Microsoft Azure Administrator Associate Training(AZ-103) Module 6

Agenda

01 Identity And Access Management in Azure

02 What is Access management?

03 Role based Access Control

04 Hands-on: Create a Custom Role

05 Role Assignment

06 Hands-On: Assigning Roles

07 What is Azure Active Directory?

08 Windows AD Vs. Azure AD

09 What is Service Audience?

10 Terminologies in Azure Active Directory

11 Hands-On: Add or Delete Users

12 Hands-On: Create groups and add members

Agenda

13 Hands-On: Adding a Custom domain

14 Identity Solution for Hybrid Environments

15 What is Azure AD Connect?

16 Features of Azure AD Connect

17 Self Service Password Reset

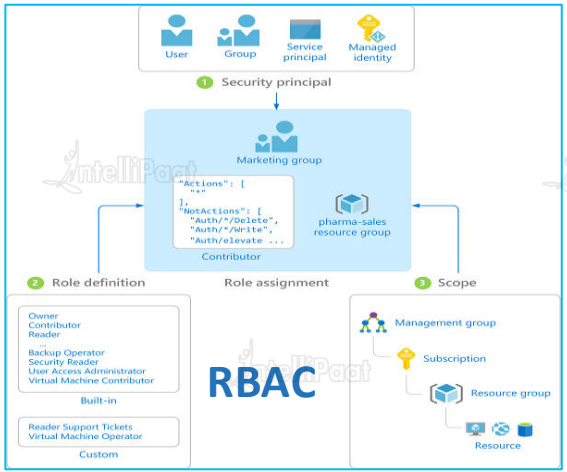
18 Hands-On: Enable self service password reset

19 Multi-factor Authentication

20 Quiz

Identity And Access Management in Azure

Azure not only offers identity and access management for Azure cloud but also for hybrid environments.



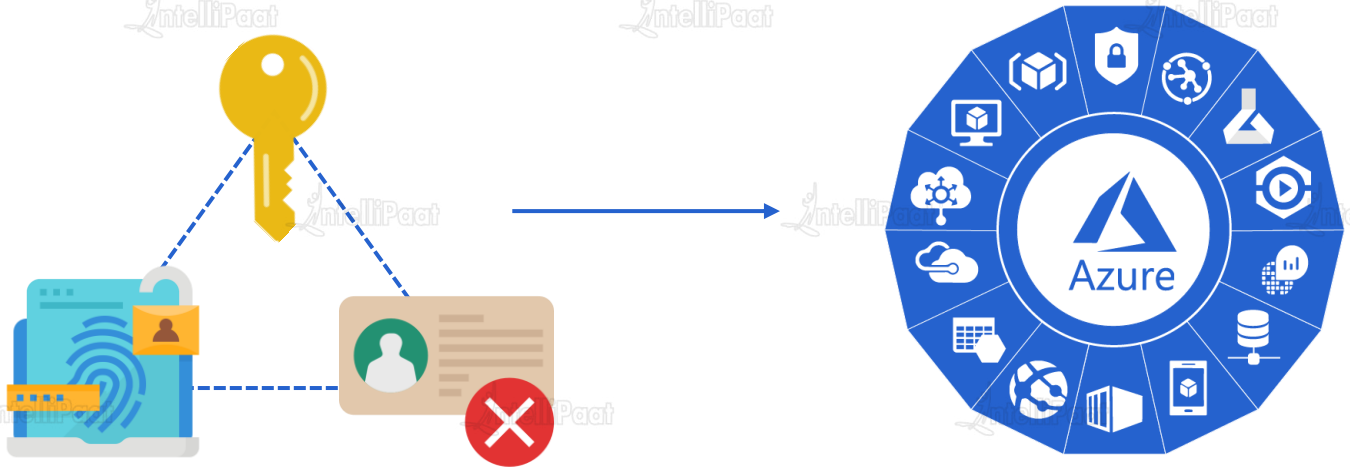
Access Control

Identity management

What Is Access management in Azure?

What is Access management in Azure?

Access management in Azure refers to the process that allows, denies or restricts access to Azure services or resources. It also includes, deciding who gets access and up to what extent, in Azure cloud.

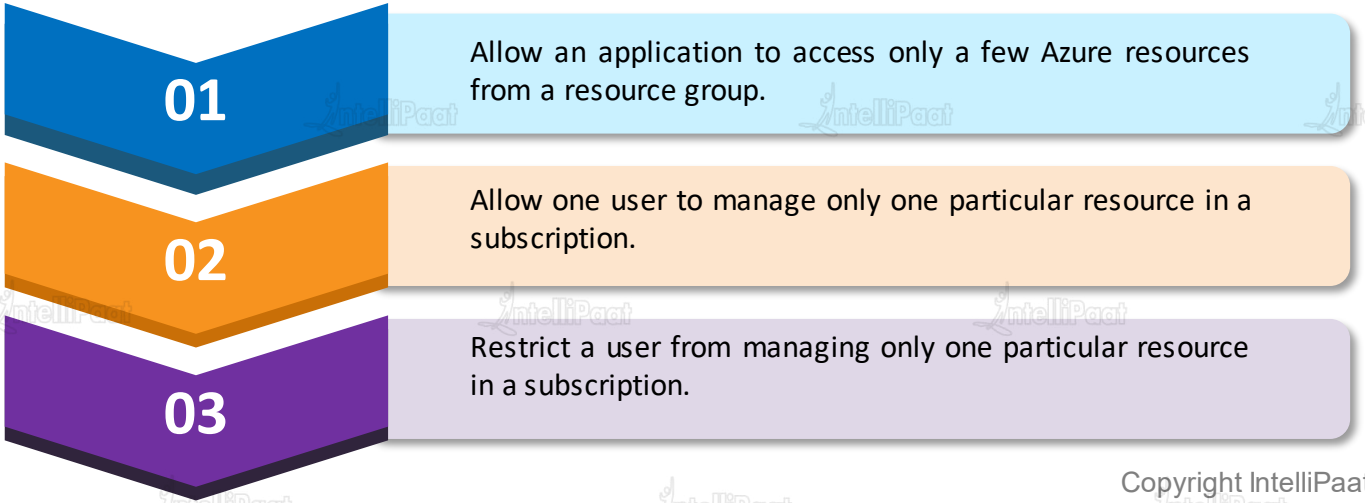


Role based Access Control

What is RBAC?

Azure employs role based access control (RBAC) method for access management in Azure cloud. RBAC is used to manage who (user) has access to Azure resources.

RBAC works by creating and assigning roles and then enforcing permissions on those roles.
You can use RBAC to:



Built-in Roles in Azure

RBAC can be used to create custom roles with permissions of our choice. There are some built-in roles in Azure with pre-defined permissions that can assigned and used.

01	02	03	04
Owner	**Contributor**	**Reader**	**User Access Administrator**
Has full access to all resources including the right to delegate access to others.	Can create and manage all types of Azure resources but can't grant access to others.	Can view existing Azure resources.	Lets you manage user access to Azure resources.

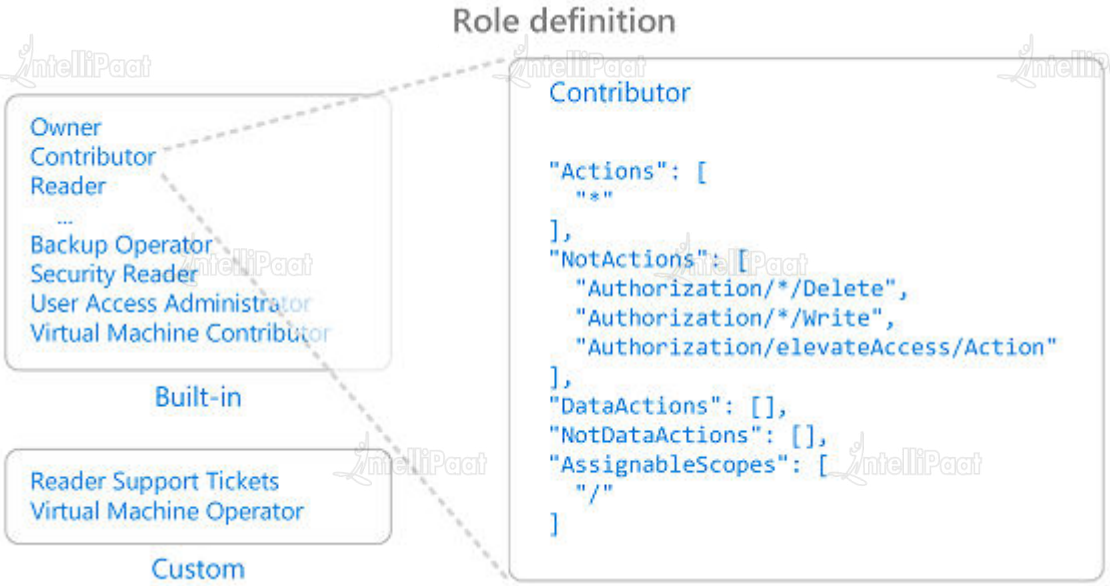
Built-in Roles in Azure

Apart from these built in roles, Azure also offers some resource specific built-in roles that can be used to perform actions on particular resources and not on other resources.

01	02	03	04
Owner	**Contributor**	**Reader**	**User Access Administrator**
Has full access to all resources including the right to delegate access to others.	Can create and manage all types of Azure resources but can't grant access to others.	Can view existing Azure resources.	Lets you manage user access to Azure resources.

What are Role Definitions?

A role definition is a collection of permissions. A role definition lists the operations that can be performed, such as read, write, and delete. It can also list the operations that can't be performed or operations related to underlying data.



Hands-On: Create a Custom role

Role Assignment

Roles assignment essentially comprises of three elements, namely, security principal, role & role definition and finally a scope.

Security principal

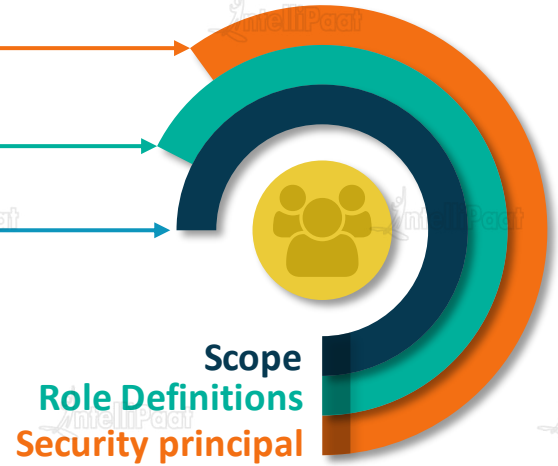
A user, group, service principal or a managed identity that is requesting access to Azure resources is called security principal.

Role Definitions

A set of permissions and operations that can or cannot be performed.

Scope

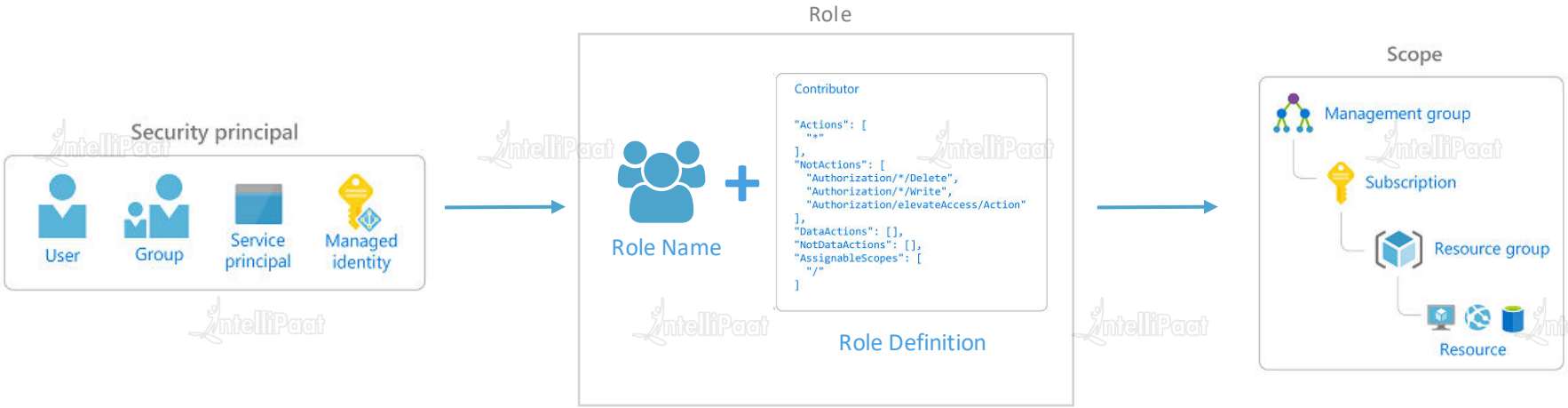
Scope is the set of resources that the access is applied to. You can specify a scope at multiple levels, like, management group, subscription, resource group, or resource.



Role Assignment

A role assignment is the process of attaching a role containing a role definition to a user, group, service principal, or managed identity at a particular scope for the purpose of granting access.

Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

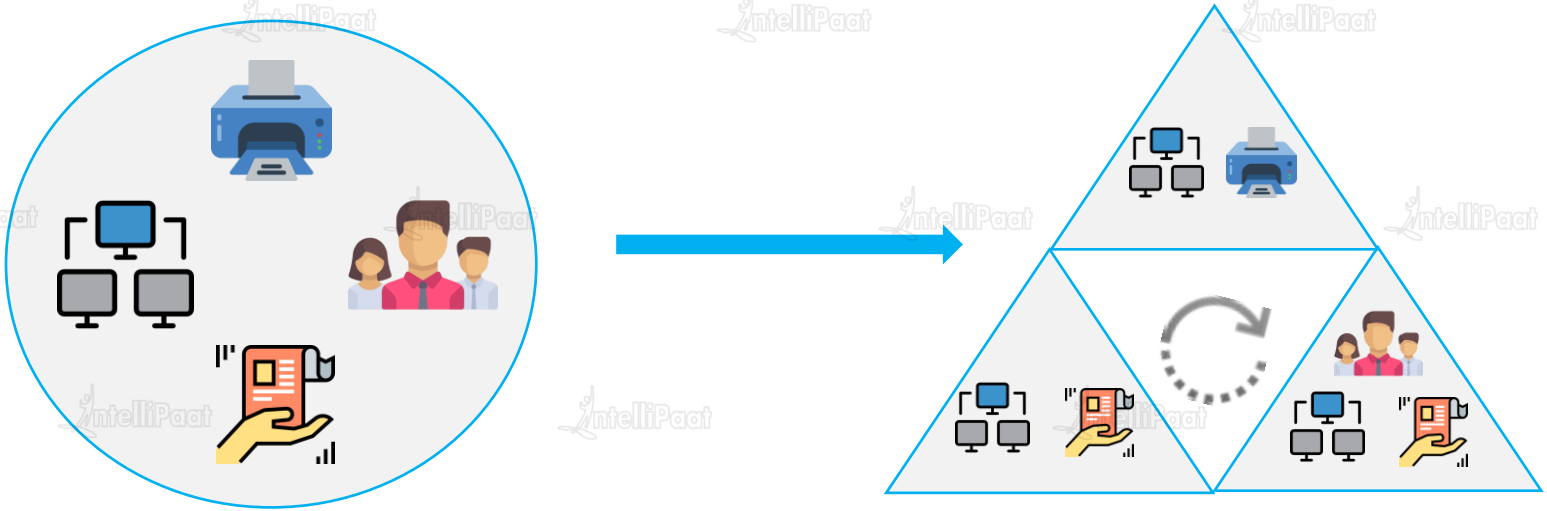


Hands-On: Configure access to Azure resources by assigning roles

Identity Management & Azure Active Directory

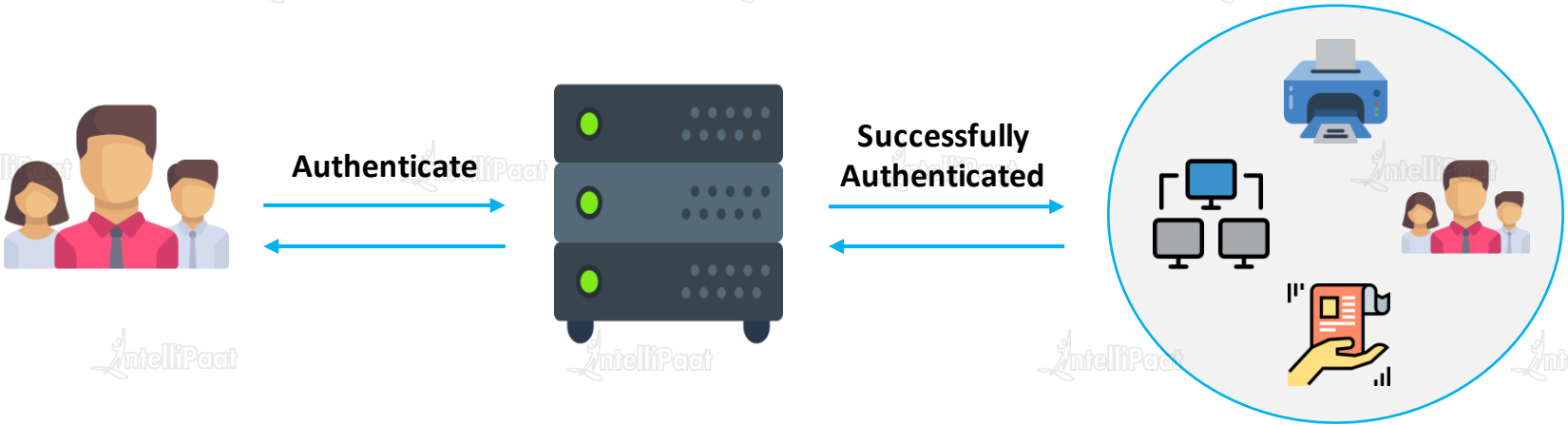
What is Active Directory?

Active directory is used to store and organize information about various elements of an organization's network such as computers, users, resources like printers, shared files or folders.



What is Active Directory?

Active directory information can be used to authenticate and authorize the users, computers, resources that are part of the organization's network.



What is Azure Active Directory?

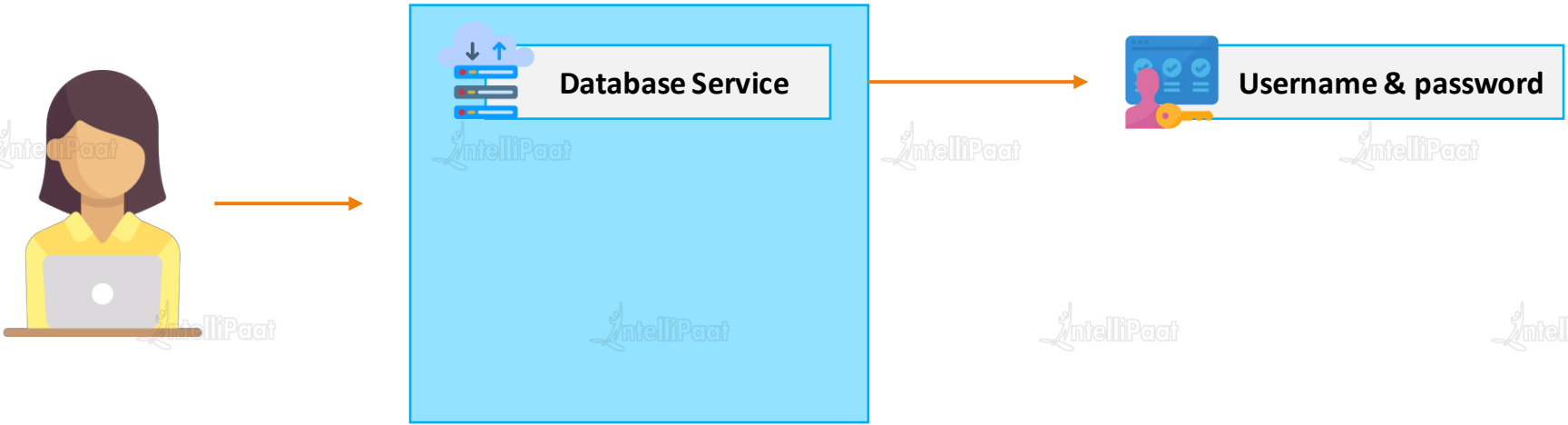
Azure Active directory (Azure AD) is the identity management solution for Azure. It is a live directory or a database that stores user accounts and their passwords, computers, files shares, security groups, permissions and so much more.

What is Azure Active Directory?

Azure active directory is Microsoft's multi tenant, identity solution for Azure. Azure AD is a one stop solution for core directory services for cloud, application access management and identity authentication.

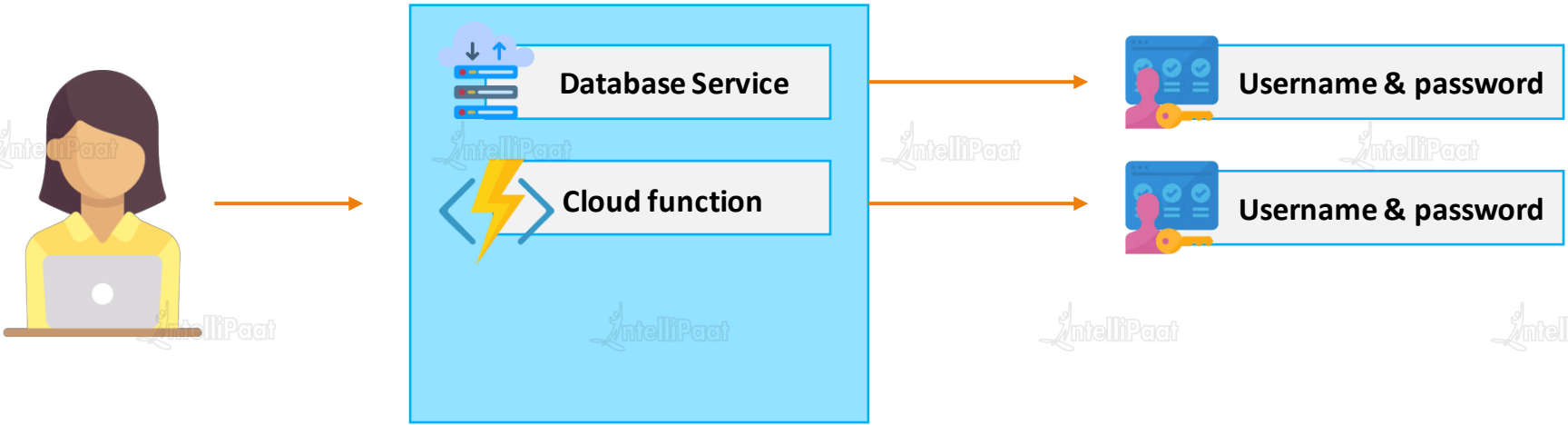
Before Azure Active Directory?

For any service that you might want to use, you are given a set of username and password, using which you can access that particular service for which the username and password is created.



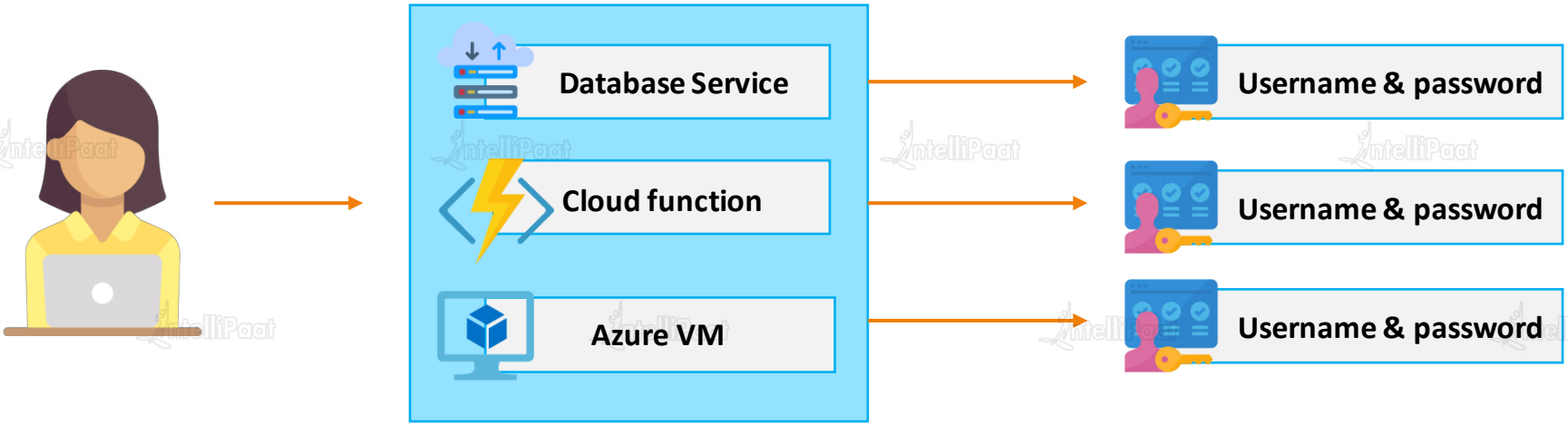
Before Azure Active Directory?

For any service that you might want to use, you are given a set of username and password, using which you can access that particular service for which the username and password is created.



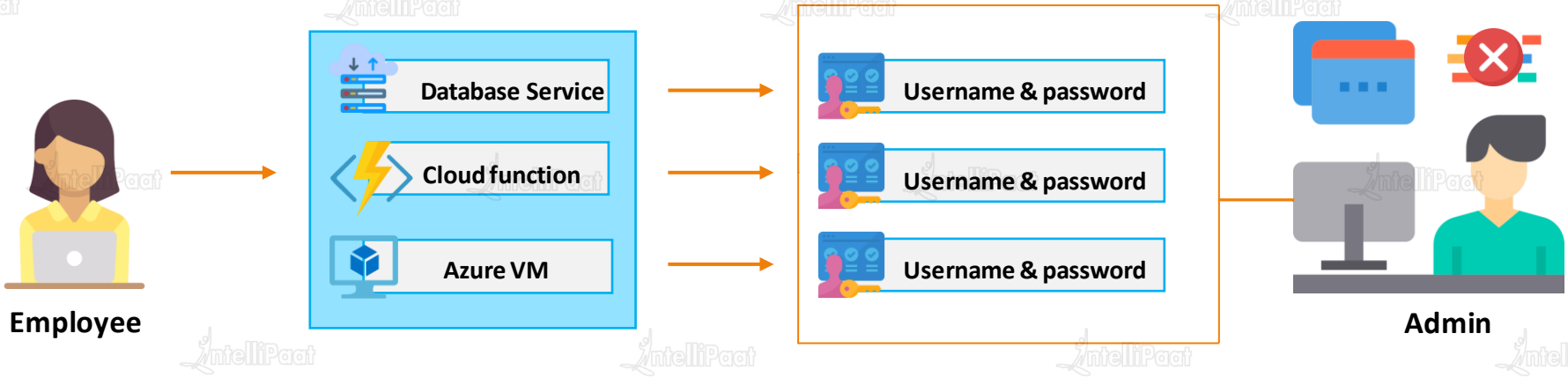
Before Azure Active Directory?

For any service that you might want to use, you are given a set of username and password, using which you can access that particular service for which the username and password is created.



Before Azure Active Directory?

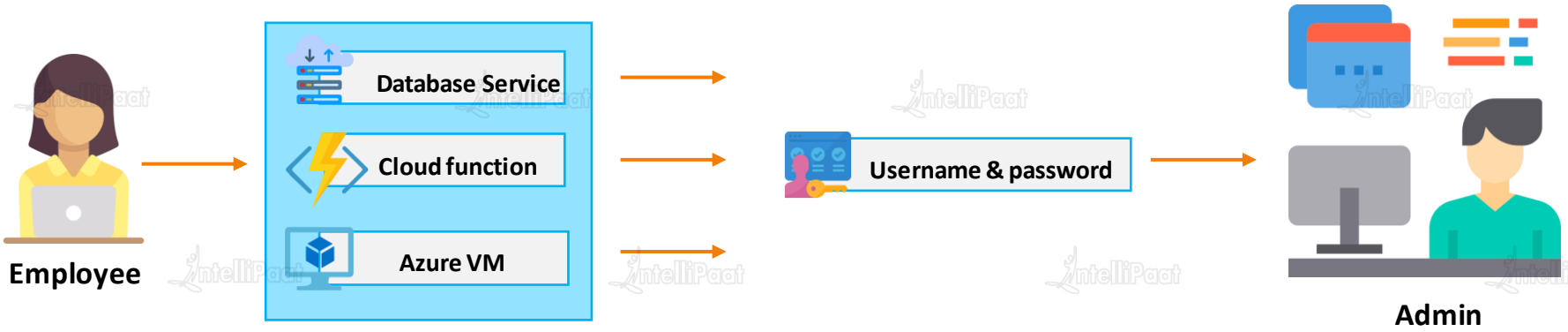
For any service that you might want to use, you are given a set of username and password, using which you can access that particular service for which the username and password is created.



After Azure Active Directory?

For any service that you might want to use, you are given a single set of username and password, using which you can access any service that you want, as long as the admin has given you the permission.

Azure Active directory provides single sign on feature

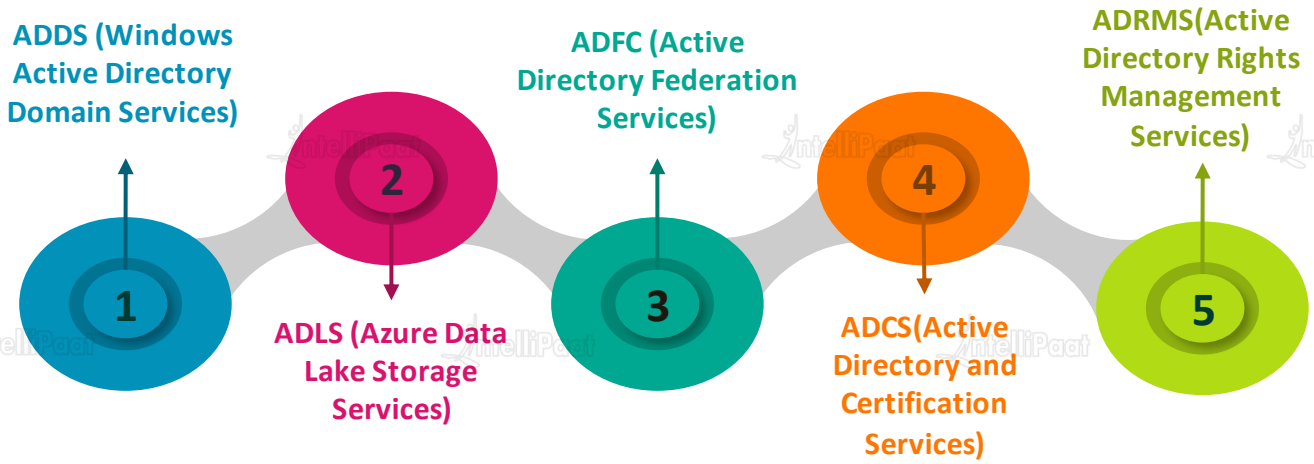


Windows AD Vs. Azure AD

What is Windows Active Directory?

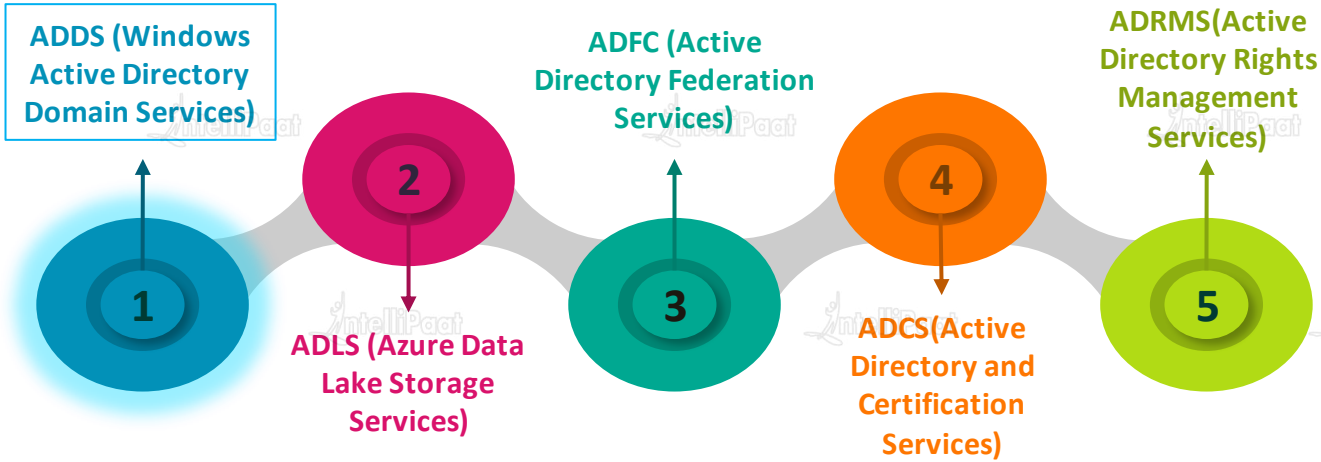
Windows Active directory is a windows OS directory service that offers a single interface for organizing and maintaining information about the organization's network.

Windows Active directory works on different layers. Each layer to perform different tasks



What is Windows Active Directory?

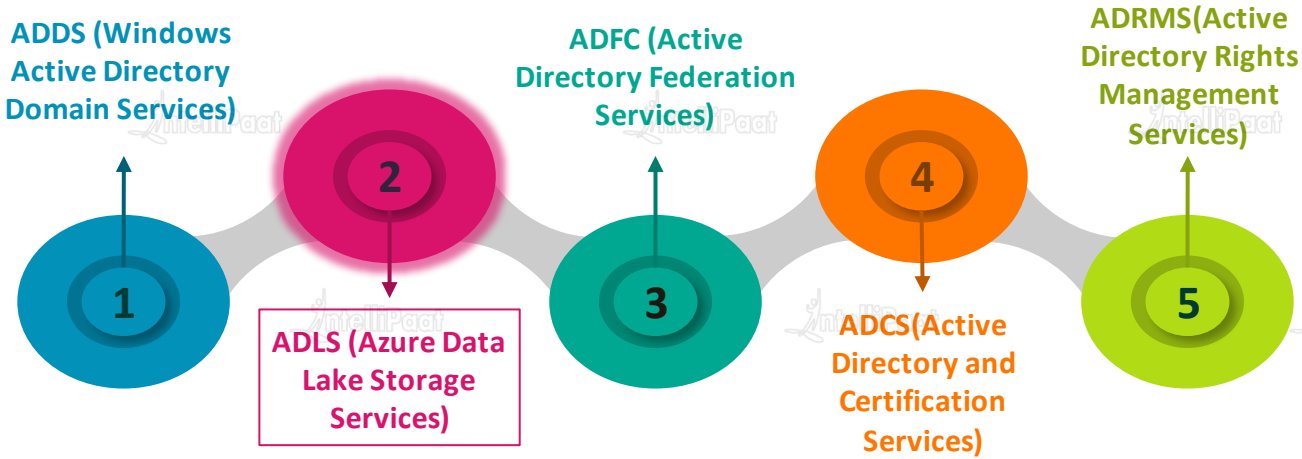
Windows Active directory works on different layers. Each layer to perform different tasks



This layer allows admins to manage and monitor the information related to user logins.

What is Windows Active Directory?

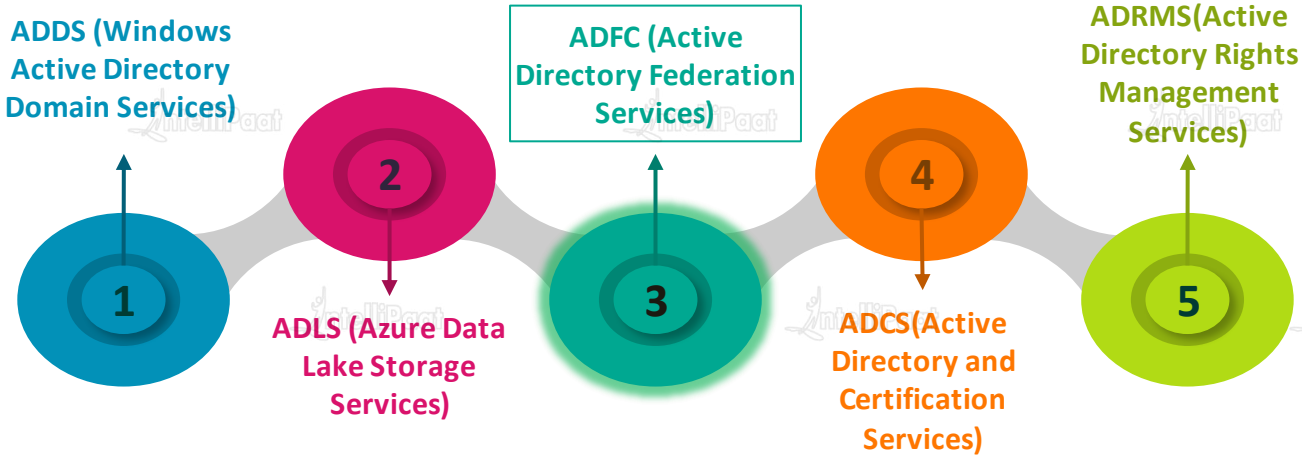
Windows Active directory works on different layers. Each layer to perform different tasks



This layer allows the admin the store any amount of data of any type and size.

What is Windows Active Directory?

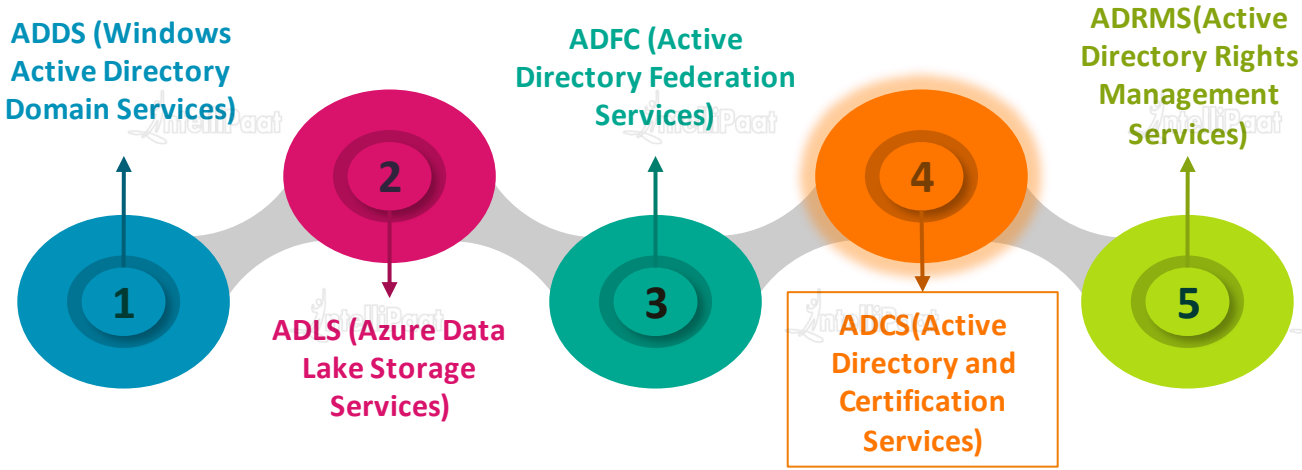
Windows Active directory works on different layers. Each layer to perform different tasks



ADFS layer allows you to have single sign-on access to systems and applications within the organization's network.

What is Windows Active Directory?

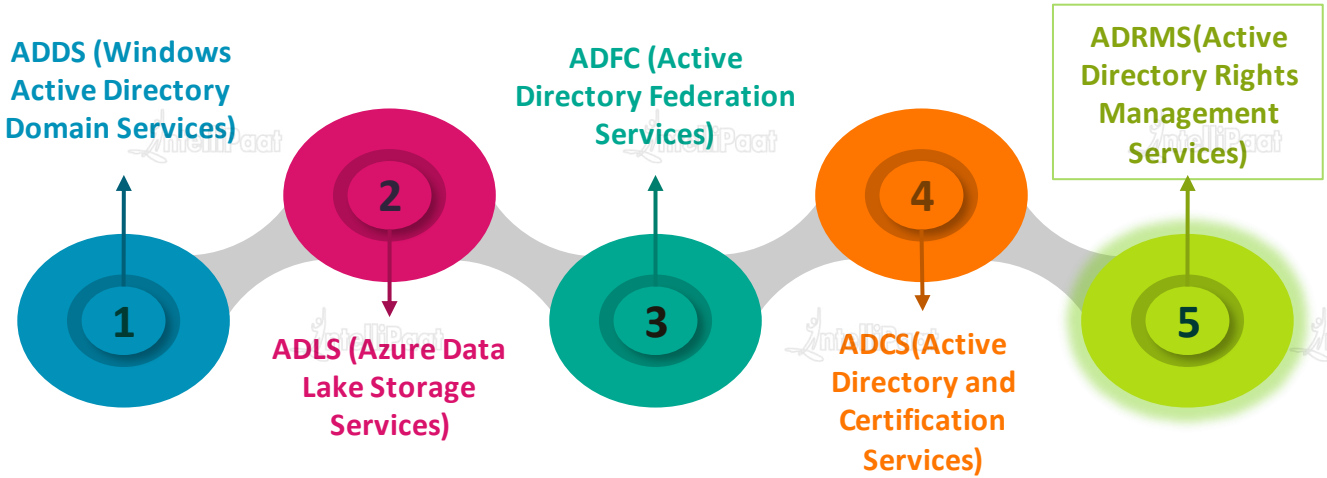
Windows Active directory works on different layers. Each layer to perform different tasks



This layers enables admins to customize services in order to issue and manage public certificates

What is Windows Active Directory?

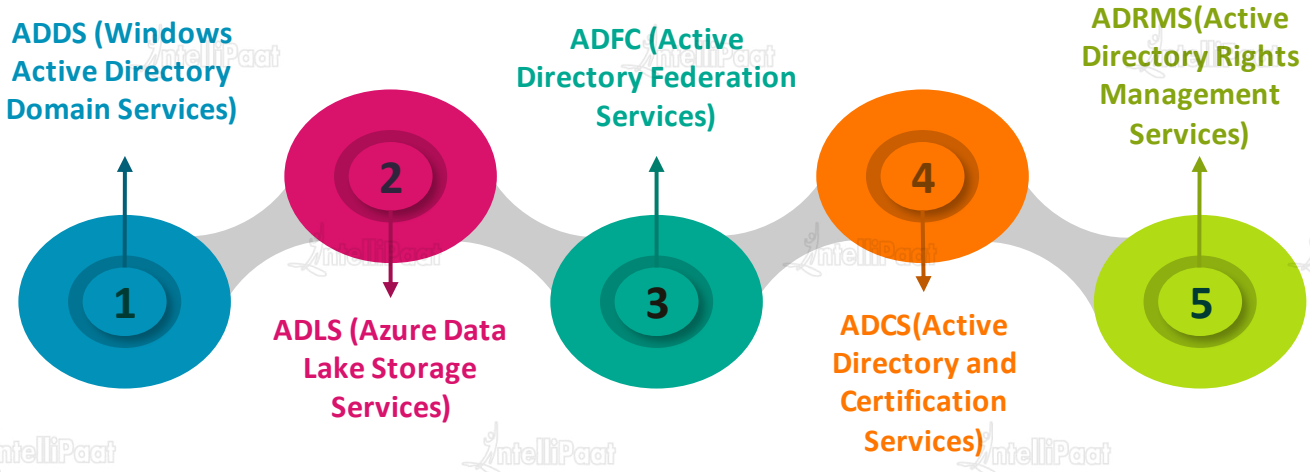
Windows Active directory works on different layers. Each layer to perform different tasks



ADRMS layer is used for data protection.

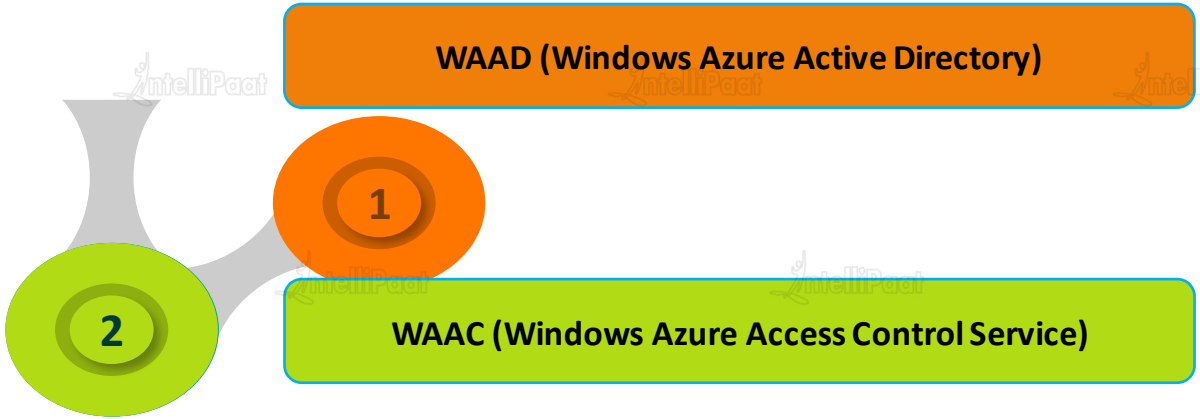
Windows AD Vs. Azure AD

Azure Active directory merged all these layers into just two layers.



Windows AD Vs. Azure AD

Azure Active directory merged all these layers into just two layers.



Service Audience

Service Audience

IT Administrator

- IT administrator will be responsible for all sign-ups and sign-ins.
- Provide relevant authentication and permissions to customers or users
- Resolve authentication issues

Application Developer

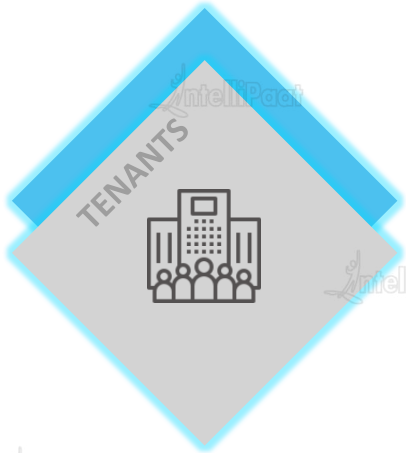
Developers get easy and hassle free access to the relevant services to develop applications

Online Customers

Online customers can access services such as office 365 and other CRM services with their Azure active directory credentials.

Terminologies in Azure Active Directory

Terminologies in Azure Active Directory



TENANTS

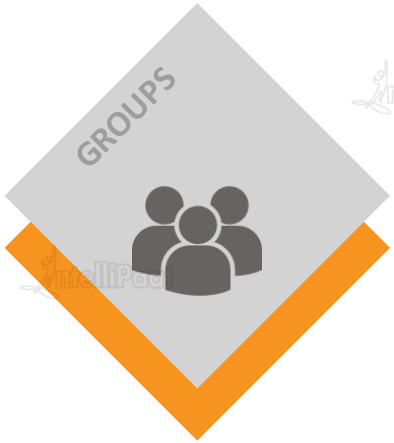
Tenant is an organization. Microsoft ensures that all the tenants or the organizations using Microsoft Cloud services stay isolated and separated, in order to maintain their services separately.

DOMAINS

A domain is a DNS zone for which the tenant has proven ownership. Each tenant has a core domain (onmicrosoft.com)

USER

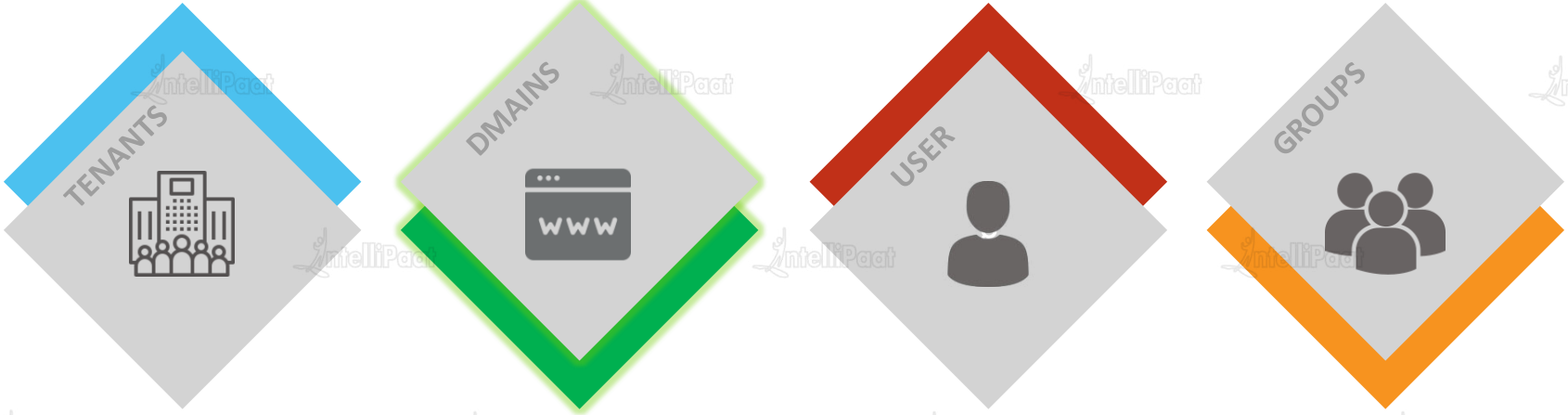
Users are the individuals that are given permission and set of username and password to access and use certain services



GROUPS

Groups are the logical group of users. Groups are created to organize the users or devices on the basis of geographic location, department, types of services or hardware characteristics.

Terminologies in Azure Active Directory



TENANTS

Tenant is an organization. Microsoft ensures that all the tenants or the organizations using Microsoft Cloud services stay isolated and separated, in order to maintain their services separately.

DOMAINS

A domain is a DNS zone for which the tenant has proven ownership. Each tenant has a core domain (onmicrosoft.com)

USER

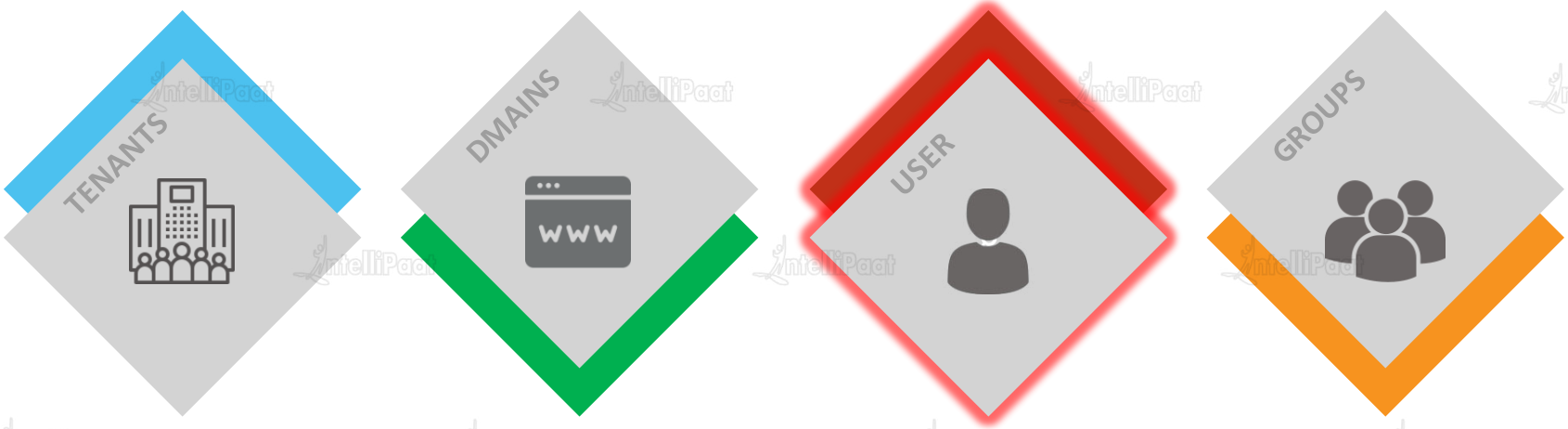
Users are the individuals that are given permission and set of username and password to access and use certain services

GROUPS

Groups are the logical group of users. Groups are created to organize the users or devices on the basis of geographic location, department, types of services or hardware characteristics.

Hands-On: Add a Custom Domain in Azure Active Directory

Terminologies in Azure Active Directory



TENANTS

Tenant is an organization. Microsoft ensures that all the tenants or the organizations using Microsoft Cloud services stay isolated and separated, in order to maintain their services separately.

DOMAINS

A domain is a DNS zone for which the tenant has proven ownership. Each tenant has a core domain (onmicrosoft.com)

USER

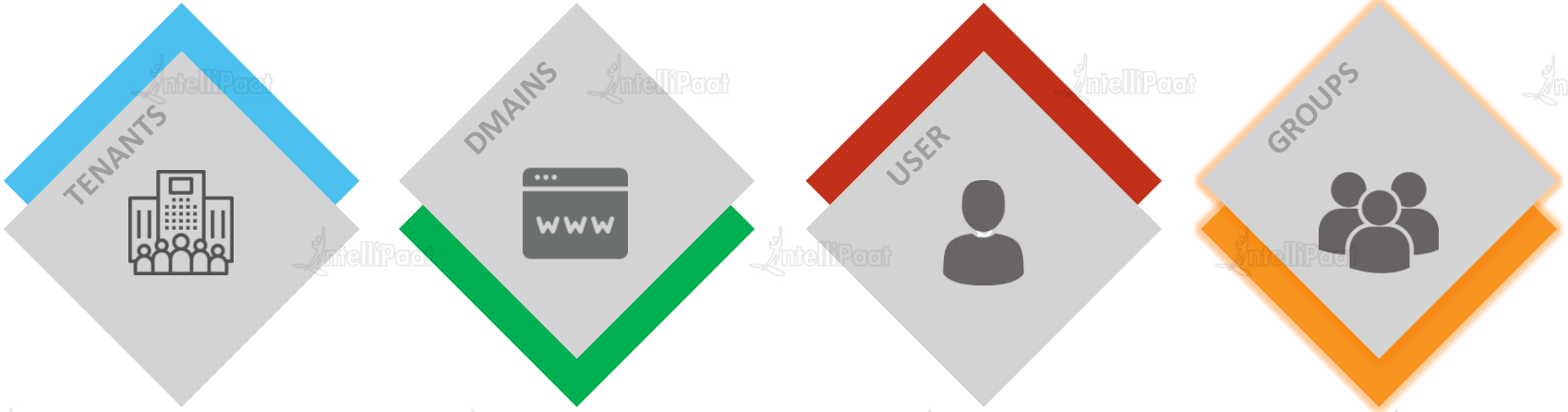
Users are the individuals that are given permission and set of username and password to access and use certain services

GROUPS

Groups are the logical group of users. Groups are created to organize the users or devices on the basis of geographic location, department, types of services or hardware characteristics.

Hands-On: Add or Delete Users using Azure Active Directory

Terminologies in Azure Active Directory



TENANTS

Tenant is an organization. Microsoft ensures that all the tenants or the organizations using Microsoft Cloud services stay isolated and separated, in order to maintain their services separately.

DOMAINS

A domain is a DNS zone for which the tenant has proven ownership. Each tenant has a core domain (onmicrosoft.com)

USER

Users are the individuals that are given permission and set of username and password to access and use certain services

GROUPS

Groups are the logical group of users. Groups are created to organize the users or devices on the basis of geographic location, department, types of services or hardware characteristics.

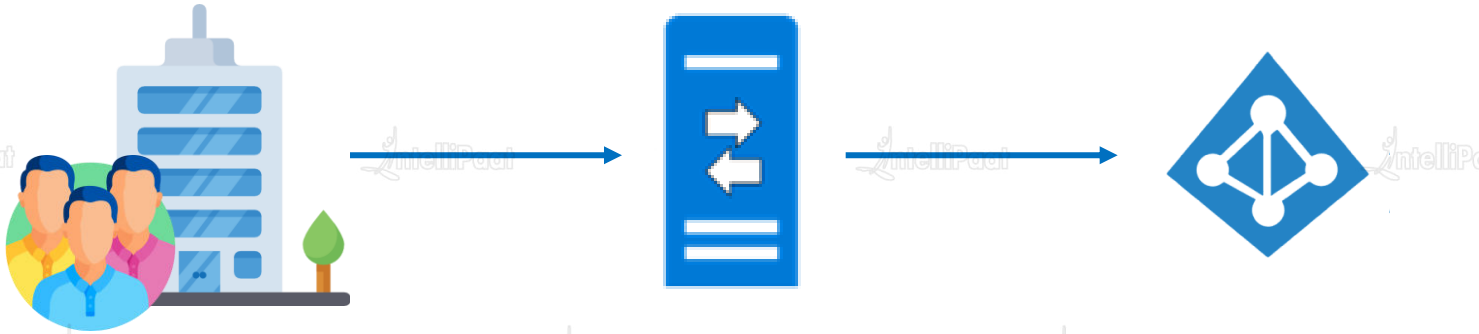
Hands-On: Create groups and Add members using Azure Active Directory

Identity Solution for Hybrid Environments

What is Azure AD Connect?

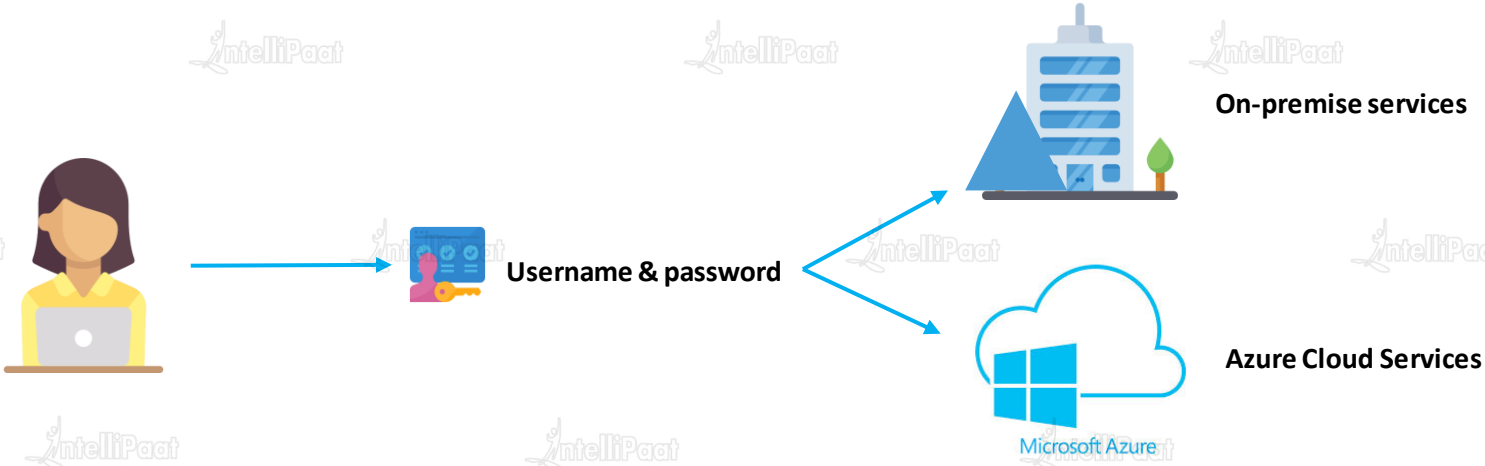
What is Azure AD Connect?

Azure AD Connect is the bridge solution offered by Azure for an organization's on premise Active Directory or identity infrastructure and cloud based Azure Active Directory.



What is Azure AD Connect?

Azure AD Connect is the bridge solution offered by Azure for an organization's on premise Active Directory or identity infrastructure and cloud based Azure Active Directory.

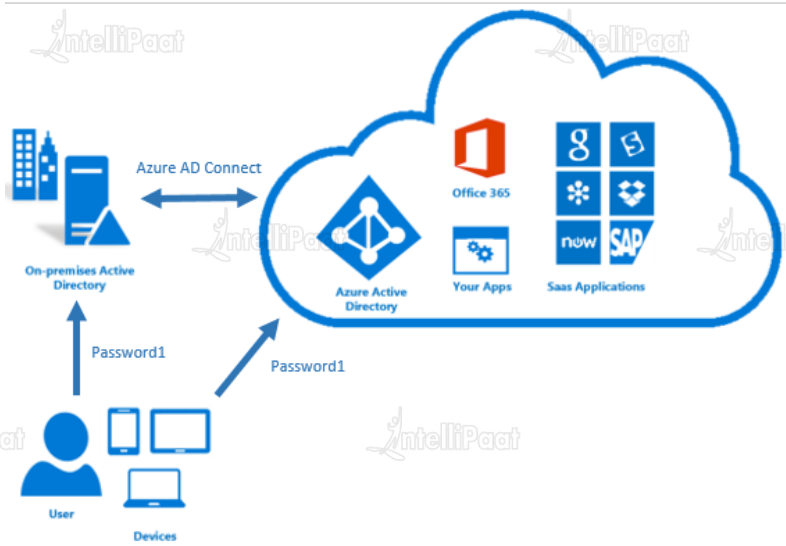


Features of Azure Active Directory Connect

Features of Azure Active Directory Connect

- Password hash synchronization
- Pass-through authentication
- Federation integration
- Synchronization
- Health Monitoring

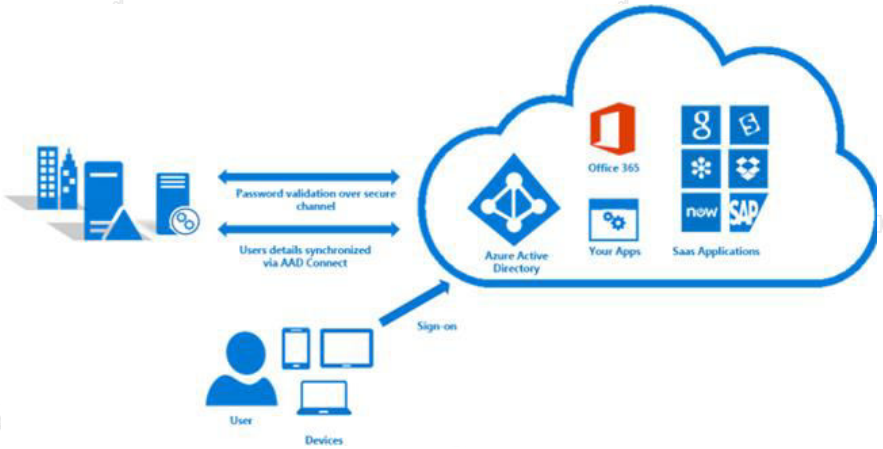
One of the sign-in methods used to accomplish hybrid identity. Azure AD Connect synchronizes a hash, of the hash, of a users password from an on-premises Active Directory instance to a cloud-based Azure AD instance.



Features of Azure Active Directory Connect

- Password hash synchronization
- Pass-through authentication
- Federation integration
- Synchronization
- Health Monitoring

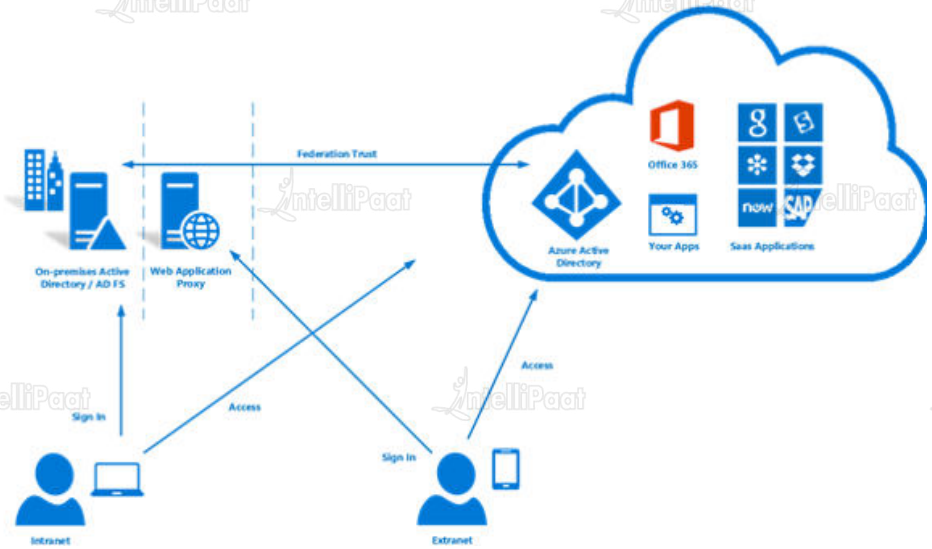
Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.



Features of Azure Active Directory Connect

- Password hash synchronization
- Pass-through authentication
- Federation integration
- Synchronization
- Health Monitoring

Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure.



Features of Azure Active Directory Connect

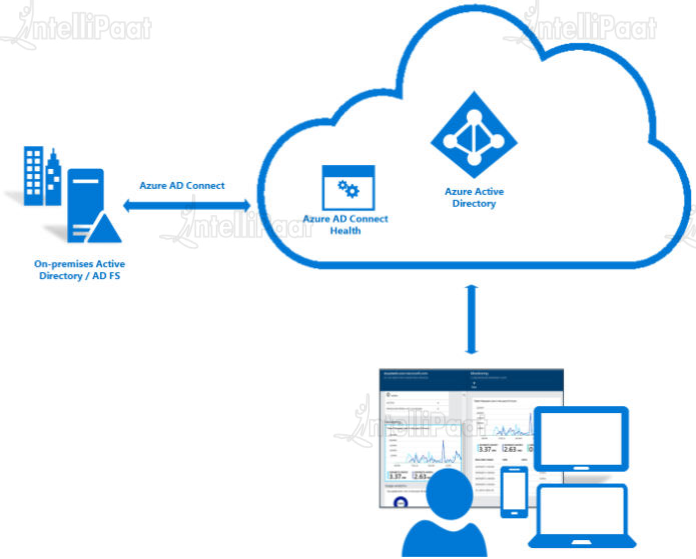
- Password hash synchronization
- Pass-through authentication
- Federation integration
- Synchronization
- Health Monitoring

Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.

Features of Azure Active Directory Connect

- Password hash synchronization
- Pass-through authentication
- Federation integration
- Synchronization
- Health Monitoring

Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.



Implementing Authentication in Azure

- Self Service password Reset
- Multi-factor Authentication

What is Self Service Password Reset

Self Service Password Reset

Self Service password reset(SSPR) offers a means for IT Admins to enable the users to reset or unlock their own passwords or accounts without any IT intervention.

If SSPR is enabled, you must select at least one of the following options/Gates for the authentication methods.

01 Mobile phone

02 Mobile app notification

03 Office phone

04 Email

05 Security questions

06 Mobile app code

Why Self Service Password Reset?

Why Self-Service Password Reset?

Reduces helpdesk Call Volumes and expedites the password reset procedure

Eliminates the drawback of many help desks, that is intruder attack to claim a new password

Ensures that password problems are only resolved after adequate user authentication

Helps users set a password of their own convenience, which later helps them remember their password easily

Hands on: Enable Self Service Password Reset

Multi-factor Authentication

What is Multi-factor Authentication?

Multi factor Authentication combines multiple number of independent credentials to create a layered defense against unauthorized authentication or unauthorized access.

For example, it might use the combination of following credentials:

- what the user knows, that is password
- what the user has, that is security token on a trusted device
- what the user is, that is biometric verification

Username

Password

Quiz

Quiz

1. What is Azure Active Directory?

A. Networking Service offered by Azure

B. Data Warehouse Service offered by Azure

B. Identity and Access management service offered by Azure

D. Another term for Azure subscription

Quiz

2. Which of the following tasks cannot be performed using rbac in Azure?

A. Grant access to an application to access some selected Azure resources from a resource group

B. Grant access to a user to access the whole resource group

B. Restrict a user from accessing the whole subscription

D. None of the above

Quiz

3. Self service password reset feature lets users login without using any authentication credentials. True or False?

A. True

B. False

Quiz

4. Which is the following statements in false?

A. Azure uses Rbac method for access management

B. There can only be one Azure Active directory per account

B. IAM services offered by Azure can only be used on Azure cloud environment and cannot be extended on hybrid environment

D. Azure Active Directory helps achieving SSO

Quiz

5. Multiple subscriptions can trust the same Azure AD directory, but each subscription can only trust a single directory.

A. True

B. False

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

support@intellipaat.com

24/7 Chat with Our Course Advisor