



# Microsoft Azure Administrator Associate Training(AZ-103)

Azure AD, MRBAC, MFA and PIM



# Agenda



- ☐ What is Azure AD
- ☐ Azure AD Editions
- ☐ AD Domain Services
- ☐ Azure AD
- ☐ Custom Domain Names
- ☐ Managing Users, Groups, Devices
- ☐ Managing Devices
- ☐ Tenants
- ☐ SSO
- ☐ Hands-On Lab
- ☐ Manage role based access control (RBAC)
- ☐ Multi-factor authentication (MFA)
- ☐ Directory Synchronization
- ☐ Implement Azure Active Directory (AD)
- ☐ Privileged Identity Management (PIM)
- ☐ Hands-On Lab

# What is Azure AD?

# What is Azure AD?



- ❑ Azure Active Directory (Azure AD) is cloud based directory and identity management.
- ❑ By using Azure AD, you can provide secure access to sensitive services & data and single sign-on (SSO).
- ❑ Azure AD supports:

Multi-factor authentication for both on-premises and cloud-resident resources.

Role-Based Access Control (RBAC)

Self-service password

Group management

Device registration

- ❑ Organizations that use AD DS can synchronize users and groups from their Active Directory domains with Azure AD to enable a SSO experience for their users accessing both on-premises and cloud-based applications.

# Azure AD:



## Azure AD Editions

### The Free Edition

- Provides user and group management, device registration, self-service password change for cloud users, and synchronization with on-premises directories.
- It is limited to 10 applications per user configured for SSO and 500,000 objects.

### The Basic Edition

- Extends the free edition's capabilities by combining group-based access management, self-service password reset for cloud users, and support for application proxy.
- The Basic edition does not impose limits on the number of directory objects, but has a limit of 10 apps per user.

### The Premium Edition

- It supports dynamic groups and self-service group management, self-service password reset.
- It offers support for an unlimited number of objects and unlimited number of apps per user.
- Azure AD Premium is available in two tiers – P1 and P2. Both tiers include all the features described above.
- Azure AD Premium P2 however, offers additional Identity Protection and Privileged Identity Management features.

# Azure AD:

## AD Domain Services



General Purpose v2 (GPv2) are storage accounts which support all features for all storage services, including Blobs, Files, Queues, and Tables.

For Block Blobs, You can choose between hot and cool storage tiers at account level, or hot, cool, and archive tiers at the blob level based on access patterns.

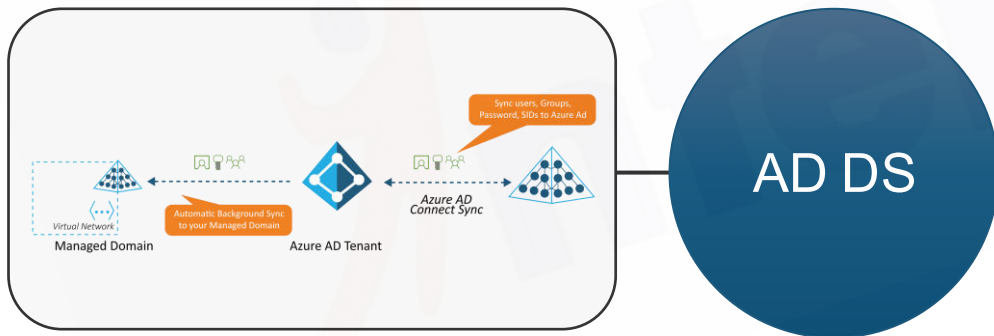
Store frequently, infrequently, and rarely accessed data in the hot, cool, and archive storage tiers respectively to optimize costs.

Importantly, any GPv1 account can be upgraded to a GPv2 account in the portal, CLI, or PowerShell.

# Azure AD:

## AD Domain Services

- ❑ Active Directory Domain Services (AD DS) is a directory service and an identity management solution.
- ❑ As a directory service, AD DS hosts a distributed database, residing on servers referred to as domain controllers.
- ❑ When comparing AD DS with Azure AD, it is important to note the following characteristics of AD DS:



- ❑ AD DS is by design single-tenant.
- ❑ AD DS uses Domain Name System (DNS) for locating domain controllers.
- ❑ AD DS relies on protocols such as Lightweight Directory Access Protocol (LDAP) for directory lookups and Kerberos for authentication.
- ❑ AD DS facilitates Group Policy Objects (GPOs)-based management.
- ❑ AD DS supports users, groups, and AD-aware applications.
- ❑ AD DS supports computer objects, representing computers that join an Active Directory domain.
- ❑ AD DS supports multi-domain forests.

# Azure AD:

## Azure AD



- ❑ Azure AD is somewhat similar to AD DS, there are some fundamental differences between them.
- ❑ The following are some of the characteristics that make Azure AD distinct:

01

Azure AD is multitenant by design.

02

Azure AD provides no support for organizational units (ous).

03

Azure AD implementation does not rely on domain controllers.

04

Azure AD supports protocols that facilitate secure communication over the internet.

05

Azure AD does not support Kerberos authentication; instead, it uses protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization).

06

Azure AD does not support LDAP; instead, it relies on the Graph Application Programming Interface (API) for directory lookups.

07

Azure AD provides no support for groups.

08

AD DS supports users, groups, and web-based applications.

09

Azure AD supports device objects representing devices that register or join an Azure AD tenant.

10

Azure AD offers federation services, and many third-party services (such as Facebook) are federated with and trust Azure AD. You can also federate AD DS with Azure AD.



# Azure AD: Custom Domain Names

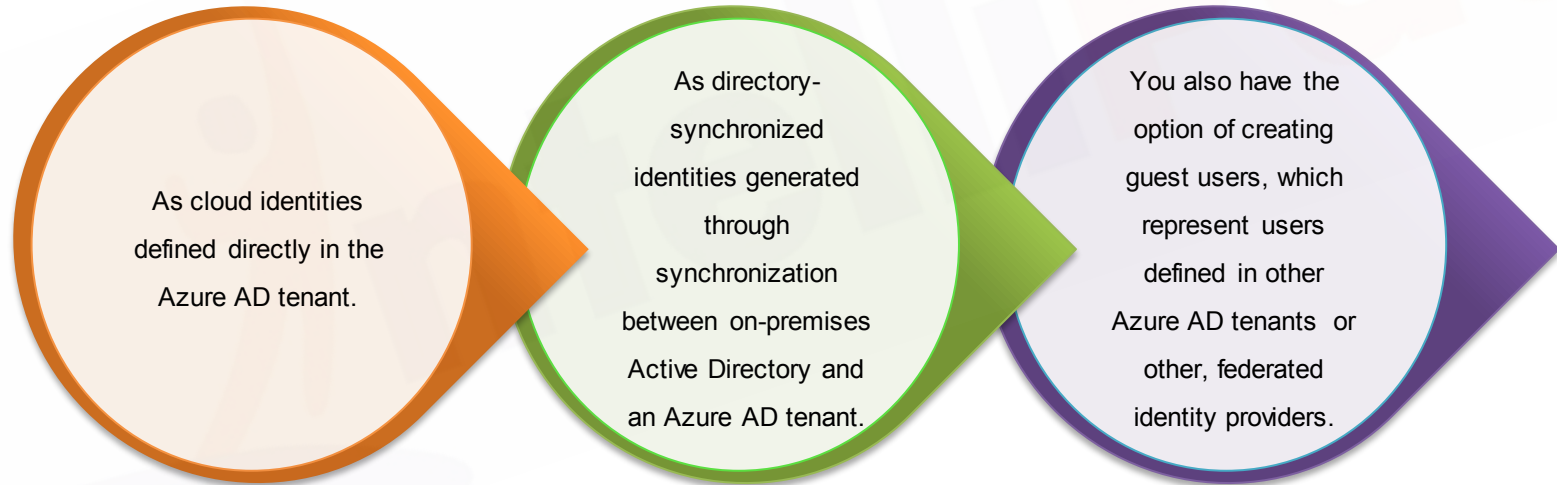


- 01** Each Azure AD tenant is assigned the default DNS domain name, consisting of a unique prefix, followed by the onmicrosoft.com suffix.
- 02** The prefix is either derived from the name of the Microsoft account you use to create an Azure subscription or provided explicitly when you create an Azure AD tenant.
- 03** It is common to add at least one custom domain name to the same Azure AD tenant.
- 04** This name utilizes the DNS domain namespace that the tenant's company or organization owns.

# Azure AD:

## Managing Users, Groups, Devices

- ❑ You can manage Azure AD users, groups, and devices by using the Azure portal, Active Directory PowerShell, Microsoft Intune admin console, or Office 365 admin center.
- ❑ There are three basic ways to create users, groups, and devices in Azure AD:



# Azure AD: Managing Devices



Users can join their Windows 10 devices to Azure AD.

If users use their Azure AD credentials to sign in to Windows 10, they can benefit from SSO functionality when accessing Office 365 and any other applications that use Azure AD for authentication, including the Azure AD Access Panel.

You can disable the ability to join devices to Azure AD or restrict it to specific Azure AD users or groups.

You can also limit the maximum number of devices per user and enforce multi-factor authentication when joining devices in Azure AD.

After a user registers a device in Azure AD, you can control its usage.

**For example**, if you determine that the device has been lost or compromised, you can delete its Azure AD object or block its ability to authenticate.

# Azure AD: Tenants



- ❑ By default, you automatically get an Azure AD tenant when you sign up for an Azure, Office 365, Microsoft Dynamics CRM Online, or Microsoft Intune subscription.
- ❑ That tenant authenticates users defined in its directory.
- ❑ You can also create additional tenants as needed.
- ❑ Support for multiple Azure AD tenants facilitates the following scenarios:

Creating separate directories for testing or other non-production purposes.

Managing multiple Azure AD tenants by using the same user credentials—as long as the corresponding user account is a Global administrator in each of them.

Adding existing users as guests to multiple Azure AD tenants, eliminating the need to maintain multiple credentials for the same user.

# Azure AD: SSO



To avoid additional authentication prompts when launching applications, configure SSO.

SSO allows users to run Azure AD–registered applications without providing a user name and password.

SSO eliminates the need to provision and maintain separate user accounts for each SaaS application.

Azure AD provides secure storage of user credentials, and provides support for federated trusts with other cloud services and identity providers.

Several commercial applications with SSO capabilities, such as Microsoft Office 365, Box, or Salesforce, are preconfigured for integration with Azure AD.

You can also use Azure AD SSO functionality to control access to on-premises applications or applications developed in-house but deployed to Azure.

# Hands-On

# Hands-On

- ❑ Configure Azure AD
- ❑ Create user in Azure AD
- ❑ Login via Azure AD
- ❑ Enable MFA.



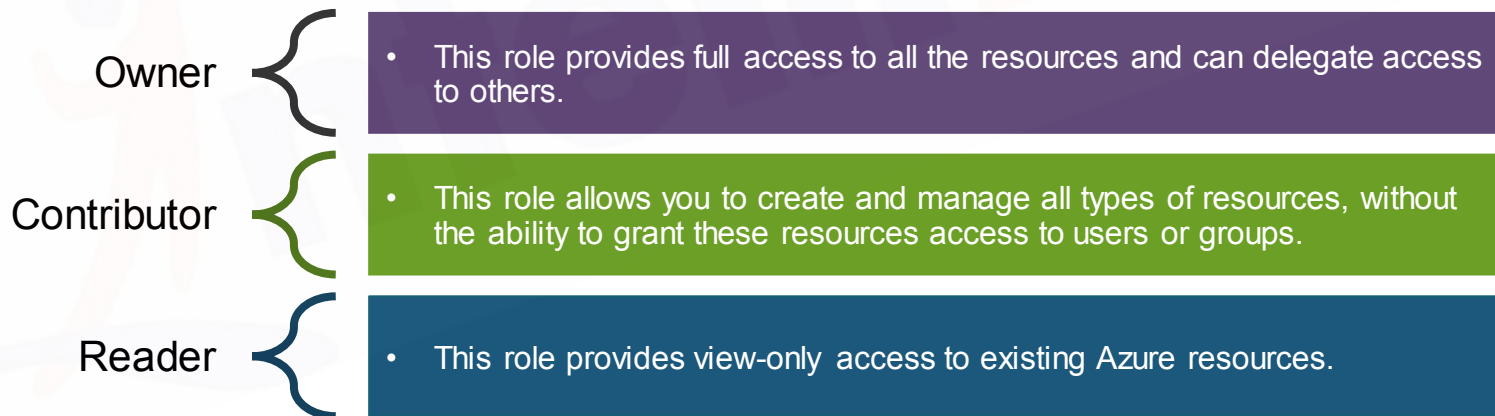
# Manage Role Based Access Control (RBAC)



# Manage Role Based Access Control (RBAC)



- ❑ RBAC enables fine-grained access management for resources that exist in an Azure subscription.
- ❑ By using RBAC, you can implement delegated management of cloud resources.
- ❑ For example, you can allow your development team to create their own virtual machines, but limit virtual networks to which those machines can be connected.
- ❑ RBAC has three basic built-in roles that apply to all resource types:



# Multi-Factor Authentication (MFA)

- ❑ Azure Multi-Factor Authentication adds an additional security layer in the authentication process by requiring more than one method of authentication to identify user identity.
- ❑ Usernames and passwords are still required to sign in to access data and applications, but an additional access method can be added as a second factor of authentication.
- ❑ Multi-factor authentication combines something that you know, such as a password or a PIN.



- You can authenticate via a phone call.
- You can authenticate via a text message.
- You can authenticate using a third-party OAuth token.

# Directory Synchronization



Directory synchronization involves copying selected user, group, contact between on-premises Active Directory and Azure AD.

In its simplest form, you install a directory synchronization component on a server with direct connectivity to your AD DS domain controllers.

After the initial synchronization completes, objects representing all on-premises user accounts, groups, contacts that are not built-in from AD DS will then automatically appear in Azure AD.

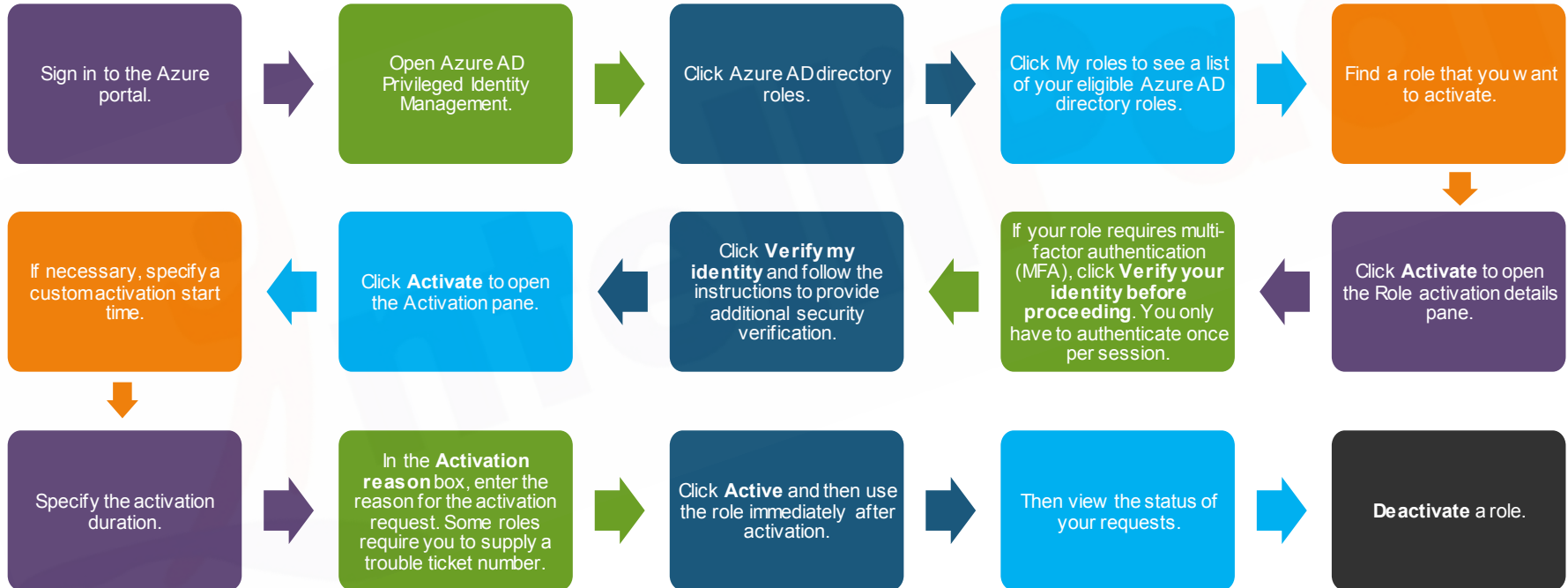
This way, AD DS users can authenticate and access Azure resources by using the same credentials as those they use to sign in to their on-premises computers.

# **Implement Azure Active Directory (AD) & Privileged Identity Management (PIM)**

# Activate Azure AD directory roles in PIM



## To Activate a role



# Assign Azure resource roles in PIM

Azure AD PIM can manage the built-in Azure resource roles, as well as custom roles, including (but not limited to):

•Owner

User Access  
Administrator

Contributor

Security Admin

Security Manager, and  
more

# Assign Azure resource roles in PIM



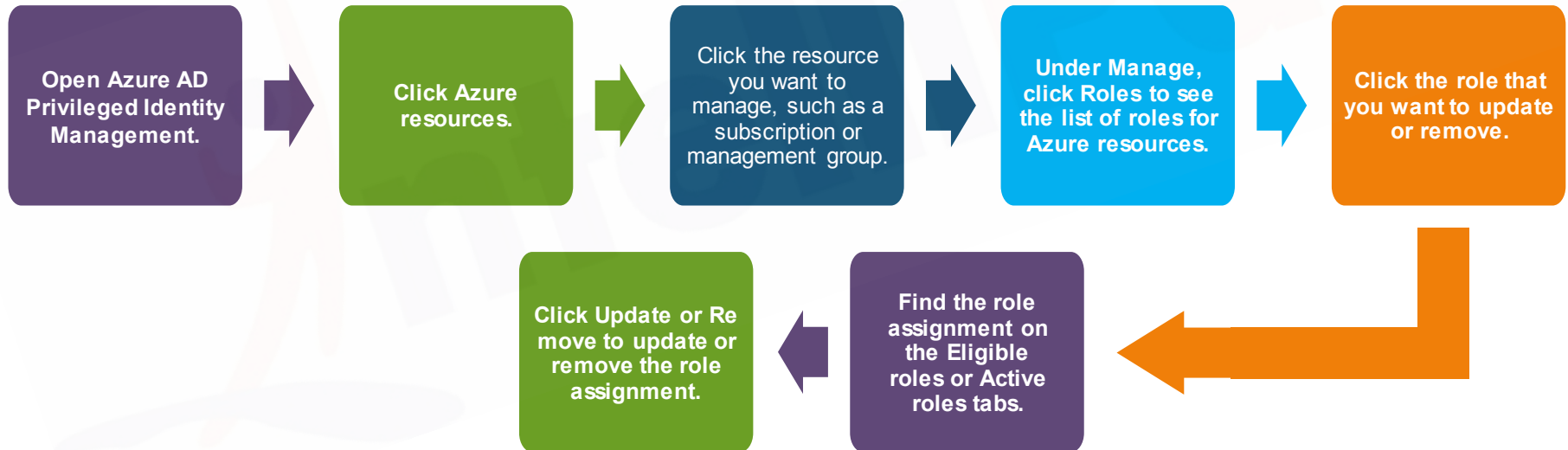
To Assign a role, follow these steps to make a user eligible for an Azure resource role:



# Assign Azure resource roles in PIM continued....



To update or remove an existing role assignment, Follow these steps to update or remove an existing role assignment.





# Approve/Deny requests for Azure AD directory roles in PIM



Microsoft Azure

Search resources, services, and docs

Home > Privileged Identity Management > Azure AD directory roles - Approve requests

Privileged Identity Ma... ✱ ✕

Azure AD directory roles - Approve requests  
default directory

Quick start

TASKS

- My roles
- My requests
- Application access
- Approve requests**
- Review access

MANAGE

- Azure AD directory roles**
- Azure resources

Overview

Quick start

TASKS

- My roles
- My requests
- Approve requests**
- Review access

MANAGE

- Roles
- Members

✓ Approve ✕ Deny ↺ Refresh

ROLE	REQUESTOR	REASON
Application Administr...	Isabe... isabe...	Configure a n
Security Reader	Ann ... ann...	Review securi

# Approve/Deny requests for Azure AD directory roles in PIM

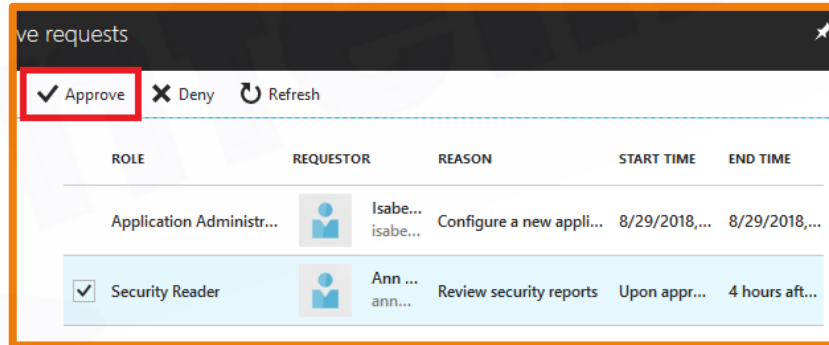


## Approve Requests

1. Select the requests you want to approve and then click **Approve** to open the Approve selected requests pane.

1. In the **Approve reason** box, type a reason.

1. Click **Approve**.



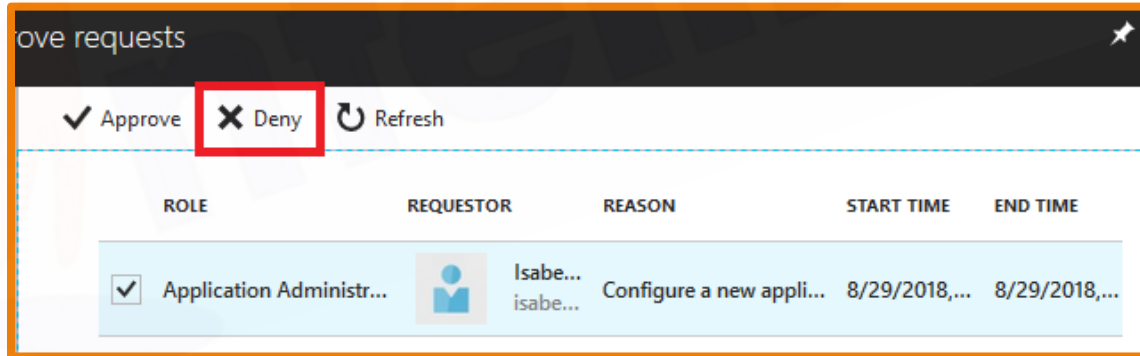
# Approve/Deny requests for Azure AD directory roles in PIM

## Deny Requests


1. Select the requests you want to deny and then click Deny to open the Deny selected requests pane.

1. In the Deny reason box, type a reason.

1. Click **Deny**.



The screenshot shows the 'Approve requests' interface. At the top, there are three buttons: 'Approve' (with a checkmark icon), 'Deny' (with an 'X' icon and highlighted by a red box), and 'Refresh' (with a circular arrow icon). Below the buttons is a table with the following columns: ROLE, REQUESTOR, REASON, START TIME, and END TIME. The table contains one row with the following data:

ROLE	REQUESTOR	REASON	START TIME	END TIME
<input checked="" type="checkbox"/> Application Administr...	 Isabe... isabe...	Configure a new appli...	8/29/2018,...	8/29/2018,...

# Little Glance to PIM



**To start using PIM in your directory, you must first enable PIM.**

Sign in to the Azure portal as a **Global Administrator** of your directory.

Click **All services** and find the **Azure AD Privileged Identity Management service**.

Click to **open** the PIM QuickStart.

In the list, click **Consent** to PIM.

Click **Verify** my identity to verify your identity with Azure MFA. You'll be asked to pick an account.

Once you have completed the verification process, click the **Consent button**.

In the message that appears, click **Yes** to consent to the PIM service.

**Sign up PIM for Azure AD roles**

1. Open **Azure AD Privileged Identity Management**. Click **Azure AD roles**.

Click **Sign up**. In the message that appears, click **Yes** to sign up PIM to manage Azure AD roles.

Navigate to your tasks.

**Add a PIM tile to the dashboard.**

1. Sign in to the Azure portal. Click **All services** and find the **Azure AD Privileged Identity Management service**.

Click to **open** the PIM QuickStart. Check **Pin blade to dashboard** to pin the PIM QuickStart blade to the dashboard.

# Hands-On

# Hands-On

- ☐ Configure Azure AD
- ☐ Create user in Azure AD
- ☐ Login via Azure AD
- ☐ Enable MFA



# QUIZ

# Quiz 1

Azure Directory(AD) is\_\_\_\_\_?

- A** a cloud based repository
- B** a cloud based command line
- C** a cloud based directory and identity management
- D** a cloud based server configuration tool





# Answer 1

Azure Directory(AD) is \_\_\_\_\_?

- A** a cloud based repository
- B** a cloud based command line
- C** a cloud based directory and identity management
- D** a cloud based server configuration tool



# Quiz 2

Which one of these is supported by Azure Directory?

- A** Server management
- B** Server configuration
- C** Multi-factor authentication for both on-premises and cloud-resident resources.
- D** Single authentication for only cloud-resident resources



# Answer 2

Which one of these is supported by Azure Directory?

**A**

Server management

**B**

Server configuration

**C**

Multi-factor authentication for both on-premises and cloud-resident resources.

**D**

Single authentication for only cloud-resident resources



# Quiz 3

What does AD Domain Service uses to locate domain controllers?

- A** General Purpose V2
- B** PowerShell
- C** Blob Storage
- D** Domain Name System



# Answer 3

What does AD Domain Service uses to locate domain controllers?

- A** General Purpose V2
- B** PowerShell
- C** Blob Storage
- D** Domain Name System



# Quiz 4

Which one of them is an Azure AD feature?

- A** Automated Configuration
- B** Server Management
- C** Single Sign-On (SSO)
- D** Single-Authentication factor



# Answer 4

Which one of them is an Azure AD feature?

- A** Automated Configuration
- B** Server Management
- C** Single Sign-On (SSO)
- D** Single-Authentication factor



# Quiz 5

Does Azure AD supports Self-Service password?

A

Yes

B

No





# Answer 5

Does Azure AD supports Self-Service password?

A

Yes

B

No



# Quiz 6

RBAC is \_\_\_\_\_?

- A** Role based authorization and configuration
- B** Role based authorization and controlling
- C** Retention based access control
- D** Role based access control



# Answer 6

RBAC is \_\_\_\_\_?

- A** Role based authorization and configuration
- B** Role based authorization and controlling
- C** Retention based access control
- D** Role based access control



# Quiz 7

Basic built-in roles that apply to all resources types?

- A Owner
- B Contributor
- C Reader
- D All of the above



# Answer 7

Basic built-in roles that apply to all resources types?

A

Owner

B

Contributor

C

Reader

D

All of the above



# Quiz 8

Which statement is correct about Multi-factor authentication (MFA)?

**A**

MFA removes the additional security layer in the authentication by enabling only one method of authentication to identify user's identity

**B**

MFA adds an additional security layer in the authentication by enabling more than one method of authentication to identify user's identity

**C**

MFA keeps the same security layer in the authentication and enhances its security by enabling more only one method of authentication to identify user's identity

**D**

All of the above



# Answer 8

Which statement is correct about Multi-factor authentication (MFA)?

**A**

MFA removes the additional security layer in the authentication by enabling only one method of authentication to identify user's identity

**B**

MFA adds an additional security layer in the authentication by enabling more than one method of authentication to identify user's identity

**C**

MFA keeps the same security layer in the authentication and enhances its security by enabling more only one method of authentication to identify user's identity

**D**

All of the above



# Quiz 9

Directory Synchronization involves copying?

- A** User
- B** Group
- C** Contact
- D** All of the above





# Answer 9

Directory Synchronization involves copying?

- A** User
- B** Group
- C** Contact
- D** All of the above



# Quiz 10

Which one of them are the important roles in PIM?

- A** Owner
- B** User Access Administrator
- C** Contributor
- D** All of the above



# Answer 10

Which one of them are the important roles in PIM?

**A**

Owner

**B**

User Access Administrator

**C**

Contributor

**D**

All of the above





**India : +91-7847955955**

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



**[sales@intellipaate.com](mailto:sales@intellipaate.com)**



**24X7 Chat with our Course Advisor**