Azure migrate vs Site recovery

Azure migrate	Site recovery
Site recommendations	Disaster recovery
Monthly cost estimate	Replication
VMware VM’s with vCenter Server	Failover
Agentless	VMWare VM’s
	HyperV VM’s
	Physical servers
	Agent-based

Disk limits

Standard HDD	Standard SSD	Premium SSD	Ultra SSD
500 MB/s	750	900	2.000
2000 IOPS	6.000	20.000	160.000
32 TB	32	32	64

Web jobs

Continuous	Triggered
Starts immediately (loop)	Starts manual / on schedule
Runs on all instances	Single load balanced instance
Remote debugging	NO remote debugging

VM migration limits

	Limit
OS Disk	2 TB
Data disk	4 TB (storage), 8TB (managed disk)
OS Disk count	1
Bitlocker	Must be off

VPN Gateway SLA

Type	Bandwith	S2S tunnels	P2S tunnels
Basic for VPN or ExpressRoute	99.9%	10	128
> Basic for VPN or ExpressRoute	99.95%	30	500

VPN Gateway SKU’s (AZ = Availability Zone)

Type	Bandwith	S2S tunnels	P2S tunnels
Basic	100 Mbps	10	128
VpnGw1	650 Mbps	30	250
VpnGw2	1 Gbps	30	500
VpnGw3	1.25 Gbps	30	1000
VpnGw4	5 Gbps	30	5000
VpnGw5	10 Gbps	30	10000
VpnGw1AZ	650	30	128
VpnGw2AZ	1 Gbps	30	128
VpnGw3AZ	1.25 Gbps	30	128

App plans

Free (6)	Shared (2)	Basic (6)	Standard (5)	Consumption (6)
- Security scan - Auth - Web sockets - Contin. depl. - Remote debug - Session (AFF cookie)	- Custom domains - Load balancer	- 64 bit - Multi instance - SSL - SLA 99.95 - Always on - Remote profiling	- Autoscale - Local cache - Backup/rest. - Depl. slots - Traffic manager	NOT: - Sessions - Web sockets - Remote profiling - SLA - Security scan - **VNET**

Storage types

	General purpose v2	General purpose v1	Blob	Block blob	File
Services	Blob, Queue, File, Tables, Disk	Blob, Queue, File, Tables, Disk	Block / append blob	Block / append blob	File
Access tiers	Hot, cool, archive		Hot, cool, archive		
Replication	LRS, GRS, RA-GRS, **ZRS**	LRS, GRS, RA-GRS	LRS, GRS, RA-GRS	LRS	LRS
Performance Tiers	Standard, (premium)	Standard, (premium)	Standard	Premium	Premium

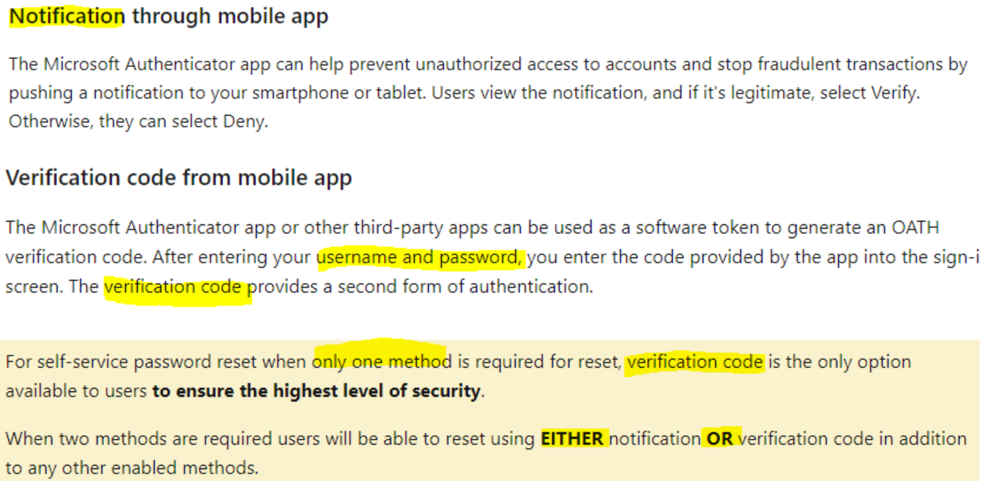
Storage replication types

Type	Sync / async	Count
LRS	Sync	3 in same data center
ZRS	Sync	3 AZ's in same region
GRS / RA-GRS	Sync LRS first, **async** to other region	6

Load balancer vs Traffic manager

Load balancer	Traffic manager
Same region VM's	Across regions
TCP/UDP level -> private (public possible)	DNS level -> public
Hash algorithm	Failover, performance

MFA authenticator app



Notification through mobile app

The Microsoft Authenticator app can help prevent unauthorized access to accounts and stop fraudulent transactions by pushing a notification to your smartphone or tablet. Users view the notification, and if it's legitimate, select Verify. Otherwise, they can select Deny.

Verification code from mobile app

The Microsoft Authenticator app or other third-party apps can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the app into the sign-i screen. The verification code provides a second form of authentication.

For self-service password reset when only one method is required for reset, verification code is the only option available to users **to ensure the highest level of security**.

When two methods are required users will be able to reset using **EITHER** notification **OR** verification code in addition to any other enabled methods.

Load balancer family

Load balancer	**Description**
Public load balancer	OSI layer 4 Internet facing
Internal load balancer	OSI layer 4 Only within a VNet Ideal for n-tier app services
Application gateway	OSI layer 7 SSL offload WAF
Traffic manager	OSI layer 7 DNS level Multiple routing methods (priority, performance, …)

Load balancer SKU's

Basic	**Standard**
Probe types: TCP, HTTP	Probe types: TCP, HTTP, HTTPS
Backend pool: single Availability or scale set	Backend pool: any blend of VM's or sets
<= 100 backend instances	<= 1000 backend instances
Frontend NOT zone redundant	Frontend zone redundant
Multiple inbound frontend configs	Multiple inbound and outbound frontend configs
NSG optional	NSG required
60-90 secs for management operations	< 30 secs for management operations
No SLA	SLA 99.99%

Difference between public / private (internal) load balancer

- PUBLIC: load balance outbound connections for VM's, by mapping private ip to a public ip
- INTERNAL: load balance traffic inside a VNET, no public ip needed

Application gateway properties

- Is a WEB TRAFFIC load balancer
- For HTTP(s) workloads
- HTTP -> HTTPS redirection
- OSI layer 7
- Url-based routing (/images, /video)
- Multi-site hosting
- WAF (OWASP core rule sets 3.0 / 2.2.9)
- SKU's: Standard (for gateway), WAF (for firewall) (v2 for more options)

Application gateway: supported in v1 and v2 SKU's

- URL-based routing
- Multi site hosting
- Traffic redirect
- WAF
- SSL
- Sessions
- Custom error pages
- Websockets
- HTTP/2
- Connection draining

Application gateway: supported in v2 SKU only

- Autoscale
- Zone redundancy
- Static VIP
- AKS controller
- Key vault integration
- Rewrite HTTP(s) headers
- Custom WAF rules

Traffic manager routing methods

Method	Description
Priority	Route to primary, fallback to backup
Weighted	Distribute based on defined or even weights
Performance	Based on smallest latency (closest endpoint)
Geographic	Users are directed to specific endpoints based on which geographic location their DNS query originates from.
Multivalue	Can only have IPv4/IPv6 addresses as endpoints
Subnet	Map sets of end-user IP address ranges to a specific endpoint

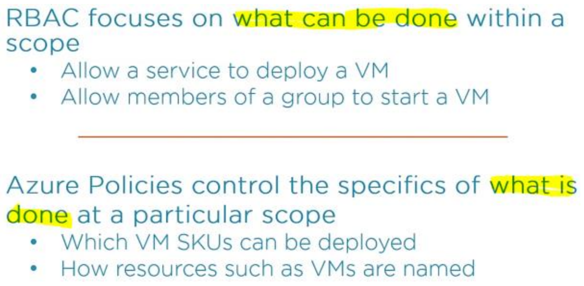
AD authentication methods

Method	SSPR	MFA
AD password	Yes	Yes
MS Authenticator app	Yes	Yes
SMS	Yes	Yes
Voice call	Yes	Yes
OAuth	Yes	Yes (preview)
Email	Yes	
Security questions	Yes	
App passwords		In some cases

Types of on-site/Azure hybrid networks

Type	Description
1a: S2S (site to site)	- Internet standard **VPN** tunnel - IPSEC/IKEv2 - Over the internet - On prem GATEWAY 2 Azure VPN GATEWAY - Bi-directional - Many-to-may - Stays online if on-prem workstation is closed
1b: P2S (point to site)	- Similar to S2S (can be done over the same VPN GATEWAY) - SSTP **VPN** tunnel - One Azure-to-many clients - Connection lost when client closes - Used for remote working
2: ExpressRoute	- High-speed connection to Azure - Maximizes security and speed - SLA 99.95% - **MPLS WAN** (**not a VPN**) - Port speeds 50 Mpbs to 10 Gbps - Uses EXPRESSROUTE GATEWAY - Hub & spoke (peer Hub VNET with other VNETS) - Bypasses internet - Connect to Office 365 and MS Cloud services - MONTOR with Network Performance Monitor (NPM)

RBAC vs Azure Policies



RBAC focuses on what can be done within a scope

- Allow a service to deploy a VM
- Allow members of a group to start a VM

Azure Policies control the specifics of what is done at a particular scope

- Which VM SKUs can be deployed
- How resources such as VMs are named

Types of RBAC roles

- Owner
    - Can manage everything including access to resources
- Contributor
    - Can manage everything except access to resources
- Reader
    - Has read-only access to everything
- User Access Administrator
    - Can manage user access to resources

RBAC Limits

- Max. 2000 role assignments per SUBSCRIPTION
- Max. 2000 custom roles per TENANT (Azure AD instance)

Custom role properties

- Can be shared across subscriptions
- Orange icon in Azure portal (blue = built-in)
- Best way to create: base on existing role, modify needed permissions
- **CAN ONLY BE CREATED BY**: Owner and User access administrator

Azure migrate server assessment types

Type	**Rec VM SIZE based on**	**Rec DISK TYPE based on**
Performance based	Recorded CPU / RAM data	Recorded IOPS / throughput data
As **on-permises**	Local VM size	Local storage type

VNET peering types

Type	**Description**
Normal	Connect 2 VNETs in the SAME REGION over the Azure backbone
Global	Connect VNETs across regions over the Microsoft backbone

What is a private DNS zone?

- Resolves domain names IN or BETWEEN virtual networks

Scenario's only supported by Azure Activity Directory Premium P2?

- Conditional access policies
- Privileged Identity Management (PIM)
- Access reviews
- Risk events investigation
- Vulner. / risky accounts detection

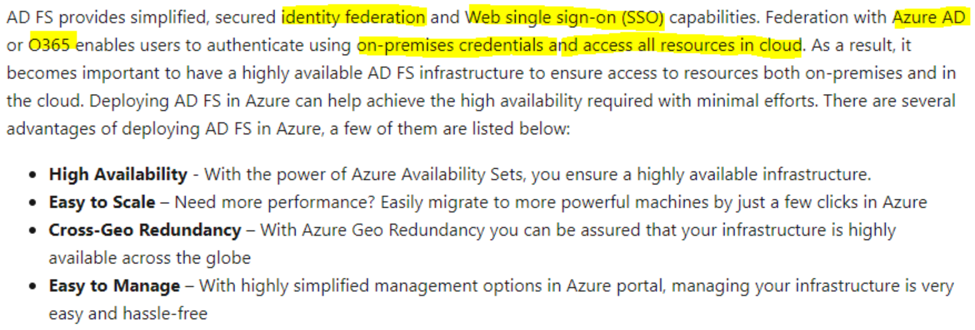
Scenario's supported by Azure Activity Directory Free?

- MFA
- Single sign-on
- Federated authentication (ADFS)
- Device registration

What is a split-horizon DNS zone?

- A public and private DNS zone with the same name, to allow access over the internet and also do DNS resolving inside virtual network

AD FS: Active Directory Federation Services



AD FS provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. Federation with Azure AD or O365 enables users to authenticate using on-premises credentials and access all resources in cloud. As a result, it becomes important to have a highly available AD FS infrastructure to ensure access to resources both on-premises and in the cloud. Deploying AD FS in Azure can help achieve the high availability required with minimal efforts. There are several advantages of deploying AD FS in Azure, a few of them are listed below:

- **High Availability** - With the power of Azure Availability Sets, you ensure a highly available infrastructure.
- **Easy to Scale** – Need more performance? Easily migrate to more powerful machines by just a few clicks in Azure
- **Cross-Geo Redundancy** – With Azure Geo Redundancy you can be assured that your infrastructure is highly available across the globe
- **Easy to Manage** – With highly simplified management options in Azure portal, managing your infrastructure is very easy and hassle-free

Important Azure built-in roles

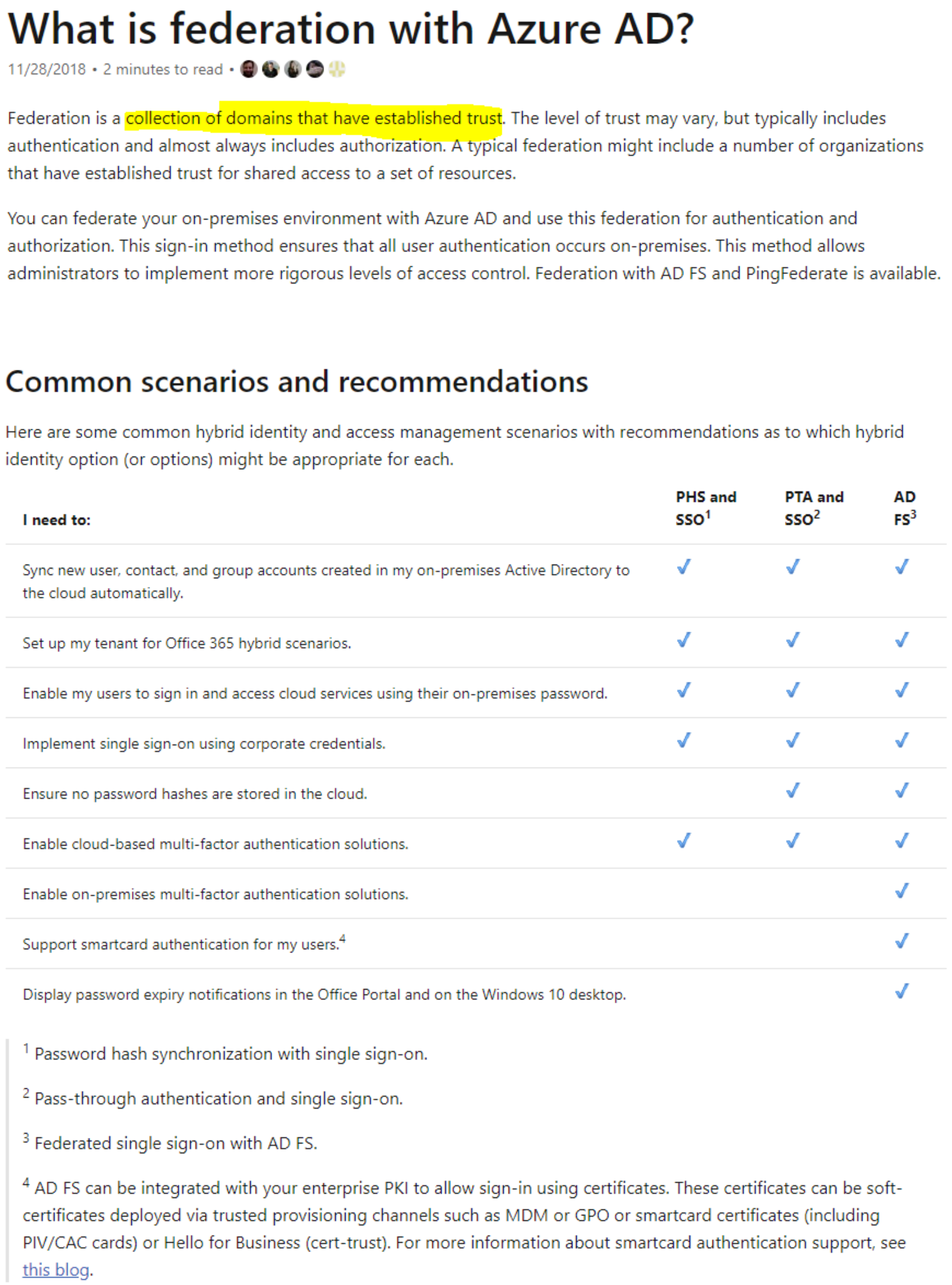
Role	**Explanation**
Security admin	**Security center only** - View/edit security policies - View security states - View/dismiss alerts/recommendations
Security reader	Same as security admin, but READ ONLY
Security manager	Manage: - Security components - Security policies - VIRTUAL MACHINES
User access administrator	Manage user access to resources, create custom roles
Network contributor	Can manage networks, NOT access them
SQL Server contributor	Manage SQL servers/database, NOT access them or the security properties
Virtual machine contributor	Manage VMs, NOT access them
Virtual machine administrator login	View VMs and login as administrator
Virtual machine user login	View VMs and login as regular user

On-prem Active Directory roles for delegation

Role	**Explanation**
Application administrator	Can manage for all applications: - Single sign-on settings - Application proxy - User/group assignments - Licensing CANNOT manage: - Conditional access
Cloud **application** administrator	= Application administrator, but no access to application proxy settings
Enterprise application **owner**	Can manage: enterprise applications that the user owns: - Single-sign on settings - User/group assignments - Adding owners CANNOT manage: - Application proxy settings - Conditional access
Application registration **owner**	Can manage application registrations the user owns: - Application manifest - Adding owners

Azure AD connect features

Feature	**Explanation**
Password hash synchronization (**PHS**)	Sign-in method that syncs on premise AD password to azure AD
Pass-through authentication (**PTA**)	Sign-in method that allows to use the on-prem password in the cloud
Federation integration	Optional. To configure a hybrid AD FS infrastructure
Synchronization	Responsible for creating users, groups, objects, and keeping identity information in sync. **Includes password hashes**
Password writeback	Sync Azure AD password changes to on-prem AD
Health monitoring	Use **Azure AD connect Health** to monitor all AD connect activity



What is federation with Azure AD?

11/28/2018 • 2 minutes to read •

Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization. A typical federation might include a number of organizations that have established trust for shared access to a set of resources.

You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises. This method allows administrators to implement more rigorous levels of access control. Federation with AD FS and PingFederate is available.

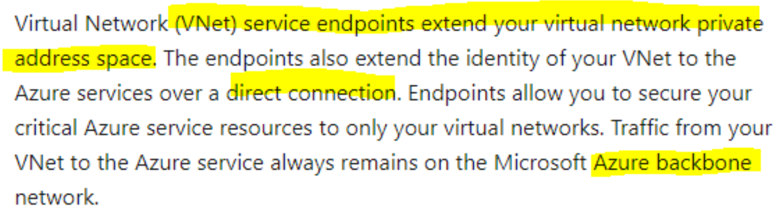
Common scenarios and recommendations

Here are some common hybrid identity and access management scenarios with recommendations as to which hybrid identity option (or options) might be appropriate for each.

I need to:	PHS and SSO[1]	PTA and SSO[2]	AD FS[3]
Sync new user, contact, and group accounts created in my on-premises Active Directory to the cloud automatically.	✓	✓	✓
Set up my tenant for Office 365 hybrid scenarios.	✓	✓	✓
Enable my users to sign in and access cloud services using their on-premises password.	✓	✓	✓
Implement single sign-on using corporate credentials.	✓	✓	✓
Ensure no password hashes are stored in the cloud.		✓	✓
Enable cloud-based multi-factor authentication solutions.	✓	✓	✓
Enable on-premises multi-factor authentication solutions.			✓
Support smartcard authentication for my users.[4]			✓
Display password expiry notifications in the Office Portal and on the Windows 10 desktop.			✓

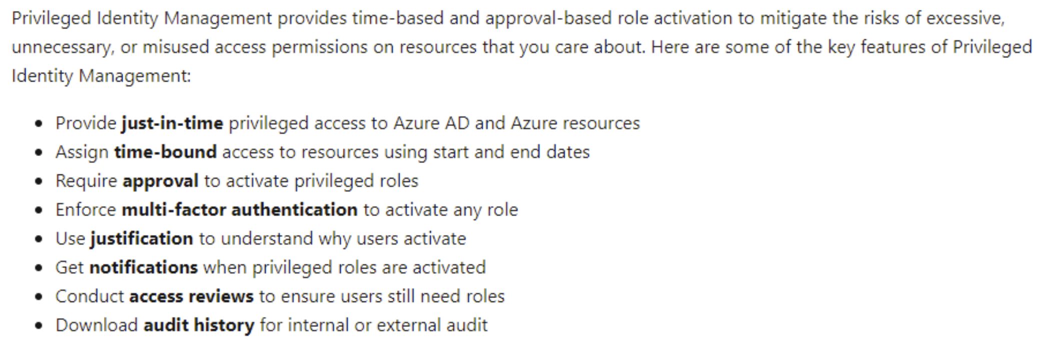
> [1] Password hash synchronization with single sign-on.
>
> [2] Pass-through authentication and single sign-on.
>
> [3] Federated single sign-on with AD FS.
>
> [4] AD FS can be integrated with your enterprise PKI to allow sign-in using certificates. These certificates can be soft-certificates deployed via trusted provisioning channels such as MDM or GPO or smartcard certificates (including PIV/CAC cards) or Hello for Business (cert-trust). For more information about smartcard authentication support, see this blog.

VNet Service Endpoint



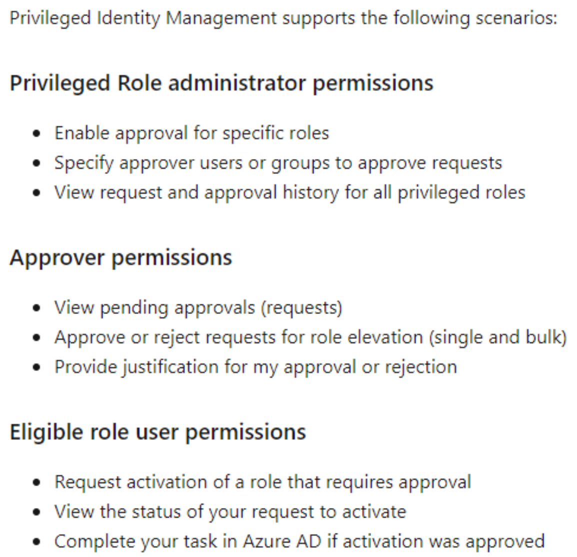
Virtual Network (VNet) service endpoints extend your virtual network private address space. The endpoints also extend the identity of your VNet to the Azure services over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network.

Privileged Identity Management



Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- Use **justification** to understand why users activate
- Get **notifications** when privileged roles are activated
- Conduct **access reviews** to ensure users still need roles
- Download **audit history** for internal or external audit



Privileged Identity Management supports the following scenarios:

Privileged Role administrator permissions

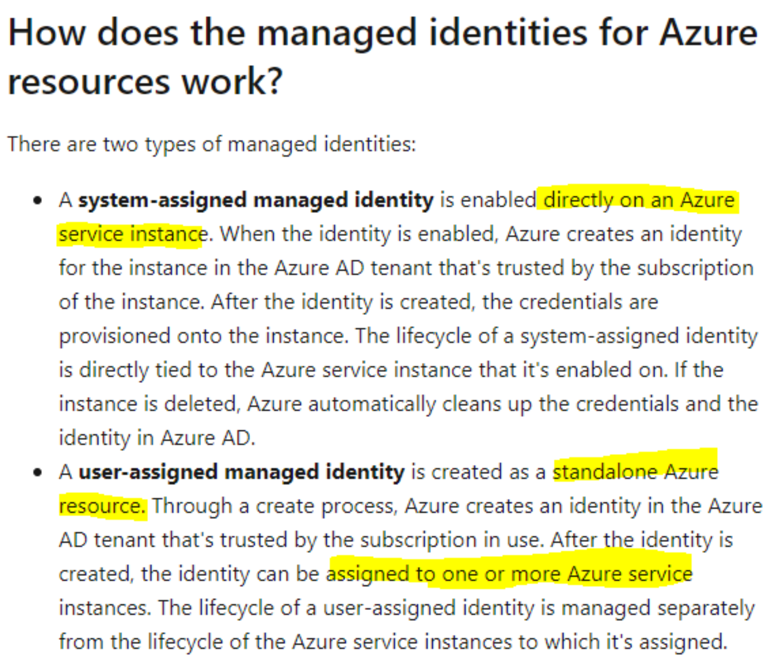
- Enable approval for specific roles
- Specify approver users or groups to approve requests
- View request and approval history for all privileged roles

Approver permissions

- View pending approvals (requests)
- Approve or reject requests for role elevation (single and bulk)
- Provide justification for my approval or rejection

Eligible role user permissions

- Request activation of a role that requires approval
- View the status of your request to activate
- Complete your task in Azure AD if activation was approved



How does the managed identities for Azure resources work?

There are two types of managed identities:

- A **system-assigned managed identity** is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it's enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.
- A **user-assigned managed identity** is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Azure AD tenant that's trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it's assigned.

How to delegate administrative access to a resource

- If the role with the user(s) that need administrative access doesn't exist:
  - Create the role and add the user(s)
- Go to the resource or resource group (can also be the subscription)
- Select IAM
- Select Role assignments
- Click Add
- Select the 'Owner' role
- Assign to the group with the user(s)
- Click save

Difference between Standard and Premium storage tier?

- Standard: magnetic drives
- Premium: SDD drives

Max CPU time per day for Free App Service plan?

- 60 minutes

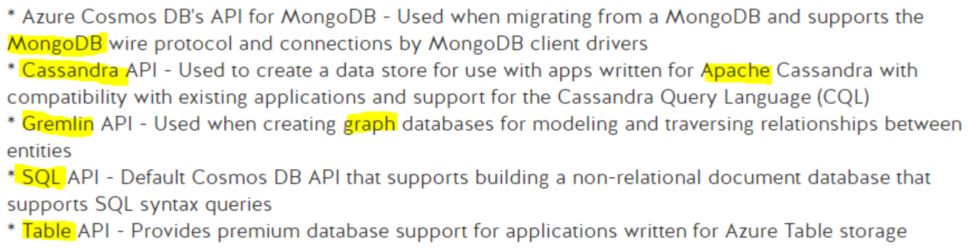
Minimum license to use AD connect?

- AD Premium P1

Docker CLI

- docker push: push an image to an Azure login server
- docker run: runs a container locally
- az acr create: creates an Azure Container Registry
- az container create: creates a container instance

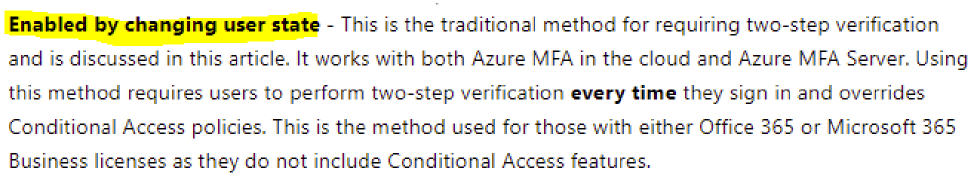
Cosmos db API types



* Azure Cosmos DB's API for MongoDB - Used when migrating from a MongoDB and supports the MongoDB wire protocol and connections by MongoDB client drivers
* Cassandra API - Used to create a data store for use with apps written for Apache Cassandra with compatibility with existing applications and support for the Cassandra Query Language (CQL)
* Gremlin API - Used when creating graph databases for modeling and traversing relationships between entities
* SQL API - Default Cosmos DB API that supports building a non-relational document database that supports SQL syntax queries
* Table API - Provides premium database support for applications written for Azure Table storage

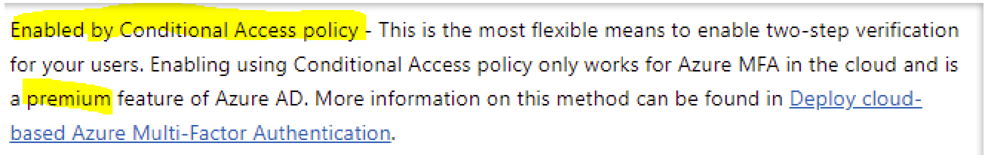
4 Ways to enable MFA

1: OFFICE



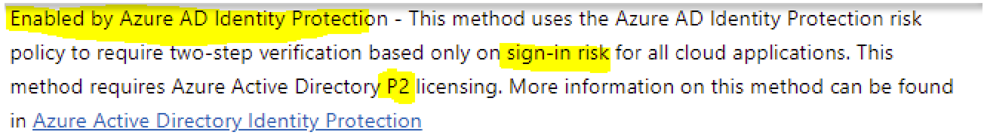
Enabled by changing user state - This is the traditional method for requiring two-step verification and is discussed in this article. It works with both Azure MFA in the cloud and Azure MFA Server. Using this method requires users to perform two-step verification **every time** they sign in and overrides Conditional Access policies. This is the method used for those with either Office 365 or Microsoft 365 Business licenses as they do not include Conditional Access features.

2: AZURE AD P2



Enabled by Conditional Access policy - This is the most flexible means to enable two-step verification for your users. Enabling using Conditional Access policy only works for Azure MFA in the cloud and is a premium feature of Azure AD. More information on this method can be found in Deploy cloud-based Azure Multi-Factor Authentication.

3: AZURE AD P2



Enabled by Azure AD Identity Protection - This method uses the Azure AD Identity Protection risk policy to require two-step verification based only on sign-in risk for all cloud applications. This method requires Azure Active Directory P2 licensing. More information on this method can be found in Azure Active Directory Identity Protection

4: AZURE AD P2

PIM: require MFA to activate role

To read

- Azure VM series: https://azure.microsoft.com/en-us/pricing/details/virtual-machines/series/