) – superset of IaaS and also includes middleware

  - Includes IAAS as well as middleware, tools, DBs
  - Supports web application life cycle
  - Avoids software licenses

- Software as a Service (SaaS)
  - Includes IAAS and PAAS.
  - You pay access fee to use the software
  - Always have the latest features
  - PaaS in Azure – common resources includes App ServiceS, Azure SQL Server, Azure Active Directory)
  - O365, Quickbooks, Abode are examples of SaaS

The final Service Model is Serverless, though it often included in SaaS. For the exam, know the main three: IaaS, PaaS, SaaS.

- Serverless
    - There are servers, but you don't manage them
    - Azure functions
    - Serverless is lower-cost solutions
    - Serverless = PaaS

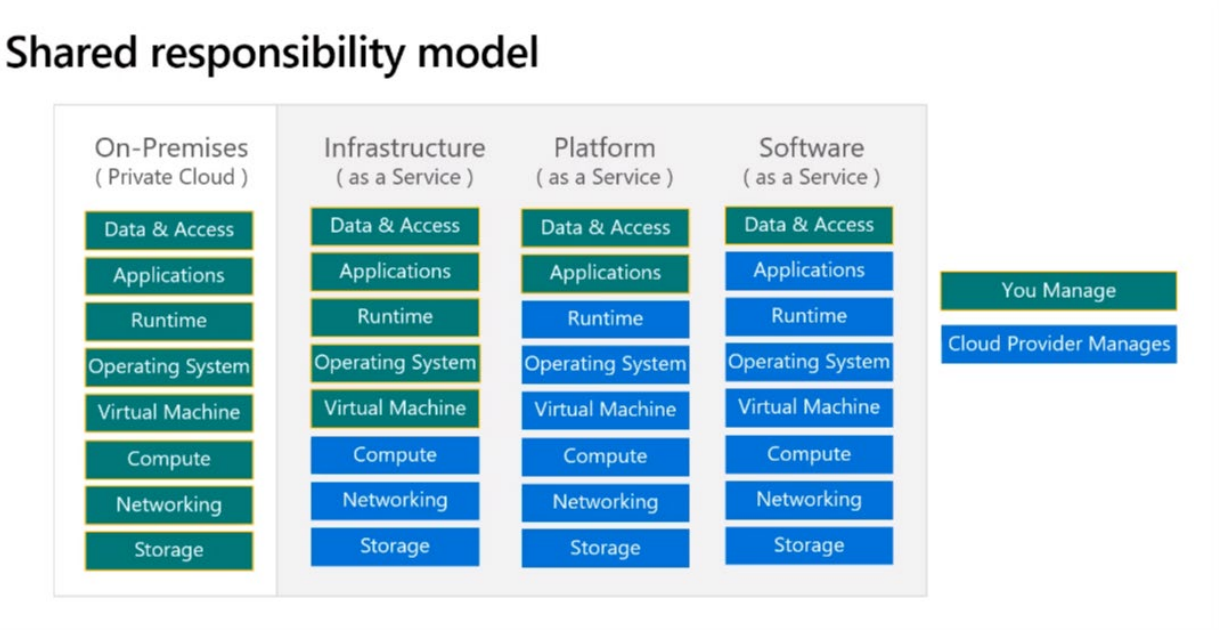
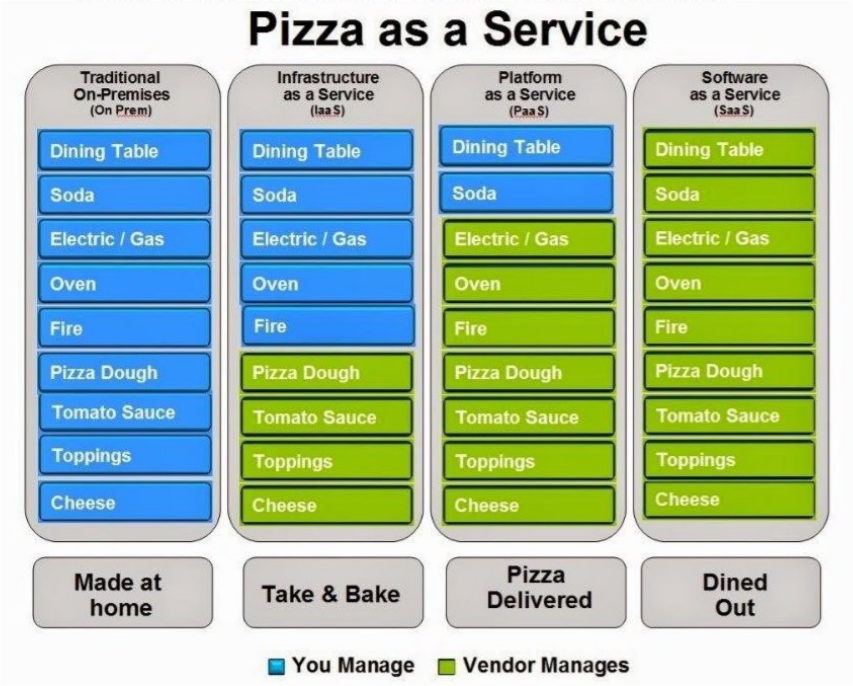


Image: https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/what-is-cloud-computing



Types of Cloud Computing

https://docs.microsoft.com/en-us/learn/modules/fundamental-azure-concepts/types-of-cloud-computing

Public cloud – Azure, AWS – delivered over the internet.

- No hardware purchases
- Monthly fees
- No control of updates to features

Private cloud –services available only to select group of people.

- You can have benefits of public cloud.
- Azure Stack
- Better security and privacy.
- You can own hardware in this situation.
- More staff required.

Hybrid – where most everyone is currently. Combination of private and public cloud.

- You cannot own hardware here.
- Avoid outages more easily
- Used when governance is an issue.
- Has more complexity - has more moving parts.

Describe Core Azure Services

Core Azure Architectural Components

1. Data center – physical building that houses connected servers.

2. Regions – set of datacenters deployed within a low-latency defined perimeter and connected through a dedicated low-latency network. (< 2ms latency between data centers).

   - Each region has more than one data center.
   - A data center is a physical location.

3. Not all regions are the same. Features will vary from region to region and not all regions will have all features
   - Prices for resources will vary between regions
   - Choosing region closest to users may be beneficial

   Speed Test (http://azurespeedtest.azurewebsites.net/)

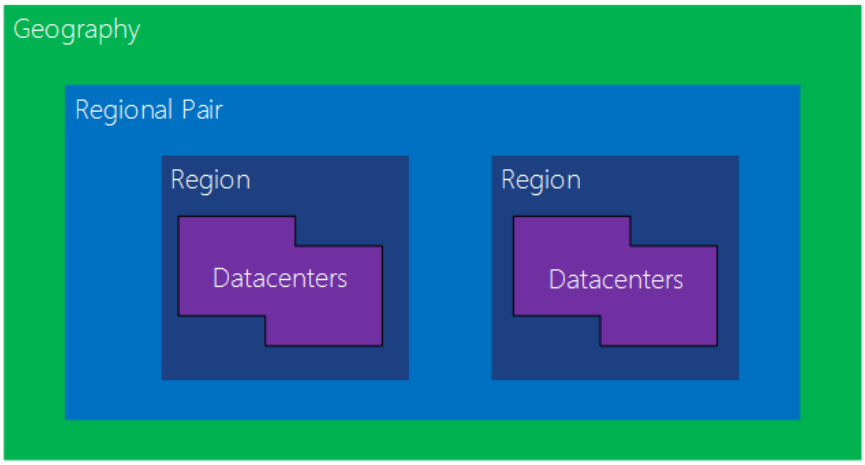
4. Geography – contains one or more regions. Used for compliance requirements (i.e., data must reside in U.S.)

5. Regions are paired. Paired regions have high connectivity and reliability and are positioned so that only one region in the pair updates at a time.
   - If Region goes down, you lose access to your resources (think of our current local data centers)
   - Region pairs provide protection in the case of a region going down.
     - If one region experiences an outage or failure, you can failover to the paired region.
   - Region Pairs cannot be chosen
   - Region Pair Examples
     - East US ----→ West US
     - East US 2. ---→ Central US
     - US Gov Virginia --→ US Gov Texas (Azizona)
6. Regions preserve data residency and compliance boundaries.

7. Some better-known services take advantage of the regional architecture, such as Geo-Redundant Storage.

8. There are special regions – such as US Government.

9. Regions exist within geographies. Per Microsoft, an Azure geography is an area of the world containing at least one Azure region - but often contains more than one region



https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions

10. Availability Zones – physical location within a region. Each zone is made up for one or more data centers.

Availability Zones – protects your resource from data center failures.

11. Each data center in an availability zone has its own cooling, power, networking.

There is a minimum of three separate zones in all enabled regions.

(NOTE: not all regions support Availability Zones)

12. Availability zones are really a combination of fault domains and update domains.

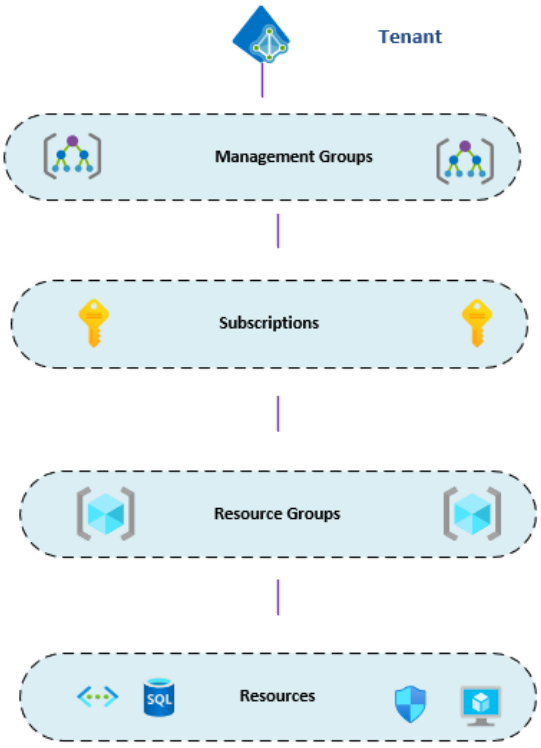
13. Resources – objects used to manage services. Everything in Azure is a resource.

14. Resource Group (RG) – containers for resources. Resources can only exist within a resource group. Typically includes resources that contain the same lifecycle.

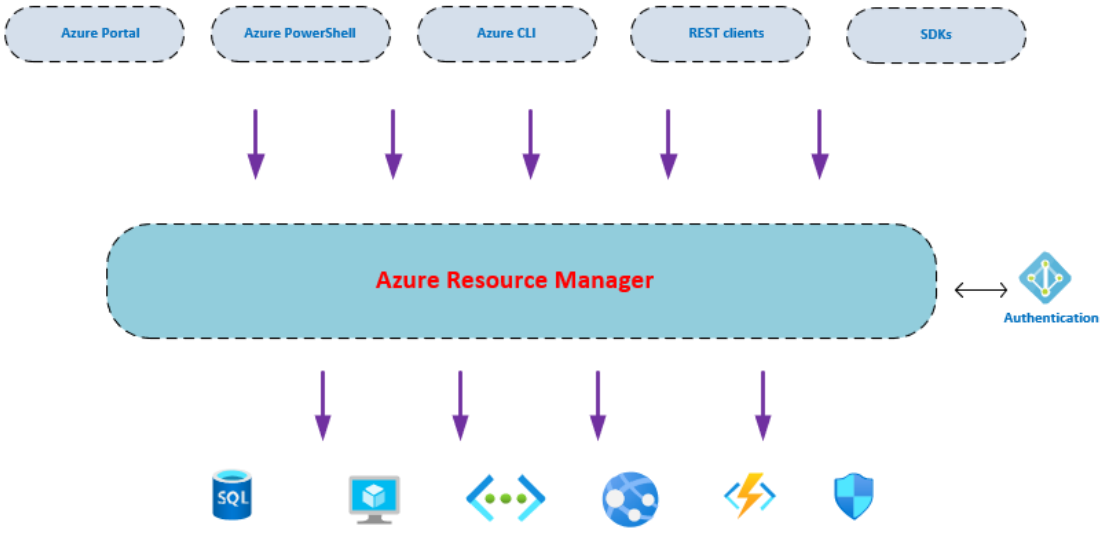
    - Resources can only exist in one Resource Group.
    - Permissions can be applied to a Resource Group (security boundary).
    - Resources can be moved from one Resource Group to another Resource Group

15. Subscriptions – used to manage costs and resources. This involves $. To get a subscription you'll associate some form of payment.

16. Management groups – used to manage policies, access, and compliance for subscriptions.



17. Azure Resource Manager (ARM) – deployment and management service for Azure. Central for all resources in Azure.



Azure Core Resources

Core Resources Available in Azure

Azure Compute

Easy to deploy, pay-as-you-go options, easily scalable.

Virtual Machines – IaaS Virtual Machines

Azure App Service – PaaS. Host web apps that doesn't require underlying infrastructure.

Serverless Computing – build apps without infrastructure.

- Azure Functions
- Azure Logic Apps
- Azure Event Grid

Virtual Machines

1. You control the OS, including maintaining patching and backups.

2. When creating, choose type of image (Windows 2019, Linux, etc.), size of VM (memory, CPU, etc.), and availability options.

3. Azure Marketplace – online store within Azure portal that includes images and resources. Some offered by Microsoft, some by third-party. You can find server images with preconfigured software already installed (at a price).

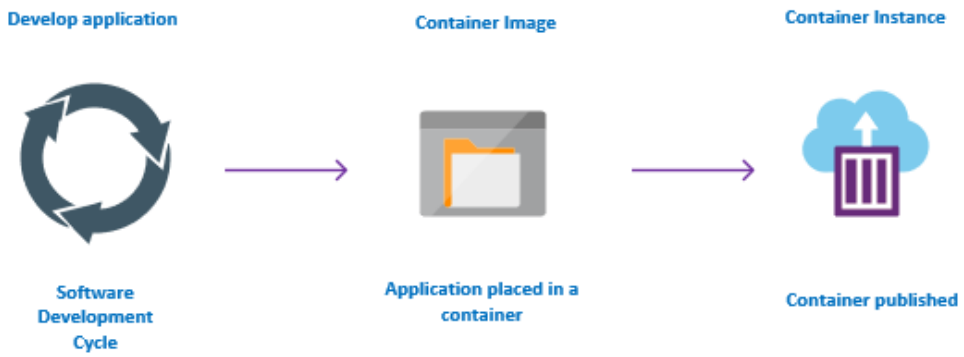
Containers

Azure Containers – virtualized environment that does not require OS. Used to add an isolated application into a package. For server-based apps, such as web apps.

The container has everything needed for the app to run – all dependencies, etc.

- Allows us to manage all dependencies.
- Increased portability
- Less overhead
- More efficient
- Consistency

Container – instance of a container image.



User develops app, adds to container, and container is published

Image – read only template, instructions for how to run container.

Container – runnable instance of the image.

Container Registry – stores container images, distributes the images.

- Docker Hub – public container registry
- Azure Container Registry – same thing, but within Azure.

Docker – standard for containers and the formatting of the containers. Provides a runtime for Docker containers.

How to host containers:

- Locally – can be installed, hosted on any local server (even workstation)
- VMs in Azure
- Azure Container Instances – used for smaller applications, but managed by Azure. PaaS that runs a container in Azure.
- For larger container needs, use Azure Kubernetes Service (AKS).
- Azure App Service – can be used to host containers.

Azure Kubernetes Service – orchestration service for containers when managing containers. This allows you to manage many containers.

- Adds identity access management (security)
- Adds Availability (regions, etc)
- Adds automatic scaling
- Adds automatic deployment

Pods – groups of containers. Pods are run on nodes.

Nodes in AKS are virtual machines in the background. This allows the advantages of other Azure services – VM Scale Sets, etc. for high availability.

Azure Container Registry (ACR) – service that manages your images. Fully managed service.

Azure App Service

PaaS service for hosting applications. It can host web apps as well as host containers.

Essentially, you upload your code and it is hosted on a backend web server that is run and managed by Azure.

When hosting your app, the URL will be https://yourappname.azurewebsites.net

You must create an App Service Plan for your app to be hosted.

Serverless Computing

This includes Azure Functions, Azure Logic Apps, and Azure Event Grid.

Azure Functions – allows you to run custom code

Azure Logic Apps – allows you to create workflows in portal, no code. Designed for automation and orchestration of scalable solutions. Key word: workflow

Example usage – move files from SFTP server to Azure storage.

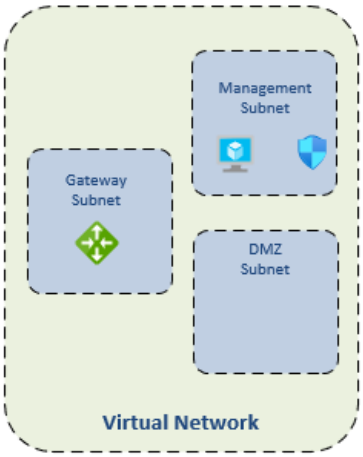
Azure Event Grid – allows you to build apps with even-based architectures. Resources raise events in Azure.

Azure Networking

Networking: allows communication between resources. Includes …

- Virtual Network (VNET)
- VPN Gateway
- Virtual Network Peering
- ExpressRoute

Virtual Network (VNET) – a defined IP address space in Azure. This creates a network boundary. The address space can be divided into subnets. Resources reside within the subnets.



By default, resources in one VNET cannot communicate with resources in another VNET. You can take steps to make that communication work (VNET peering).

Virtual networks in Azure can be protected by Network Security Groups and Network Virtual Appliances.

Connections to/from Azure

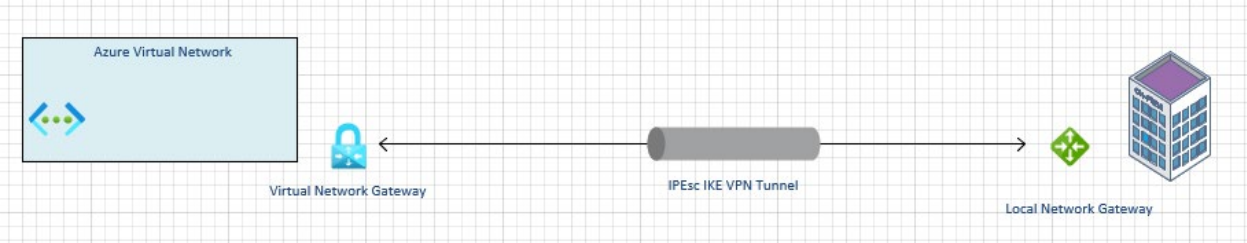
Site-to-Site VPN – allows you to connect Azure VNETs with on-premises networks and resources.

Point-to-Site VPN – allows you to create a private and secure connect from externally into the Azure network.

ExpressRoute – a dedicated private network that uses a provider to connect between Azure and on-premises. High-performance.

- ExpressRoute provided layer 3 connectivity between on-prem and Azure
- Built-in redundancy
- QoS for specific services

Note: ExpressRoute connections are NOT encrypted by default. If desired, you can add encryption.



Azure VPNs require a resource in Azure called a vpn gateway. This is a resource that incurs charges based on the size of traffic it can handle. It is similar to an on-prem firewall. In fact, the VPN Gateway makes a connection to the on-prem firewall when setting up site-to-site connections.

VPN Gateways can be either policy-based or route-based. Almost always you will want route-based at this time.

- Policy-based VPN Gateway
    - supports IKEv1 only.

    - Static routing used
    - Used in legacy scenarios

- Route-based VPN Gateway
    - IKEv2
    - Dynamic routing (BGP)
    - Allows multiple connections

Windows Virtual Desktop

Remote workstations in Azure that users can access. This provides full desktop for users.

Managed service in Azure. Support for Windows, Mac, iOS, Android, HTML5

Can you Windows 10 Multi-Session, which allows multiple users to share the resources of a Windows 10 VM (as they do with RDS using Windows Server OS).

Works well leveraging O365 OneDrive for Business and Azure File Shares

Uses Azure AD for authentication and supports MFA

Azure Data Services

Kinds of Data

- Structured – relational
    - Azure SQL Database
    - Azure Database for MySQL
    - Azure Database for PostgreSQL

- Unstructured – does not follow a schema (Image files, PDFs, etc.
    - Azure Blob Storage
    - Azure File Storage
    - Azure Disk Storage (disk images, SQL databases)

- NoSQL – semi-structured
    - Cosmos DB

Azure SQL Database Options

1. SQL Server on VM
    - Full control of SQL Server
    - Full features of SQL

2. Azure SQL Database – PaaS. Provides 99.99 availability. Can be server-based or serverless – but in either case this is NOT VM based. This is cheapest model.
   This has slightly less features that on-prem SQL (such as collation options).
   This always runs the latest version of SQL
   Can be single database or Elastic Pool (shared resources between db's)
   Service tiers
3. Azure SQL Managed Instance – PaaS. Provides 99.99 availability.
   This option is fully managed. Can use VNets and use VPN tunnel. Can contain up to 100 db's on the instance.

Other Database Options

Cosmos DB – NoSQL database. Non-relational database. This is a PaaS offering from Microsoft.

- Good fit for serverless app when fast response times are needed
- Used as backend for many gaming applications – such as Halo
- Used to power O365, Azure

Azure Database for MySQL – relational database built on MySQL. Provides 99.99 availability. PaaS.

Azure Database for PostgreSQL – relational database built on PostgreSQL.

Azure Storage Services

Storage:

- Blob (binary large object)
- Disk – attach to VMs.
- Table
- File
- Queue

Locally Redundant Storage (LRS) - copies data synchronously 3 times within a single physical location in the primary region. Least expensive. Protects against server rack and drive failures, but not disaster.

Geo Redundant Storage (GRS) – copies data synchronously 3 times within a single physical location in the primary region and asynchronously replicates to secondary region.

Zone Redundant Storage (ZRS) - copies data synchronously across 3 Azure availability zones for the primary region. Each AV is separate physical location.

Storage Account URLs

https://mystore1.queue.core.windows.net

https://mystore1.table.core.windows.net

…file.core.windows.net

…blob.core.windows.net

File Storage

SMB support, so will work as file share with drive letter

Blob Storage

- Optimized for storing massive amounts of unstructured data
- Steaming video/images
- Log files
- Backups

There are three types of blobs:

- Block Blobs – text, binary data, (<4.7 TB)
- Append – optimized for append operations. Works best for logging needs.
- Page Blobs – files up to 8 TB. Frequent, random read/write
  - VM disks stored here

Blob Pricing Tiers

- Hot – frequently accessed. Higher speed, higher costs.
- Cool – lower costs, lower costs. 30 days.
- Archive – low cost

Describe Core Solutions & Management Tools

Core Solutions in Azure

1. Artificial Intelligence (AI) – adaptive computing that improves over time based on the interactions and results of decisions.

2. Web API – API accessible from servers that accept HTTP requests

3. Rest API – design of URL style that is used to expose API's functionality

Artificial Intelligence (AI)

4. AI approaches:

   - Deep Learning – modeled on neural network of human mind – improve through experience
   - Machine Learning – data science technique; uses existing data to forecast future outcomes

5. Microsoft has three primary AI products:

- Azure Machine Learning
- Azure Cognitive Services
- Azure Bot Service

6. Azure Cognitive Services – prebuild machine learning models that allows apps to logically analyze your data.
   - ability to understand the content of images, video, and audio. Ability to translate text. Provides ability to add multilanguage support to sites. Includes personalizer service to predict user behavior.

7. Azure Cognitive Services:
   - Language – apps can process language and learn how to predict what users want
   - Speech – convert speech to text
   - Vision – add recognition abilities when analyzing pics, videos
   - Decision – add personalized recommendations for users

8. Azure Bot Services – virtual agent that interfaces with humans in natural language. Relies on other AI services behind the scenes.

9. Azure Machine Learning – platform for making decisions. Uses historical data to predict future outcomes. Gives total control of design and training of algorithm using your own data.

   - Create models and define rules for making decisions based on data
   - Models can be used to generate algorithm that outcome decisions based on the data

Azure IoT

10. Internet of Things (IoT) – Internet connected devices embedded in everyday objects which allows them to send/receive data (telemetry).

11. IoT Hub – required to make IoT work. IoT Hub allows for communication between the cloud and the IoT devices. It then allows this data to be used for development.

    - This is a managed service (PaaS)
    - Secure, reliable and scalable
    - Integrates with many Azure services.
    - Works with many programming languages

To begin, you will create the IoT Hub service in Azure.

12. Azure IoT Central – allows for connecting devices to the cloud, and provides templates for building apps.
    - Delivery Platform for IoT.
    - SaaS
    - Little technical knowledge is required
    - Service for managing IoT devices

13. Azure Sphere – set of components which allow you to build IoT applications.

    - Vendors will include chips in their hardware which allow apps to be built that interact with the hardware
    - Sphere adds an OS layer which allows interaction
    - Allows Microsoft to update and secure the apps and devices
    - Security is big part of this service
    - Managed service, PaaS

Azure Big Data

14. Big Data – helps in extraction, processing and analysis of information that is too big and complex to deal with in traditional solutions.

15. Big Data characteristics:

    - Velocity – how fast and how often is data arriving. How fast does the data need to be processed.
    - Volume – size of data
    - Variety – is data structured or not.

    If one of the three metrics is high, the data is considered to be big data.

    Big Data solutions offer:

    - Speed
    - Enhanced decision making (because of quicker data processing)
    - Cost Savings

16. Azure Data Lake Analytics – data lake = very large body of data. Data Lake does parallel processing and allows you to focus on analytics.

17. HDInsights – similar to Data Lake Analytics and based on open-source. Includes Apache Hadoop, Spark and Kafka.

18. Azure Data Bricks – based on Apache Spark (distributed cluster-computing framework). This can run and process data on many computers at the same time.

19. Azure Synapse Analytics – Azure's data warehouse solution. Used for reporting and data analysis.

DevOps

20. DevOps is an approach to align software development processes and automation. Microsoft has three main offerings in the DevOps environment.

21. Azure DevOps Services – suite of services designed for software development lifecycle.

    - Azure Repos – source code repository
    - Azure Boards – agile project management suite that includes Kanban board, etc.
    - Azure Pipelines – CI/CD (continuous integration, continuous delivery) pipeline tool
    - Azure Artifacts – artifact repository
    - Azure Test Plans – automated test tool

    Azure DevOps – SaaS

22. GitHub – one of largest code repositories for open-source software.
    - Git – decentralized source-code management tool
    - GitHub – hosted version of Git

23. GitHub offers the following:
    - Shared source-code repository
    - Facilitates project management
    - Reporting, discussion features

- CI/CD pipeline automation tool
- Collaboration forum

24. GitHub Actions – enables workflow automation with triggers for lifecycle events.

25. GitHub – lighter weight than Azure DevOps

26. Azure DevOps – more focused on enterprise development

27. Azure DevOps Labs – automated process of build, set up, tear down VMs that contain software projects. ARM templates preferred method of DevOps Labs.

Azure Management Tools

1. Azure Monitoring Services:
   - Azure Advisor
   - Azure Monitor
   - Azure Service Health

2. Azure Advisor – makes recommendations based on your resources to improve security, implement best practice, and save money. The recommendations are in five categories:
   - Reliability
   - Security
   - Performance
   - Cost
   - Operational Excellence

   Want to optimize budget in Azure? Azure Advisor.

3. Azure Monitor – monitoring service that collects data from Azure and on-premises resources. Many other Azure services utilize this behind the scenes.

4. Azure Health Service – provides configurable view of Azure services and their status and health. Includes service issues, planned maintenance, and health advisories.

   View at status.azure.com

5. Infrastructure as Code (IoC) – managing Azure environment and resources with code, primarily ARM template-based solutions.

6. Two approaches to IoC – imperative code and declarative code.
   - Imperative – each step to achieve outcome is spelled out (PowerShell)
   - Declarative – only final outcome is defined (ARM templates)

7. Azure Portal – web interface to access Azure. Most Azure resources are available in this manner.

8. Azure Mobil App – iOS and Android app to access Azure. Allows you to monitor status of resources, alerts, etc. You can also run commands using the Azure CLI.

9. Azure PowerShell – PowerShell with specific Azure modules installed to manage the environment.

10. Azure CLI – command line tool that uses the Azure API to run commands in Bash. Can be run on Windows, Mac, Linux as well as within the portal.

11. ARM Templates (Azure Resource Manager Templates) – written in JSON to execute code. Used to configure desired state.

12. Azure Functions – service that runs in stateless/serverless environment to perform some task. Can be written in several different languages. Functions are the smallest compute service in Azure. It is called by a web address.

13. Azure Logic Apps – low code/no code dev platform. Service that helps automate tasks and processes. Designed in a web-based designer and reacts to triggers

Describe General Security and Network Features

Security Features

Azure Security Center

1. Azure Security Center is a monitoring service that provides insight into the security posture of Azure resources as well as on-prem resources.

2. Security posture – cybersecurity policies and controls to facilitate how you can predict, prevent, and respond to security threats.

    - Integrated with Azure Advisor

3. Azure Advisor –analyzes your configurations and usage to offer personalized, actionable recommendations to help you optimize your Azure resources for reliability, security, operational excellence, performance, and cost.

4. Secure Score – this is an objective measurement of your security posture.

5. There are two tiers of the Azure Security Center:

    - Free – natively part of Azure and provides continuous assessment and security recommendations. Does not include Azure Defender.

    - Paid – Azure Defender is included. this includes monitoring of resources on-prem and in Azure, security alerts, and advanced capabilities, including:

        - just in time (JIT) VM access.
        - Adaptive network security – monitors traffic and access patterns and makes specific recommendations for hardening NSGs.

6. Azure Security Center can be integrated with Azure Logic Apps (via connectors) and allow workflow creation – create responses that occur for specific security alerts.

Azure Key Vault

7. Azure Key Vault – centralized location for storing resource and application secrets. Azure Key Vault is a managed service – PaaS.

8. Key Vault can manage the following:

    - Secrets (passwords, passphrases)
    - Certificates
    - encryption keys.

9. Benefits of Azure Key Vault:
    - Central repository
    - Secure
    - Natively integrated with Azure services
    - Logging and monitoring

Azure Dedicated Hosts

10. Azure can provide dedicated hardware for customers that only the customers can access. It is not shared hardware.

    This is most often used for compliance and regulatory reasons.
    Allows customer to decide on the number of processors, VM sizes, etc. within a host.

Azure Sentinel

11. Azure Sentinel is a Security Information and Event Management (SIEM) solution. It monitors for threats and events – from Azure resources, on-prem and other solutions (such as Carbon Black).

    (SIEM market leaders include Splunk and LogRhythm)

12. Collects data and analyzes using AI; can use built-in orchestration to respond to things.

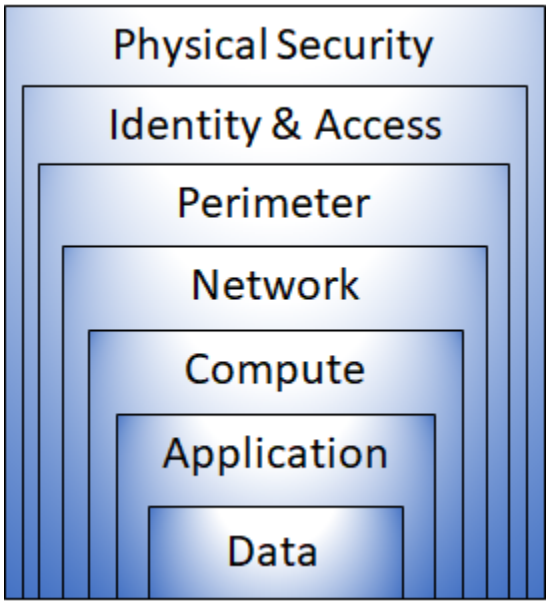
Azure Sentinel is a real-time threat analysis tool – it is very much geared toward security-minded skillsets.

Kusto Query Language (KQL) used within Sentinel for queries, etc.

Network Security

Defense in Depth: Azure

1. Defense in Depth – objective is to protect information and prevent unauthorized access. A defense-in-depth strategy uses a layers of defense mechanisms to slow the advance of an attack.



This image is used throughout Microsoft's documentation pertaining to security.

Data	Data encryption at rest
Application	SSL/TLS

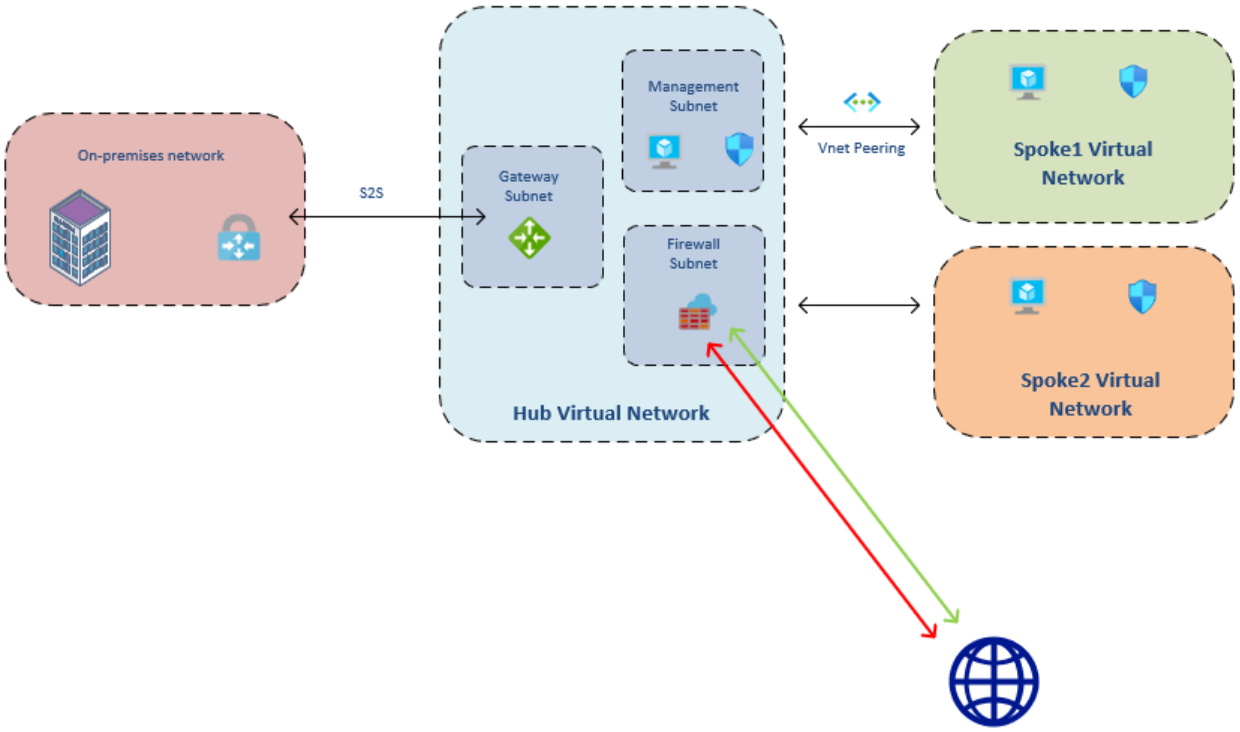
Compute	OS patching, disk encryption
Network	network security rules
Perimeter	DDoS protection, firewalls
Identity	AAD user auth
Physical	Datacenters – first line of defense.

Reference: https://docs.microsoft.com/en-us/learn/modules/azure-well-architected-security/2-defense-in-depth

2. Microsoft notes the principles used to define a security posture:
    - Confidentiality – principle of least privilege
    - Integrity – prevent unauthorizes changes to data, data validation. Digital signatures, hash algorithms.
    - Availability – services available to authorized users only.

Azure Firewall

3. Azure Firewall – monitors incoming/outgoing traffic and determines whether to allow or deny. Azure Firewall is a managed service that protects resources within Azure.



4. Azure Firewalls are stateful – meaning it considers all the traffic in a network connection. It looks inside the packets and can detect patterns.

   Stateless firewalls – look only at packet, where packet originated and its destination.

5. Azure Firewall is integrated with Azure Monitor for logging and analytics. Azure Firewall works at the layer 4 and 7 layers of the OSI model.

6. Benefits of Azure Firewall:

   - Native high availability
   - Scalability
   - Inbound/outbound filtering rules
   - NAT support
   - Azure Monitoring logging

7. Azure Firewall allows the following configurations:
   - Application rules
   - Network rules
   - NAT rules

Azure DDoS Protection

8. Distributed denial of service attacks – attacks that attempt to overwhelm and exhaust an application's resources, ultimately bringing the application down. Azure's DDoS service helps identify such behavior and protects against it.

9. As a cloud benefit is scalability and elasticity, DDoS attacks can potentially cause an application (website) to increase resource allocation to compensate for the new demand – causing unexpected expenses!

10. Azure DDoS has two tiers of service:

    - Basic – free with Azure subscription. Always-on traffic monitoring. Provides same level of defense as O365. Ensures that Azure's infrastructure is not compromised.
    - Standard – provides additional defenses tuned to Azure. Policies can be applied to specific pubic Ips associated in your network.

Network Security Groups (NSG)

11. Network Security Groups (NSG) are a layer 3 & 4 network security service that allows you to filter traffic to and from Azure resources within VNets.

12. Network Security Groups are composed of rules. The NSG rules contain the following elements:

    - Name
    - Priority – can be from 100 to 4096. Lower number equals a higher priority. Once a rule is triggered the processing stops.
    - Source or destination – IP address, IP range, service tag, application security group
    - Protocol – TCP, UDP, ICMP, any
    - Direction – inbound or outbound
    - Port Range – ex. 3389
    - Action: Allow, Deny

Describe Identity, Governance, Privacy & Compliance

Azure Identity Services

Authentication and Authorization

Authentication (AuthN) – proving who you are or what something is (can be for a person or service). You are who you say you are. Azure AD is used to authentication.

- Examples
  - User logging in with password
  - Face ID on iPhone
- Uses Open ID Connect (OIDC)

Authorization (AuthZ) – comes after authentication. Grants permissions to an authenticated user or resource. RBAC is used for authorization.

- Examples
  - User allowed to create virtual machine
  - User allowed access to server room
- Uses OAuth 2.0

1. Active Directory | Azure Active Directory | Azure Active Directory Domain Services

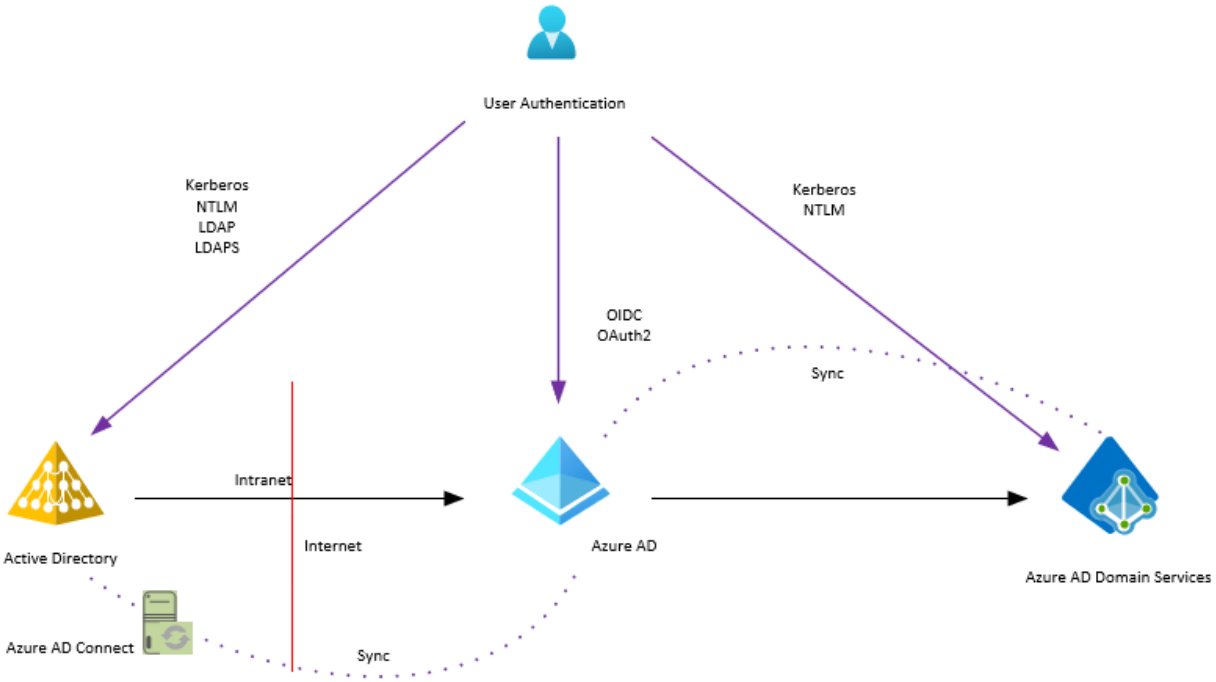
   - Active Directory
     - User/computer registration on-premises

- Identity and access management service
- GPO
- Kerberos and NTLM support
- Schema management – you can create custom objects
- Hierarchical

- Azure AD
  - User/computer registration
  - Flat structure

- Azure Active Directory Domain Services
  - PaaS service
  - NTLM and Kerberos support
  - A managed AD instance in Azure. It can be populated by on-prem AD.
  - Not quite as many features as on-prem Active Directory

2. Azure AD Connect – small utility installed on-prem that allows you to sync users, groups and computers to Azure AD.



3. Azure AD provides the following services:
    - Authentication
    - Single sign-on
    - Application management
    - Device management

4. Azure AD Single Sign-On – allows you to use one username and password for multiple applications.
    - A key feature of Azure AD
    - Can integrate with other third-party services

5. Multi-factor authentication – process of adding an additional form of identification in the sign-in process. This provides additional security during the authentication process. This can include:
    - Something you know
    - Something you have
    - Something you are

6. Azure AD MFA is a service. Azure Active Directory includes MFA – even the free version of Azure AD.
    - With advanced versions of Azure AD (P1 and P2 licenses), MFA can be tied to conditional access and privileged access.

   Comparison of MFA features available in Azure AD can be found here: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-multi-factor-authentication?azure-portal=true

7. Conditional Access – this is a feature in Azure AD that can add variables to the authentication process – variables such as location of sign-in attempt, device state of user, and who the user is. The variables are referred to as signals.

    - Common use – user can log into resources with no additional requirements at company headquarters. If same user attempts to access resources from coffee shop, MFA may be required during authentication.

Conditional Access is available with Azure AD P1 or P2 license.

Azure Governance Features

1. Cloud Adoption Framework – a set of tools and documentation that provide valuable information on the implementation and approach to cloud resources. The Cloud Adoption Framework consists of the following stages:

    - Define Strategy
    - Make a Plan
    - Ready your organization
    - Adopt the cloud
    - Govern/Manage cloud environment

2. Roles allow the grouping of permissions that can be assigned.
    - Users can be members of a role
    - Groups can be members of a role

3. Members of roles inherit all the permissions assigned to the role

4. Process of integrating roles:

    - Choose existing role or create new role
    - Assign members to the role
    - Configure the scope for the role (resource group, subscription, etc.)

5. Primary Built-in Roles:
    - Owner role – admin rights over all resources (within scope)
    - Contributor role – almost full permissions. This gives user full rights over all resources in scope, except the ability to grant access
    - Reader role – view all resources in scope

6. Resource Locks – another tool in Azure that can be used as a safeguard for the environment. There are two types of locks:
    - CanNotDelete – even if authorized (RBAC), the resource cannot be deleted unless the lock is removed.
    - ReadOnly - even if authorized (RBAC), the resource can be read, but it cannot be be deleted or changed unless the lock is removed.

7. Tags – a tool used to organize and categorize resources in Azure. Tags are a way to add metadata to your resource.

8. Tags can be used in many beneficial ways, including:
    - Resource management – searching for resources based on tag/metadata
    - Security - classifying resources that policies and permissions are applied to
    - Cost management – tags can be applied that indicate a specific program or department is responsible for the costs associated
    - Automation (shut down all servers with “DEV” tag at 5 PM)
    - Governance – specific resources that fall under certain requirements or guidelines

9. Tags can be managed via portal, PowerShell, CLI, ARM templates, policies

10. Tag structure example:
    - AppName
    - CostCenter
    - Owner
    - Environment
    - Backup

11. Azure Policy – a tool for management and organization within Azure. Used to control and audit resources.
    - Policies can be applied to management groups, subscriptions, or resource group.
    - Policies are inherited by all child objects of scope
        - You can have exclusions of subgroups

12. Azure Policy Process:
    - Create policy definition
    - Assign policy to resources
    - Review results

13. Azure Policy Initiatives - Groups of policies are known as initiatives. Designed to organized many pieces of a larger goal.

14. Azure Blueprints – this is a standardization feature that can be applied to resources in Azure. It allows you to apply structure to multiple subscriptions.

    Blueprints are guides and patterns for making things.

    Blueprints can be applied to 4 types of artifacts:
    - RBAC
    - Resource Group definitions
    - Azure policy
    - ARM templates

15. Blueprints can be applied to subscriptions or management groups.

16. Blueprints are similar to ARM templates.

Privacy and Compliance Resources

1. Azure has compliance offerings based on four categories:
    - Global
    - US Government
    - Industry
    - Regional

2. Microsoft Privacy Statement – explains what personal info Microsoft collects, how it is used, and for what purposes.

https://privacy.microsoft.com/en-US/privacystatement

3. Online Services Terms (OST) – Microsoft's legal agreement with its customers. This applies to services licenses through a subscription.

   https://www.microsoft.com/licensing/terms/product/ForallOnlineServices

4. Data Protection Addendum – further defines data processing, encryption, and security terms for online services.

   To find DPAm go to the following link and search for DPA:
   https://www.microsoftvolumelicensing.com/DocumentSearch.aspx

5. Trust Center – part of Microsoft Trusted Cloud Initiative and provides detailed information about security, privacy, compliance, policies.

   https://microsoft.com/trust-center

6. Azure compliance documentation – detailed documentation about legal and regulatory standards and compliance on Azure.

   https://docs.microsoft.com/en-us/azure/compliance/

7. Azure Government – separate instance of Azure that provides security and compliance needs of US agencies.
   - Meets IRS 1075 requirements
   - Meets CJIS requirements
   - Meets FedRAMP requirements

8. Azure China – separate instance of Azure located in China. It is an independently operated by 21Vianet, a Chinese company.

   - Only locally registered companies with less than 50 percent foreign investment can provide cloud services.
   - This is the first foreign public cloud service provider in China in compliance with government regulations.

Describe Azure Cost Management & SLA

Cost Management and Planning

1. Cloud Model – Pay only for what you use. This model has a lot of potential cost advantages, but you must be sure to understand the way costs are incurred to avoid any surprises.

2. Factors that affect costs in Azure include:
   Resource types – performance tiers, access tiers, etc.
   Usage Meters – tracks the usage of resources. CPU, PIP, etc.
   Services
   Locations
   Ingress/Egress traffic – egress (out of Azure) is where the charges need to closely monitored.

3. Location of resources impacts price. Microsoft has billing zones which are used for cost purposes. The prices in one zone will often vary from the prices in another zone.

4. Billing Zones:
   - Zone 1 – Australia Central, West Europe, Canada West, West/East US
   - Zone 2 – Japan West, Korea South,
   - Zone 3 – Brazil South, South Africa West

Microsoft Sites Useful for Cost Estimates and Budget

5. Microsoft provides a calculator to assist in the budgeting and planning process.

   https://azure.microsoft.com/pricing/calculator

6. Microsoft provides a Total Cost of Ownership Calculator which helps estimate costs over time and assists in comparing costs of Azure to on-prem resources.

   https://azure.microsoft.com/en-us/pricing/tco/calculator/

This tool allows you to input the resources currently in your on-prem datacenters and estimate costs.

The TCO Calculator includes costs for electricity, power, and human resources.

Per Microsoft, the TCO calculator provides the guidance through three broad steps:

Define Workloads – on-prem servers, etc.

Adjust Assumptions

View Report

7. TCO cost categories:
   - Servers
   - Databases
   - Storage
   - Networking

Purchasing Azure Services

8. There are different kinds of methods to purchase Azure agreements:

   Free trials
   Pay-as-You-Go
   Member Offers
   Visual Studio
   MPN

9. There are three primary ways to purchase Azure services:
   - Enterprise Agreement
   - Web Direct (via portal, credit card)
   - Cloud Solution Provider (SHI)

   The different methods have different billing rates. Promotions and discounts can be applied.

10. Azure Advisor – tool that helps identify underutilized or underused resources in Azure.

11. Azure Reservations (AR) – discounted pricing based on longer-term commitment. You can prepay for one or three years to reduce the price.

    Azure Cost Management + Billing includes the following features:

    - Reporting
    - Budgets
    - Alerting
    - Recommendations

Cost Management Best Practices

12. Cost Management tools and practices:

    - Use Azure Monitor
    - User spending limits
    - Use Azure reservations where appropriate
    - Locations matter – this will not save a lot of money, but it could be of value over time.
    - User Azure Cost Management and Billing
    - Use Tags to identify costs and owners
    - Keep a clean house – delete unused resources.
    - Deallocate VMs when able.
    - Azure Hybrid Benefit

13. Tags – can also be used to add metadata that can be used to identify and control costs.

14. Azure Cost Management – service within portal that shows spending, budgets and allows the management of cost control.

SLA's and Service Lifecycles

1. Service Level Agreement (SLA) – formal agreement between company and customer setting expectations of performance that the company commits to upholding.

2. Azure services have their own SLA.

3. SLA's contain the following features:

   - Introduction – includes expectations, scope of SLA
   - General Terms – includes common terms used in the SLA, how to submit claims, receive credit, and limitations
   - SLA Details – defines the specific guarantees of the service. Many SLA's focus on uptime and latency commitments.

SLA percentage	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9	10.1 minutes	43.2 minutes	8.76 hours
99.95	5 minutes	21.6 minutes	4.38 hours
99.99	1.01 minutes	4.32 minutes	52.56 minutes
99.999	6 seconds	25.9 seconds	5.26 minutes

Source: https://docs.microsoft.com/en-us/learn/modules/choose-azure-services-sla-lifecycle/2-what-are-service-level-agreements

Check for service outages : https://status.azure.com/status

4. If Azure SLAs are not met, you can be eligible for service credits – Microsoft applies a credit to your account based on the specifics of the missed SLA.

5. Workload – a solution consisting of a set of services. An example workload may include a load balancer, two virtual machines and a database.

6. Composite SLA – combine the individual SLAs of each component of a solution to determine the overall (composite) SLA.

VM SLA	99.99
SQL DB SLA	99.99
Load Balancer	99.99

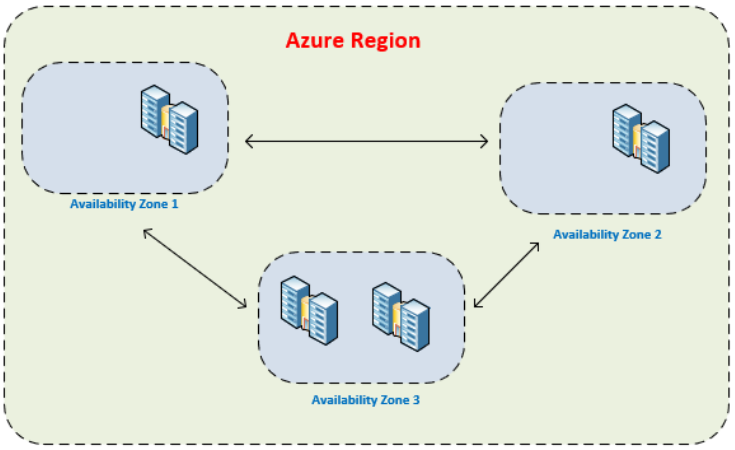
To find composite SLA, multiple all the SLA's together.

Availability Zones –physical location within a region. Each zone is made up for one or more data centers. These protect your resource from data center failures.

Each data center in an availability zone has its own cooling, power, networking.

There are at least three zones in each (enabled) region.

You can increase your SLA by making use of Availability Zones. When you deploy two or more VMs in two or more Availability Zones, you can reach 99.99 % SLA.



Service Lifecycles

1. Service Lifecycle – the maturity and release of Azure services follows defined stages.

    - Each service begins in development phase – gather requirements, build service
    - Pubic Preview – limited release, feedback provided to Microsoft
    - General Availability (GA) – service is ready for all users, production-ready

2. To find preview services, search in Azure portal for "preview"

    You can also check here: https://preview.portal.azure.com/

3. Preview services have limited support and warranty – typically not to be used in production.

4. To find latest updates from Azure, keep an eye on this site:

   https://azure.microsoft.com/en-us/updates/