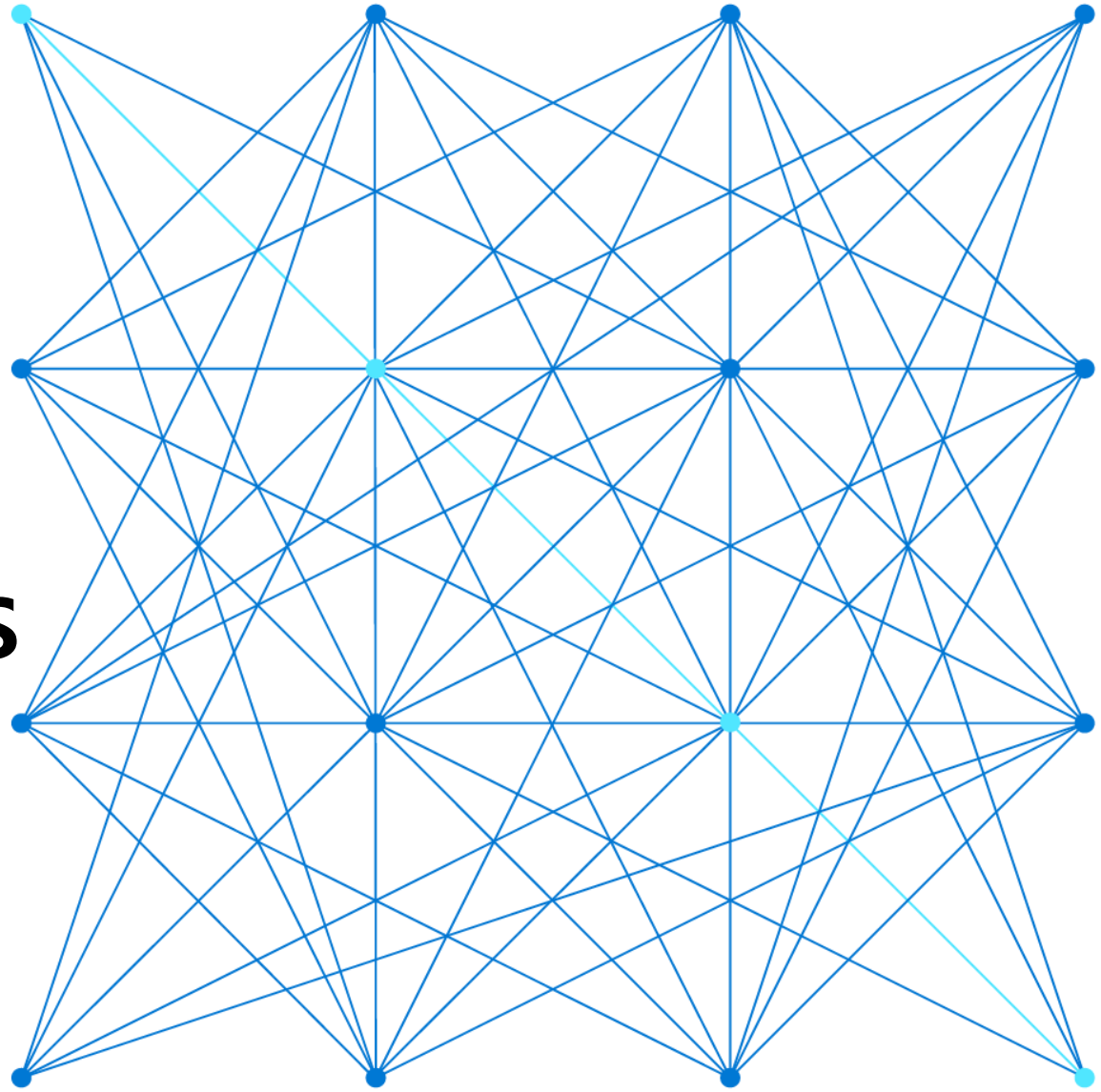
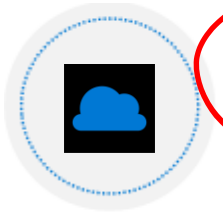
Microsoft Azure

AZ-500

Microsoft Azure Security Technologies

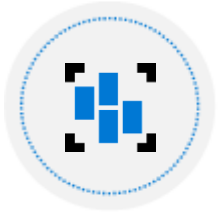


AZ-500 Agenda



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

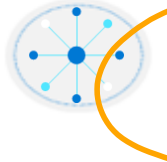
Hybrid Identity

Azure AD Identity Protection

Azure AD Privileged Identity Management

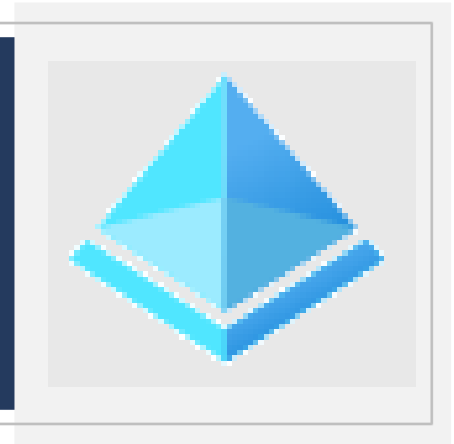
Enterprise Governance

Application Security



Module Labs

Azure Active Directory



Azure Active Directory (Azure AD)

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

Work or School Account

ID Provider

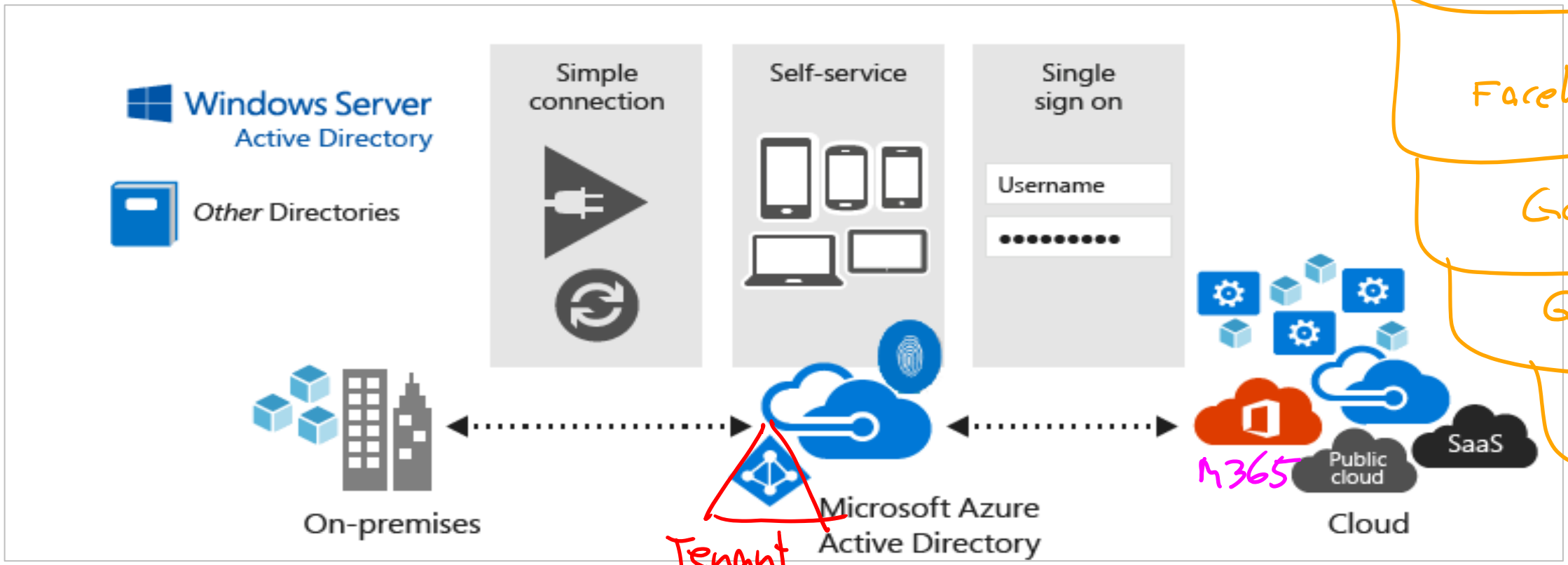
MS Account

Facebook

Google

GitHub

Okta



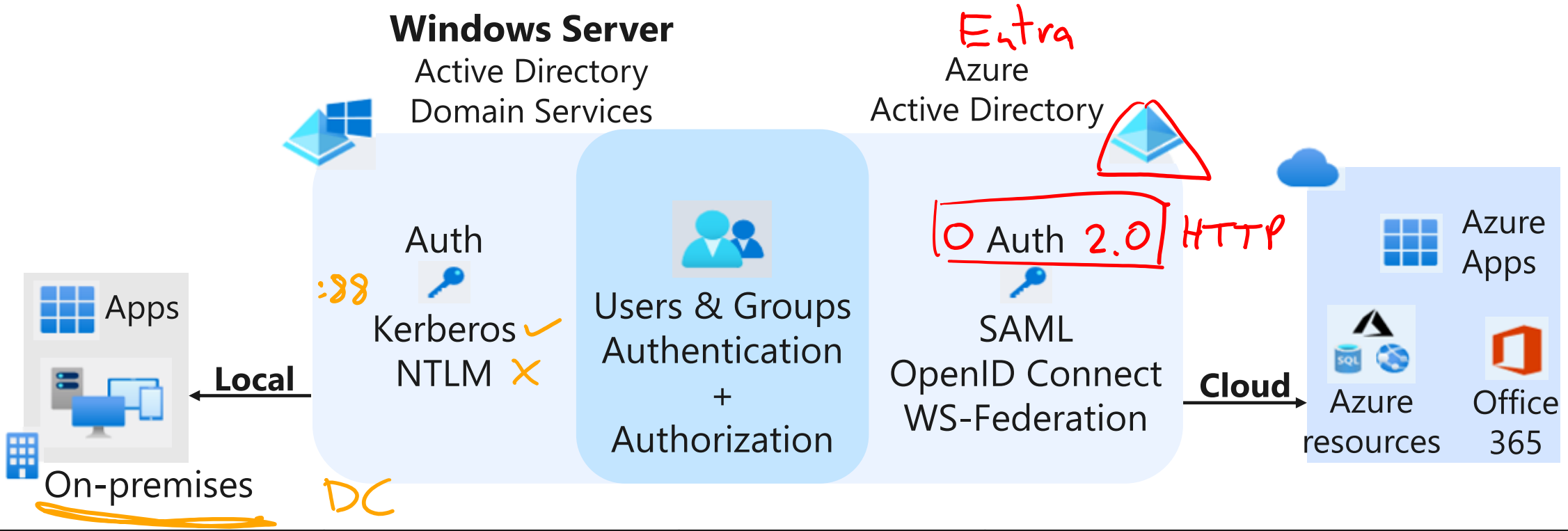
Microsoft's multi-tenant cloud-based directory and identity management service

Identity management capabilities and integration

Integrates with Windows Server Active Directory

Provides SSO access

Azure AD versus Active Directory Domain Services (AD DS)

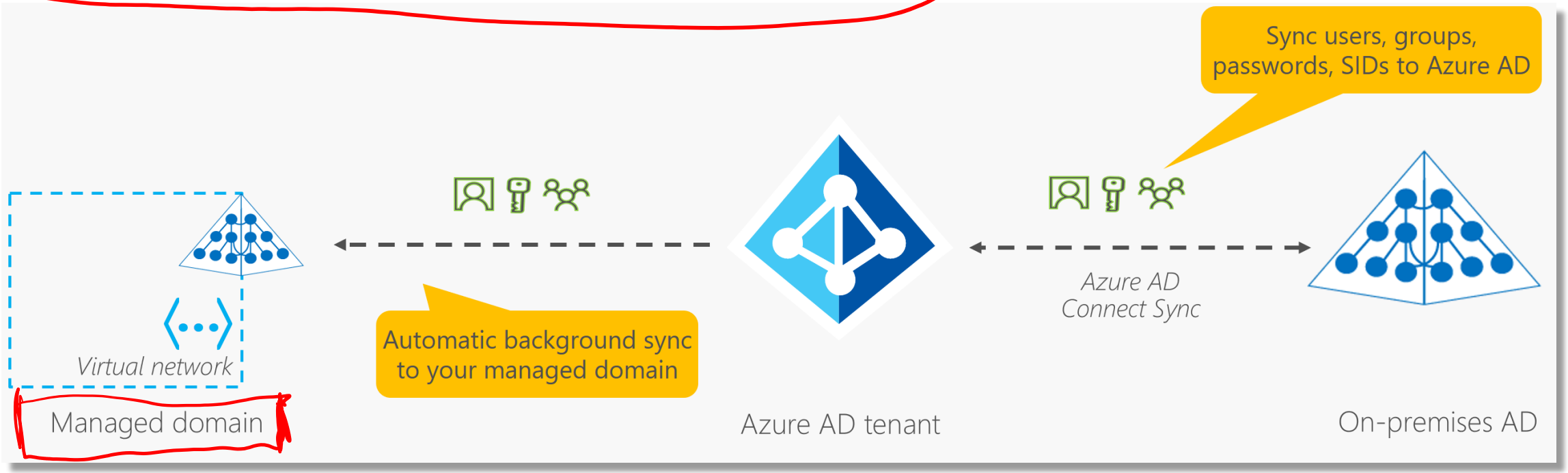


Service	Authentication	Structure	What it's used for
Azure Active Directory	Includes SAML, OpenID Connect (based on OAuth), WS-Federation	Tenants	Internet-based services and applications like Office 365, Azure services, and third-party SaaS applications
Active Directory Domain Services	Kerberos, NTLM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

Roles for Azure AD (sample)

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.

Azure Active Directory Domain Services

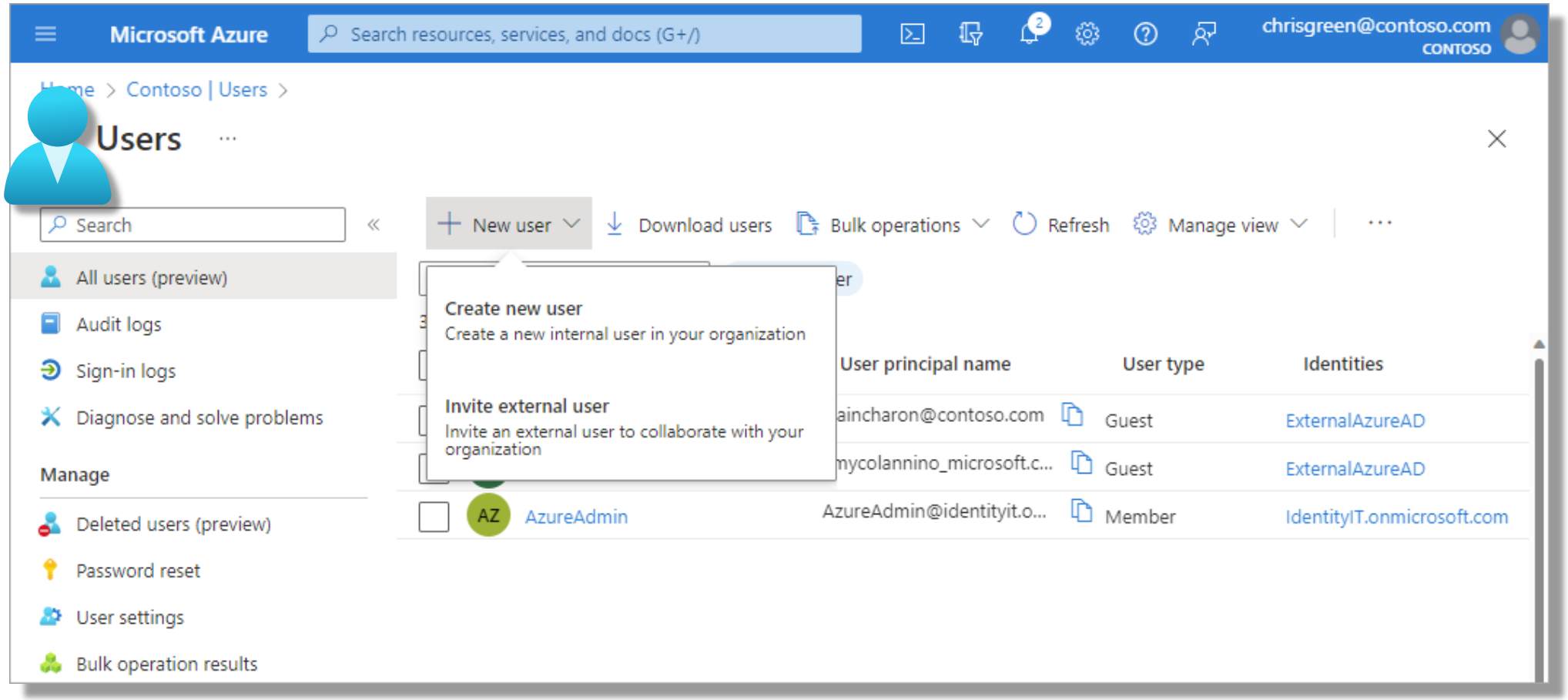


- Azure Active Directory Domain Services (Azure AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/New Technology LAN Manager (NTLM) authentication.

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

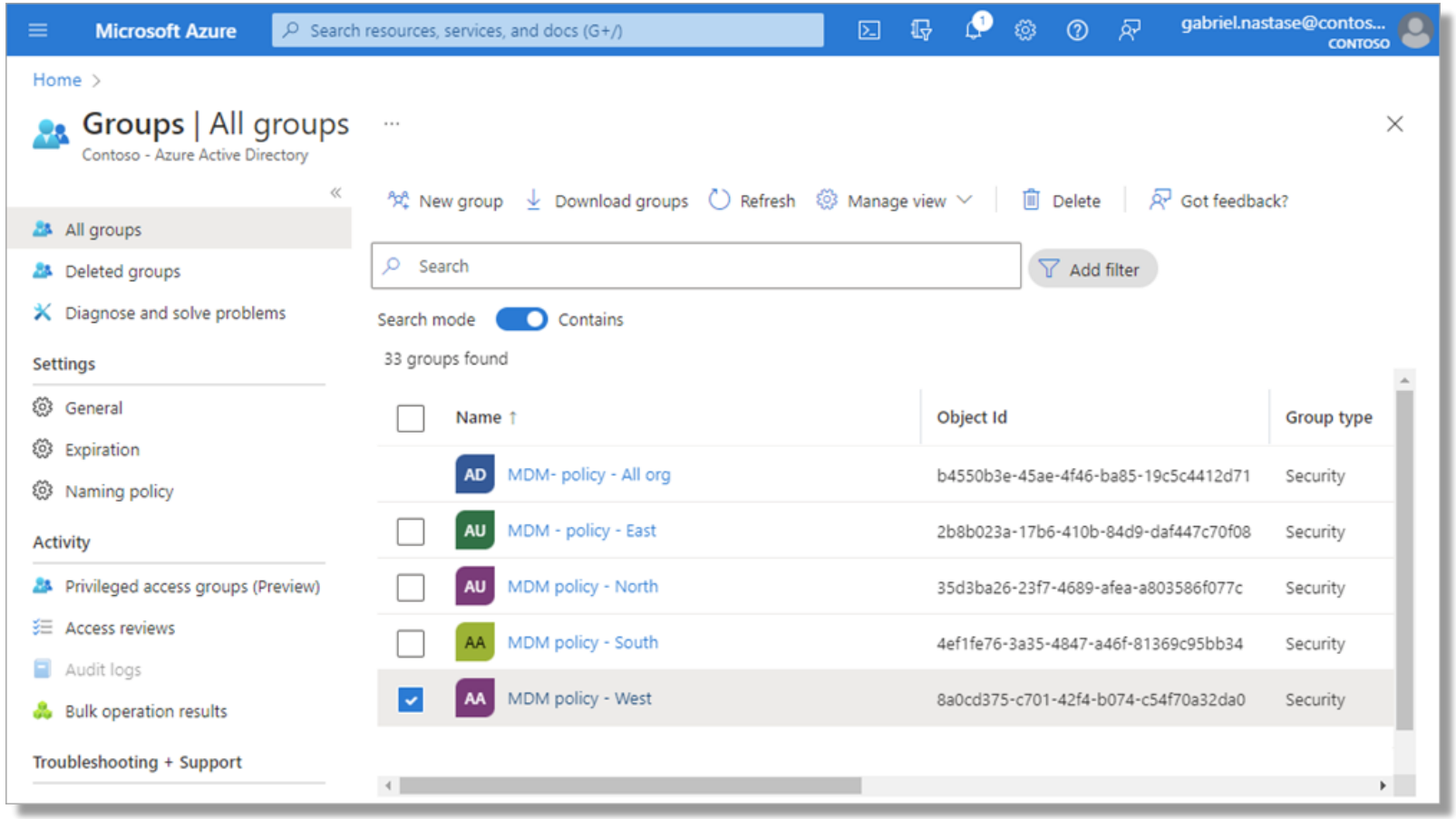
Azure AD Users

- 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.



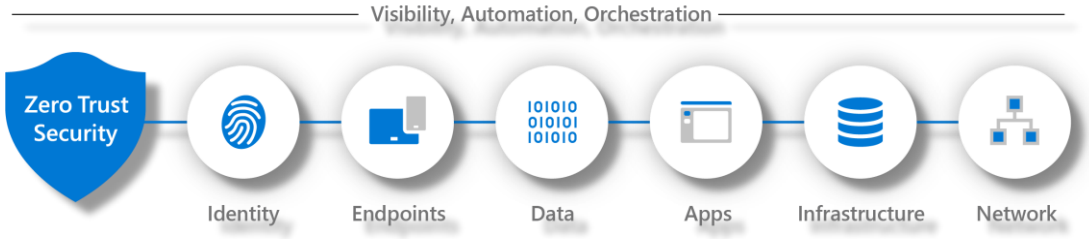
Azure AD Groups

- 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.

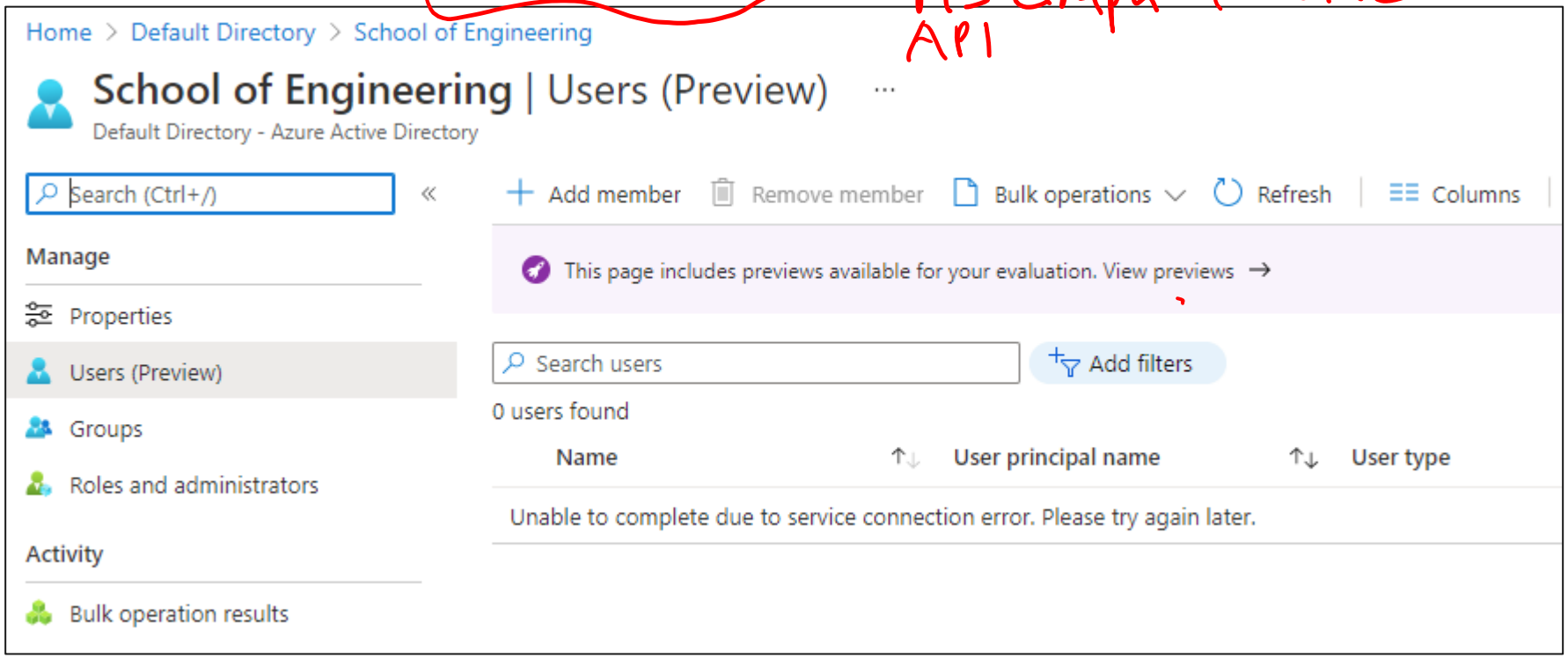
- Limiting access to Azure AD resources to only those users who need access is one of the core security principles of Zero Trust.



Administrative Units in Azure AD

Azure AD Graph (ADAL old)

MS Graph (MSAL new) API



Azure CLI Tool az vm list

Admin Unit Members

- Users
- Groups

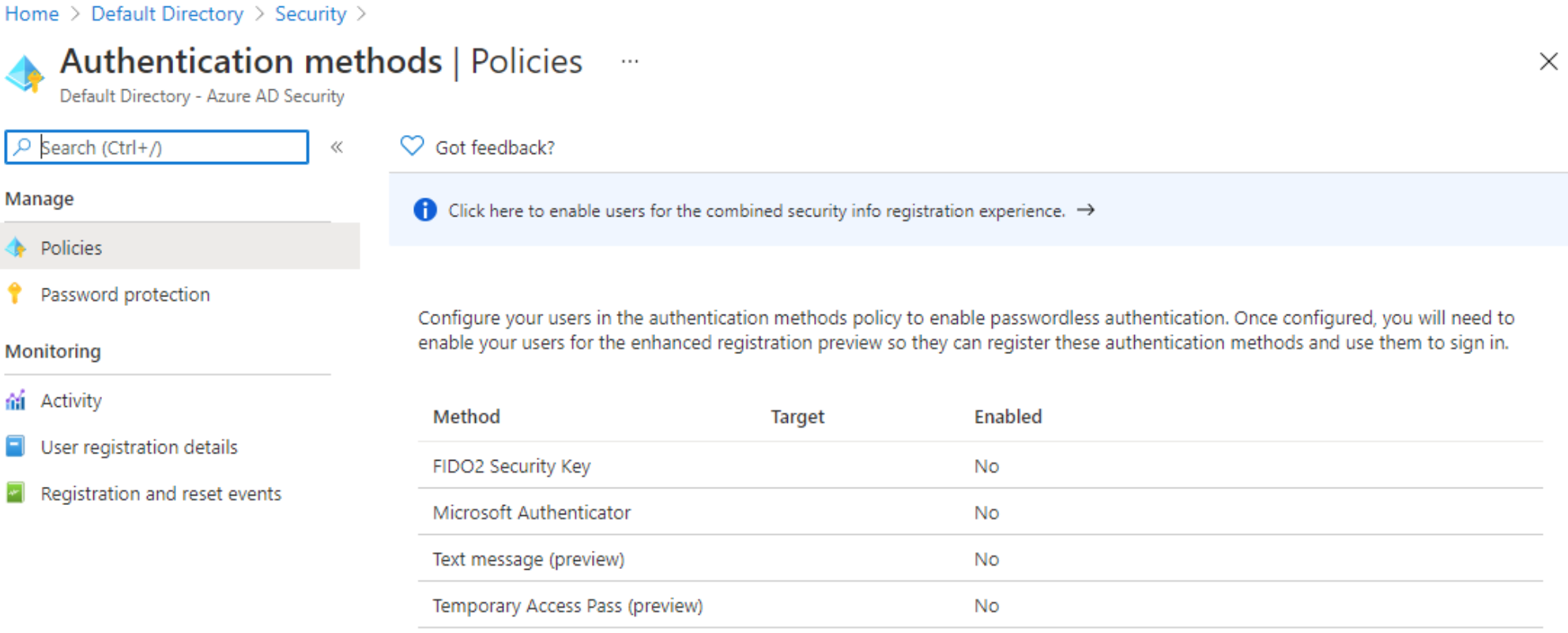
Usage

Delegate administration of AD resources to specific person or role

Configure using

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

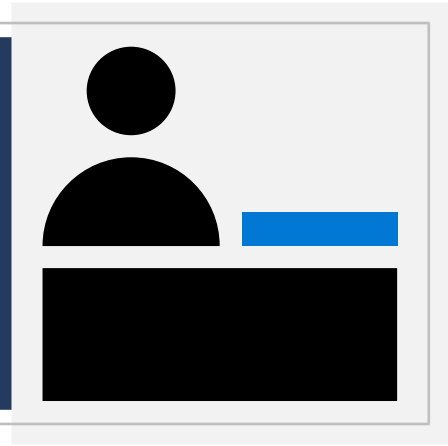
Passwordless



Log in without using a password, ever.

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

Hybrid Identity



Hybrid Identity

- Azure AD Connect
- Azure AD Connect cloud sync
- Authentication Options
  1. Password Hash Synchronization (PHS) ←
  3. Pass-through Authentication (PTA)
  2. Federation with Azure AD
- Authentication Decision Tree
- Password Writeback

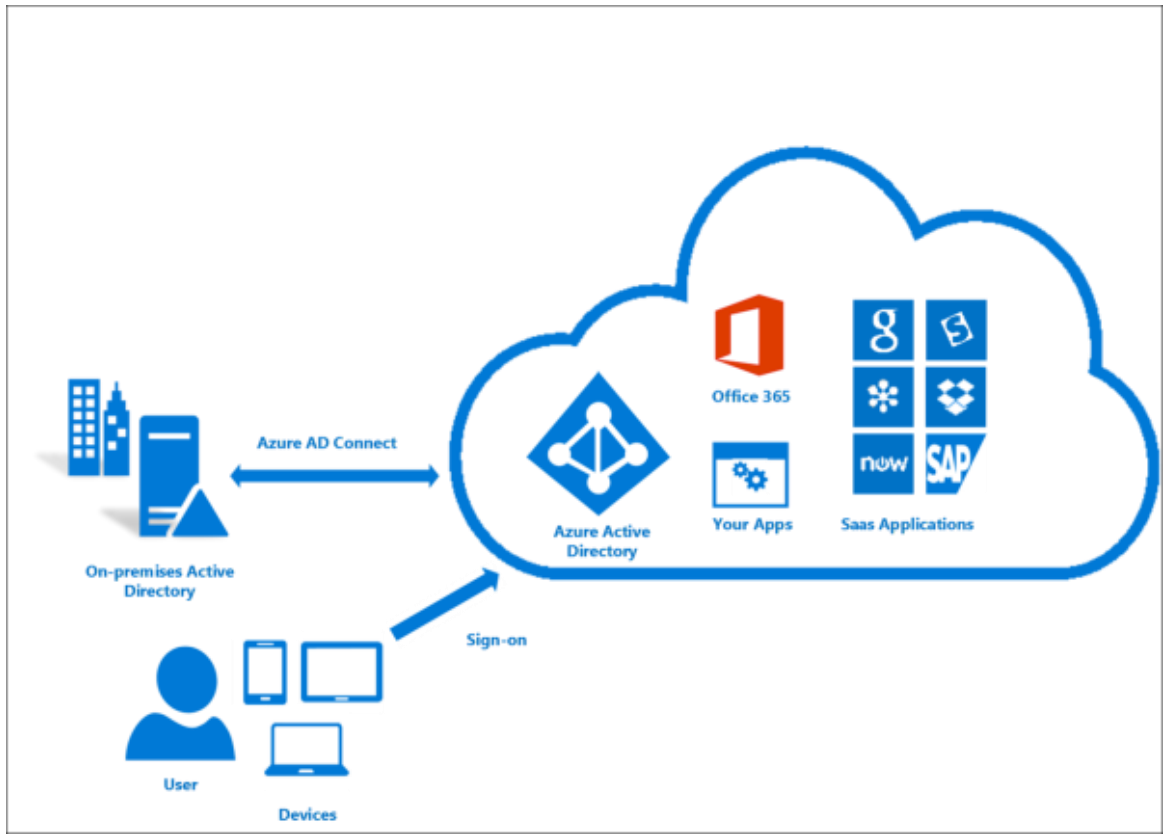
on Prem AD-DS + AD-FS + Proxies

Azure AD Connect

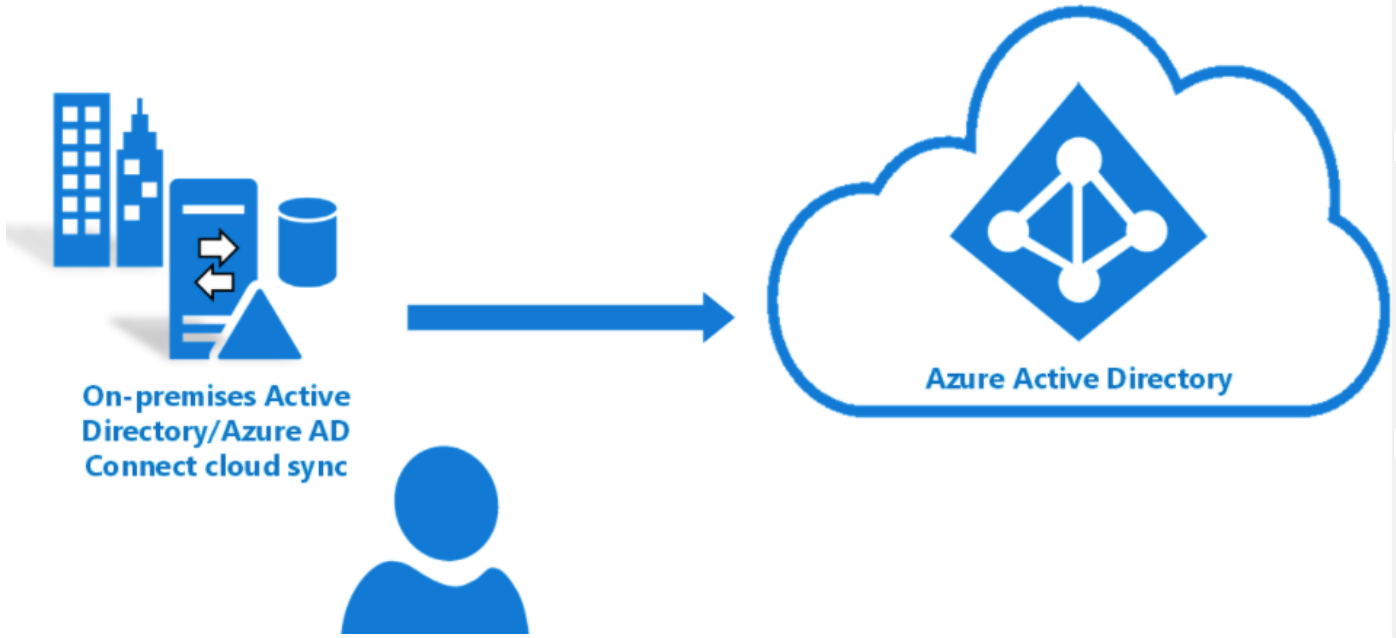
Integrate your on-premises directories with Azure Active Directory

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

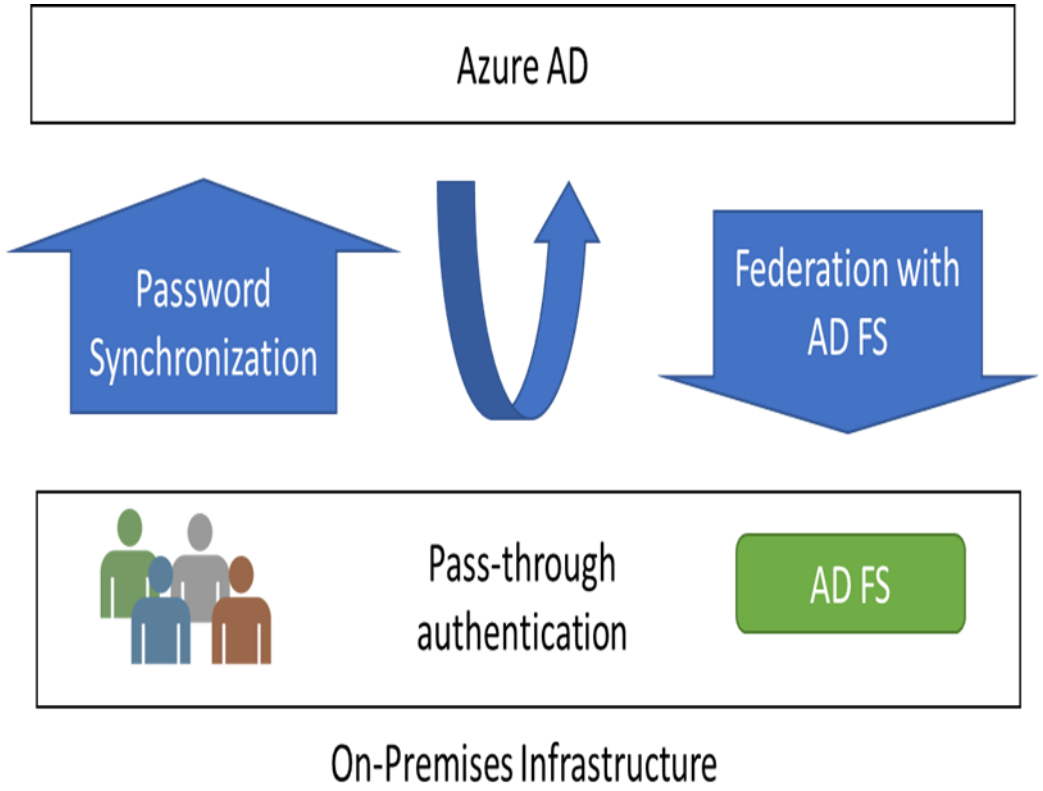
Runs stand-alone or along-side Azure AD Connect

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



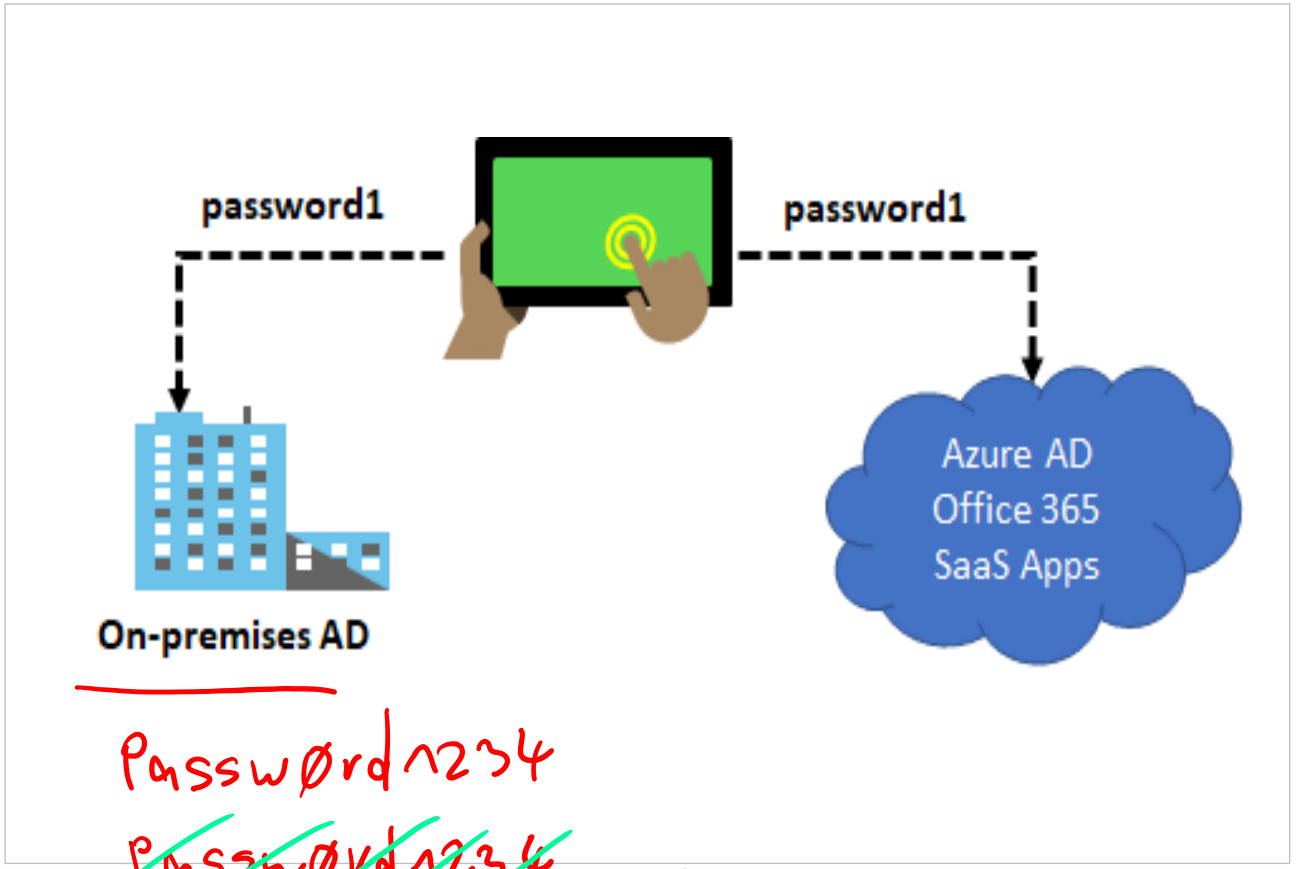
Password Hash Synchronization

QC
Anton Zeilinger

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

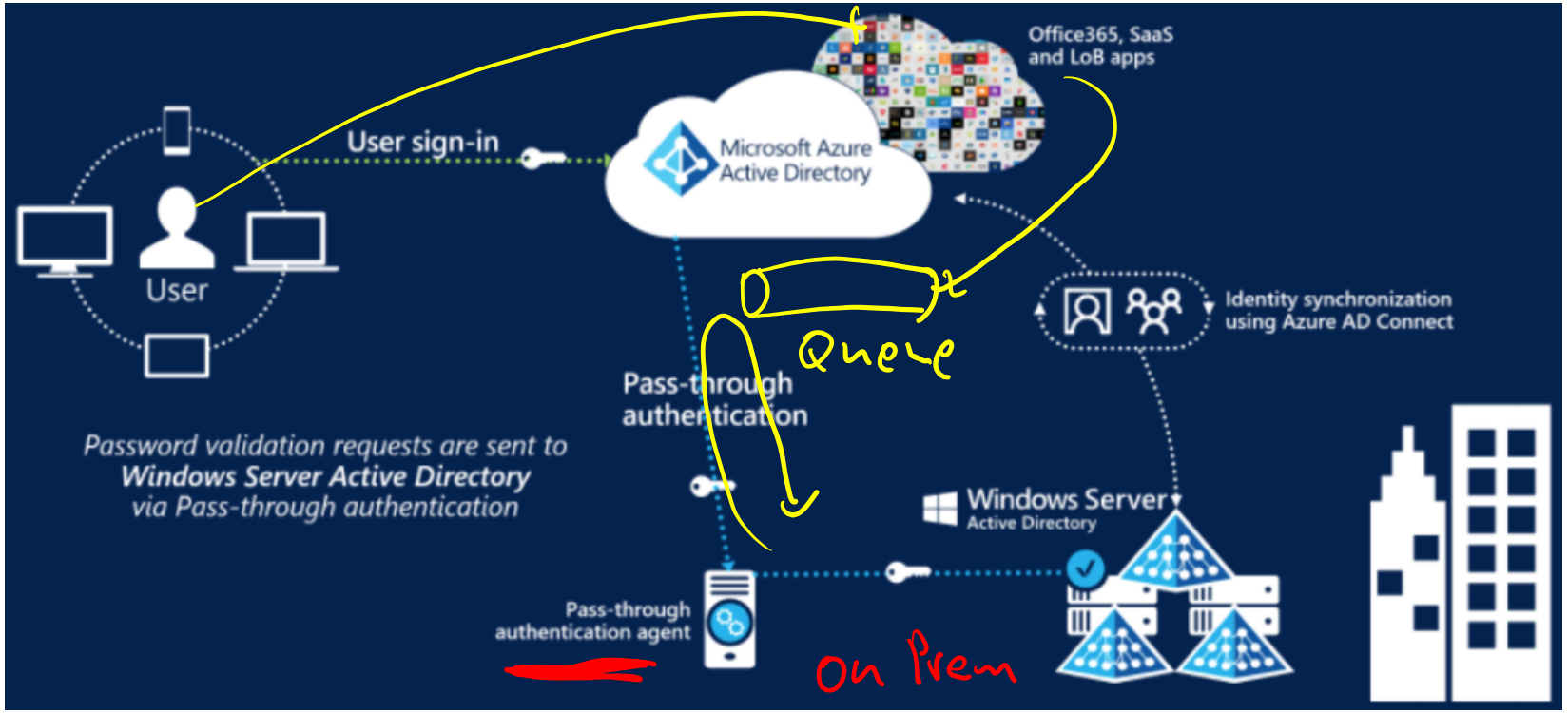
Sign into Azure AD services using the on-premises password

Improve the productivity of your users and reduce your helpdesk costs



Pass-through Authentication

PTA



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

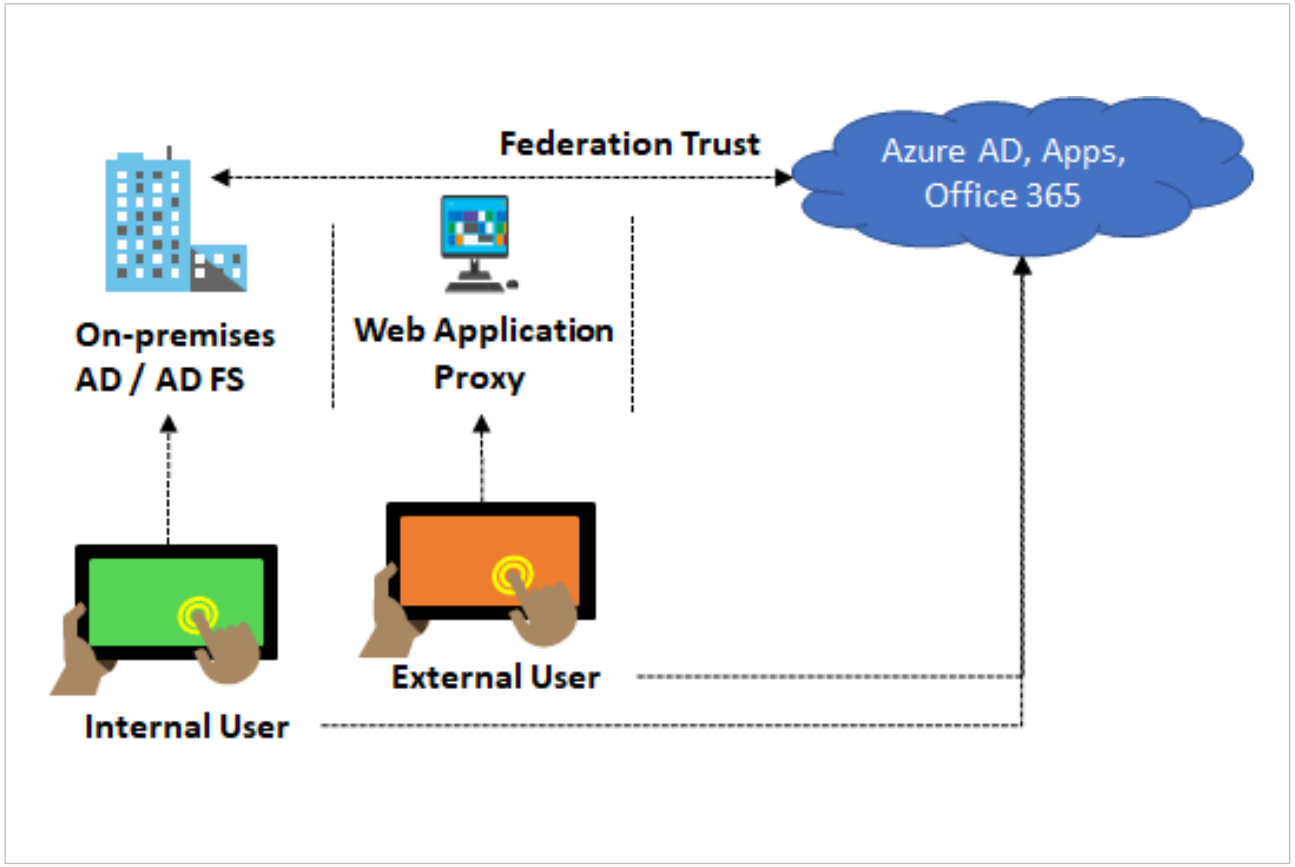
Is not only for user sign-in but allows an organization to use other Azure AD features – MFA and Self-Service Password Reset

Federation with Azure AD

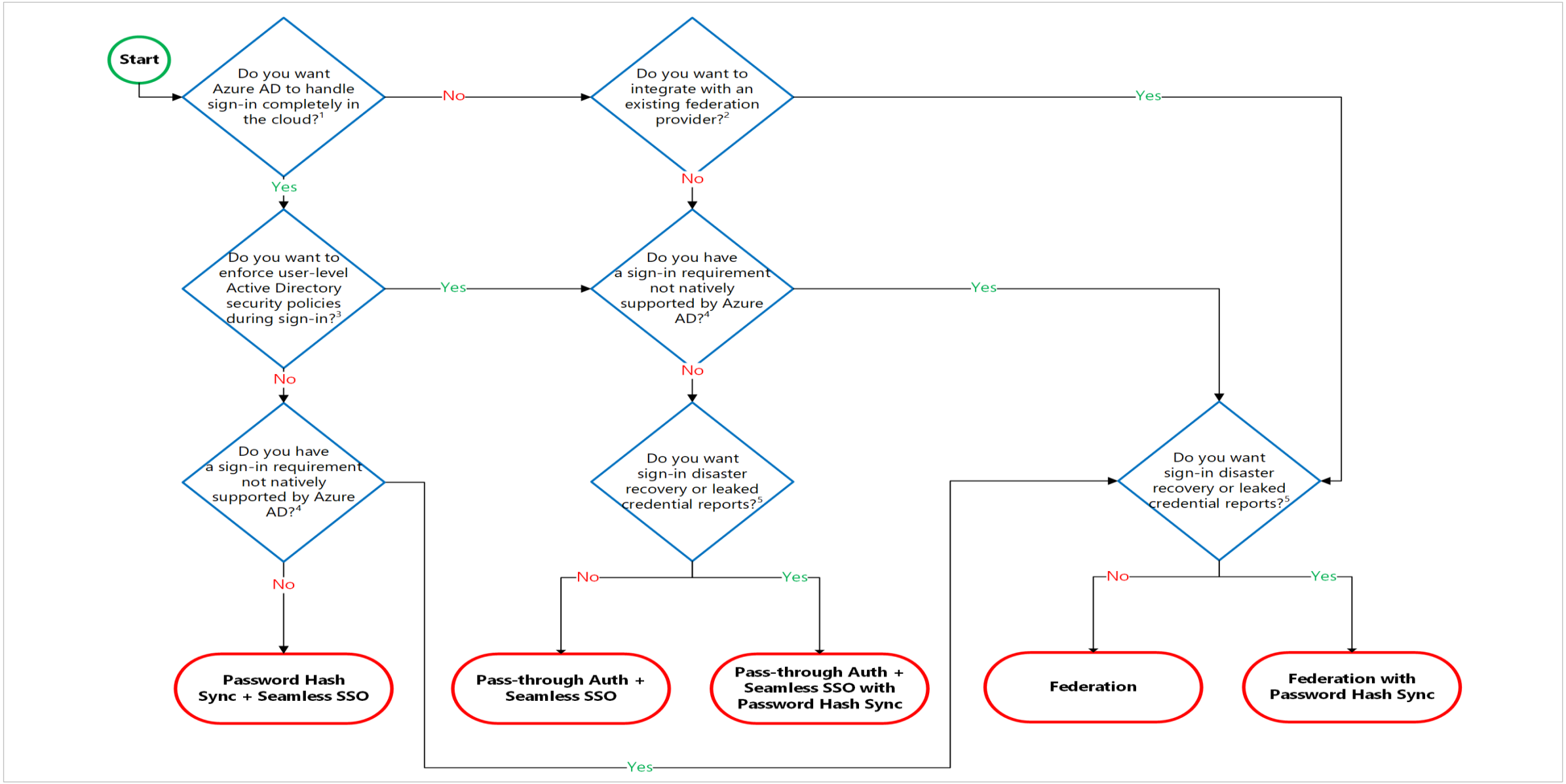
Federation is a collection of domains that have established trust

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



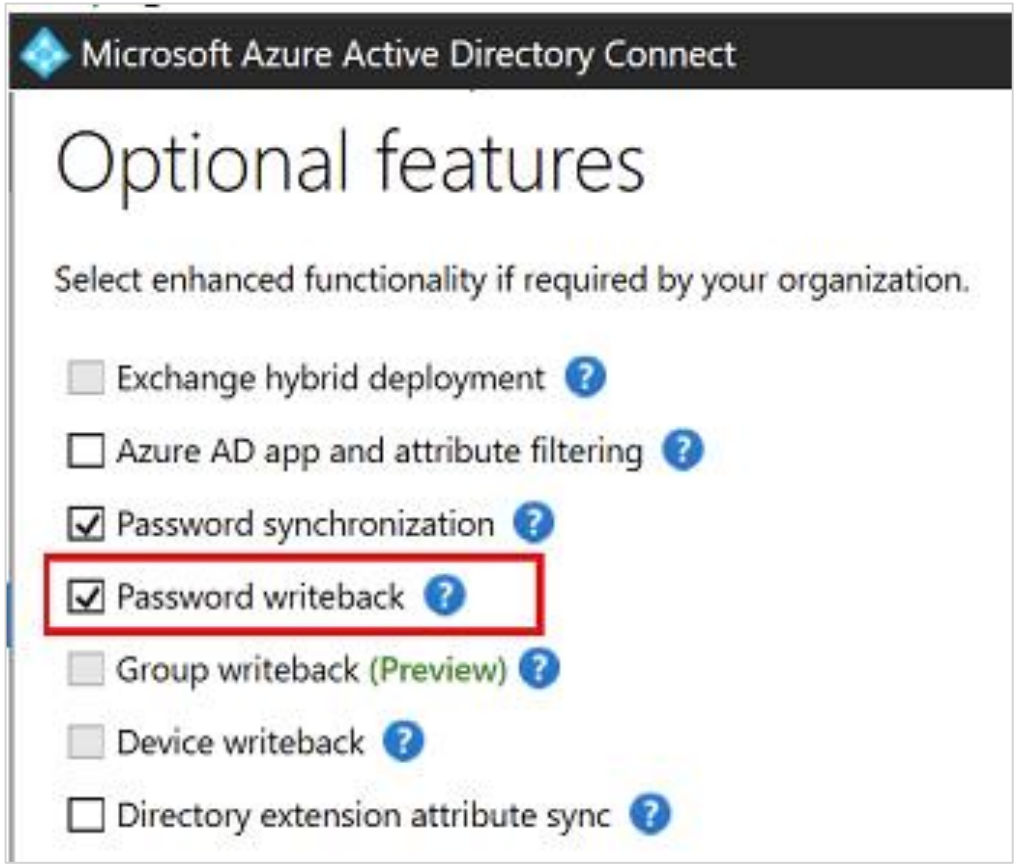
Password Writeback

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



P@55w.rd|123

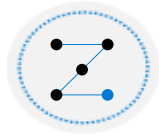
MFA
Risk

Azure AD Identity Protection

CA

Azure AD Identity Protection

Azure AD Identity Protection

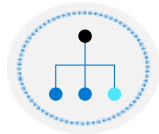


Risk Events

User Risk Policy

Sign-in Risk Policy

Azure MFA concepts

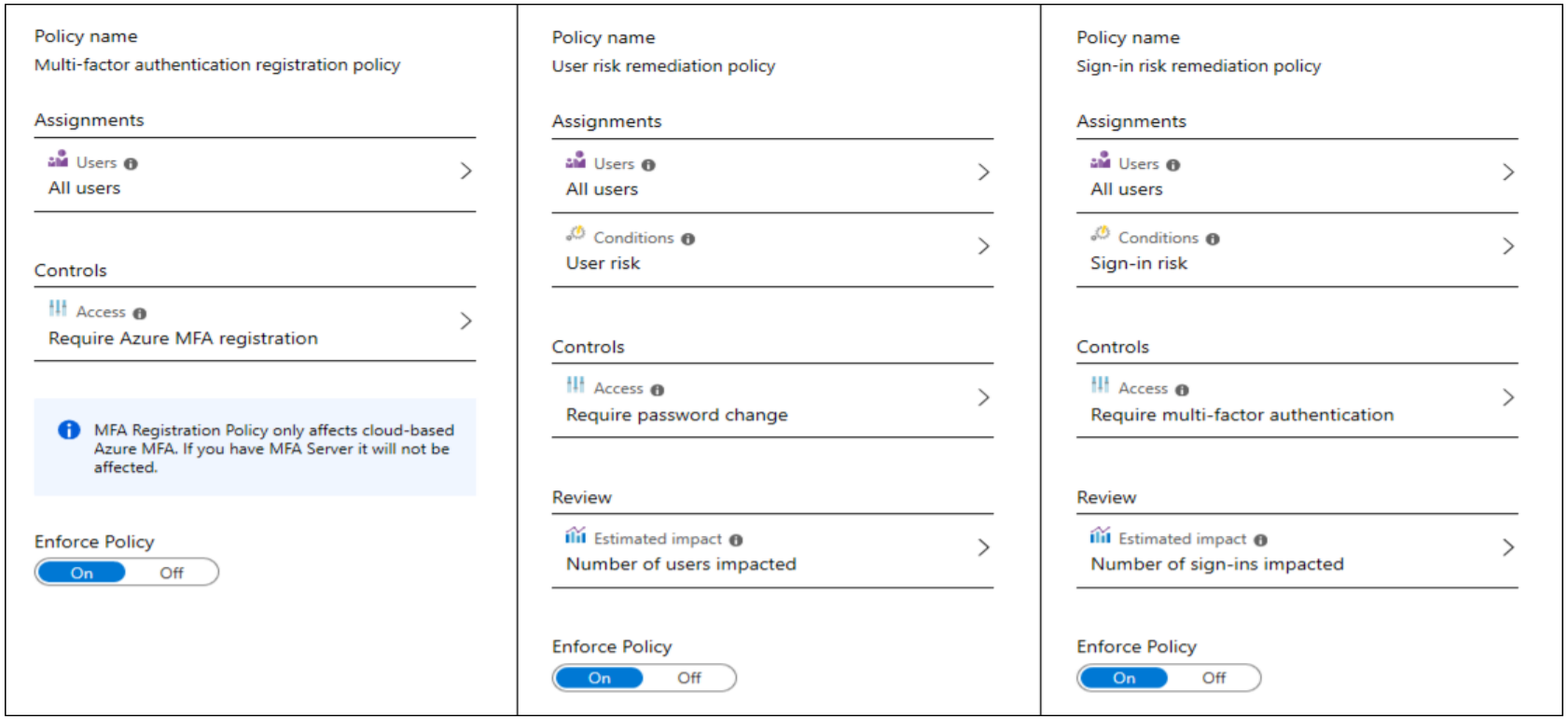


Azure AD Conditional Access

Conditions

Access Reviews

Azure AD Identity Protection Features



Automate the detection and remediation of identity-based risks

Investigate risks using data in the portal

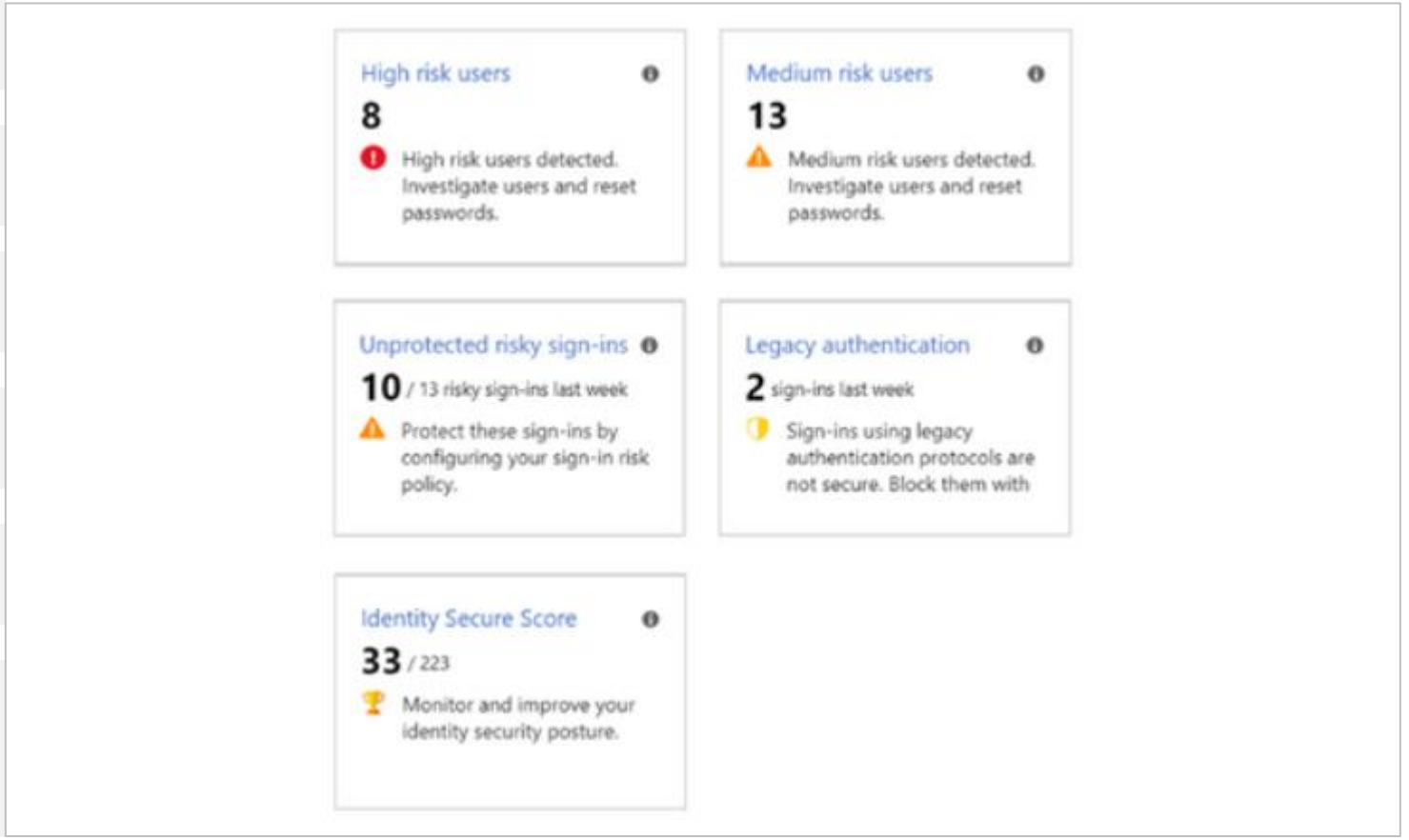
Export risk detection data to third-party utilities for further analysis

Azure Identity Protection Risk Events

High
Medium
Low
None

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

- 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



User Risk Policy

Applied to user sign-ins

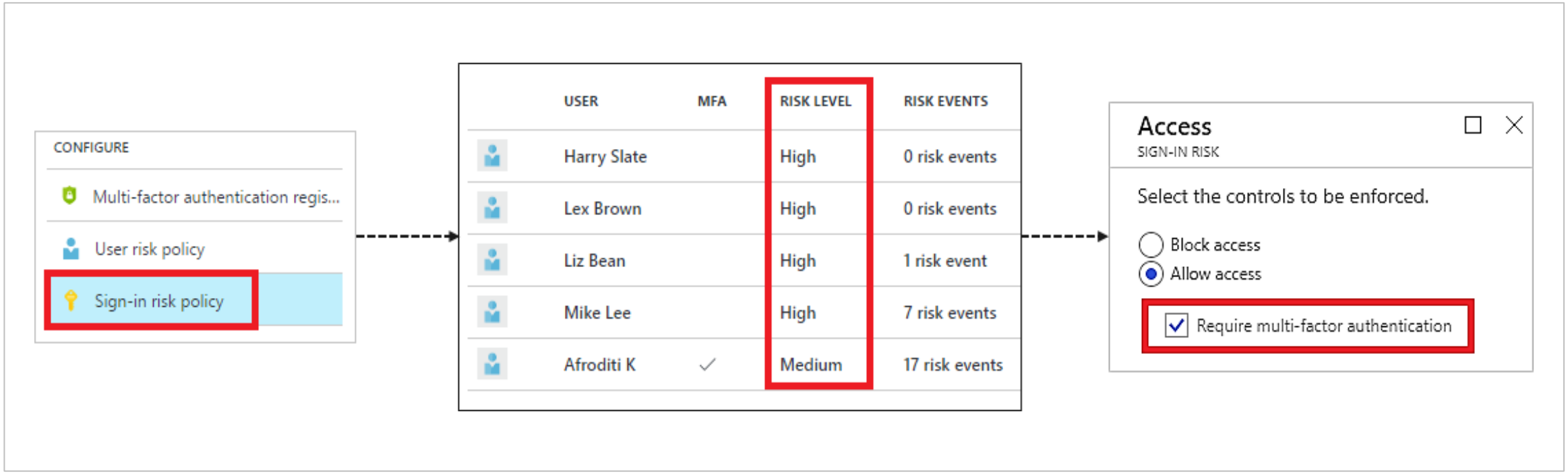
Provide the condition (risk level) and action (block or allow)

Use a low threshold for greater security

Automatically respond based on a specific user's risk level

Use a high threshold during policy roll out

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

No Costs ⟶ Per User MFA

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)

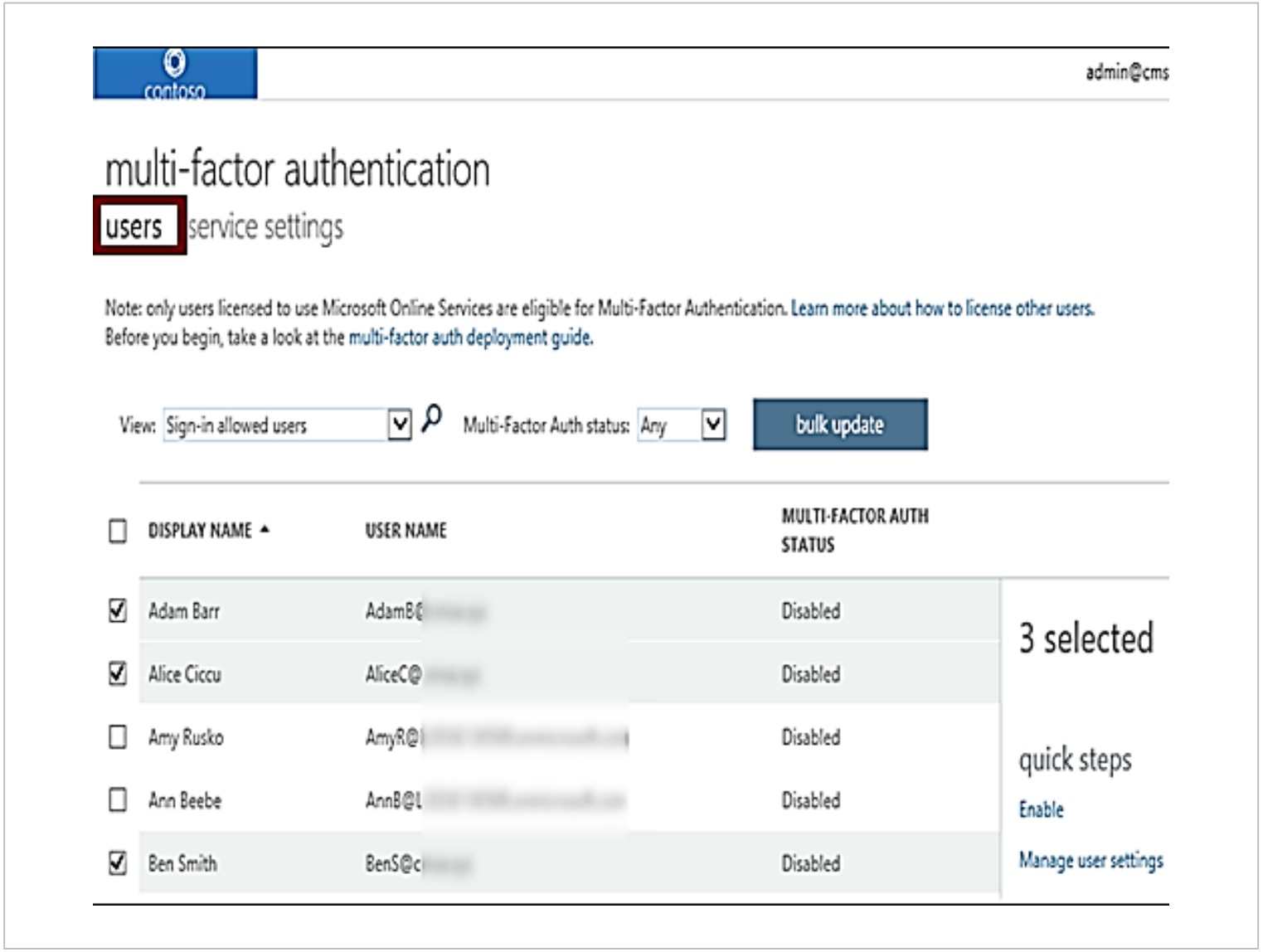
Enabling MFA

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

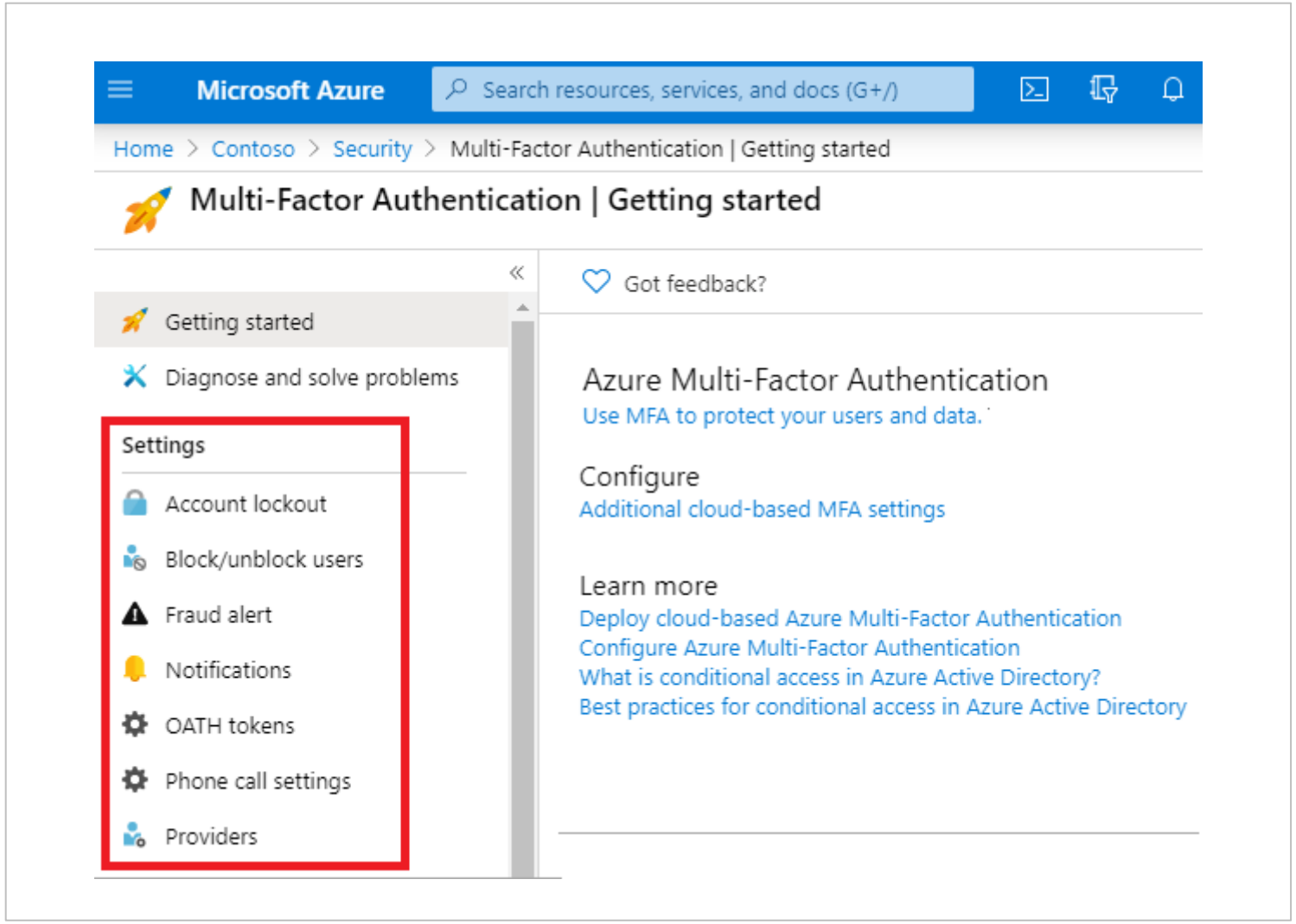


MFA Settings

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



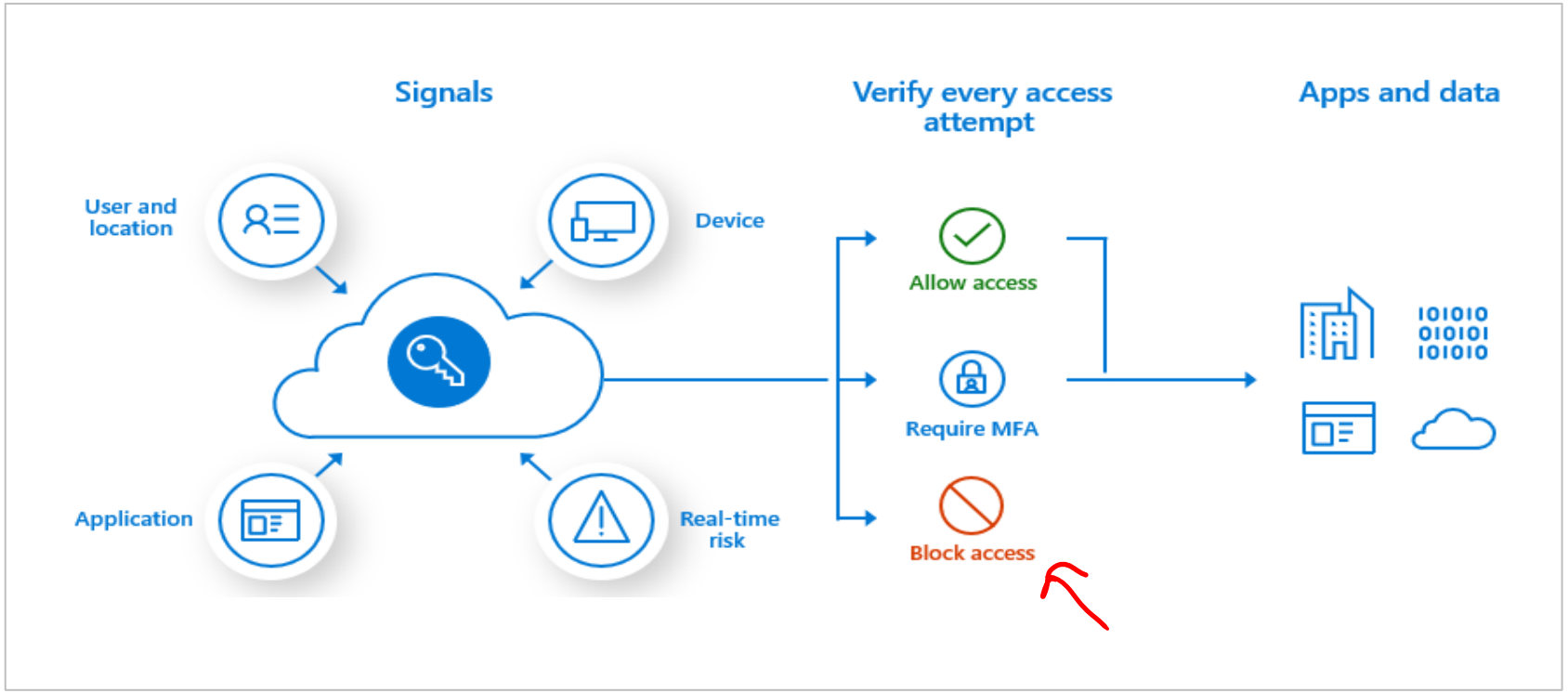
Azure AD Conditional Access

Identity management is the new control plane

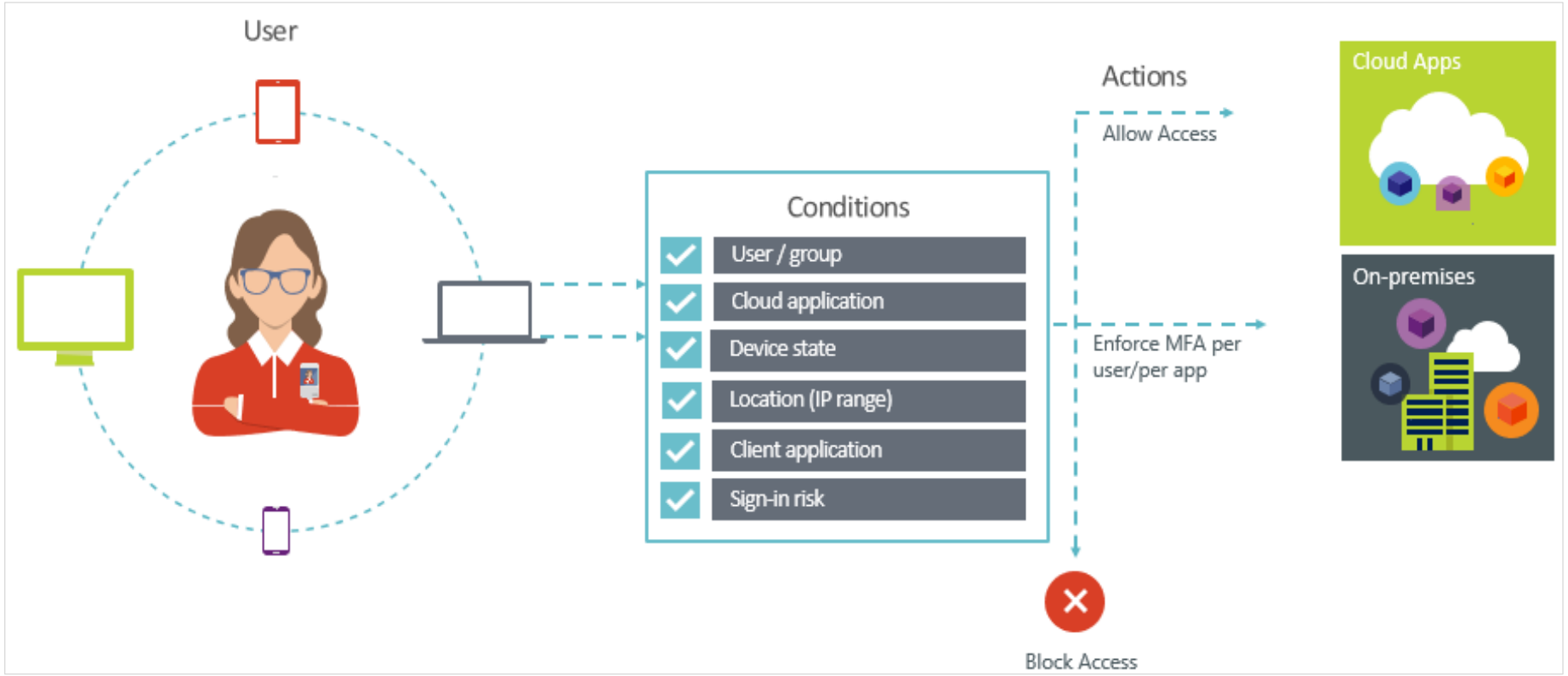
Use signals to make an informed decision

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

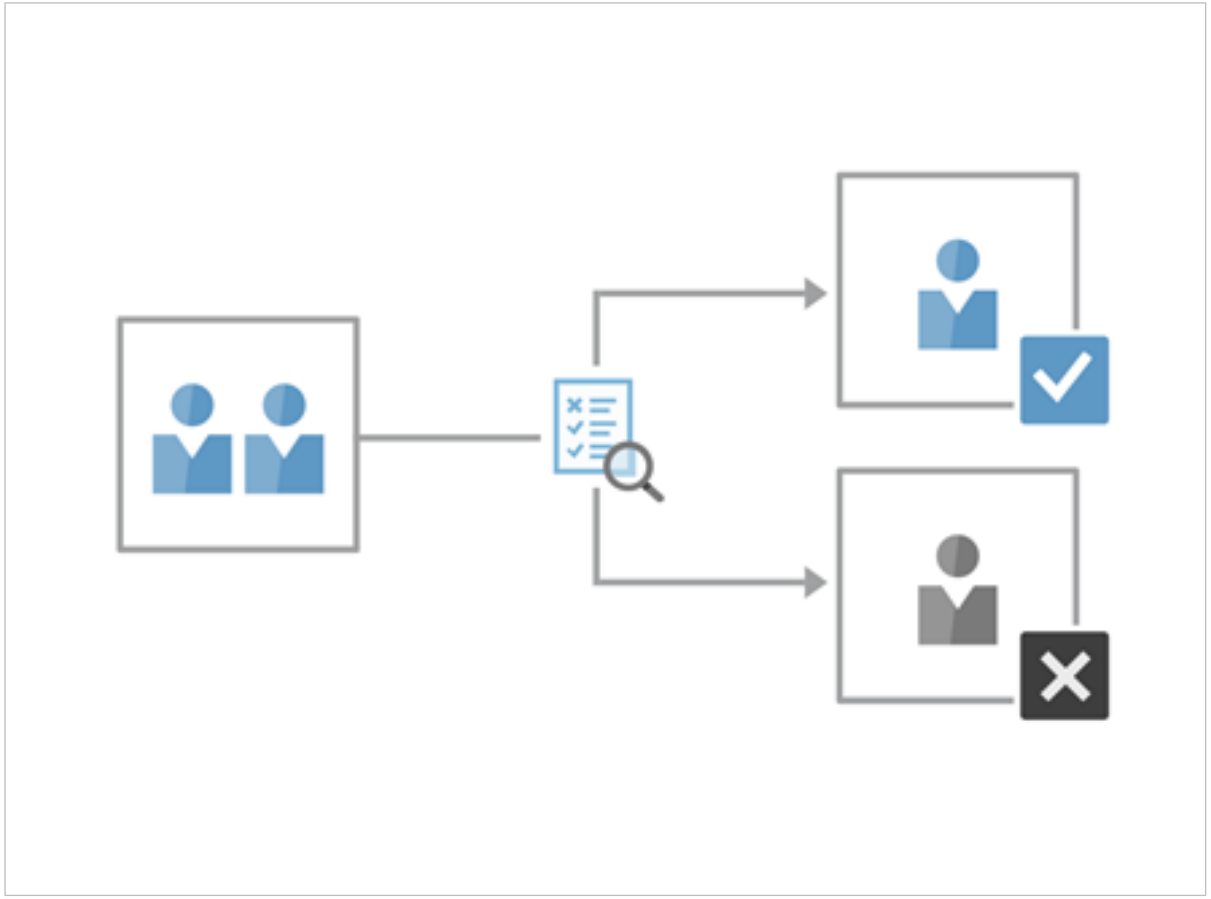
Evaluate guest user access

Evaluate employee access to applications and group membership

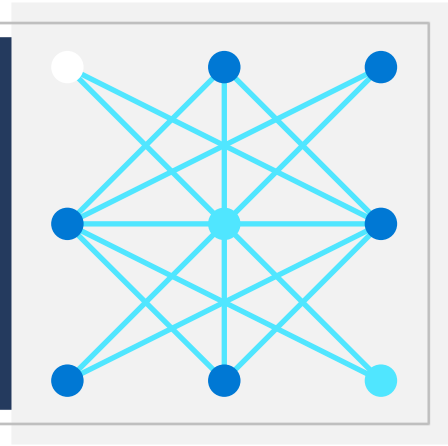
Track reviews for compliance or risk-sensitive applications

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

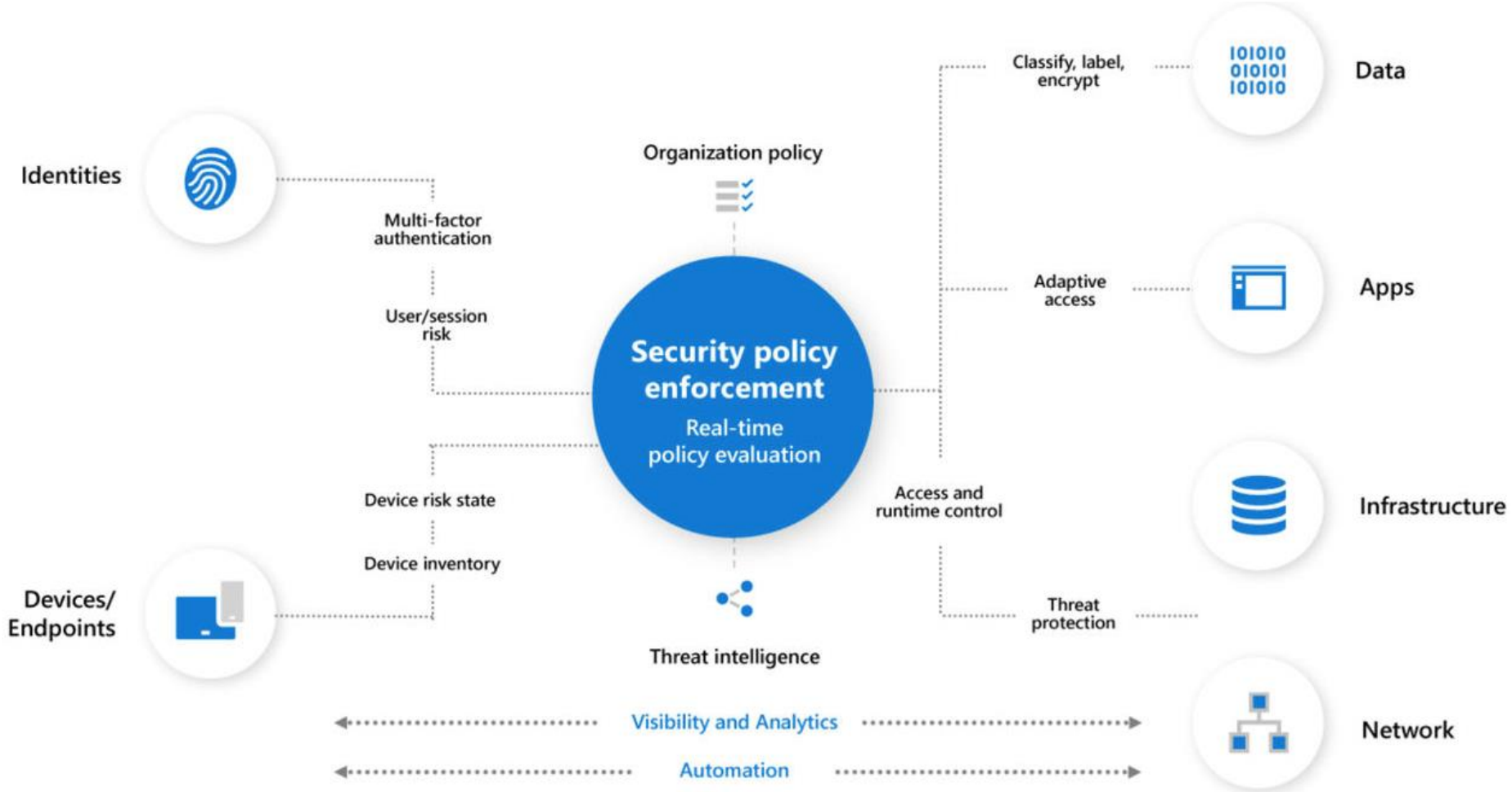
PIM Onboarding

PIM Configuration Settings

PIM Workflow

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)

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

Premium 2

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

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

eligebal

PIM Onboarding

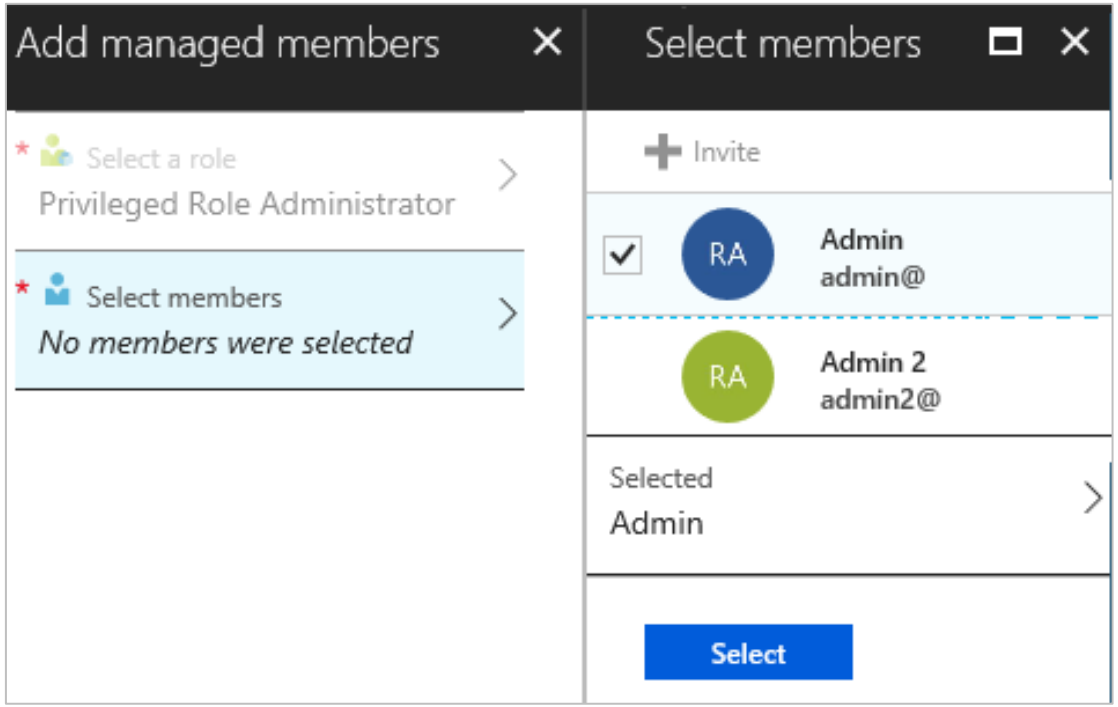
PIM automatically enable when a privileged role goes into **PIM** or **Roles and Administrators**

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

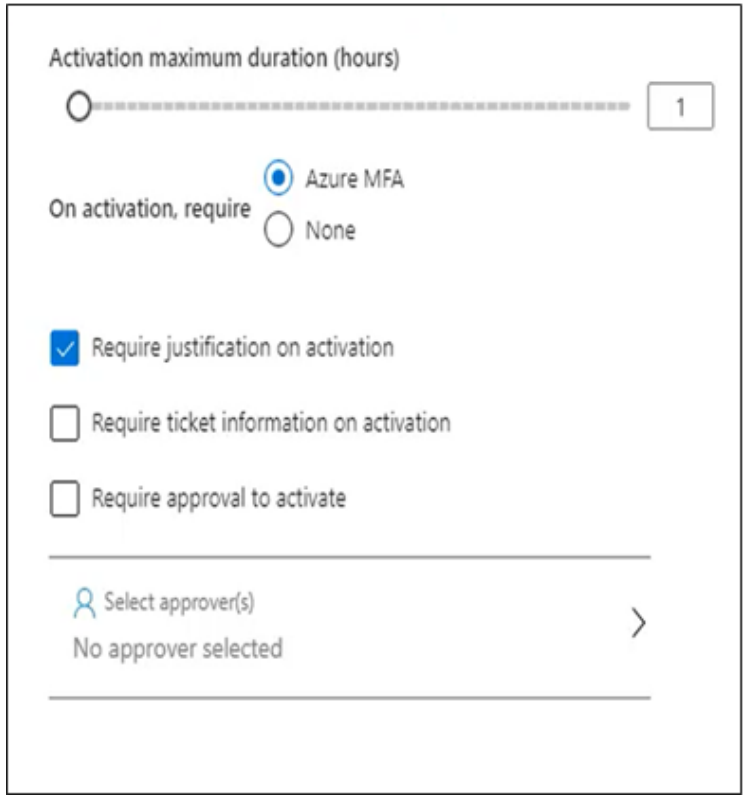
Ensure there are always at least two Privileged Role Administrators



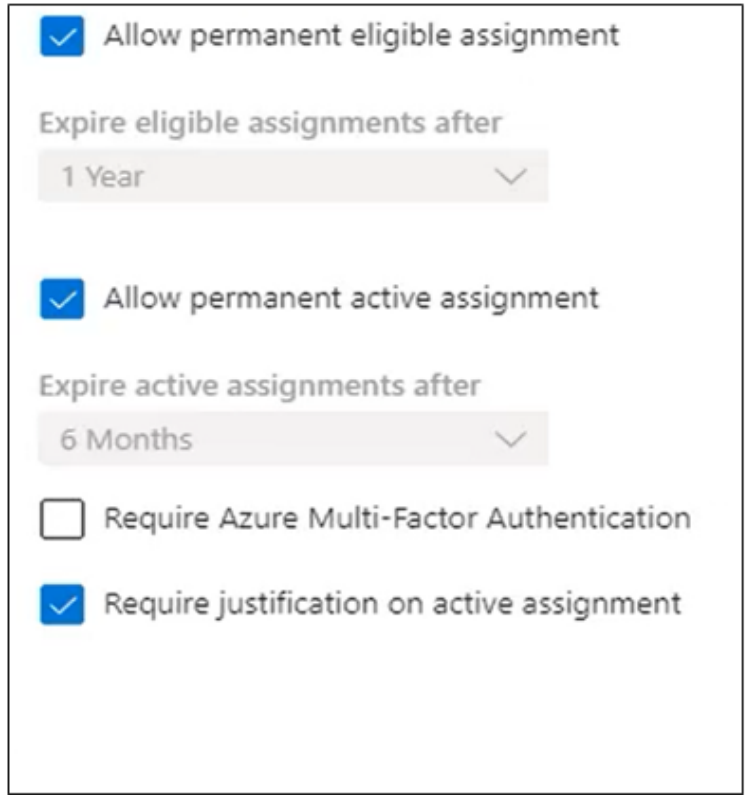
PIM Configuration Settings

Settings can be different for Azure AD roles and Azure resources

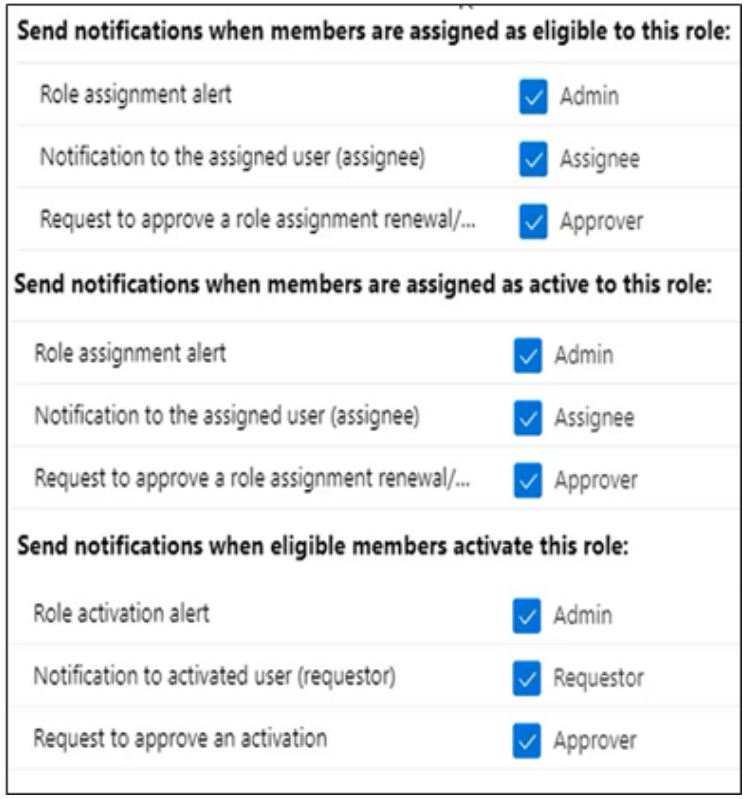
Activation



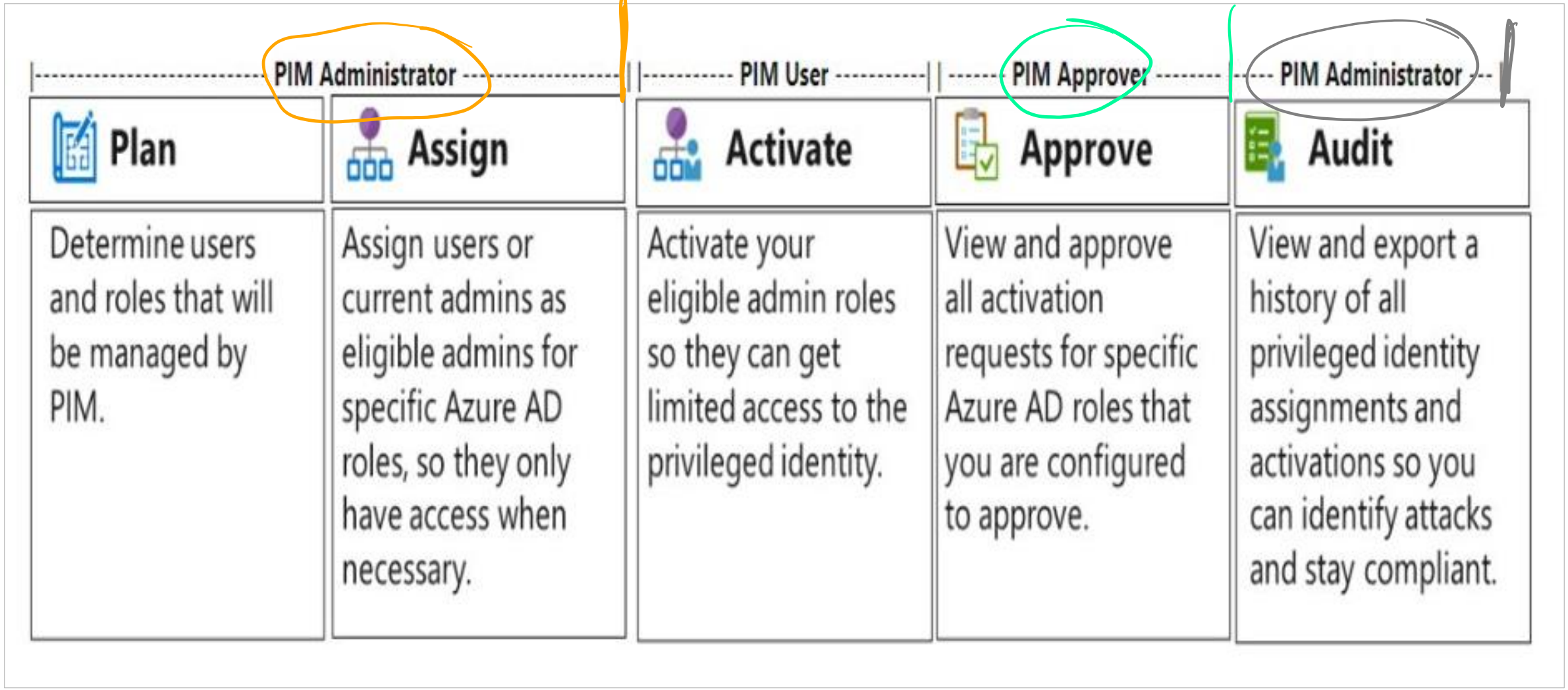
Assignment



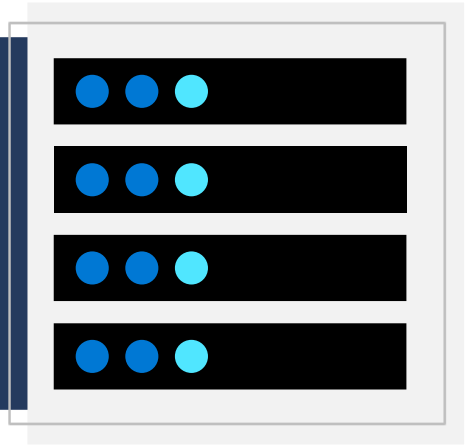
Notifications



PIM Workflow



Application Security



Application Security

Microsoft Identity Platform

Azure AD Application Scenarios

App Registration

Microsoft Graph Permissions

Managed Identities

Web App Certificates

Microsoft Identity Platform

Bicep → JSON → ARM → Azure

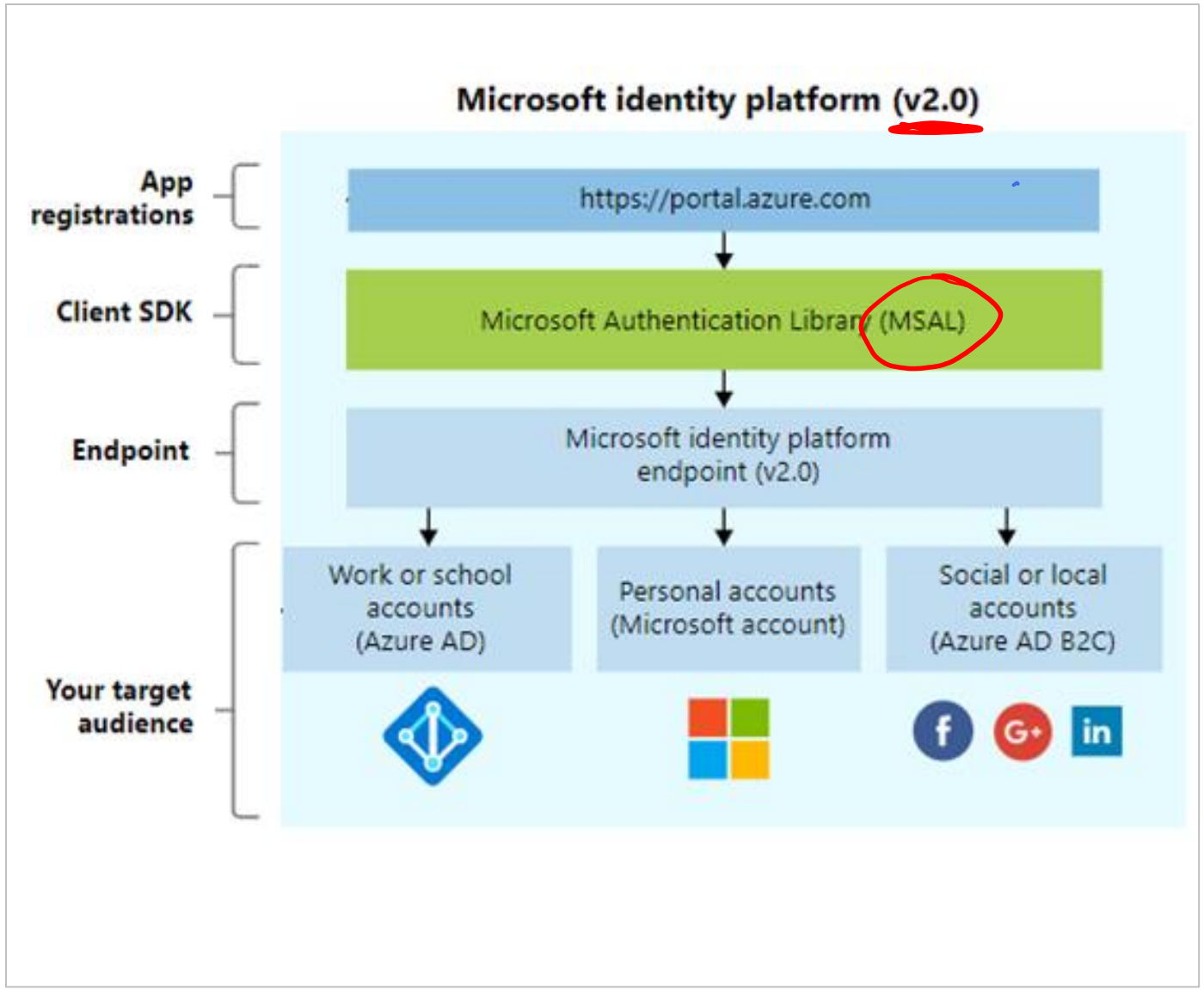
Write code once and authenticate any Microsoft identity into your application

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

M365



Azure AD Application Scenarios

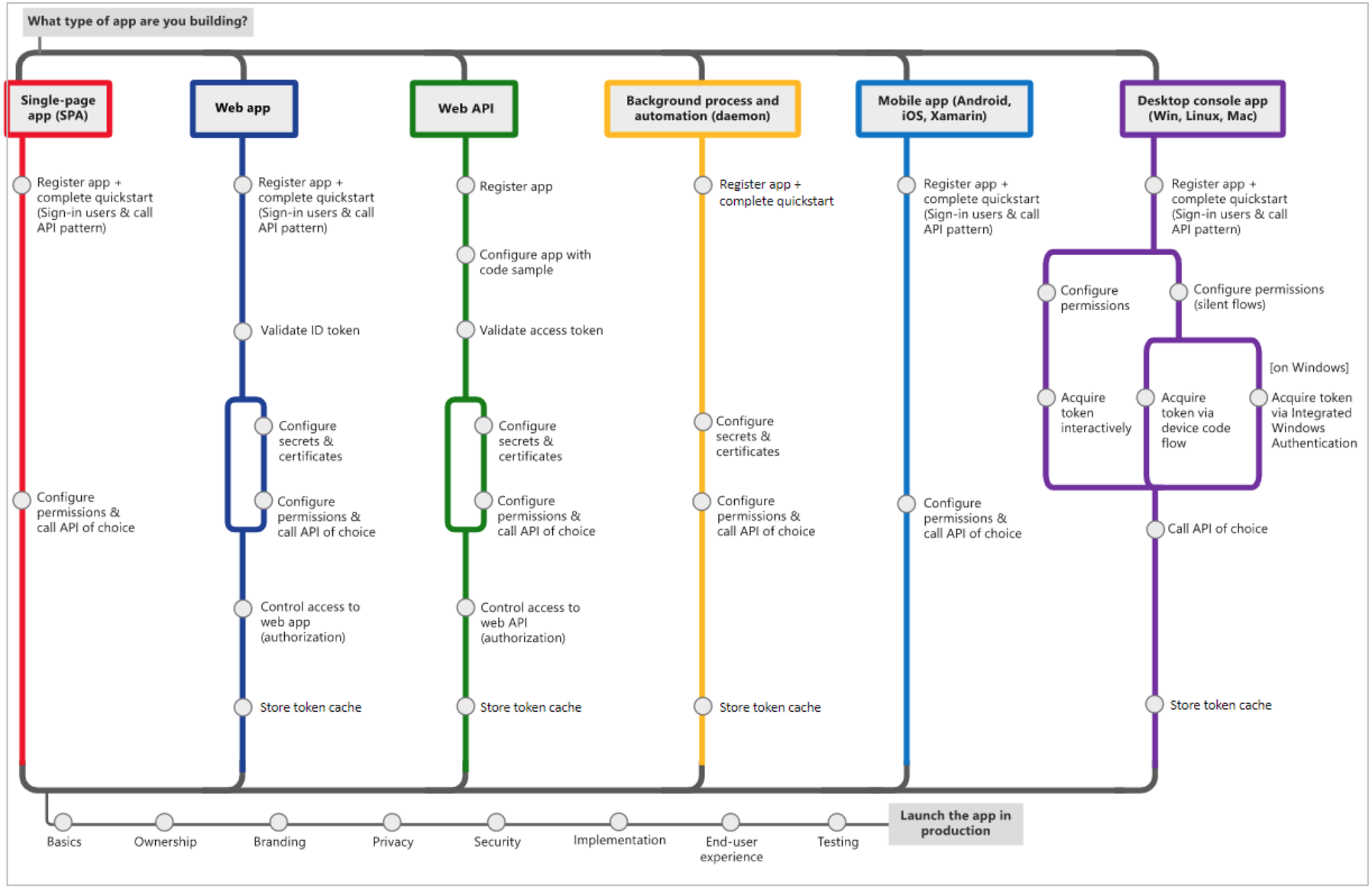
Single page frontends that run in a browser

Web browser to a web application

Web API on behalf of a user

Web applications that need resources from a web API

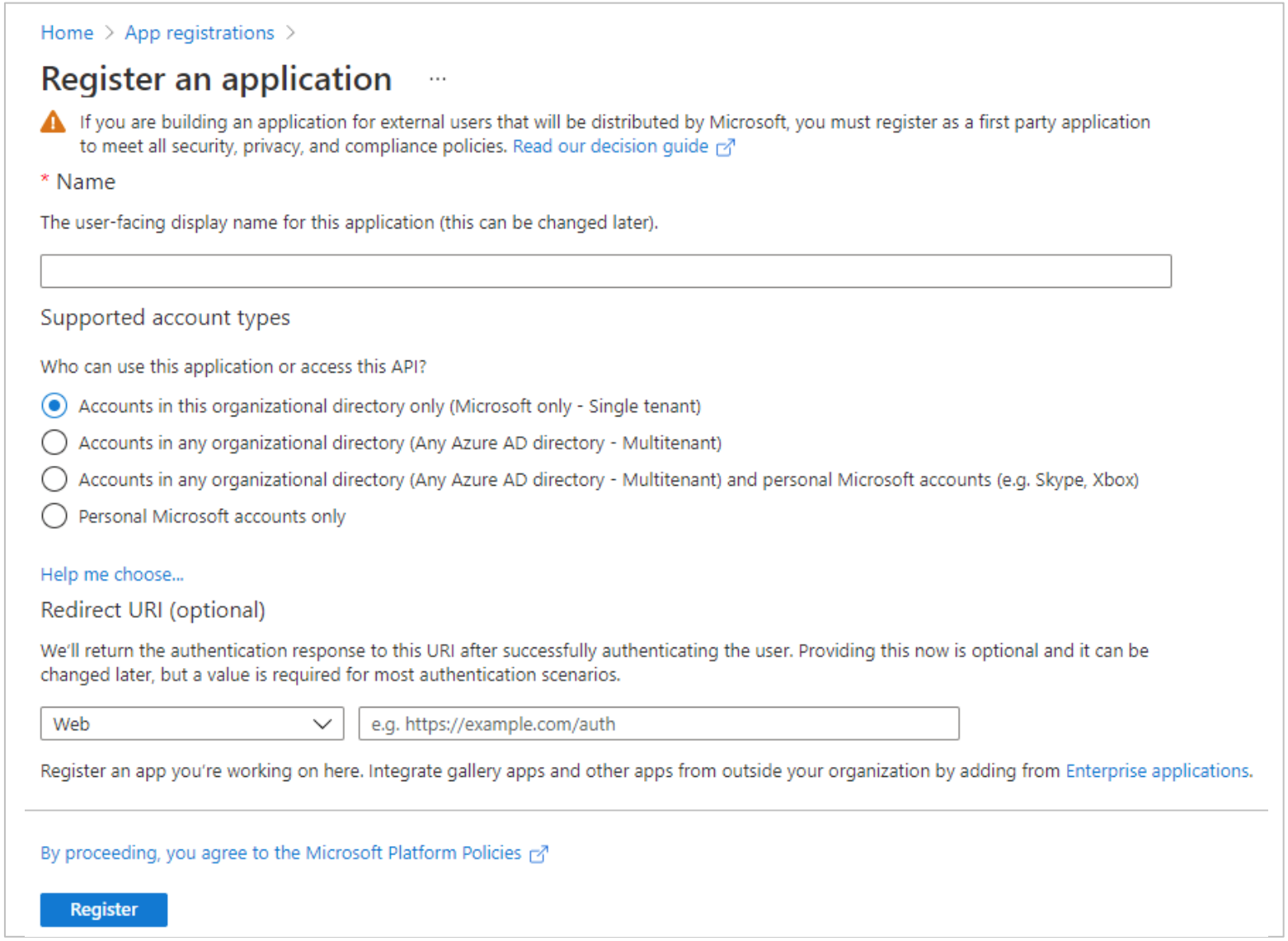
Daemon or server application that needs resources from a web API



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.



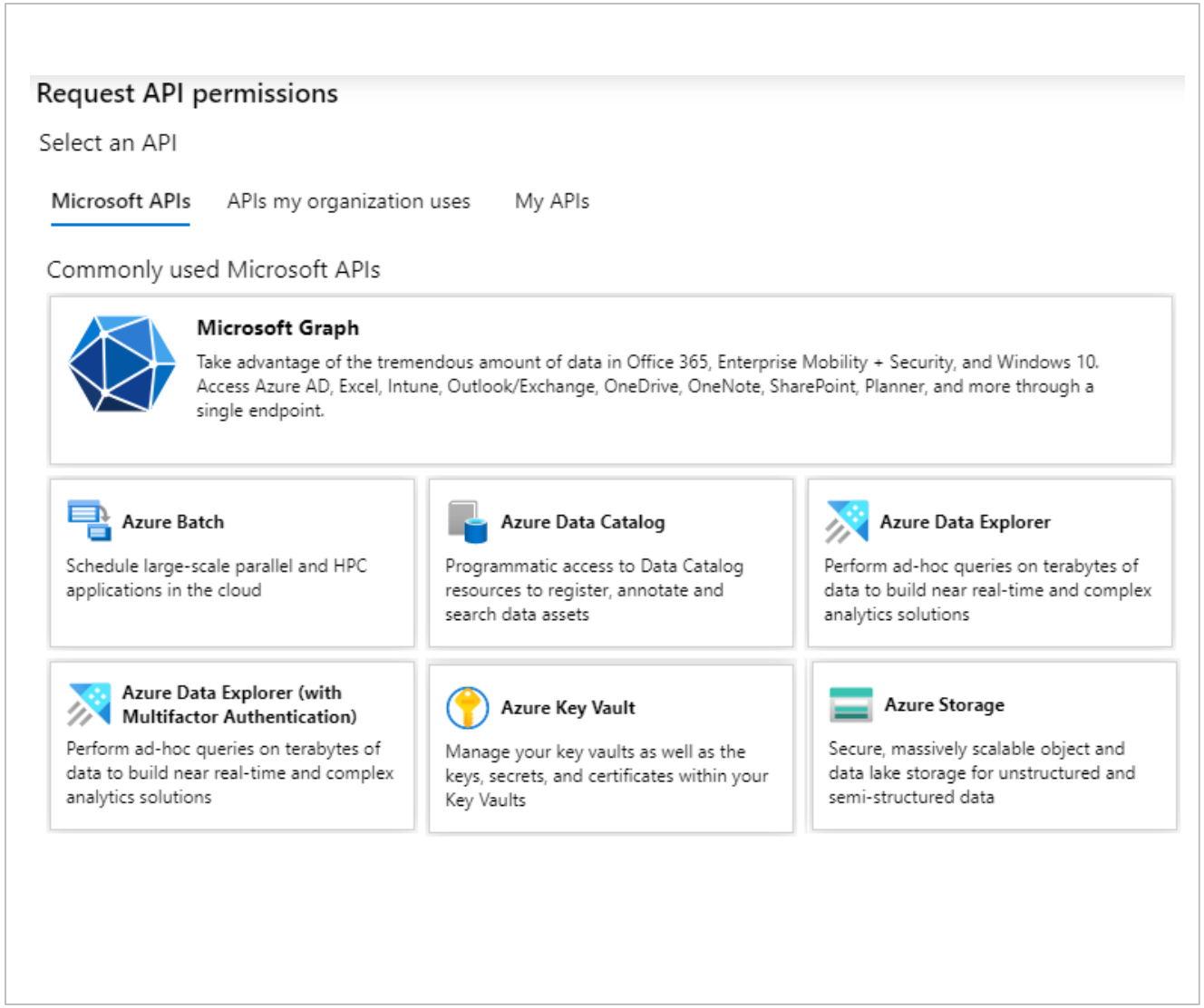
Microsoft Graph Permissions

Scope

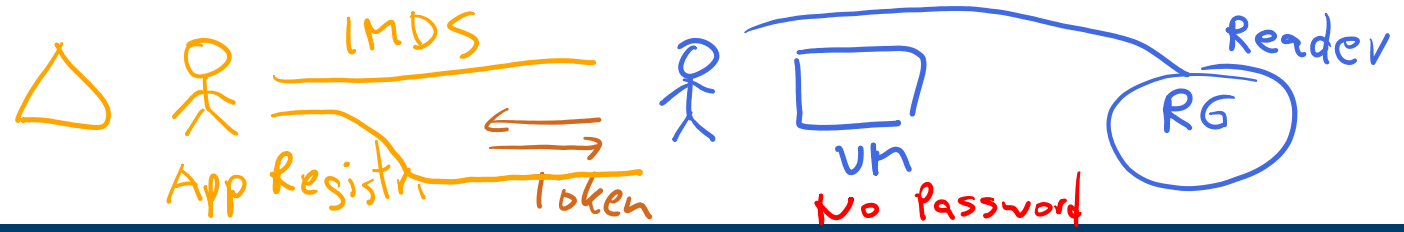
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process

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

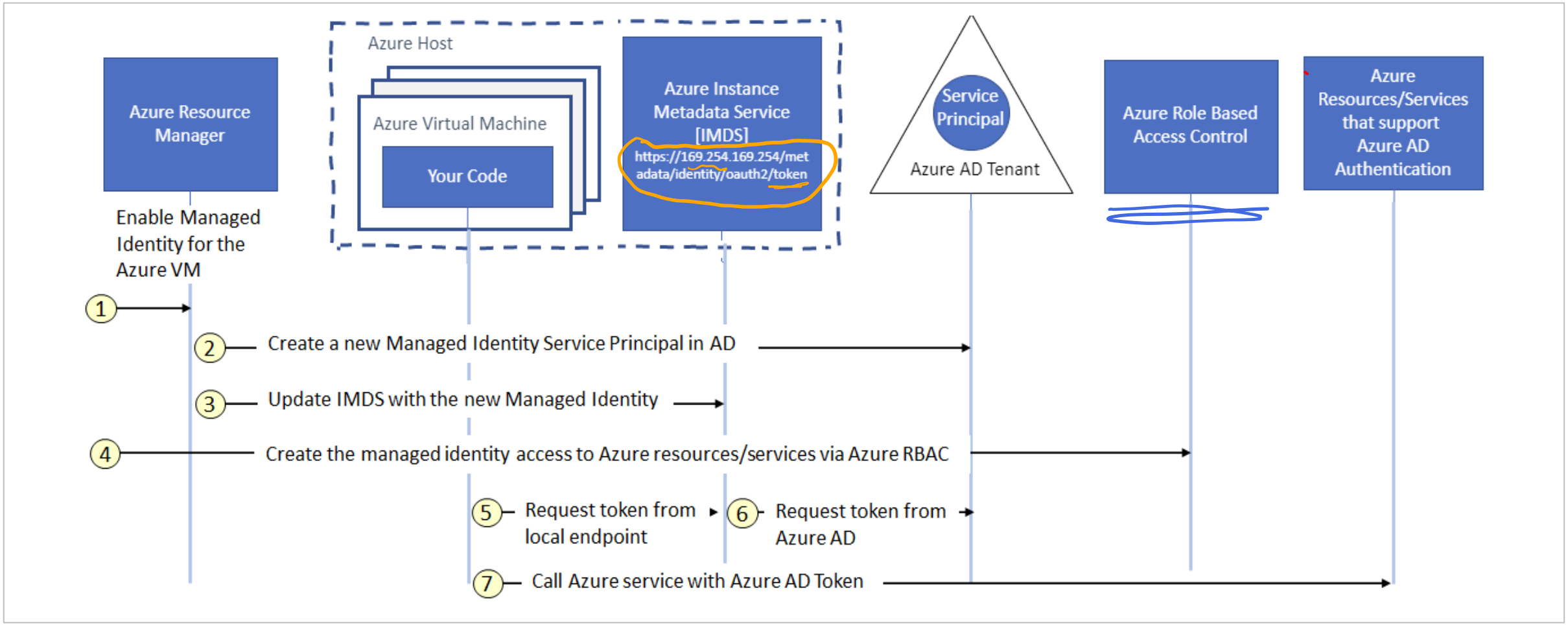
Application permissions are used by apps that run without a signed-in user present



Managed Identities



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



Tim Berners-Lee

www

Azure App Services
Overview

App Services

App Service Environments

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

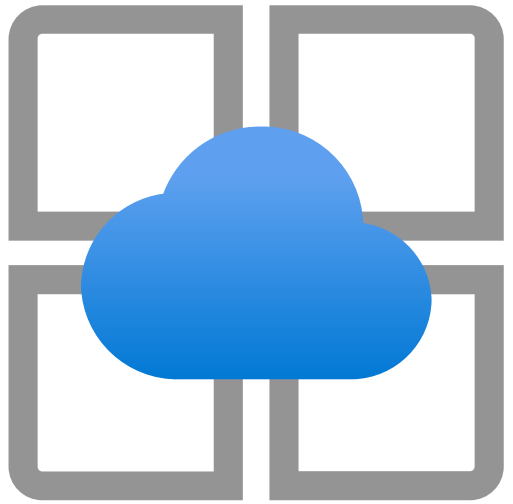
Internal line-of-business applications

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.

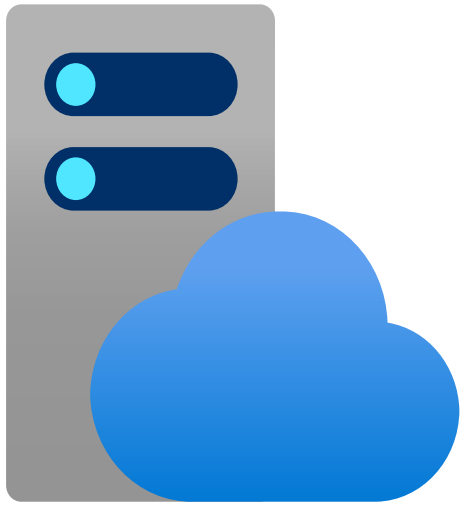
Operating System (Windows, Linux)

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)

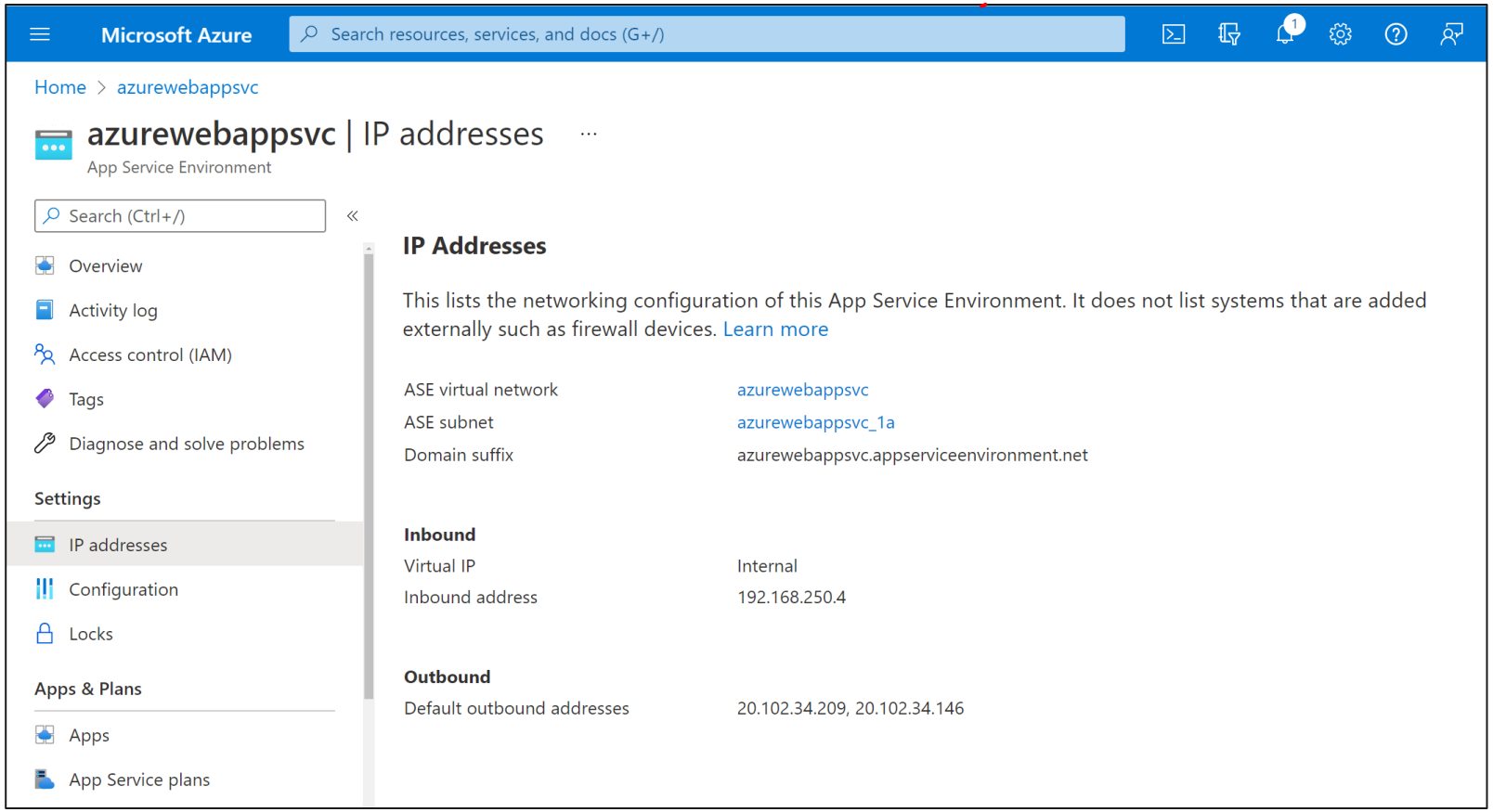


App Service Plans

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



Availability Zone Support for App Service Environments

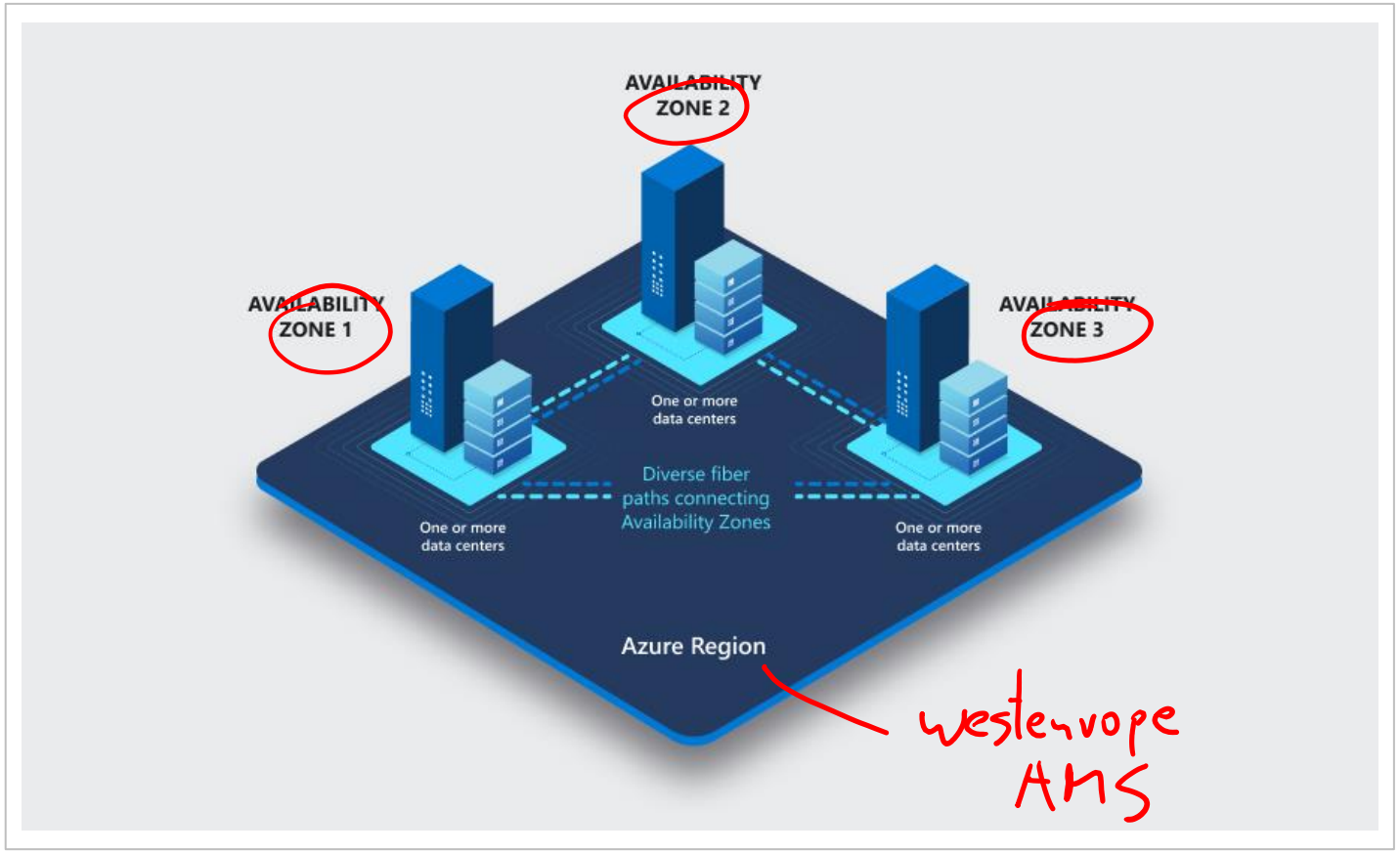
App services can be deployed across availability zones. The architecture is known as zone redundancy.

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.

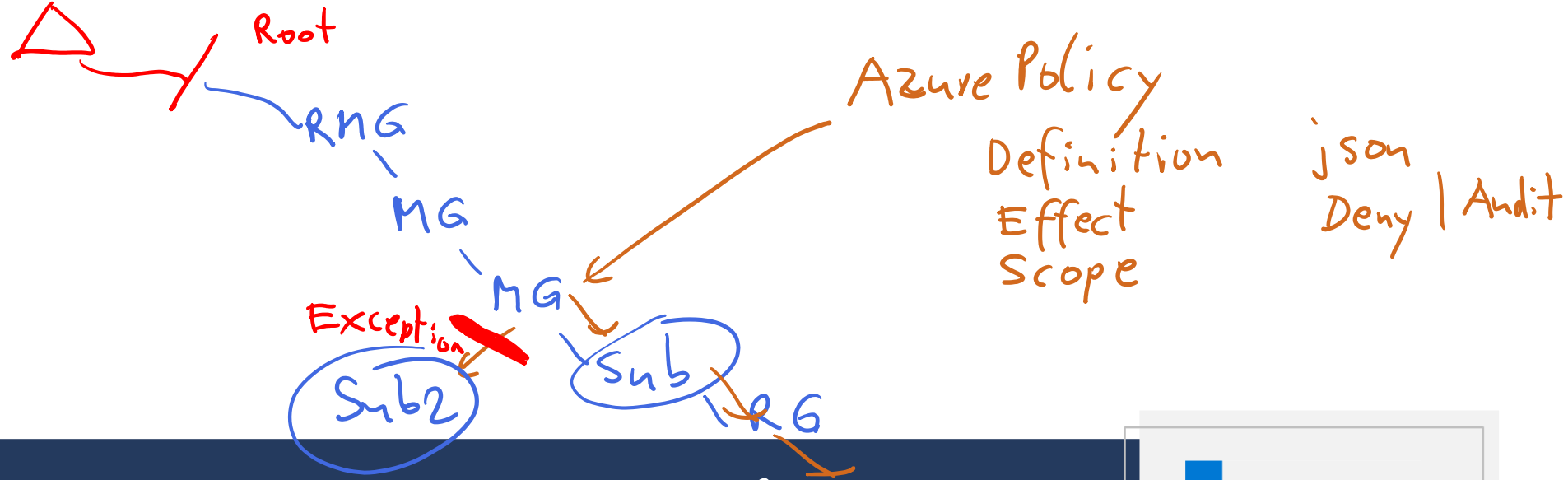


App Service Environment Certificates

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

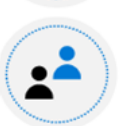
Azure Policy

Azure Role Based Access Control (RBAC)

Azure RBAC vs Azure Policies

Built-in Roles

Resource Locks



Azure Blueprints

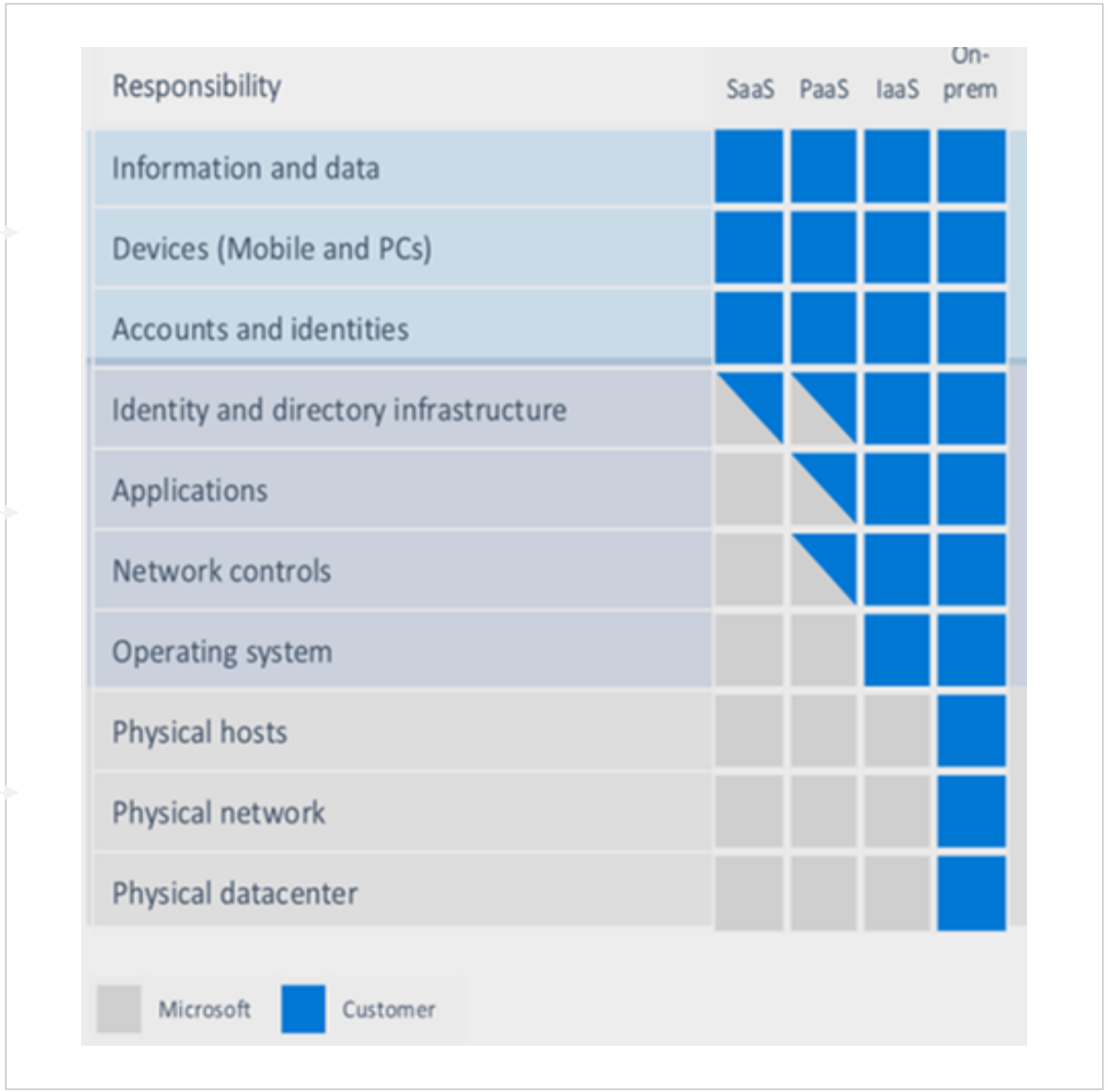
Azure Subscription Management

Shared Responsibility Model

Responsibility always retained by the customer

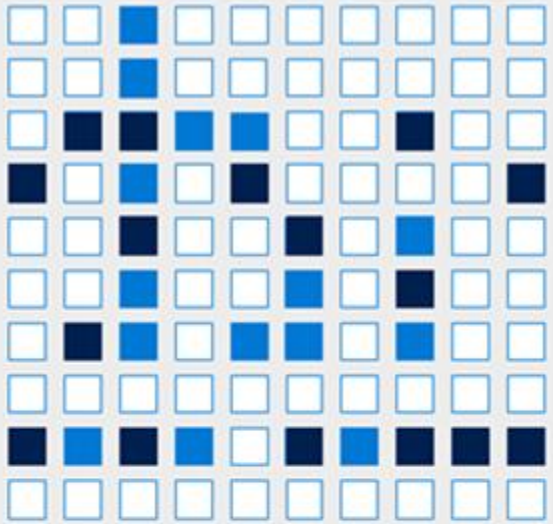
Responsibility varies by service type

Responsibility transfers to cloud provider

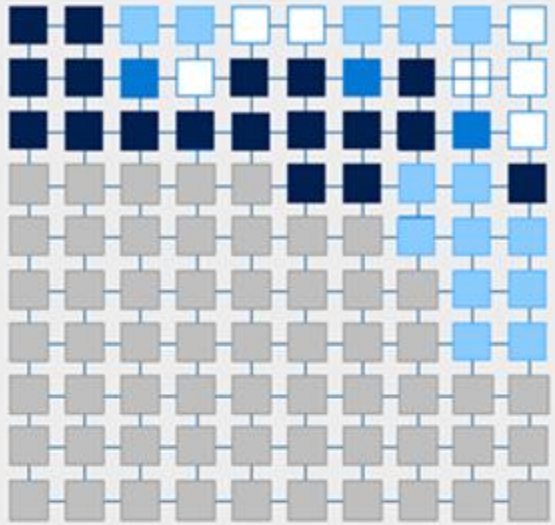


Azure Cloud Security Advantages

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:

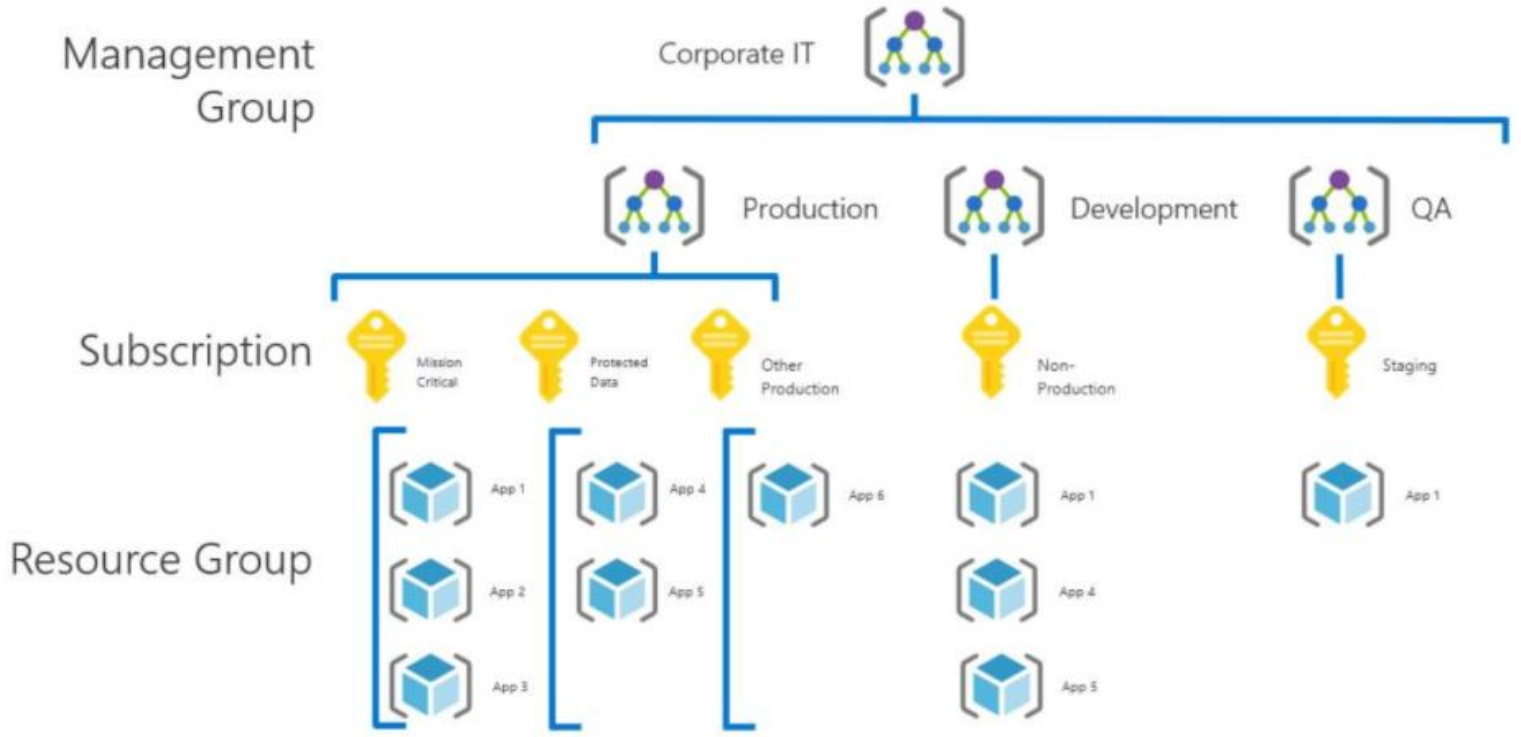
- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use cloud intelligence to improve detection/response time

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

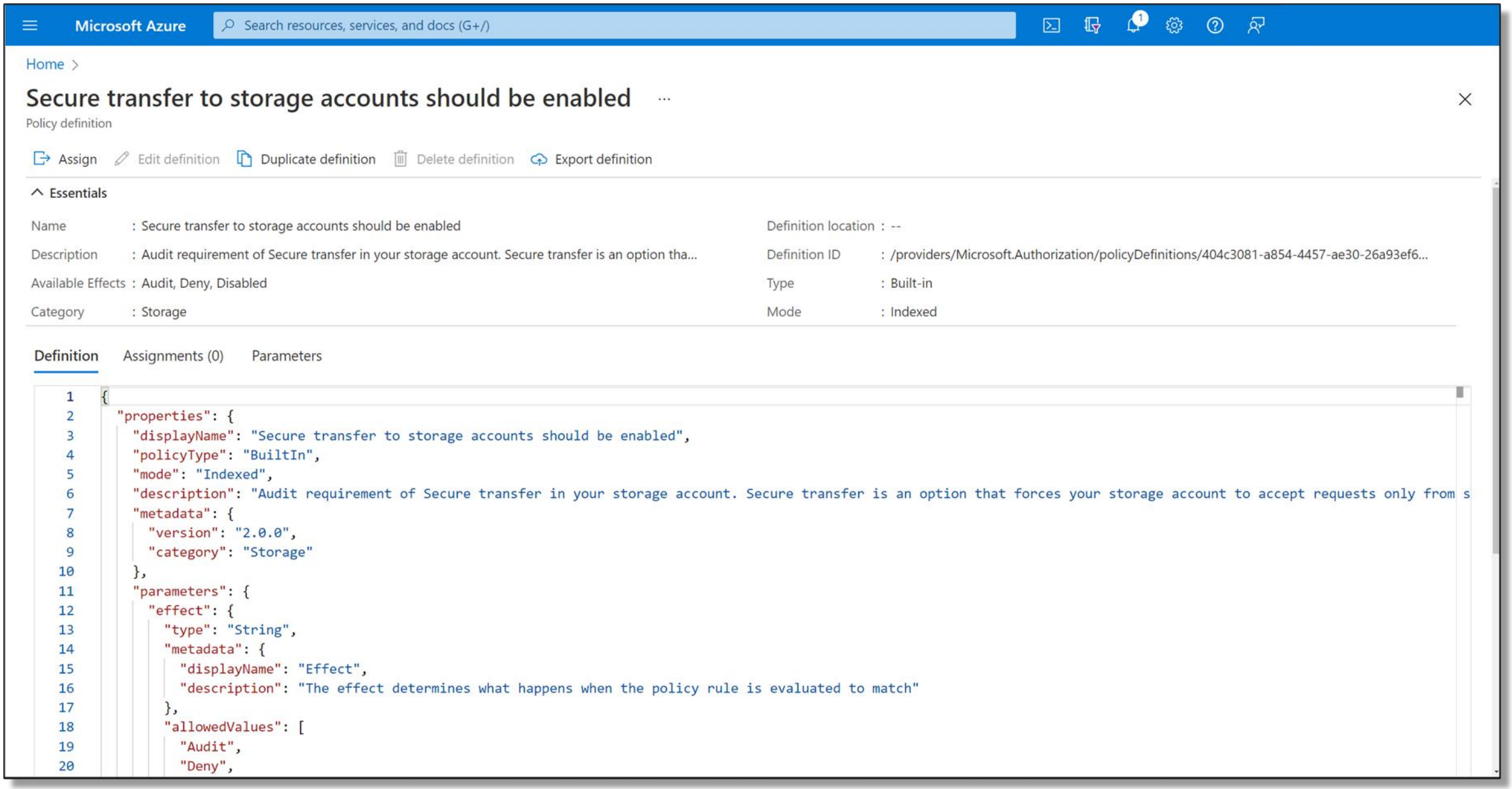
Advantages:

- Enforcement and compliance
- Apply policies at scale
- Remediation

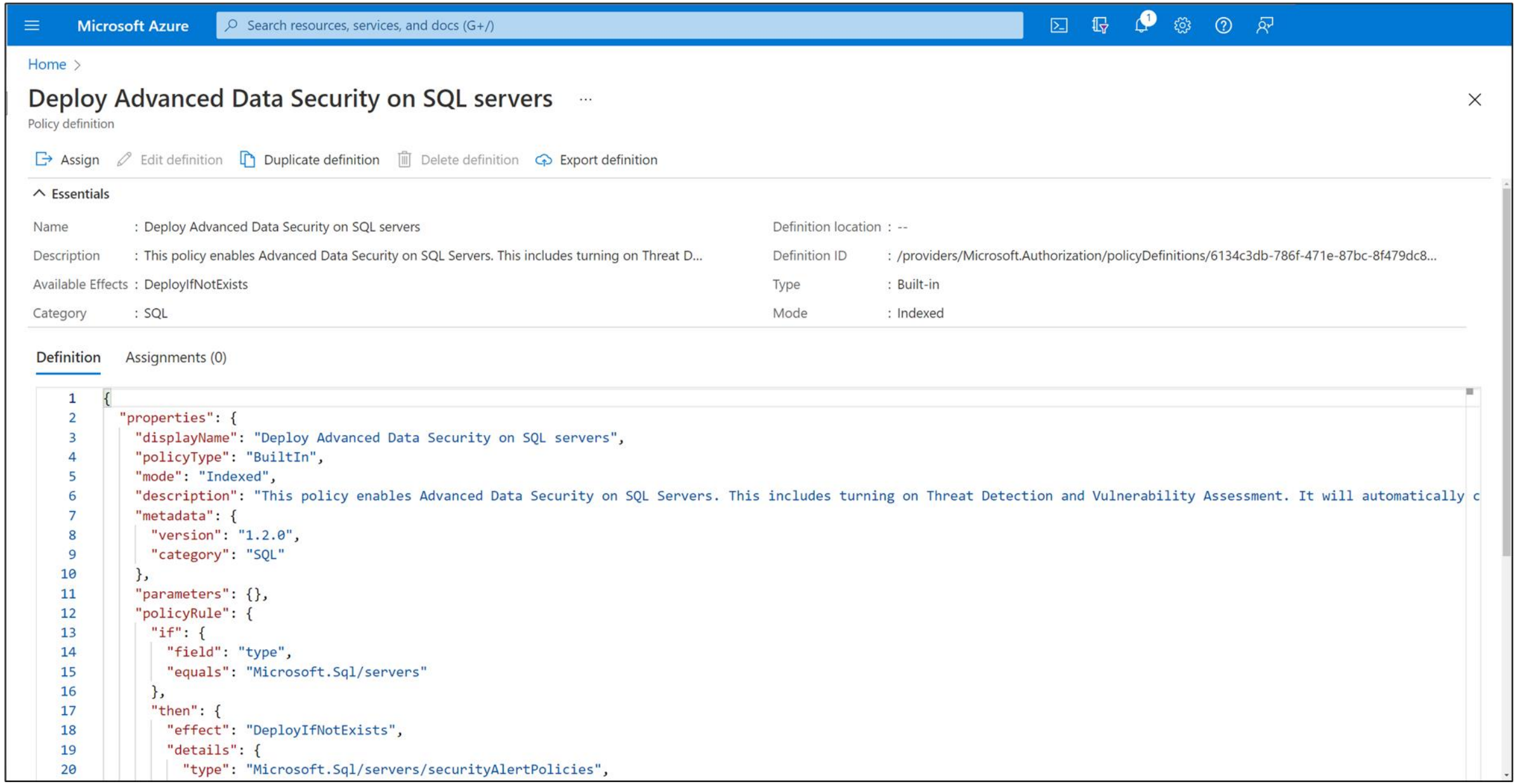
Usage Cases
Allowed resource types - Specify the resource types that your organization can deploy.
Allowed virtual machine SKUs – Specify a set of virtual machine SKUs that your organization can deploy.
Allowed locations – Restrict the locations your organization can specify when deploying resources.
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.

Key : Value
CC : 471

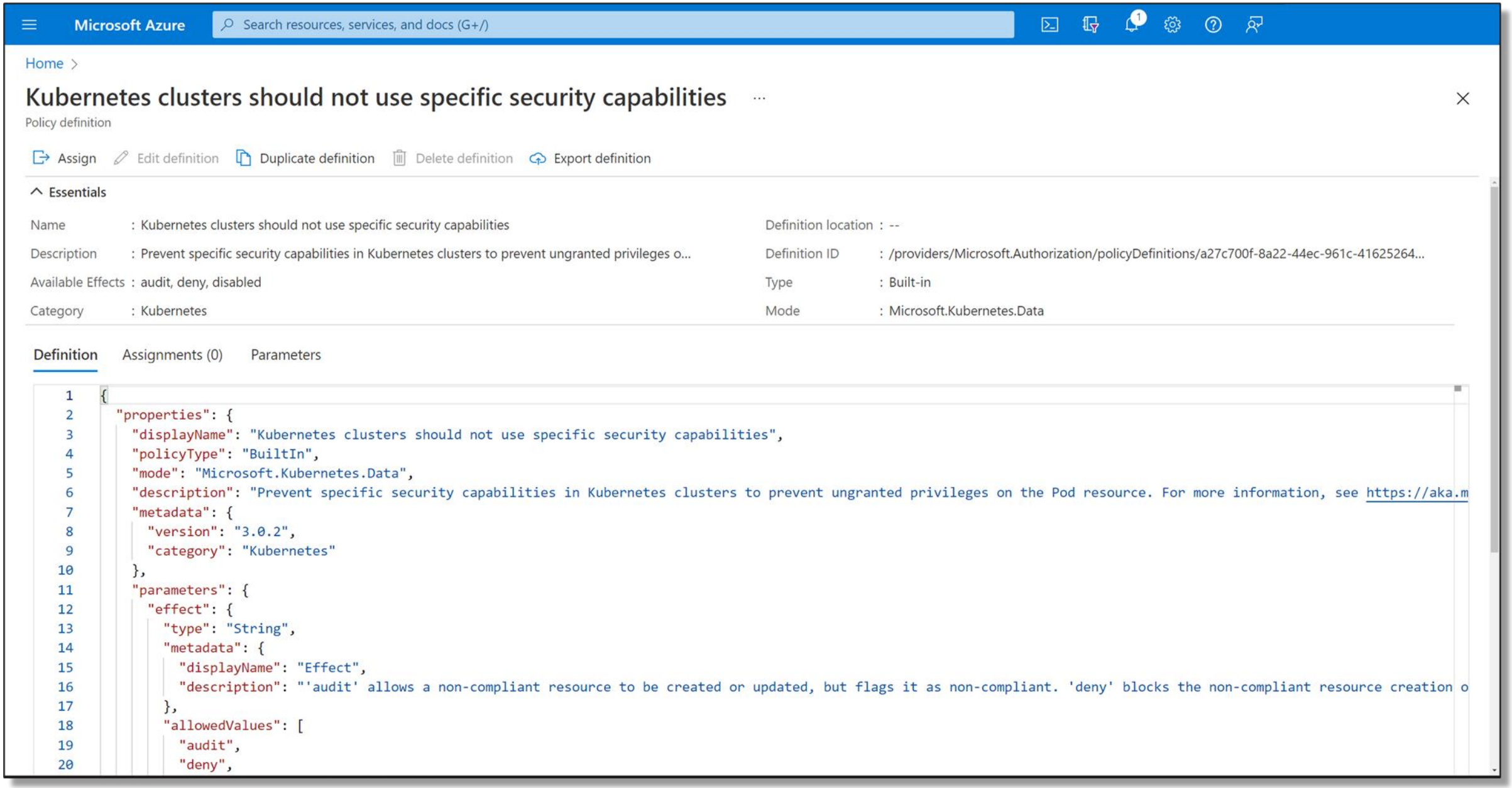
Azure Policy – Storage



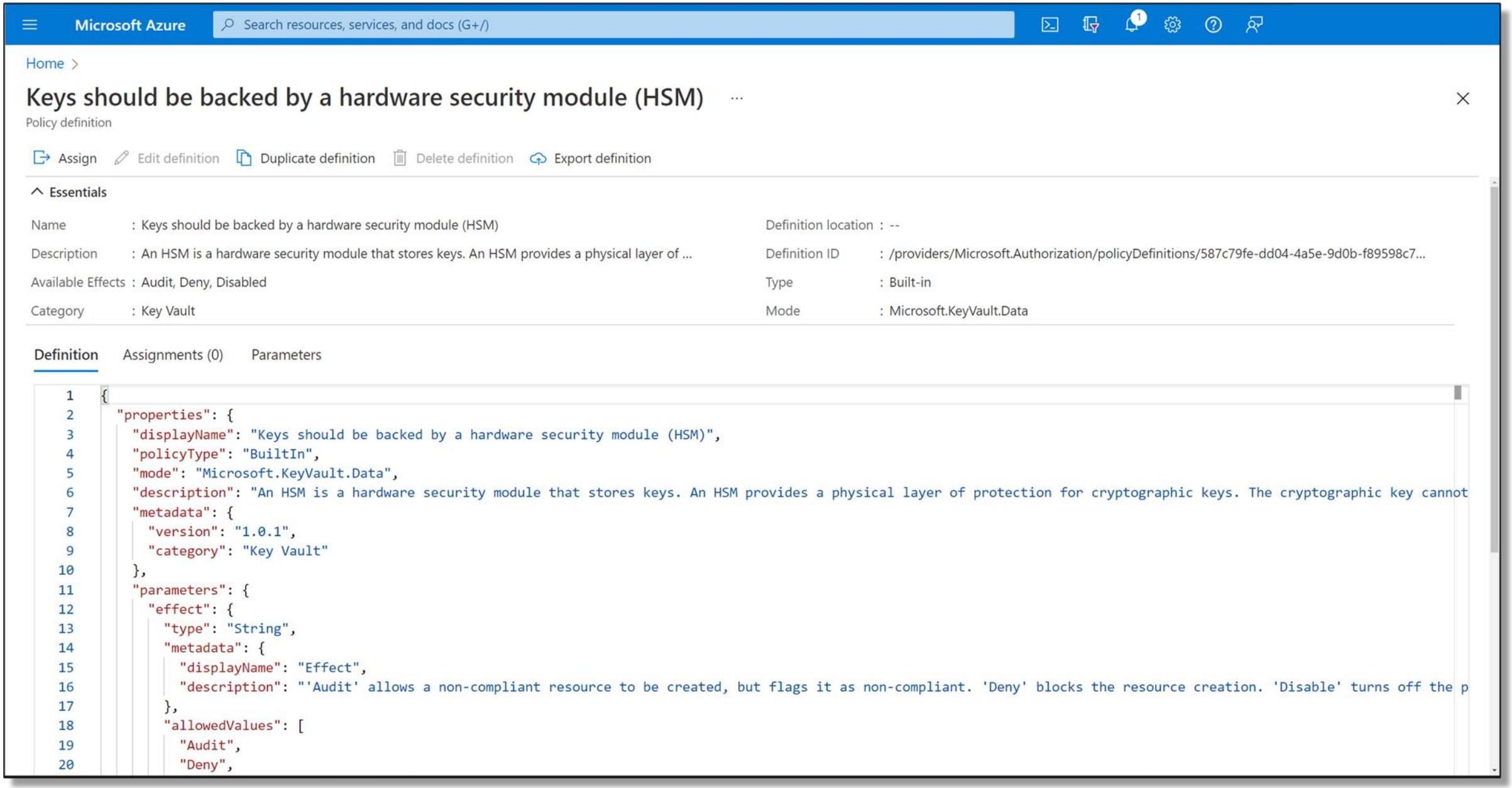
Azure Policy – SQL



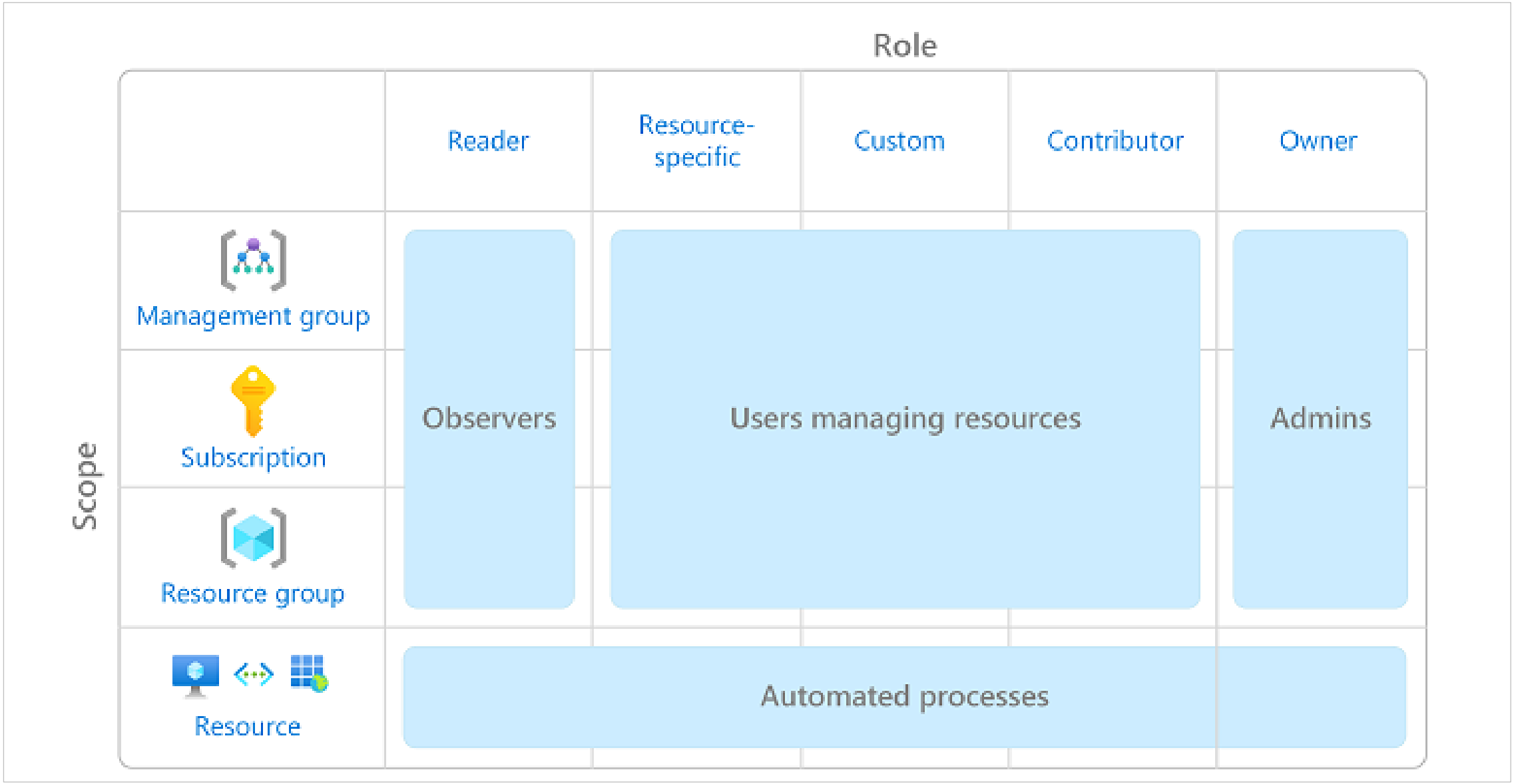
Azure Policy – Kubernetes



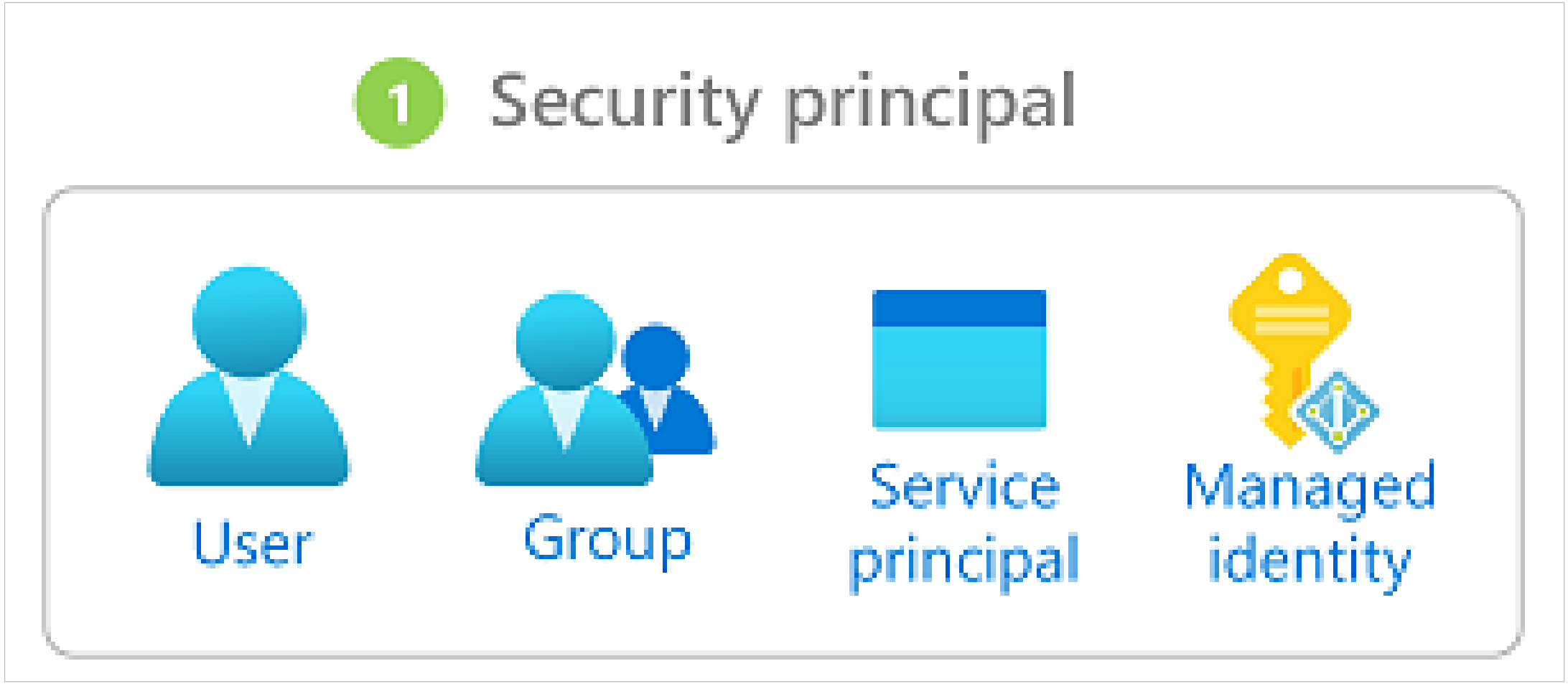
Azure Policy – Key Vault



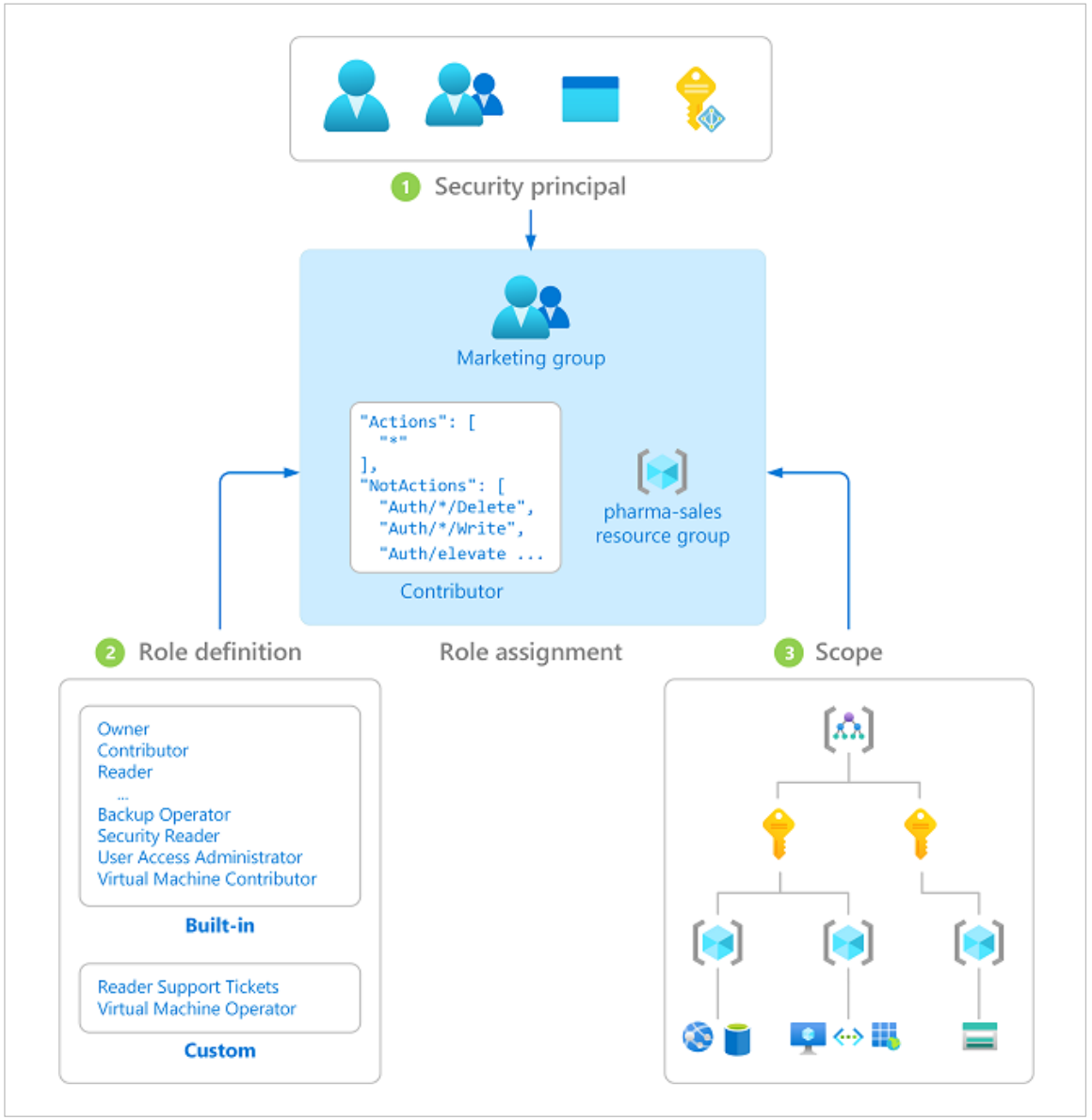
Azure Role-Based Access Control



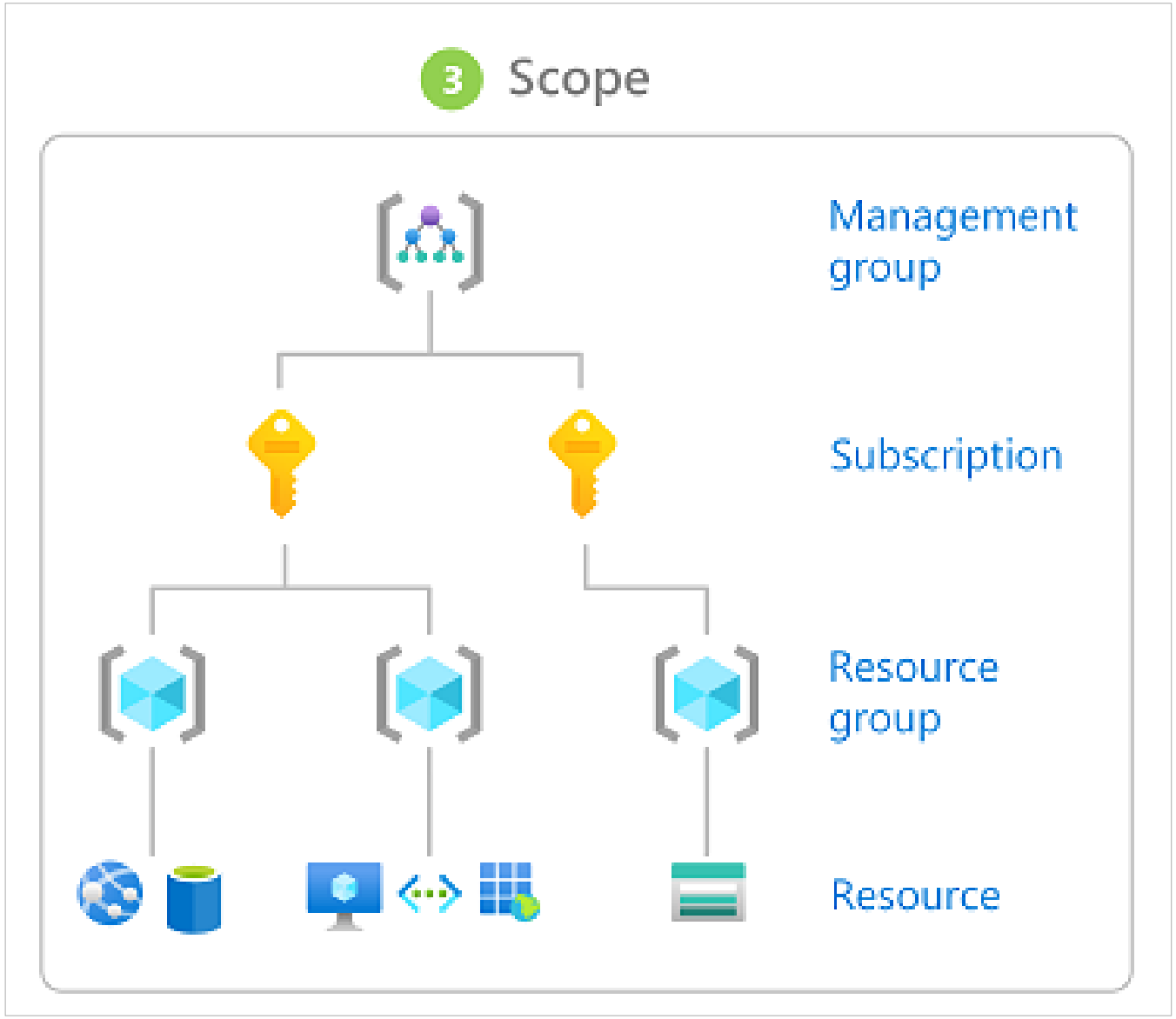
Azure Role-Based Access Control – Security Principal



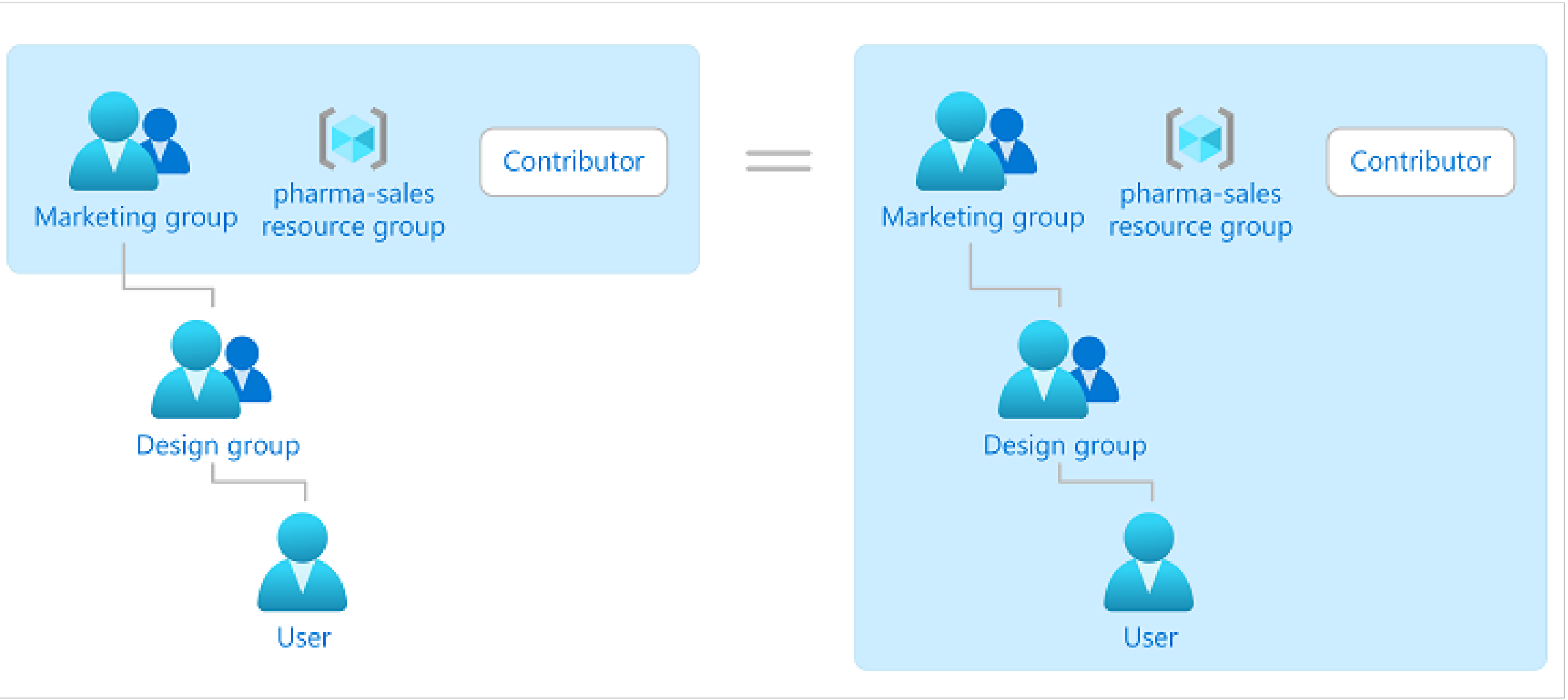
Azure Role-Based Access Control – Role Assignments



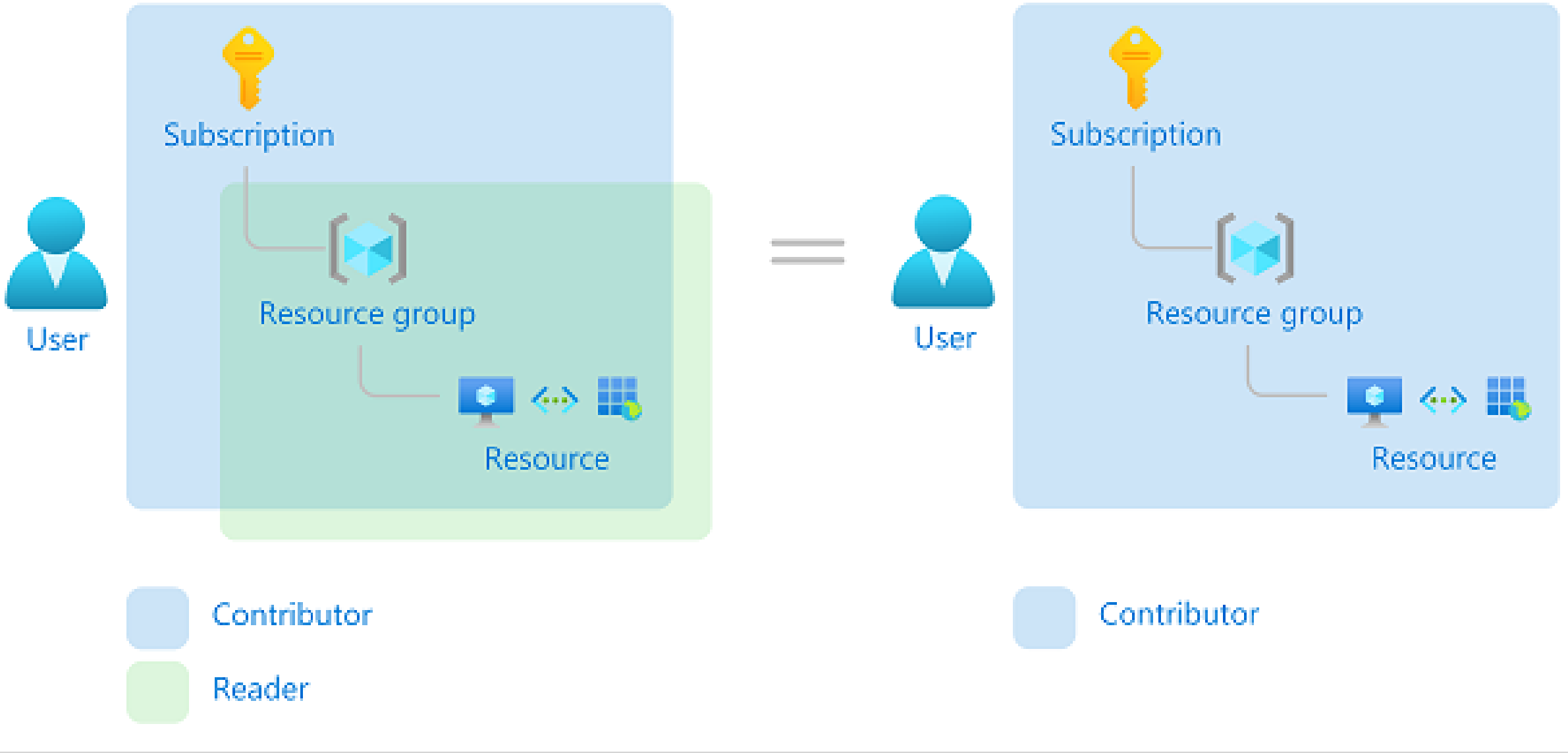
Azure Role-Based Access Control – Scope



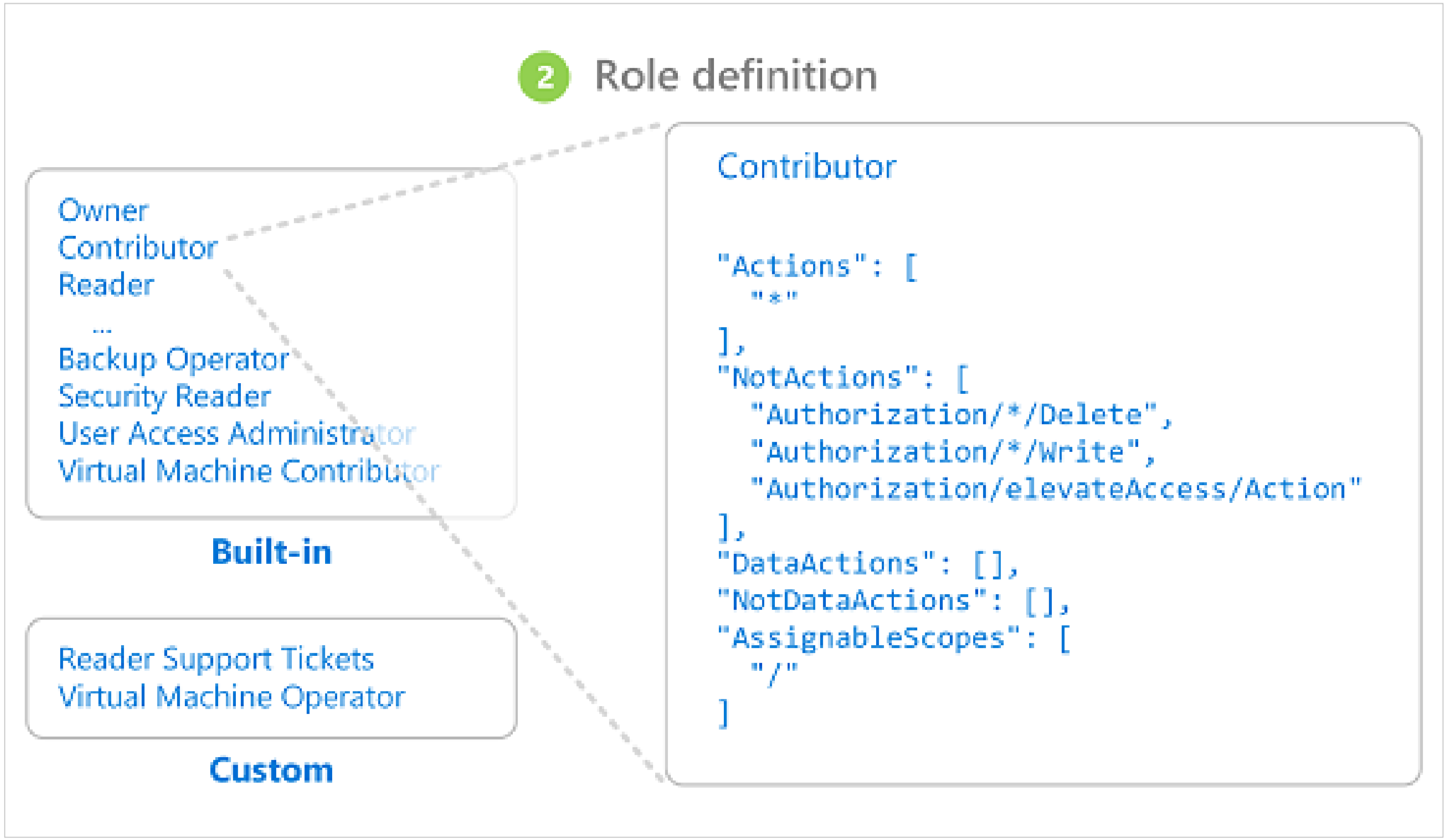
Azure Role-Based Access Control – Groups



Azure Role-Based Access Control – Multiple role assignments

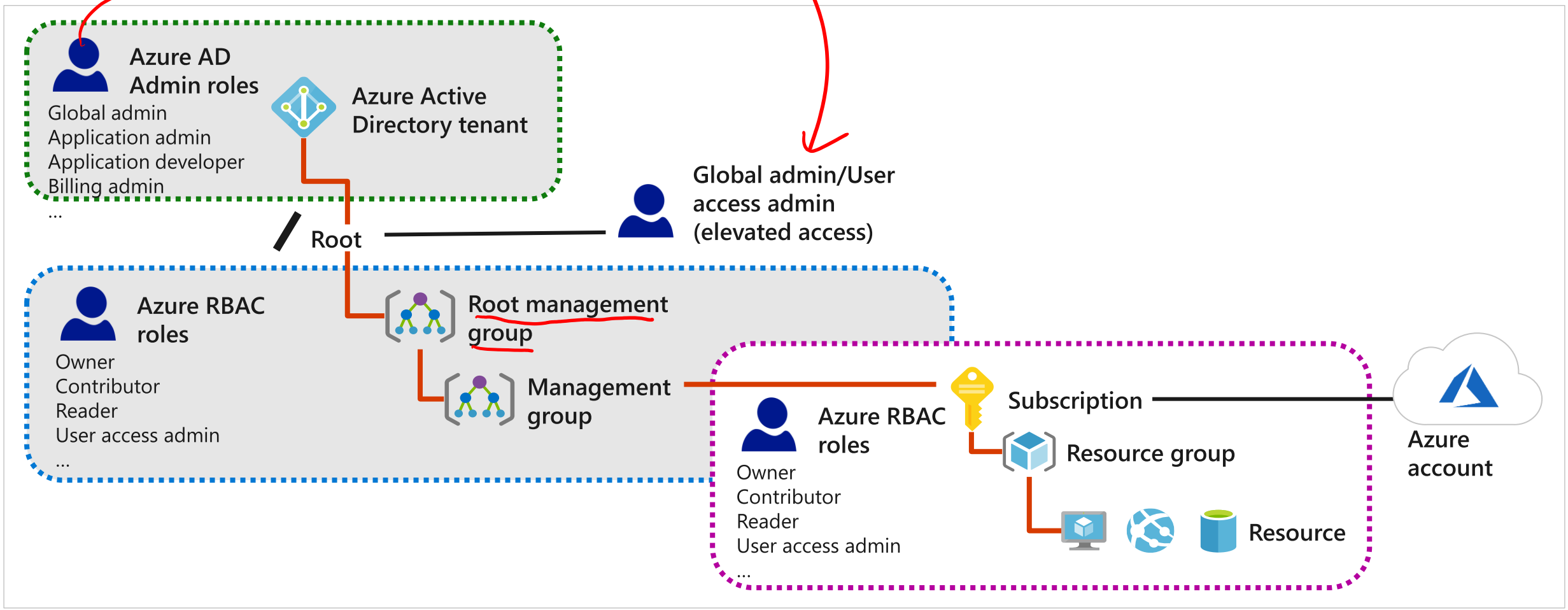


Azure Role-Based Access Control – Role Definition

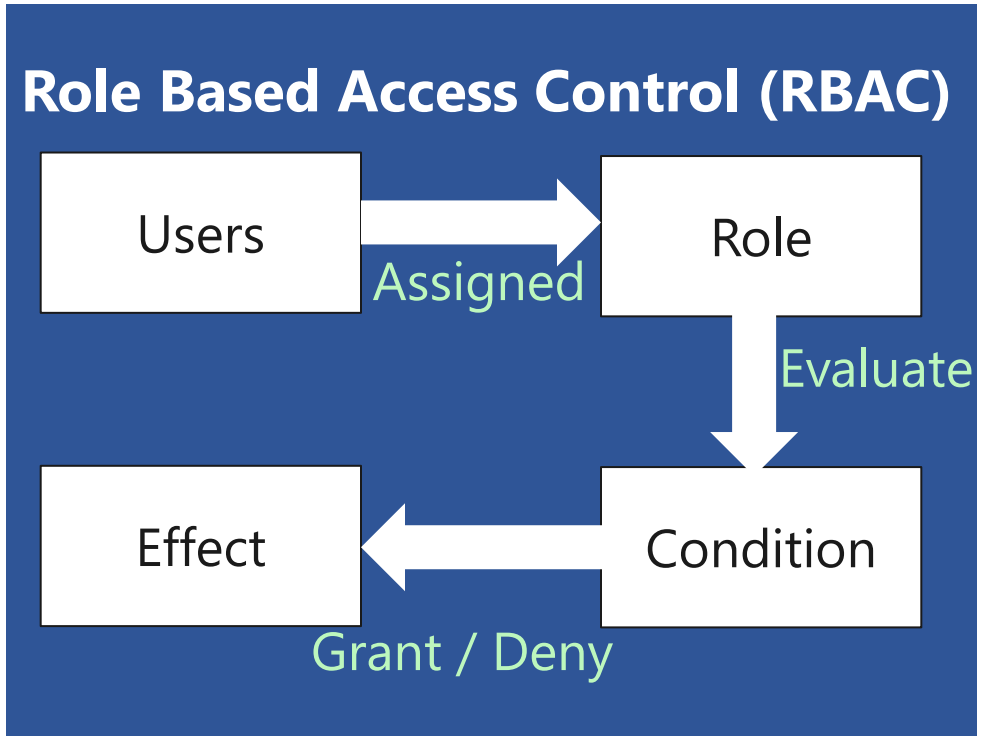


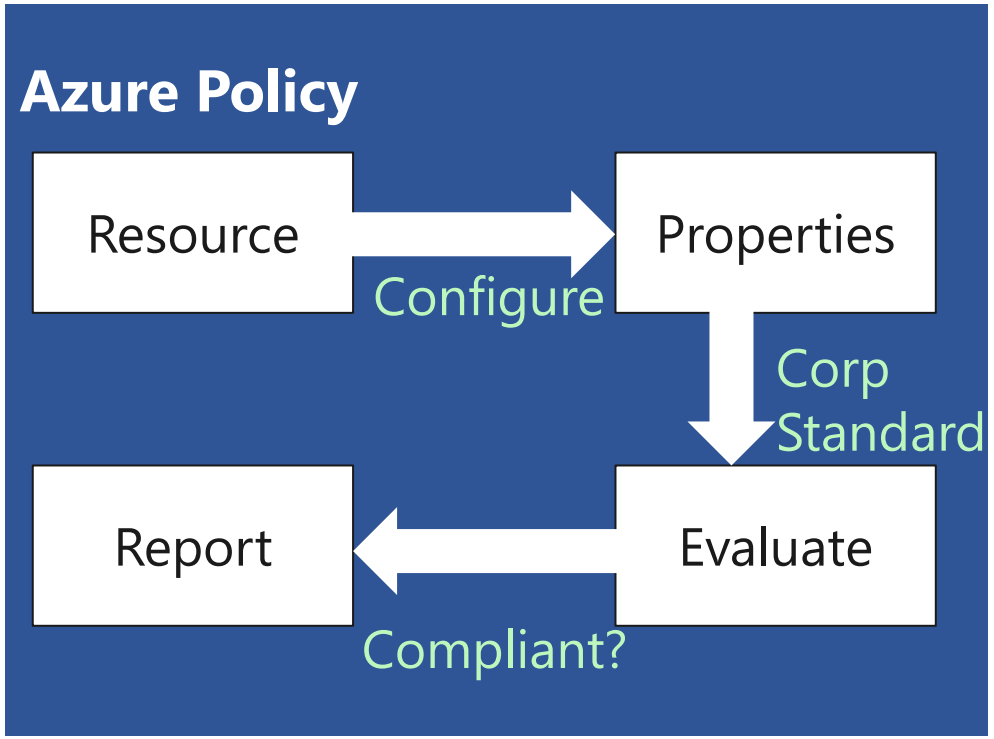
Azure Role-Based Access Control

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



Azure RBAC vs Azure Policies





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

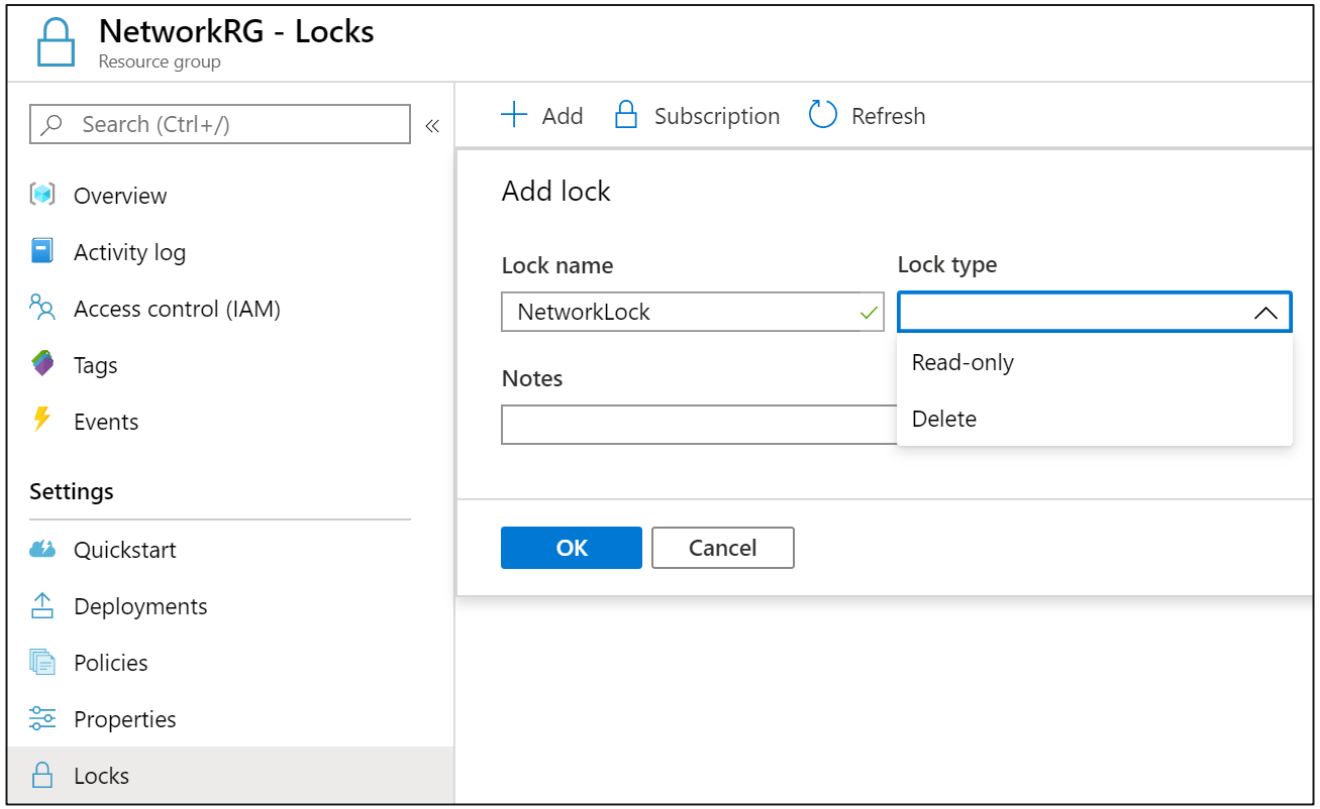
Resource Locks

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

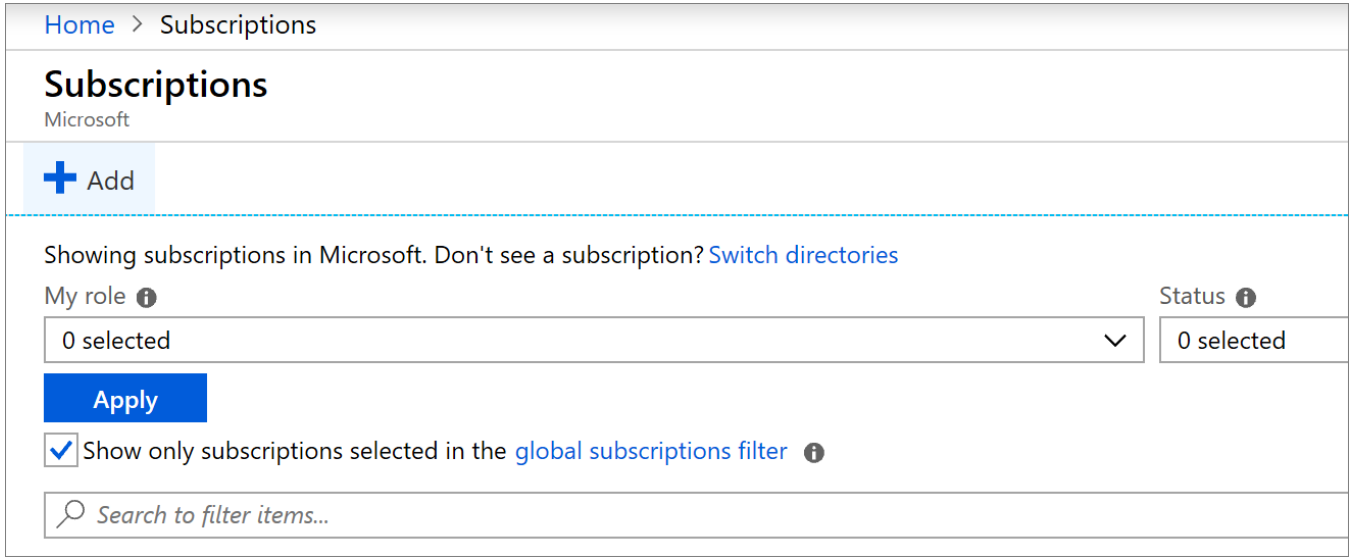
A package or container for composing focus-specific sets of standards, patterns, and requirements

Azure Subscription Management

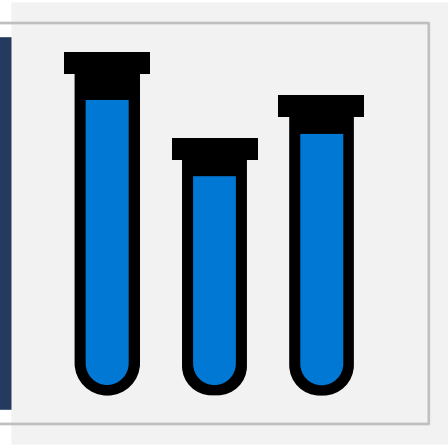
The Account Owner role can create Azure subscriptions.

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.



Module - Labs



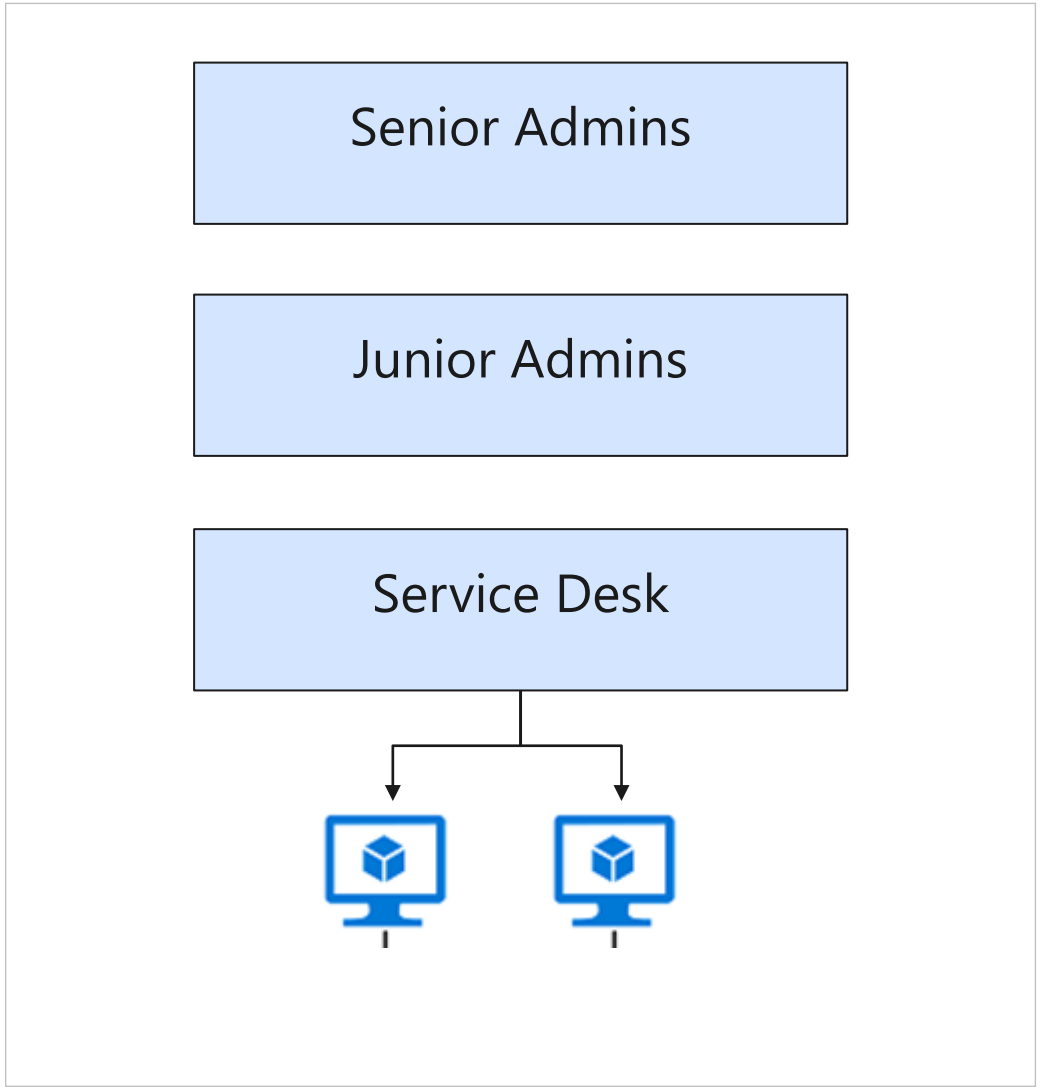
Lab 01 – Role-Based Access Control

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.



Lab 01 – Role-Based Access Control

Default Azure AD tenant

Exercise1, Task1, Task2

Senior Admins
Membership type: Assigned

Cloud user
Joseph Price

Exercise2, Task1, Task2

PowerShell

Junior Admins
Membership type: Assigned

Cloud user
Isabel Garcia

Exercise3, Task1, Task2

CLI

Service Desk
Membership type: Assigned

Cloud user
Dylan Williams

Exercise4, Task2

Virtual Machine Contributor

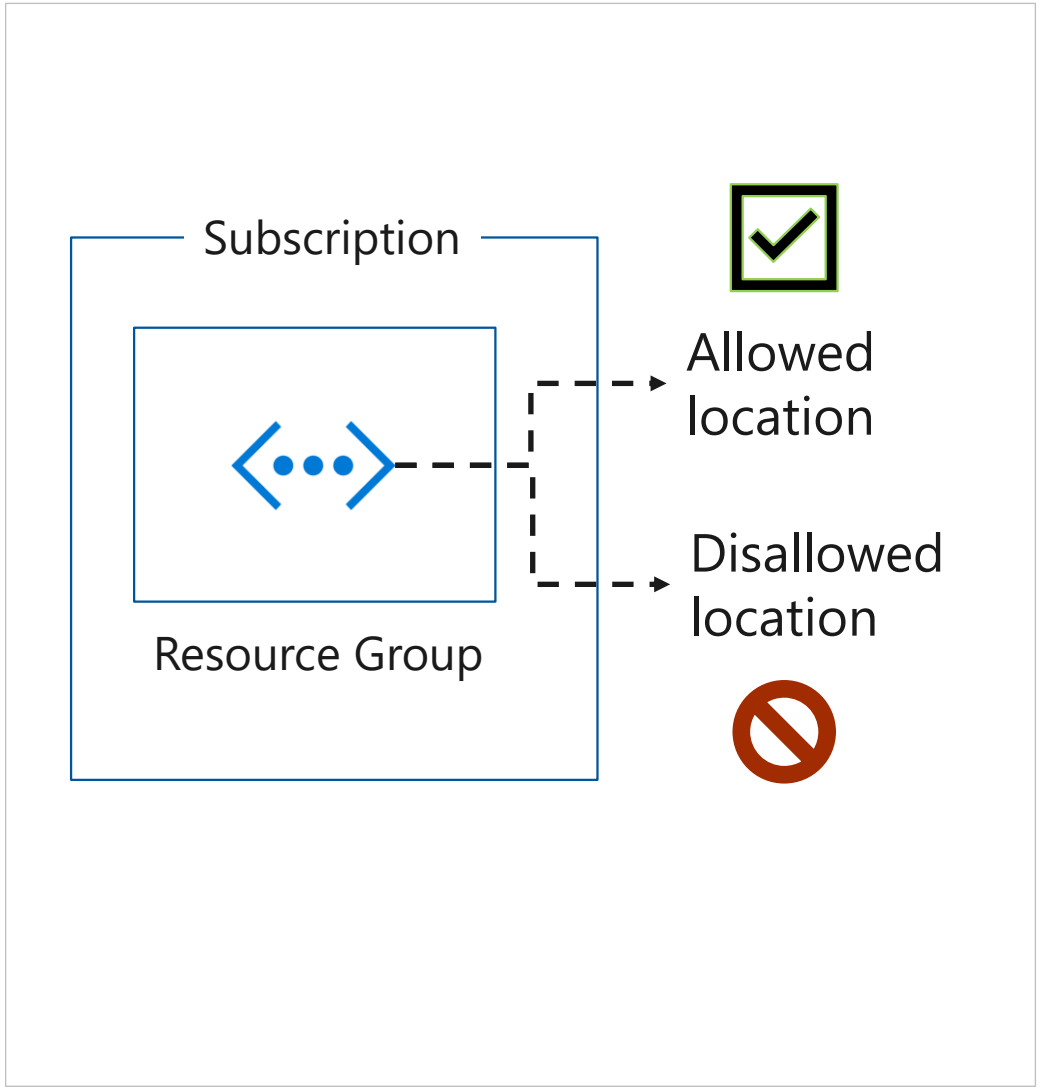
Exercise4, Task1

AZ500Lab01

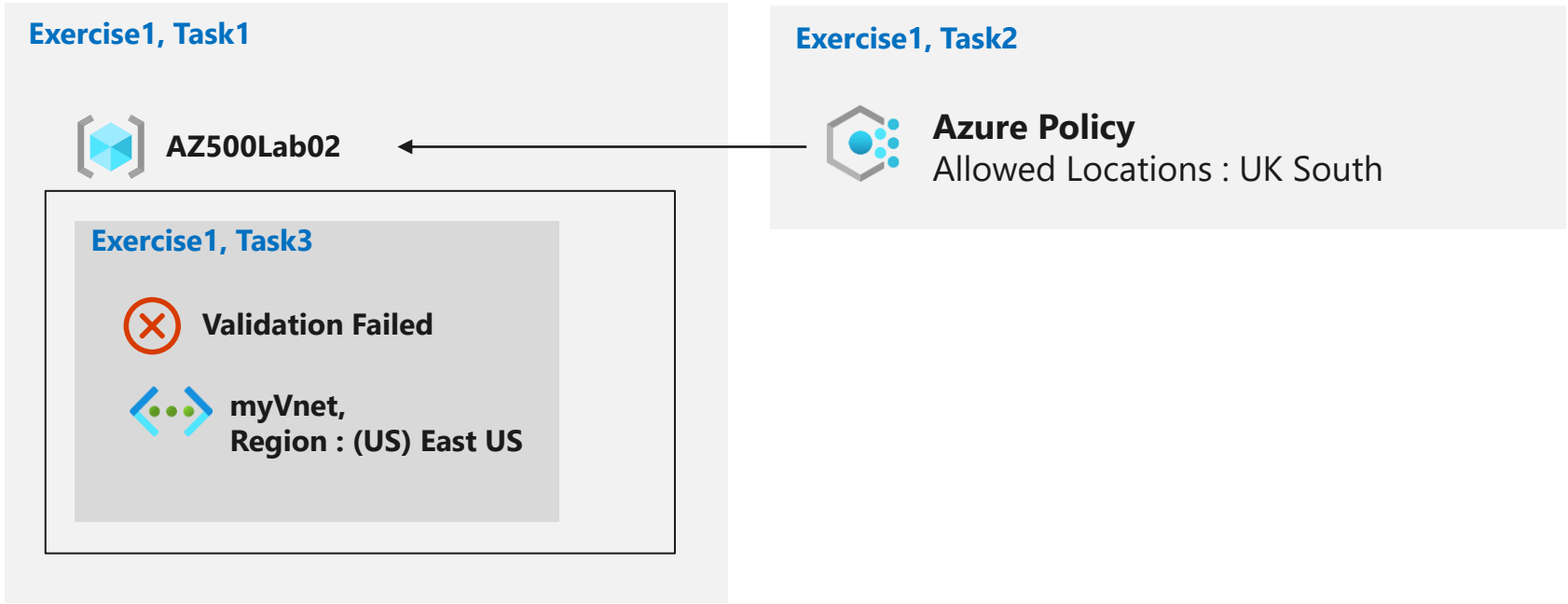
Lab 02 – Azure Policy

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.



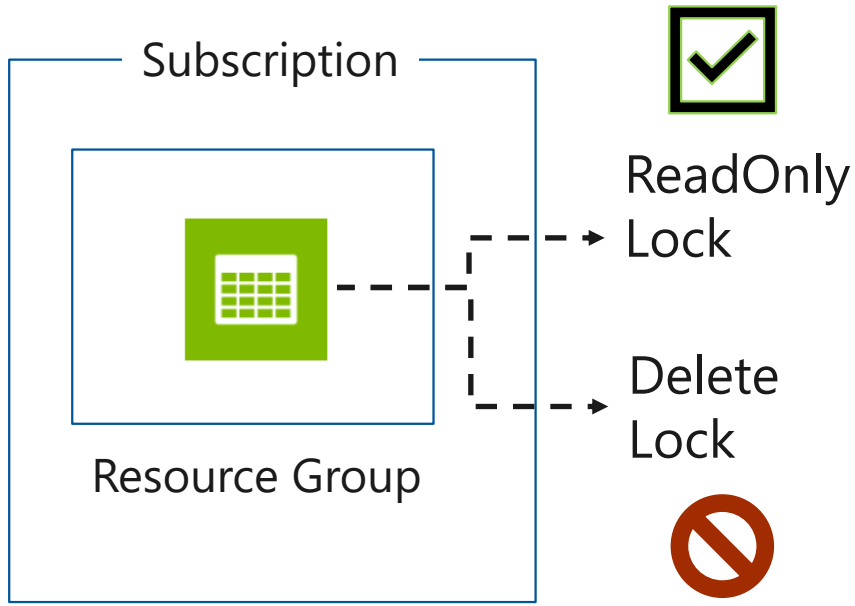
Lab 02 – Azure Policy



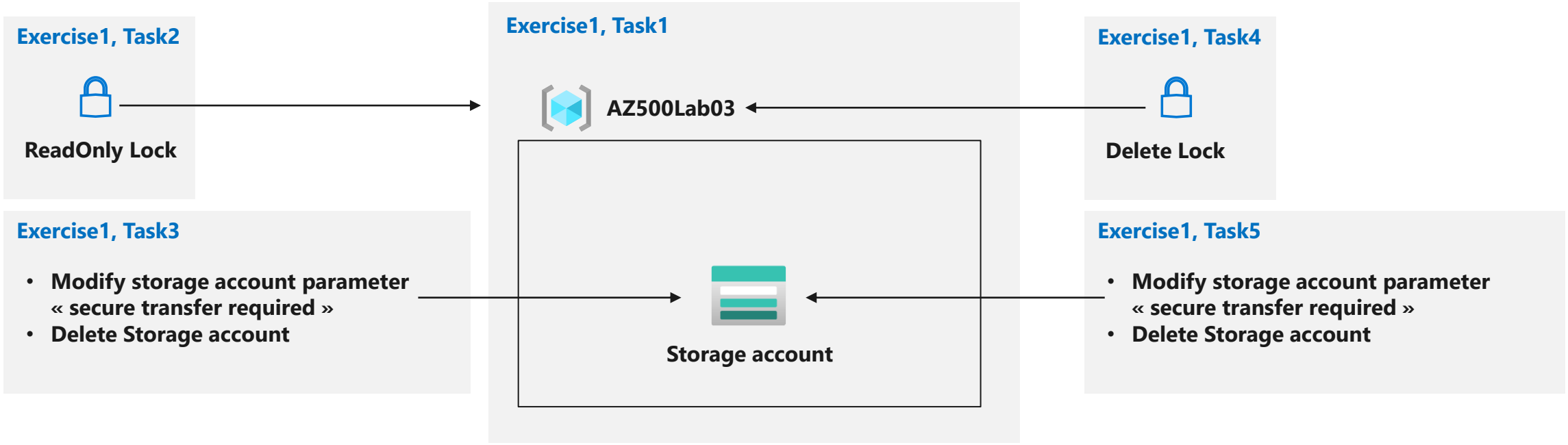
Lab 03 – Resource Manager Locks

Prevent a storage account configuration from being changed.

Prevent a storage account from being deleted.



Lab 03 – Resource Manager Locks

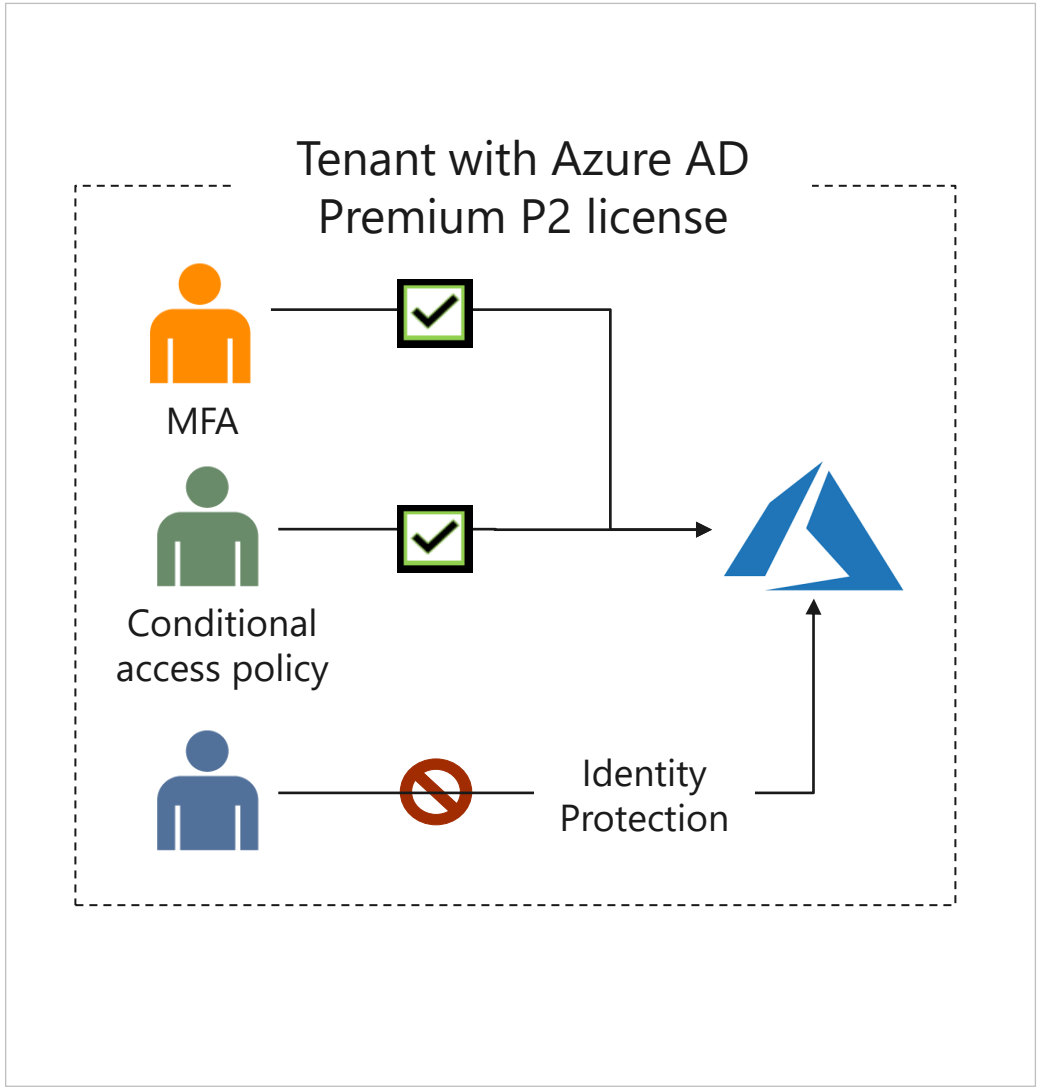


Lab 04 – MFA - Conditional Access - Identity Protection

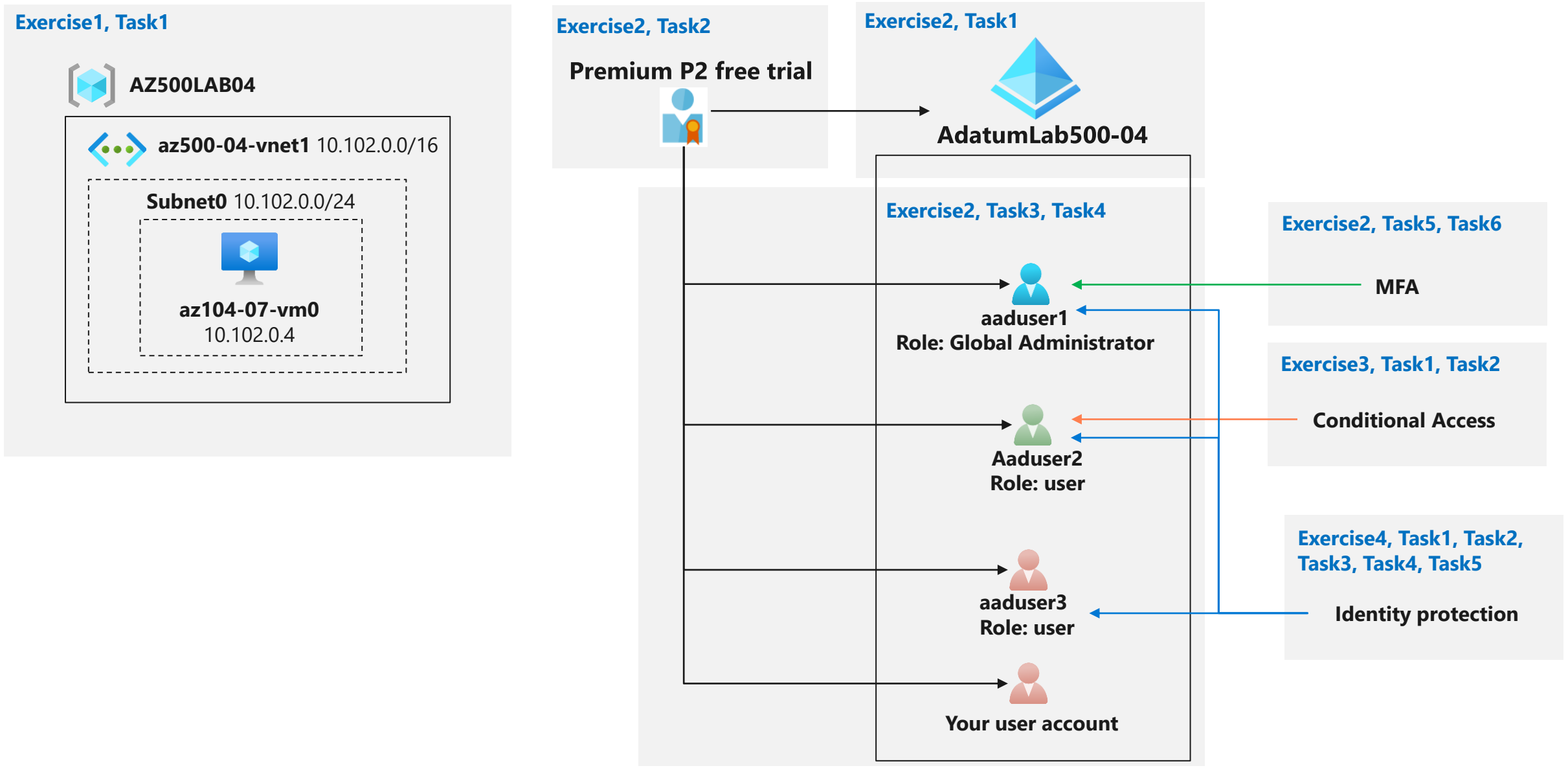
Implement and test Azure MFA.

Implement and test Azure AD Conditional Access Policies.

Implement and test Azure AD Identity Protection.



Lab 04 – MFA - Conditional Access - Identity Protection



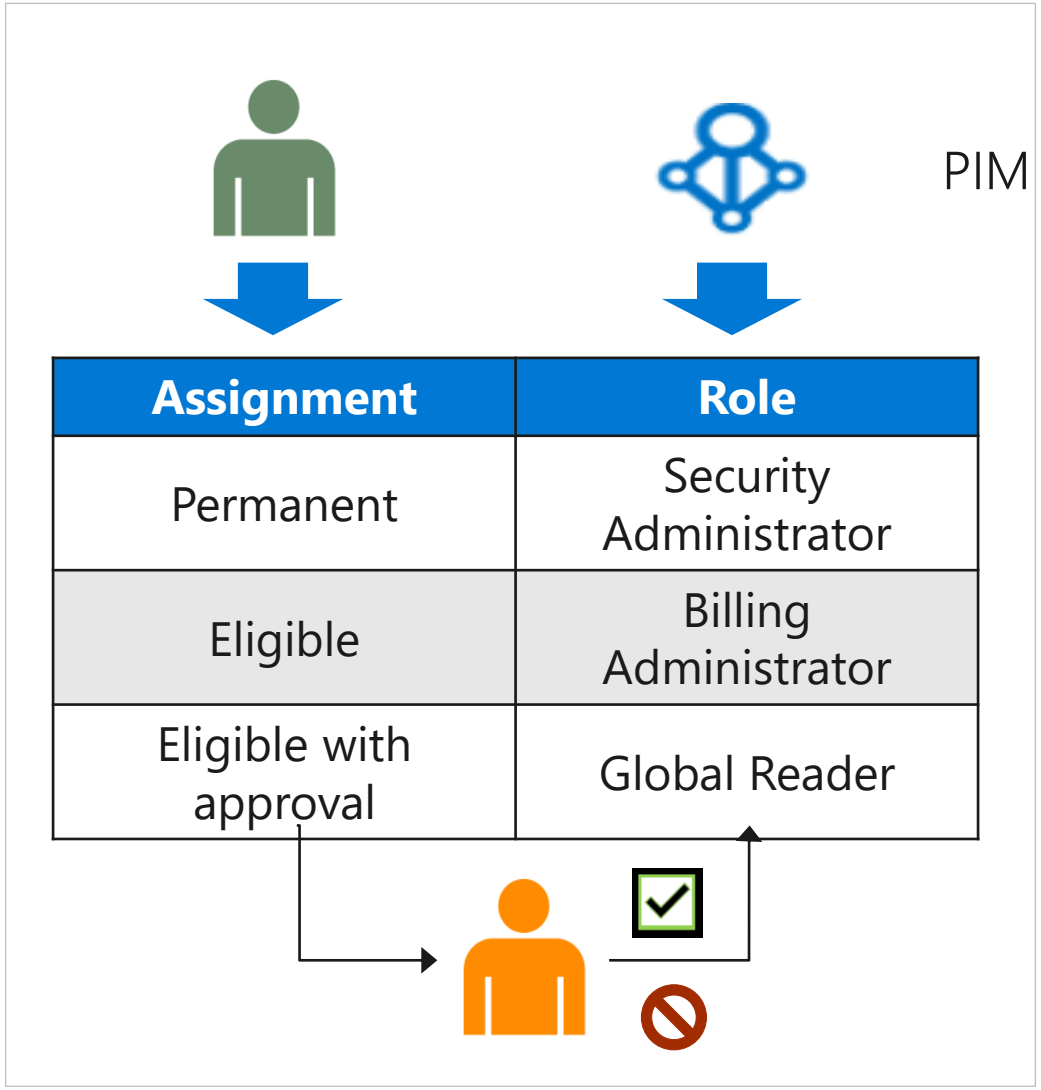
Lab 05 – Azure AD Privileged Identity Management

Onboard PIM.

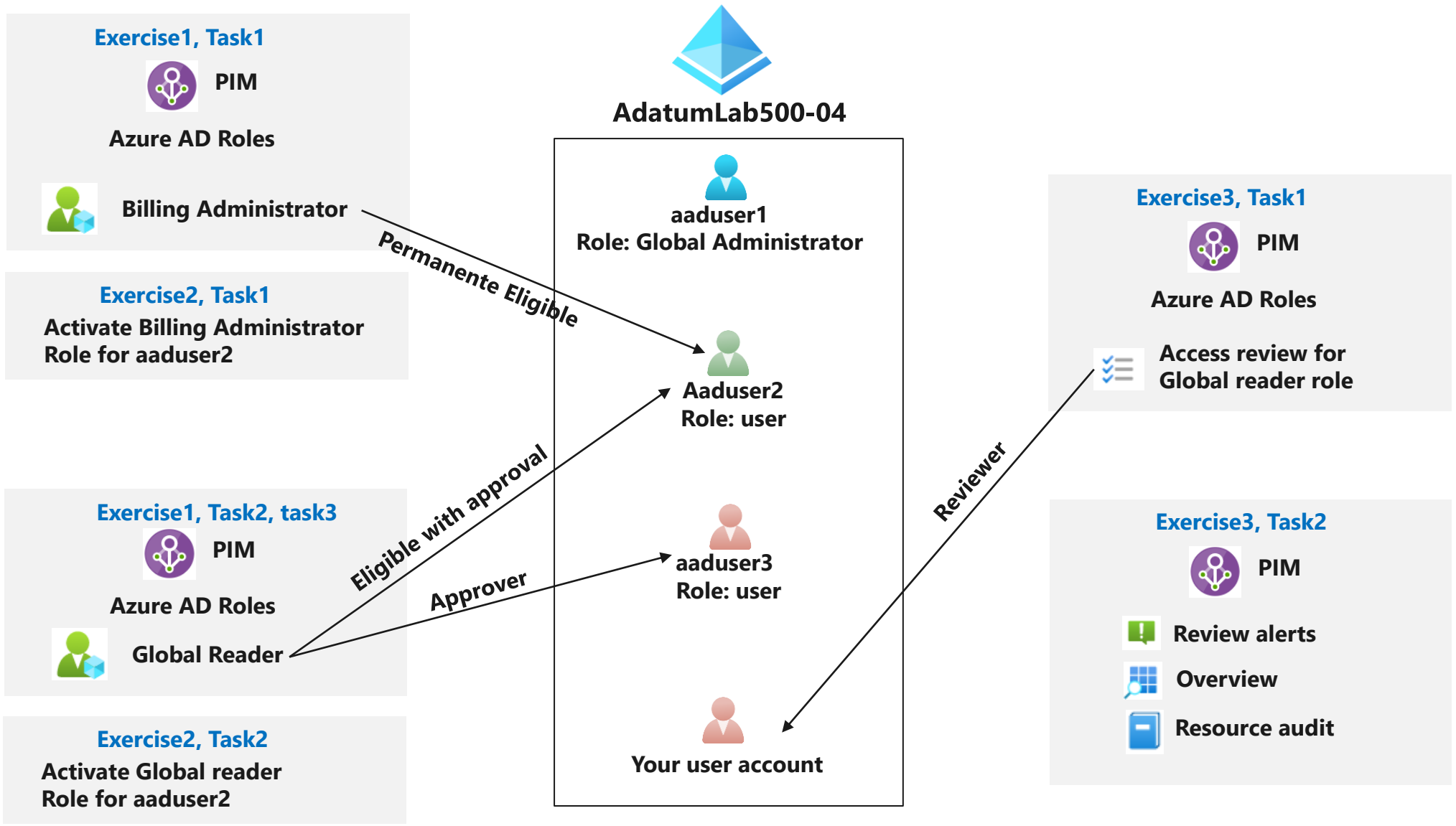
Configure PIM users and roles.

Activate PIM roles with and without approval.

Create an Access Review and review PIM auditing features.



Lab 05 – Azure AD Privileged Identity Management

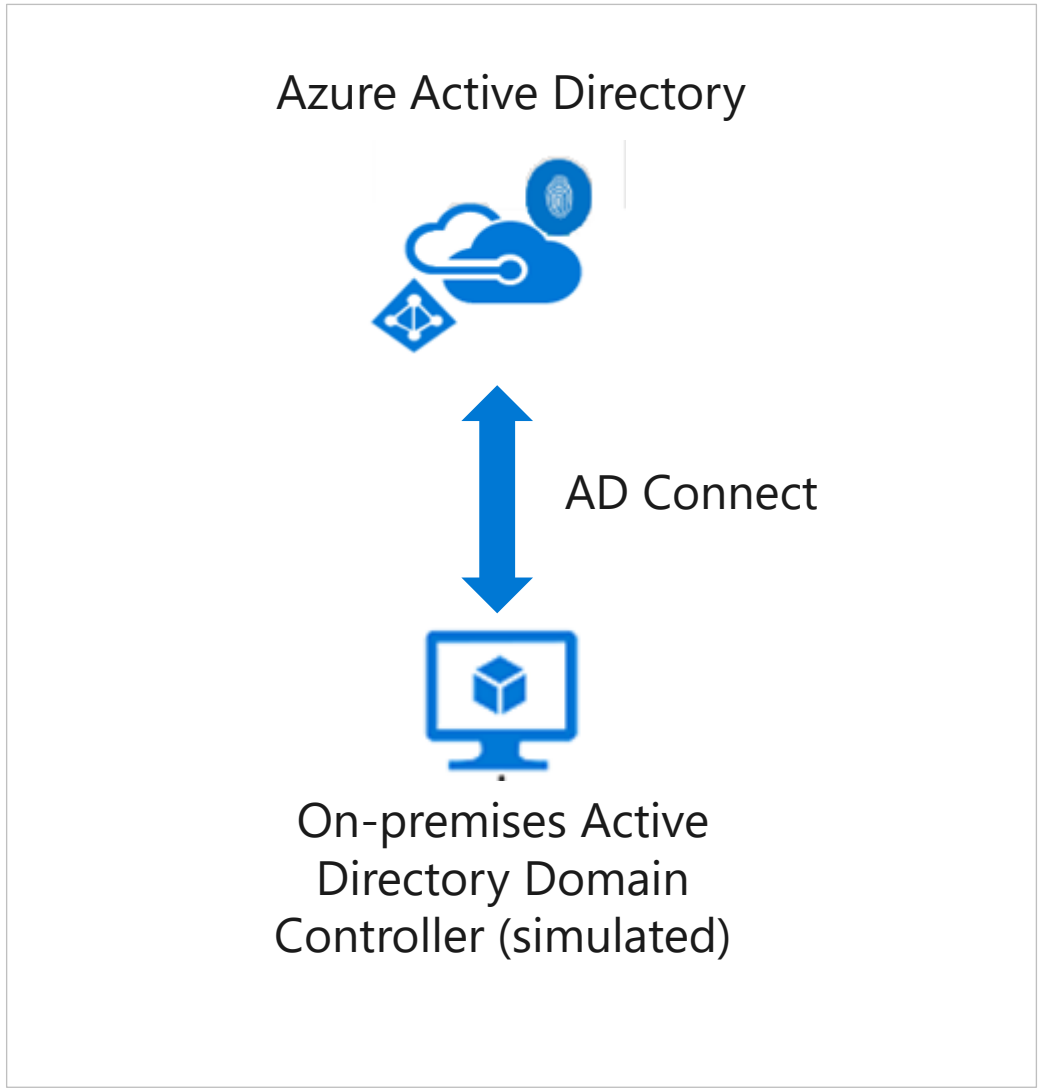


Lab 06 – Implement Directory Synchronization

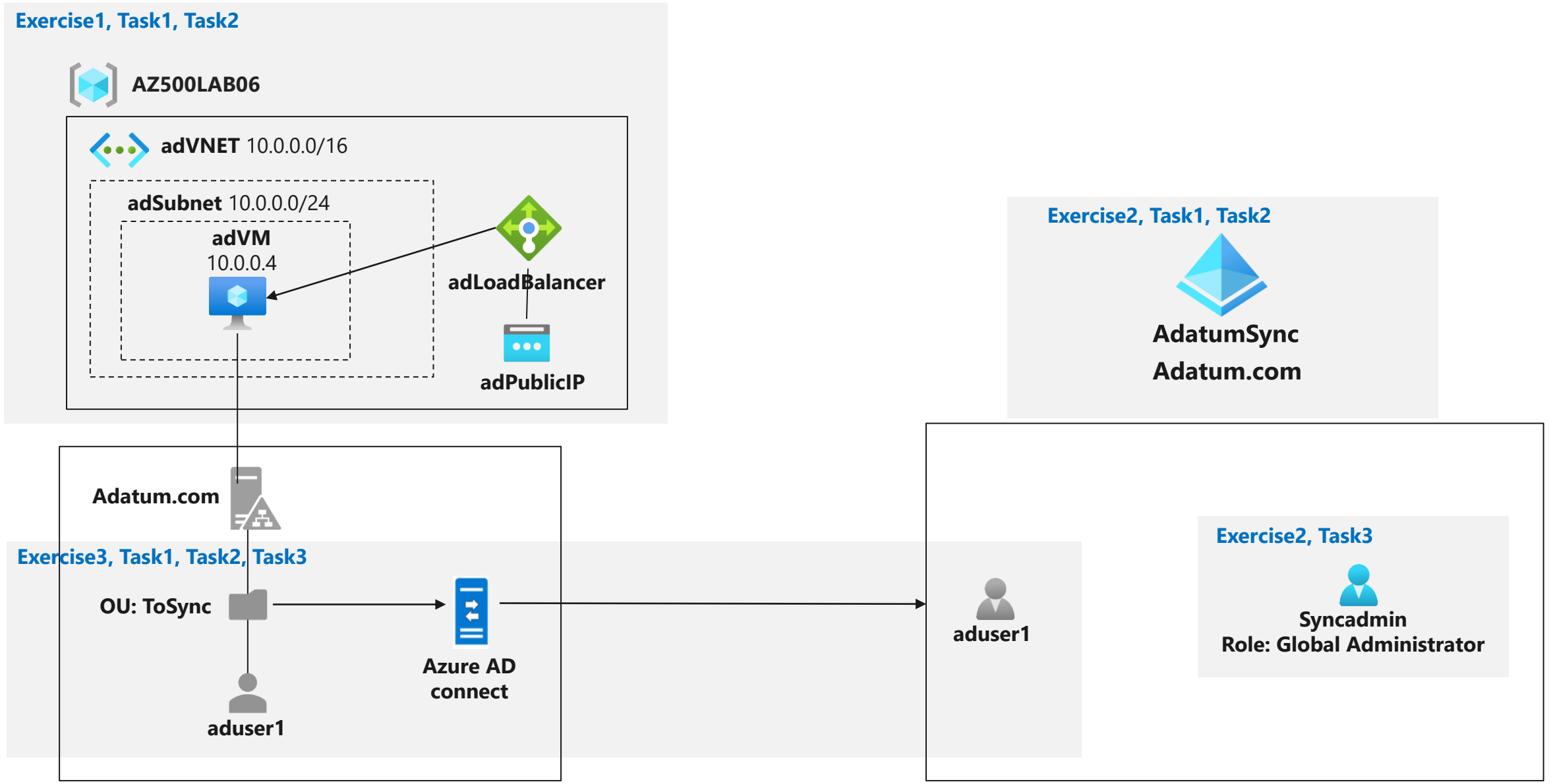
Deploy an Azure VM hosting an Active Directory domain controller.

Create and configure an Azure Active Directory tenant.

Synchronize Active Directory forest with an Azure Active Directory tenant.



Lab 06 – Implement Directory Synchronization



End of presentation