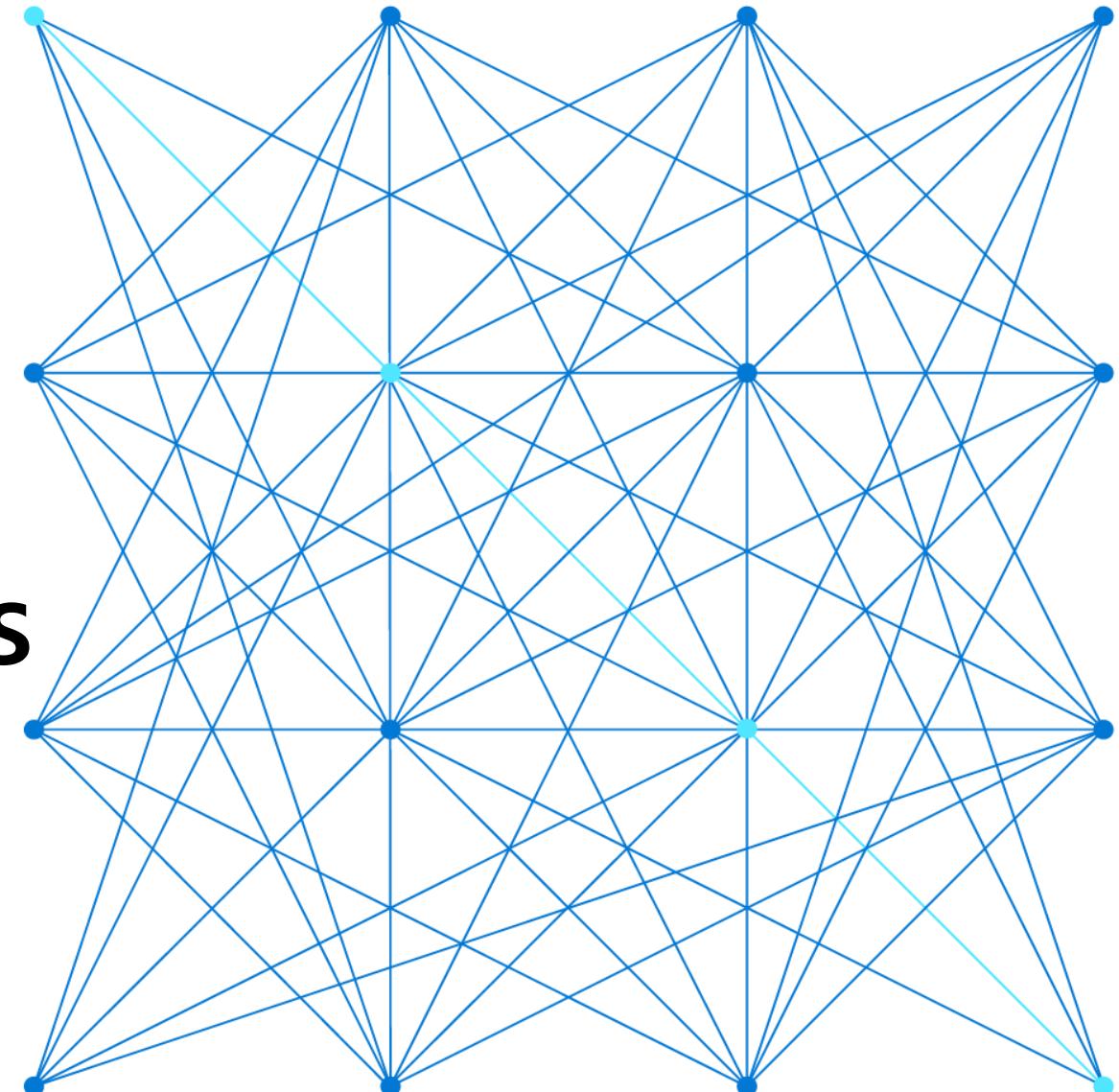


# AZ-500

# Microsoft Azure Security Technologies



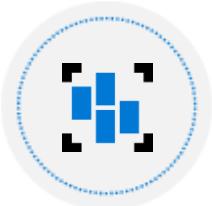
# AZ-500 Agenda



**Learning Path 1 Identity and Access** ←



**Learning Path 2 Implement Platform Protection**

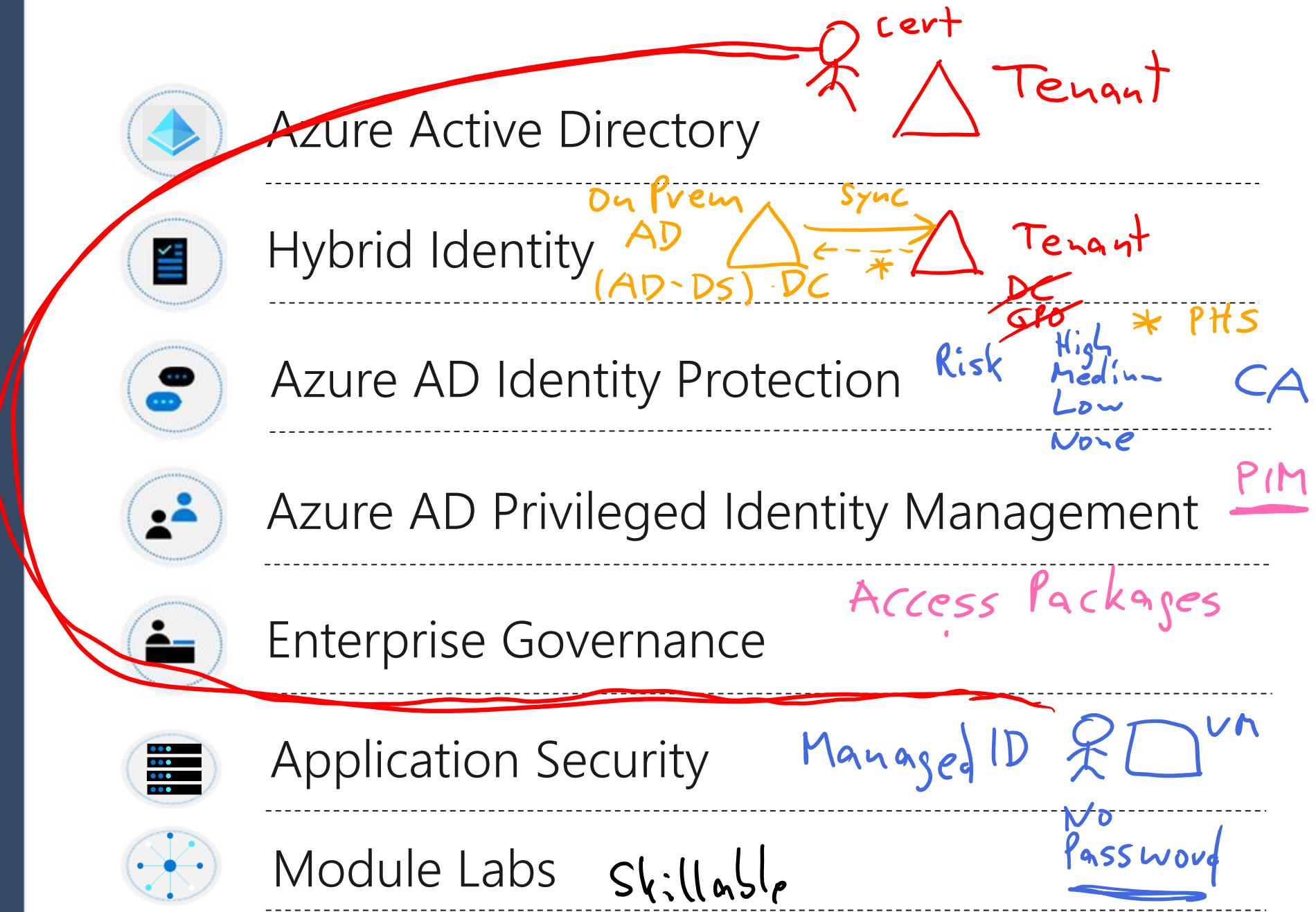


**Learning Path 3 Data and Application Security**



**Learning Path 4 Security Operations**

# Learning Path: Identity and Access



# Azure Active Directory



MS Account  
Google  
Twitter  
GitHub

## Azure Active Directory (Azure AD)

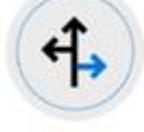
Tenant ID Provider  
E3 E5



Azure AD features



Azure AD versus Active Directory Domain Services (AD DS)



Roles for Azure AD



Azure AD Domain Services



Azure AD Users



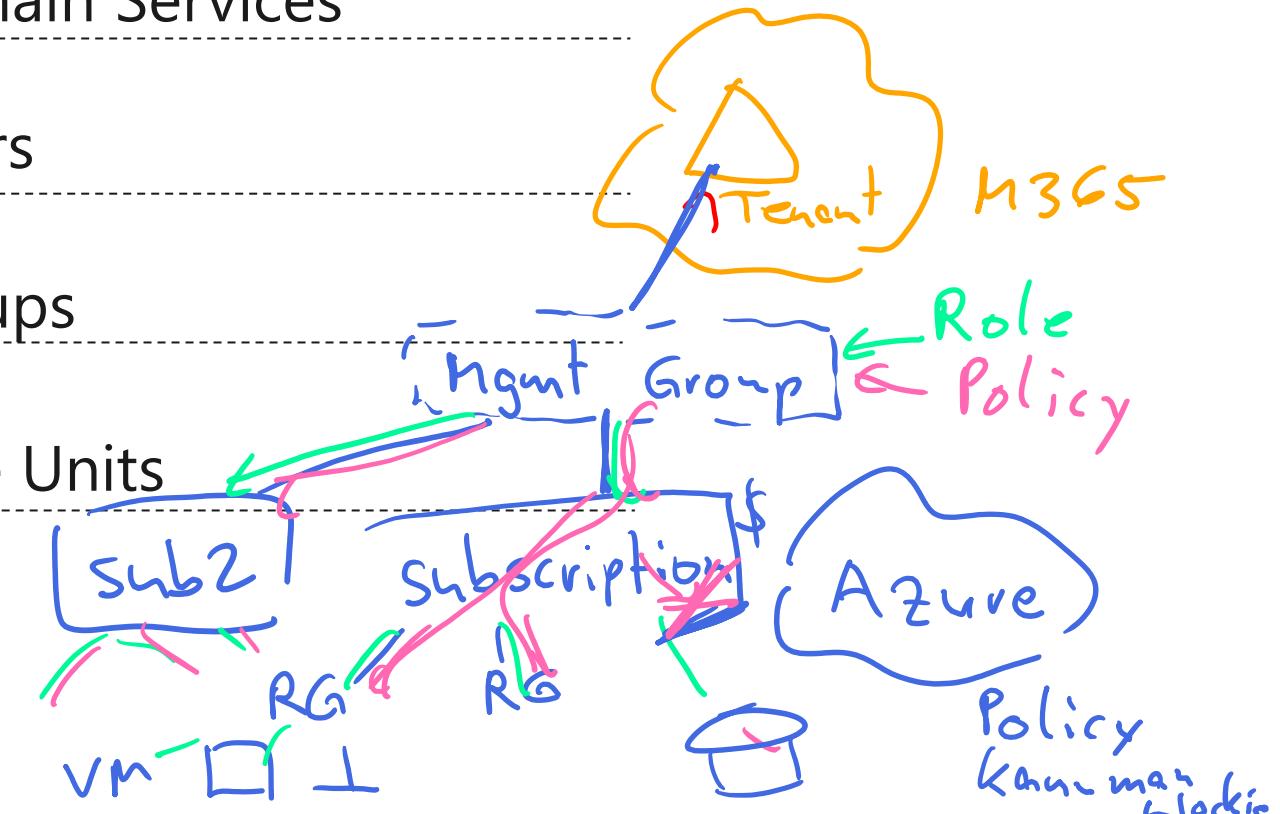
Azure AD Groups



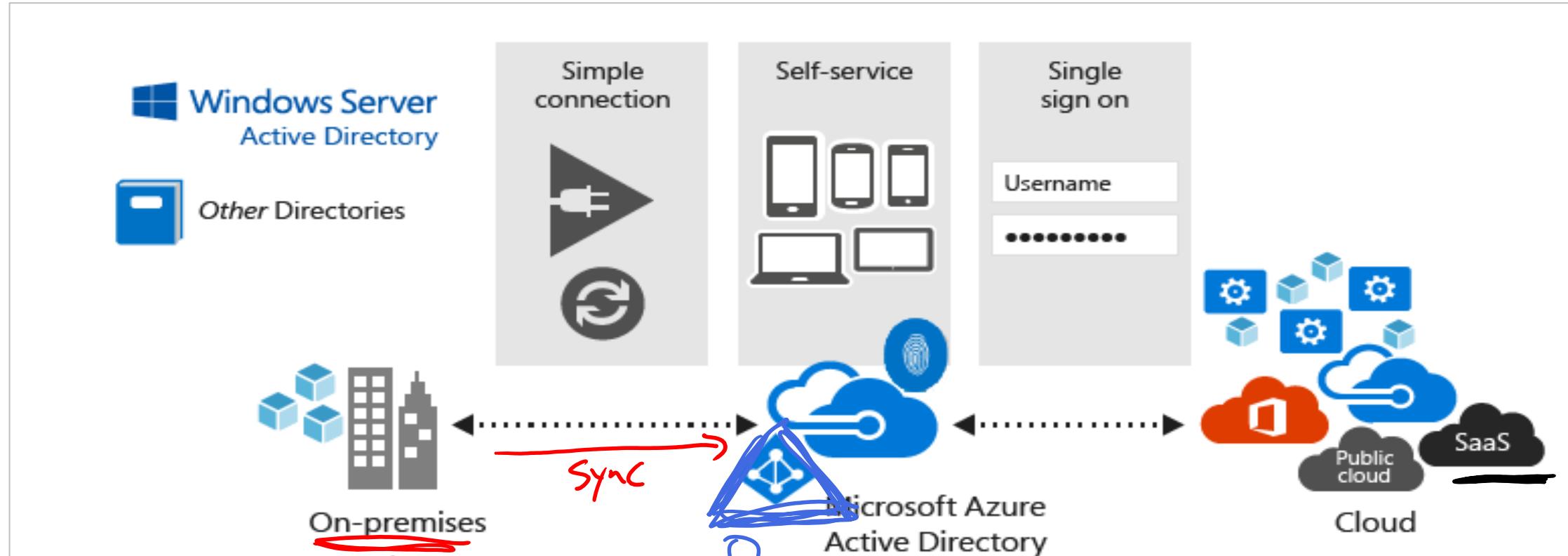
Administrative Units



Passwordless



# Azure Active Directory Features



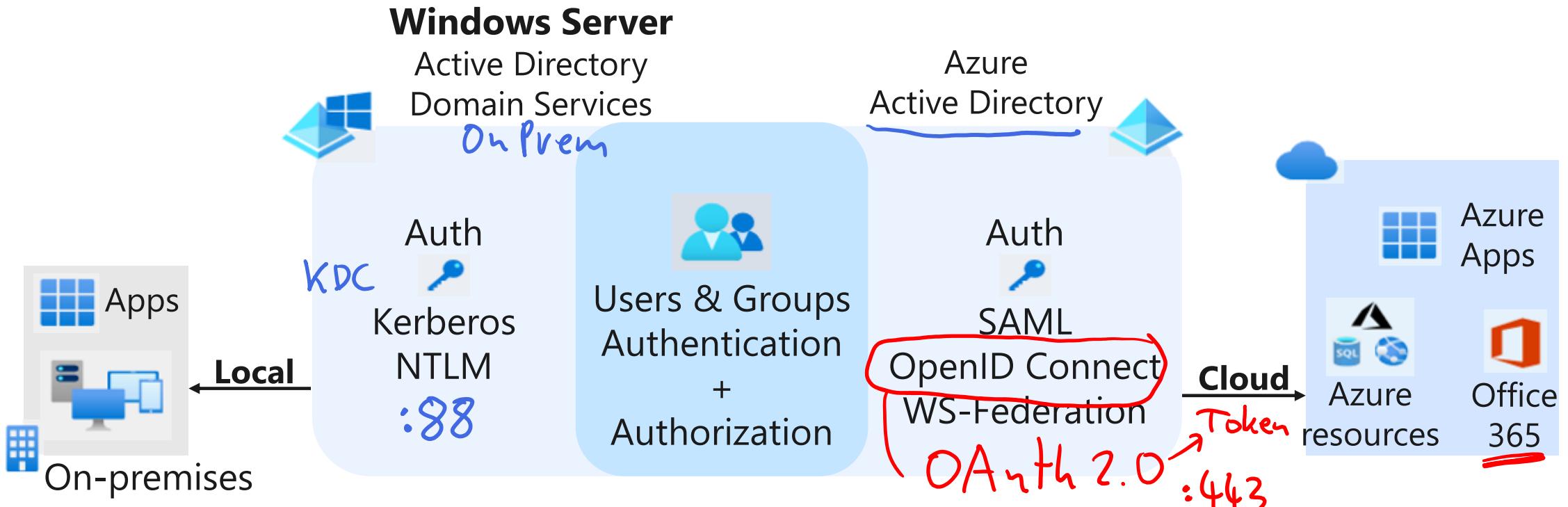
Microsoft's multi-tenant cloud-based directory and identity management service

Identity management capabilities and integration

Integrates with Windows Server Active Directory

Provides SSO access

# Azure AD versus Active Directory Domain Services (AD DS)



Service	Authentication	Structure	What it's used for
Azure Active Directory	Includes SAML, OpenID Connect (based on OAuth), WS-Federation	Tenants	Internet-based services and applications like Office 365, Azure services, and third-party SaaS applications
Active Directory Domain Services	Kerberos, NTLM	Forests, domains, organizational units	Authentication and authorization for on-premises printers, applications, file services, and more

RBAC

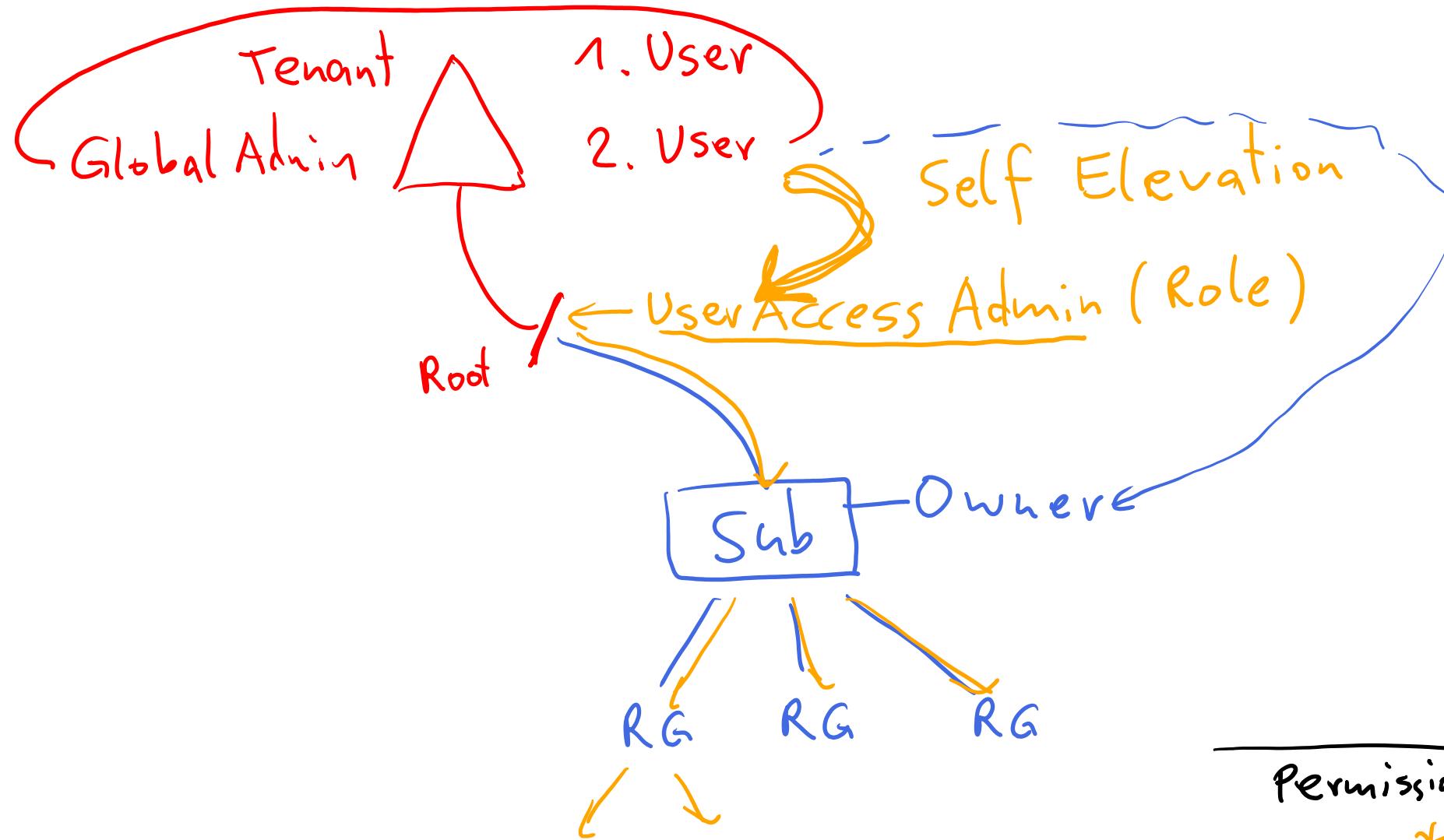
## Roles for Azure AD (sample)

RBAC

Azure

Owner Reader

Built-in Role	Description
Global Administrator	Users with this role have access to all administrative features in Azure Active Directory
Security Administrator	Users with this role have permissions to manage security-related features in the Microsoft 365 Security Center, Security Center, Azure Active Directory Identity Protection, Azure Information Protection, and Office 365 Security & Compliance Center
Billing Administrator	Makes purchases, manages subscriptions, manages support tickets, and monitors service health
Global Reader	Users in this role can read settings and administrative information across Microsoft 365 services but can't take management actions.



Role = Permission

---

Permission

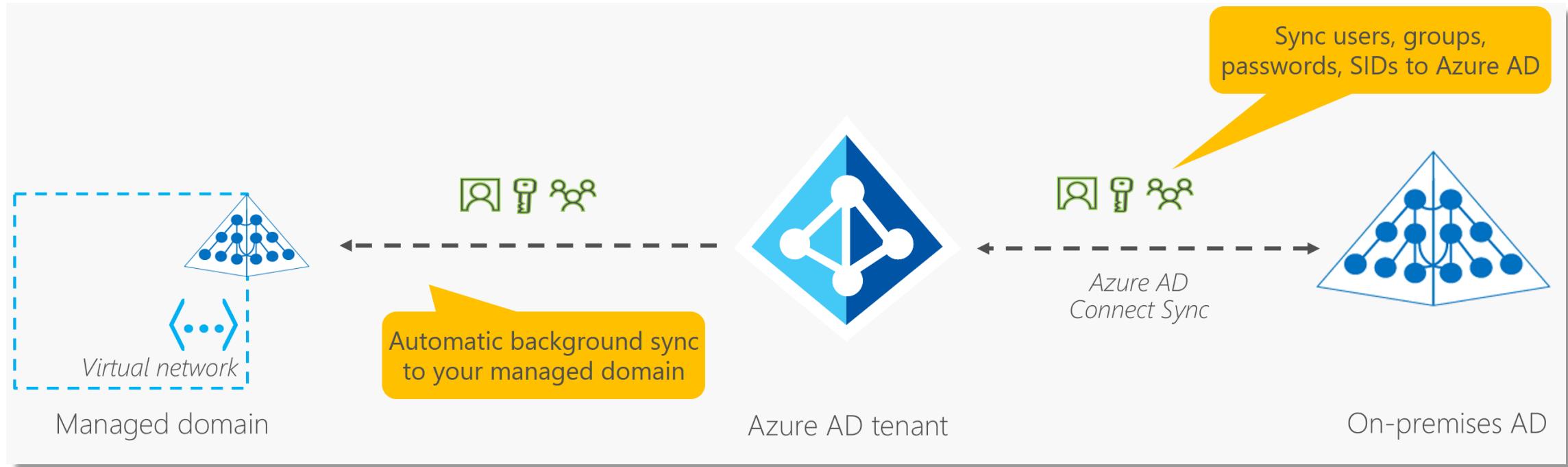
\* / Read

Azure Provider

---

Data Permission

# Azure Active Directory Domain Services



- Azure Active Directory Domain Services (Azure AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/New Technology LAN Manager (NTLM) authentication.



You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

# Azure AD Users

- Add new users or delete existing users from your Azure Active Directory (Azure AD) tenant.
  - To add or delete users, you must be a User Administrator or Global Administrator.

The screenshot shows the Microsoft Azure portal interface for managing users. The top navigation bar includes the Microsoft Azure logo, a search bar, and user account information (chrisgreen@contoso.com, CONTOSO). The left sidebar has a 'Users' icon and links for 'All users (preview)', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', 'Deleted users (preview)', 'Password reset', 'User settings', and 'Bulk operation results'. The main content area is titled 'Users' and shows a table of users. A modal window is open over the table, with the 'New user' button highlighted. The modal contains two options: 'Create new user' (Create a new internal user in your organization) and 'Invite external user' (Invite an external user to collaborate with your organization). The table below the modal lists three users:

User principal name	User type	Identities
aincharon@contoso.com	Guest	ExternalAzureAD
mycolannino_microsoft.c...	Guest	ExternalAzureAD
AzureAdmin@identityit.o...	Member	IdentityIT.onmicrosoft.com

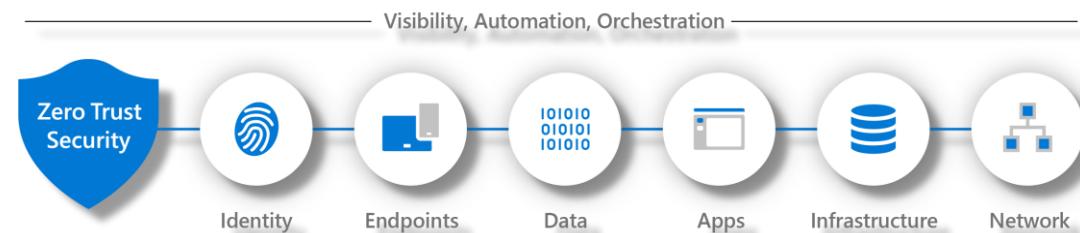
# Azure AD Groups

- Azure Active Directory (Azure AD) provides several ways to manage access to resources, applications, and tasks.

- With Azure AD groups, you can grant access and permissions to a group of users instead of each individual user.

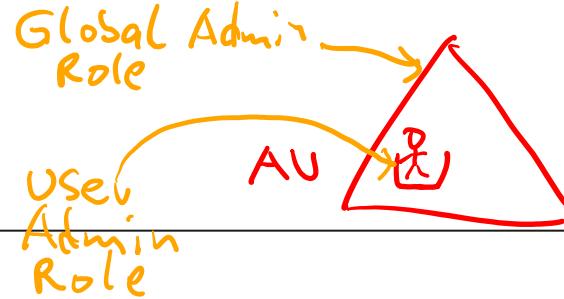
- Limiting access to Azure AD resources to only those users who need access is one of the core security principles of Zero Trust.

Name	Object Id	Group type
MDM- policy - All org	b4550b3e-45ae-4f46-ba85-19c5c4412d71	Security
MDM - policy - East	2b8b023a-17b6-410b-84d9-daf447c70f08	Security
MDM policy - North	35d3ba26-23f7-4689-afea-a803586f077c	Security
MDM policy - South	4ef1fe76-3a35-4847-a46f-81369c95bb34	Security
MDM policy - West	8a0cd375-c701-42f4-b074-c54f70a32da0	Security



AU

# Administrative Units in Azure AD



The screenshot shows the 'School of Engineering | Users (Preview)' page in the Azure Active Directory portal. The left sidebar includes 'Properties', 'Users (Preview)' (which is selected), 'Groups', and 'Roles and administrators'. The main area has a search bar, 'Add member', 'Remove member', 'Bulk operations', 'Refresh', and 'Columns' buttons. A message indicates 'This page includes previews available for your evaluation. View previews →'. Below is a search bar for users, a filter button, and a table header for 'Name', 'User principal name', and 'User type'. A message at the bottom states 'Unable to complete due to service connection error. Please try again later.'

## Admin Unit Members

- Users
- Groups

## Usage

Delegate administration of AD resources to specific person or role

## Configure using

- PowerShell / MS Graph
- Azure AD portal
- M365 Admin Center

# Passwordless

Home > Default Directory > Security >

The screenshot shows the 'Authentication methods | Policies' page in the Azure AD Security section. The left sidebar includes 'Search (Ctrl+ /)', 'Manage' (selected), 'Policies' (highlighted), 'Password protection', 'Monitoring', 'Activity', 'User registration details', and 'Registration and reset events'. The main content area has a 'Got feedback?' button and a note about enabling combined security info registration. It also contains a table of authentication methods:

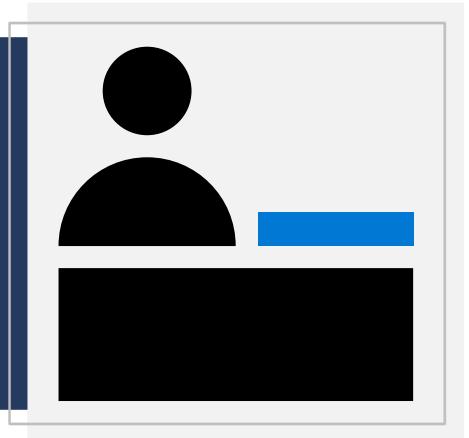
Method	Target	Enabled
FIDO2 Security Key		No
Microsoft Authenticator		No
Text message (preview)		No
Temporary Access Pass (preview)		No

Log in without using a password, ever.

- Increased security
- Better user experience
- More insights with logs and audits

AzureAD Connect

# Hybrid Identity



# Hybrid Identity



Azure AD Connect



Azure AD Connect cloud sync



Authentication Options



Password Hash Synchronization (PHS)



Pass-through Authentication (PTA)



Federation with Azure AD



Authentication Decision Tree



Password Writeback

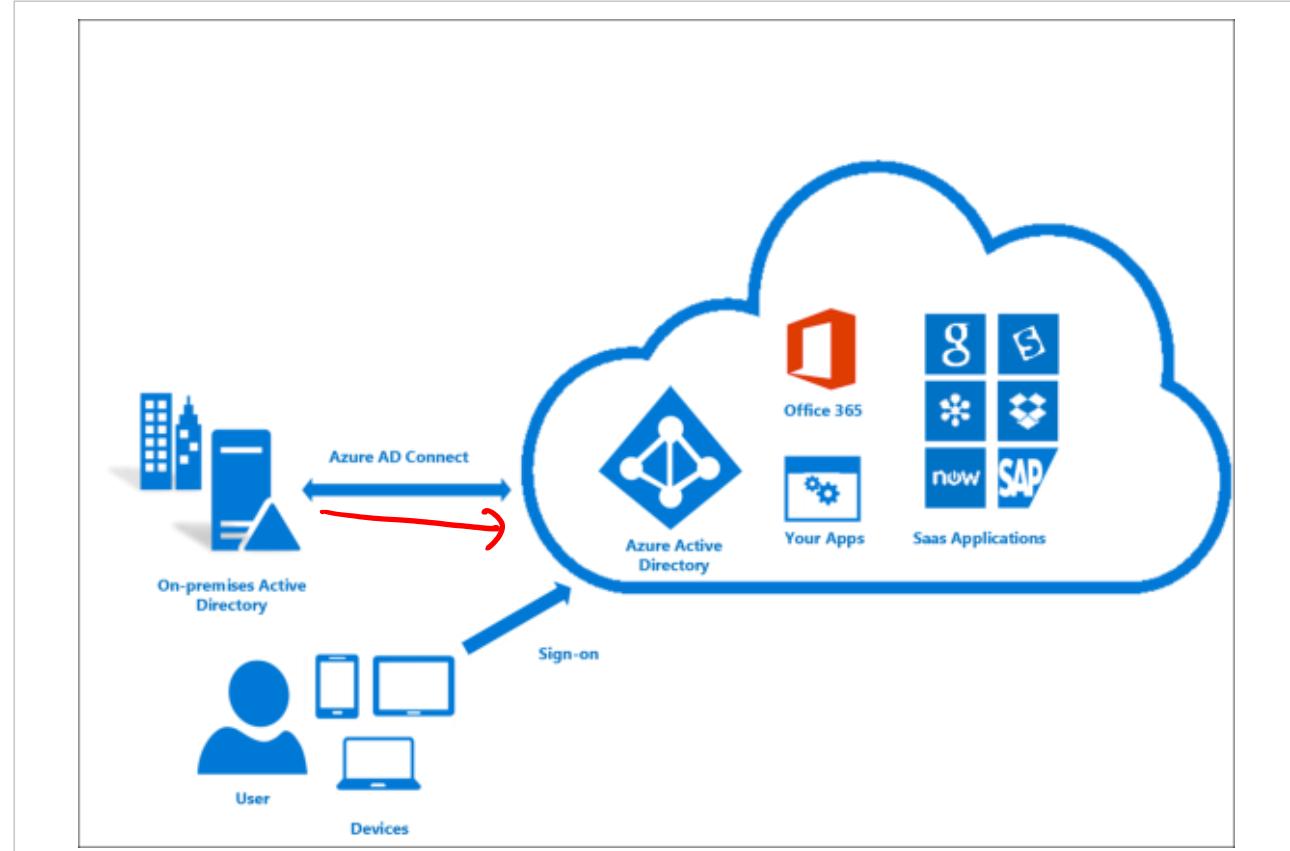
# Azure AD Connect

Tool Free

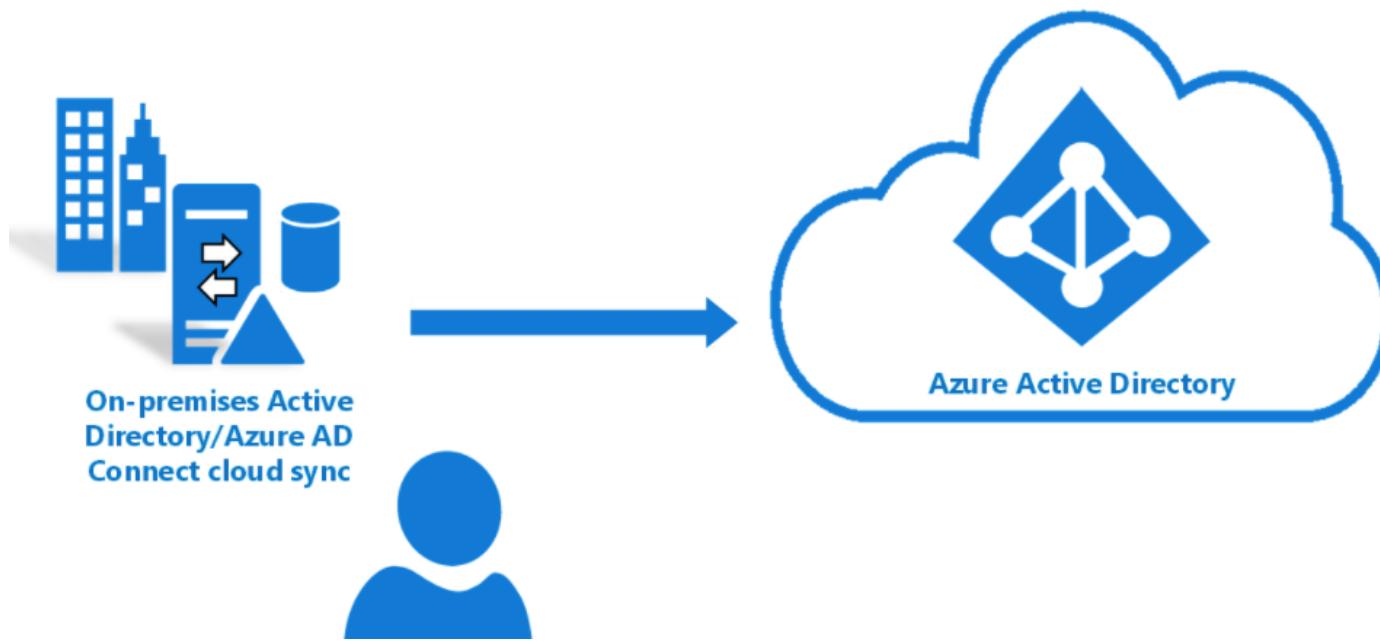
Integrate your on-premises directories with Azure Active Directory

Provides a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD

There are several authentication options to enable hybrid identity



# Azure AD Connect Cloud Sync



Alternate method to integrate your on-premises directories with Azure Active Directory

Uses the Azure AD cloud provisioning agent

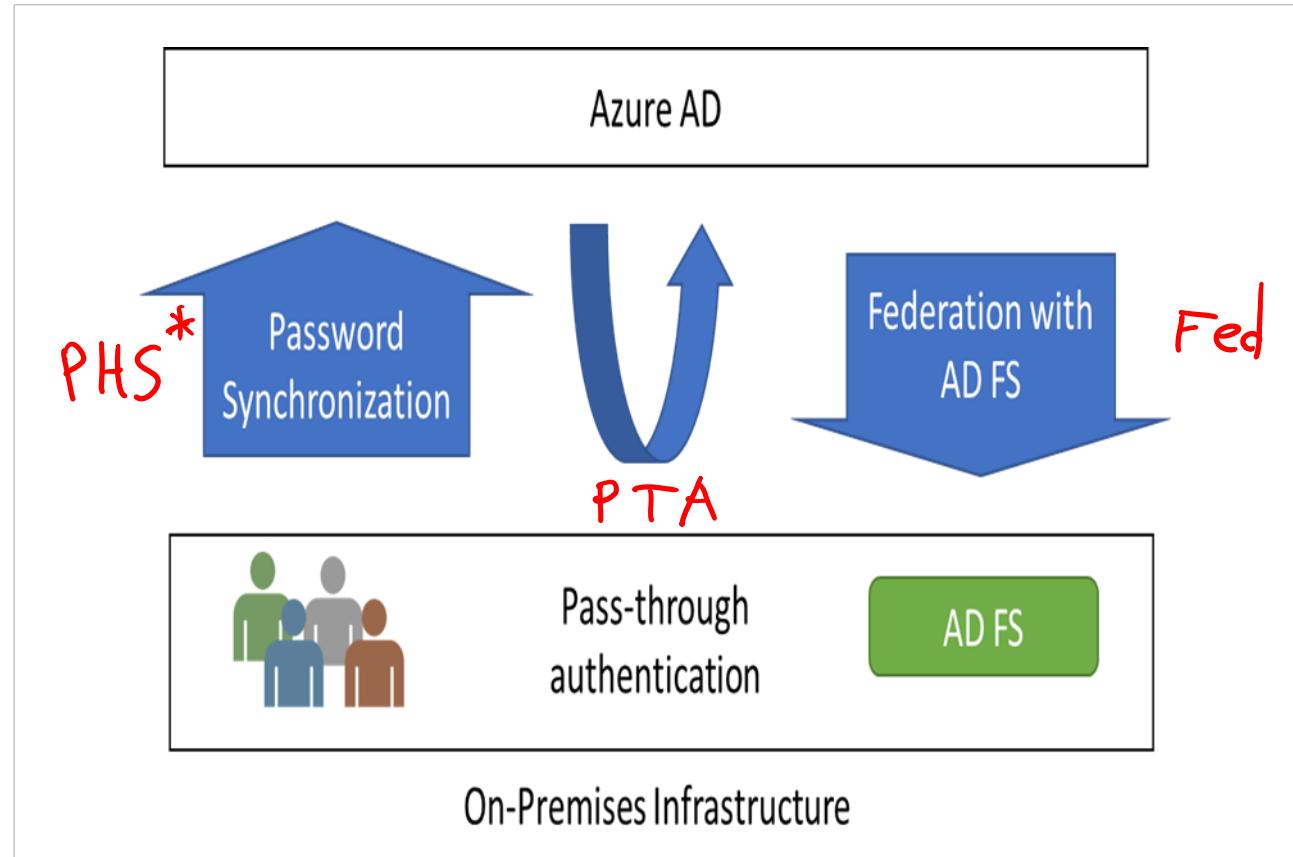
Runs stand-alone or along-side Azure AD Connect

# Authentication Options

Password Hash Synchronization (PHS) can synchronize an encrypted version of the password hash for user accounts

Pass-through authentication (PTA) authenticates the username and password with the on-premises domain controllers

AD FS is the Microsoft implementation of an identity federation solution that uses claims-based authentication



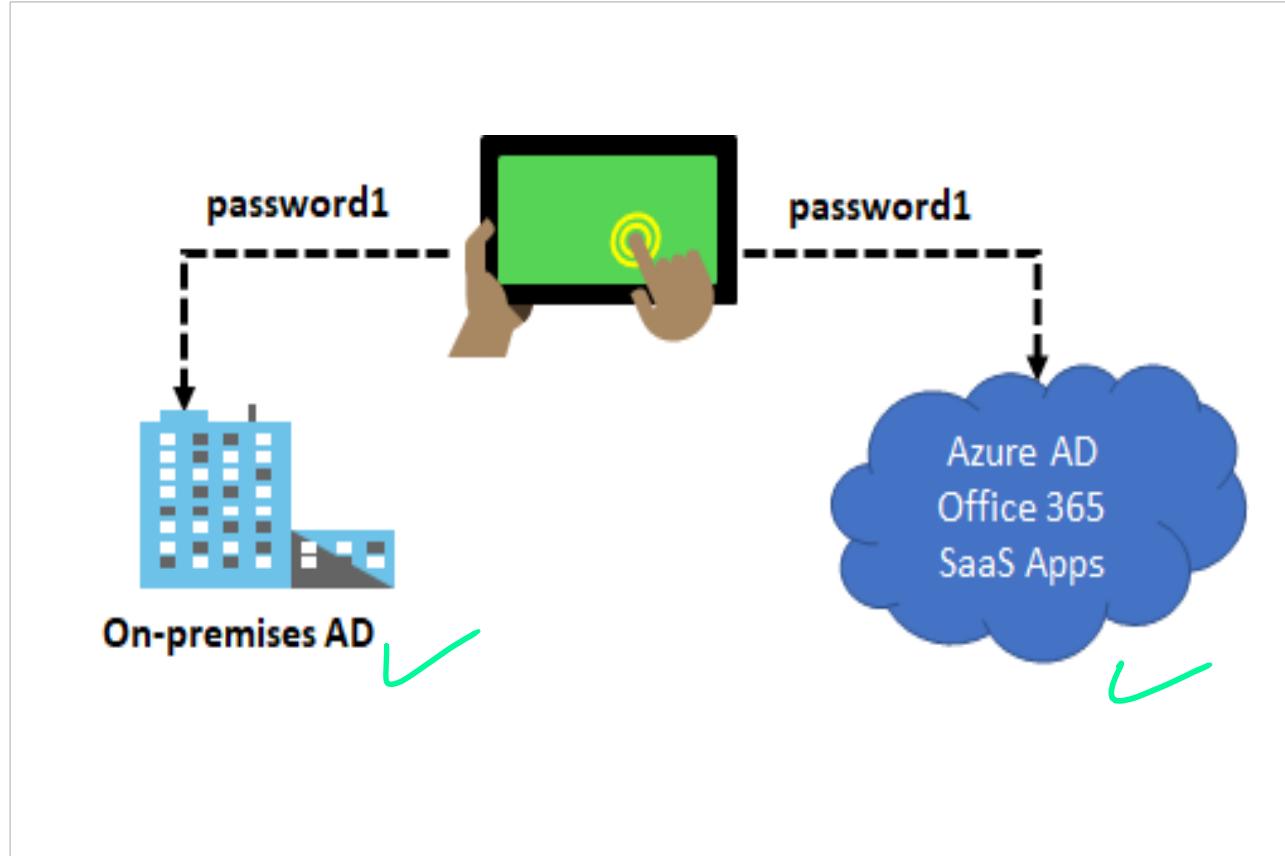
# Password Hash Synchronization

PHS

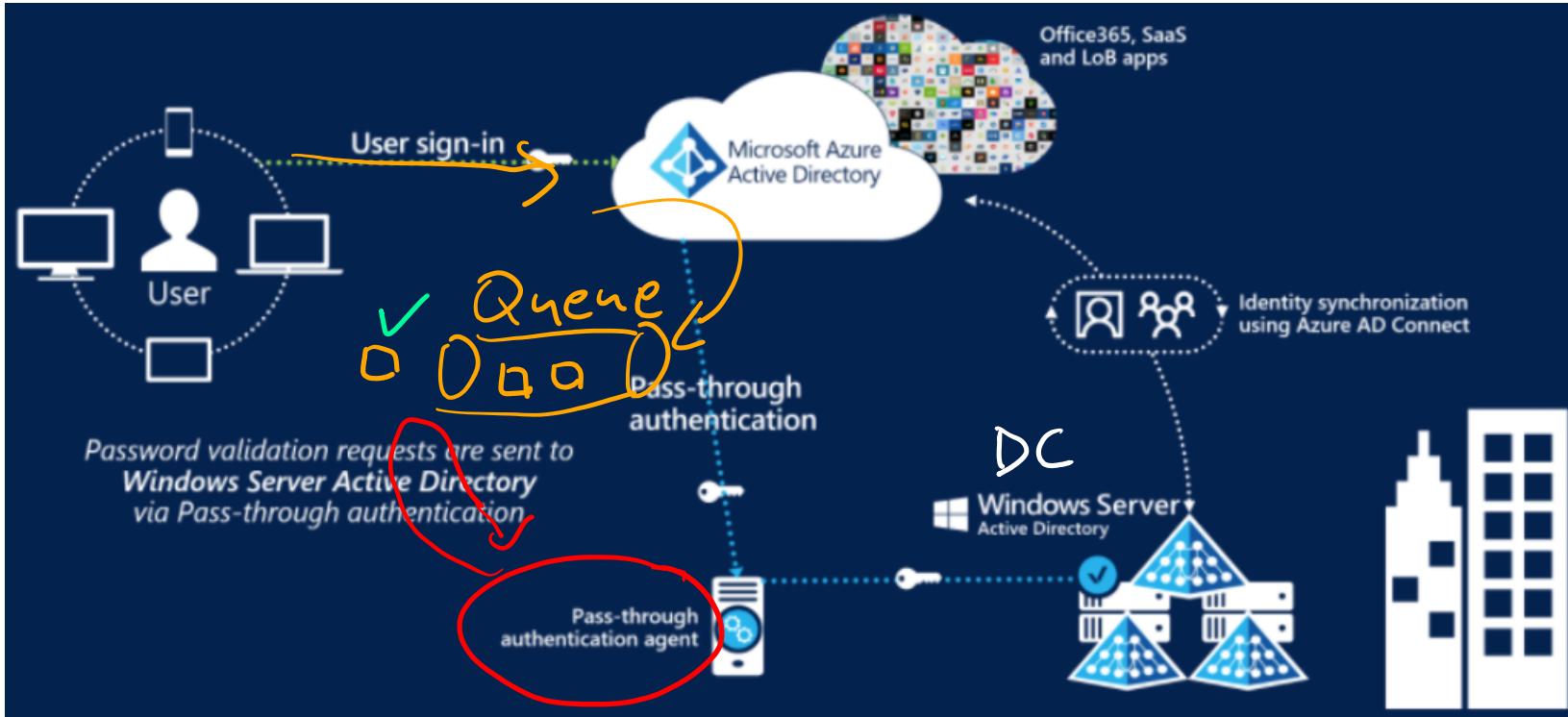
Password hash synchronizes user passwords from on-premises Active Directory to cloud-based Azure AD

Sign into Azure AD services using the on-premises password

Improve the productivity of your users and reduce your helpdesk costs



# Pass-through Authentication



Supports user sign-in into all web browser-based applications and into Microsoft Office client applications

Is a free feature and can be enabled via Azure AD Connect

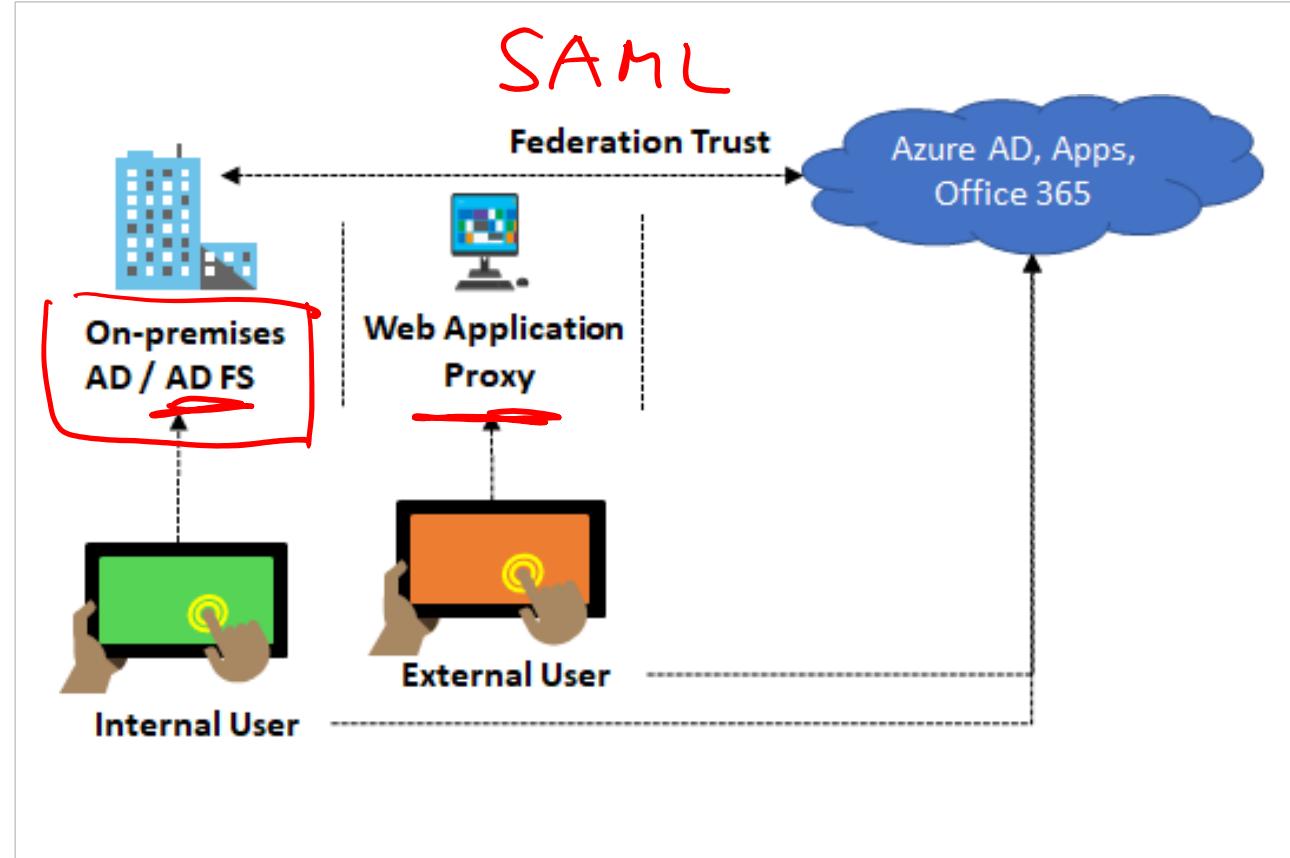
Is not only for user sign-in but allows an organization to use other Azure AD features – MFA and Self-Service Password Reset

# Federation with Azure AD

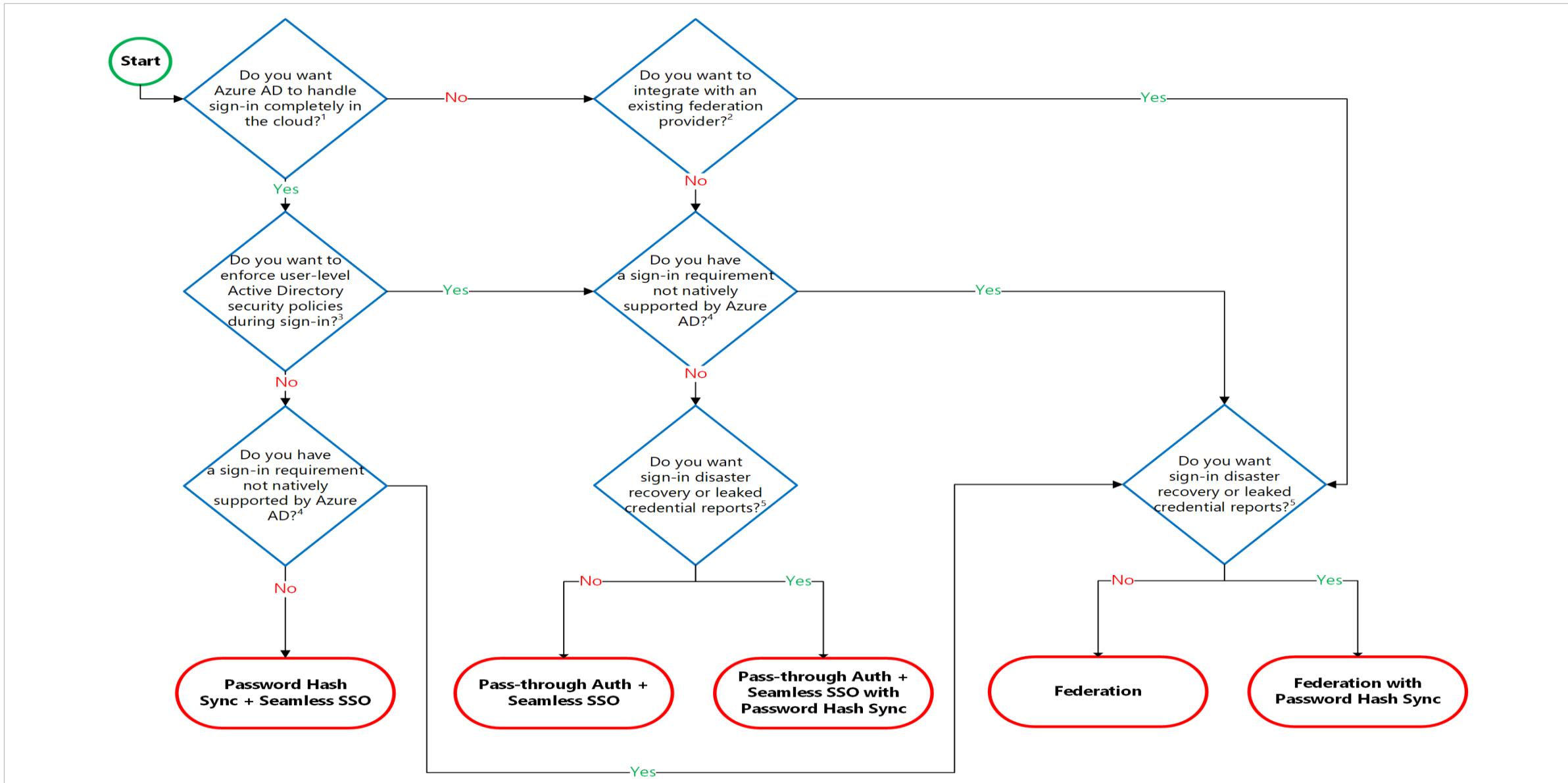
Federation is a collection of domains that have established trust

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



# Authentication Decision Tree



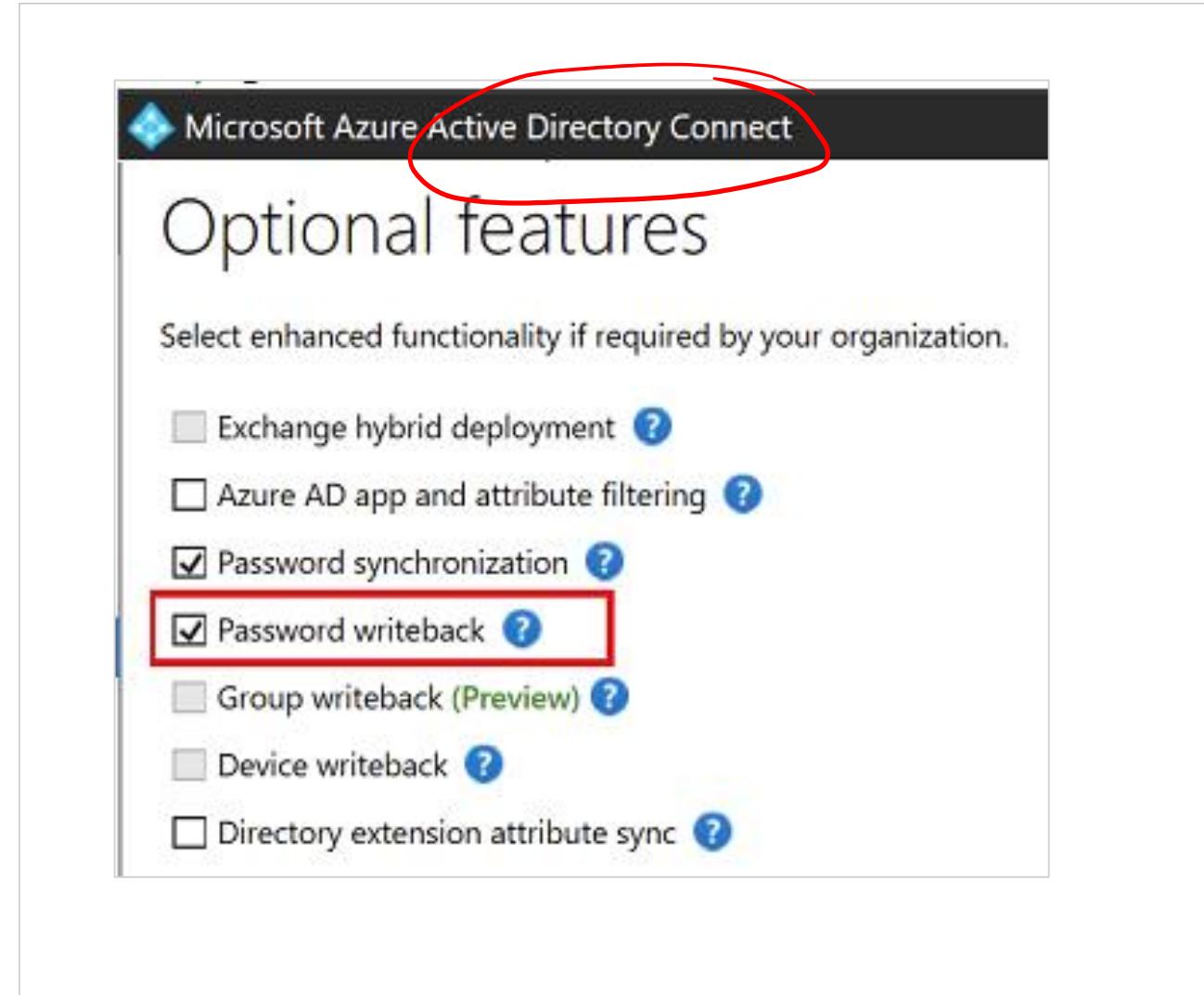
# Password Writeback

Use Password Writeback to configure Azure AD to write passwords back to your on-premises Active Directory

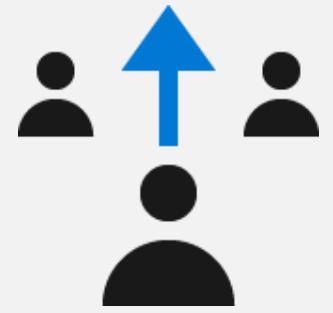
A component of Azure AD Connect

Available to subscribers of Premium Azure Active Directory editions

Removes the need to set up and manage an on-premises SSPR solution



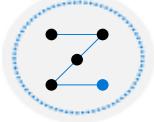
# Azure AD Identity Protection



# Azure AD Identity Protection



Azure AD Identity Protection



Risk Events



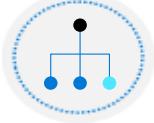
User Risk Policy



Sign-in Risk Policy



Azure MFA concepts



Azure AD Conditional Access



Conditions



Access Reviews

# Azure AD Identity Protection Features

<p>Policy name Multi-factor authentication registration policy</p> <p>Assignments</p> <p>Users All users &gt;</p> <p>Controls</p> <p>Access Require Azure MFA registration &gt;</p> <p><span style="background-color: #e0f2e0; padding: 5px;">MFA Registration Policy only affects cloud-based Azure MFA. If you have MFA Server it will not be affected.</span></p> <p>Enforce Policy <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 10px; display: inline-block;">On <input type="radio"/> Off <input checked="" type="radio"/></span></p>	<p>Policy name User risk remediation policy</p> <p>Assignments</p> <p>Users All users &gt;</p> <p>Conditions User risk &gt;</p> <p>Controls</p> <p>Access Require password change &gt;</p> <p>Review</p> <p>Estimated impact Number of users impacted &gt;</p> <p>Enforce Policy <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 10px; display: inline-block;">On <input type="radio"/> Off <input checked="" type="radio"/></span></p>	<p>Policy name Sign-in risk remediation policy</p> <p>Assignments</p> <p>Users All users &gt;</p> <p>Conditions Sign-in risk &gt;</p> <p>Controls</p> <p>Access Require multi-factor authentication &gt;</p> <p>Review</p> <p>Estimated impact Number of sign-ins impacted &gt;</p> <p>Enforce Policy <span style="border: 1px solid #ccc; border-radius: 15px; padding: 2px 10px; display: inline-block;">On <input type="radio"/> Off <input checked="" type="radio"/></span></p>
--	--	---

Automate the detection and remediation of identity-based risks

Investigate risks using data in the portal

Export risk detection data to third-party utilities for further analysis

# Azure Identity Protection Risk Events

Each detected suspicious action is stored in a record called a risk event

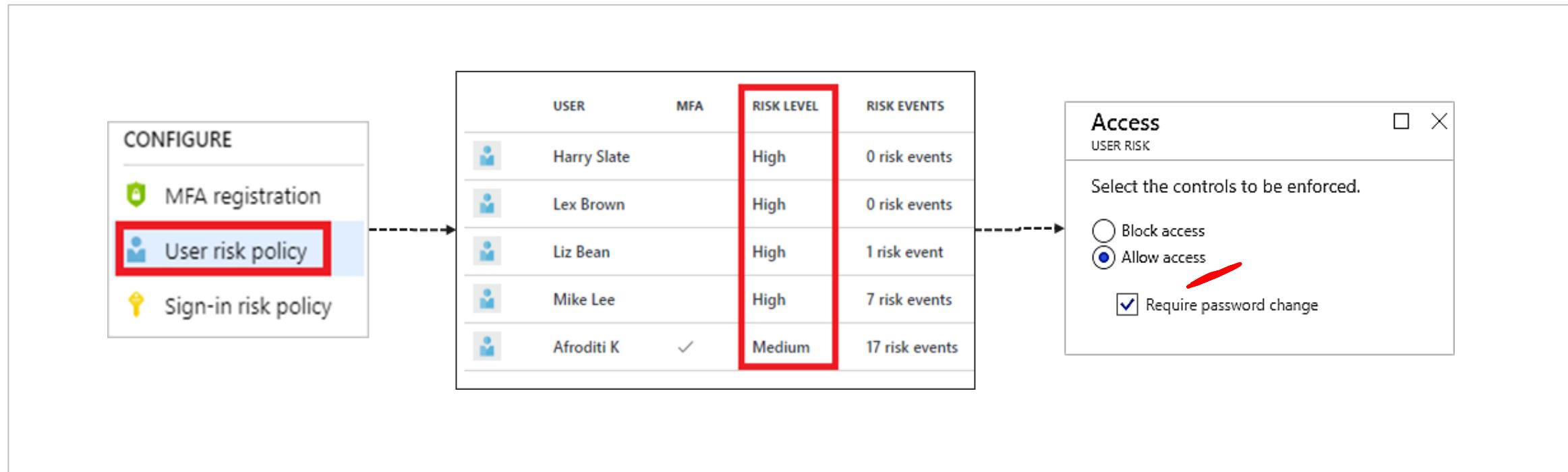
The screenshot shows the Azure Identity Protection Risk Events dashboard. On the left, a vertical list of risk events is displayed:

- Leaked credentials
- Sign in from anonymous IP addresses
- Impossible travel to atypical locations
- Sign in from unfamiliar locations
- Sign in from infected devices
- Sign in from IP addresses with suspicious activity

On the right, six risk event cards are shown in a grid:

- High risk users**: 8. Description: High risk users detected. Investigate users and reset passwords.
- Medium risk users**: 13. Description: Medium risk users detected. Investigate users and reset passwords.
- Unprotected risky sign-ins**: 10 / 13 risky sign-ins last week. Description: Protect these sign-ins by configuring your sign-in risk policy.
- Legacy authentication**: 2 sign-ins last week. Description: Sign-ins using legacy authentication protocols are not secure. Block them with
- Identity Secure Score**: 33 / 223. Description: Monitor and improve your identity security posture.

# User Risk Policy



Applied to user sign-ins

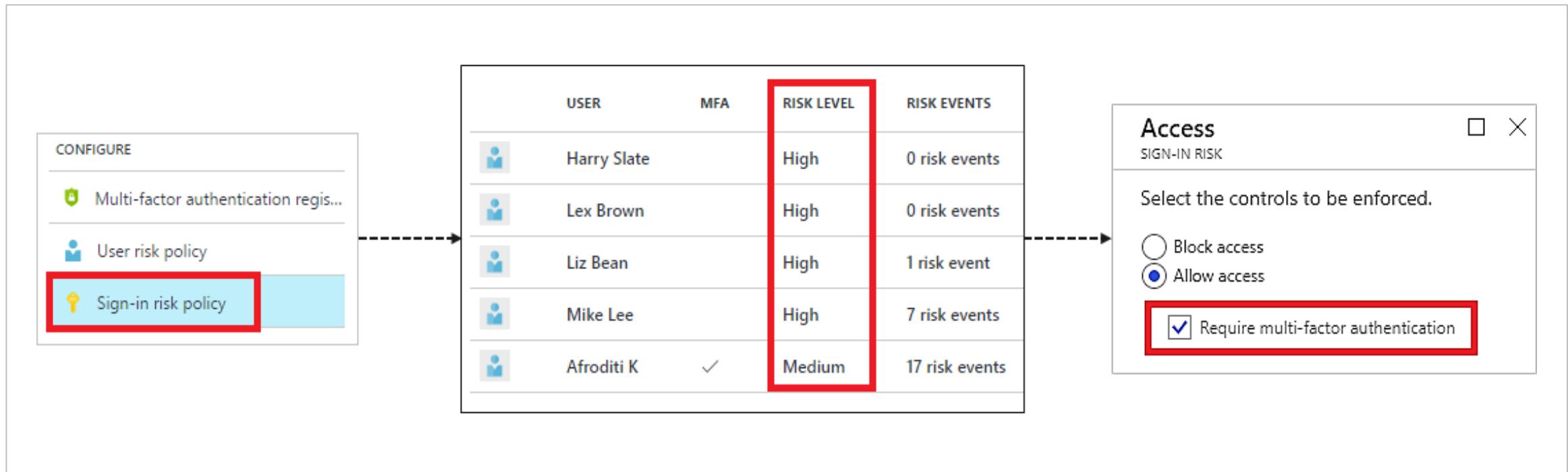
Automatically respond  
based on a specific user's  
risk level

Provide the condition (risk  
level) and action (block or  
allow)

Use a high threshold during  
policy roll out

Use a low threshold for  
greater security

# Sign-in Risk Policy



Applied to all browser traffic and sign-ins using modern authentication

Provide the condition (risk level) and action (block or allow)

Automatically respond to a specific risk level

Target all policies to specific users – omit certain types of users

# Azure MFA Concepts

The security of MFA two-step verification lies in its layered approach

Authentication methods include:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)

**Username**

test@xxx.com

**Password**

\*\*\*\*\*



# Enabling MFA

Select the users that you want to modify and enable for MFA

User states can be Enabled, Enforced, or Disabled

On first-time sign-in, after MFA has been enabled, users are prompted to configure their MFA settings

Azure MFA is included free of charge for global administrator security

The screenshot shows the 'multi-factor authentication' service settings page for the 'users' section. At the top, there's a note about licensing requirements and a link to the deployment guide. Below that, there are filters for 'View: Sign-in allowed users' and 'Multi-Factor Auth status: Any'. A 'bulk update' button is also present. The main table lists five users:

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS	
<input checked="" type="checkbox"/>	Adam Barr	AdamB@contoso.com	Disabled	3 selected quick steps Enable Manage user settings
<input checked="" type="checkbox"/>	Alice Ciccu	AliceC@contoso.com	Disabled	
<input type="checkbox"/>	Amy Rusko	AmyR@contoso.com	Disabled	
<input type="checkbox"/>	Ann Beebe	AnnB@lumartech.com	Disabled	
<input checked="" type="checkbox"/>	Ben Smith	BenS@contoso.com	Disabled	

# MFA Settings

Account Lockout – temporarily lock accounts if too many denied authentication attempts occur.

Block/Unblock Users – block specific users from being able to receive MFA requests.

Fraud Alerts - Users can report fraudulent attempts to access their resources

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo, a search bar containing 'Search resources, services, and docs (G+)', and three icons: a square, a document, and a bell. Below the header, the breadcrumb navigation shows 'Home > Contoso > Security > Multi-Factor Authentication | Getting started'. The main title is 'Multi-Factor Authentication | Getting started' with a rocket icon. On the left, a sidebar menu has 'Getting started' (with a rocket icon) highlighted in grey, while 'Diagnose and solve problems' (with a cross icon) is unselected. A red rectangular box highlights the 'Settings' section, which contains the following items: 'Account lockout', 'Block/unblock users', 'Fraud alert', 'Notifications', 'OATH tokens', 'Phone call settings', and 'Providers'. To the right of the sidebar, there's a 'Got feedback?' link, followed by sections for 'Azure Multi-Factor Authentication' (with a sub-link 'Use MFA to protect your users and data.'), 'Configure' (with a sub-link 'Additional cloud-based MFA settings'), and 'Learn more' (with links to 'Deploy cloud-based Azure Multi-Factor Authentication', 'Configure Azure Multi-Factor Authentication', 'What is conditional access in Azure Active Directory?', and 'Best practices for conditional access in Azure Active Directory').

# Azure AD Conditional Access

Policy

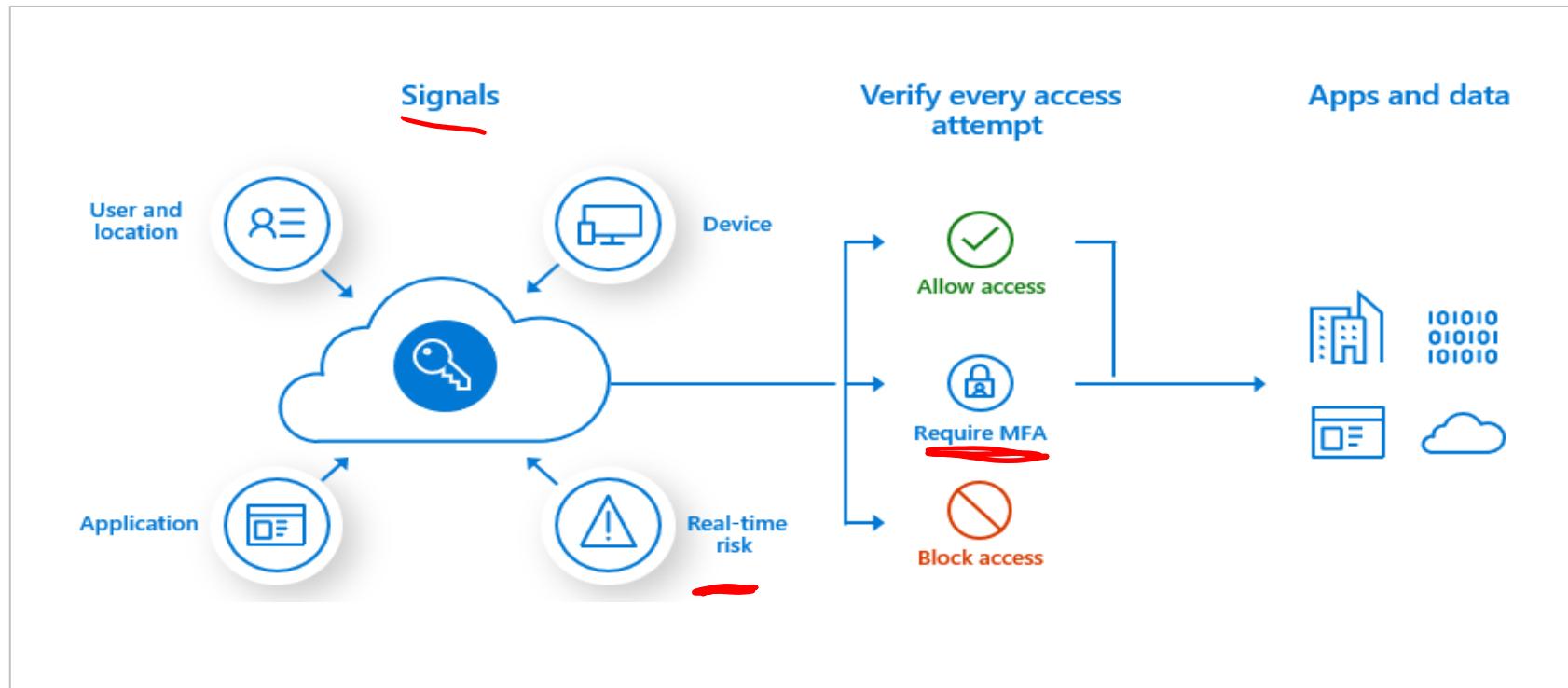
P2  
PIM  
Privileged Identity Manage

Identity management is the new control plane

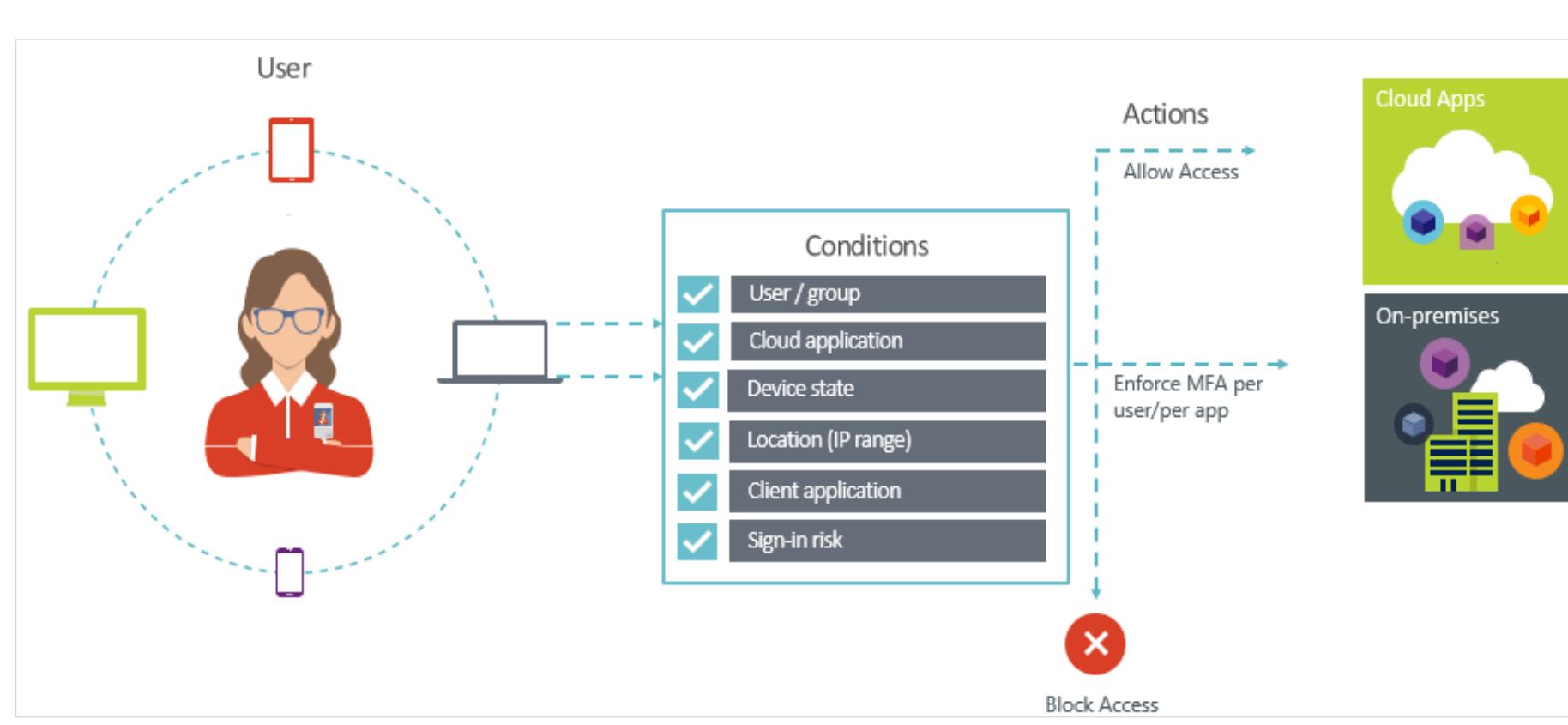
Use signals to make an informed decision

Base the decision on organizational policy

Enforce the decision across resources



# Conditions



**Conditions –**  
“When this happens”

**Access controls –**  
“Then do this”

Provides two step authentication verification

Lets you enforce controls on access to apps based on specific conditions

# Access Reviews

Enable organizations to recertify group memberships, application access, and privileged role assignments

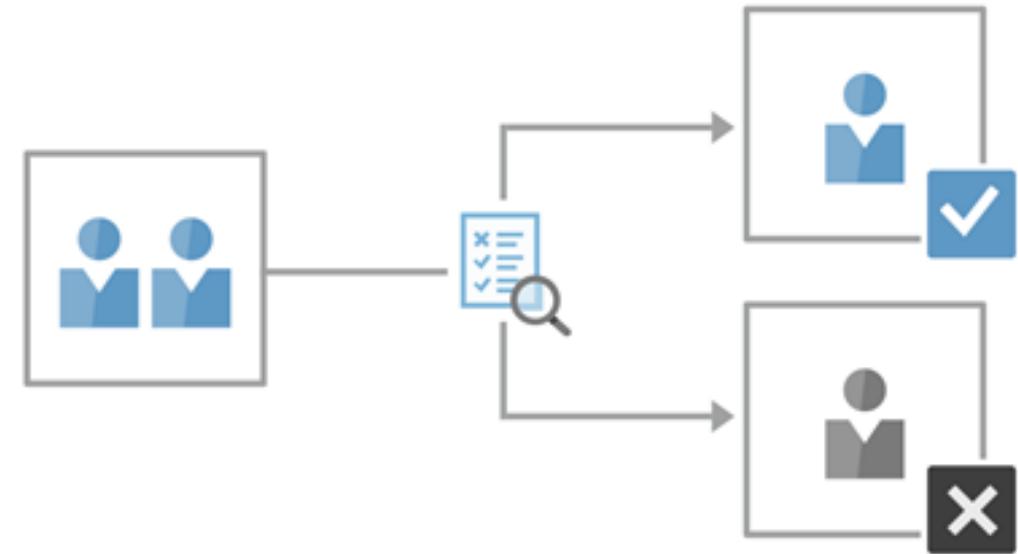
Evaluate guest user access

Evaluate employee access to applications and group membership

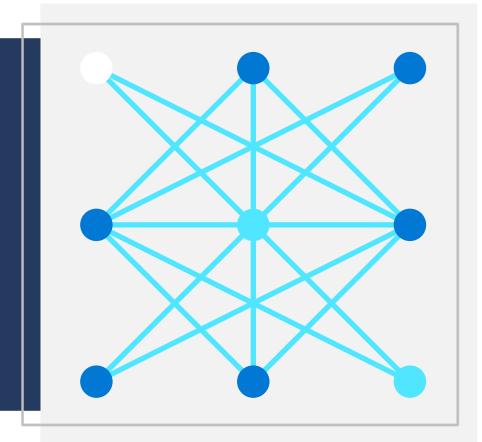
Track reviews for compliance or risk-sensitive applications

Evaluate the role assignment of administrative users (PIM)

Premium P2 license – Global admins or User Admins membership



# Privileged Identity Management



# Privileged Identity Management (PIM)



Microsoft's Zero Trust Model

---



Microsoft Identity Management Evolution

---



PIM Features

---



PIM Scope

---



PIM Onboarding

---



PIM Configuration Settings

---

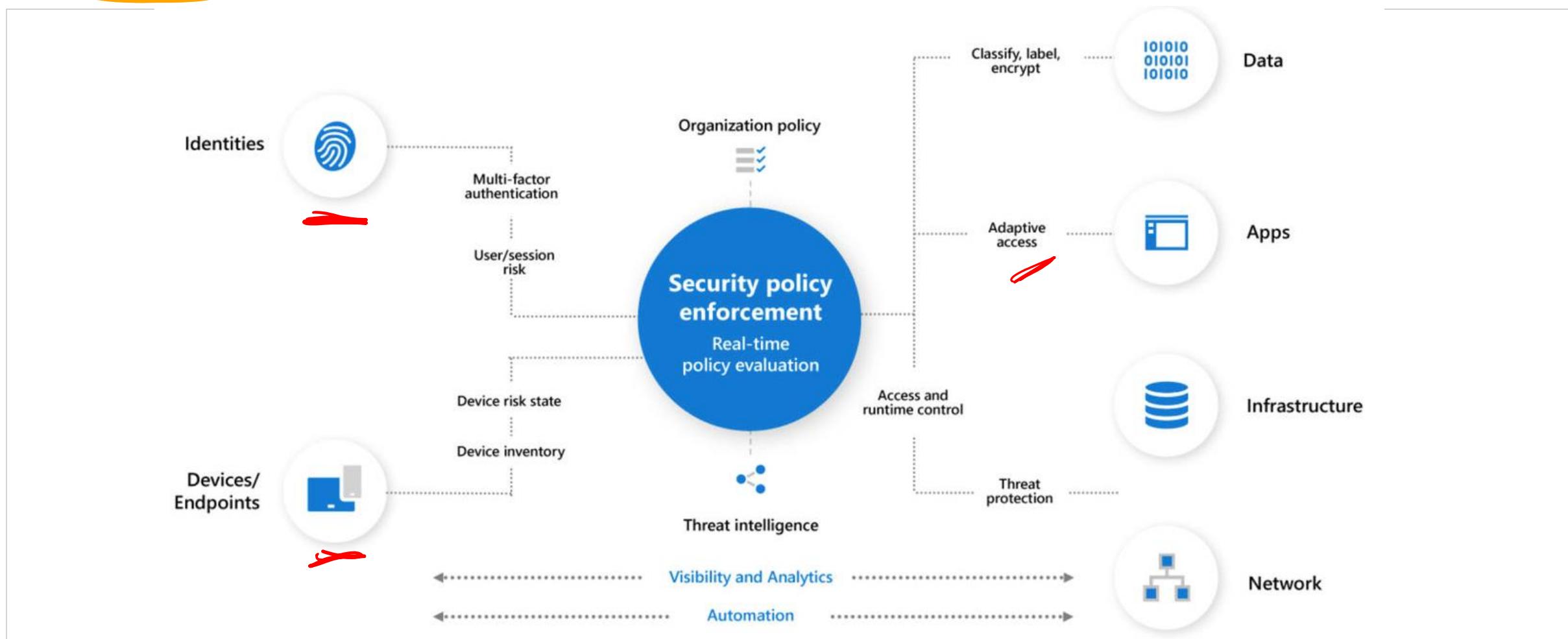


PIM Workflow

AAA

# Microsoft's Zero Trust Model

Assume breach and verify each request as though it originates from an open network



# Microsoft Identity Management Evolution

We recommend Azure AD Privileged Identity Management as the service to help protect your privileged accounts

## Traditional

- On-premises identity provider is in use
- No SSO is present between cloud and on-premises apps
- Visibility into identity risk is very limited

## Advanced

- Cloud identity federates with on-premises system
- Conditional access policies gate access and provide remediation actions
- Analytics improve visibility

## Optimal

- Password less authentication is enabled
- User, device, location and behavior is analyzed in real time to determine risk and deliver ongoing protection
- MFA is enforced

# Azure AD Privileged Identity Management (PIM)

→ Cosmos · DB

Time-based and approval-based role activation for privileged users

Just-in-time privileged access  
to Azure



Time-bound access to  
resources



Approval to activate privileged  
roles

Multi-factor authentication to  
activate any role

Justification to understand why  
users activate

Notifications when privileged  
roles are activated

Access reviews to ensure users  
still need roles

Audit history for internal or  
external audit

# PIM Scope

## Azure AD Roles

Assign users to a role – users must elevate to use the privileges granted by the role

Prioritize protecting Azure AD roles that have the greatest number of permissions

## Azure resources

Identify the management groups and subscriptions

Resources most vital for your organization or host the most sensitive data

Resources that core, customer-facing applications depend on - PIM will help you discover these resources

## Privileged Identity Management

Privileged Identity Management

### Manage

 Azure AD roles

 Azure resources

Which Azure AD roles and resources should be protected with PIM?

# PIM Onboarding

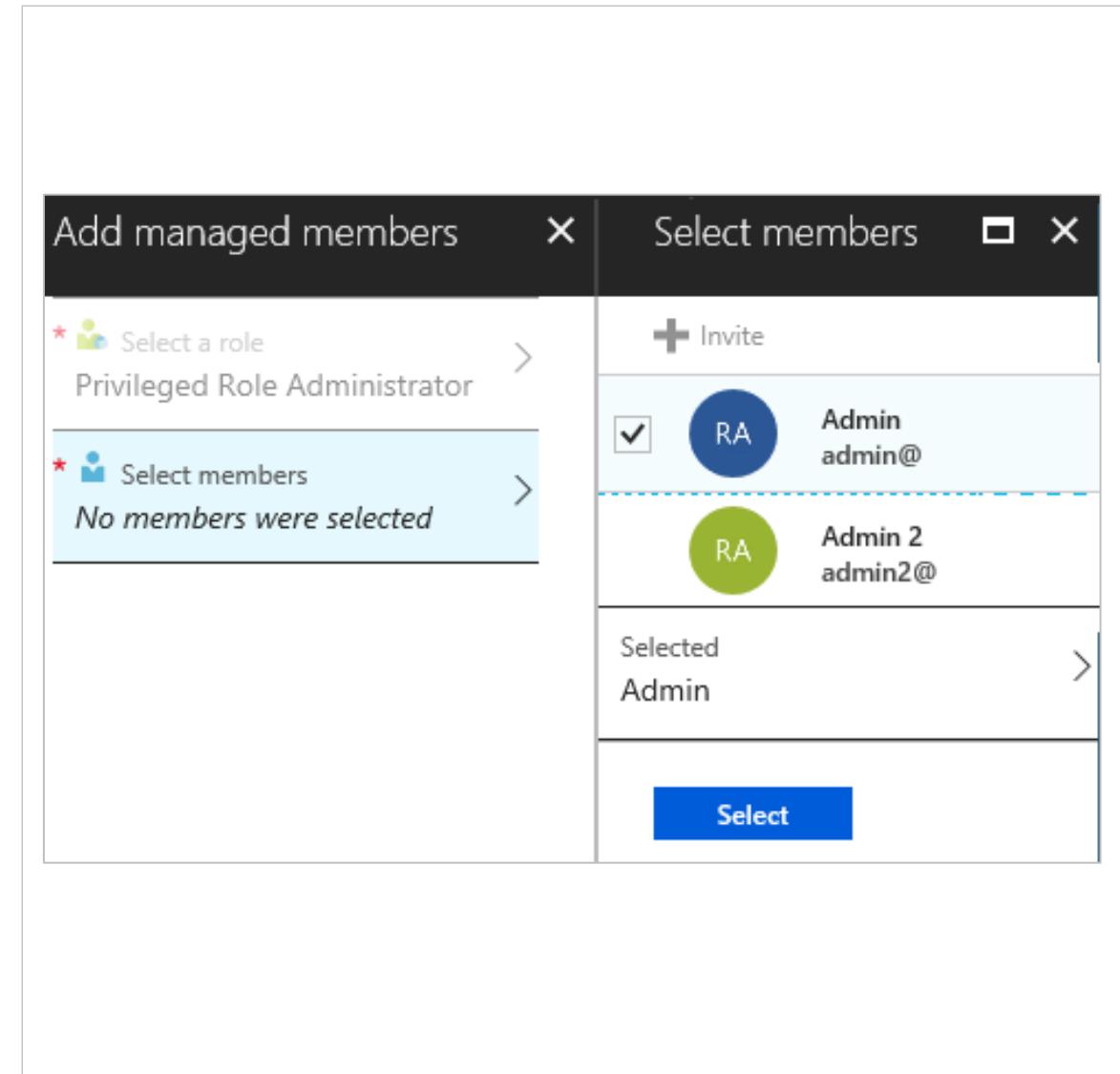
PIM automatically enable when a privileged role goes into **PIM** or **Roles and Administrators**

The Global administrator (first user) who enables PIM gets write access

The first user can assign others to the Privileged Role Administrator

Global administrators (not first user), Security administrators, and Security readers have read-only access

Ensure there are always at least two Privileged Role Administrators



# PIM Configuration Settings

Settings can be different for Azure AD roles and Azure resources

## Activation

Activation maximum duration (hours)

0  1  24  48  72  96  120  144  168  192  240  288  336  360  432  468  504  540  576  600  648  684  720  756  792  828  864  900  936  972  1008  1044  1080  1104  1140  1176  1200  1248  1284  1320  1356  1392  1428  1464  1500  1536  1572  1608  1644  1680  1716  1752  1788  1824  1860  1896  1932  1968  2004  2040  2076  2112  2148  2184  2220  2256  2292  2328  2364  2400  2436  2472  2508  2544  2580  2616  2652  2688  2724  2760  2796  2832  2868  2904  2940  2976  3012  3048  3084  3120  3156  3192  3228  3264  3300  3336  3372  3408  3444  3480  3516  3552  3588  3624  3660  3696  3732  3768  3804  3840  3876  3912  3948  3984  4020  4056  4092  4128  4164  4200  4236  4272  4308  4344  4380  4416  4452  4488  4524  4560  4596  4632  4668  4704  4740  4776  4812  4848  4884  4920  4956  4992  5028  5064  5100  5136  5172  5208  5244  5280  5316  5352  5388  5424  5460  5496  5532  5568  5604  5640  5676  5712  5748  5784  5820  5856  5892  5928  5964  6000  6036  6072  6108  6144  6180  6216  6252  6288  6324  6360  6396  6432  6468  6504  6540  6576  6612  6648  6684  6720  6756  6792  6828  6864  6900  6936  6972  7008  7044  7080  7116  7152  7188  7224  7260  7296  7332  7368  7404  7440  7476  7512  7548  7584  7620  7656  7692  7728  7764  7800  7836  7872  7908  7944  7980  8016  8052  8088  8124  8160  8196  8232  8268  8304  8340  8376  8412  8448  8484  8520  8556  8592  8628  8664  8700  8736  8772  8808  8844  8880  8916  8952  8988  9024  9060  9096  9132  9168  9204  9240  9276  9312  9348  9384  9420  9456  9492  9528  9564  9600  9636  9672  9708  9744  9780  9816  9852  9888  9924  9960  9996  10032  10068  10104  10140  10176  10212  10248  10284  10320  10356  10392  10428  10464  10500  10536  10572  10608  10644  10680  10716  10752  10788  10824  10860  10896  10932  10968  11004  11040  11076  11112  11148  11184  11220  11256  11292  11328  11364  11400  11436  11472  11508  11544  11580  11616  11652  11688  11724  11760  11796  11832  11868  11904  11940  11976  12012  12048  12084  12120  12156  12192  12228  12264  12300  12336  12372  12408  12444  12480  12516  12552  12588  12624  12660  12696  12732  12768  12804  12840  12876  12912  12948  12984  13020  13056  13092  13128  13164  13200  13236  13272  13308  13344  13380  13416  13452  13488  13524  13560  13596  13632  13668  13704  13740  13776  13812  13848  13884  13920  13956  13992  14028  14064  14100  14136  14172  14208  14244  14280  14316  14352  14388  14424  14460  14496  14532  14568  14604  14640  14676  14712  14748  14784  14820  14856  14892  14928  14964  15000  15036  15072  15108  15144  15180  15216  15252  15288  15324  15360  15396  15432  15468  15504  15540  15576  15612  15648  15684  15720  15756  15792  15828  15864  15900  15936  15972  16008  16044  16080  16116  16152  16188  16224  16260  16296  16332  16368  16404  16440  16476  16512  16548  16584  16620  16656  16692  16728  16764  16800  16836  16872  16908  16944  16980  17016  17052  17088  17124  17160  17196  17232  17268  17304  17340  17376  17412  17448  17484  17520  17556  17592  17628  17664  17700  17736  17772  17808  17844  17880  17916  17952  17988  18024  18060  18096  18132  18168  18204  18240  18276  18312  18348  18384  18420  18456  18492  18528  18564  18600  18636  18672  18708  18744  18780  18816  18852  18888  18924  18960  18996  19032  19068  19104  19140  19176  19212  19248  19284  19320  19356  19392  19428  19464  19500  19536  19572  19608  19644  19680  19716  19752  19788  19824  19860  19896  19932  19968  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540  19576  19612  19648  19684  19720  19756  19792  19828  19864  19900  19936  19972  19000  19036  19072  19108  19144  19180  19216  19252  19288  19324  19360  19396  19432  19468  19504  19540

# PIM Workflow

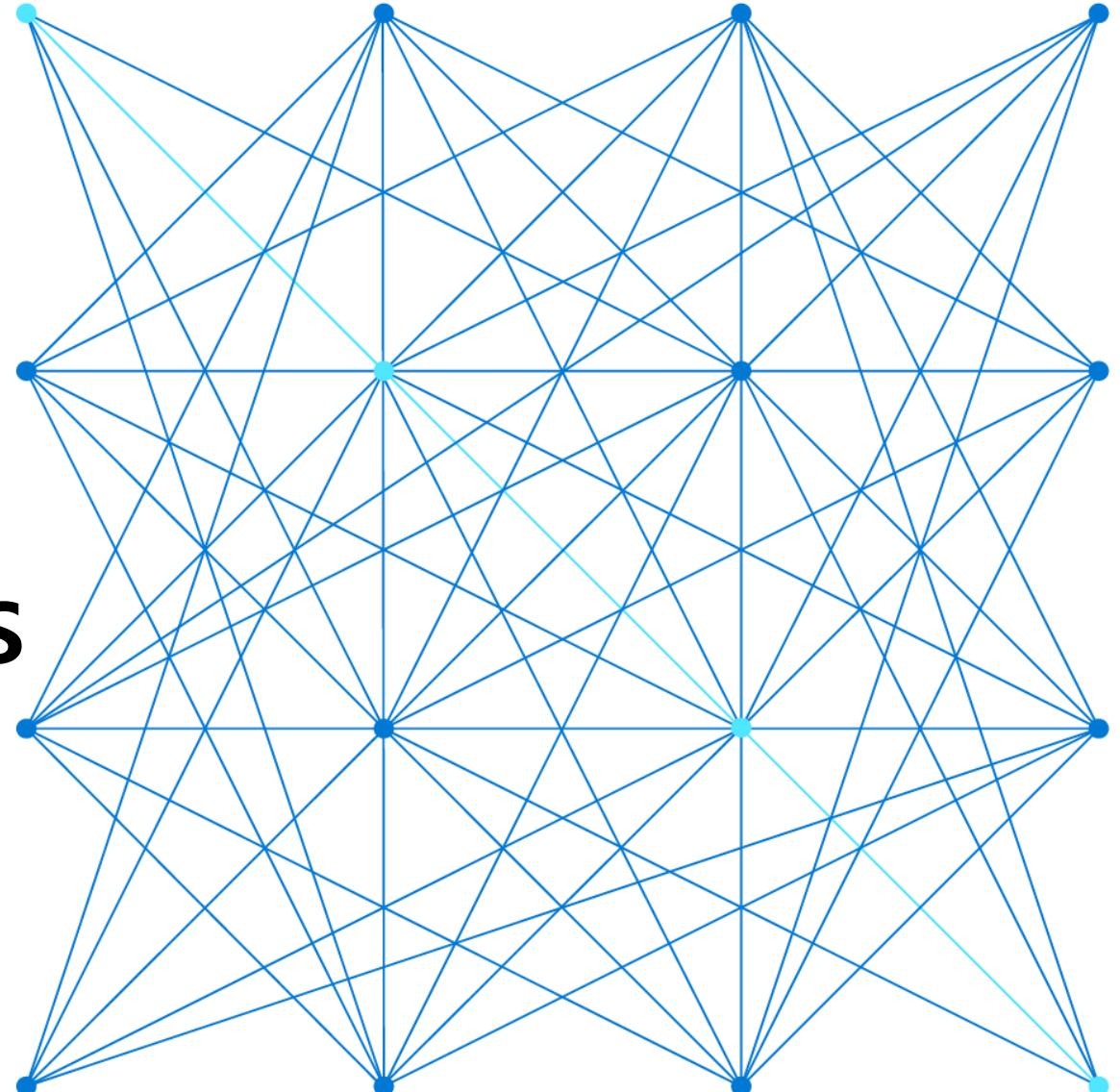
PIM Administrator		PIM User	PIM Approver	PIM Administrator
 Plan	 Assign	 Activate	 Approve	 Audit
Determine users and roles that will be managed by PIM.	Assign users or current admins as eligible admins for specific Azure AD roles, so they only have access when necessary.	Activate your eligible admin roles so they can get limited access to the privileged identity.	View and approve all activation requests for specific Azure AD roles that you are configured to approve.	View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant.

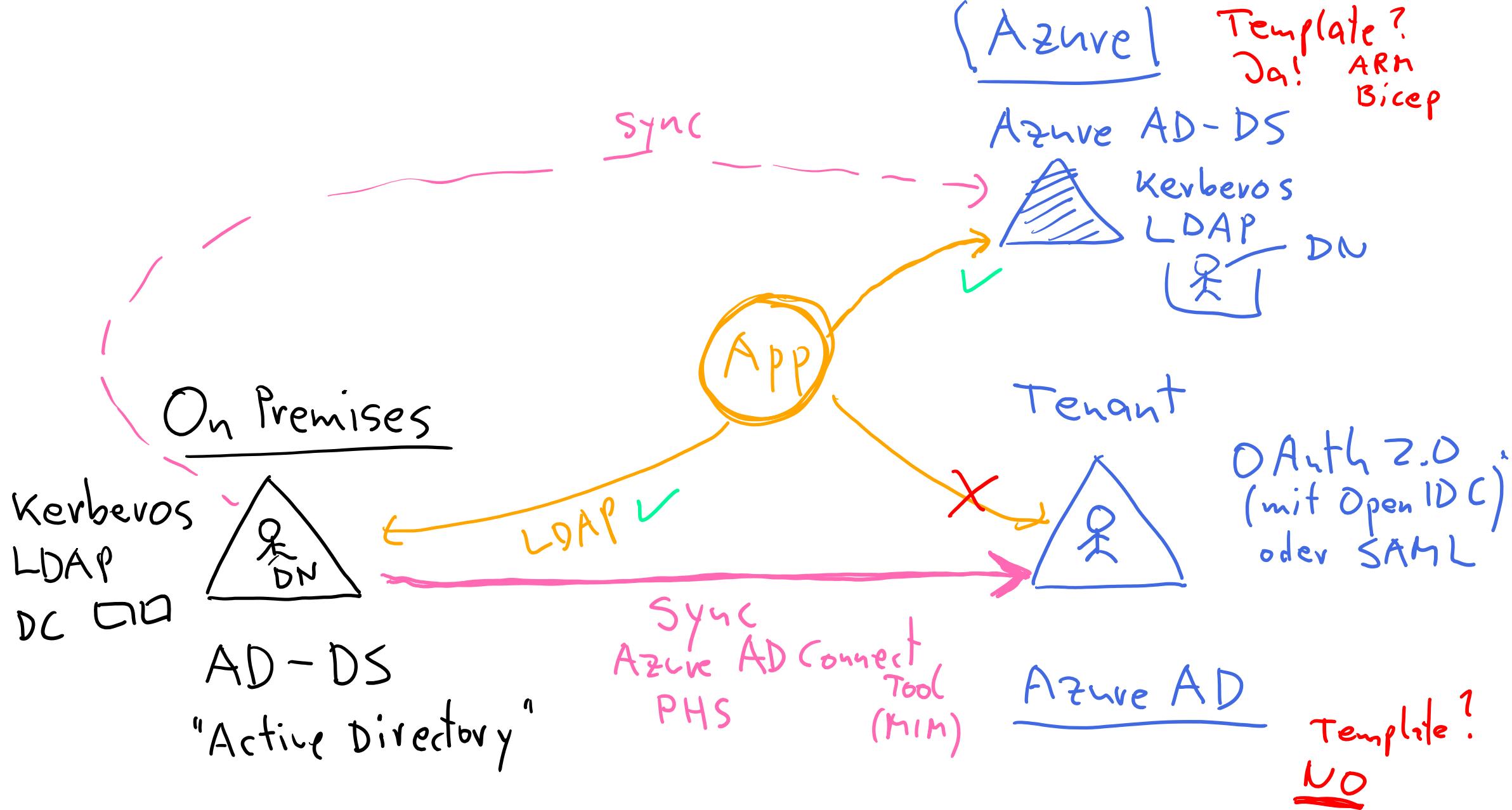
AZ-500

Tag 2

# Microsoft Azure Security Technologies

Guten Morgen!





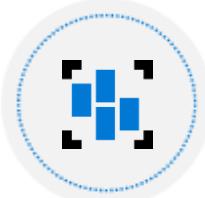
# AZ-500 Agenda



**Learning Path 1   Identity and Access**



**Learning Path 2   Implement Platform Protection**



**Learning Path 3   Data and Application Security**



**Learning Path 4   Security Operations**

# Learning Path: 1 Identity and Access



Azure Active Directory



Hybrid Identity

△ → △  
Tenant



Azure AD Identity Protection

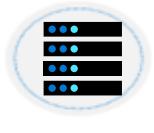
Risk



Azure AD Privileged Identity Management



Enterprise Governance



Application Security

Managed ID



Module Labs

# Application Security



# Application Security



Microsoft Identity Platform



Azure AD Application Scenarios



App Registration



Microsoft Graph Permissions



Managed Identities



Web App Certificates

# Microsoft Identity Platform

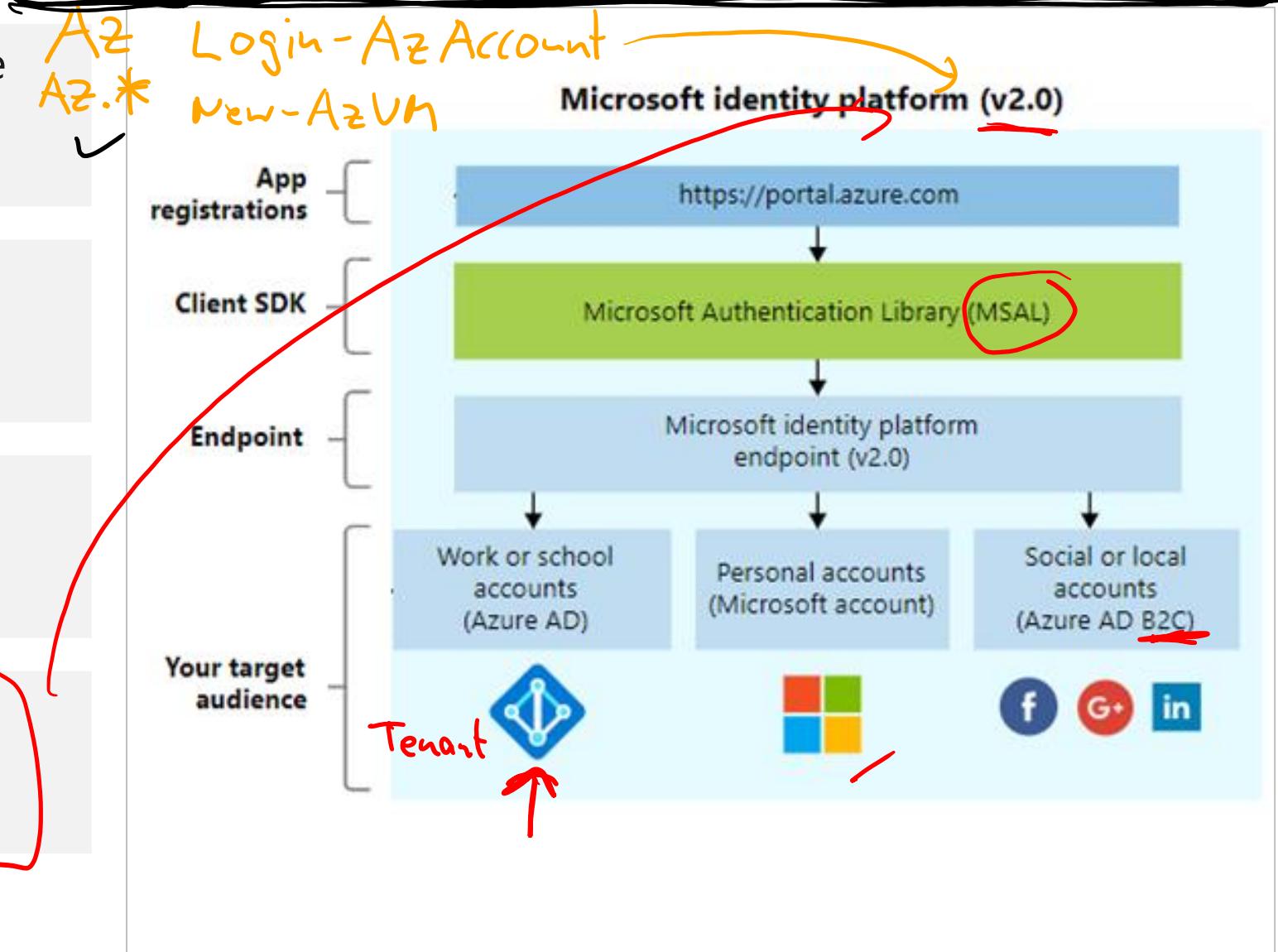
Azure AD Connect-AzureAD Azure AD Graph → V1.0 (ADAL)

Write code once and authenticate any Microsoft identity into your application

Simple to use, provides a single sign-on experience

Use the portal to register and configure your application

Use the Microsoft Graph API for programmatic application configuration



# Azure AD Application Scenarios

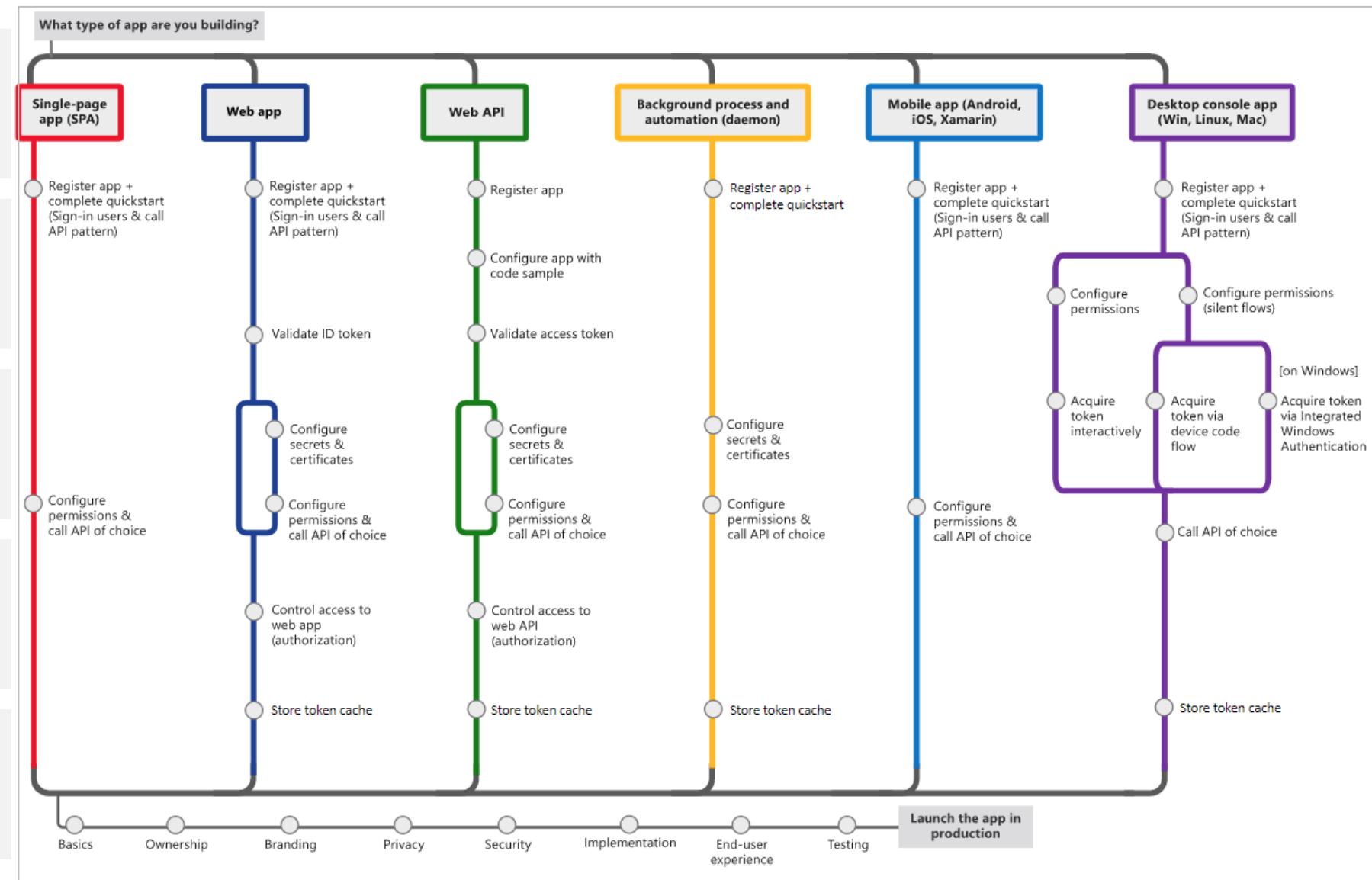
Single page frontends  
that run in a browser

Web browser to a web  
application

Web API on behalf of a  
user

Web applications that  
need resources from a  
web API

Daemon or server  
application that needs  
resources from a web API



# App Registration

Any application that outsources authentication to Azure AD must be registered in a directory

Registration creates token information including a unique application id.

Home > App registrations >

## Register an application

**⚠️** If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. [Read our decision guide ↗](#)

\* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Microsoft only - Single tenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)  
 Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web  e.g. <https://example.com/auth>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the Microsoft Platform Policies [↗](#)

**Register**

# Microsoft Graph Permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process

Delegated permissions are used by apps that have a signed-in user present

Application permissions are used by apps that run without a signed-in user present

Request API permissions

Select an API

[Microsoft APIs](#)   [APIs my organization uses](#)   [My APIs](#)

Commonly used Microsoft APIs

 **Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 **Azure Batch**  
Schedule large-scale parallel and HPC applications in the cloud

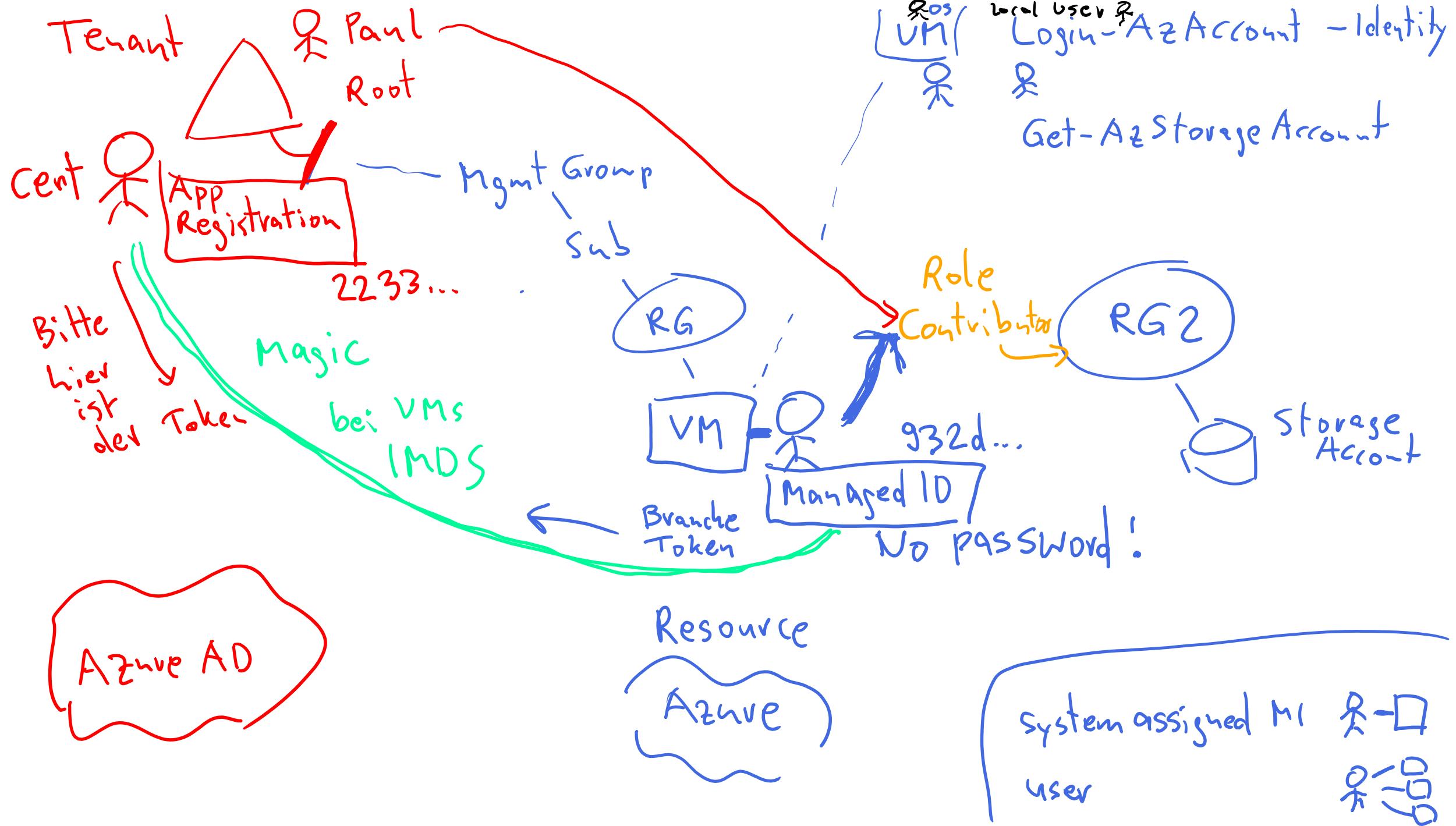
 **Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets

 **Azure Data Explorer**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

 **Azure Data Explorer (with Multifactor Authentication)**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

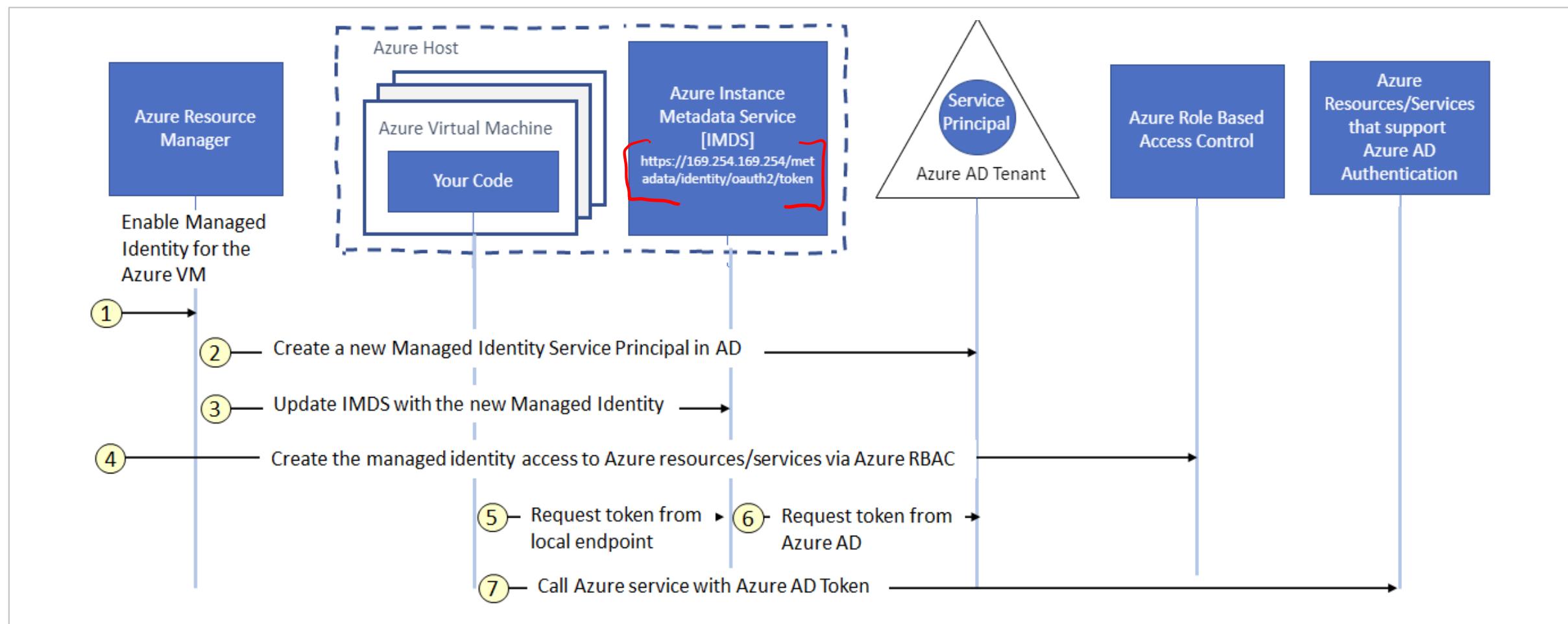
 **Azure Key Vault**  
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

 **Azure Storage**  
Secure, massively scalable object and data lake storage for unstructured and semi-structured data



# Managed Identities

Managed identities use Azure AD authentication to authenticate services – no code in the application. Identities can be system-assigned or user-assigned.



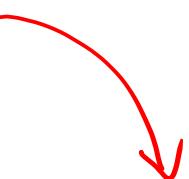
# Azure App Services Overview



PaaS

# App Services

Code  
CI/CD



Microsoft  
.NET



JS



Go Ruby



# App Service Environments

The ASE is a single tenant deployment of the Azure App Service that runs in your virtual network.

Internal line-of-business applications

Applications that need more than 30 App Service plan instances

Single tenant system to satisfy internal compliance or security requirements

Network isolated application housing

Multi-tier applications



App Service  
Environments

# App Service Plans

An App Service plan defines a set of compute resources for a web app to run.

Operating System (Windows, Linux)

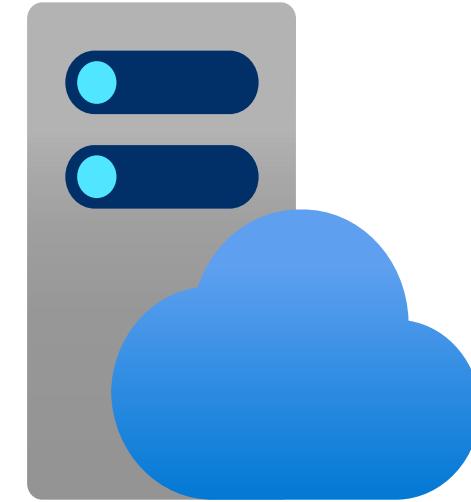
Region (West US, East US, etc.)

Number of VM instances

Size of VM instances (Small, Medium, Large)

Pricing tier (Free, Shared Basic, Standard, Premium, PremiumV2, V3, Isolated, Isolated V2)

Deployment slots



# App Service Plans

# App Service Environment Networking

An App Service Environment has the following network information at creation:

App Service Environment Subnet

Domain Suffix

Virtual IP (VIP)

Inbound Address

Default Outbound Address

The screenshot shows the Azure portal interface with the following details:

- IP Addresses**: Lists networking configuration for the App Service Environment.
  - ASE virtual network: azurewebappsvc
  - ASE subnet: azurewebappsvc\_1a
  - Domain suffix: azurewebappsvc.appserviceenvironment.net
- Inbound**:
  - Virtual IP: Internal
  - Inbound address: 192.168.250.4
- Outbound**: Default outbound addresses: 20.102.34.209, 20.102.34.146

The left sidebar shows the navigation menu for the 'IP addresses' section of the 'azurewebappsvc' App Service Environment.

# Availability Zone Support for App Service Environments

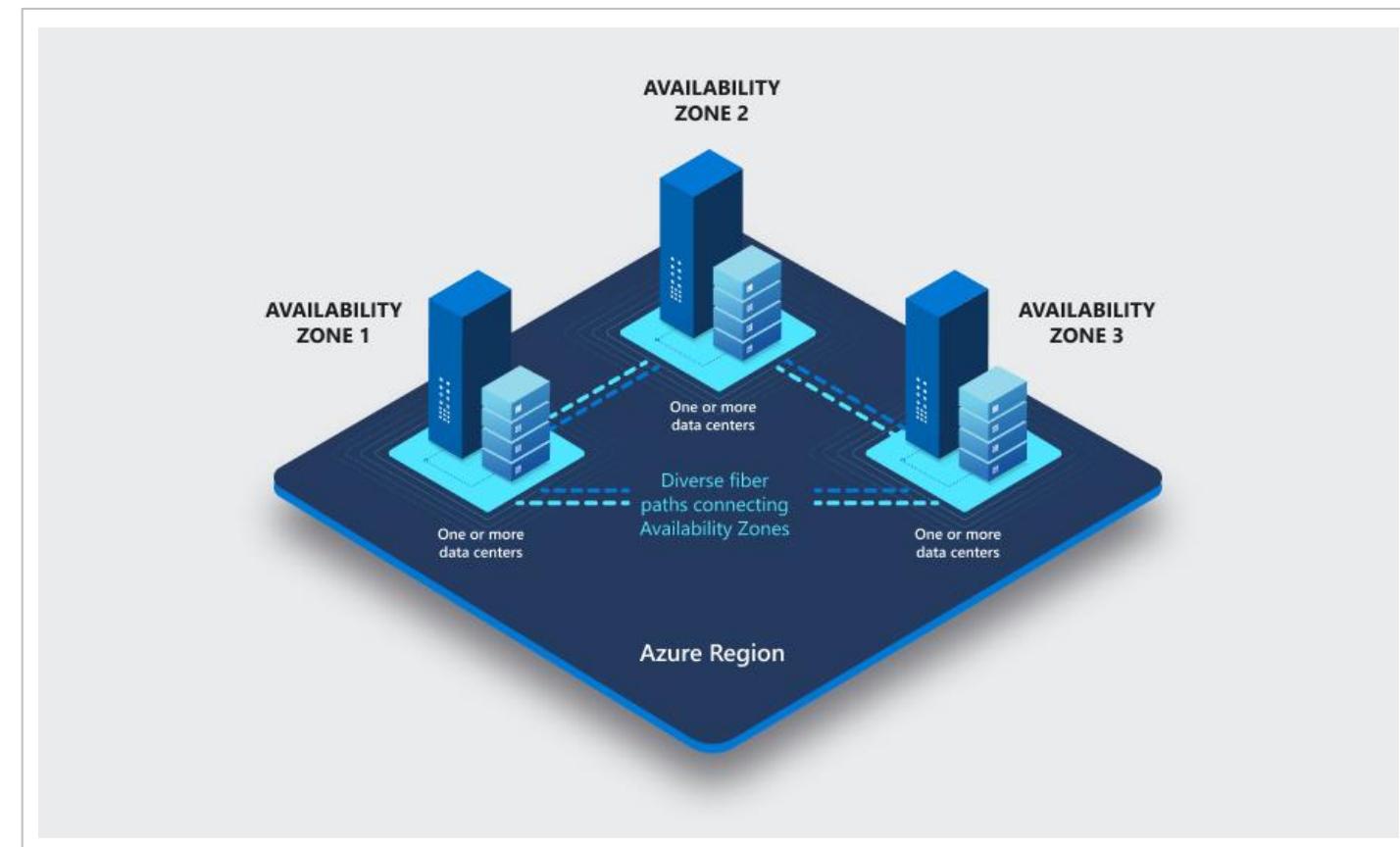
App services can be deployed across availability zones. The architecture is known as zone redundancy.

Azure regions feature datacenters deployed within a latency-defined perimeter.

Availability Zones are connected through a dedicated regional low-latency network.

Tolerance to failures is achieved because of redundancy and logical isolation of Azure services.

To ensure resiliency, a minimum of three separate availability zones are present in all availability zone-enabled regions.



# App Service Environment Certificates

The following options are available to enable certificates in App Service.

Create a free App Service managed certificate

Purchase an App Service certificate

Import a certificate from Key Vault

Upload a private certificate

Upload a public certificate

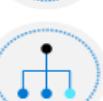


App Service  
Certificates

# Enterprise Governance



# Enterprise Governance

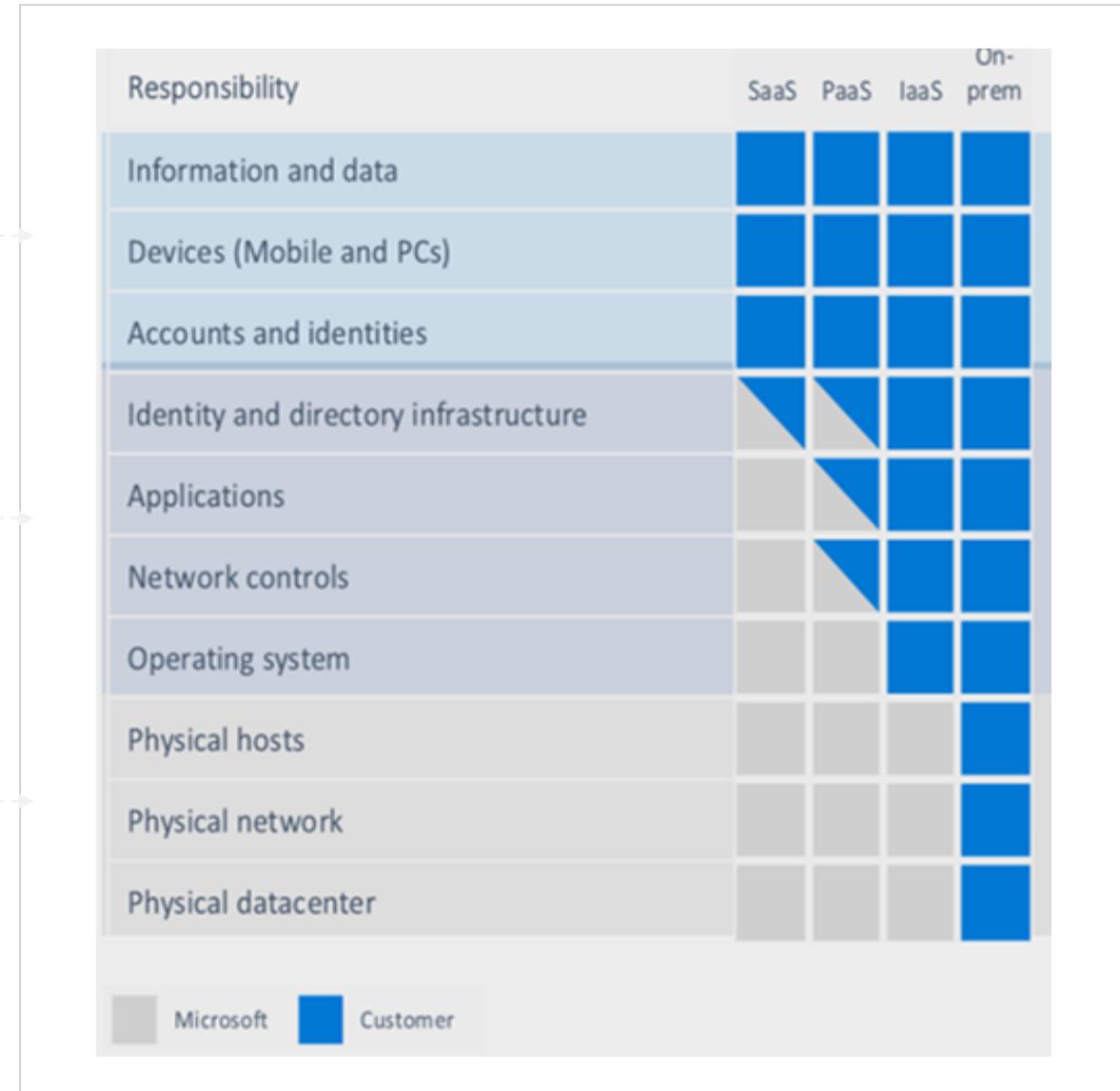
-  Shared Responsibility Model
-  Azure Cloud Security Advantages
-  Azure Hierarchy
-  Azure Policy
-  Azure Role Based Access Control (RBAC)
-  Azure RBAC vs Azure Policies
-  Built-in Roles
-  Resource Locks
-  Azure Blueprints
-  Azure Subscription Management

# Shared Responsibility Model

Responsibility always retained by the customer

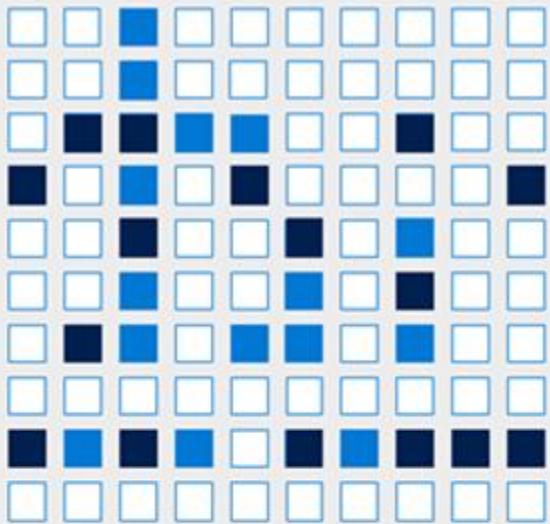
Responsibility varies by service type

Responsibility transfers to cloud provider

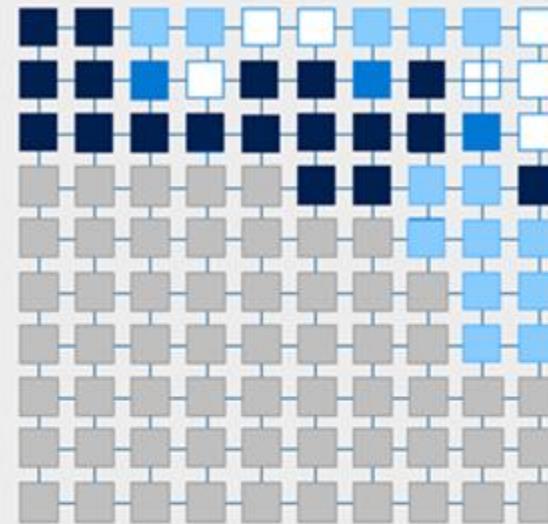


# Azure Cloud Security Advantages

## Traditional Approach



## Cloud-Enabled Approach



Security is a challenging and under-resourced function

- Satisfied responsibility
- Partially met responsibility

- Unmet responsibility
- Cloud provider responsibility

Cloud Technology enables security to:

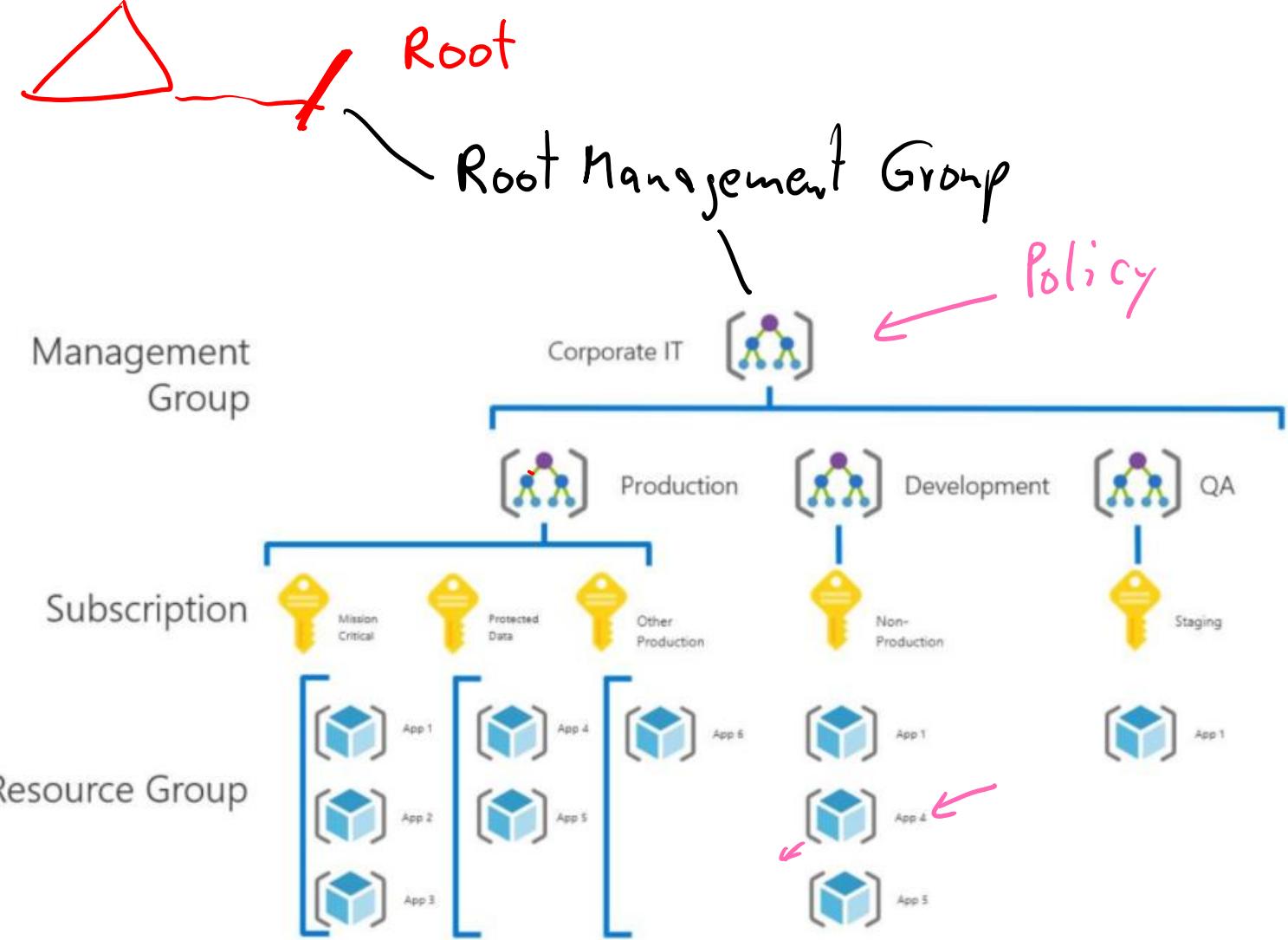
- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use cloud intelligence to improve detection/response time

# Azure Hierarchy

Management groups provides a level to manage multiple subscriptions

Subscriptions provision products and services for an account

Resource groups are containers for resources that share the same life cycle



# Azure Policy

Azure Policy is a service in Azure that you use to create, assign and, manage policies

Azure Policy runs evaluations and scans for non-compliant resources

Advantages:

- Enforcement and compliance
- Apply policies at scale
- Remediation

## Usage Cases

**Allowed resource types** - Specify the resource types that your organization can deploy.

**Allowed virtual machine SKUs** – Specify a set of virtual machine SKUs that your organization can deploy.

**Allowed locations** – Restrict the locations your organization can specify when deploying resources.

**Require tag and its value** - Enforces a required tag and its value.

**Azure Backup should be enabled for Virtual Machines** – Audit if Azure Backup service is enabled for all Virtual machines.

B Series

# Azure Policy – Storage

Microsoft Azure Search resources, services, and docs (G+) 1 ? Export

Home > Secure transfer to storage accounts should be enabled ...

Policy definition

Assign Edit definition Duplicate definition Delete definition Export definition

Essentials

Name	: Secure transfer to storage accounts should be enabled	Definition location	: --
Description	: Audit requirement of Secure transfer in your storage account. Secure transfer is an option tha...	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/404c3081-a854-4457-ae30-26a93ef6...
Available Effects	: Audit, Deny, Disabled	Type	: Built-in
Category	: Storage	Mode	: Indexed

Definition Assignments (0) Parameters

```
1 {
2   "properties": {
3     "displayName": "Secure transfer to storage accounts should be enabled",
4     "policyType": "BuiltIn",
5     "mode": "Indexed",
6     "description": "Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from s",
7     "metadata": {
8       "version": "2.0.0",
9       "category": "Storage"
10    },
11    "parameters": {
12      "effect": {
13        "type": "String",
14        "metadata": {
15          "displayName": "Effect",
16          "description": "The effect determines what happens when the policy rule is evaluated to match"
17        },
18        "allowedValues": [
19          "Audit",
20          "Deny",
21        ]
22      }
23    }
24  }
```

# Azure Policy – SQL

Microsoft Azure Search resources, services, and docs (G+) 1 ? ?

Home > Deploy Advanced Data Security on SQL servers X

Policy definition

Assign Edit definition Duplicate definition Delete definition Export definition

Essentials

Name : Deploy Advanced Data Security on SQL servers	Definition location : --
Description : This policy enables Advanced Data Security on SQL Servers. This includes turning on Threat D...	Definition ID : /providers/Microsoft.Authorization/policyDefinitions/6134c3db-786f-471e-87bc-8f479dc8...
Available Effects : DeployIfNotExists	Type : Built-in
Category : SQL	Mode : Indexed

Definition Assignments (0)

```
1  {
2    "properties": {
3      "displayName": "Deploy Advanced Data Security on SQL servers",
4      "policyType": "BuiltIn",
5      "mode": "Indexed",
6      "description": "This policy enables Advanced Data Security on SQL Servers. This includes turning on Threat Detection and Vulnerability Assessment. It will automatically c",
7      "metadata": {
8        "version": "1.2.0",
9        "category": "SQL"
10      },
11      "parameters": {},
12      "policyRule": {
13        "if": {
14          "field": "type",
15          "equals": "Microsoft.Sql/servers"
16        },
17        "then": {
18          "effect": "DeployIfNotExists",
19          "details": {
20            "type": "Microsoft.Sql/servers/securityAlertPolicies",
21            "name": "Deploy Advanced Data Security on SQL servers"
22          }
23        }
24      }
25    }
26  }
```

# Azure Policy – Kubernetes

Microsoft Azure Search resources, services, and docs (G+) 1 ? Export

Home > Kubernetes clusters should not use specific security capabilities ...

Policy definition

Assign Edit definition Duplicate definition Delete definition Export definition

Essentials

Name	: Kubernetes clusters should not use specific security capabilities	Definition location	:	--
Description	: Prevent specific security capabilities in Kubernetes clusters to prevent ungranted privileges o...	Definition ID	:	/providers/Microsoft.Authorization/policyDefinitions/a27c700f-8a22-44ec-961c-41625264...
Available Effects	: audit, deny, disabled	Type	:	Built-in
Category	: Kubernetes	Mode	:	Microsoft.Kubernetes.Data

Definition Assignments (0) Parameters

```
1 {  
2   "properties": {  
3     "displayName": "Kubernetes clusters should not use specific security capabilities",  
4     "policyType": "BuiltIn",  
5     "mode": "Microsoft.Kubernetes.Data",  
6     "description": "Prevent specific security capabilities in Kubernetes clusters to prevent ungranted privileges on the Pod resource. For more information, see https://aka.ms",  
7     "metadata": {  
8       "version": "3.0.2",  
9       "category": "Kubernetes"  
10    },  
11    "parameters": {  
12      "effect": {  
13        "type": "String",  
14        "metadata": {  
15          "displayName": "Effect",  
16          "description": "'audit' allows a non-compliant resource to be created or updated, but flags it as non-compliant. 'deny' blocks the non-compliant resource creation o  
17        },  
18        "allowedValues": [  
19          "audit",  
20          "deny",  
21        ]  
22      }  
23    }  
24  }  
25}
```

# Azure Policy – Key Vault

Microsoft Azure Search resources, services, and docs (G+/-) 1 ? Help Feedback

Home > Keys should be backed by a hardware security module (HSM) ...

Policy definition

Assign Edit definition Duplicate definition Delete definition Export definition

Essentials

Name : Keys should be backed by a hardware security module (HSM)	Definition location : --
Description : An HSM is a hardware security module that stores keys. An HSM provides a physical layer of ...	Definition ID : /providers/Microsoft.Authorization/policyDefinitions/587c79fe-dd04-4a5e-9d0b-f89598c7...
Available Effects : Audit, Deny, Disabled	Type : Built-in
Category : Key Vault	Mode : Microsoft.KeyVault.Data

Definition Assignments (0) Parameters

```
1 {  
2   "properties": {  
3     "displayName": "Keys should be backed by a hardware security module (HSM)",  
4     "policyType": "BuiltIn",  
5     "mode": "Microsoft.KeyVault.Data",  
6     "description": "An HSM is a hardware security module that stores keys. An HSM provides a physical layer of protection for cryptographic keys. The cryptographic key cannot",  
7     "metadata": {  
8       "version": "1.0.1",  
9       "category": "Key Vault"  
10    },  
11    "parameters": {  
12      "effect": {  
13        "type": "String",  
14        "metadata": {  
15          "displayName": "Effect",  
16          "description": "'Audit' allows a non-compliant resource to be created, but flags it as non-compliant. 'Deny' blocks the resource creation. 'Disable' turns off the p",  
17        },  
18        "allowedValues": [  
19          "Audit",  
20          "Deny",  
21        ]  
22      }  
23    }  
24  }  
25}
```

# Azure Role-Based Access Control

	Role					
	Reader	Resource-specific	Custom	Contributor	Owner	
Scope	 Management group	Observers	Users managing resources			
 Subscription					Admins	
 Resource group						
 Resource	Automated processes					

# Azure Role-Based Access Control – Security Principal

1

Security principal



User



Group

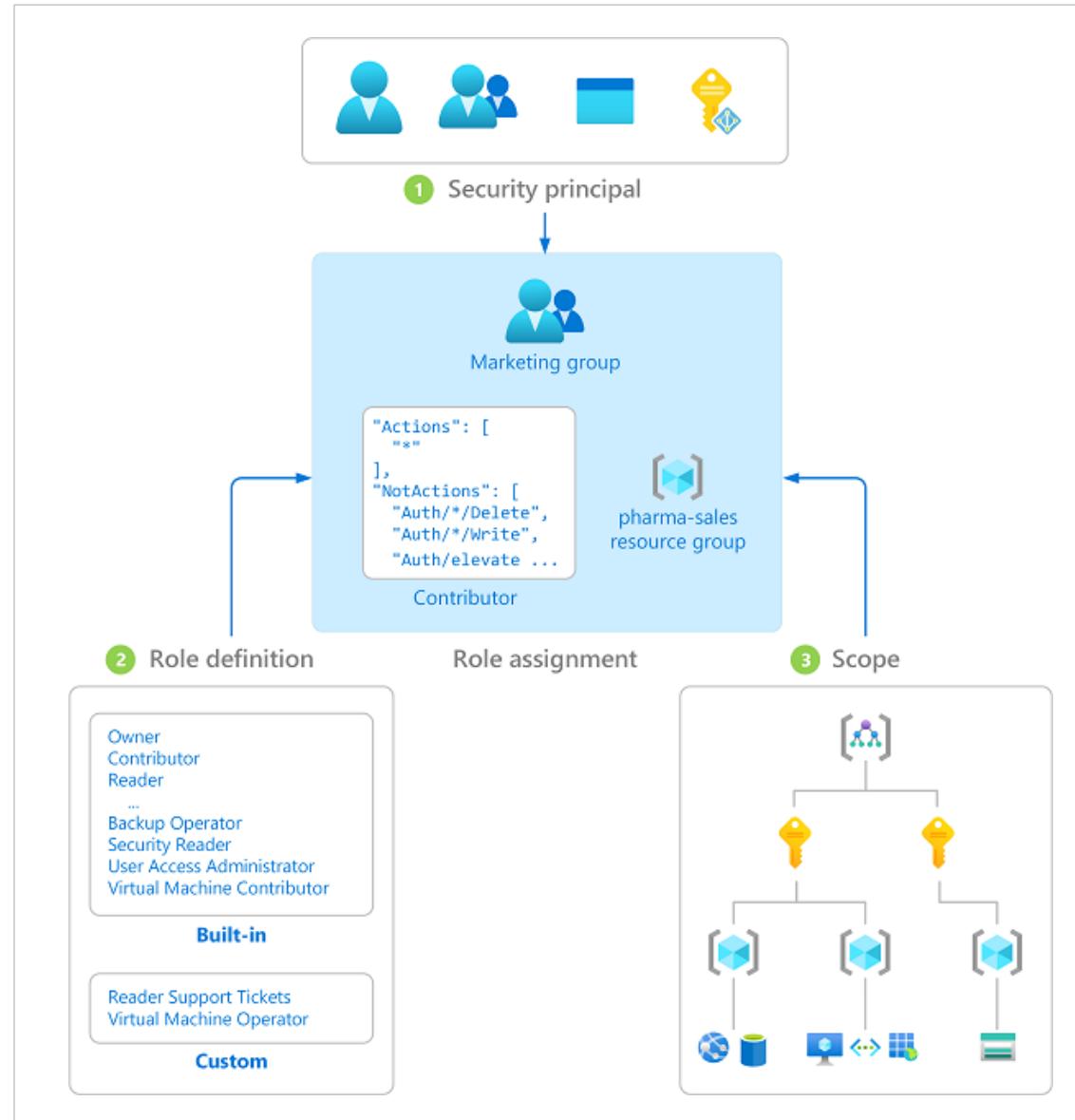


Service  
principal

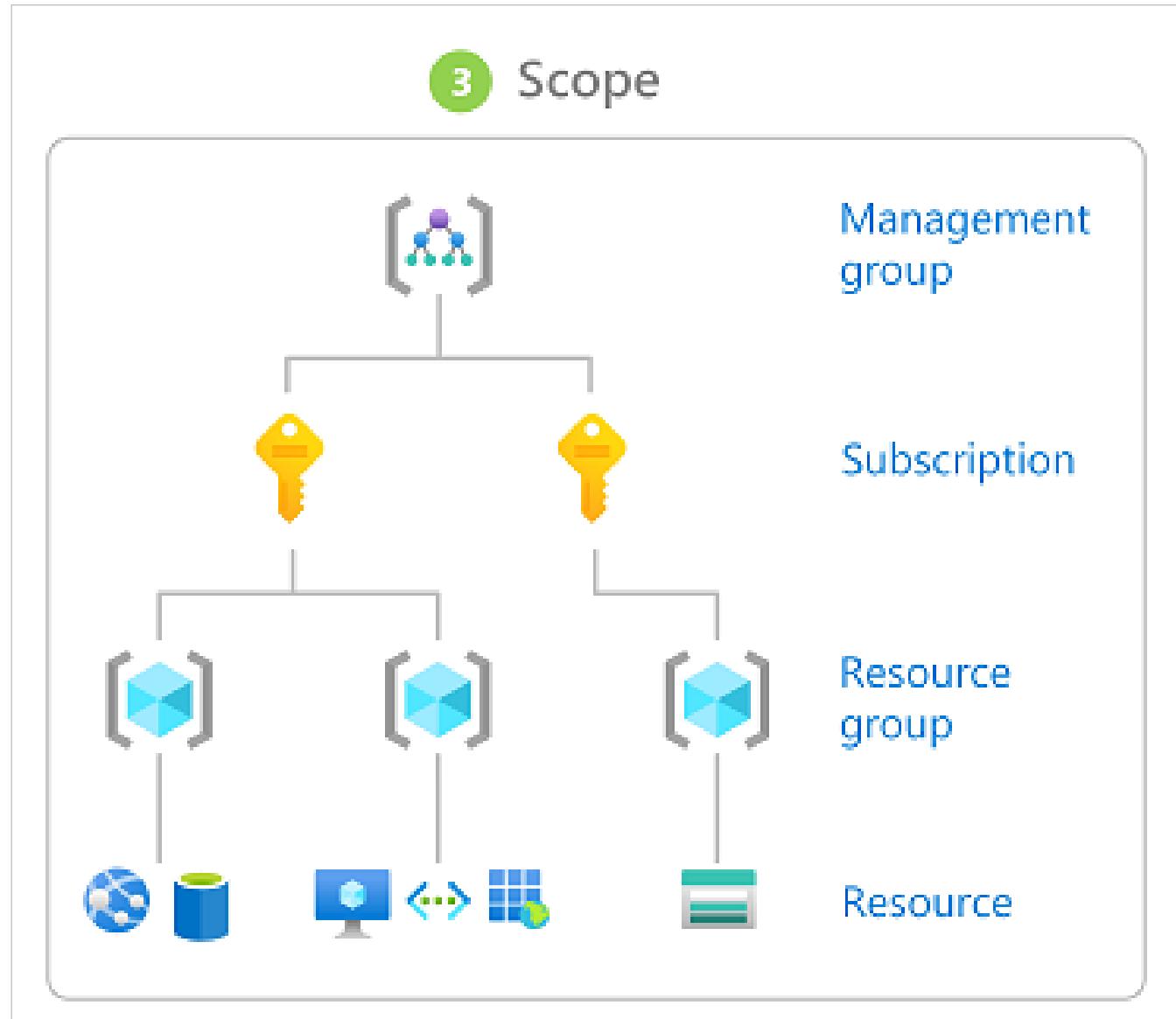


Managed  
identity

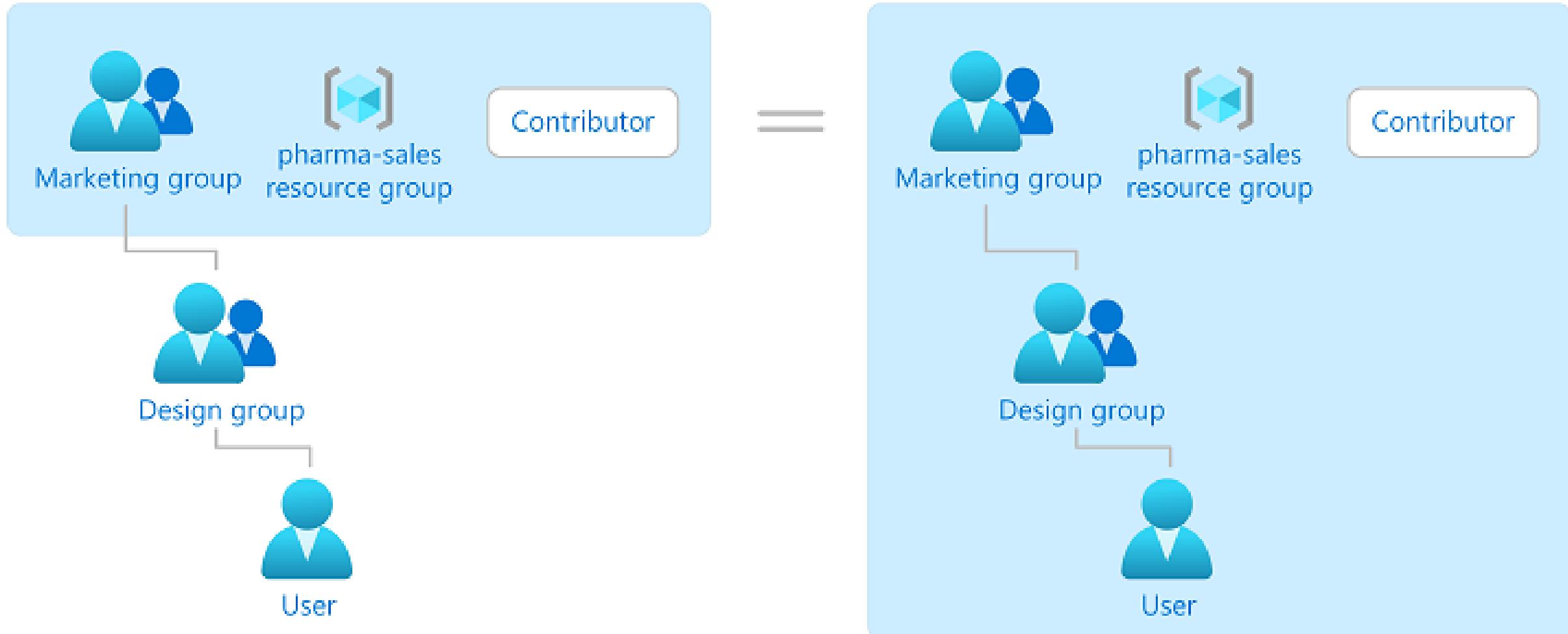
# Azure Role-Based Access Control – Role Assignments



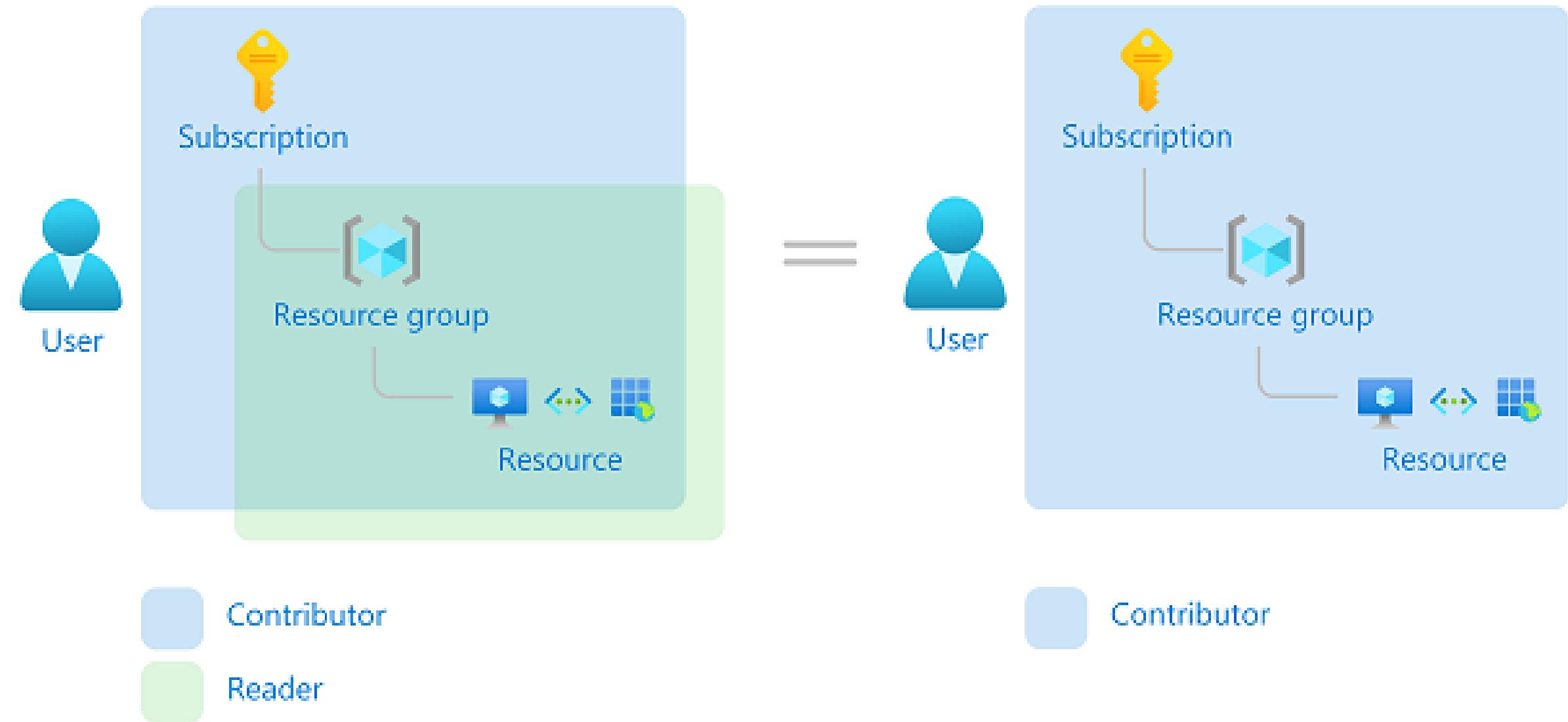
# Azure Role-Based Access Control – Scope



# Azure Role-Based Access Control – Groups



# Azure Role-Based Access Control – Multiple role assignments



# Azure Role-Based Access Control – Role Definition

## 2 Role definition

Owner  
Contributor  
Reader  
...

Backup Operator  
Security Reader  
User Access Administrator  
Virtual Machine Contributor

Built-in

Reader Support Tickets  
Virtual Machine Operator

Custom

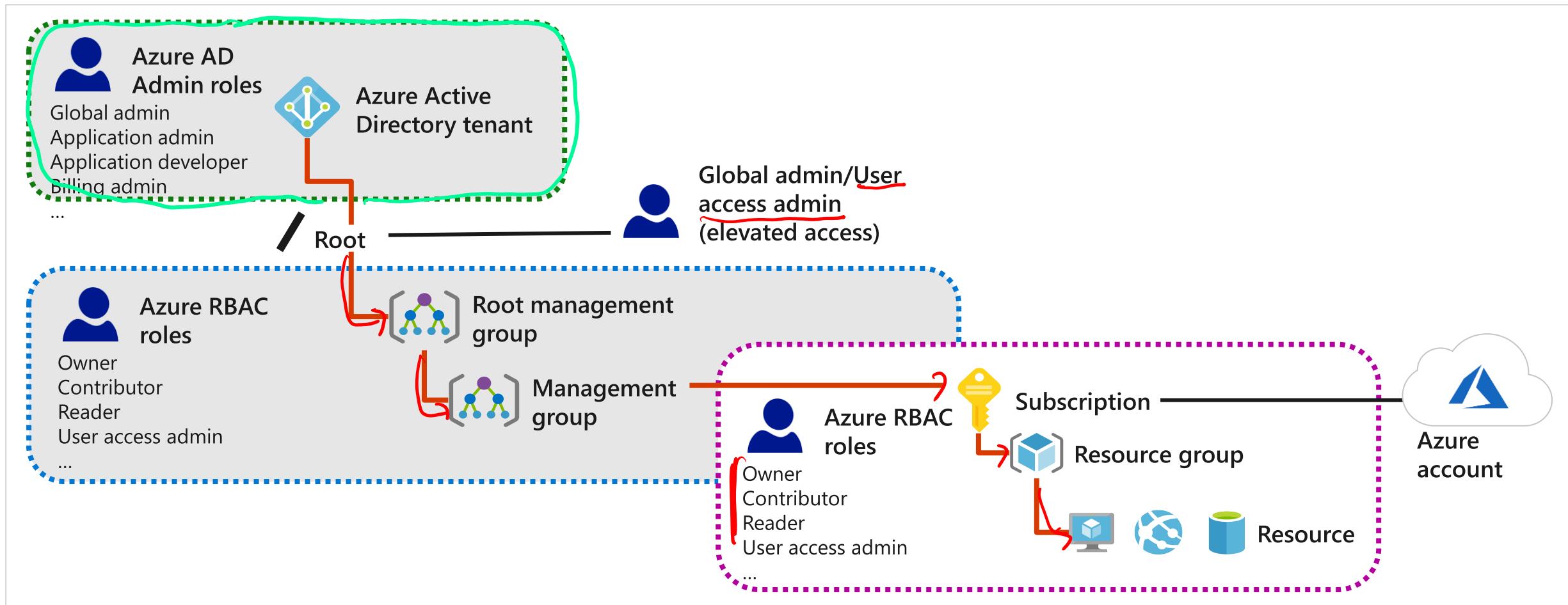
Contributor

```
"Actions": [  
    "*"  
],  
"NotActions": [  
    "Authorization/*/Delete",  
    "Authorization/*/Write",  
    "Authorization/elevateAccess/Action"  
],  
"DataActions": [],  
"NotDataActions": [],  
"AssignableScopes": [  
    "/"  
]
```

# Azure Role-Based Access Control

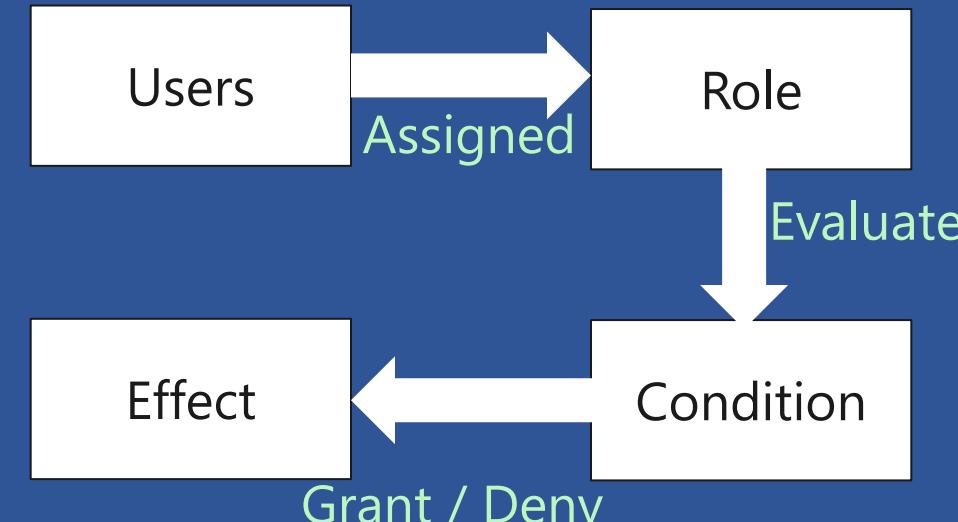
Classic  
2011  
9b 2013  
RBAC  
+ classic

Azure AD Admin roles and Azure RBAC roles work together to authenticate users.

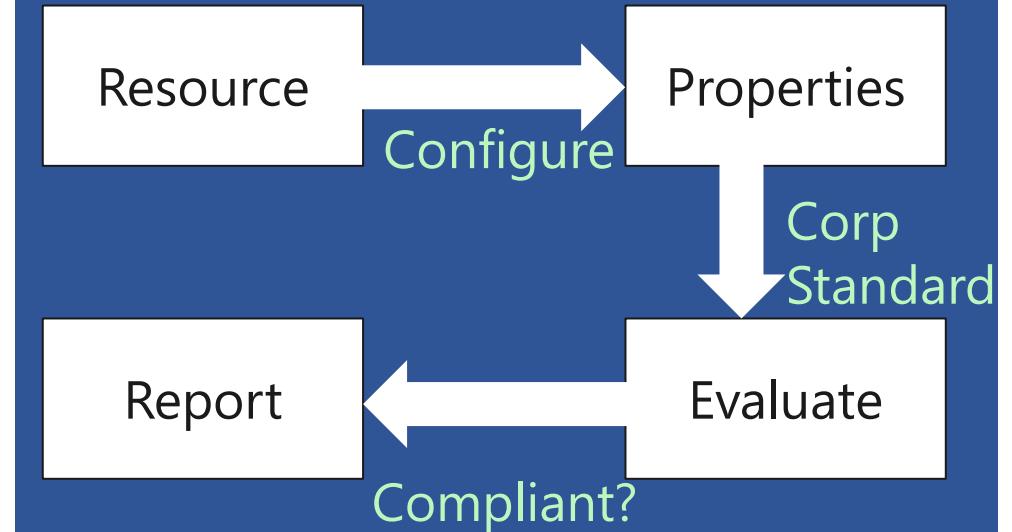


# Azure RBAC vs Azure Policies

## Role Based Access Control (RBAC)



## Azure Policy



Azure RBAC manages who has access to Azure resources, what areas they have access to and what they can do with those resources.

Azure Policies focus on resource properties during deployment and for already existing resources.

# Built-in Roles for Azure Resources

Built-in Role	Description
Owner	Allows you to manage everything including access to resources
Contributor	Allows you to manage everything except managing access to resources
Reader	Allows you to view everything but not make any changes
User Access Administrator	Allows you to manage user access to Azure resources

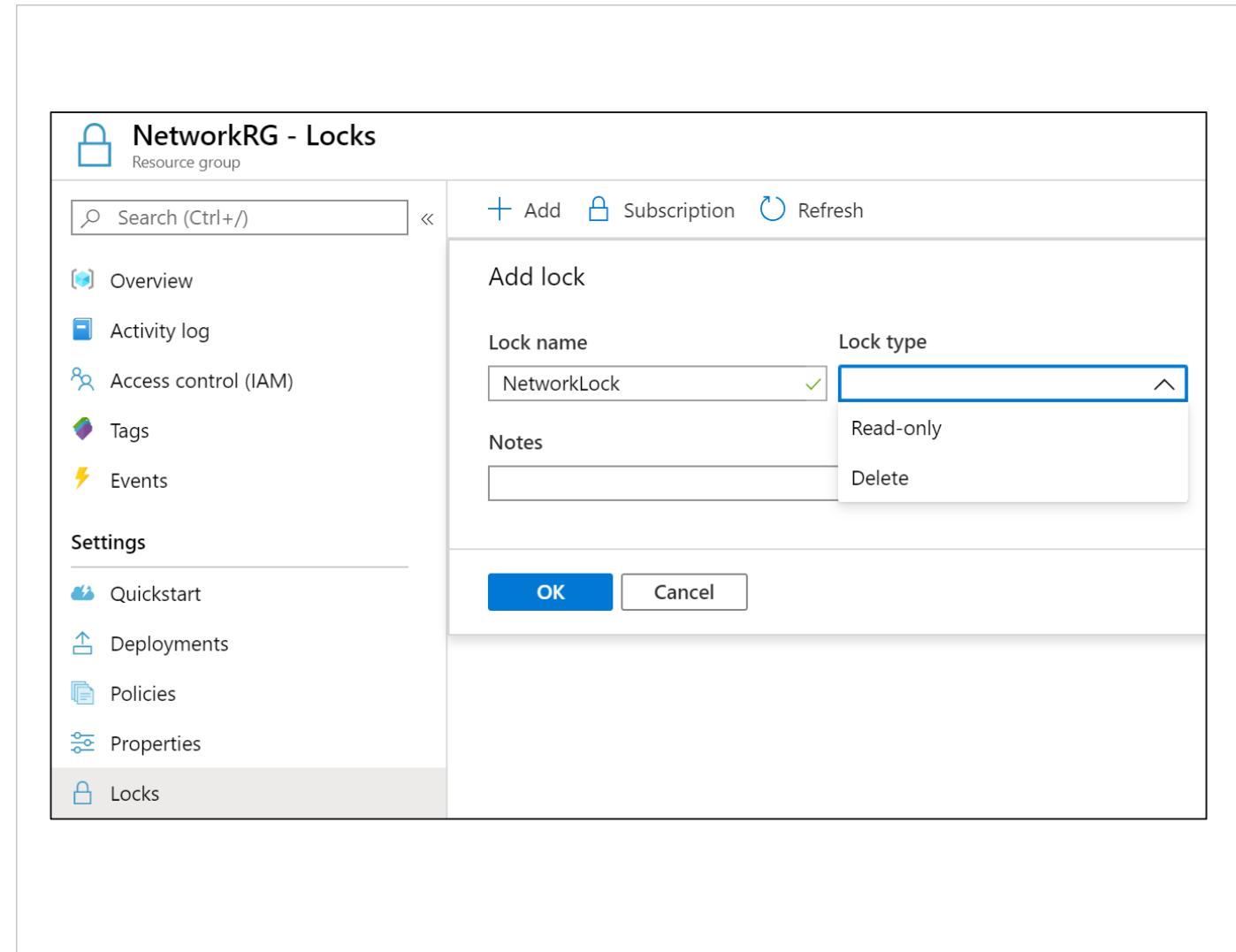
# Resource Locks

Associate the lock with a subscription, resource group, or resource

Locks are inherited by child resources

Read-Only locks prevent any changes to the resource

Delete locks prevent deletion



# Azure Blueprints (preview)

Designed to help with environment setup

Create reusable environment definitions that can recreate your Azure resources and apply your policies instantly

A package or container for composing focus-specific sets of standards, patterns, and requirements



# Azure Subscription Management

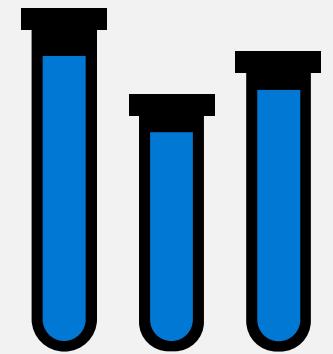
The Account Owner role can create Azure subscriptions.

Organizations assign Azure subscriptions to various business units.

If you're an Enterprise Agreement(EA) customer, your enterprise administrators can transfer billing ownership of your subscriptions between accounts.

The screenshot shows the Azure portal's 'Subscriptions' page. At the top, there's a breadcrumb navigation from 'Home > Subscriptions'. Below it, the title 'Subscriptions' is followed by 'Microsoft'. A large blue 'Add' button with a plus sign is prominently displayed. A message below the button says 'Showing subscriptions in Microsoft. Don't see a subscription? [Switch directories](#)'. There are two dropdown menus: 'My role' which shows '0 selected' and has an 'Apply' button, and 'Status' which also shows '0 selected'. A checked checkbox says 'Show only subscriptions selected in the [global subscriptions filter](#)'. A search bar at the bottom is labeled 'Search to filter items...'. The overall interface is clean with a white background and light gray header elements.

# Module - Labs



# Lab 01 – Role-Based Access Control

Use the Portal to create a Senior Admins group with member Joseph Price.

Use PowerShell to create a Junior Admins group with member Isabel Garcia.

Use the CLI to create a Service Desk group with member Dylan Williams.

Assign the Service Desk group Virtual Machine Contributor permissions.

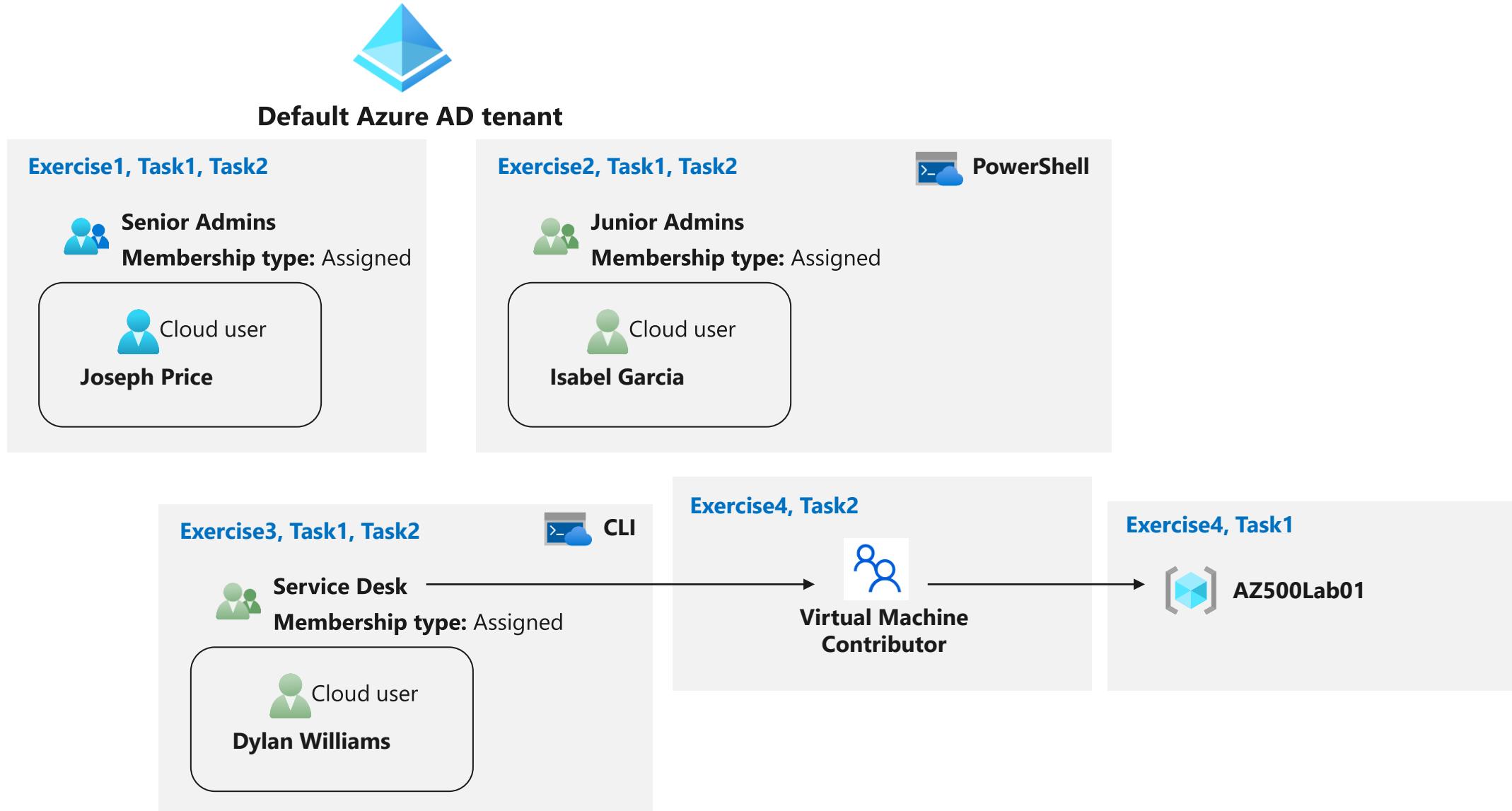
Senior Admins

Junior Admins

Service Desk



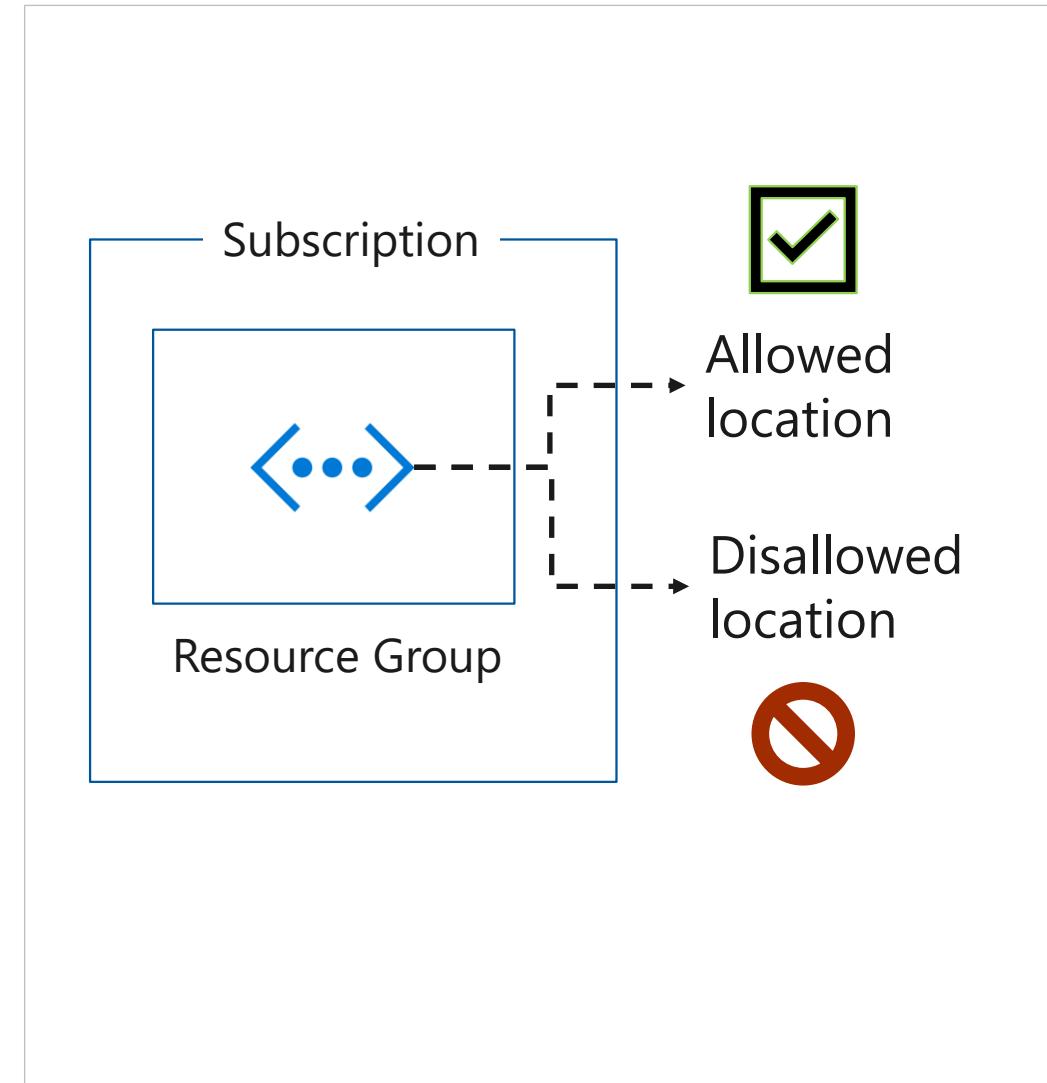
# Lab 01 – Role-Based Access Control



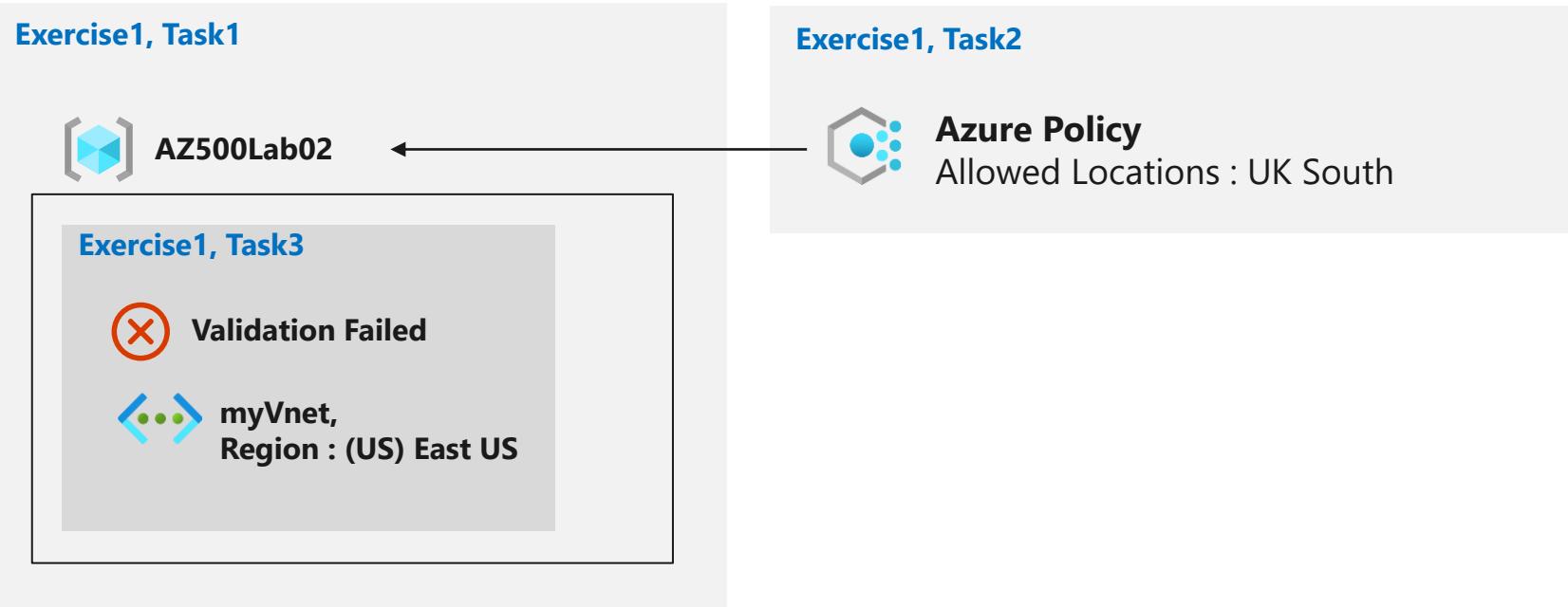
# Lab 02 – Azure Policy

Create an Allowed Locations policy that ensures resources are only created in a specific region.

Test to ensure resources are only created in the Allowed Location.



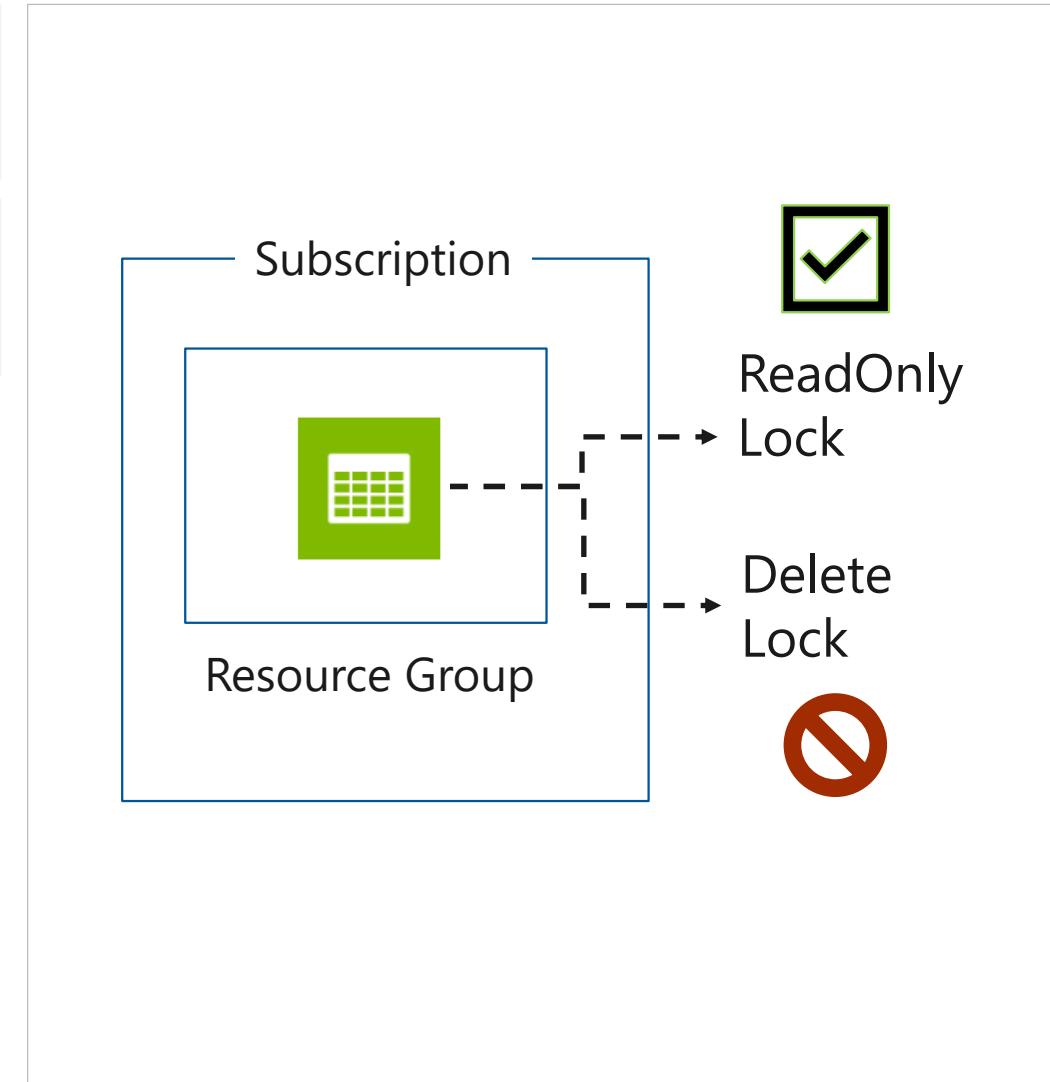
# Lab 02 – Azure Policy



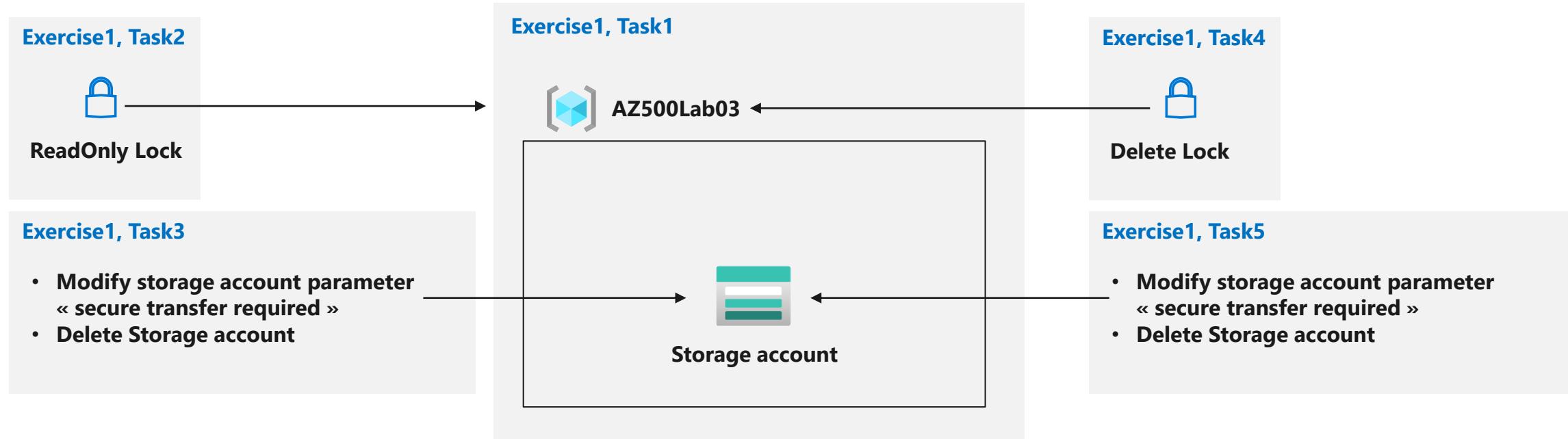
# Lab 03 – Resource Manager Locks

Prevent a storage account configuration from being changed.

Prevent a storage account from being deleted.



# Lab 03 – Resource Manager Locks

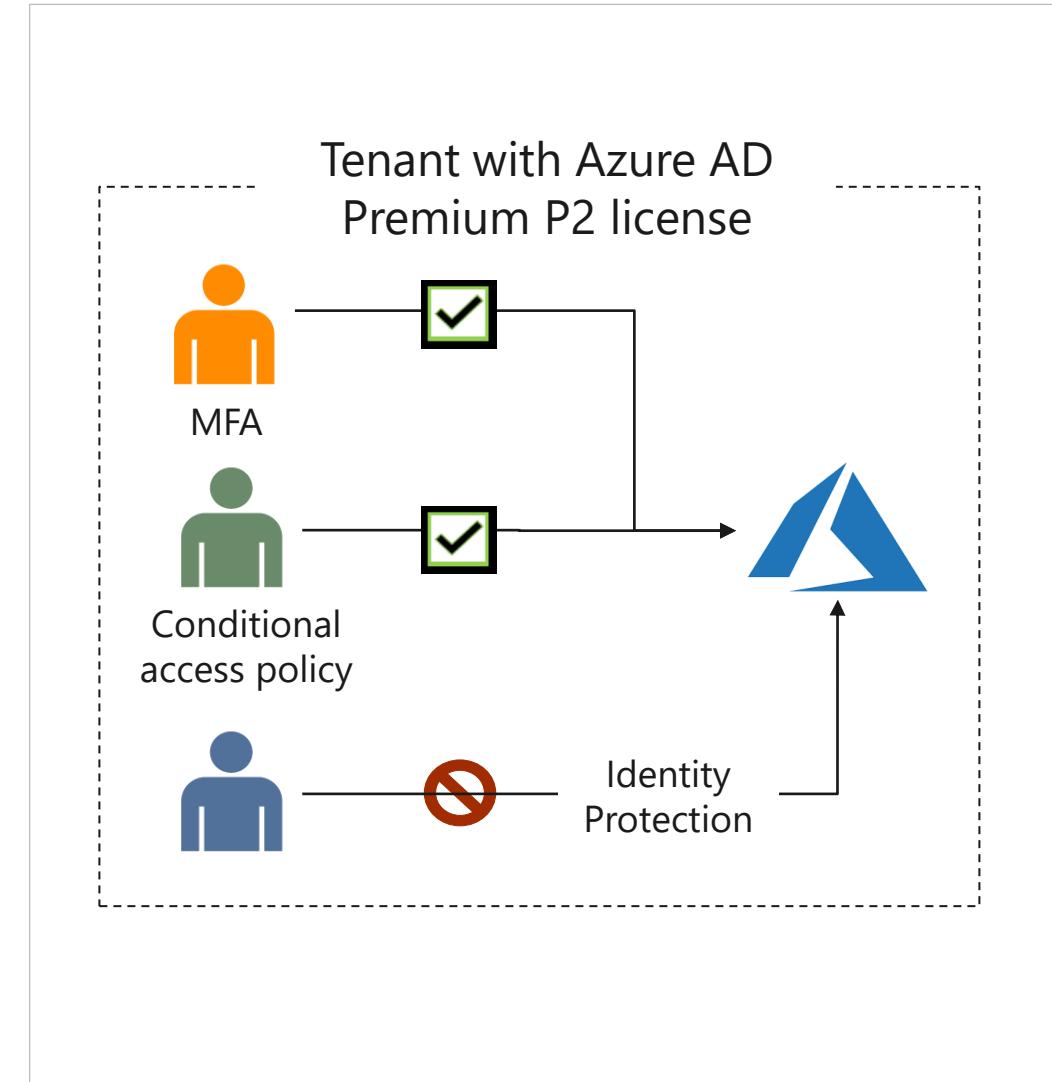


# Lab 04 – MFA - Conditional Access - Identity Protection

Implement and test Azure MFA.

Implement and test Azure AD Conditional Access Policies.

Implement and test Azure AD Identity Protection.



# Lab 04 – MFA - Conditional Access - Identity Protection

Exercise1, Task1



az500-04-vnet1 10.102.0.0/16

Subnet0 10.102.0.0/24



az104-07-vm0  
10.102.0.4

TOR

Exercise2, Task2

Premium P2 free trial



Exercise2, Task1



AdatumLab500-04

Exercise2, Task3, Task4



aaduser1  
Role: Global Administrator



Aaduser2  
Role: user



aaduser3  
Role: user



Your user account

Exercise2, Task5, Task6

MFA  
per user MFA

Exercise3, Task1, Task2

Conditional Access  
Portal → MFA

Exercise4, Task1, Task2,  
Task3, Task4, Task5

Identity protection

Medium → MFA

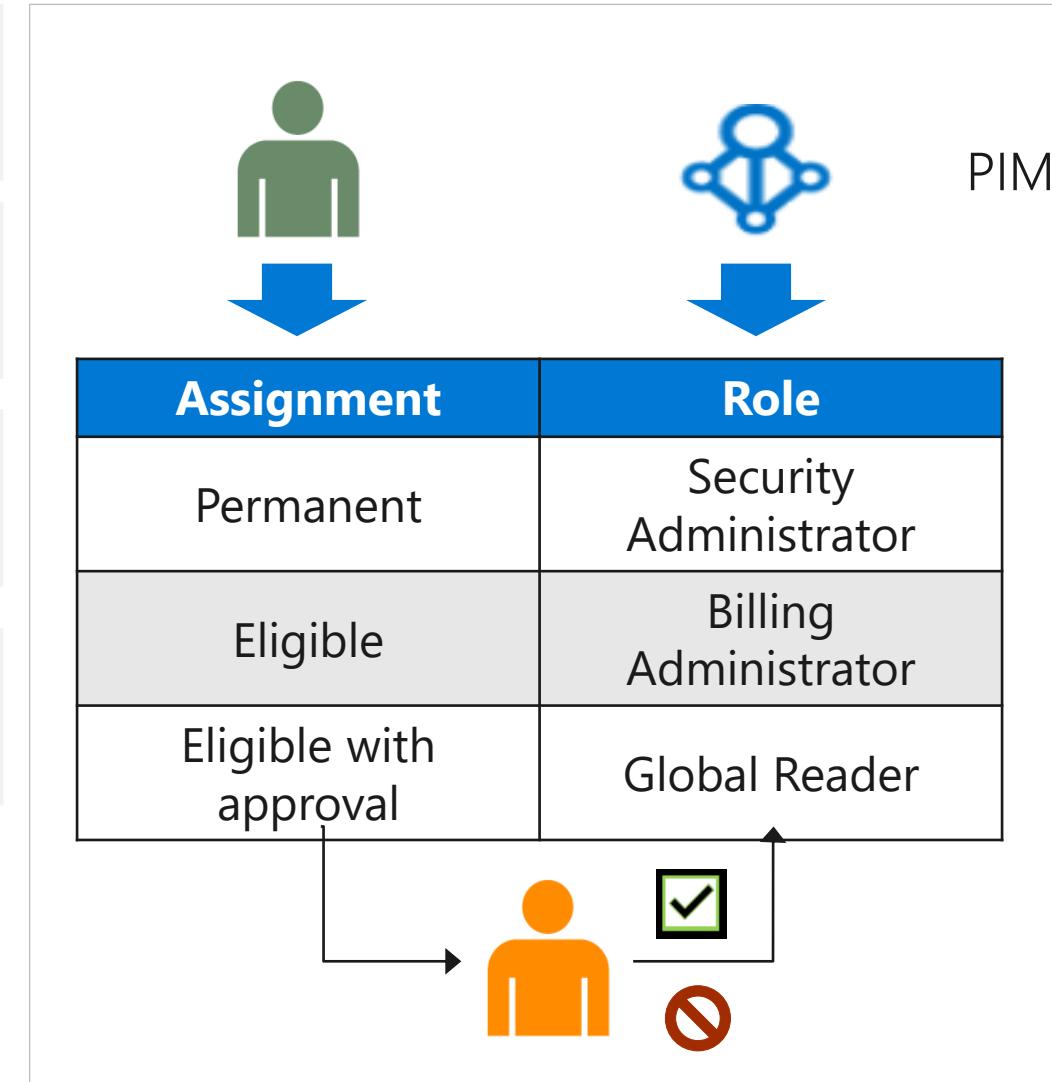
# Lab 05 – Azure AD Privileged Identity Management

Onboard PIM.

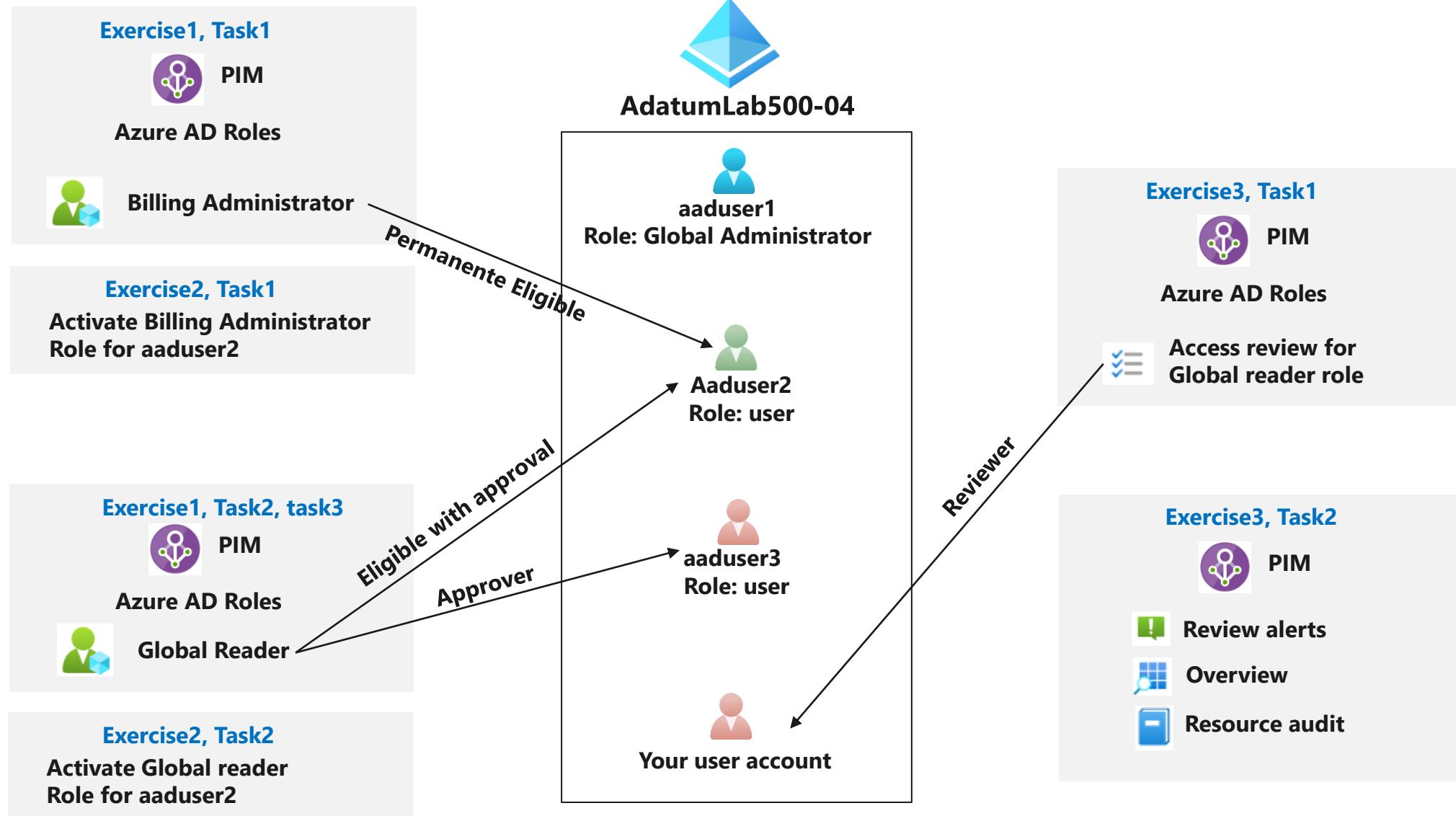
Configure PIM users and roles.

Activate PIM roles with and without approval.

Create an Access Review and review PIM auditing features.



# Lab 05 – Azure AD Privileged Identity Management



# Lab 06 – Implement Directory Synchronization

Deploy an Azure VM hosting an Active Directory domain controller.

Create and configure an Azure Active Directory tenant.

Synchronize Active Directory forest with an Azure Active Directory tenant.

Azure Active Directory



AD Connect



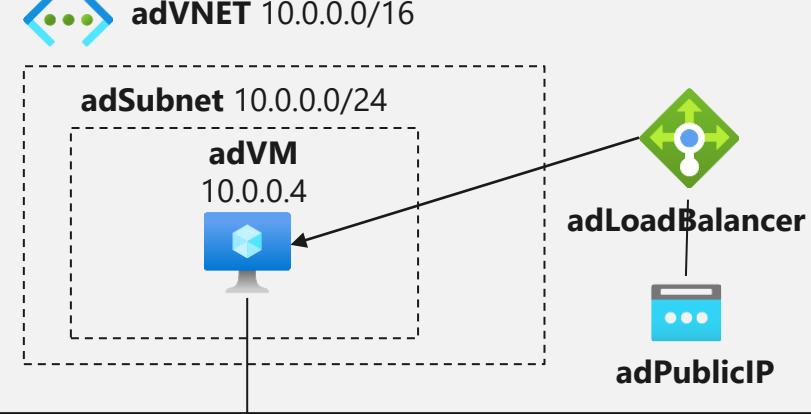
On-premises Active  
Directory Domain  
Controller (simulated)

# Lab 06 – Implement Directory Synchronization

Exercise1, Task1, Task2



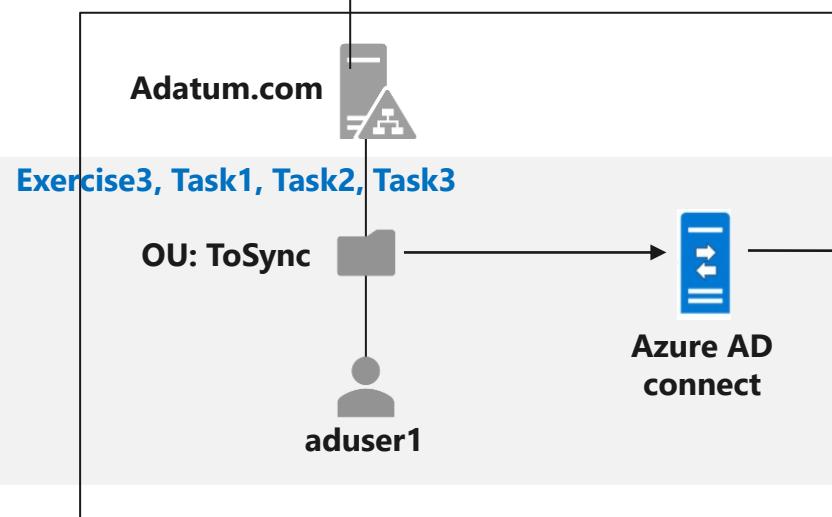
adVNET 10.0.0.0/16



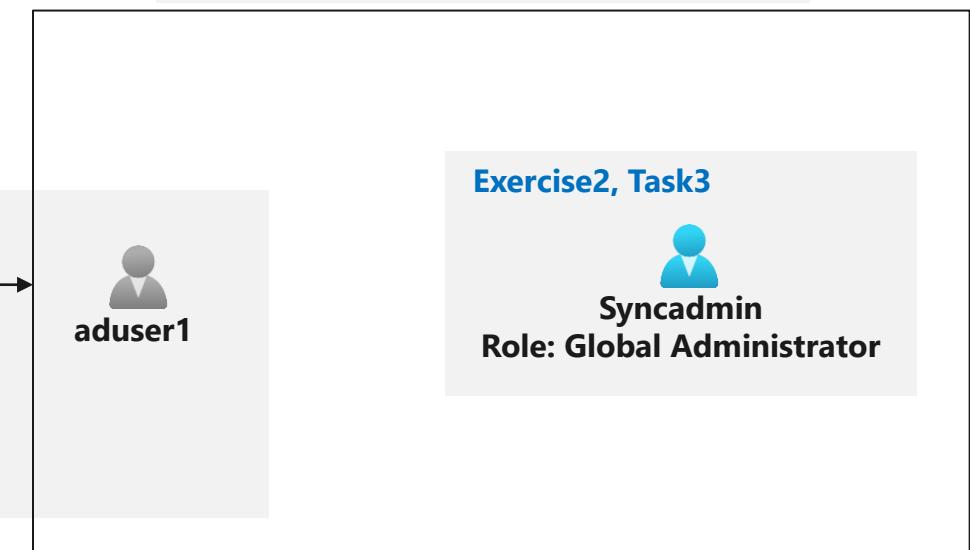
Exercise2, Task1, Task2



**AdatumSync**  
**Adatum.com**



Exercise3, Task1, Task2, Task3



Exercise2, Task3

**End of presentation**