Microsoft Azure Administrator Associate Training(AZ-104)

Module 8

Copyright Intellipaat. All rights reserved.

Agenda

- 01 Identity and Access Management in Azure
- 02 What is Access Management?
- 03 Role-based Access Control
- 04 What is Azure Active Directory?
- 05 Role Assignment
- 06 Windows AD vs Azure AD
- 07 Azure AD Users
- 08 Azure AD Groups
- 09 Azure AD Domains and Tenants
- 10 Terminology in Azure Active Directory
- 11 What is Service Audience?
- 12 Authentication Options

Copyright Intellipaat. All rights reserved.

Agenda

13 Azure AD Connect

14 Self Service Password Reset

15 Multi-factor Authentication

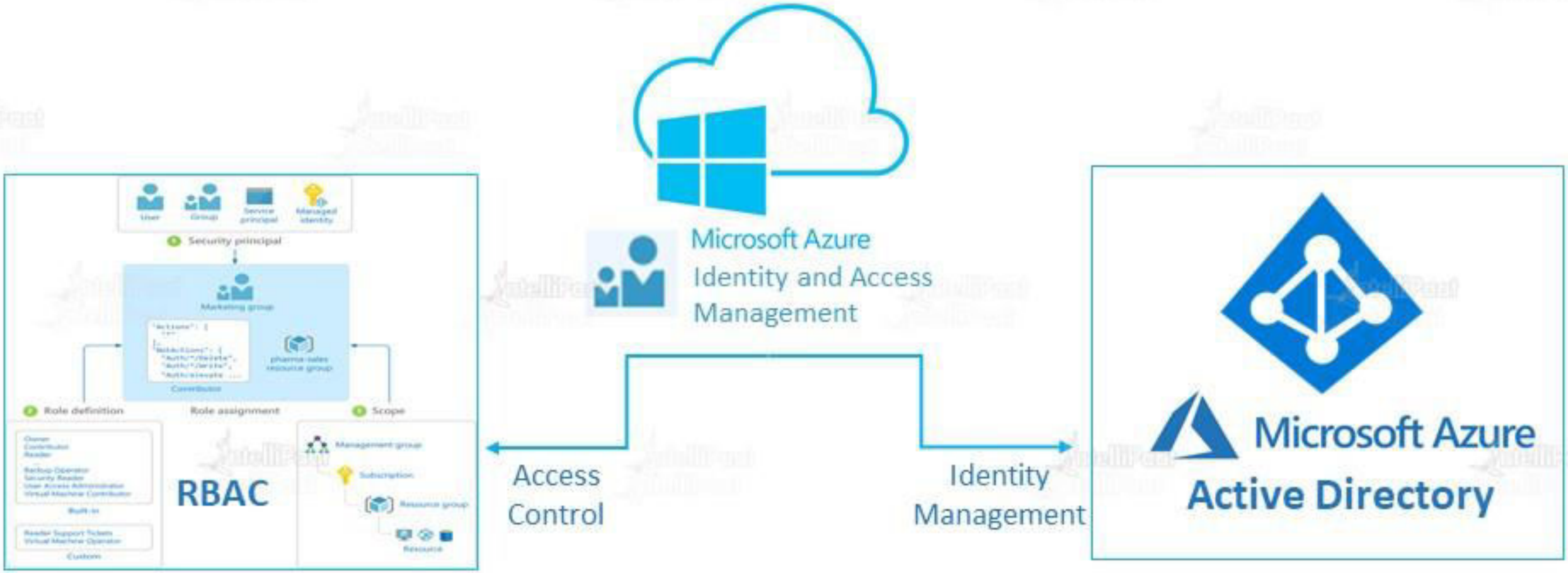
16 Azure Resource Locks

17 Quiz

Copyright Intellipaat. All rights reserved.

Identity and Access Management in Azure

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



RBAC

Microsoft Azure Identity and Access Management

Access Control

Identity Management

Microsoft Azure Active Directory

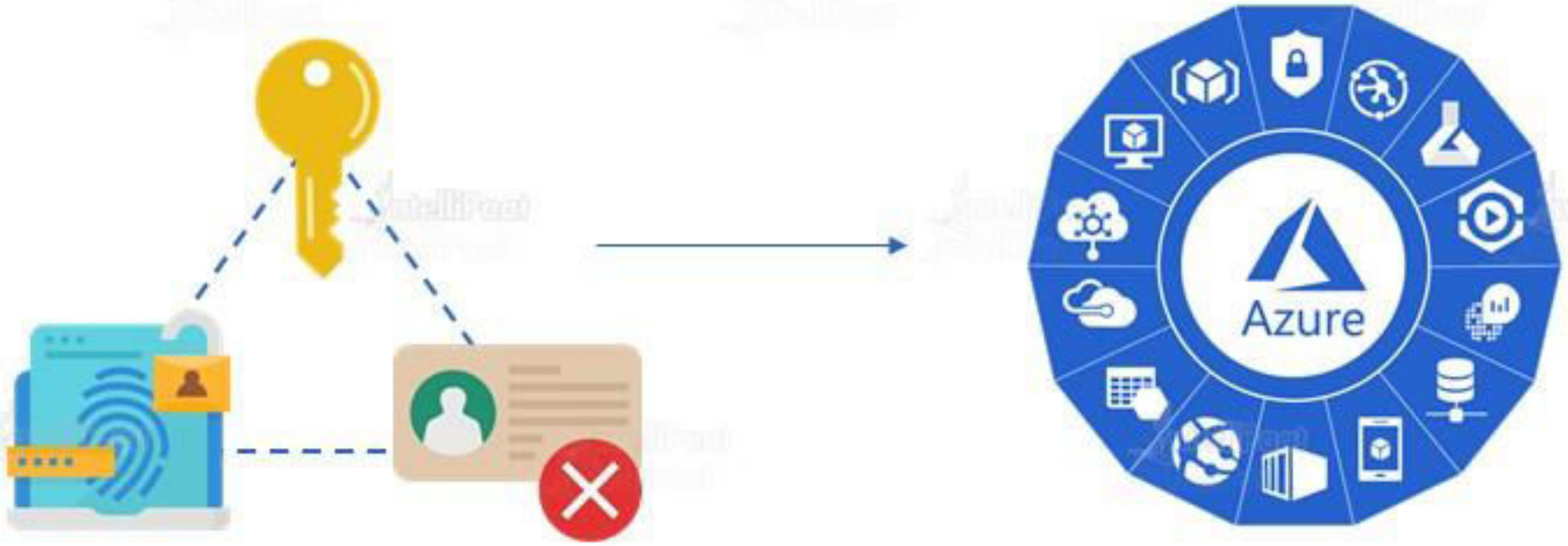
Copyright Intellipaat. All rights reserved.

What is Access Management in Azure?

Copyright Intellipaat. All rights reserved.

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



Copyright Intellipaat. All rights reserved.

Role-based Access Control

Copyright Intellipaat. All rights reserved.

What is RBAC?

Azure employs the 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

We can use RBAC to:

01 Allow an application to access only a few Azure resources from a resource group

02 Allow a user to manage only one particular resource in a subscription

03 Restrict a user from managing a particular resource in a subscription

Copyright Intellipaat. All rights reserved.

Built-in Roles in Azure

RBAC can be used to create custom roles with permissions of our choice. Although, 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 the existing Azure resources	Lets us manage user access to Azure resources

Copyright Intellipaat. All rights reserved.

Built-in Roles in Azure

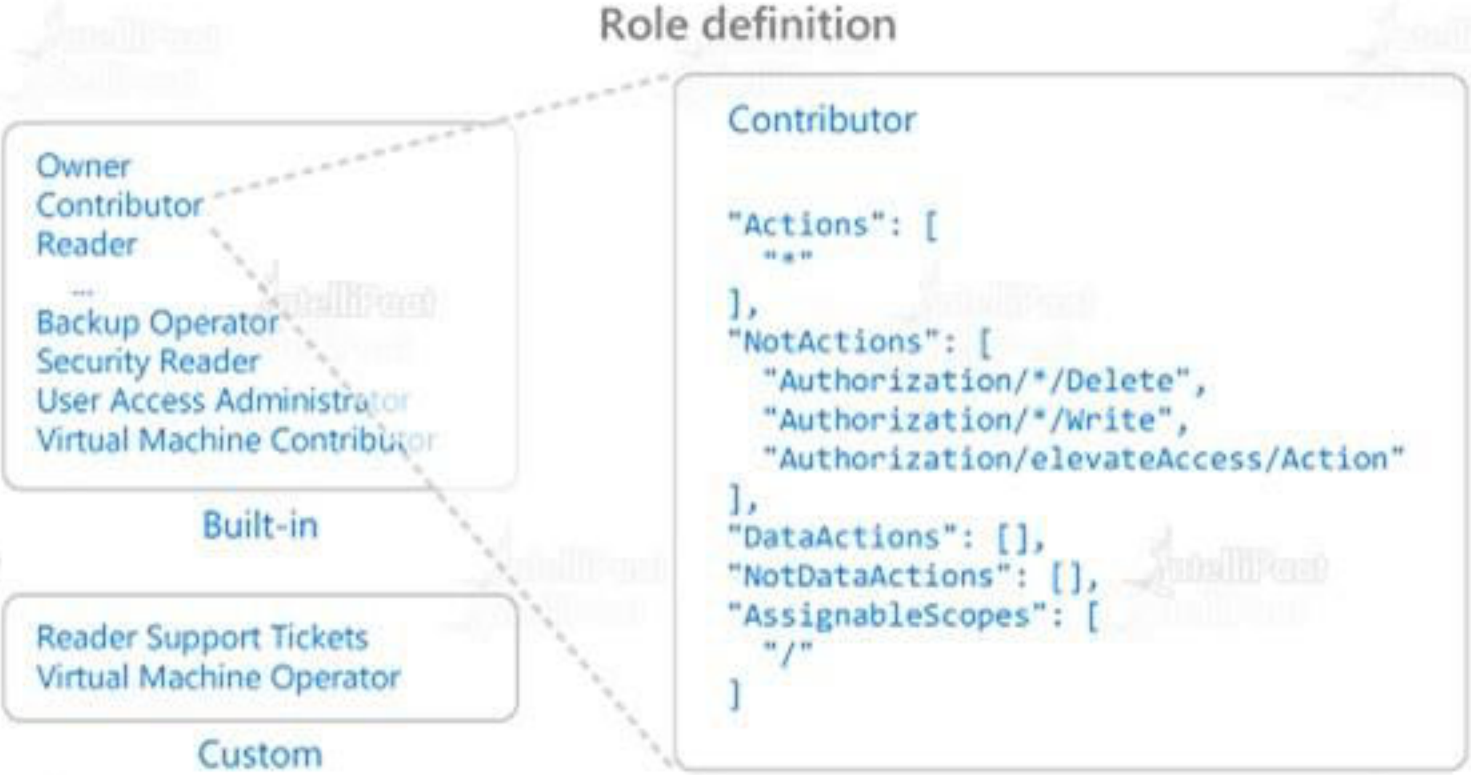
Apart from these built-in roles, Azure also offers some resource-specific built-in roles that can be used to perform actions on particular resources and not on other resources

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 the existing Azure resources	Lets us manage user access to Azure resources

Copyright Intellipaat. All rights reserved.

What are Role Definitions?

A role definition is a collection of permissions. It 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 those operations that are related to underlying data



Role definition

Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

Built-in

Reader Support Tickets
Virtual Machine Operator

Custom

Contributor

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

Copyright Intellipaat. All rights reserved.

Hands-on: Creating a Custom Role

Copyright Intellipaat. All rights reserved.

Hands-on

1. Create a Custom role in Azure AD

2. Assign the role to users, groups or tenants

Copyright Intellipaat. All rights reserved.

Role Assignment

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

Security Principal

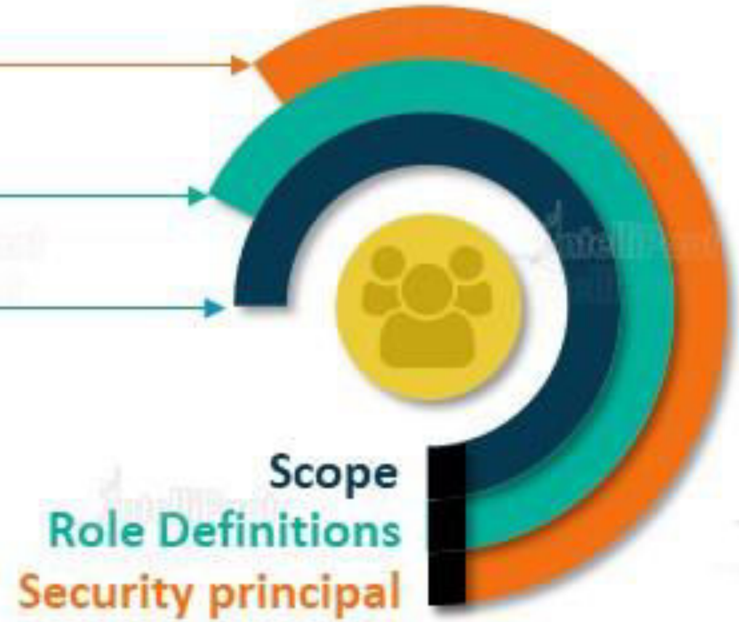
A user, group, service principal, or a managed identity that is requesting access to Azure resources is called a security principal

Role Definitions

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

Scope

It is the set of resources to which access is applied. We can specify a scope at multiple levels, such as management group, subscription, resource group, or resource

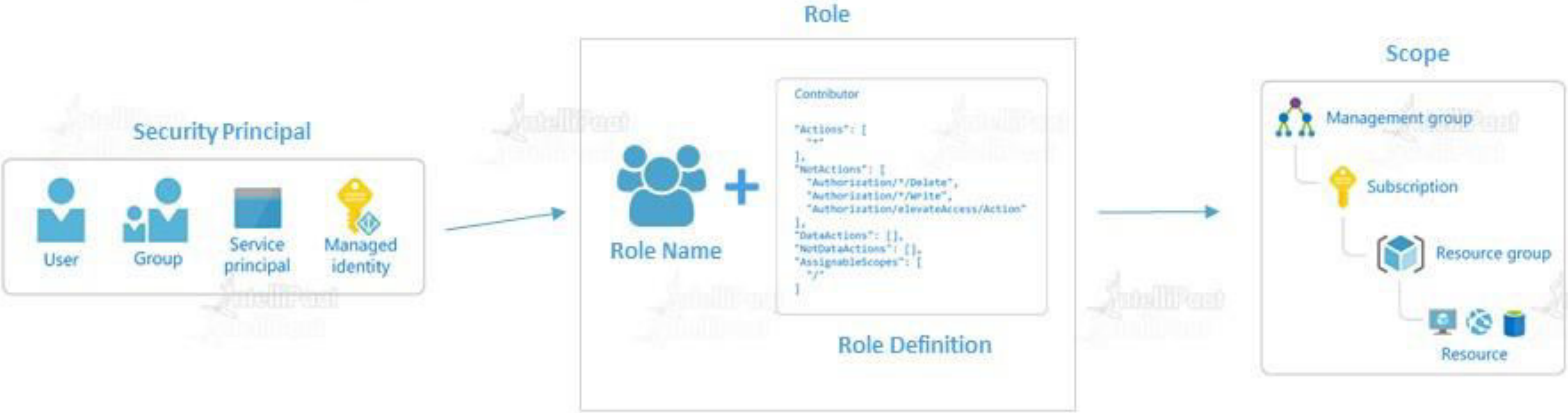


Copyright Intellipaat. All rights reserved.

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 the role assignment



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

Copyright Intellipaat. All rights reserved.

Hands-on: Configuring Access to Azure Resources by Assigning Roles

Copyright Intellipaat. All rights reserved.

Hands-on

1. Assign a custom role to User by creating a Role assignment

2. Check if the role access has been granted

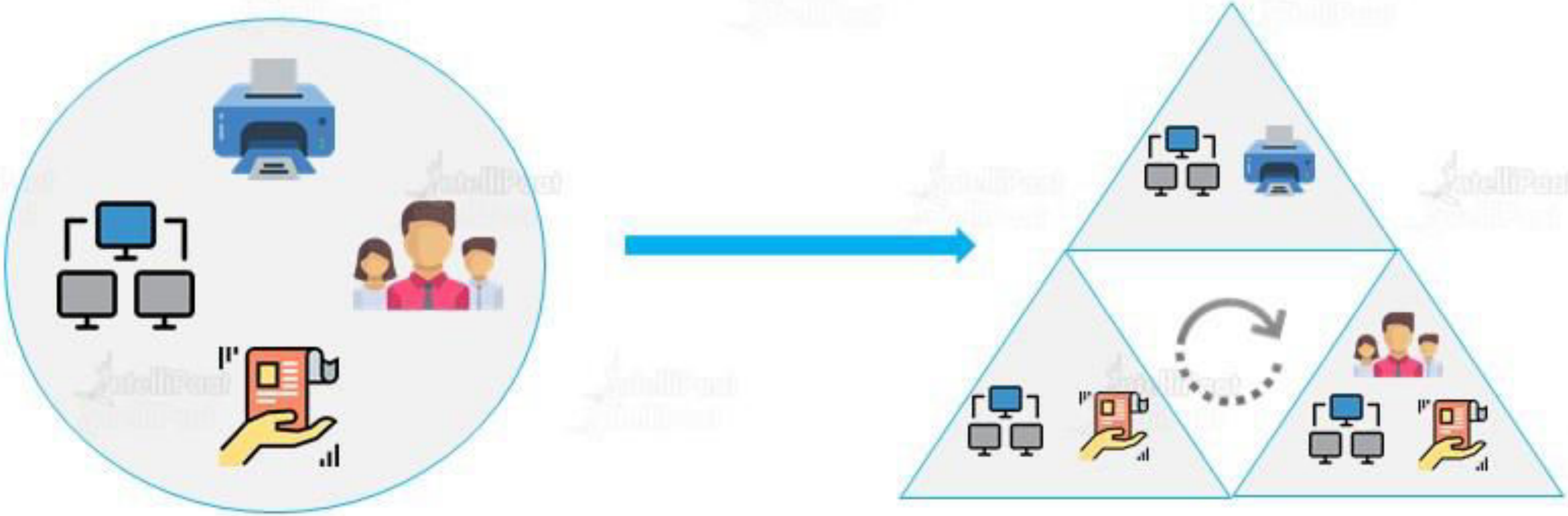
Copyright Intellipaat. All rights reserved.

Identity Management & Azure Active Directory

Copyright Intellipaat. All rights reserved.

What is Active Directory?

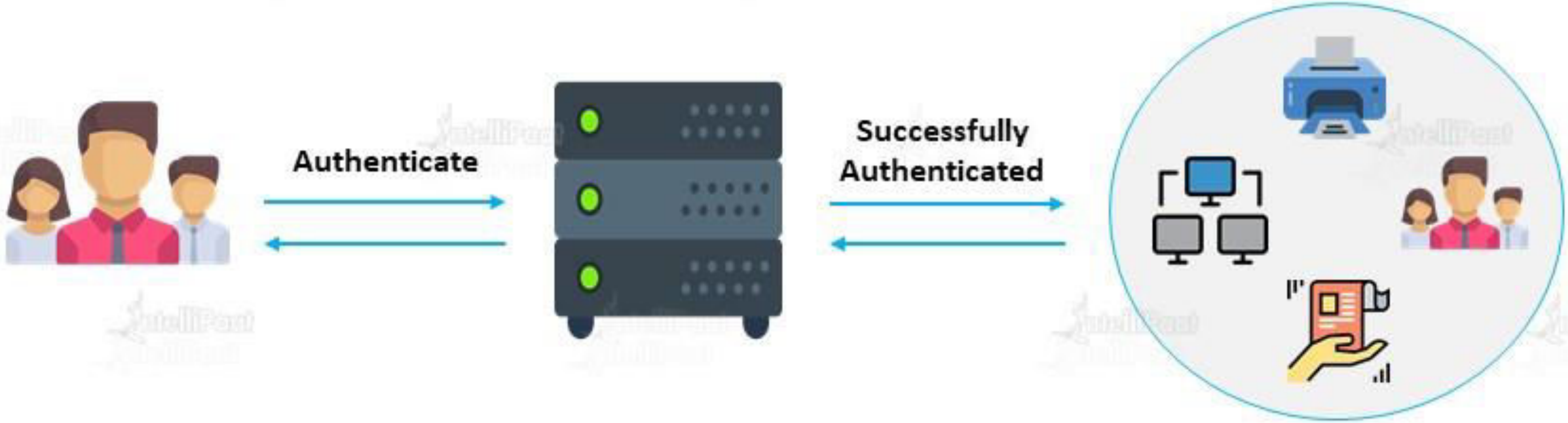
Active Directory is used to store and organize information about various elements of an organization's network such as computers, users, resources such as printers, shared files, or folders



Copyright Intellipaat. All rights reserved.

What is Active Directory?

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



Copyright Intellipaat. All rights reserved.

What is Azure Active Directory?

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

Copyright Intellipaat. All rights reserved.

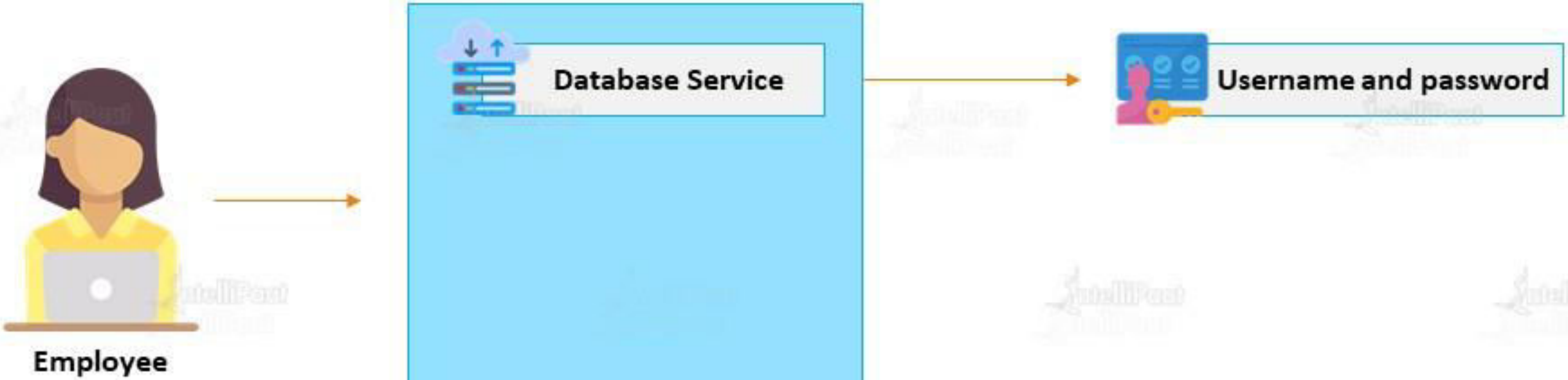
What is Azure Active Directory?

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

Copyright Intellipaat. All rights reserved.

Before Azure Active Directory

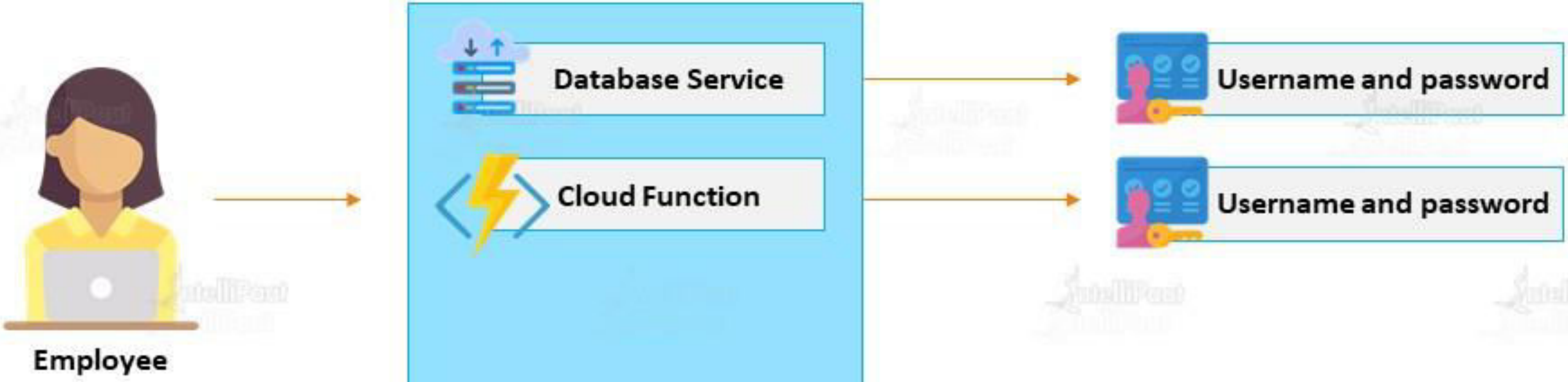
For any service that we want to use, we are given a set of username and password. Using this, we can access the particular service for which the username and password is created



Copyright Intellipaat. All rights reserved.

Before Azure Active Directory

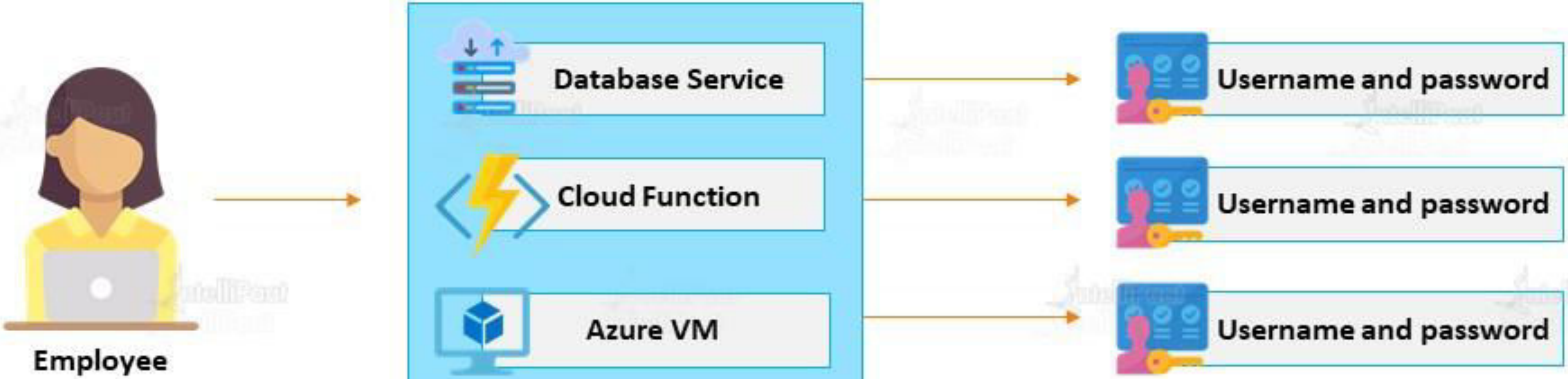
For any service that we want to use, we are given a set of username and password. Using this, we can access the particular service for which the username and password is created



Copyright Intellipaat. All rights reserved.

Before Azure Active Directory

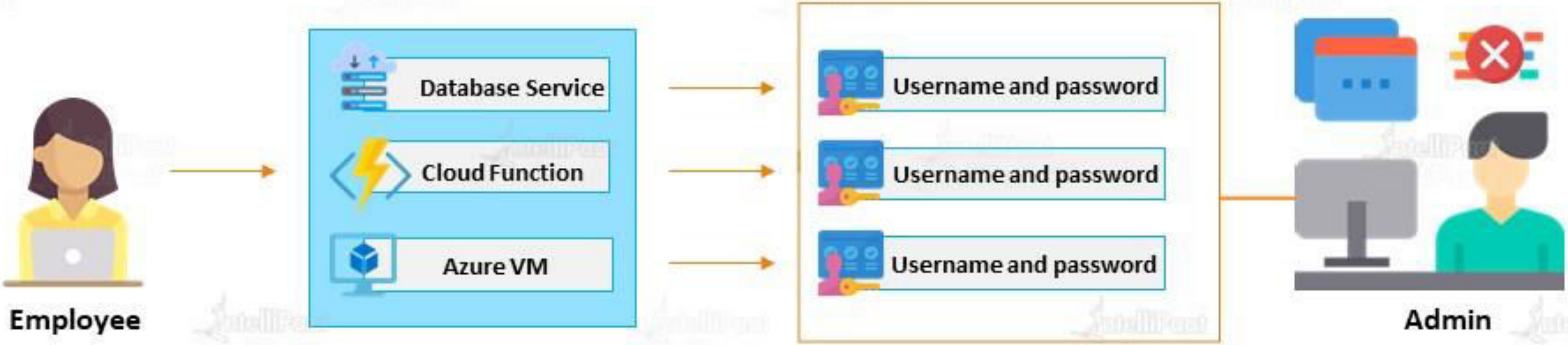
For any service that we want to use, we are given a set of username and password. Using this, we can access the particular service for which the username and password is created



Copyright Intellipaat. All rights reserved.

Before Azure Active Directory

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

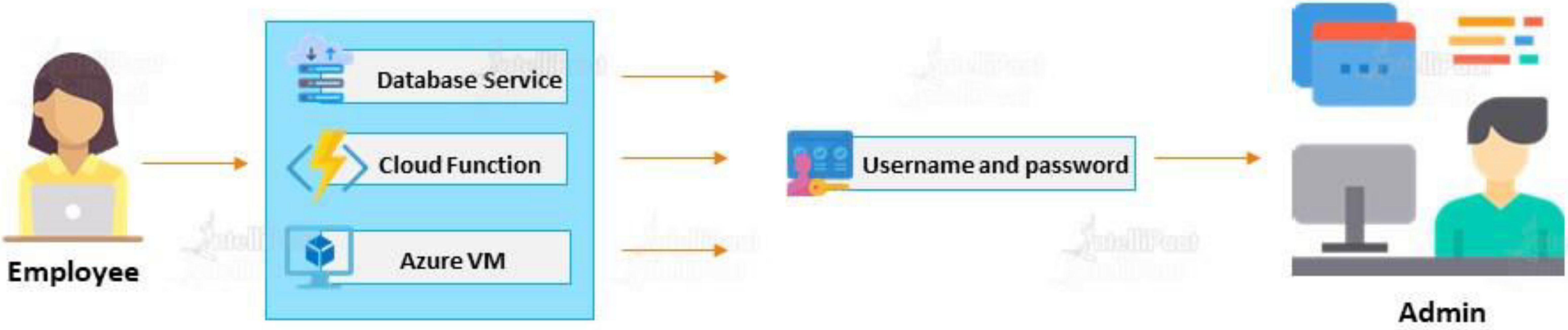


Copyright Intellipaat. All rights reserved.

After Azure Active Directory

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

Azure Active Directory provides the single sign-on feature



Copyright Intellipaat. All rights reserved.

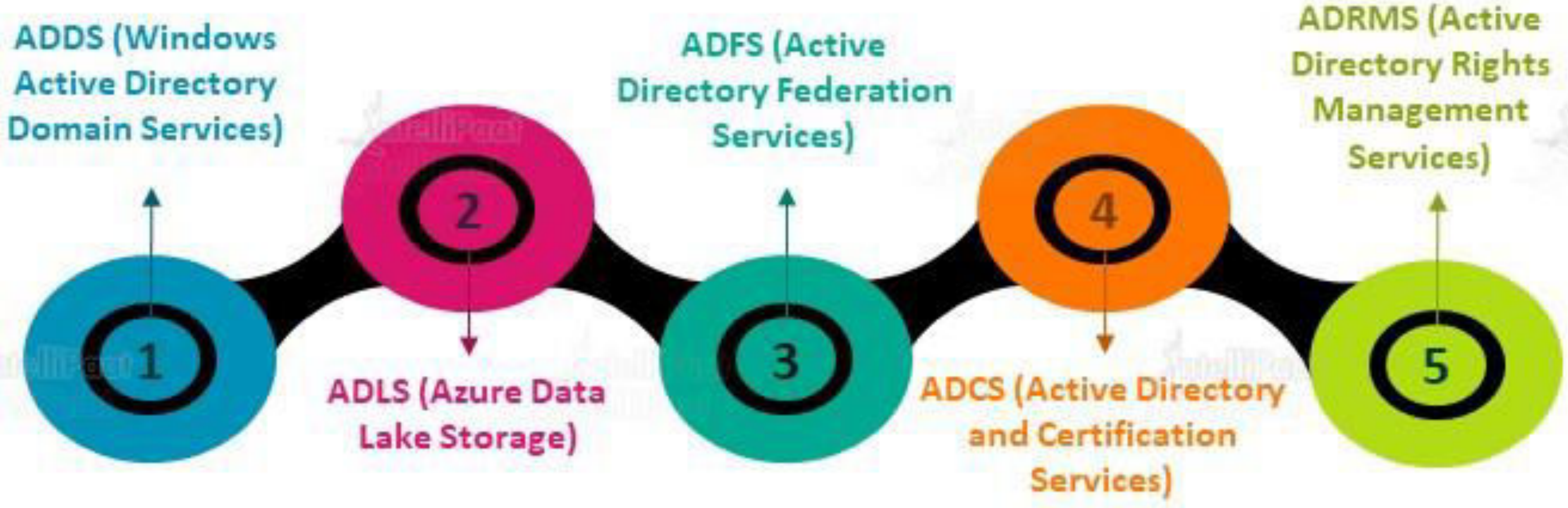
Windows AD vs Azure AD

Copyright Intellipaat. All rights reserved.

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 an organization's network

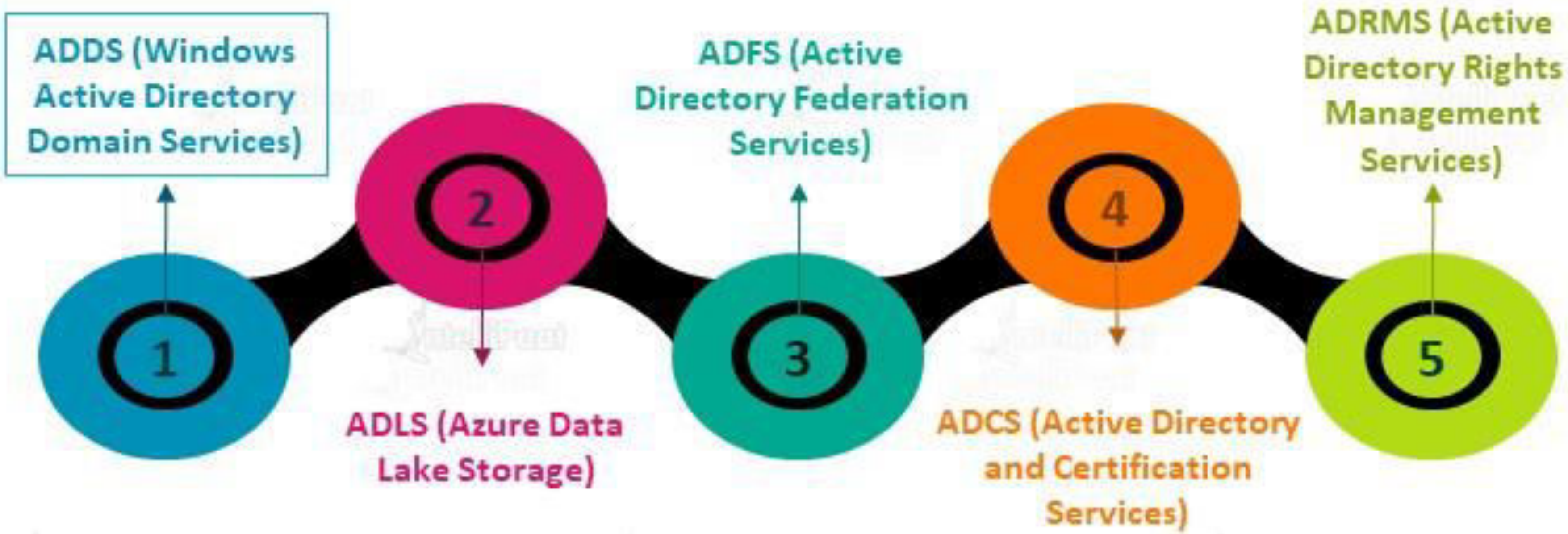
Windows Active Directory works on different layers, each layer to perform different tasks


ADDS (Windows Active Directory Domain Services)
1
2
ADLS (Azure Data Lake Storage)
ADFS (Active Directory Federation Services)
3
4
ADCS (Active Directory and Certification Services)
ADRMS (Active Directory Rights Management Services)
5

Copyright Intellipaat. All rights reserved.

What is Windows Active Directory?

Windows Active Directory works on different layers, each layer to perform different tasks

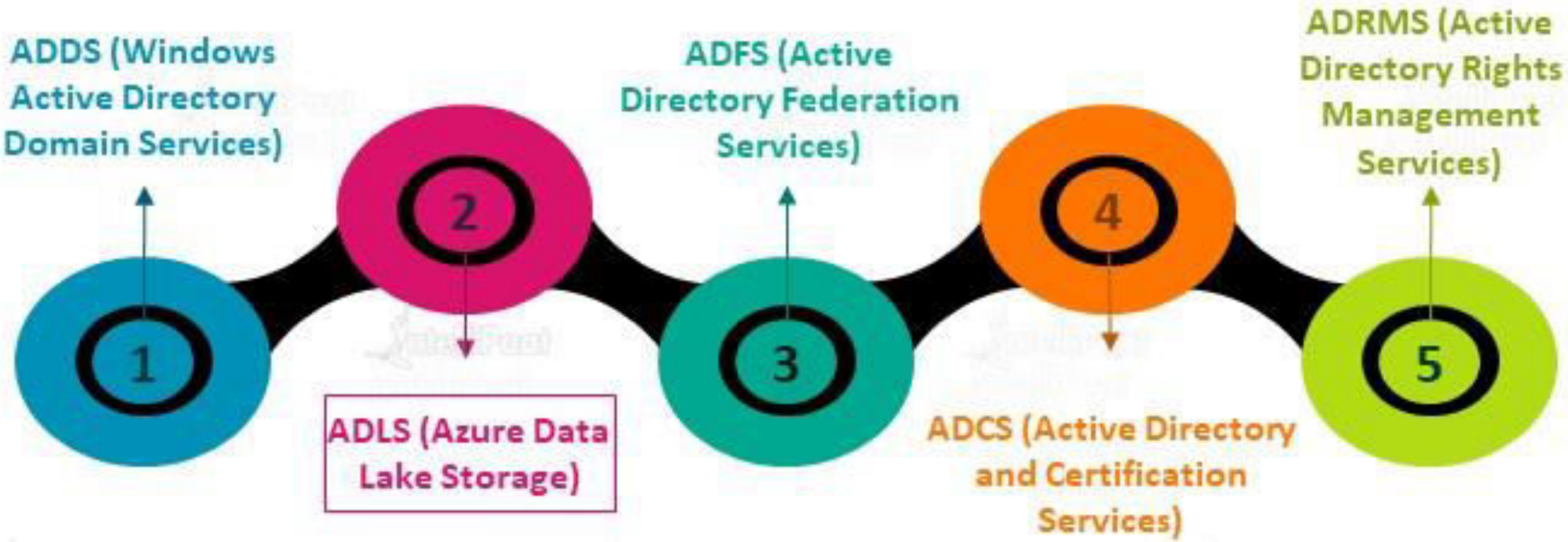

ADDS (Windows Active Directory Domain Services)
1
2
ADLS (Azure Data Lake Storage)
ADFS (Active Directory Federation Services)
3
4
ADCS (Active Directory and Certification Services)
ADRMS (Active Directory Rights Management Services)
5

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

Copyright Intellipaat. All rights reserved.

What is Windows Active Directory?

Windows Active Directory works on different layers, each layer to perform different tasks



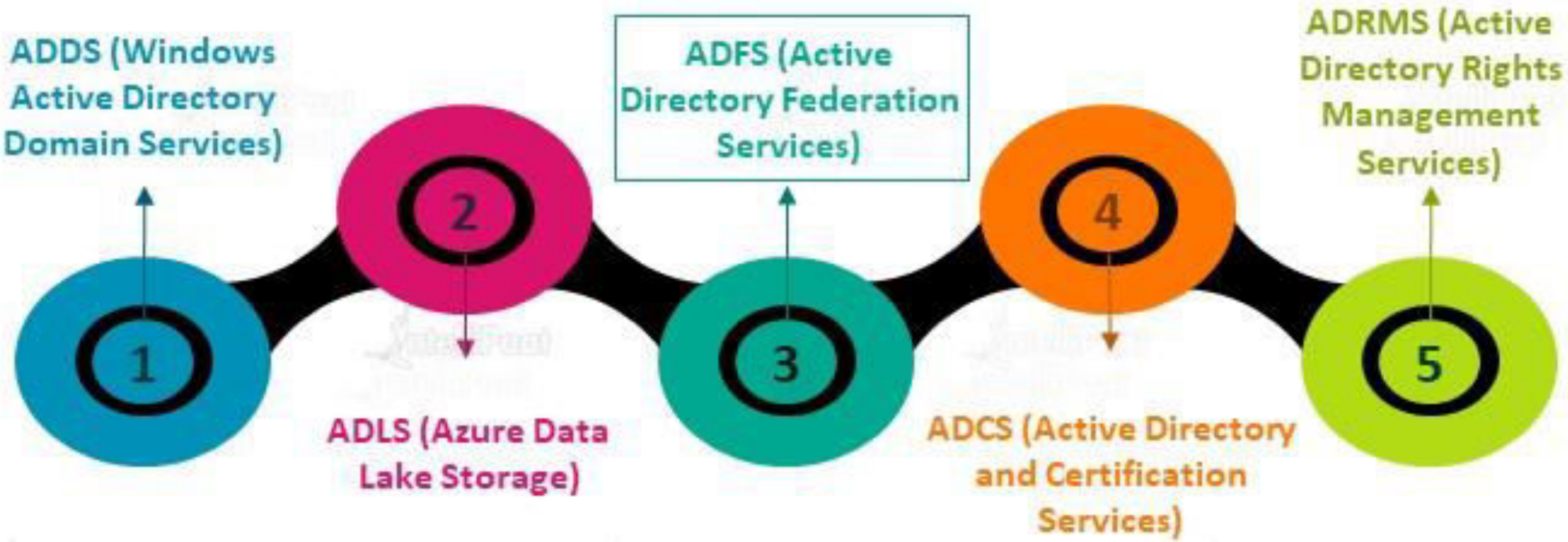
ADDS (Windows Active Directory Domain Services)
1
2
ADLS (Azure Data Lake Storage)
ADFS (Active Directory Federation Services)
3
4
ADCS (Active Directory and Certification Services)
ADRMS (Active Directory Rights Management Services)
5

This layer allows admins to store any amount of data of any type and size

Copyright Intellipaat. All rights reserved.

What is Windows Active Directory?

Windows Active Directory works on different layers, each layer to perform different tasks



ADDS (Windows Active Directory Domain Services)

ADLS (Azure Data Lake Storage)

ADFS (Active Directory Federation Services)

ADCS (Active Directory and Certification Services)

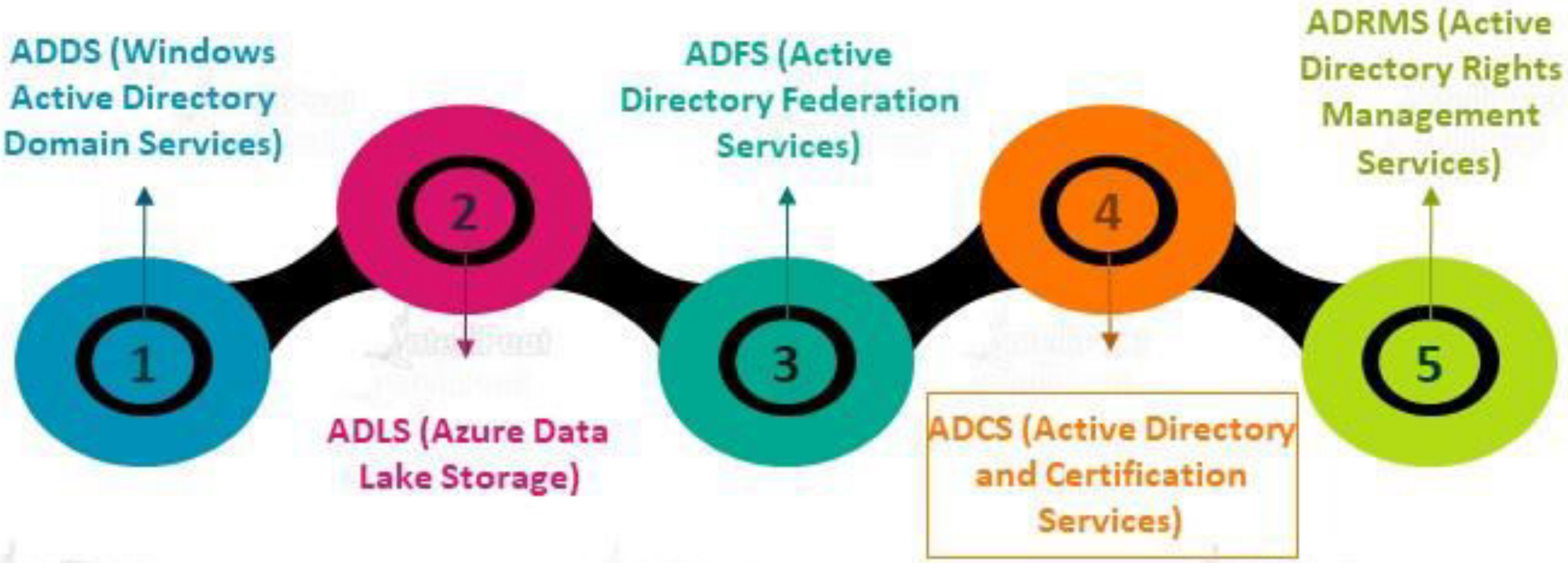
ADRMS (Active Directory Rights Management Services)

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

Copyright Intellipaat. All rights reserved.

What is Windows Active Directory?

Windows Active Directory works on different layers, each layer to perform different tasks

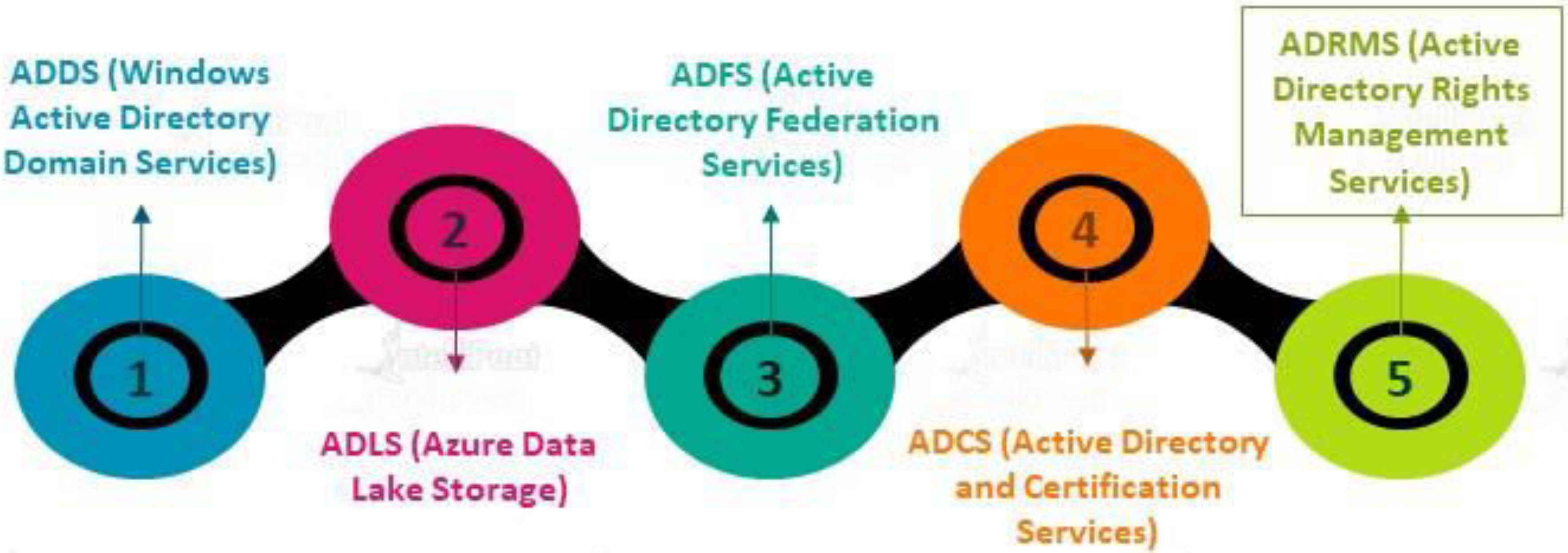

ADDS (Windows Active Directory Domain Services)
1
2
ADLS (Azure Data Lake Storage)
ADFS (Active Directory Federation Services)
3
4
ADCS (Active Directory and Certification Services)
ADRMS (Active Directory Rights Management Services)
5

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

Copyright Intellipaat. All rights reserved.

What is Windows Active Directory?

Windows Active Directory works on different layers, each layer to perform different tasks

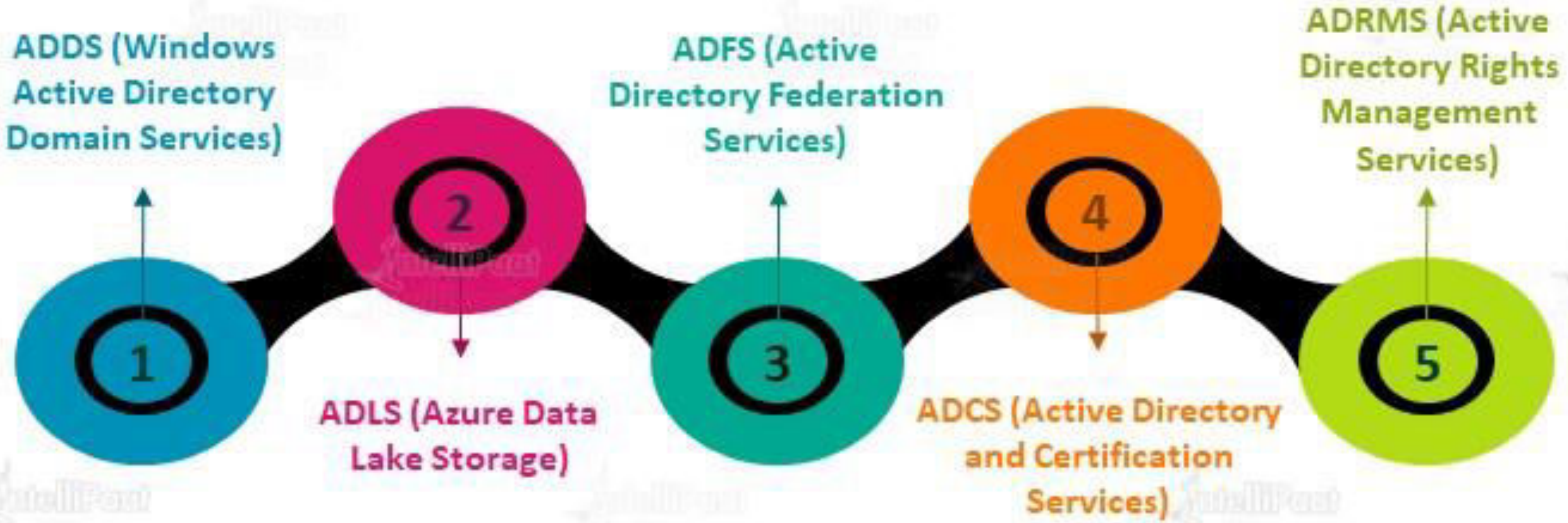

ADDS (Windows Active Directory Domain Services)
1
2
ADLS (Azure Data Lake Storage)
ADFS (Active Directory Federation Services)
3
4
ADCS (Active Directory and Certification Services)
ADRMS (Active Directory Rights Management Services)
5

ADRMS layer is used for data protection

Copyright Intellipaat. All rights reserved.

Windows AD vs Azure AD

Azure Active Directory merges all these layers into just two layers


ADDS (Windows Active Directory Domain Services)
1
2
ADLS (Azure Data Lake Storage)
ADFS (Active Directory Federation Services)
3
4
ADCS (Active Directory and Certification Services)
ADRMS (Active Directory Rights Management Services)
5

Copyright Intellipaat. All rights reserved.

Windows AD vs Azure AD

Azure Active Directory merges all these layers into just two layers

WAAD (Windows Azure Active Directory)

WAAC (Windows Azure Access Control Service)

Copyright Intellipaat. All rights reserved.

Service Audience

Copyright Intellipaat. All rights reserved.

Service Audience

IT Administrator

- ✓ The IT administrator will be responsible for all sign-ups and sign-ins
- ✓ Provides relevant authentication and permissions to customers or users
- ✓ Resolves authentication issues

Application Developer

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

Online Customers

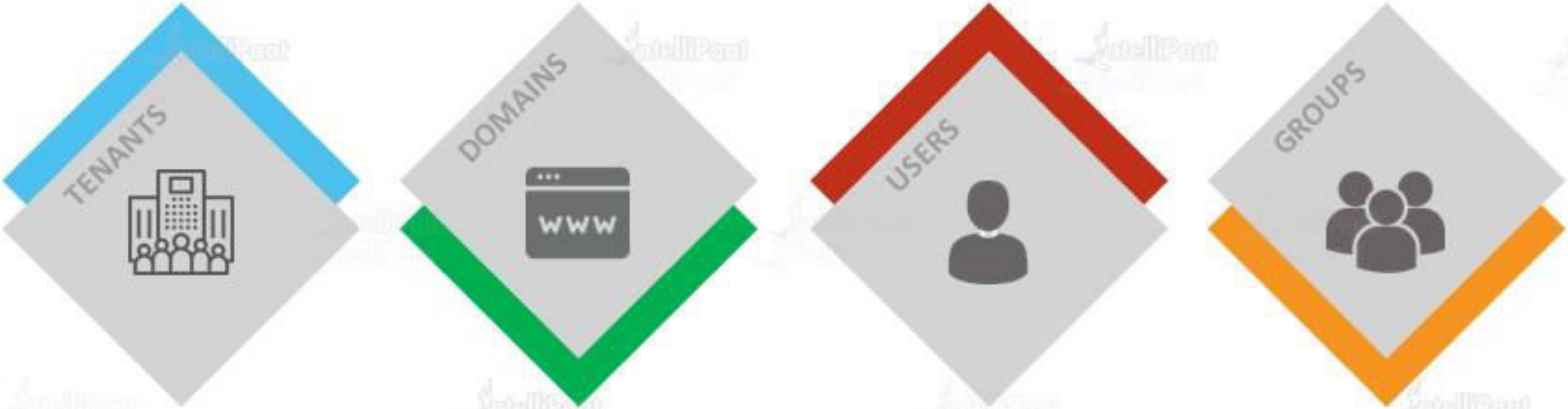
- ✓ Online customers can access services such as Office 365 and other CRM services with their Azure AD credentials

Copyright Intellipaat. All rights reserved.

Terminology in Azure Active Directory

Copyright Intellipaat. All rights reserved.

Terminology in Azure Active Directory



Tenants

A tenant is an organization. Microsoft ensures that all tenants or organizations using Microsoft Cloud services stay isolated and separated to maintain their services separately

Domains

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

Users

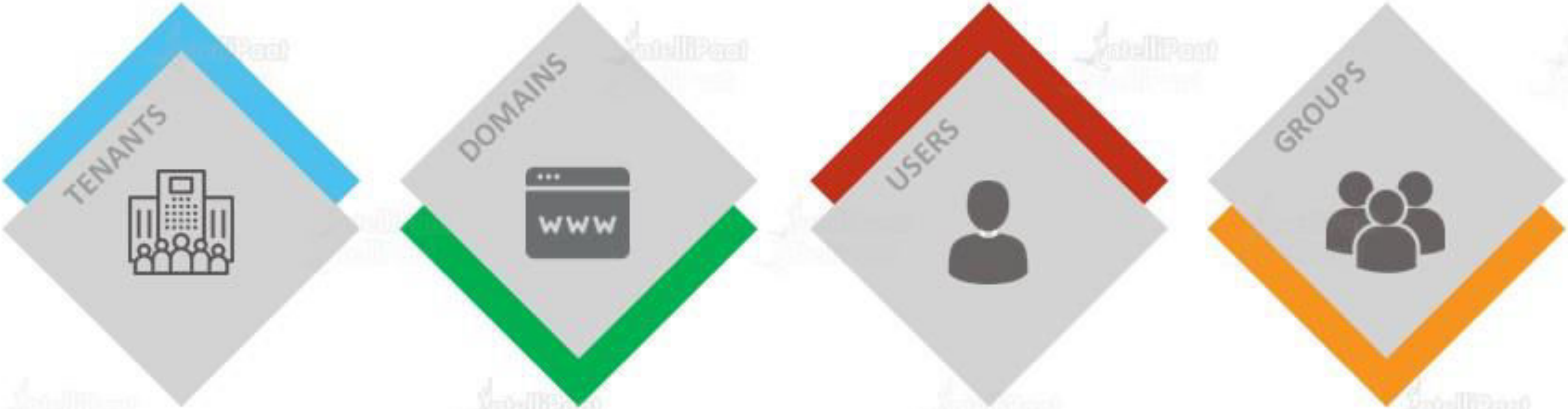
Users are individuals who are given the permission and a set of username and password to access and use certain services

Groups

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

Copyright Intellipaat. All rights reserved.

Terminology in Azure Active Directory



Tenants

A tenant is an organization. Microsoft ensures that all tenants or organizations using Microsoft Cloud services stay isolated and separated to maintain their services separately

Domains

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

Users

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

Groups

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

Copyright Intellipaat. All rights reserved.

Hands-on: Adding a Tenant in Azure Active Directory

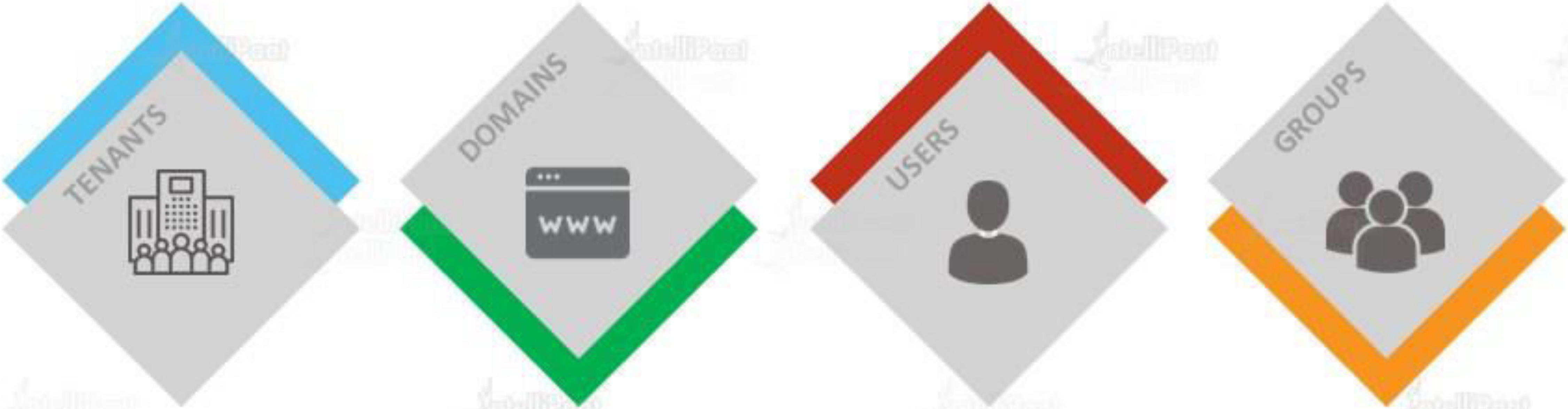
Copyright Intellipaat. All rights reserved.

Hands-on

1. **Deploy a new Tenant for your Organization in the Azure AD**

Copyright Intellipaat. All rights reserved.

Terminology in Azure Active Directory



Tenants

A tenant is an organization. Microsoft ensures that all tenants or organizations using Microsoft Cloud services stay isolated and separated to maintain their services separately

Domains

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

Users

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

Groups

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

Copyright Intellipaat. All rights reserved.

Hands-on: Adding or Deleting Users Using Azure Active Directory

Copyright Intellipaat. All rights reserved.

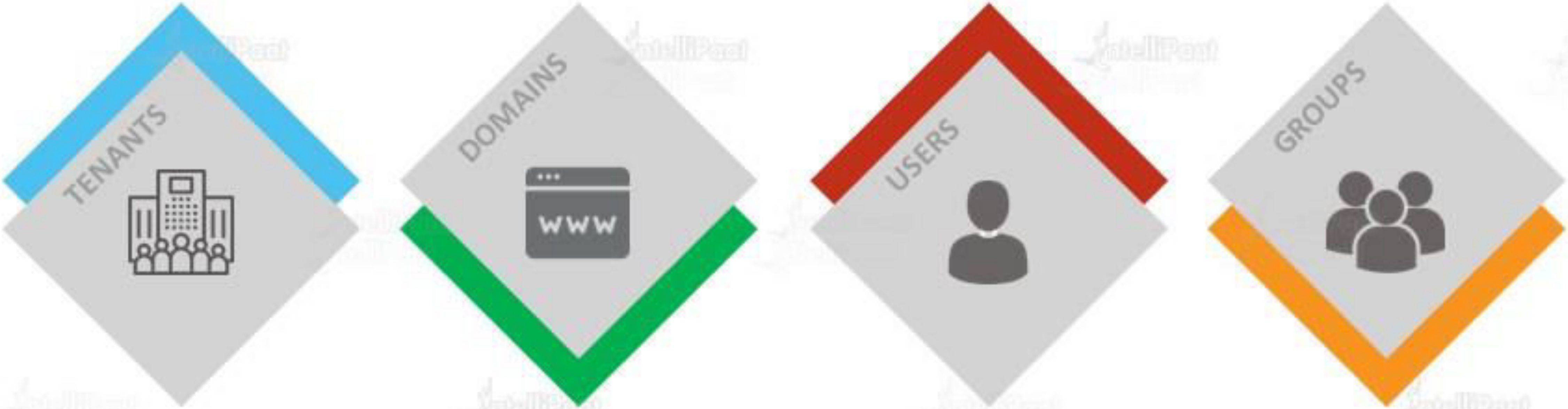
Hands-on

1. Create Users in the Tenant Deployed

2. Delete the users that are not there in the organization

Copyright Intellipaat. All rights reserved.

Terminology in Azure Active Directory



Tenants

A tenant is an organization. Microsoft ensures that all tenants or organizations using Microsoft Cloud services stay isolated and separated to maintain their services separately

Domains

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

Users

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

Groups

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

Copyright Intellipaat. All rights reserved.

Hands-on: Creating Groups & Adding Members Using Azure Active Directory

Copyright Intellipaat. All rights reserved.

Hands-on

1. Create a Group in the Azure AD

2. Add members in that group that must be assigned similar role assignments

Copyright Intellipaat. All rights reserved.

Azure Policies

Copyright Intellipaat. All rights reserved.

Azure Policies

Azure Policies is a service provided by Microsoft Azure to be able to create, manage, and assign new policies to Azure resources

They make sure that the resources adhere to the **service-level agreement** and **corporate standards**

Copyright Intellipaat. All rights reserved.

How is Azure Policies different from RBAC?

RBAC focuses on user action at different roles, whereas Azure Policies focuses on resource properties during deployment and on the resources that have already been deployed. Azure Policies controls properties such as the types or location of Azure resources

Copyright Intellipaat. All rights reserved.

Identity Solution for Hybrid Environments

Copyright Intellipaat. All rights reserved.

Implementing Authentication in Azure

- ❑ Self Service Password Reset
- ❑ Multi-factor Authentication

Copyright Intellipaat. All rights reserved.

What is Self Service Password Reset?

Copyright Intellipaat. All rights reserved.

Self Service Password Reset

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

If SSPR is enabled, we must select at least one of the following options/gates for authentication

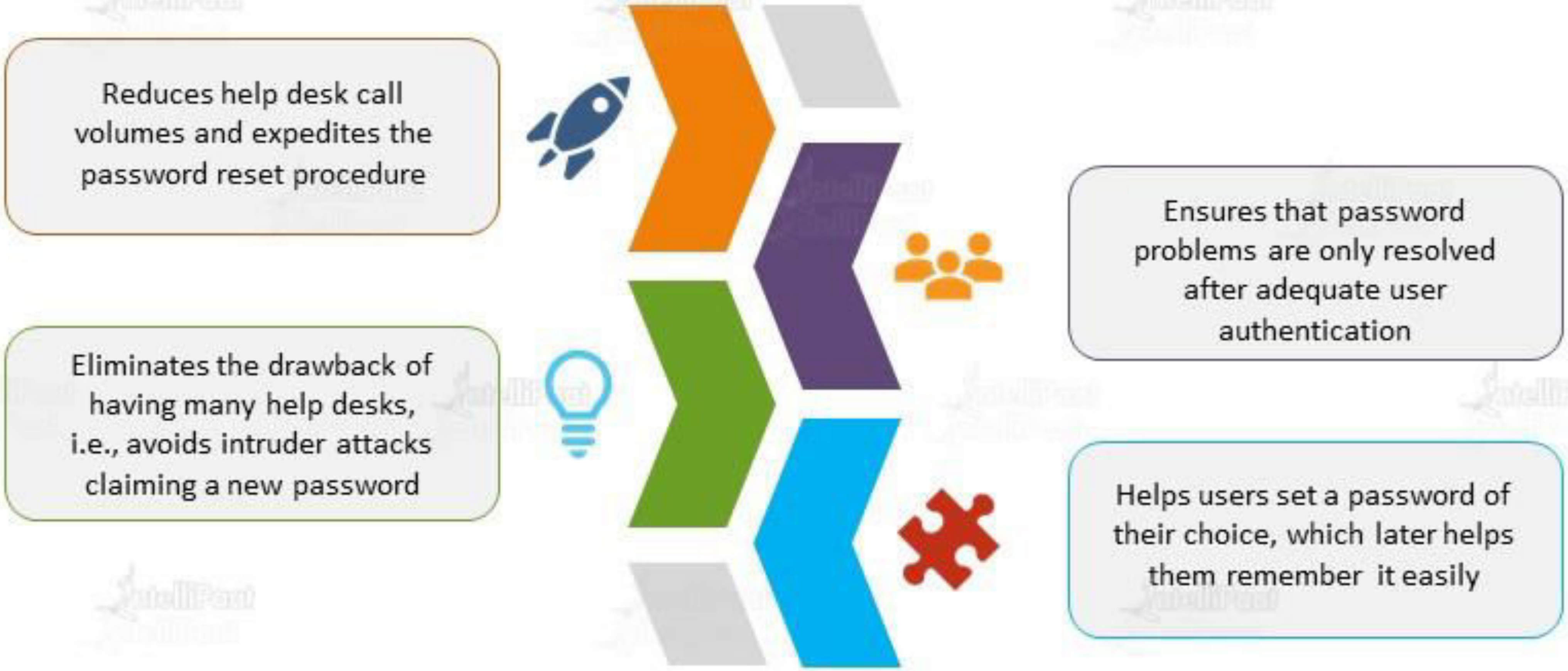
- 01 Mobile phone
- 02 Mobile app notification
- 03 Office phone
- 04 Email
- 05 Security questions
- 06 Mobile app code

Copyright Intellipaat. All rights reserved.

Why Self Service Password Reset?

Copyright Intellipaat. All rights reserved.

Why Self Service Password Reset?



Reduces help desk call volumes and expedites the password reset procedure

Eliminates the drawback of having many help desks, i.e., avoids intruder attacks claiming a new password

Ensures that password problems are only resolved after adequate user authentication

Helps users set a password of their choice, which later helps them remember it easily

Copyright Intellipaat. All rights reserved.

Hands-on: Enabling Self Service Password Reset

Copyright Intellipaat. All rights reserved.

Multi-factor Authentication

Copyright Intellipaat. All rights reserved.

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, i.e., the password
- What the user has, i.e., the security token on a trusted device
- What the user is, i.e., the biometric verification

Username

Password

Copyright Intellipaat. All rights reserved.

Azure AD Join

Copyright Intellipaat. All rights reserved.

What are Azure AD Joined Devices?

AD joined devices are signed in for using an organizational Azure AD account

The main purposes behind AD Join are:

- Windows deployments of work-owned devices
- Access to organizational apps and resources from any Windows device
- Cloud-based management of work-owned devices
- Signing in of users to their devices with their Azure AD or synced Active Directory work or school accounts

Copyright Intellipaat. All rights reserved.

Use Cases: Azure AD Join

One of the major cases where Azure AD Join is used is when the organization does not have an on-premises Windows Server AD infrastructure. A few other scenarios are given below:

- When organization’s users primarily need to access Office 365 or other SaaS apps integrated with Azure AD
- When transitioning to cloud-based infrastructure using Azure AD and MDM like Microsoft Intune
- When providing joining capabilities to workers in remote branch offices with limited on-premises infrastructure
- When users sign in to their devices with their Azure AD or synced Active Directory work or school accounts

Copyright Intellipaat. All rights reserved.

Azure Resource Locks

Resource lock is a service provided by Azure to make sure that our subscription, resource group, or resource is not being accidently deleted or modified by other users in our organization
The owner and the user access administrator are granted the roles to authorize users. The lock level can be set to:

CanNotDelete

Here, users can read and modify, but they cannot delete resources

ReadOnly

ReadOnly is analogous to the Reader role. Here, the users may read but cannot modify or delete the resources

Copyright Intellipaat. All rights reserved.

Hands-on: Applying Resource Locks

Copyright Intellipaat. All rights reserved.

Quiz

Copyright Intellipaat. All rights reserved.

Quiz

1. What is Azure Active Directory?

A. A networking service offered by Azure

B. A data warehouse service offered by Azure

C. An identity and access management service offered by Azure

D. Another term for Azure subscription

Copyright Intellipaat. All rights reserved.

Quiz

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

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

B. Granting a user to access the whole resource group

C. Restricting a user from accessing the whole subscription

D. None of the above

Copyright Intellipaat. All rights reserved.

Quiz

3. The self service password reset feature lets users log in without using any authentication credentials.

A. True

B. False

Copyright Intellipaat. All rights reserved.

Quiz

4. Which of the following statements is false?

A. Azure uses the RBAC method for access management

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

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

D. Azure Active Directory helps achieving SSO

Copyright Intellipaat. All rights reserved.

Quiz

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

A. True

B. False

Copyright Intellipaat. All rights reserved.

☎ India: +91-7847955955

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

✉ support@intellipaat.com

24/7 Chat with Our Course Advisor

Copyright Intellipaat. All rights reserved.