Microsoft

Authentication and Authorization

Learn.
Connect.
Explore.

Authentication and Authorization

Authentication - Process of proving that you are who you say you are

Azure AD

Azure Subscription

Authorization to use resources in Azure

Overview on Azure Active Directory

- **Azure Active Directory (Azure AD)** is Microsoft's cloud-based identity and access management service
- Azure AD helps your employees sign in and access resources
- **External resources**, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications.
- **Internal resources**, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

Scenario

Cloud Architect uses Azure Active Directory to manage identities, you will work on such tasks as: -

With the help of Azure Active Directory, you can create Users

We don’t need any separate infrastructure

Azure Active Directory (Azure AD) is a cloud-based identity and access management service.

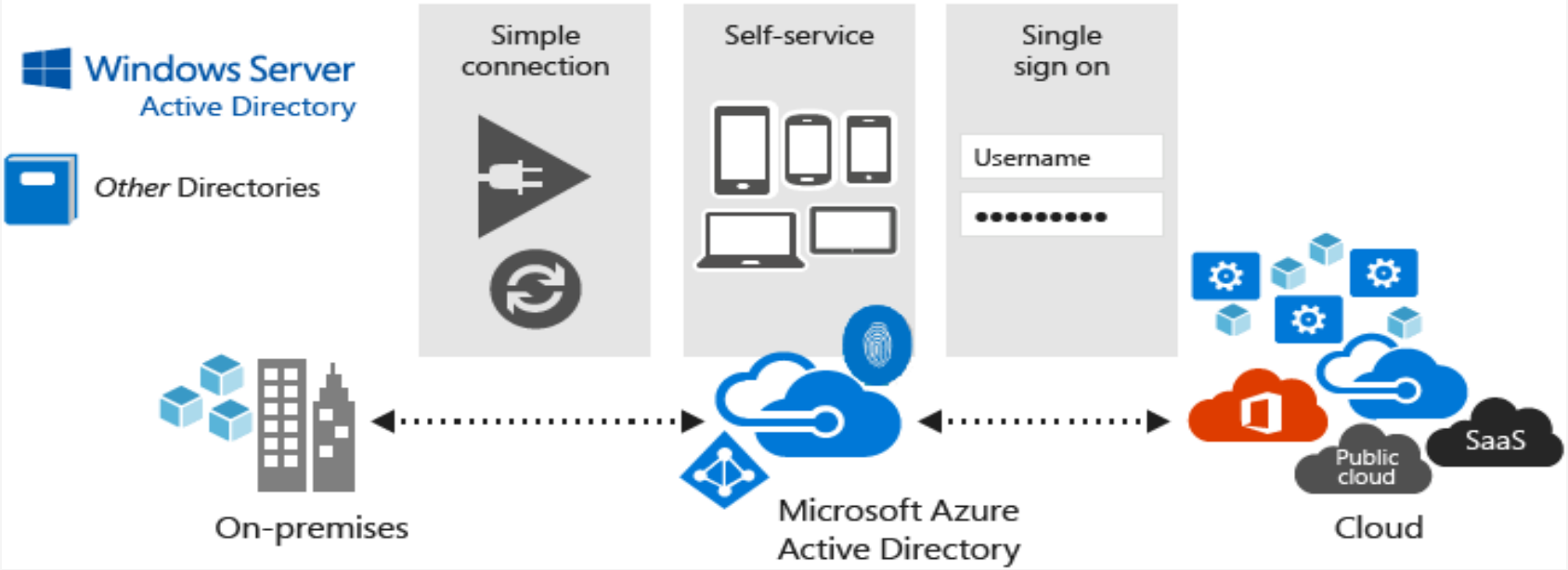
Define a strategy for using Azure AD and Azure AD Domain Services to lock down access to your solutions.

Who uses Azure AD?

- Azure AD is intended for:
  - IT Admins
  - App developers
  - Microsoft 365, Office 365, Azure, or Dynamics CRM Online subscribers:

What is Azure Active Directory?

Azure Active Directory Features



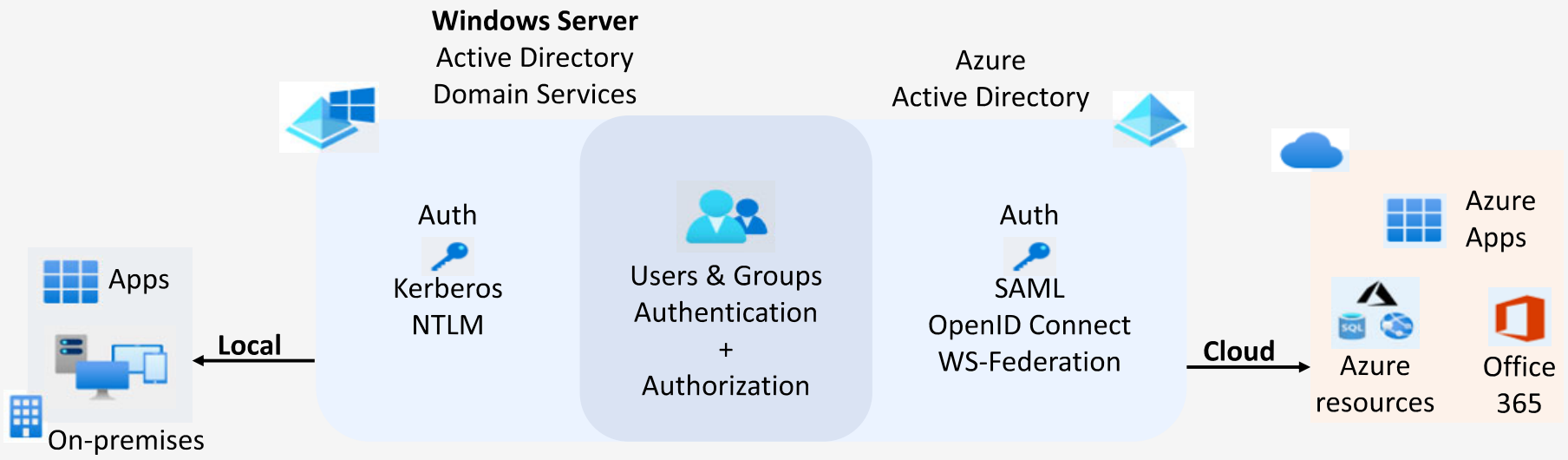
Microsoft's multi-tenant cloud-based directory and identity management service

Identity management capabilities and integration

Integrates with Windows Server Active Directory

Provides SSO access

Azure AD Vs Active Directory Domain Services (AD DS)

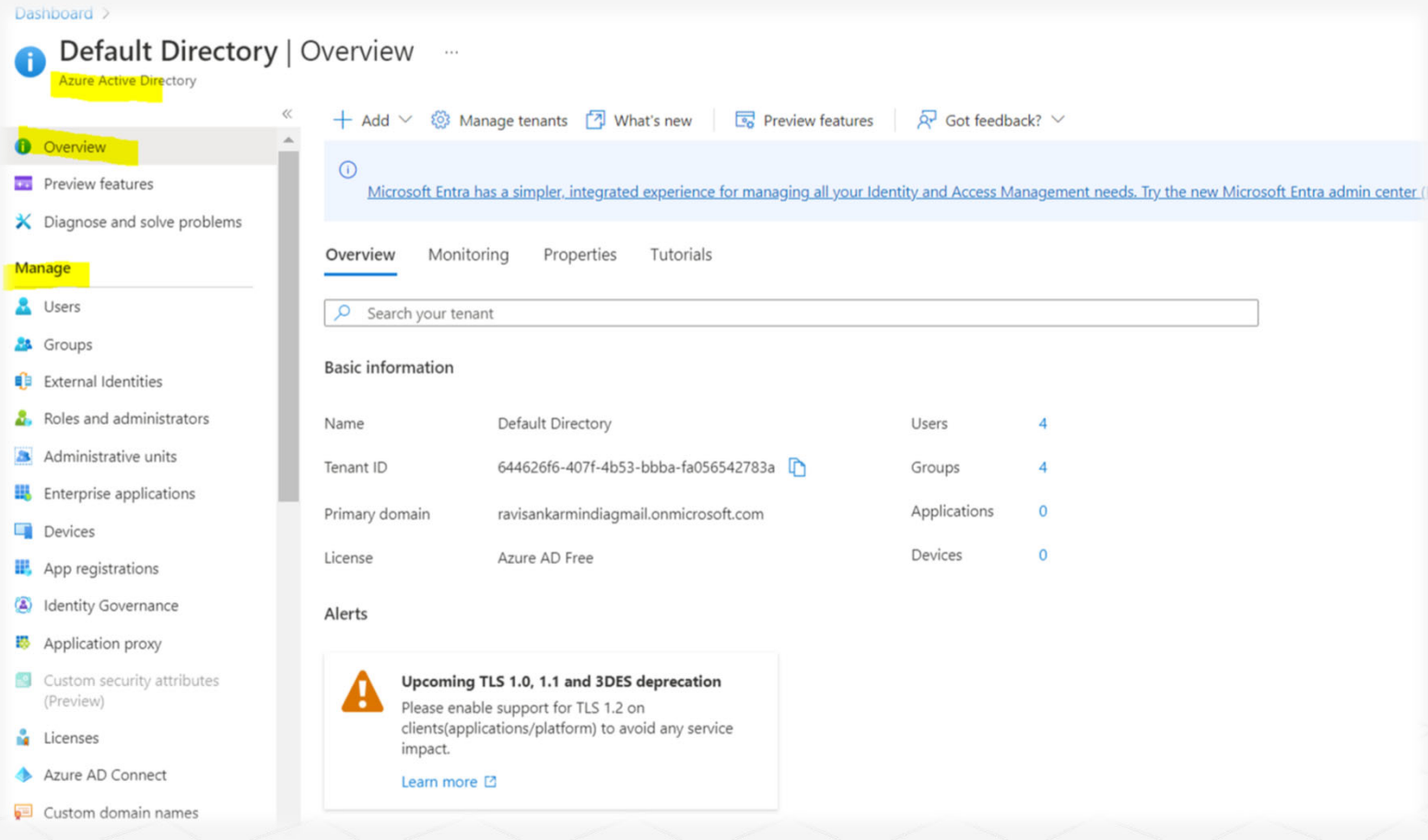


Service	Authentication	Structure	What it's used for
Azure Active Directory	Includes SAML, OpenID Connect (based on OAuth), WS-Federation	Tenants	Internet-based services and applications like Office 365, Azure services, and third-party SaaS applications
Active Directory Domain Services	Kerberos, NTLM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

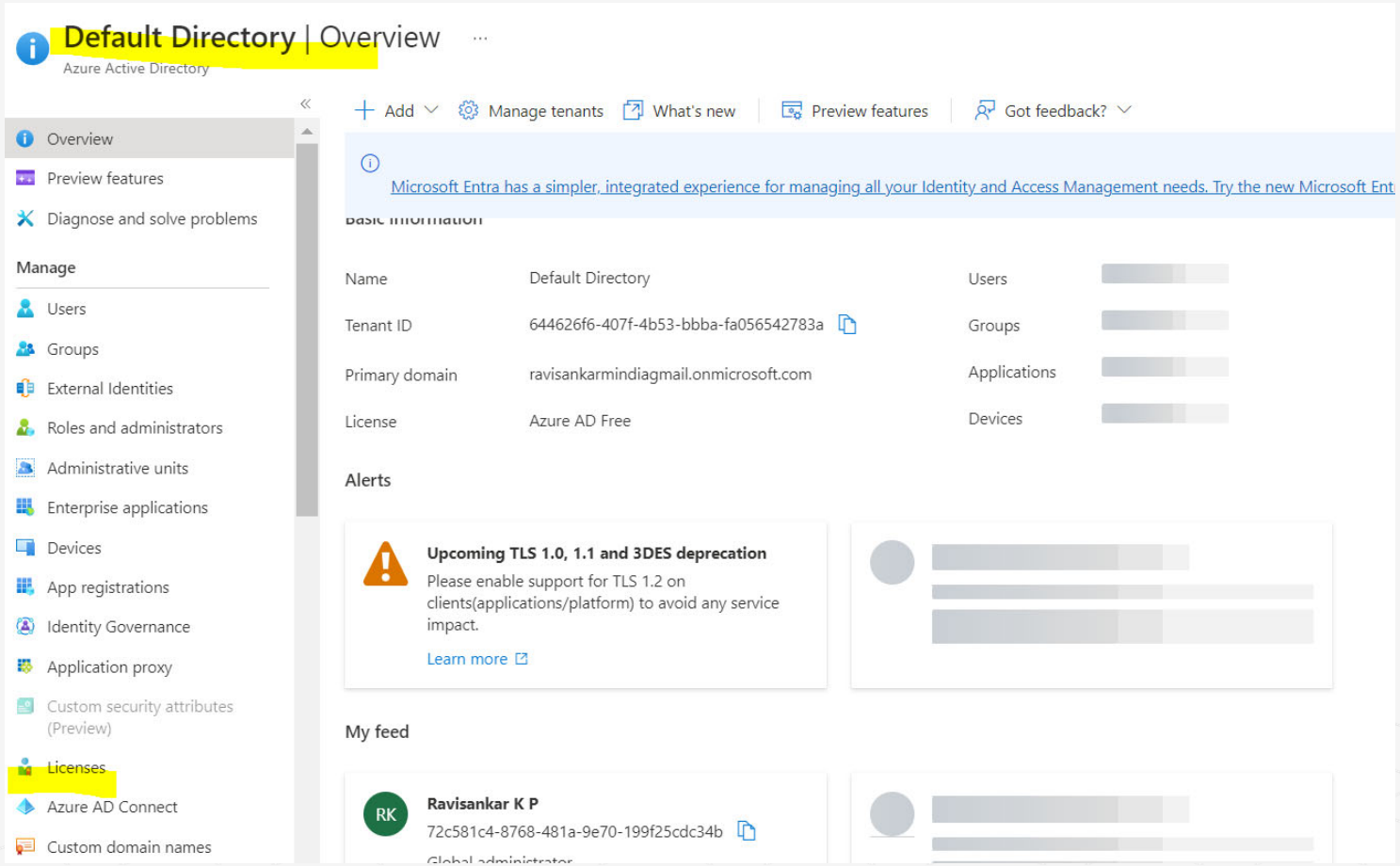
Identity Manage capabilities and integration

- **Azure AD** also includes :-
  - Full suite of identity management capabilities including multifactor authentication (MFA)
  - Device registration, self-service password management, self-service group management,
  - Privileged Account management, role-based access control, application usage monitoring, rich auditing and security monitoring, and alerting.
- Azure AD can be integrated with an existing Windows Server Active Directory

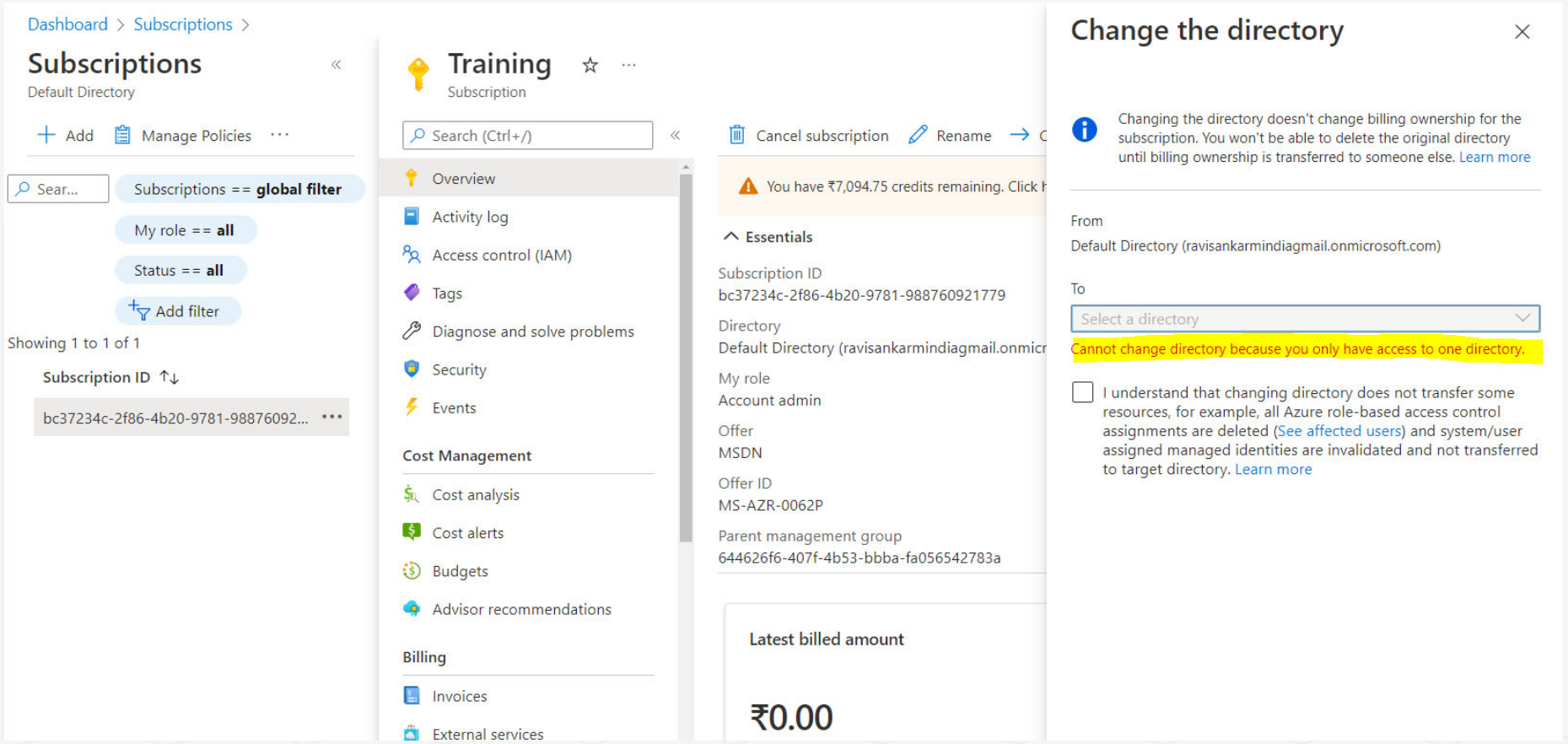
Explore Azure AD Options



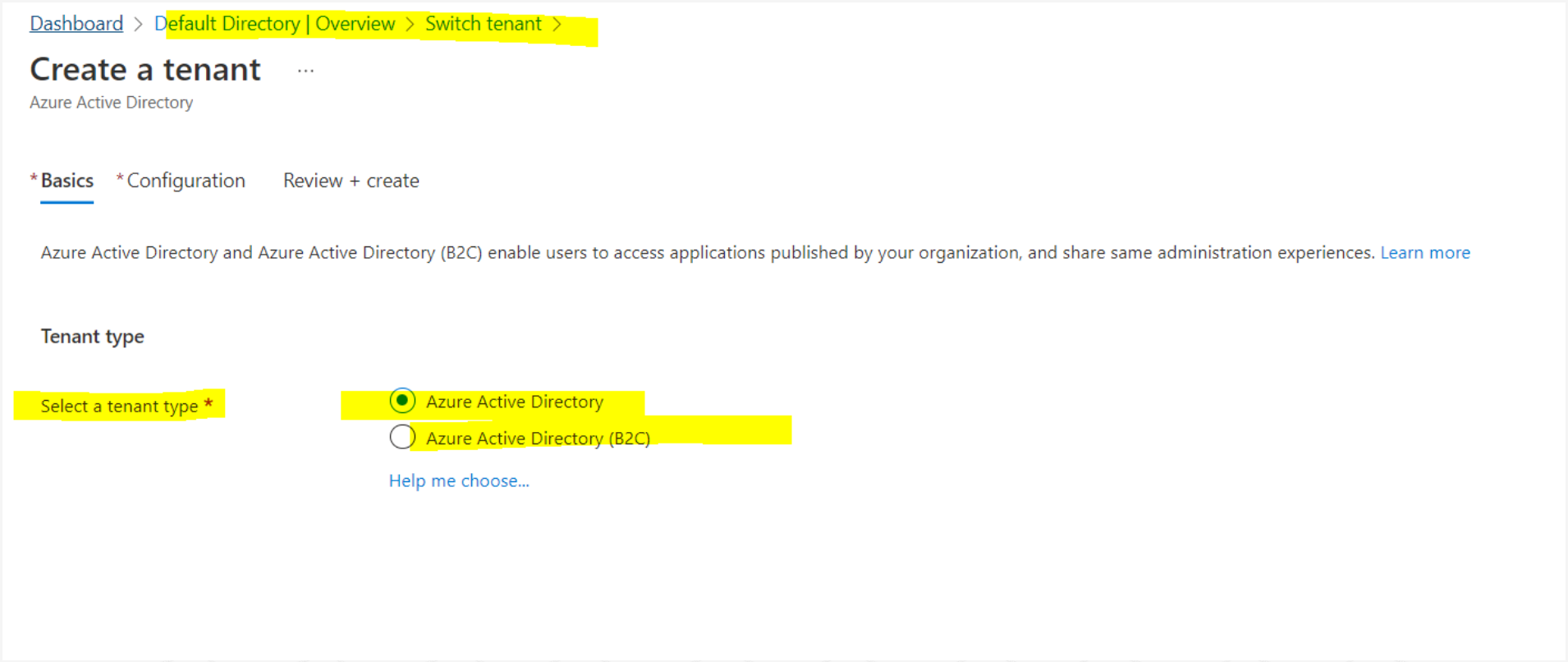
Subscribing Trial version of Azure Premium Licence



Changing Directory



Changing Directory – Create Tenant



Azure AD Editions

1

Azure Active Directory comes in four editions—**Free**, **Microsoft 365 Apps**, **Premium P1**, and **Premium P2**.

2

The Free edition is included with an Azure subscription.

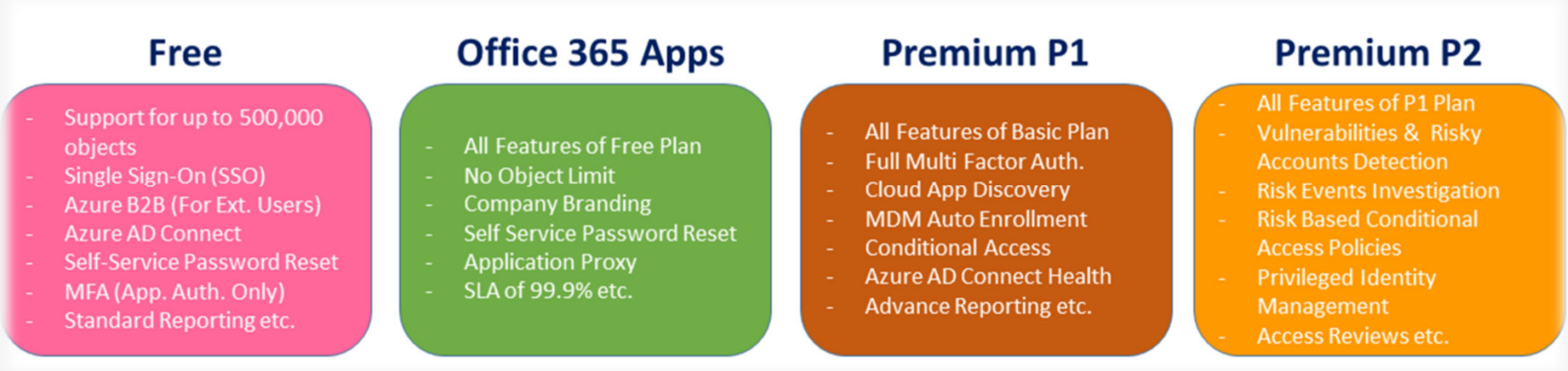
3

The Premium editions are available through a Microsoft Enterprise Agreement, the Open Volume License Program, and the Cloud Solution Providers program.

4

Azure and Microsoft 365 subscribers can also buy Azure Active Directory Premium P1 and P2 online.

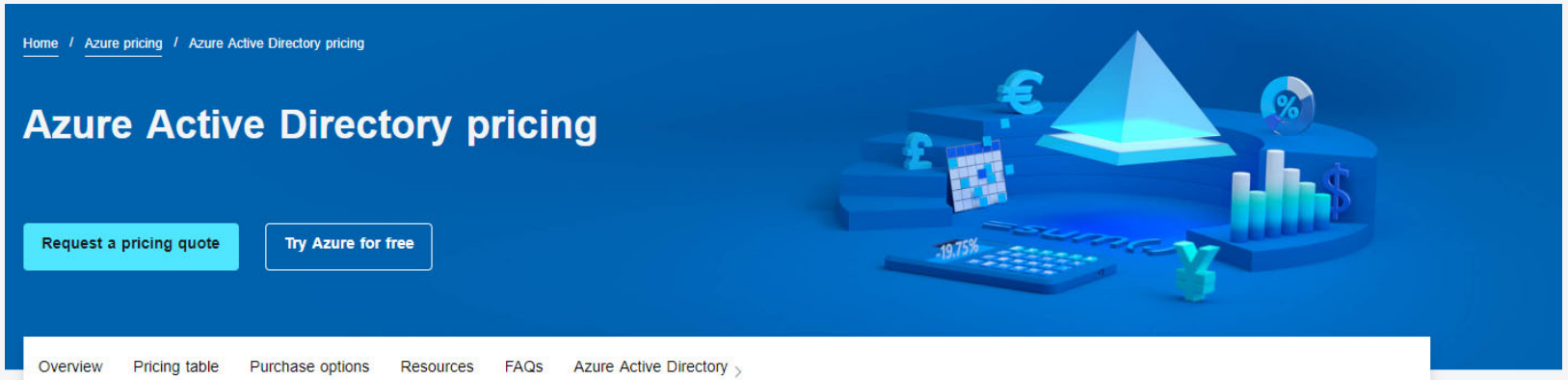
Azure AD Editions



Azure AD Editions

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	500,000	Unlimited	Unlimited	Unlimited
Single Sign-On	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access Management	X	X	X	X
Business to Business Collaboration	X	X	X	X
Identity & Access Management for Microsoft 365 apps		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access Management			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

Azure Active Directory pricing



Synchronise on-premises directories and enable single sign-on

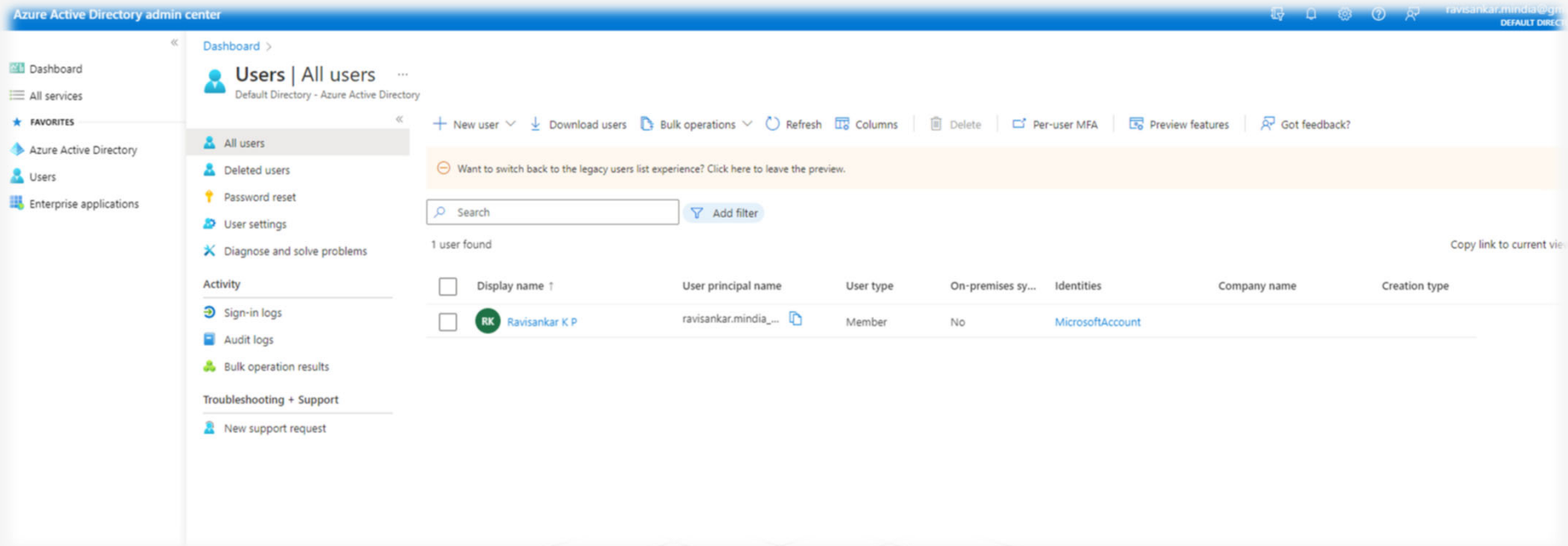
Microsoft Azure Active Directory is a comprehensive identity and access management cloud solution that combines core directory services, application access management and advanced identity protection.

Explore pricing options

Apply filters to customise pricing options to your needs.

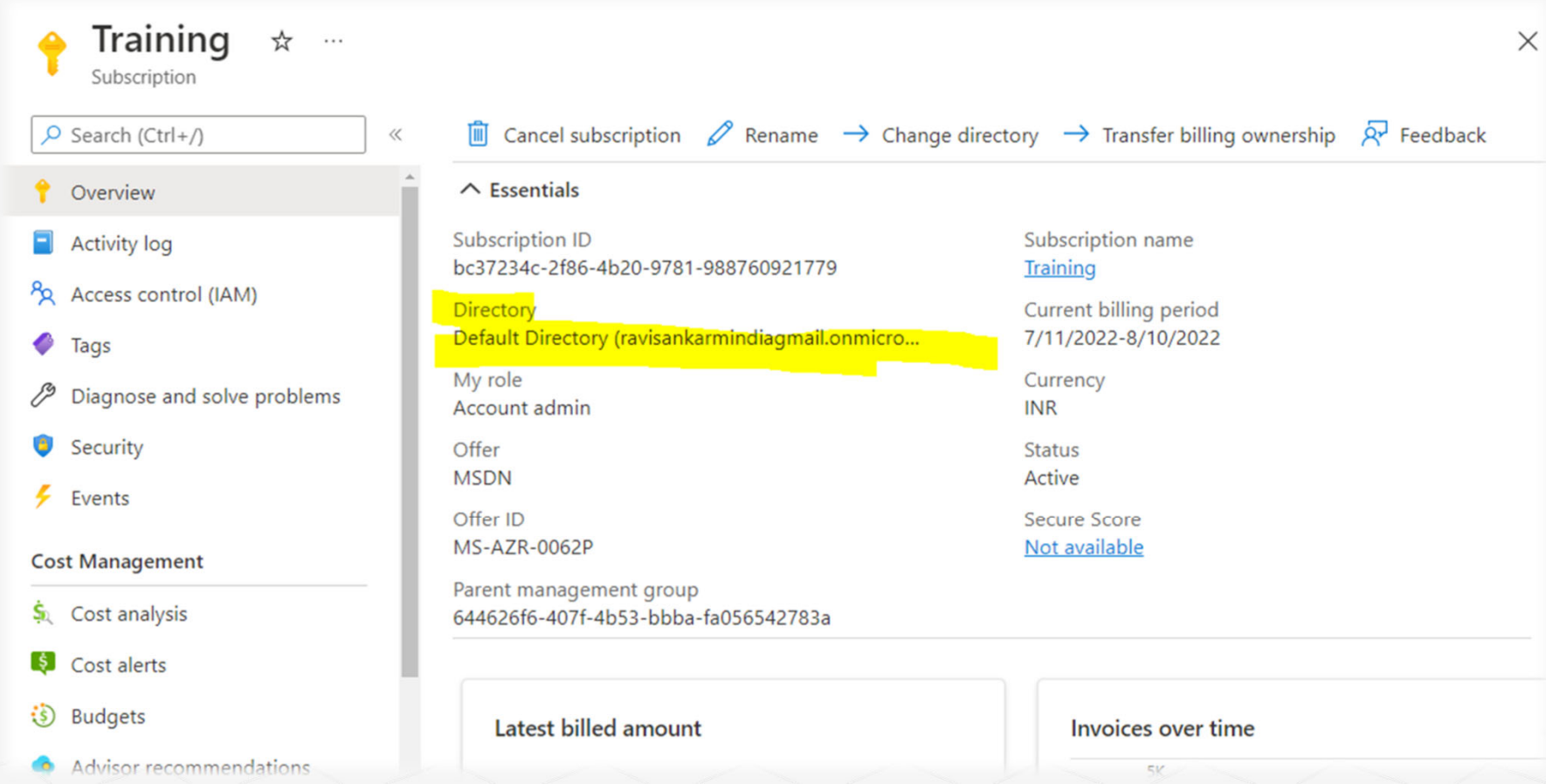
Prices are estimates only and are not intended as actual price quotes. Actual pricing may vary depending on the type of agreement entered with Microsoft, date of purchase, and the currency exchange rate. Prices are calculated based on US dollars and converted using Thomson Reuters benchmark rates refreshed on the first day of each calendar month. Sign in to the Azure pricing

Azure Active Directory Admin Center



https://aad.portal.azure.com/

Trust between Azure Subscription and Azure AD



Microsoft

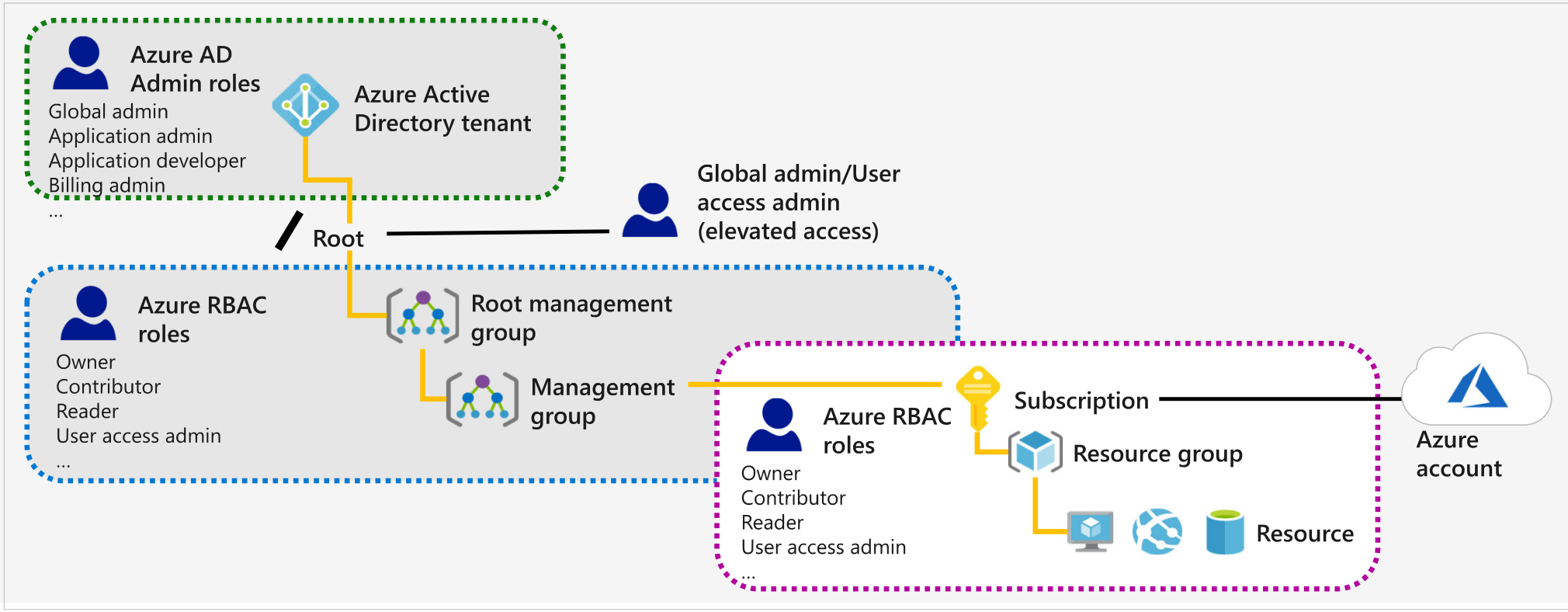
Role Based Access Control

Learn.
Connect.
Explore.

What is Role Based Access Control ?

Azure Role-Based Access Control

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



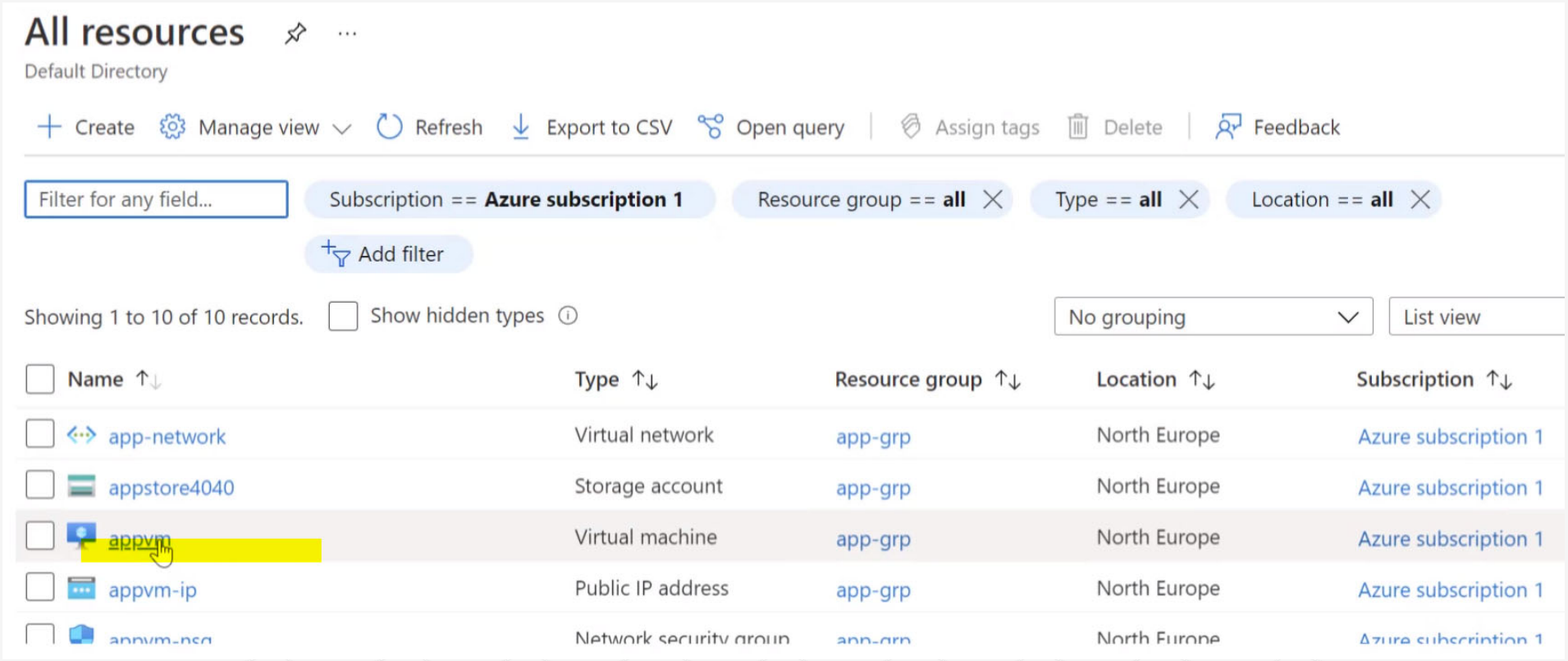
Azure built-in roles

All

Built-in role	Description	ID
General		
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.	b24988ac-6180-42a0-ab88-20f7382dd24c
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	8e3af657-a8ff-443c-a75c-2fe8c4bcb635
Reader	View all resources, but does not allow you to make any changes.	acdd72a7-3385-48ef-bd42-f606fba81ae7
User Access Administrator	Lets you manage user access to Azure resources.	18d7d88d-d35e-4fb5-a5c3-7773c20a72d9

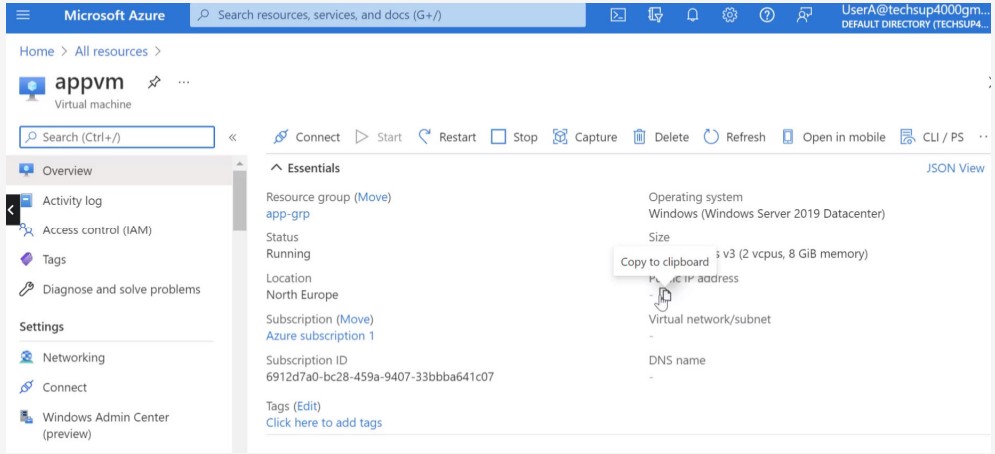
Note: - We can create custom roles

Lab 1 – Role Based Assignments | Reader Role

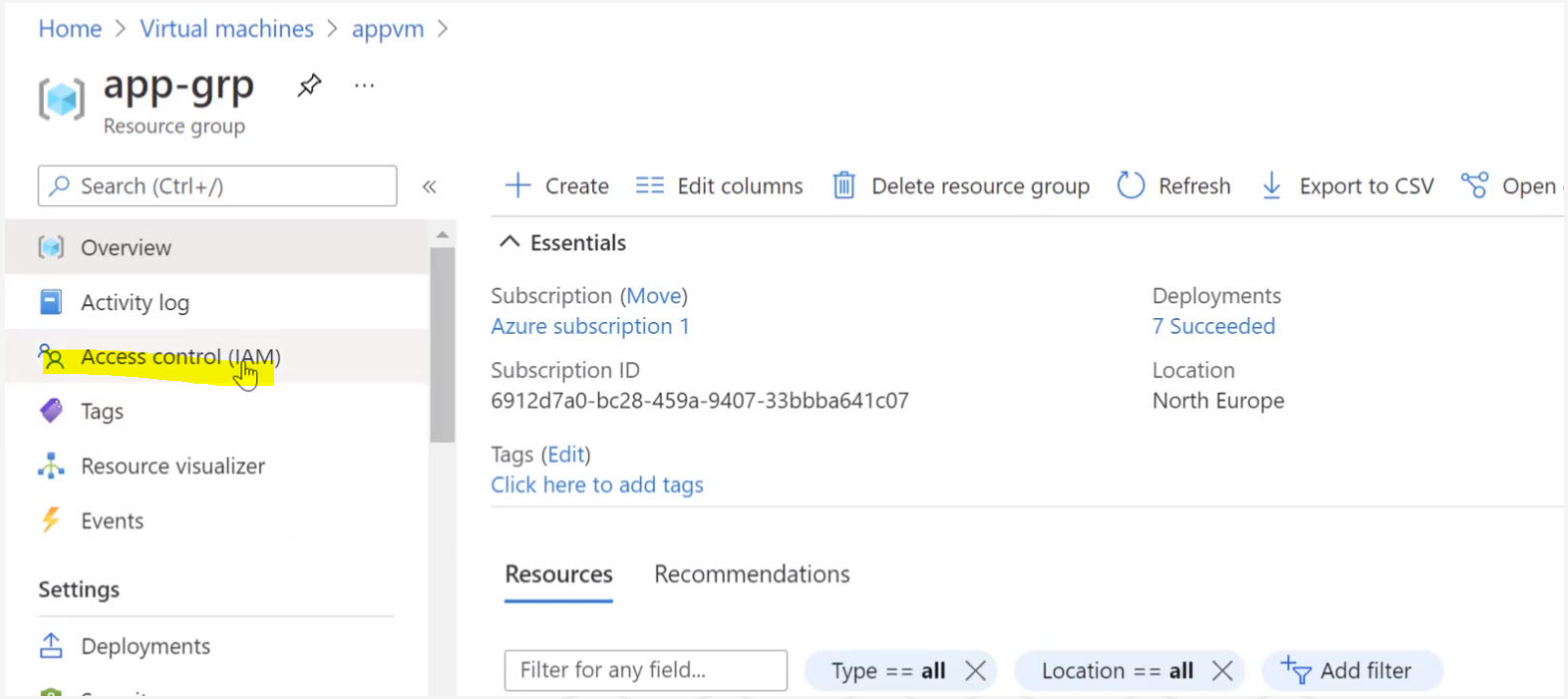


Lab – Role Based Assignments

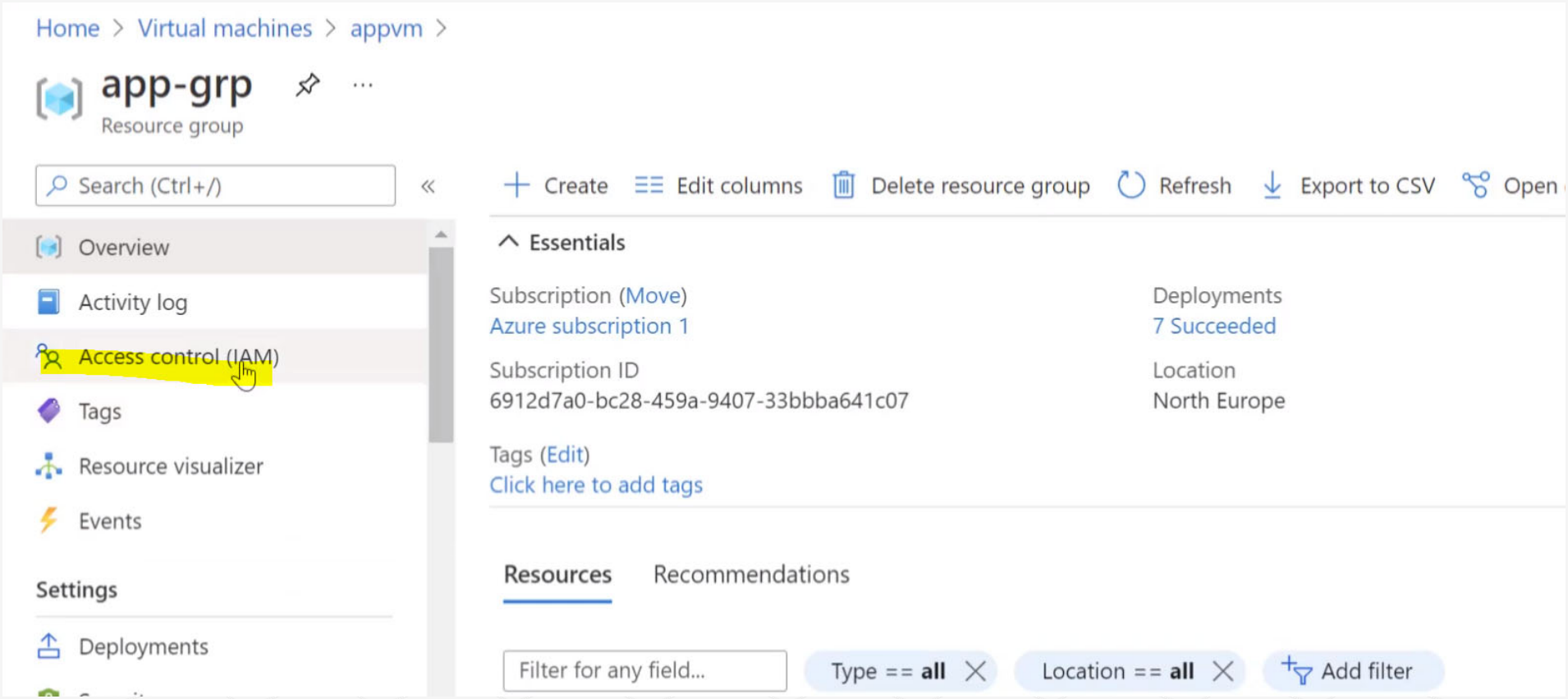
Note: - Other resource information won't be available because Public IP / Private IP is a separate resource.



Lab 2 – Role Based Assignments | Reader - Resource Group Level

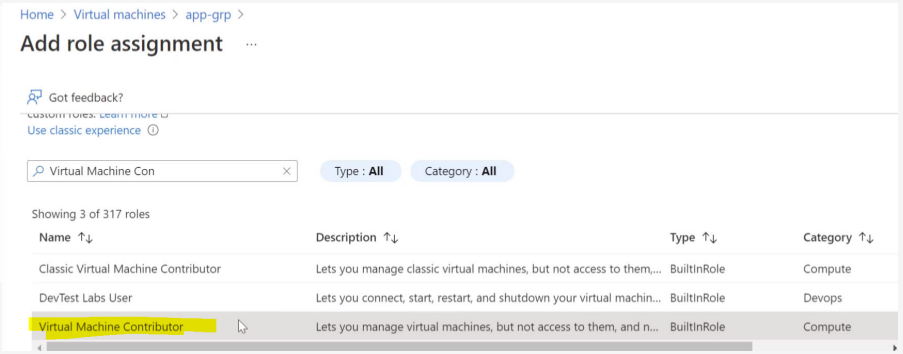


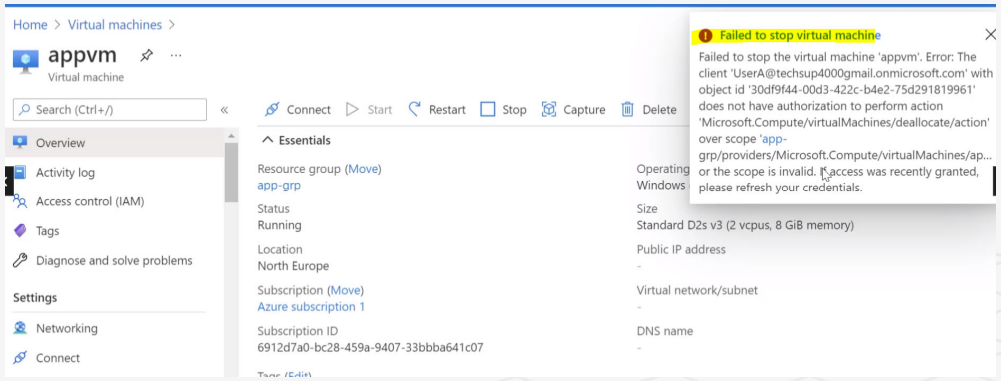
Lab 3 – Role Based Assignments | Reader - Subscription Level



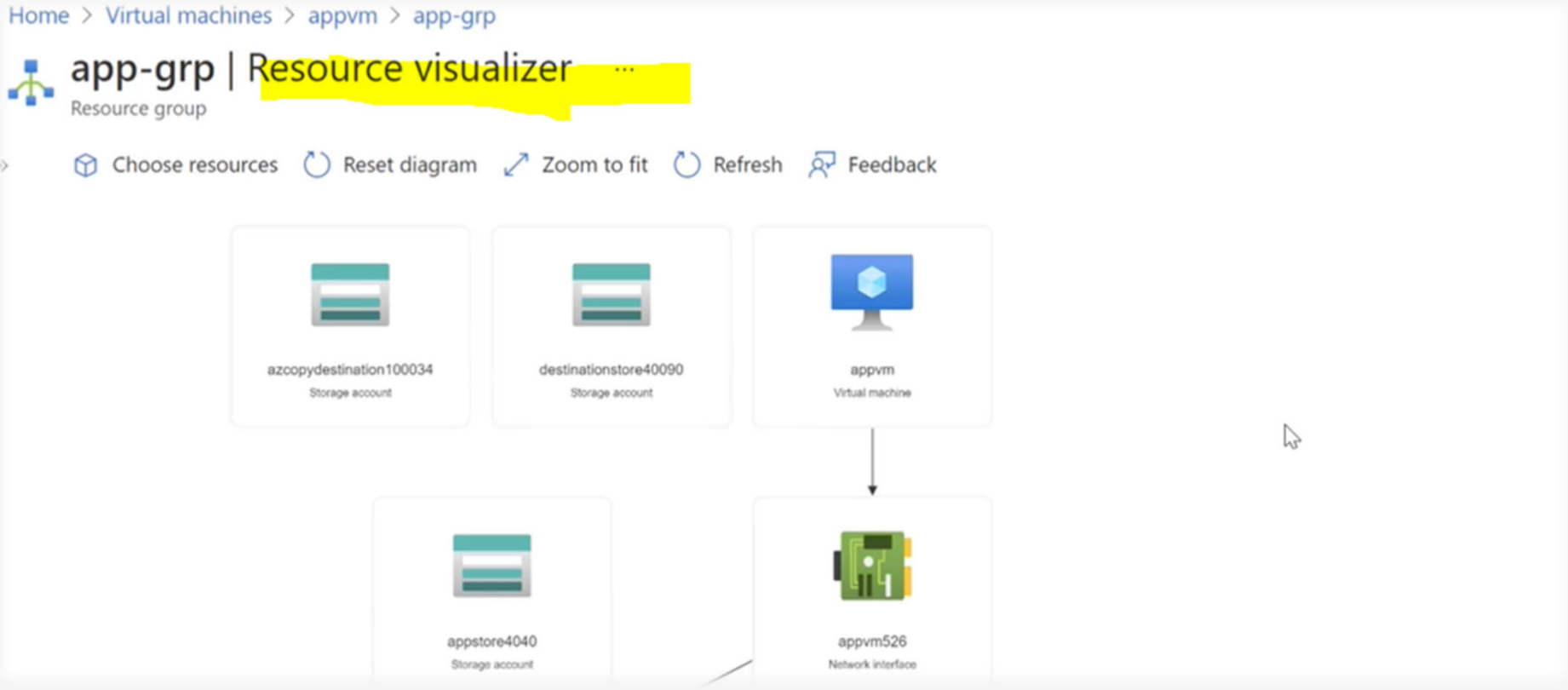
Lab 4 – Role Based Assignments | Contributor Role

Role	View	Change	Assign Permissions
Reader	✓	✗	✗
Contributor	✓	✓	✗
Owner	✓	✓	✓

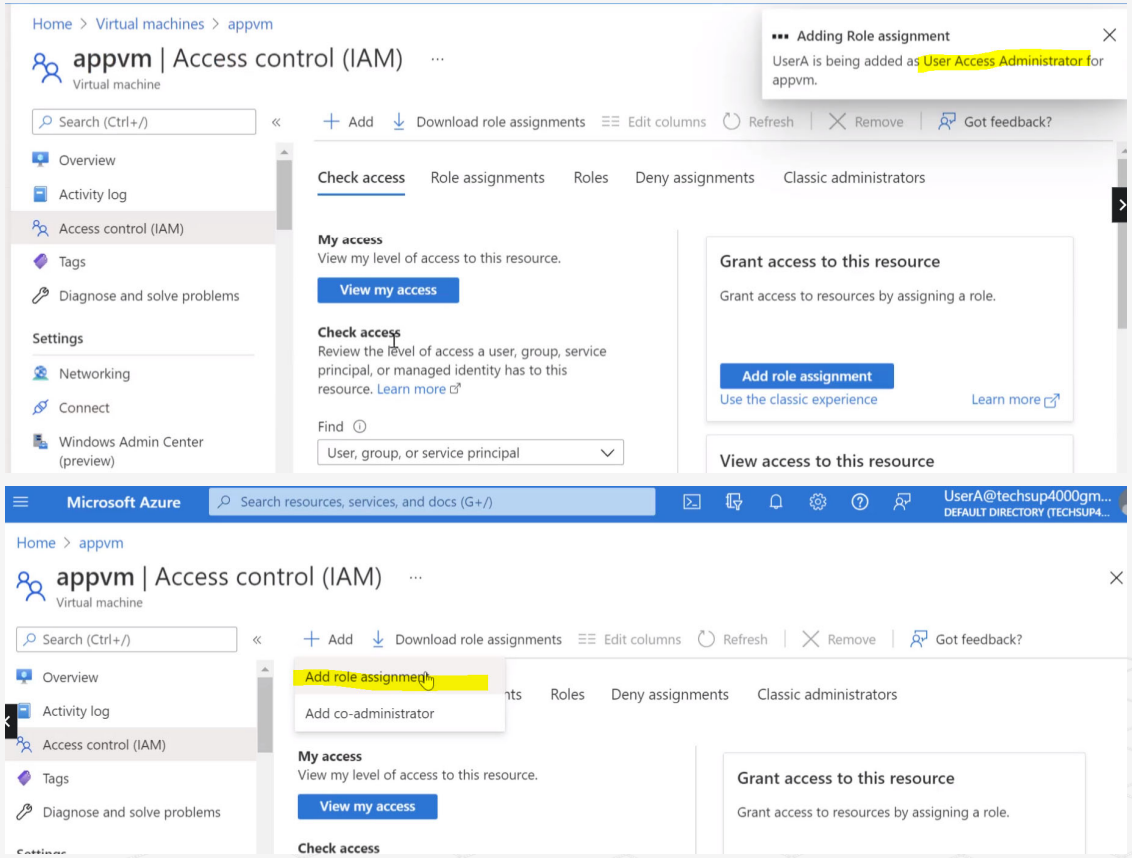




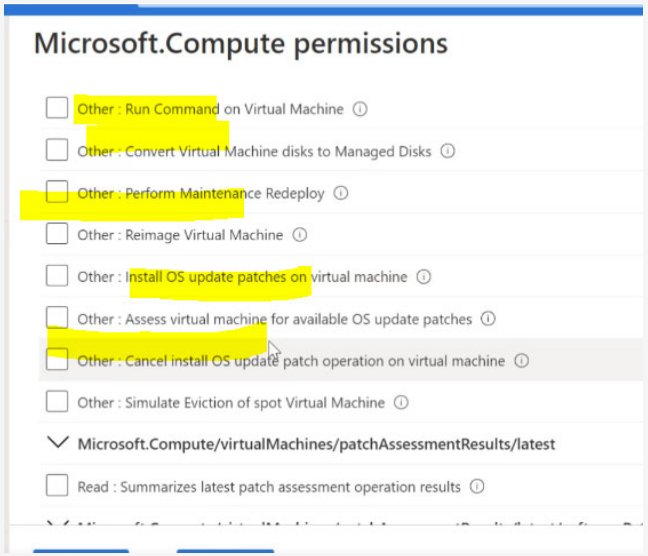
Resource Visualizer



Role Based Assignments | User Access Administrator Role



Lab 5 : - Custom roles for Azure resources



If the built-in roles for Azure resources don't meet the specific needs of your organization, you can create your own custom roles.

Just like built-in roles, you can assign custom roles to users, groups, and service principals at management group, subscription, and resource group scopes.

Custom roles can be shared between subscriptions that trust the same Azure AD directory.

There is a limit of 5,000 custom roles per directory. (For Azure Germany and Azure China 21Vianet, the limit is 2,000 custom roles.)

Custom roles can be created using the Azure portal, Azure PowerShell, Azure CLI, or the REST API.

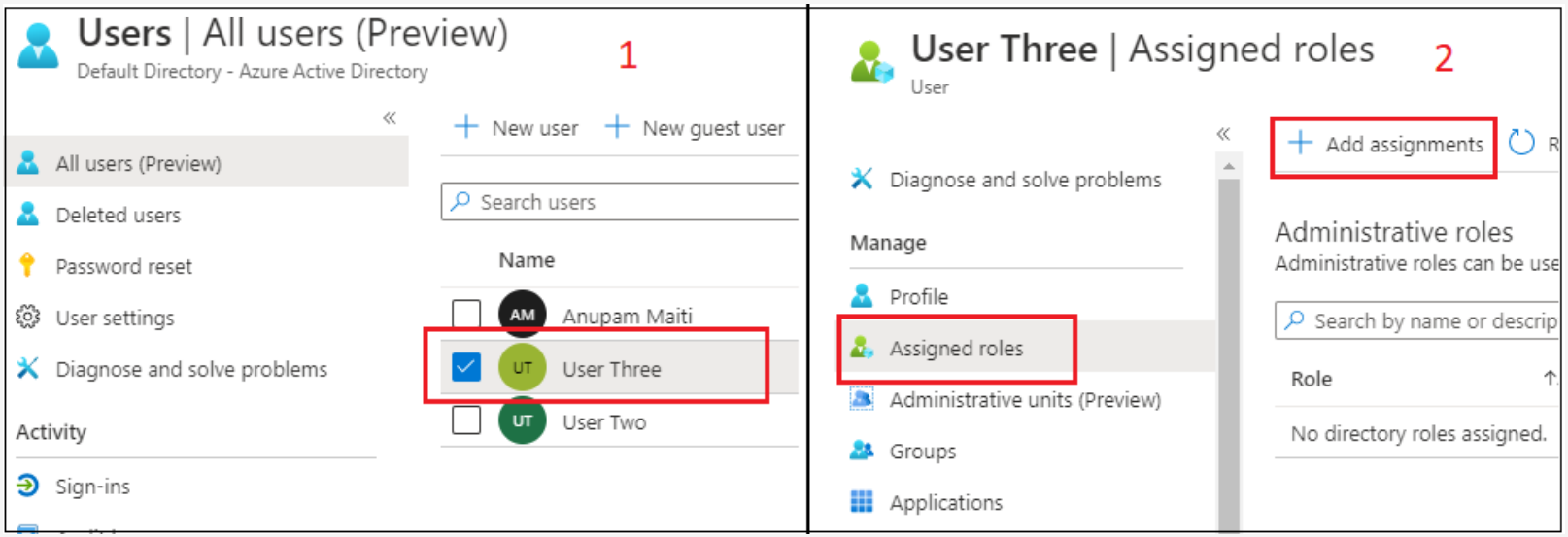
Custom role limits

The following list describes the limits for custom roles.

Each directory can have up to **5000** custom roles.

Azure Germany and Azure China 21Vianet can have up to 2000 custom roles for each directory.

Azure AD Roles Vs RBAC

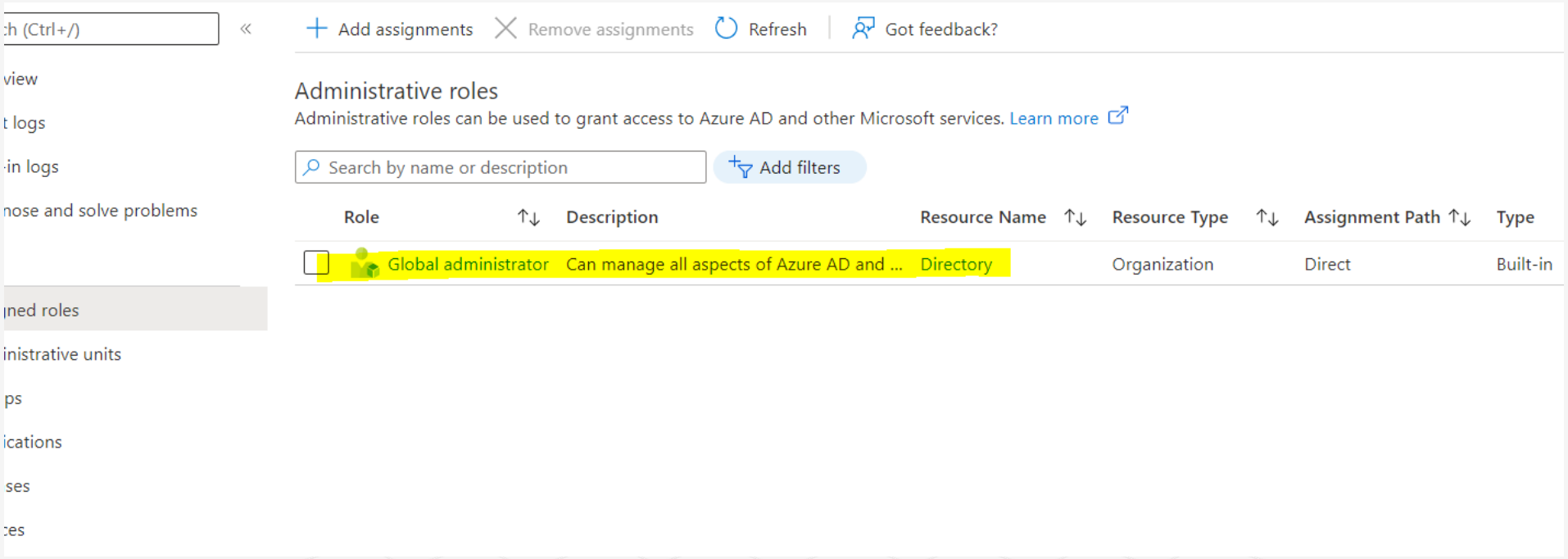


- Note :- Authorization Vs Tasks
- Creating a User / Managing Password
- Azure AD Roles and RBAC are different
- Azure AD role is having permission to complete certain action in Azure Active Directory

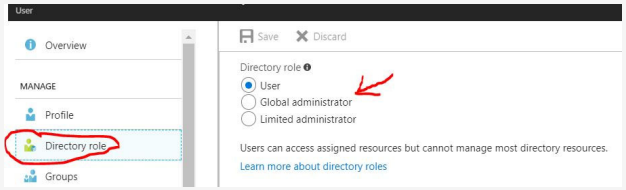
Investigate roles in Azure AD

- Using Azure Active Directory (Azure AD), you can **designate limited administrators** to manage identity tasks in less-privileged roles.
- **Administrators** can be assigned for such purposes as adding or changing users, assigning administrative roles, resetting user passwords, managing user licenses, and managing domain names

Limit the use of Global administrators



Limit the use of Global administrators



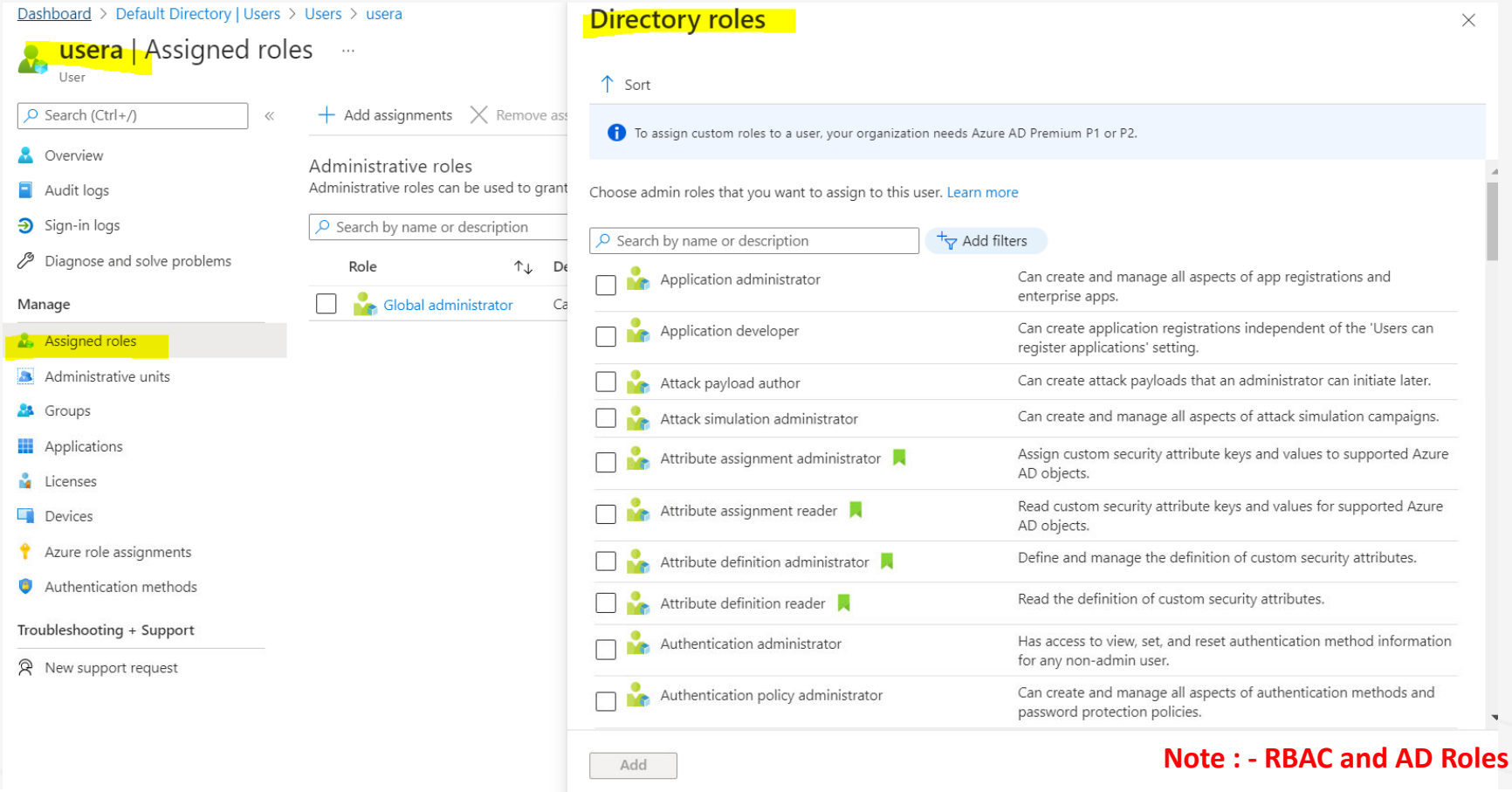
By default, the person who signs up for an Azure subscription is assigned the Global administrator role for the Azure AD organization.

Users who are assigned to the Global administrator role can read and modify every administrative setting in your Azure AD organization.

Only **Global administrators** and **Privileged Role administrators** can delegate administrator roles.

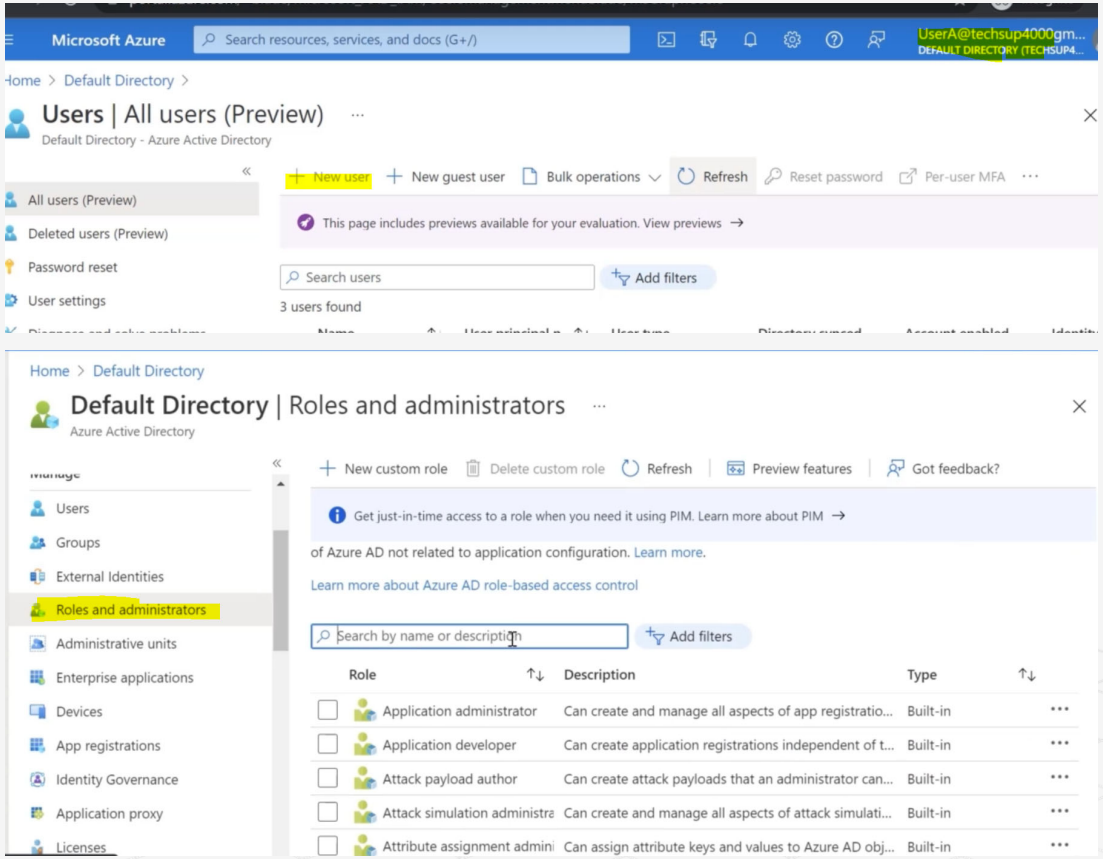
As a best practice, we recommend that you assign this role to fewer than five people in your organization

Assigning AD Roles / Available roles



Note : - RBAC and AD Roles are different

Lab 4: - Assigning AD Roles



- Login with New User and Point to AD for creating User
- Case Study – Delegating a User for creating User account (User Administrator Role)
- Assignments can be added from the user itself or Role and Administrator Option
- We can add Users and Group

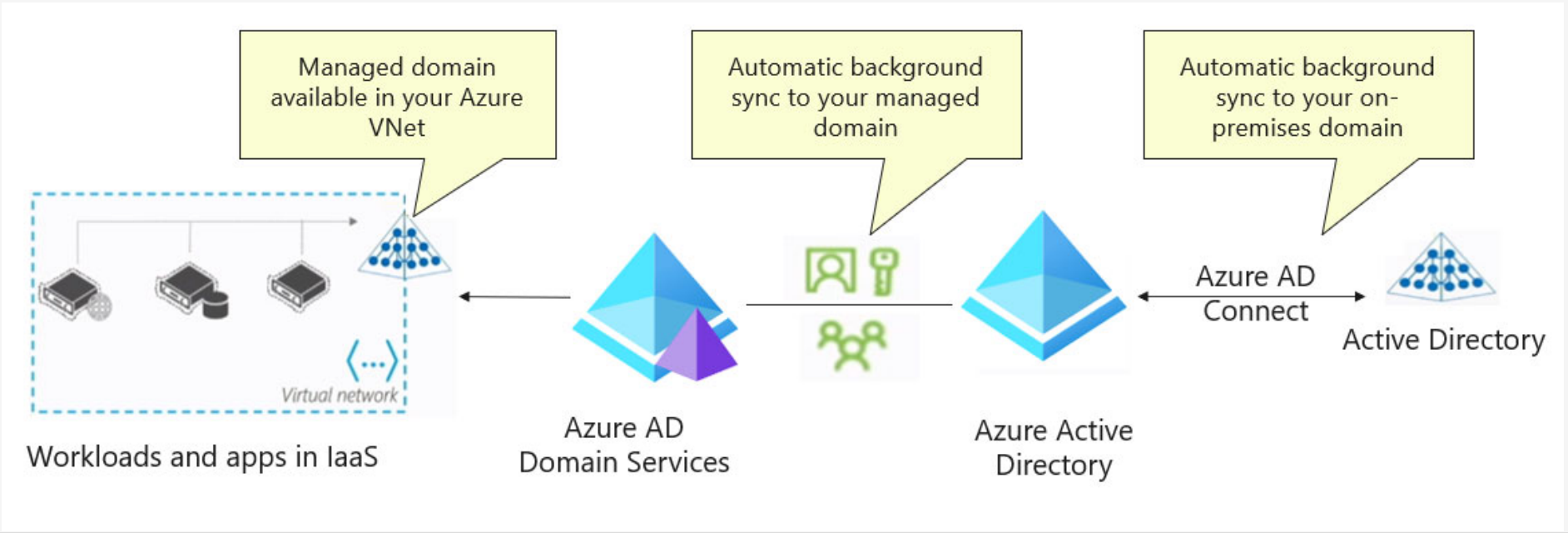
Summary

- For most organizations, the security of business assets depends on the integrity of the privileged accounts that administer and manage IT systems.
- **Cyber-attackers** focus on privileged access to infrastructure systems (such as Active Directory and Azure Active Directory) to gain access to an organization’s sensitive data.
- Traditional approaches that focus on securing the entrance and exit points of a network as the primary security perimeter are less effective due to the rise in the use of SaaS apps and personal devices on the Internet.
- The natural replacement for the network security perimeter in a complex modern enterprise is the authentication and authorization controls in an organization's identity layer.

Summary

- The natural replacement for the network security perimeter in a complex modern enterprise is the authentication and authorization controls in an organization's identity layer.
- Privileged administrative accounts are effectively in control of this **new security perimeter.**

Deploy Azure AD Domain Services (Azure ADDS)



Integrated with Azure AD

Use your corporate credentials and passwords

NTLM and Kerberos authentication

High availability and simple deployment experience

Deploy Azure AD 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 / NTLM authentication* that is fully compatible with Windows Server Active Directory.
- You use these domain services **without the need** to deploy, manage, and patch domain controllers in the cloud.
- Azure AD DS integrates with your existing Azure AD tenant, which makes it possible for users to sign in using their existing credentials
- You can also use existing groups and user accounts to secure access to resources, which provides a smoother lift-and-shift of on-premises resources to Azure.

Deploy Azure AD Domain Services

- Azure AD DS replicate's identity information from Azure AD, so it works with Azure AD tenants that are cloud-only.
- It can be synchronized with an on-premises Active Directory Domain Services (AD DS) environment.

Azure AD DS features and benefits

Simplified deployment experience: Azure AD DS is enabled for your Azure AD tenant using a single wizard in the Azure portal.

Integrated with Azure AD: User accounts, group memberships, and credentials are automatically available from your Azure AD tenant. Changed replicated

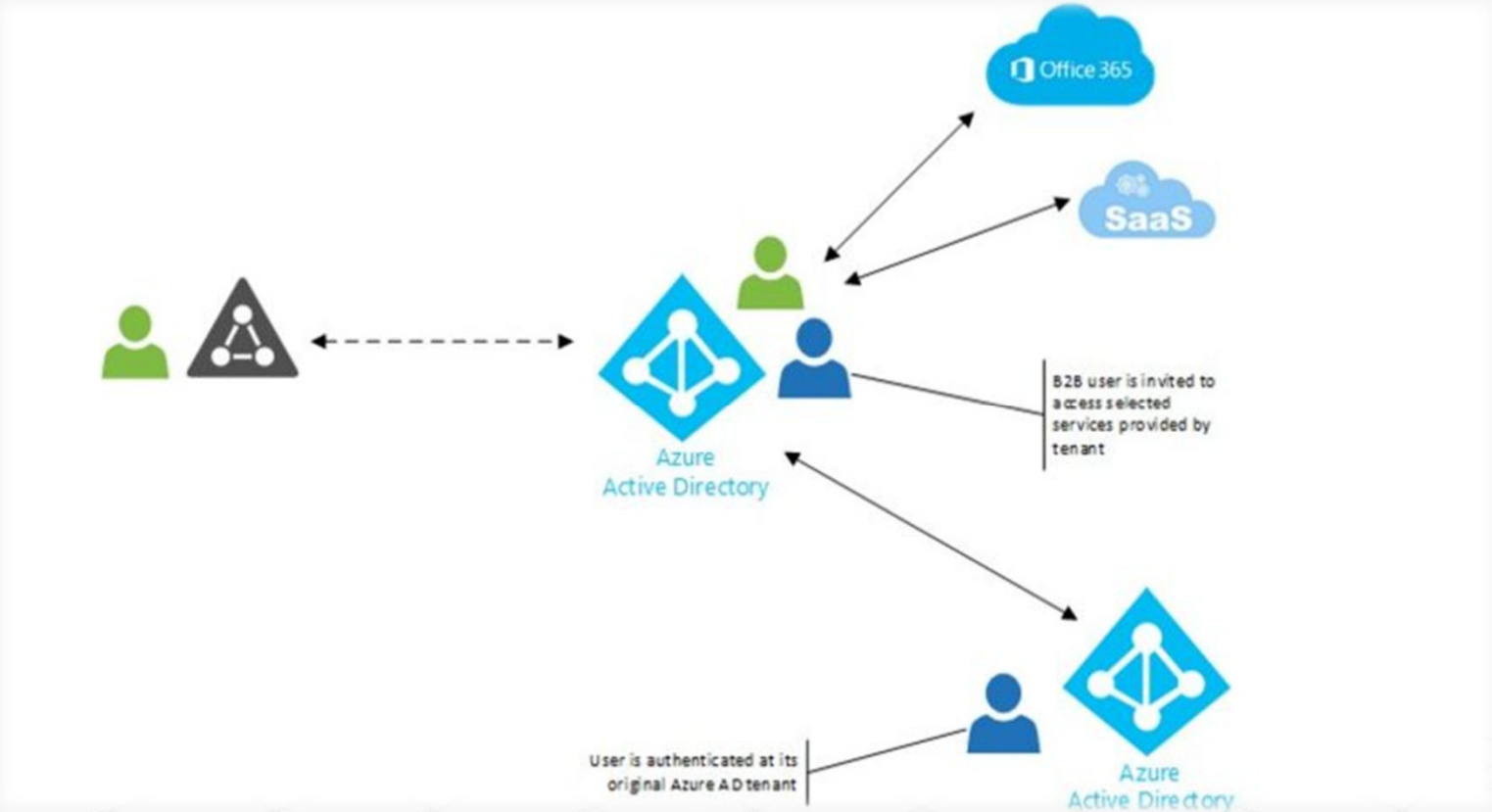
Use your corporate credentials/passwords: Passwords for users in Azure AD DS are the same as in your Azure AD tenant. Users can use their corporate credentials to domain-join machines, sign in interactively or over remote desktop, and authenticate against the Azure AD DS managed domain.

Azure AD DS features and benefits

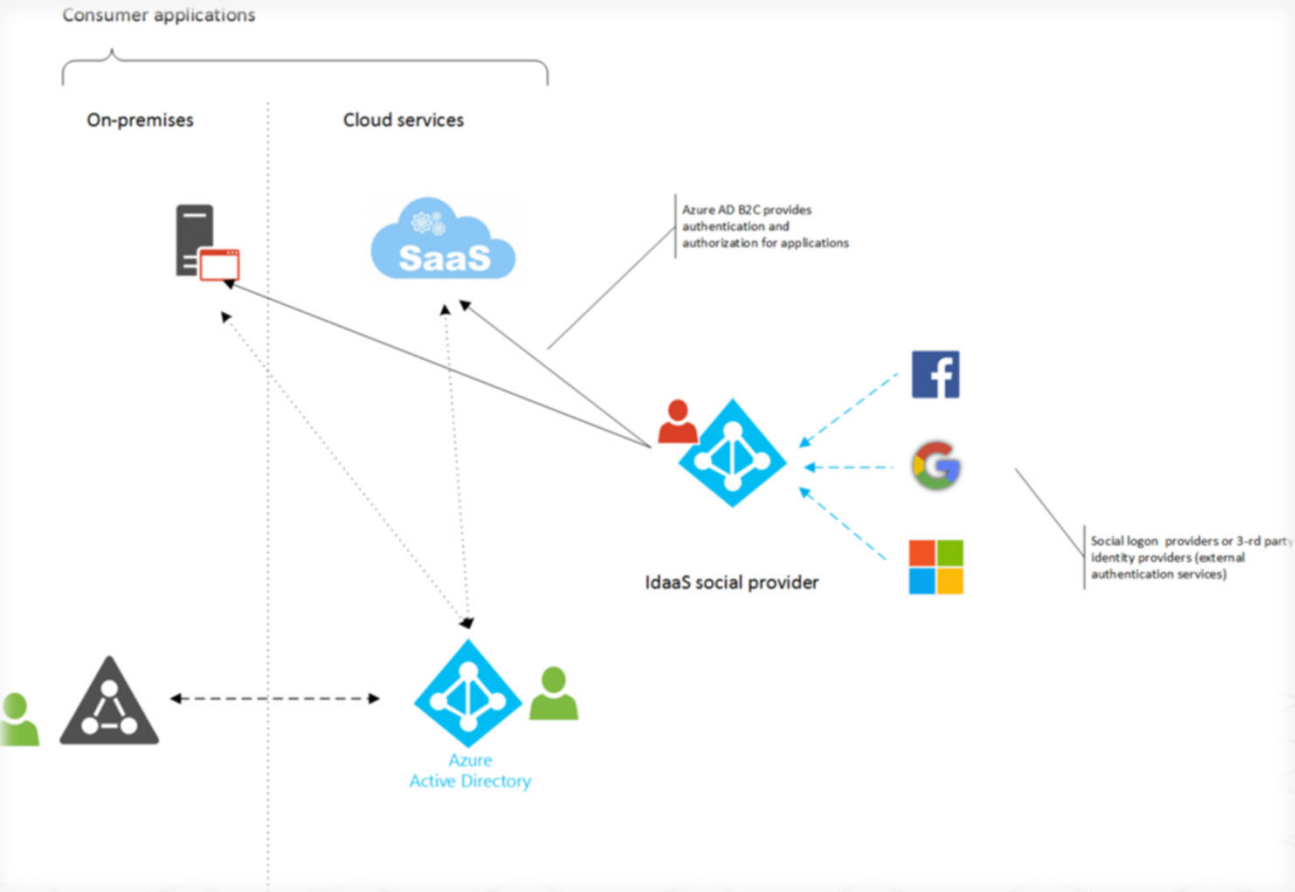
NTLM and Kerberos authentication: With support for NTLM and Kerberos authentication, you can deploy applications that rely on Windows-integrated authentication.

High availability: Azure AD DS includes multiple domain controllers, which provide high availability for your managed domain. This high availability guarantees service uptime and resilience to failures.

What is Azure AD B2B? – Additional information – Self Study



What is Azure AD B2C? – Additional information – Self Study



Knowledge Check Questions

Knowledge Check

Q 1 : - An Azure virtual machine would be a good option when you need to _____.

A. Build a development environment

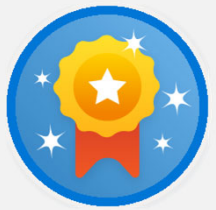
B. Run a custom application in azure

C. Extend your datacenter to the cloud

D. All the above

E. No of the above

End of presentation




Any Questions ?

Thank You

Break