



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

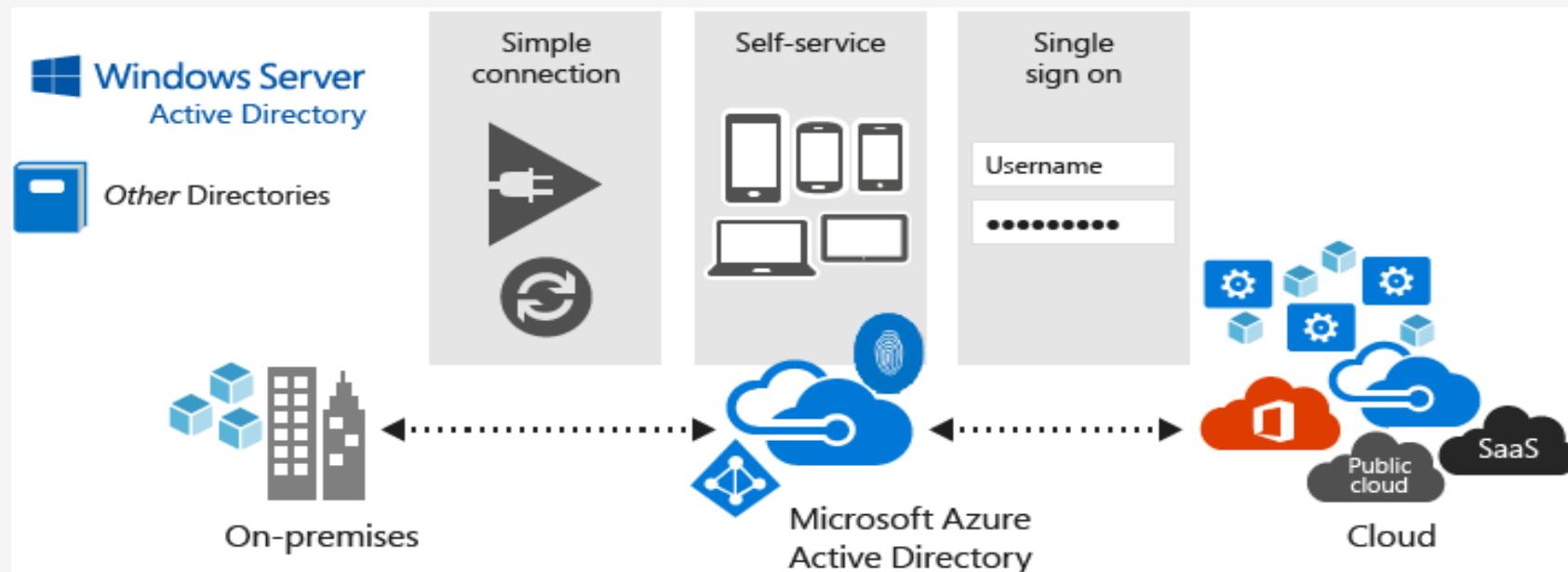


Subscription



Role-based access control

Azure Active Directory Features



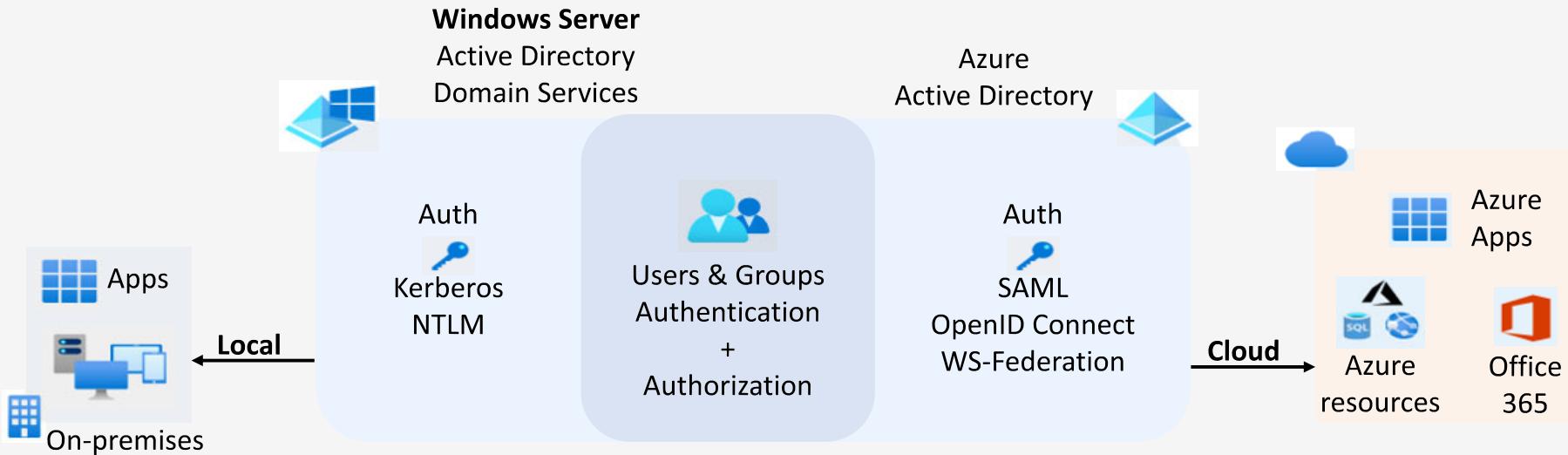
Microsoft's multi-tenant cloud-based directory and identity management service

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

Dashboard >

Default Directory | Overview

Azure Active Directory

- Overview**
- Preview features
- Diagnose and solve problems
- Manage**
 - Users
 - Groups
 - External Identities
 - Roles and administrators
 - Administrative units
 - Enterprise applications
 - Devices
 - App registrations
 - Identity Governance
 - Application proxy
 - Custom security attributes (Preview)
 - Licenses
 - Azure AD Connect
 - Custom domain names

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center.

[Add](#) [Manage tenants](#) [What's new](#) [Preview features](#) [Got feedback?](#)

[Overview](#) [Monitoring](#) [Properties](#) [Tutorials](#)

Search your tenant

Basic information

Name	Default Directory	Users	4
Tenant ID	644626f6-407f-4b53-bbba-fa056542783a	Groups	4
Primary domain	ravisankarmind@gmail.onmicrosoft.com	Applications	0
License	Azure AD Free	Devices	0

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation

Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

[Learn more](#)

Subscribing Trial version of Azure Premium Licence

Default Directory | Overview ...

Azure Active Directory

Add Manage tenants What's new Preview features Got feedback?

Basic Information

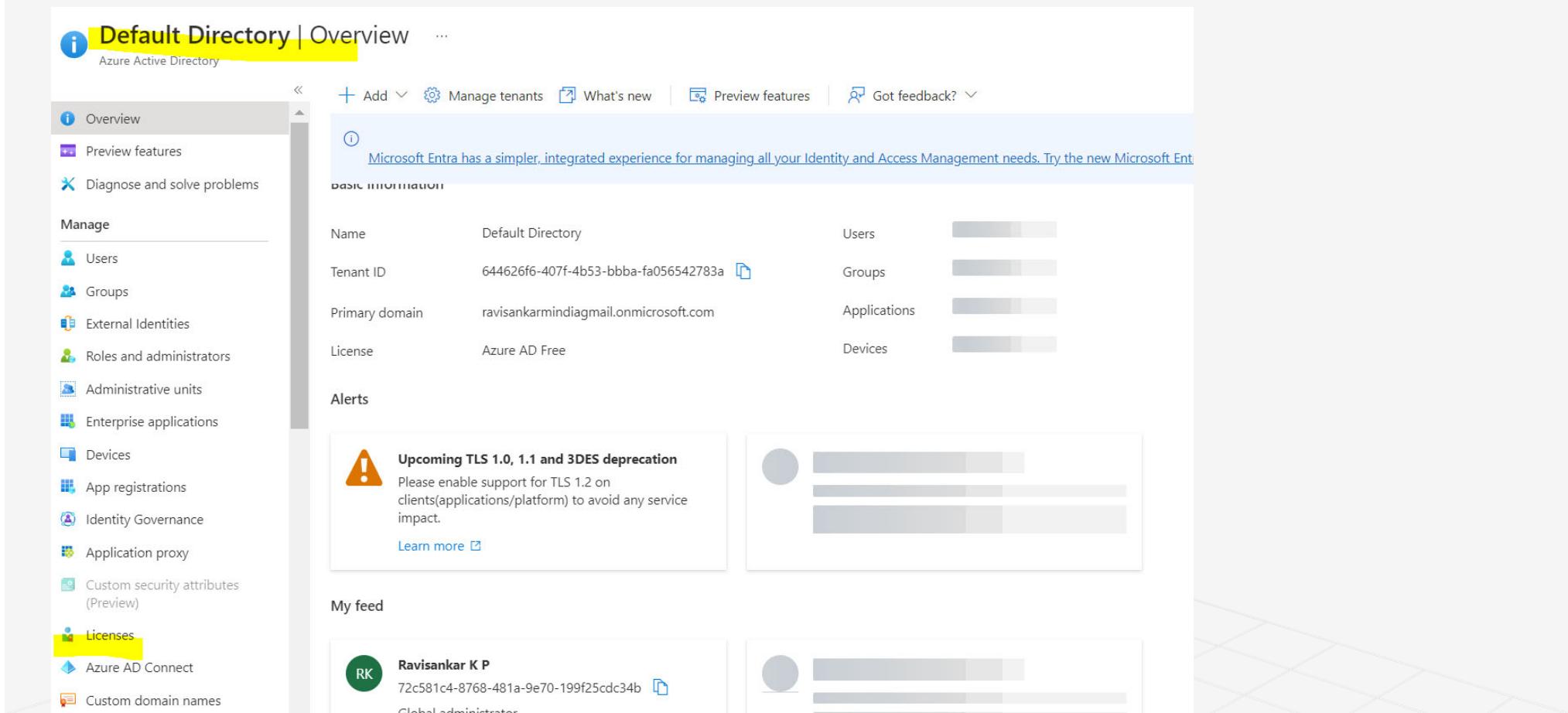
Name	Default Directory	Users	[Progress Bar]
Tenant ID	644626f6-407f-4b53-bbba-fa056542783a	Groups	[Progress Bar]
Primary domain	ravisankarmidi@gmail.onmicrosoft.com	Applications	[Progress Bar]
License	Azure AD Free	Devices	[Progress Bar]

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation
Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.
[Learn more](#)

My feed

Ravisankar K P
72c581c4-8768-481a-9e70-199f25cdc34b
Global administrator



Changing Directory

The screenshot shows the Azure portal interface with three main windows:

- Subscriptions** (Left): Shows a list of subscriptions. One subscription, "Training", is selected. Filters include "global filter", "My role == all", and "Status == all".
- Training Subscription Details** (Center): Displays the "Training" subscription's overview. It includes a warning about credits remaining, a list of essentials (Subscription ID, Directory, My role, Offer, Parent management group), and a billing section showing ₹0.00.
- Change the directory** (Right): A modal dialog explaining that changing the directory does not affect billing ownership. It shows the "From" field set to "Default Directory (ravisankarmindiagmail.onmicrosoft.com)" and the "To" field set to "Select a directory". A note states: "Cannot change directory because you only have access to one directory." A checkbox for understanding the implications is present.

Changing Directory – Create Tenant

[Dashboard](#) > [Default Directory | Overview](#) > [Switch tenant](#) >

Create a tenant ...

Azure Active Directory

* Basics * Configuration Review + create

Azure Active Directory and Azure Active Directory (B2C) enable users to access applications published by your organization, and share same administration experiences. [Learn more](#)

Tenant type

Select a tenant type *

Azure Active Directory

Azure Active Directory (B2C)

[Help me choose...](#)

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

Free

- Support for up to 500,000 objects
- Single Sign-On (SSO)
- Azure B2B (For Ext. Users)
- Azure AD Connect
- Self-Service Password Reset
- MFA (App. Auth. Only)
- Standard Reporting etc.

Office 365 Apps

- All Features of Free Plan
- No Object Limit
- Company Branding
- Self Service Password Reset
- Application Proxy
- SLA of 99.9% etc.

Premium P1

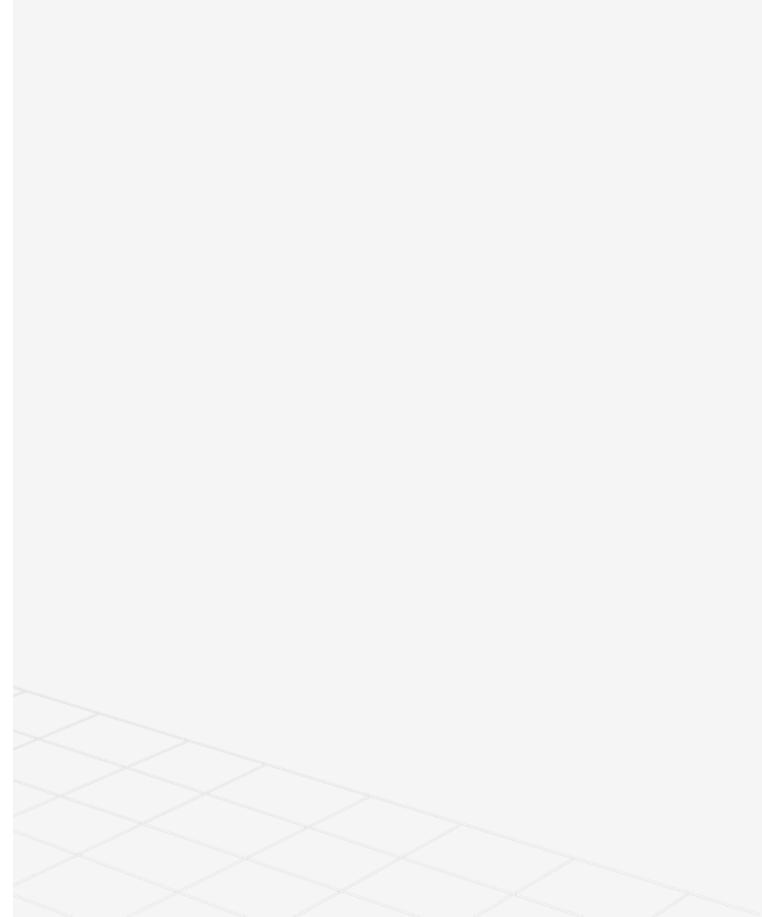
- All Features of Basic Plan
- Full Multi Factor Auth.
- Cloud App Discovery
- MDM Auto Enrollment
- Conditional Access
- Azure AD Connect Health
- Advance Reporting etc.

Premium P2

- All Features of P1 Plan
- Vulnerabilities & Risky Accounts Detection
- Risk Events Investigation
- Risk Based Conditional Access Policies
- Privileged Identity Management
- Access Reviews etc.

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

Home / Azure pricing / Azure Active Directory pricing

Azure Active Directory pricing

[Request a pricing quote](#) [Try Azure for free](#)



Overview Pricing table Purchase options Resources FAQs Azure Active Directory >

**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

The screenshot shows the Azure Active Directory Admin Center interface. The left sidebar includes links for Dashboard, All services, Favorites (Azure Active Directory, Users, Enterprise applications), Activity (Sign-in logs, Audit logs, Bulk operation results), and Troubleshooting + Support (New support request). The main content area is titled "Users | All users" under "Default Directory - Azure Active Directory". It features a search bar and filter options. A message at the top says, "Want to switch back to the legacy users list experience? Click here to leave the preview." Below this, it shows "1 user found" with a table containing one row:

<input type="checkbox"/>	Display name ↑	User principal name	User type	On-premises sy...	Identities	Company name	Creation type
<input type="checkbox"/>	Ravisankar K P	ravisankar.mindia...	Member	No	MicrosoftAccount		

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

Trust between Azure Subscription and Azure AD

The screenshot shows the Azure portal interface for a subscription named "Training". The left sidebar lists various management categories like Overview, Activity log, Access control (IAM), Tags, etc. The main content area displays the "Essentials" section with detailed subscription information. A yellow highlight is applied to the "Default Directory" field, which contains the value "ravisankarmindiagmail.onmicrosoft.com".

Setting	Value
Subscription ID	bc37234c-2f86-4b20-9781-988760921779
Subscription name	Training
Current billing period	7/11/2022-8/10/2022
Currency	INR
Status	Active
Secure Score	Not available
Parent management group	644626f6-407f-4b53-bbba-fa056542783a

Below the essentials section, there are two cards: "Latest billed amount" and "Invoices over time".



Role Based Access Control

Learn.
Connect.
Explore.

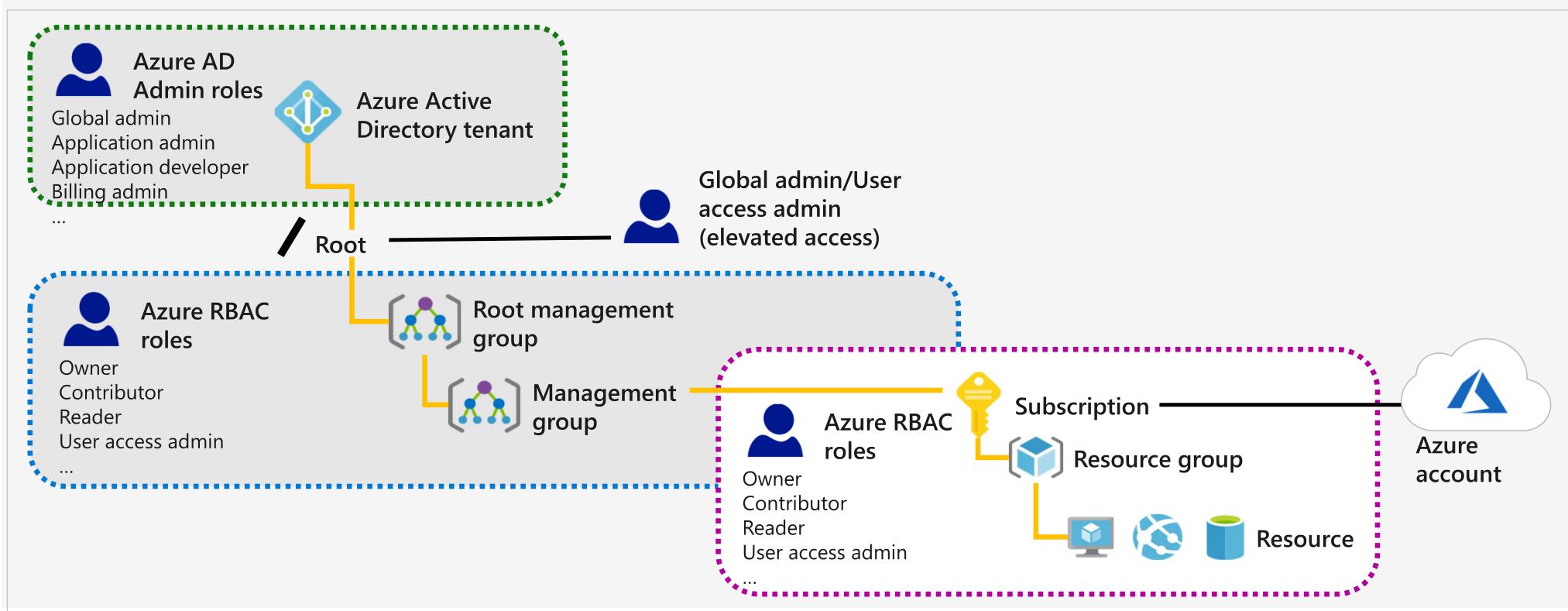


What is Role Based Access Control ?



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

All resources ⚡ ...

Default Directory

+ Create Manage view Refresh Export to CSV Open query Assign tags Delete Feedback

Filter for any field... Subscription == Azure subscription 1 Resource group == all Type == all Location == all

Add filter

Showing 1 to 10 of 10 records. Show hidden types ⓘ No grouping List view

<input type="checkbox"/> Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
<input type="checkbox"/> app-network	Virtual network	app-grp	North Europe	Azure subscription 1
<input type="checkbox"/> appstore4040	Storage account	app-grp	North Europe	Azure subscription 1
<input type="checkbox"/> appvm	Virtual machine	app-grp	North Europe	Azure subscription 1
<input type="checkbox"/> appvm-ip	Public IP address	app-grp	North Europe	Azure subscription 1
<input type="checkbox"/> appvm-nsg	Network security group	app-grp	North Europe	Azure subscription 1

Lab – Role Based Assignments

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

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, a search bar, and various icons. On the right, it shows the user's name (UserA@techsup4000gm...) and the default directory (TECHSUP4...).

The main content area displays a virtual machine named "appvm". The left sidebar has a tree view with "Overview" selected, followed by "Activity log", "Access control (IAM)", "Tags", and "Diagnose and solve problems". Below that is a "Settings" section with "Networking", "Connect", and "Windows Admin Center (preview)".

The right pane shows the "Essentials" section for the VM. It includes details like Resource group (Move), app-grp, Status (Running), Location (North Europe), Subscription (Move), Azure subscription 1, Subscription ID (6912d7a0-bc28-459a-9407-33bbba641c07), and Tags (Edit). There's also a "Copy to clipboard" button for the IP address.

At the bottom right of the essentials pane, there's a "JSON View" link.

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

Home > Virtual machines > appvm >

 **app-grp** ⚡ ...
Resource group

« + Create Edit columns Delete resource group ⟳ Refresh ⬇ Export to CSV 🔗 Open

[?] Overview ▲ Essentials

Activity log

🔍 Access control (IAM) Subscription (Move) Deployments
Azure subscription 1 7 Succeeded

Tags Subscription ID Location
Resource visualizer 6912d7a0-bc28-459a-9407-33bbba641c07 North Europe

Events

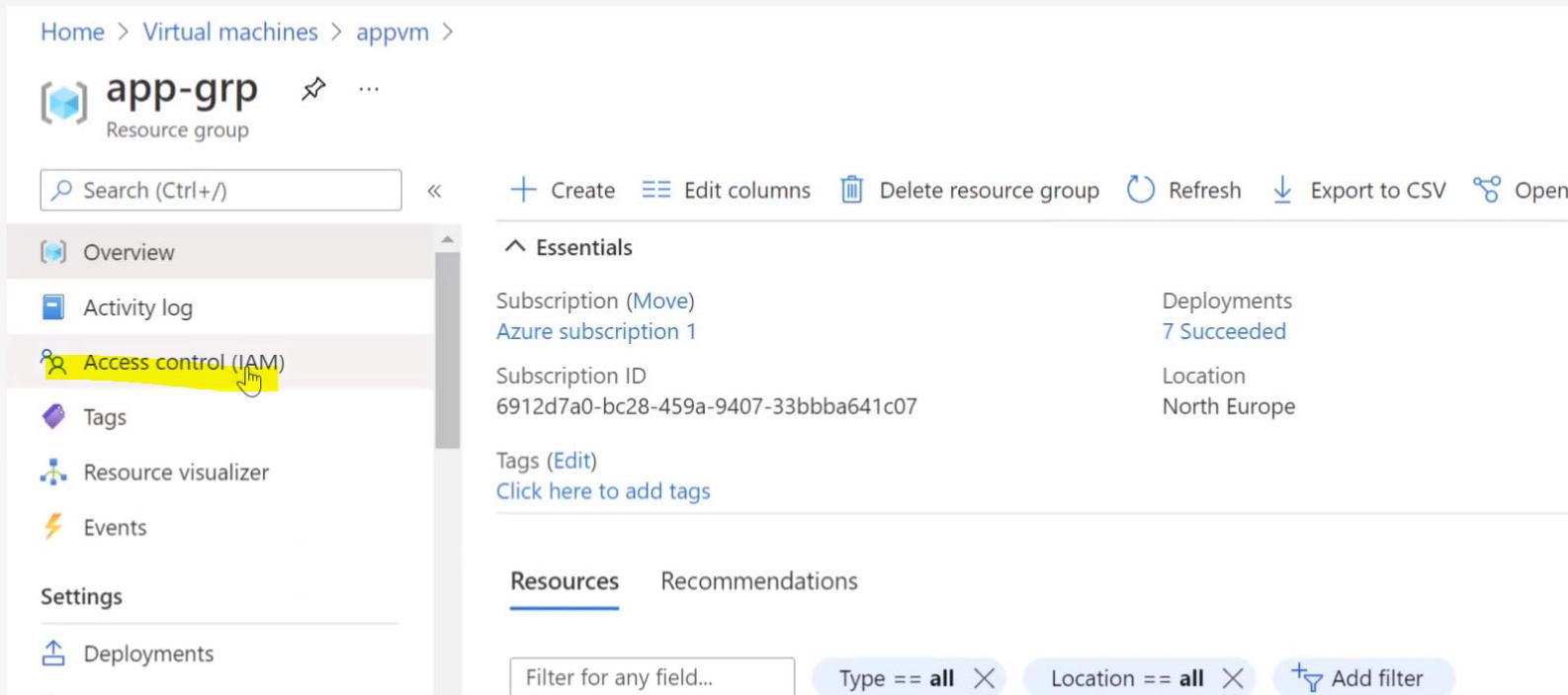
Settings

Deployments

...

Resources Recommendations

Type == all X Location == all X + Add filter



Lab 3 – Role Based Assignments | Reader - Subscription Level

Home > Virtual machines > appvm >

The screenshot shows the Azure Resource Group 'app-grp' overview page. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Deployments, and a partially visible 'Logs' link. The 'Access control (IAM)' link is highlighted with a yellow box and a cursor icon. The main content area displays the 'Essentials' section with details: Subscription (Move) to Azure subscription 1, Deployment count (7 Succeeded), Subscription ID (6912d7a0-bc28-459a-9407-33bbba641c07), Location (North Europe), and Tags (Edit). Below this is the 'Resources' section, which is currently empty. Filter options at the bottom allow filtering by Type (all), Location (all), and adding a filter.

app-grp

Resource group

Search (Ctrl+ /)

Create Edit columns Delete resource group Refresh Export to CSV Open

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Subscription (Move)
Azure subscription 1

Deployment
7 Succeeded

Subscription ID
6912d7a0-bc28-459a-9407-33bbba641c07

Location
North Europe

Tags (Edit)
Click here to add tags

Resources Recommendations

Filter for any field... Type == all Location == all Add filter

Lab 4 – Role Based Assignments | Contributor Role

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

Home > Virtual machines >

appvm ...

Virtual machine

Search (Ctrl+ /)

Connect Start Restart Stop Capture Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Resource group (Move) **app-grp**

Status Running

Location North Europe

Subscription (Move) **Azure subscription 1**

Subscription ID 6912d7a0-bc28-459a-9407-33bbba641c07

Failed to stop virtual machine

Failed to stop the virtual machine 'appvm'. Error: The client 'UserA@techsup400@gmail.onmicrosoft.com' with object id '30df944-00d3-422c-b4e2-75d291819961' does not have authorization to perform action 'Microsoft.Compute/virtualMachines/deallocate/action' over scope 'app-grp/providers/Microsoft.Compute/virtualMachines/appvm' or the scope is invalid. Access was recently granted, please refresh your credentials.

Home > Virtual machines > app-grp >

Add role assignment ...

Got feedback? ...

Custom roles: [Learn more](#) [Use classic experience](#)

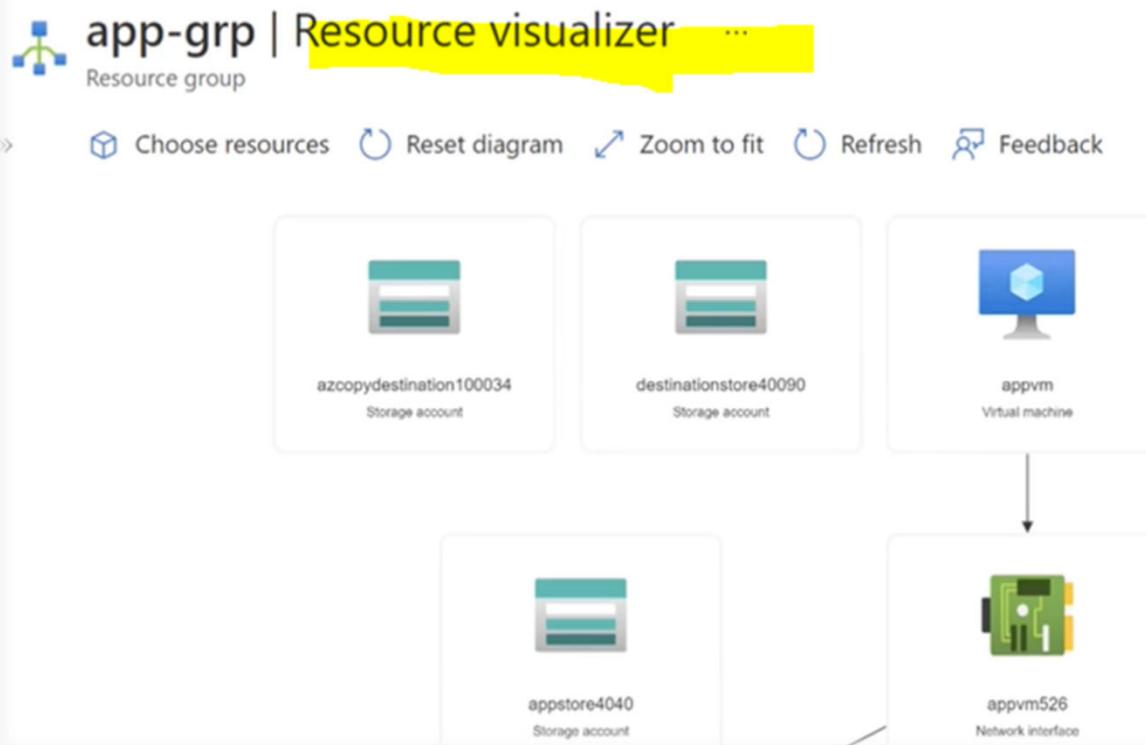
Virtual Machine Con Type : All Category : All

Showing 3 of 317 roles

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓
Classic Virtual Machine Contributor	Lets you manage classic virtual machines, but not access to them,...	BuiltInRole	Compute
Dev/Test Labs User	Lets you connect, start, restart, and shutdown your virtual machin...	BuiltInRole	Devops
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and n...	BuiltInRole	Compute

Resource Visualizer

Home > Virtual machines > appvm > app-grp



Role Based Assignments | User Access Administrator Role

The screenshot shows the Microsoft Azure portal interface for managing access control (IAM) on a virtual machine named 'appvm'. The top navigation bar includes 'Microsoft Azure', a search bar, and user information ('UserA@techsup4000gm...'). The main page displays the 'Access control (IAM)' section for 'appvm', with tabs for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', and 'Settings'. The 'Access control (IAM)' tab is selected. On the right, a modal window titled 'Adding Role assignment' shows the message 'UserA is being added as User Access Administrator for appvm.' Below the modal, there are buttons for 'Add', 'Download role assignments', 'Edit columns', 'Refresh', 'Remove', and 'Got feedback?'. The main content area has tabs for 'Check access', 'Role assignments', 'Roles', 'Deny assignments', and 'Classic administrators', with 'Check access' currently selected. It features sections for 'My access' (with a 'View my access' button), 'Check access' (with a 'Find' input field and dropdown), and 'Grant access to this resource' (with a 'Add role assignment' button). The bottom of the page shows a navigation bar with 'Home > appvm'.

Lab 5 : - Custom roles for Azure resources

Microsoft.Compute permissions

- Other : Run Command on Virtual Machine ⓘ
- Other : Convert Virtual Machine disks to Managed Disks ⓘ
- Other : Perform Maintenance Redeploy ⓘ
- Other : Reimage Virtual Machine ⓘ
- Other : Install OS update patches on virtual machine ⓘ
- Other : Assess virtual machine for available OS update patches ⓘ
- Other : Cancel install OS update patch operation on virtual machine ⓘ
- Other : Simulate Eviction of spot Virtual Machine ⓘ

▼ Microsoft.Compute/virtualMachines/patchAssessmentResults/latest

- Read : Summarizes latest patch assessment operation results ⓘ

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

The image displays two screenshots from the Azure Active Directory (AAD) portal. The left screenshot, labeled '1', shows the 'Users | All users (Preview)' page. It lists users Anupam Maiti (AM), User Three (UT), and User Two (UT). The user 'User Three' is highlighted with a red box. The right screenshot, labeled '2', shows the 'User Three | Assigned roles' page. It displays the 'Assigned roles' section, which is currently empty. A red box highlights the '+ Add assignments' button.

- 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

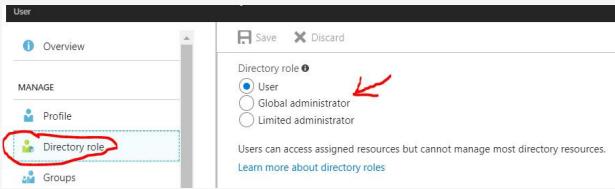
Limit the use of Global administrators

The screenshot shows the Azure portal interface for managing administrative roles. The left sidebar has a 'Global administrator' section selected. The main content area is titled 'Administrative roles' with a sub-instruction: 'Administrative roles can be used to grant access to Azure AD and other Microsoft services.' A 'Learn more' link is available. Below this is a search bar and a 'Add filters' button. A table lists the roles:

Role	Description	Resource Name	Resource Type	Assignment Path	Type
<input type="checkbox"/> Global administrator	Can manage all aspects of Azure AD and ...	Directory	Organization	Direct	Built-in

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

Dashboard > Default Directory | Users > Users > usera

usera | Assigned roles ...

User

Search (Ctrl+/
)

+ Add assignments X Remove ass

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Troubleshooting + Support

New support request

Directory roles

Sort

To assign custom roles to a user, your organization needs Azure AD Premium P1 or P2.

Choose admin roles that you want to assign to this user. [Learn more](#)

Search by name or description

Add filters

Role	Description
<input type="checkbox"/> Global administrator	Can create and manage all aspects of app registrations and enterprise apps.
<input type="checkbox"/> Application administrator	Can create application registrations independent of the 'Users can register applications' setting.
<input type="checkbox"/> Application developer	Can create attack payloads that an administrator can initiate later.
<input type="checkbox"/> Attack payload author	Can create and manage all aspects of attack simulation campaigns.
<input type="checkbox"/> Attack simulation administrator	Assign custom security attribute keys and values to supported Azure AD objects.
<input type="checkbox"/> Attribute assignment administrator	Read custom security attribute keys and values for supported Azure AD objects.
<input type="checkbox"/> Attribute assignment reader	Define and manage the definition of custom security attributes.
<input type="checkbox"/> Attribute definition administrator	Read the definition of custom security attributes.
<input type="checkbox"/> Attribute definition reader	Has access to view, set, and reset authentication method information for any non-admin user.
<input type="checkbox"/> Authentication administrator	Can create and manage all aspects of authentication methods and password protection policies.
<input type="checkbox"/> Authentication policy administrator	

Add

Note : - RBAC and AD Roles are different

Lab 4: - Assigning AD Roles

The screenshot shows two overlapping Azure Active Directory management pages:

- Top Window: Users | All users (Preview)**
 - Header: Microsoft Azure, Search resources, services, and docs (G+), UserA@techsup4000gm..., DEFAULT DIRECTORY (TECHSUP4...).
 - Breadcrumbs: Home > Default Directory > Users | All users (Preview).
 - Left sidebar: All users (Preview), Deleted users (Preview), Password reset, User settings.
 - Content: New user, New guest user, Bulk operations, Refresh, Reset password, Per-user MFA.
 - Note: This page includes previews available for your evaluation. View previews →
 - Search bar: Search users, Add filters.
 - Results: 3 users found.
- Bottom Window: Default Directory | Roles and administrators**
 - Header: Microsoft Azure, Search resources, services, and docs (G+), UserA@techsup4000gm..., DEFAULT DIRECTORY (TECHSUP4...).
 - Breadcrumbs: Home > Default Directory > Default Directory | Roles and administrators.
 - Left sidebar: Manage (Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses).
 - Content:
 - New custom role, Delete custom role, Refresh, Preview features, Got feedback?
 - Note: Get just-in-time access to a role when you need it using PIM. Learn more about PIM →
 - Note: of Azure AD not related to application configuration. Learn more.
 - Learn more about Azure AD role-based access control.
 - Search bar: Search by name or description, Add filters.
 - Table: Role, Description, Type, Actions (three dots).

Role	Description	Type	Action
Application administrator	Can create and manage all aspects of app registration...	Built-in	...
Application developer	Can create application registrations independent of t...	Built-in	...
Attack payload author	Can create attack payloads that an administrator can...	Built-in	...
Attack simulation administra	Can create and manage all aspects of attack simulati...	Built-in	...
Attribute assignment admini	Can assign attribute keys and values to Azure AD obj...	Built-in	...

- 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

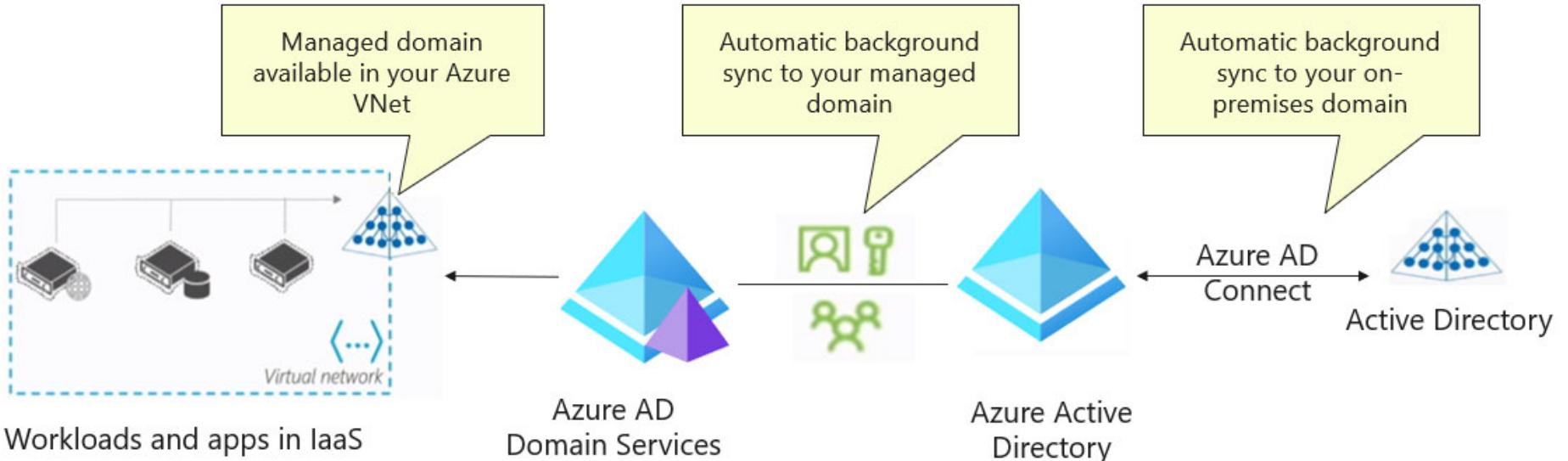
Summary

- 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. Changes 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

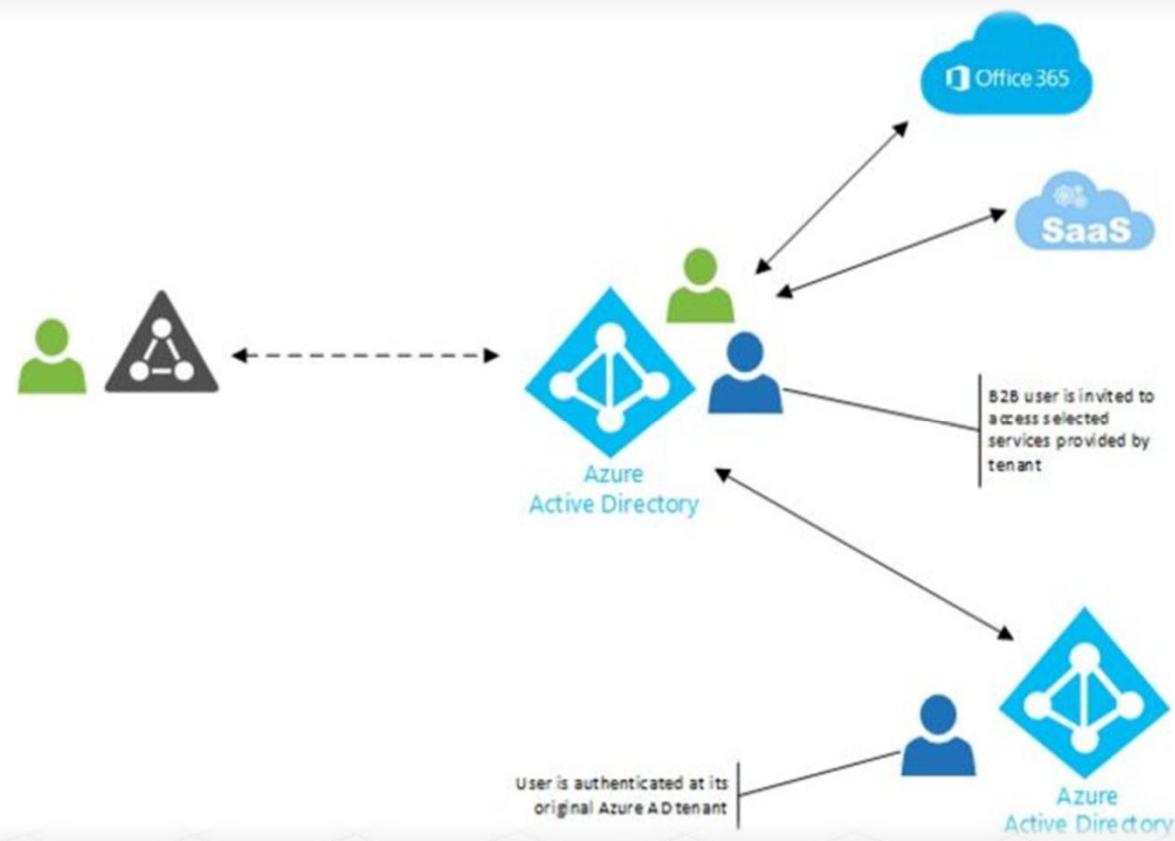


NTLM and Kerberos authentication: With support for NTLM and Kerberos authentication, you can deploy applications that rely on Windows-integrated authentication.

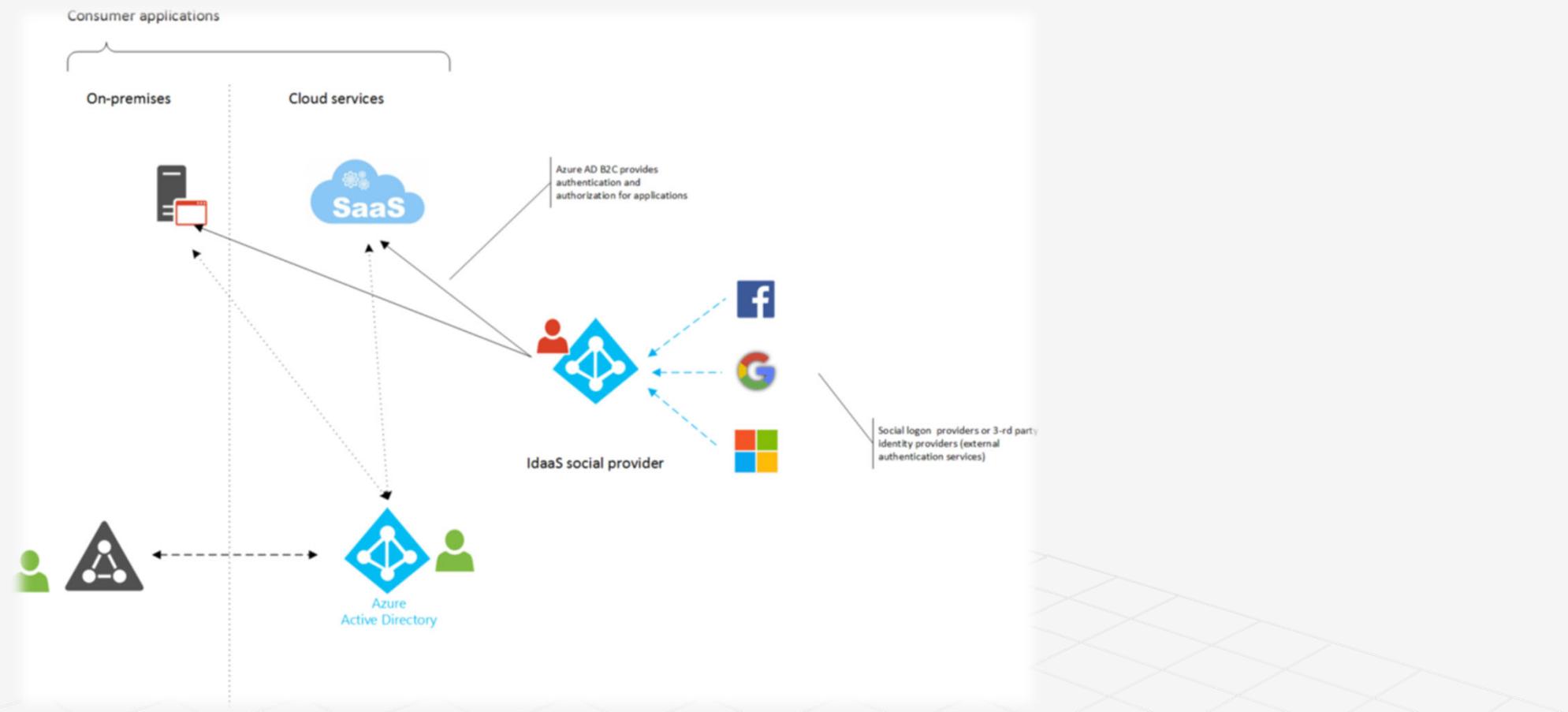


High availability: Azure AD DS includes multiple domain controllers, which provide high availability for your managed domain. This high availability guarantees service uptime and resilience to failures.

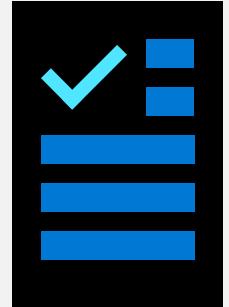
What is Azure AD B2B? – Additional information – Self Study



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



Knowledge Check Questions



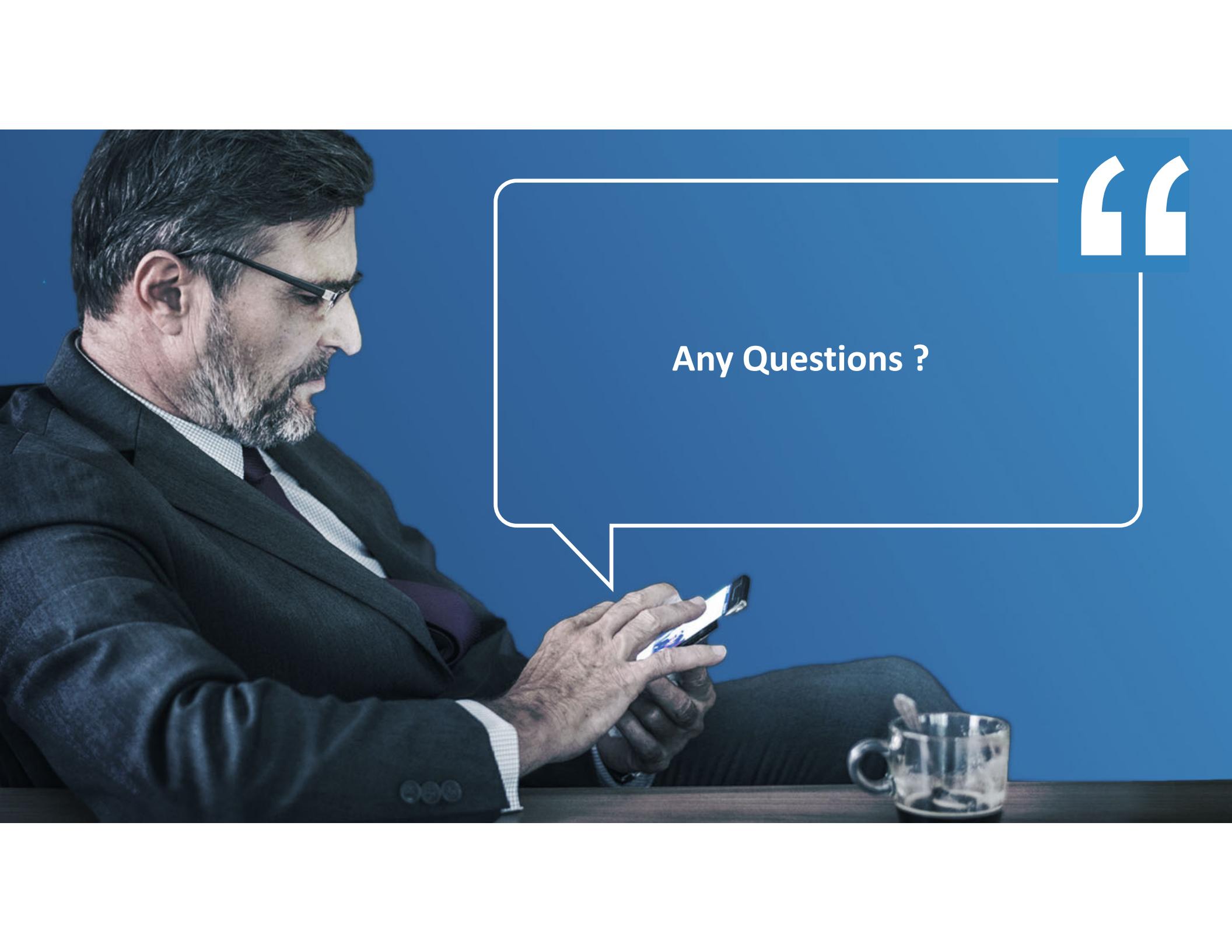
Knowledge Check

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

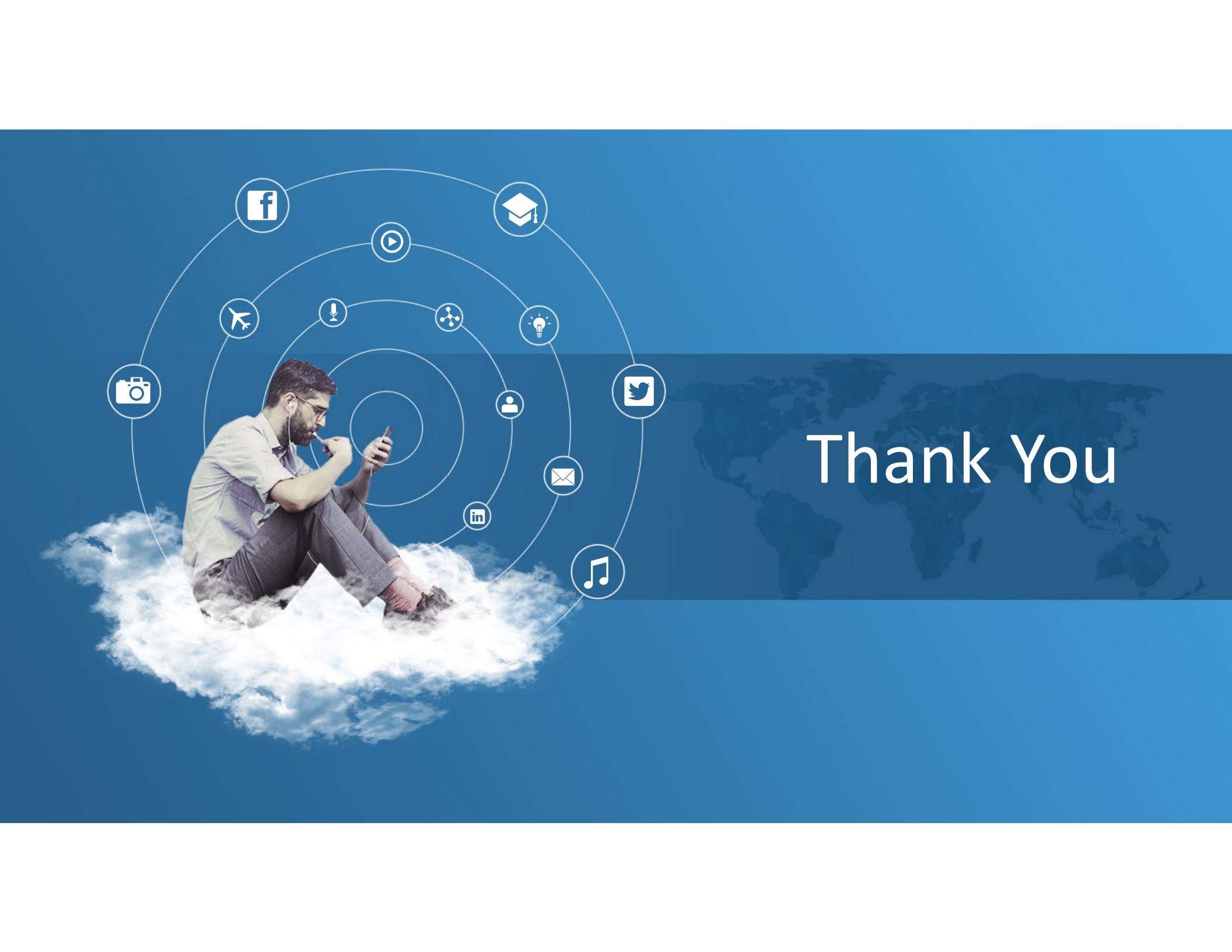
End of presentation





Any Questions ?

“



Thank You

A close-up photograph of a person's hands and torso. The person is wearing a dark grey or black suit jacket over a light-colored shirt. They are holding a silver smartphone in their right hand, which is positioned towards the bottom right of the frame. The background is a solid blue color.

Break

