AZ-103: Exam Notes

Friday, 10 May 2019 5:13 pm

Important URLS:

Exam Info - https://www.microsoft.com/en-us/learning/exam-az-103.aspx
Exam breakdown - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VwUF
Udemy Course - https://www.udemy.com/course/az-100-skylines-academy/
Labs - https://www.microsoft.com/handsonlabs/selfpacedlabs ; https://handsonlabs.microsoft.com/handsonlabs/SelfPacedLabs#page=1&sort=Most%20Popular ; https://github.com/MicrosoftLearning/AZ-103-MicrosoftAzureAdministrator

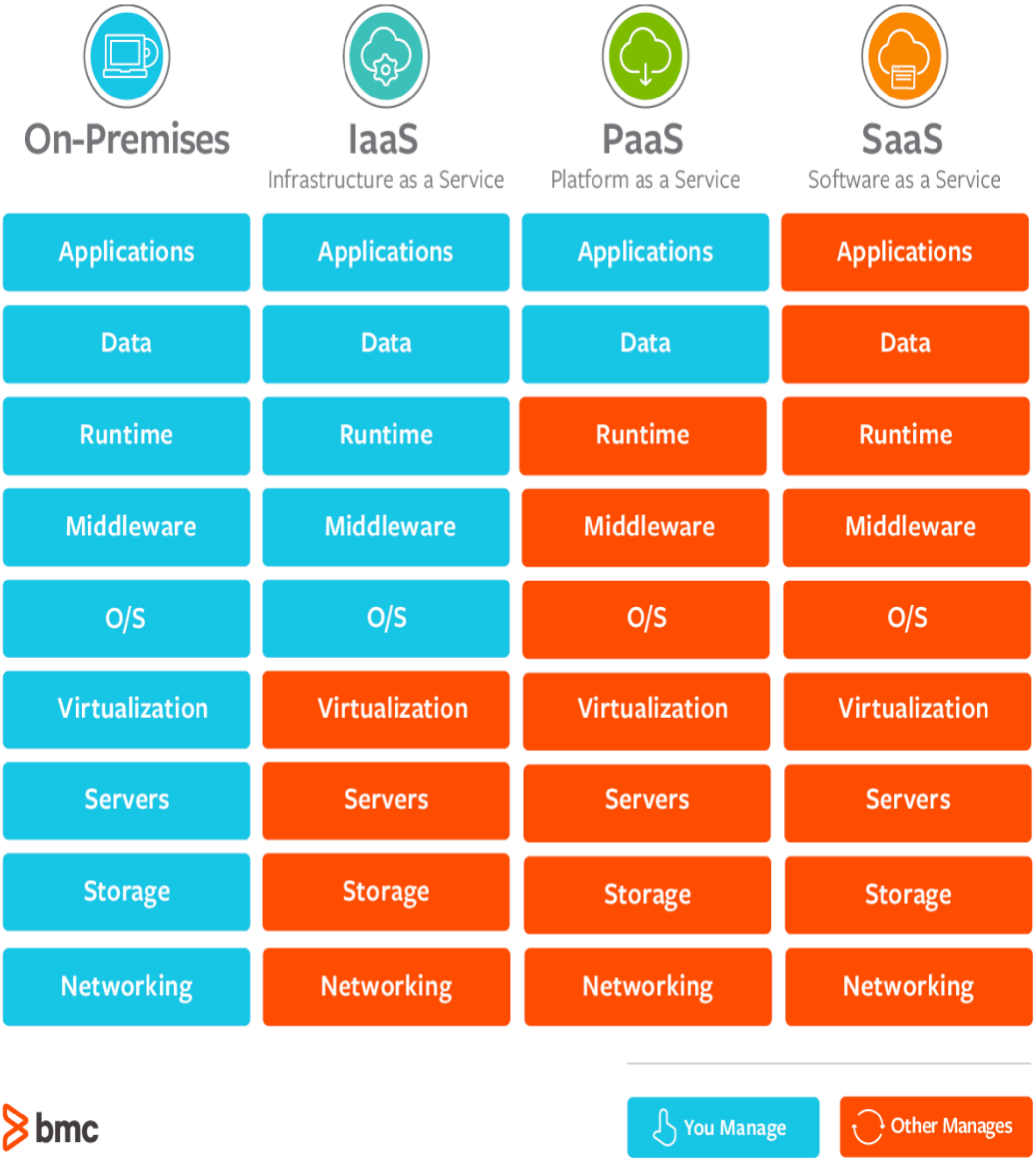
Different types of Cloud Distributions:

- **Infrastructure-as-a-Service (IaaS)**
  - → Third-party providing tools for users to create VMs, storage, firewalls, load balancers, etc.
  - → Similar to PaaS but more customization to the needs of the solution; which means more effort for the users.
  - → Examples: AWS, Azure

- **Platform-as-a-Service (PaaS)**
  - → Third-party providing a framework to users to develop applications and software. All servers, storage and networking are managed by third-party
  - → User does not interact with OS or middleware configuration
  - → Examples: Windows Azure Applications

- **Software-as-a-Service (SaaS)**
  - → Delivering applications to users; usually just in a browser with no need for installations
  - → Eliminates the need to have IT support staff and frees up time for technical staff to focus on more important matters
  - → Ideal to use when you are a small company who just need non-specialised software

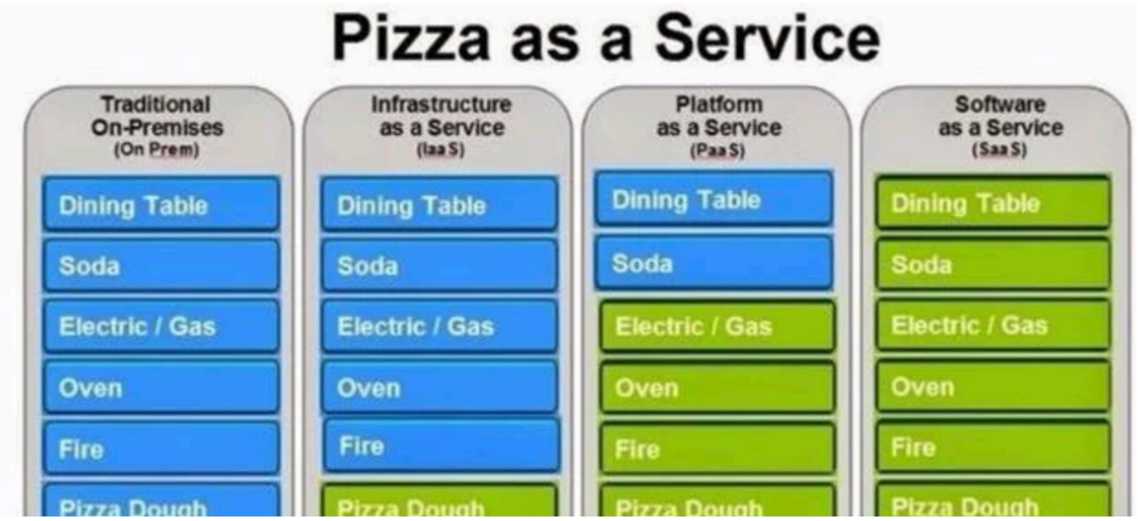
→ Examples: Google Apps, Microsoft Office 365



On-Premises	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
🟦 Applications	🟦 Applications	🟦 Applications	🟧 Applications
🟦 Data	🟦 Data	🟦 Data	🟧 Data
🟦 Runtime	🟦 Runtime	🟧 Runtime	🟧 Runtime
🟦 Middleware	🟦 Middleware	🟧 Middleware	🟧 Middleware
🟦 O/S	🟦 O/S	🟧 O/S	🟧 O/S
🟦 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟦 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟦 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟦 Networking	🟧 Networking	🟧 Networking	🟧 Networking

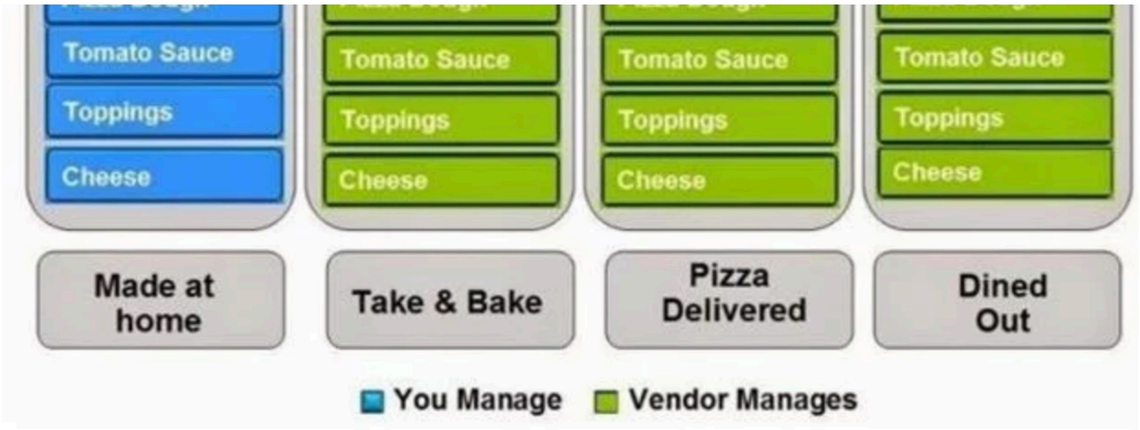
🟦 You Manage

🟧 Other Manages



Pizza as a Service

Traditional On-Premises (On Prem)	Infrastructure as a Service (laa S)	Platform as a Service (Paa S)	Software as a Service (Saa S)
🟦 Dining Table	🟦 Dining Table	🟦 Dining Table	🟩 Dining Table
🟦 Soda	🟦 Soda	🟦 Soda	🟩 Soda
🟦 Electric / Gas	🟦 Electric / Gas	🟩 Electric / Gas	🟩 Electric / Gas
🟦 Oven	🟦 Oven	🟩 Oven	🟩 Oven
🟦 Fire	🟦 Fire	🟩 Fire	🟩 Fire
🟦 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough



Cloud deployment models:

- Public
  - All resources are managed and owned by Cloud provider (Azure). Cheap and easy to manage.
  - Shared hardware with other apps
- Private
  - Azure Stack
  - Hardware used by one business
  - Hosted in a private datacentre. Needed by some organisations for security reasons
- Hybrid
  - Migration tactic for testing and easier migration process
  - Can be used for cloud bursting - once private stack has hit a peak, only use public stack then.
  - Some businesses have regulations which would make hybrid cloud the best option

<u>Manage Azure subscriptions and resources (15-20%):</u>

Monitoring:

- Monitor and Visualize Metrics
  - Numerical values to help you understand resource health, operation, performance
- Query and Analyse Logs
  - Activity, diagnostic logs.
  - Alert logic/queries to render graphs and analytics
- Setup and Alert Actions
  - Triggers under certain conditions to perform autonomous tasks

Resource Groups (RCs):

- Grouping resources based on life cycle, domains, geography; so you can delete them together if needed.
- Resource locks to limit a users ability to update or delete resources
- Azure Policies are implemented to enforce governance/business rules to ensure that user don't perform any actions that are not beneficial or wanted by the owner.
    - For example, only create instances in specific regions
- Resources from differing RCs can still interact/communicate with each other

Implement and manage storage (15-20%):

Create and configure storage accounts:

Choosing between Blobs, Files and Disks:

- Disks: for specific VMs
- Files: access files across multiple machines
- Blobs: Access app data from anywhere. Large amount of objects to store images, videos, etc.

Block Blobs:

- Text or binary files
- A single blob can contain up to 50,000 blocks of up to 100MB each which is a total size of 4.75TB

Page Blobs:

- Efficient for read/write
- Used by Azure VMs
- Up to 8TB in size

Storage Tiers:

1. Hot
    a. High storage cost
    b. Low access cost
2. Cold
    a. Low storage cost
    b. High access cost
    c. Intended for data to be cool for ~30days
3. Archive
    a. Lowest storage

   a. Lowest storage
   b. Highest access
   c. Archive storage is offline and cannot be read

Replication:

- Locally-redundant storage (LRS)
  - Replicated in single storage unit
  - Cheapest option
  - Data will be unavailable if datacentre goes down
- Zone-redundant storage (ZRS):
  - Replicated across 3 availability zones/datacentres within one region
  - Data is unavailable if whole zone goes down (ie. Australia East)
- Geo-redundant storage (GRS):
  - Replicated across to another region (ie. Australia East -> Australia Central)
  - Read-access only after failover has occurred
- Read-access GRS (RA-GRS):
  - Same as GRS except you can read data at any time

Managing access - Container Permissions:

- Shared Access Signature (SAS)
  - A query string added on a URL of a storage resource to inform Azure on what access should be granted
  - These strings use hash-based encryption
  - Similar to resource groups, policies can be implemented to restrict access to what is desired
  - Account SAS: Granted at the account level
  - Service SAS: granted at service level

Custom Domain Mapping:

1. Your Domain
   a. Point CNAME record mydomain.com to blob-domain.net
   b. Incurs downtime while Azure verifies domain
2. 'Asverify' Domain
   a. Verify.mydomain.com to asverify.blob-domain.net
   b. After this step, point CNAME record to blob-domain.net
   c. 'Use Indirect CNAME Validation'
   d. No downtime

Storage Diagnostics:

Storage Diagnostics:

- Logs can be configured to be produced upon any CRUD operation that occurs to a storage account
- Alerts can be configured to triggered under certain conditions affecting a storage account (ie. Send email after a high number of requests)

Azure storage has the following security features:

- Encryption at rest
- Encryption in transit
- CORS support (Cross-Origin Resource Sharing)
    - Only cross-loads resources from trusted domains/servers
- Role-based Access Control (RBAC)
    - Can assign roles to subscriptions, resource groups or individual containers
- Audit access
    - Logs every access and interaction on storage aswell as providing analytics

Import and export data to Azure:

- Data migration to Cloud
    - Online upload
    - Data Box (Azure gives you a HDD to upload to -> mail back to Azure. Up to 40TB)
- Content distribution
- Backup
- Data recovery

CDN: utilizes a cache server nearby to you to improve latency with server; no matter where the original server is located.

CDN options:

- Verizon: specializes in URL redirect and mobile device rules
- Akamai: specializes in media streaming capabilities

Implement Azure backup:

Business continuity strategies:

- High availability: run another instance in case of failure
- Disaster recovery: run apps in secondary datacentre if failure occurs. No single point of failure.

- No single point of failure.
- Backup/restore data

Azure MARS [Microsoft Azure Recovery Services] Backup:
- Backup on-premises files to vault
- Backup specific files in VM to vault
- Backup non-azure servers
- Can backup 3 times a day; better RPO
- Only supports Windows OS
- Not application aware. Only file/disk snapshot.

Deploy and manage virtual machines (VMs) (15-20%):

Create and configure a VM for Windows and Linux:

VM Types:

Type	Purpose
A1 - Basic	Basic VM. For testing/development.
A2 - Standard	General-purpose VMs.
B- Burstable	Burstable instances the can use full capacity of CPU when needed.
D - General Purpose	Built for enterprise apps.
E - Memory Optimized	High memory-to-CPU ratio.
F - CPU Optimised	High CPU-to-memory ratio.
G - Godzilla	Very large instance instances ideal for large databases and big data.
H - High performance compute	High-end computational needs such as molecular modelling or other scientific applications.
L - Storage optimized	High disk throughput and IO.
M - Large Memory	Large-scale memory option that allows for 3.5TB RAM
N - GPU	GPU enabled instances

N - GPU enabled	GPU-enabled instances
SAP HANA	Specialized instances purposely built and certified for tunning SAP HANA

VM Specializations:

S: Storage premium options available
M: Memory premium options available
R: Remote direct memory access (RDMA)

Azure Compute Units (ACUs):

- Microsoft created performance benchmark/measurements
- A VM with 200 ACU is twice as powerful as a VM with 100ACU

Manage Azure VM Storage and Networking:

VM Availability Sets:

- Running a group of VMs across multiple, isolated physical servers
  - Ensures uptime during a hardware or software failure occurs in a server
- Essential for running a reliable service that uses numerous VMs

VM Scale Sets:

- Autoscaling groups
- Provides redundancy, improved performance and consistency
- Max. 1000 VMs in a set
- One size/type VM for the entire scale set

Implement and Manage Virtual Networking (30-35%):

Best to do hands-on labs for this section

IP Addressing:

- Dynamic Host Configuration Protocol (DHCP) DHCP based addresses
- IP Address are not allocated until object is created
- Static and Dynamic IP options available

Connectivity between Virtual Networks:

- Site-to-Site (S2S)

- Site-to-Site (S2S)
    - S2S VPN is a connection over IPsec/IKE
    - Connecting two offices together
- Point-to-Site (P2S)
    - Connecting one user to a VNET (ie. OpenVPN)
- VNET Peering
    - Configuring different VNETs to be able to communicate with each others resources
- ExpressRoute
    - Private connection directly to Azure Datacentre
    - High speed/cost

Configure Name Resolution:

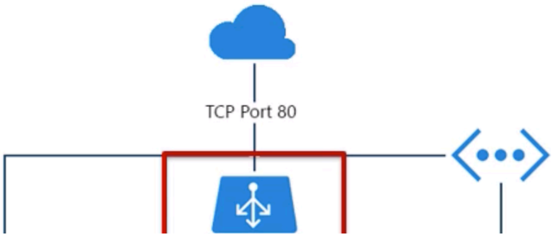
- Customer Provided DNS or Azure Provided DNS
- VM specific configuration

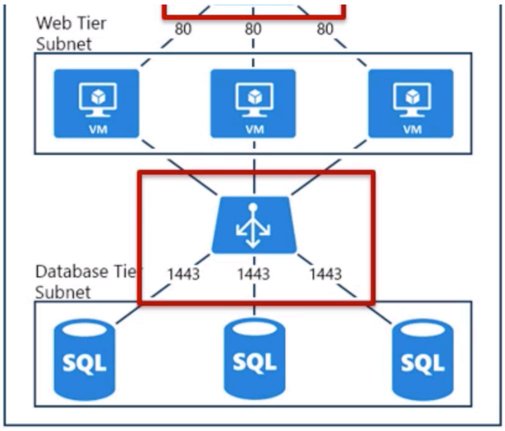
Create and Configure a Network Security Group (NSG):

- NSG:
    - Network filter - Security groups in AWS
    - Inbound/Outbound rules
    - Restricted to subnet or NIC (Network Interface Card)
- Rules:
    - Enforced on priority (100 - 4096); lowest number first
    - Tags - Azure provides default tags to be used:
        - Virtual Network
        - Azure Load Balancer
        - Internet

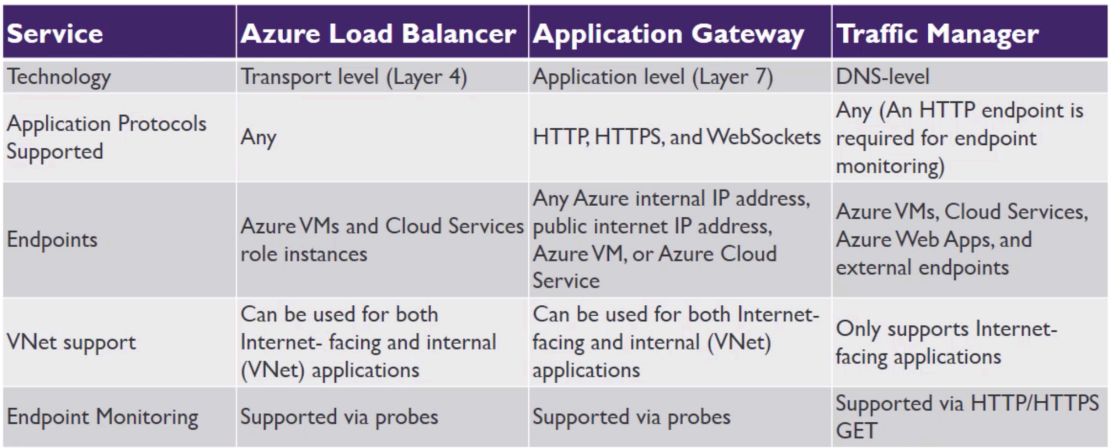
Load Balancing:

- Azure Load Balancer
    - Transport Layer [4]
    - Service Monitoring
    - Automated reconfiguration
    - Hash Based Distribution
    - Internal and Public
        - Better for Internal or UAT. Public is best for App Gateway





- Application Gateway
  - Application Layer [7]
  - Cookie based session affinity
  - SSL Offloading
  - End-to-end SSL
  - Web Application Firewalls (WAFs)
  - URL Based Content Routing
  - Requires its own subnet



Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport level (Layer 4)	Application level (Layer 7)	DNS-level
Application Protocols Supported	Any	HTTP, HTTPS, and WebSockets	Any (An HTTP endpoint is required for endpoint monitoring)
Endpoints	Azure VMs and Cloud Services role instances	Any Azure internal IP address, public internet IP address, Azure VM, or Azure Cloud Service	Azure VMs, Cloud Services, Azure Web Apps, and external endpoints
VNet support	Can be used for both Internet- facing and internal (VNet) applications	Can be used for both Internet-facing and internal (VNet) applications	Only supports Internet-facing applications
Endpoint Monitoring	Supported via probes	Supported via probes	Supported via HTTP/HTTPS GET

Azure Monitor:

- Collects, analyses and stores data based on the performance and availability of your Azure stack
  - Logs
  - Analytics/Metrics
- Able to configure Alerts
- Application Insights provide real-time data and visual representations of your application; as well as anomalies

Manage Identities (15-20%):

Azure Active Directory (AD):

- Enterprise Identity Solution - Single identity for users and keep them

- Enterprise Identity Solution - Single identity for users and keep them in sync across the enterprise
    - Create users and groups with varying levels of user permissions
- Single sign-on - SSO access to apps and infrastructure services
- Multifactor Authentication (MFA) - enhance security and authentication services
- Self service - Empower users to request passwords resets themselves, as well as request access to specific apps and services if needed
    - Password resets need to be enabled and configured based on Groups, methods available and number of methods required (1 or 2) to authenticate user.

Azure AD Connect:

- Used to link an on-premises AD and Cloud Azure AD. This dual component of AD is called Hybrid Identity.
- There are three methods of authentication:
    1. Password hash synchronization
        i. Syncs a hash of a users password on both ADs
        ii. Reduces the number of passwords a user has to 1
        iii. Passwords are stored in <u>TWO</u> places.
        iv. Can provide Seamless Single Sign-On (SSSO)
            1) Automatically logs on users to Azure AD if they are using a corporate device on their corporate network
    2. Pass-through authentication
        i. Requests for Azure AD logins are 'passed-through' to on-premises
        ii. Passwords are <u>ONLY</u> stored on-premises
        iii. Can provide Seamless Single Sign-On (SSSO)
    3. Federation Services (AD FS)
        i. Utilizes on-premises Federation services and infrastructure
        ii. Not covered on exam

Conditional Access:

- Requires certain conditions to be met before it allows an AD login. Broken down into Controls and Conditions.
- Controls:
    - User and Role
    - Trusted/complaint devices
    - Location (IP authentication)
    - Authentication method
- Conditions:

- Conditions:
    - Allow/block access
    - Limited access
    - Require MFA
    - Force password reset

- Synchronization services
    - Password hash sync - see above
    - Password writeback - once a password is updated in one location (ie. On-premises), it is also updated on the other (ie. Azure AD)
    - Device writeback - provides another method of authentication by making a list of approved devices to use for AD

Azure AD Business-to-Consumer (B2C):

- Third party handles authentication. Enabled for:
    - Social accounts (ie. Facebook, twitter)
    - Enterprise accounts (ie. Microsoft)
- Can also make local accounts if the user doesn't want to use or have a third-party account
- As the name suggests, it is integrated to benefit the consumer

Azure AD Business-to-Business (B2B):

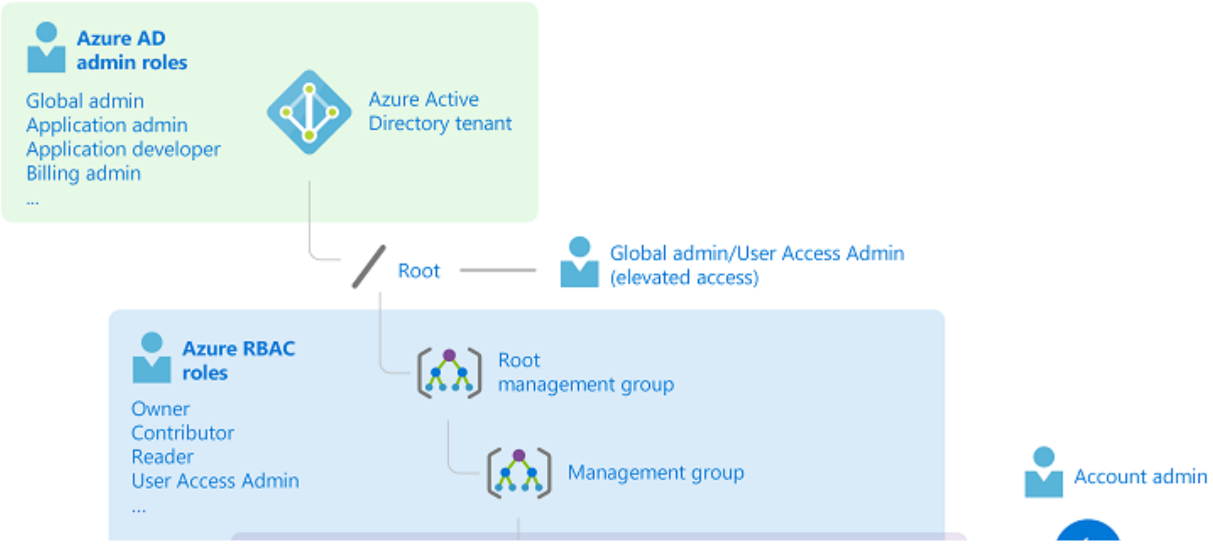
- Integrated to benefit the business; allows for collaboration from users outside of the AD
- Invite other ADs or send invites to individual emails.

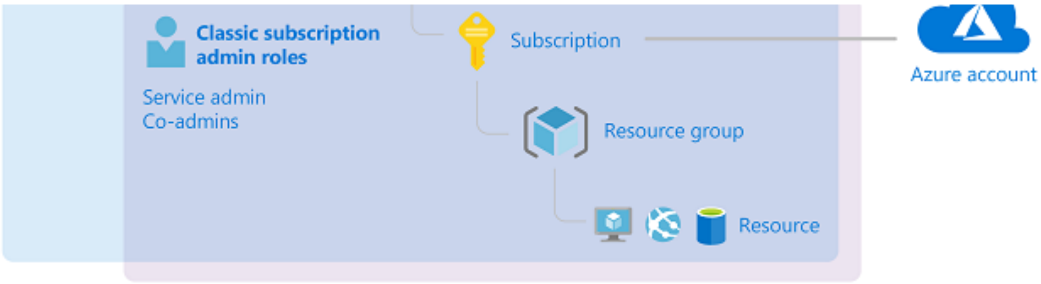
More info about AD and Hybrid Identities - https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity

User Groups and Roles:

- Azure has 3 types of Access Control (AC) mechanisms
- Classic:
    - Account Administrator:
        - 1 per account
        - Manages subscriptions, billing
        - Assigns Service Admins
    - Service Administrator:
        - 1 per subscription
        - Manages services in Portal
        - Assigns users to Co-Admin role

        - Assigns users to Co-Admin role
    - Co-Admin:
        - Same privileges as Service Admin minus any control over subscription
        - Can also assign co-admin role
- Azure Role-Based AC (RBAC):
    - Managed in Access Control (IAM)
    - There are over 70 built in roles - main roles listed below. Note: They are `suffix's`; for example, you could have a Virtual Machine Contributor, Network Contributor etc
    - Owner:
        - Full access to all
        - Delegate access to others
    - Contributor
        - Create and manage resources
        - Cannot grant access
    - Reader
        - View Azure resources
    - User Access Administrator
        - Manage User access
- Azure AD:
    - Basically only has control over AAD related services; no baring on other cloud services
    - Global Admin
        - Manage access to all AAD
        - Reset passwords for users or admins
    - User Admin
    - Billing Admin





More info on AC: https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?context=azure/active-directory/users-groups-roles/context/ugr-context