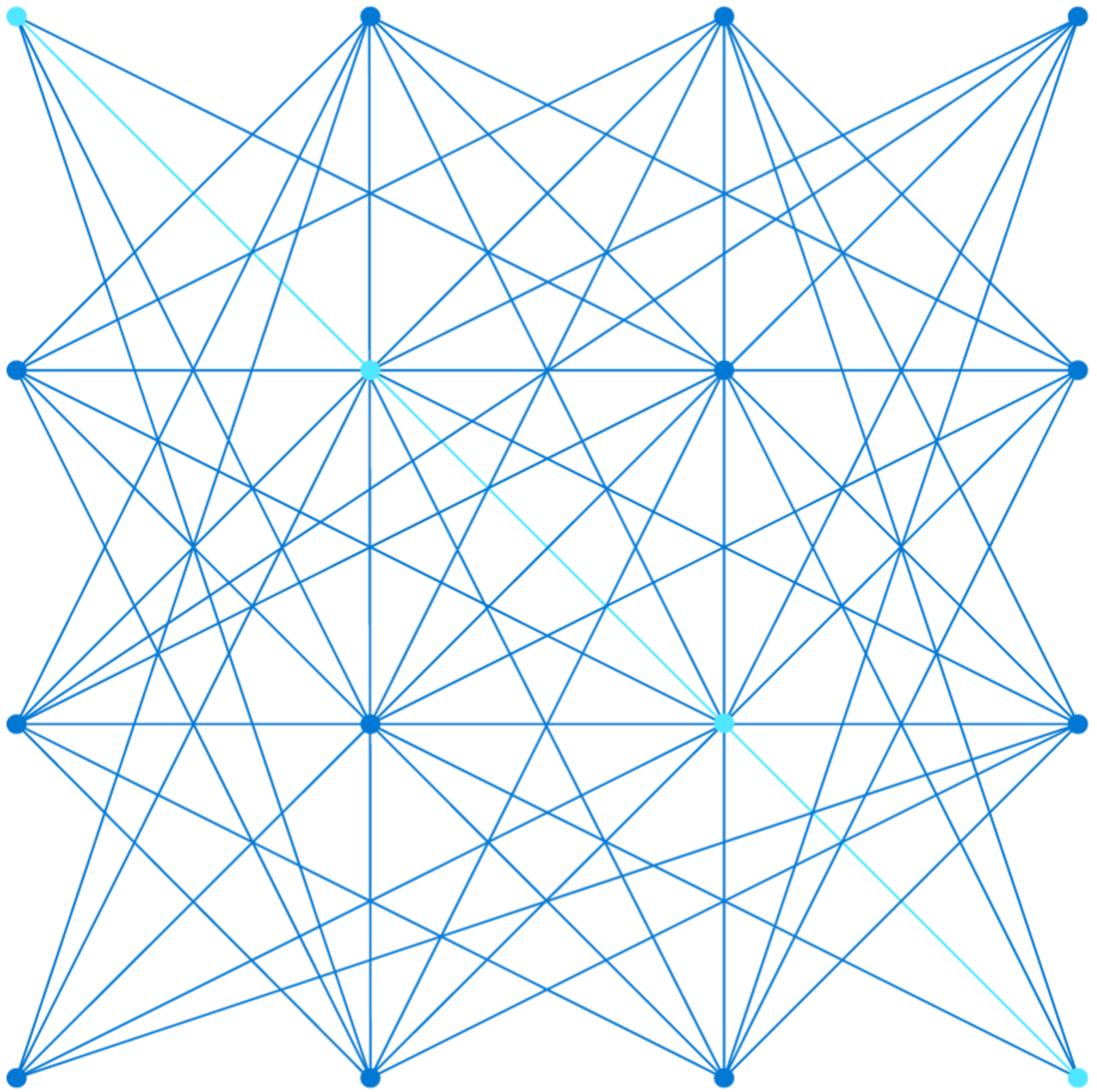
Microsoft Azure

AZ-104T00A
Module 01:
Microsoft Entra ID



Module Overview

Lesson 01: Microsoft Entra ID

Lesson 02: Users and Groups

Lesson 03: Module 01 Lab and Review

Lesson 01: Microsoft Entra ID

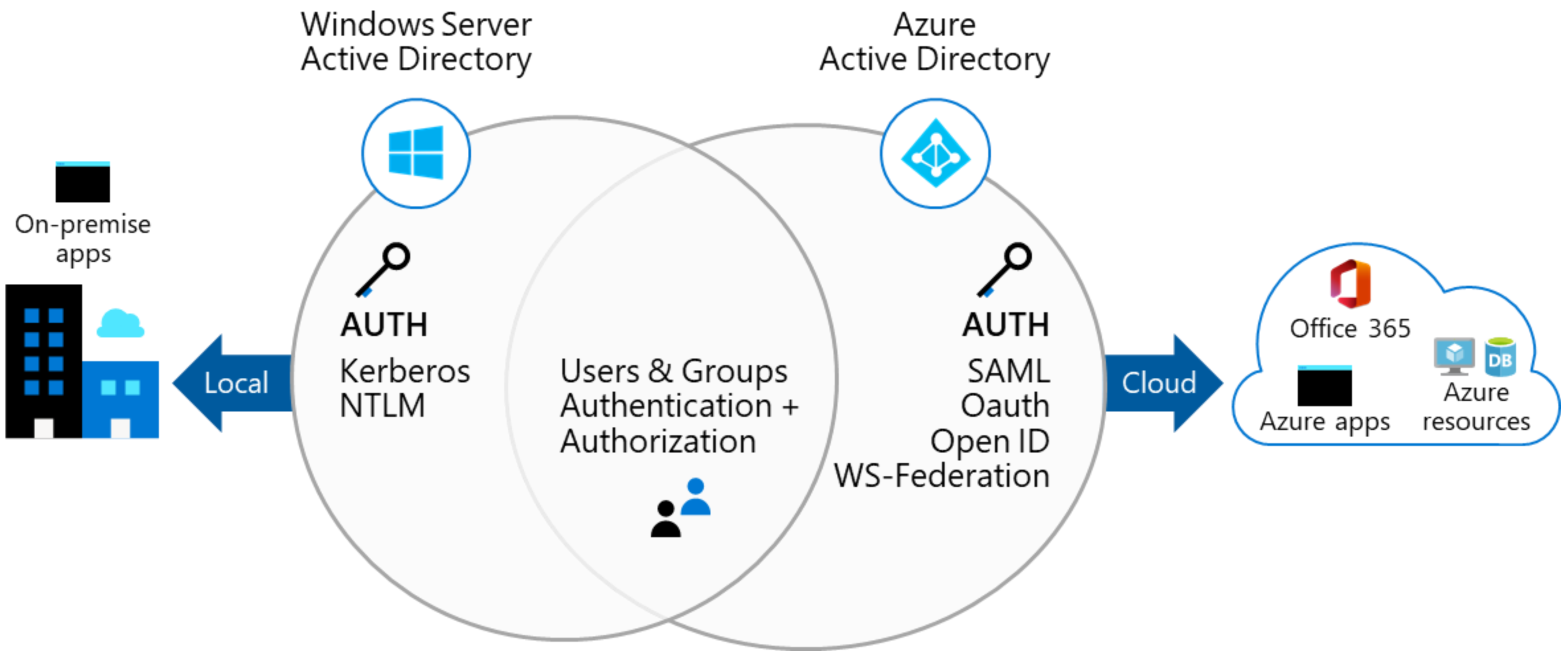
Microsoft Entra ID Overview

- Introduction
- Benefits and Features
- Concepts
- AD DS vs Entra ID
- Microsoft Entra Editions
- Self-Service Password Reset

Microsoft Entra ID

A cloud-based suite of identity management capabilities that enables you to securely manage access to Azure services and resources for your users

Provides application management, authentication, device management, and hybrid identity



Microsoft Entra Features

Feature	Description
SSO	Secure single sign-on to web apps on cloud and to on-premises app
Ubiquitous device support	Works with iOS, macOS, Android, Windows devices. Offers common experience across devices.
Secure remote access	Enable secure remote access for on-premises web apps. Include MFA, conditional policies, and group-based access management.
Cloud extensibility	Extend to cloud to help manage consistent set of users, groups, passwords and device across environments
Sensitive data protection	Offers unique identity protection capabilities to secure sensitive data and apps.
Self-service support	Delegate selected administrators tasks. Provide self-service app access and password management through verification steps.

Microsoft Entra Concepts

Concept	Description
Identity	An object that can be authenticated
Account	An identity that has data associated with it
Entra account	An identity created through Azure AD or another Microsoft cloud service
Azure tenant/directory	A dedicated and trusted instance of Azure AD, a Tenant is automatically created when your organization signs up for a Microsoft cloud service subscription • Additional instances of Azure AD can be created • Azure AD is the underlying product providing the identity service • The term *Tenant* means a single instance of Azure AD representing a single organization • The terms *Tenant* and *Directory* are often used interchangeably
Azure subscription	Used to pay for Azure cloud services

AD DS vs Microsoft Entra ID

Azure AD is primarily a fully managed identity solution, and designed for HTTP and HTTPS communications

Queried using the REST API over HTTP and HTTPS. Instead of LDAP

Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization). Instead of Kerberos

Includes federation services, and many third-party services (such as Facebook)

Azure AD users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs)

Microsoft Entra ID Editions

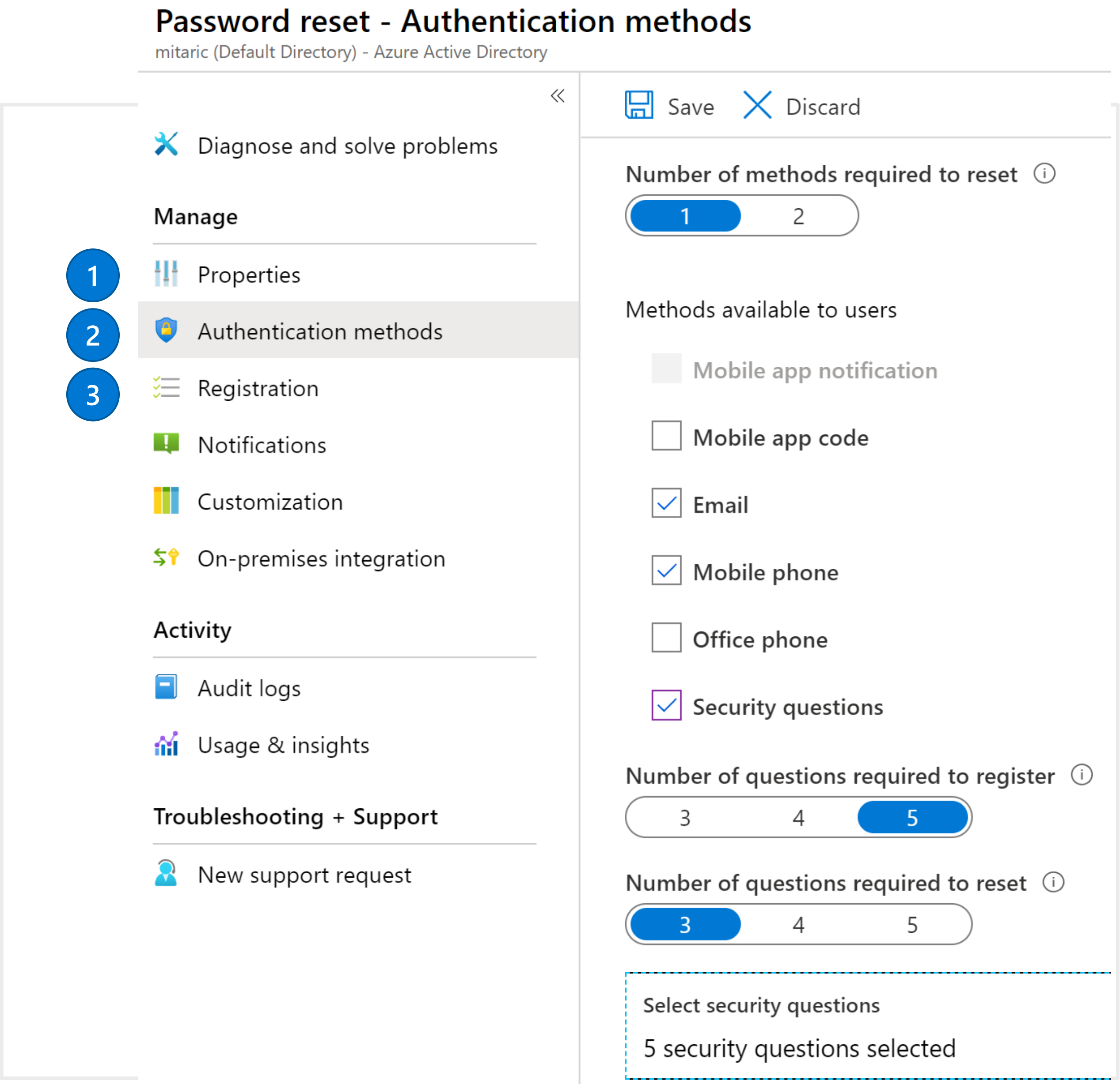
Feature	Free	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit
Single Sign-On	Unlimited	Unlimited	Unlimited
Core Identity and Access Management	X	X	X
Business-to-business Collaboration	X	X	X
Identity & Access for O365		X	X
Premium Features		X	X
Hybrid Identities		X	X
Advanced Group Access		X	X
Conditional Access		X	X
Identity Protection			X
Identity Governance			X

Self-Service Password Reset

1. Determine who can use self-service password reset

2. Choose the number of authentication methods required and the methods available (email, phone, questions)

3. You can require users to register for SSPR (same process as MFA)



Password reset - Authentication methods

mitaric (Default Directory) - Azure Active Directory

Number of methods required to reset: [✓ 1] 2

Methods available to users

□ Mobile app notification

□ Mobile app code

☑ Email

☑ Mobile phone

□ Office phone

☑ Security questions

Number of questions required to register: 3 4 [✓ 5]

Number of questions required to reset: [✓ 3] 4 5

Select security questions

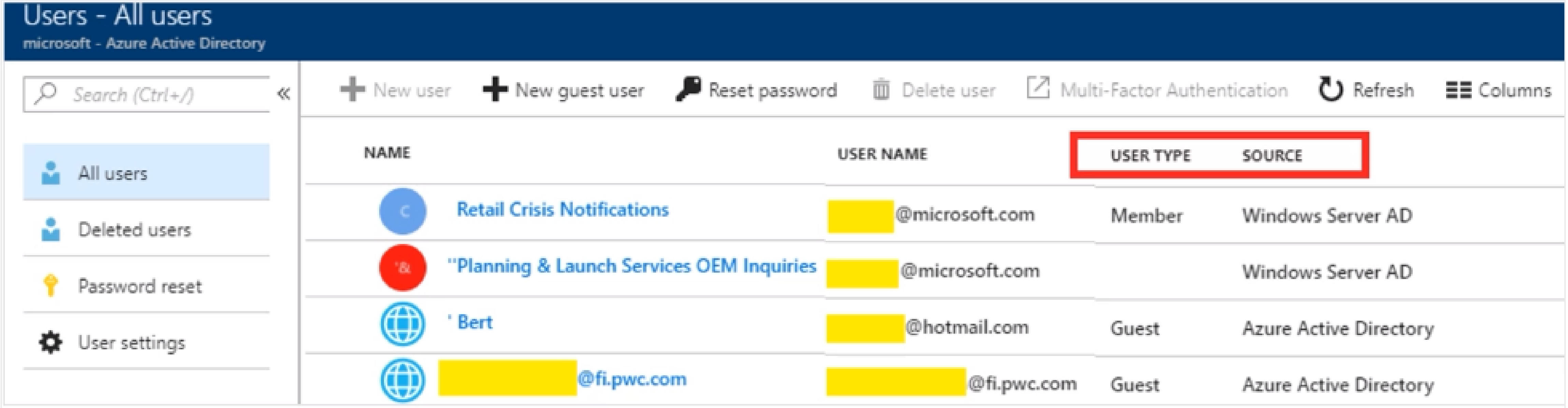
5 security questions selected

Lesson 02: Users and groups

Users and Groups Overview

- User Accounts
- Managing User Accounts
- Bulk User Accounts
- Group Accounts
- Managing Multiple Directories
- Demonstration – Users and Groups

User Accounts



Users - All users

microsoft - Azure Active Directory

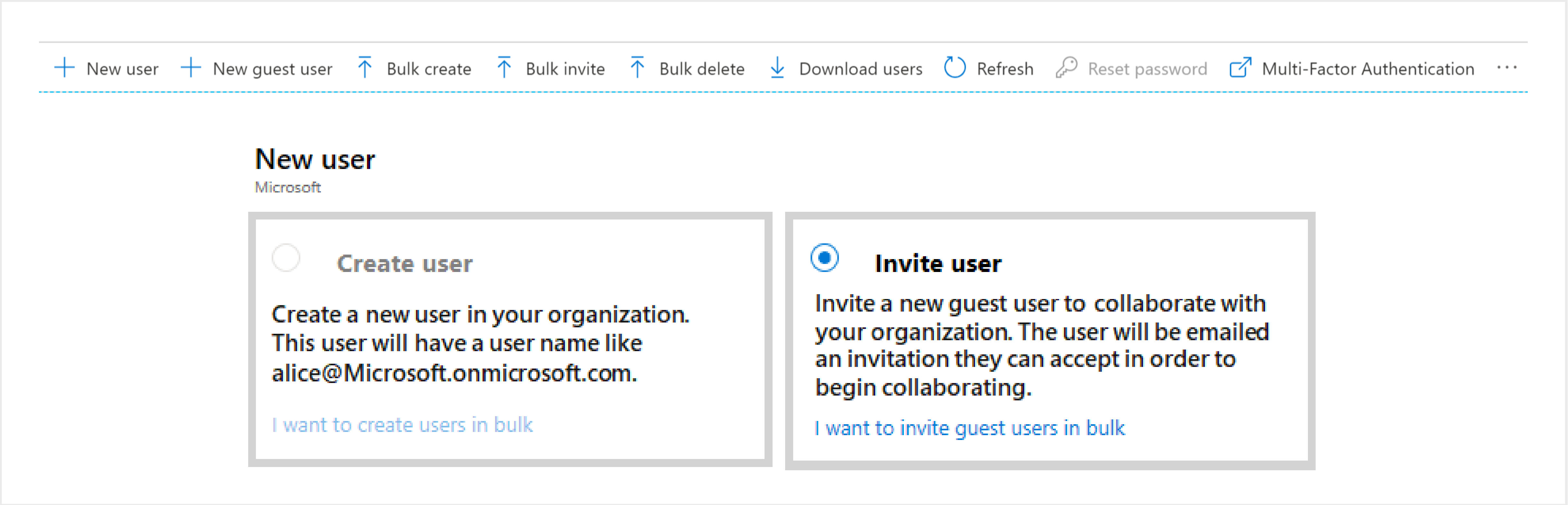
NAME	USER NAME	USER TYPE	SOURCE
Retail Crisis Notifications	[redacted]@microsoft.com	Member	Windows Server AD
"Planning & Launch Services OEM Inquiries	[redacted]@microsoft.com		Windows Server AD
' Bert	[redacted]@hotmail.com	Guest	Azure Active Directory
[redacted]@fi.pwc.com	[redacted]@fi.pwc.com	Guest	Azure Active Directory

All users must have an account

The account is used for authentication and authorization

Identity Sources: Cloud, Directory-synchronized, and Guest

Managing User Accounts



New user

Microsoft

○ Create user

Create a new user in your organization. This user will have a user name like alice@Microsoft.onmicrosoft.com.

I want to create users in bulk

● Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

I want to invite guest users in bulk

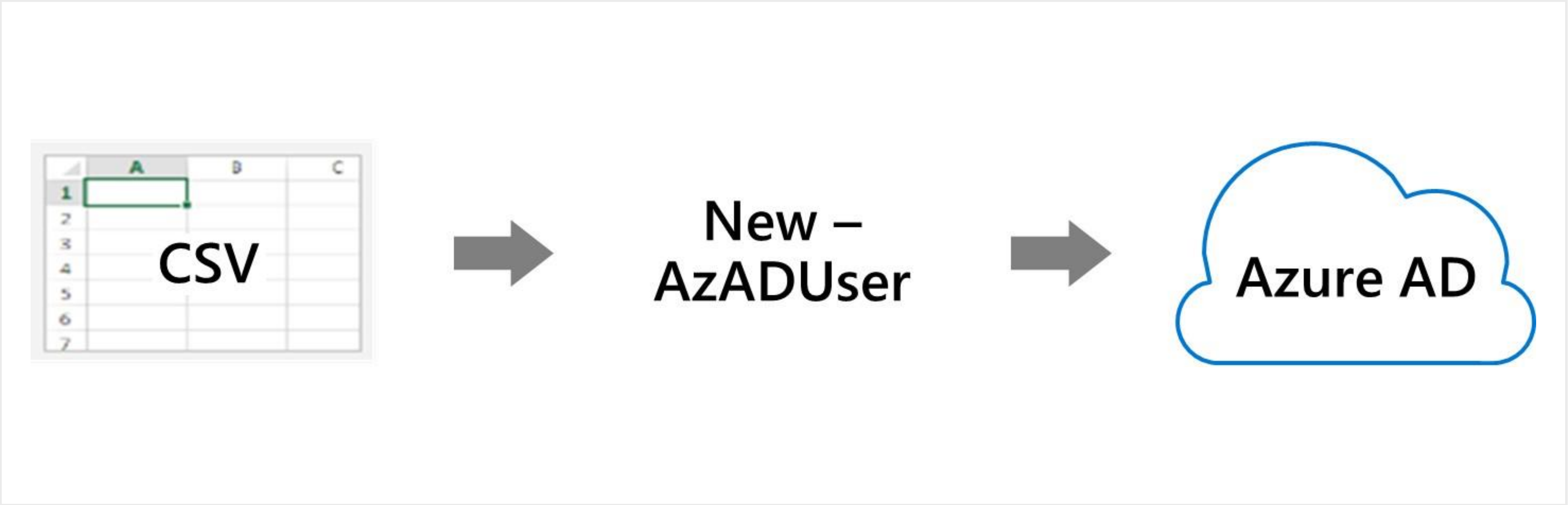
Must be Global Administrator or User Administrator to manage users

User profile (picture, job, contact info) is optional

Deleted users can be restored for 30 days

Sign in and audit log information is available

Bulk User Accounts

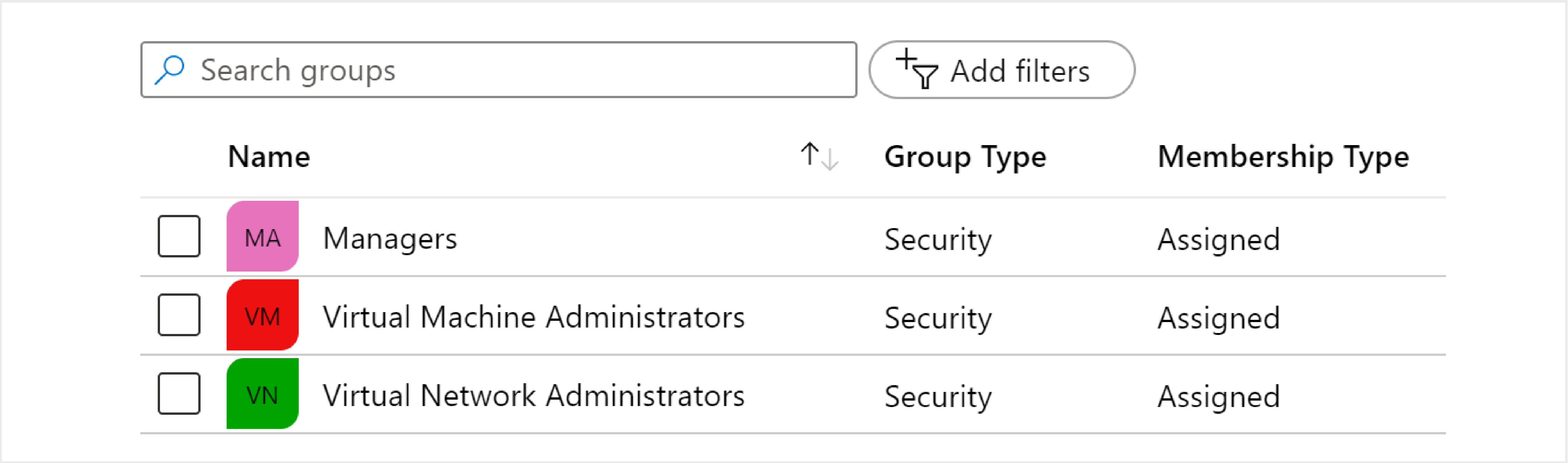


Create the comma-separated values (CSV) file with the list of all the users and their properties

Loop through the file processing each user

Consider error handling, duplicate users, initial password settings, empty properties, and when the account is enabled

Group Accounts



		Name	Group Type	Membership Type
☐	MA	Managers	Security	Assigned
☐	VM	Virtual Machine Administrators	Security	Assigned
☐	VN	Virtual Network Administrators	Security	Assigned

Group Types

- Security groups
- Microsoft 365 groups

Assignment Types

- Assigned
- Dynamic User
- Dynamic Device (Security groups only)

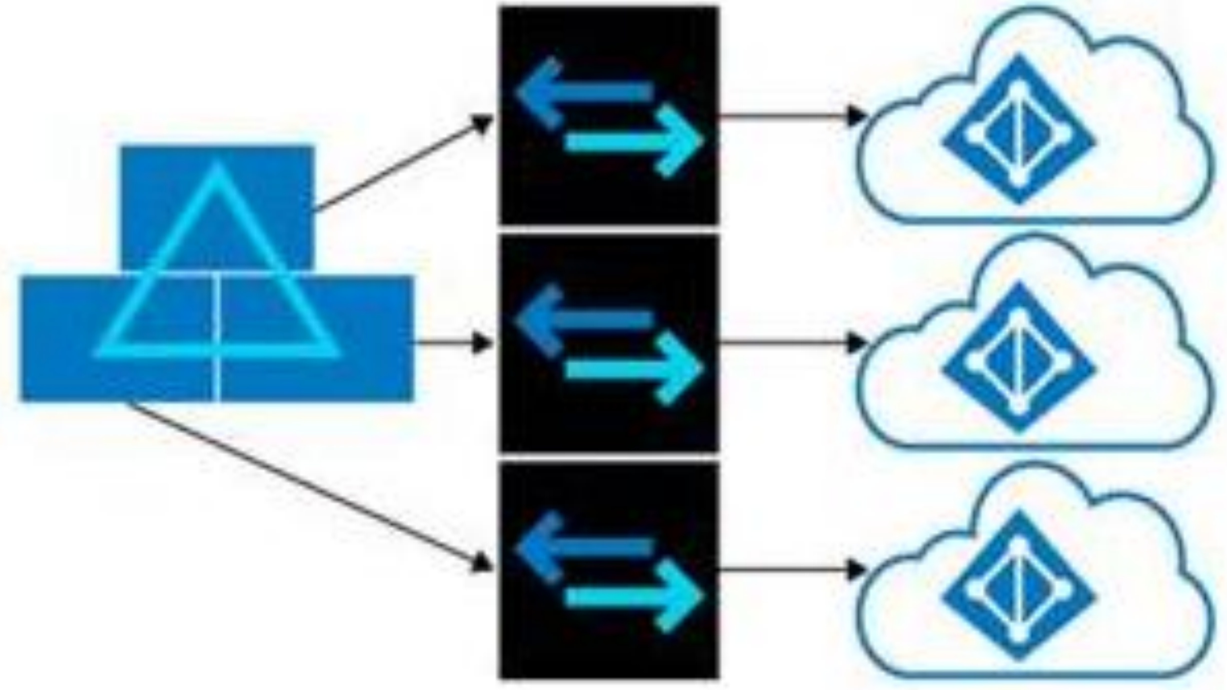
Managing Multiple Directories

Each Azure AD organization is fully independent: a peer that is logically independent from the other Azure AD organizations you manage

There is no parent-child relationship between organizations

Independence includes:

- Resource independence
- Administration independence
- Synchronization independence



Knowledge Checks (5 min)

Knowledge Check

Question: Which choice correctly describes Microsoft Entra ID?

a) Microsoft Entra ID can be queried through LDAP.
b) Microsoft Entra ID is primarily an identity solution.
c) Microsoft Entra ID uses organizational units (OUs) and group policy objects (GPOs).

Knowledge Check

Question: Which choice correctly describes Microsoft Entra ID?

a) Microsoft Entra ID can be queried through LDAP.
b) Microsoft Entra ID is primarily an identity solution.
c) Microsoft Entra ID uses organizational units (OUs) and group policy objects (GPOs).

Knowledge Check

Question: What term defines a dedicated and trusted instance of Microsoft Entra ID?

a) Azure tenant
b) Identity
c) Microsoft Entra account

Knowledge Check

Question: What term defines a dedicated and trusted instance of Microsoft Entra ID?

a) Azure tenant
b) Identity
c) Microsoft Entra account

Knowledge Check

Question: Which is true about Microsoft Entra ID?

a) Microsoft Entra ID includes federation services.
b) Microsoft Entra ID uses Kerberos authentication.
c) Microsoft Entra ID organizes users and groups into organization units.

Knowledge Check

Question: Which is true about Microsoft Entra ID?

a) Microsoft Entra ID includes federation services.
b) Microsoft Entra ID uses Kerberos authentication.
c) Microsoft Entra ID organizes users and groups into organization units.

Lesson 03: Module 01 Lab and Review

Lab 01 – Manage Azure Active Directory identities

Lab scenario

In order to allow Contoso users to authenticate by using Azure AD, you have been tasked with provisioning users and group accounts. Membership of the groups should be updated automatically based on the user job titles. You also need to create a test Azure AD tenant with a test user account and grant that account limited permissions to resources in the Contoso Azure subscription.

Objectives

Task 1:
Create and configure Azure AD users

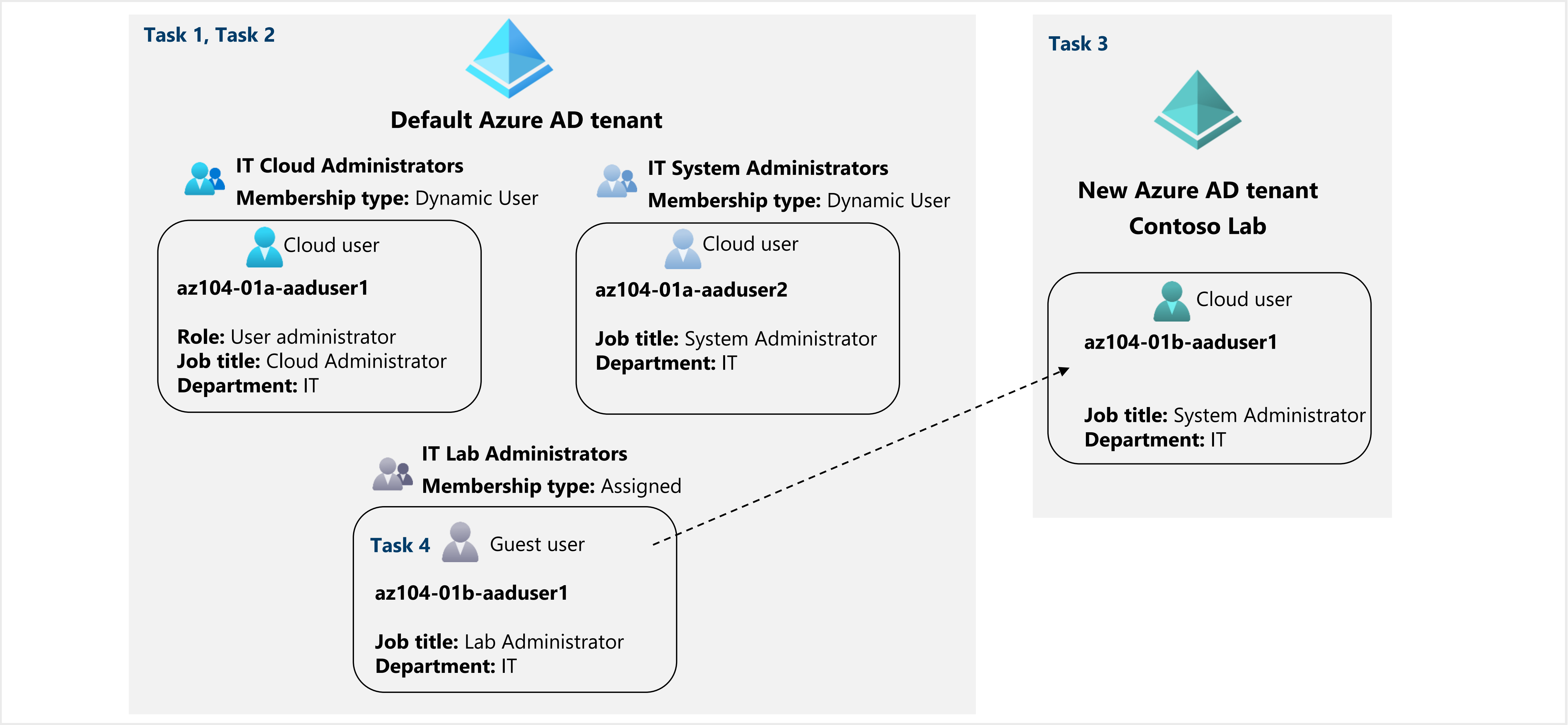
Task 2:
Create Azure AD groups with assigned and dynamic membership

Task 3:
Create an Azure Active Directory (AD) tenant

Task 4:
Manage Azure AD guest users

Next slide for an architecture diagram →

Lab 01 – Architecture diagram



Task 1, Task 2

Default Azure AD tenant

IT Cloud Administrators
Membership type: Dynamic User

Cloud user

az104-01a-aaduser1

Role: User administrator
Job title: Cloud Administrator
Department: IT

IT System Administrators
Membership type: Dynamic User

Cloud user

az104-01a-aaduser2

Job title: System Administrator
Department: IT

IT Lab Administrators
Membership type: Assigned

Task 4

Guest user

az104-01b-aaduser1

Job title: Lab Administrator
Department: IT

Task 3

New Azure AD tenant
Contoso Lab

Cloud user

az104-01b-aaduser1

Job title: System Administrator
Department: IT

Module Review

Module Review Questions

Microsoft Learn Modules (docs.microsoft.com/Learn)

Create Azure users and groups in Azure Active Directory

Manage users and groups in Azure Active Directory

Secure Azure Active Directory users with Multi-Factor Authentication

Allow users to reset their password with Azure Active Directory self-service password reset

Secure your application by using OpenID Connect and Azure AD

End of presentation