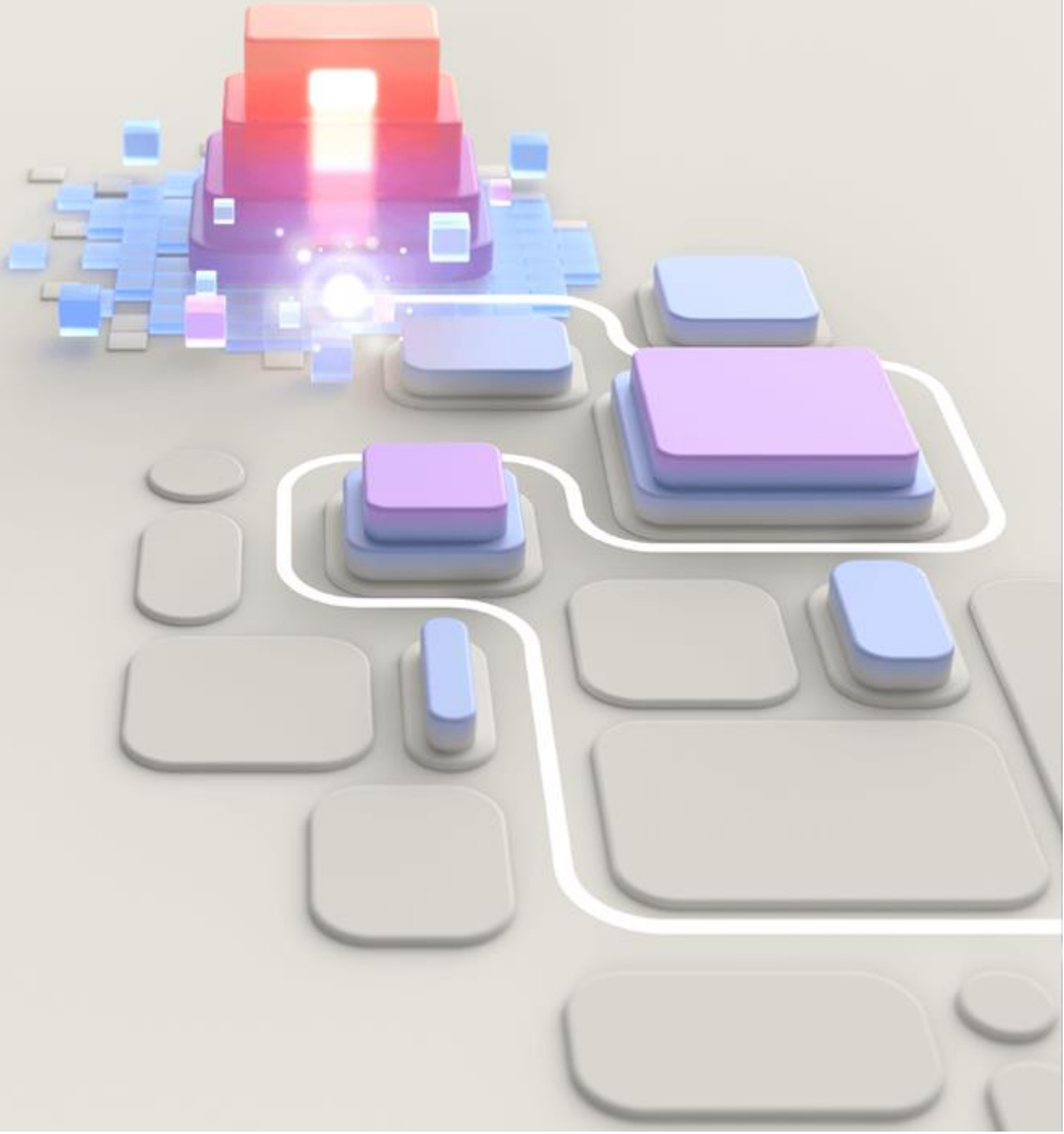
Microsoft

AZ-104

Administer Identity

Entra ID



AZ-104 Course Outline

01: Administer Identity ← RBAC

02: Administer Governance and Compliance ← RBAC , Policy

03: Administer Azure Resources

04: Administer Virtual Networking

05: Administer Intersite Connectivity

06: Administer Network Traffic Management

07: Administer Azure Storage

08: Administer Azure Virtual Machines

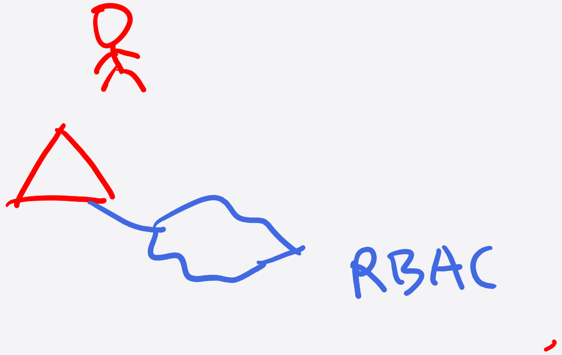
09: Administer PaaS Compute Options

10: Administer Data Protection

11: Administer Monitoring

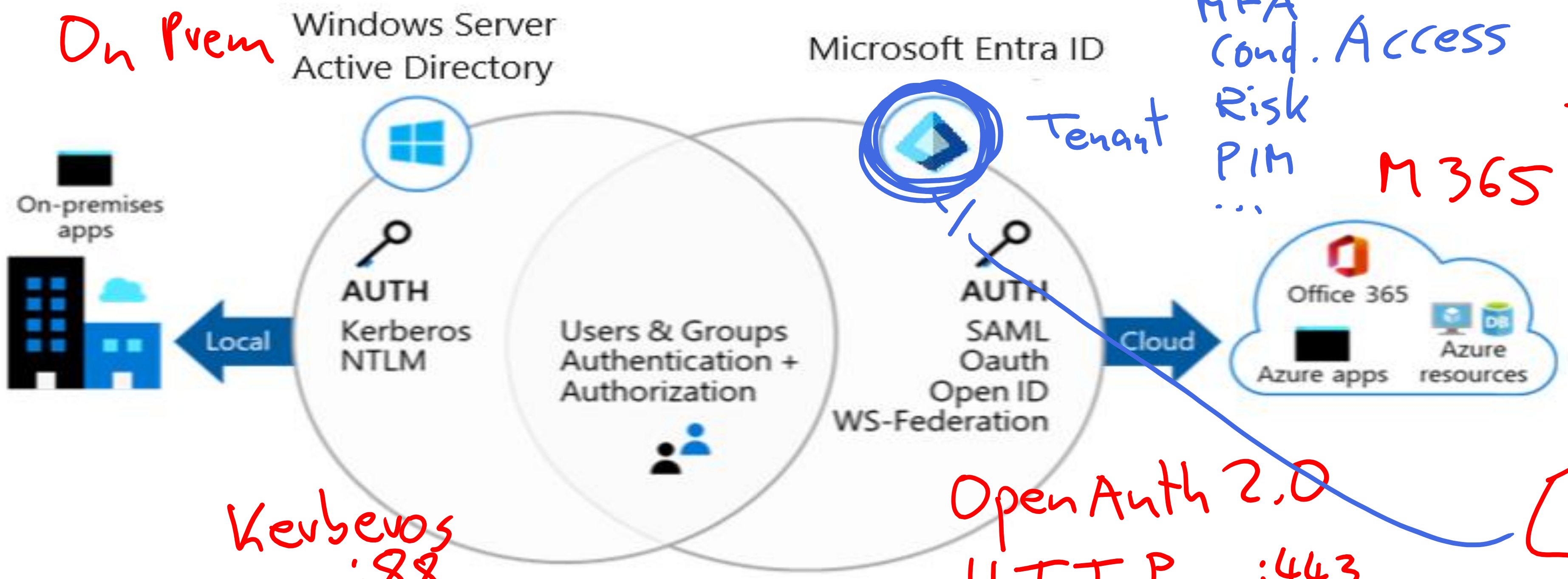
Learning Objectives

- Understand Microsoft Entra ID
- Configure User and Group Accounts
- Lab 01 - Manage Microsoft Entra ID Identities



Understand Microsoft Entra ID

Examine Microsoft Entra ID



On Prem

Authentication
MFA
Cond. Access
Risk
PIM
...

Tenant

Authorization

M 365

Kerberos
:88

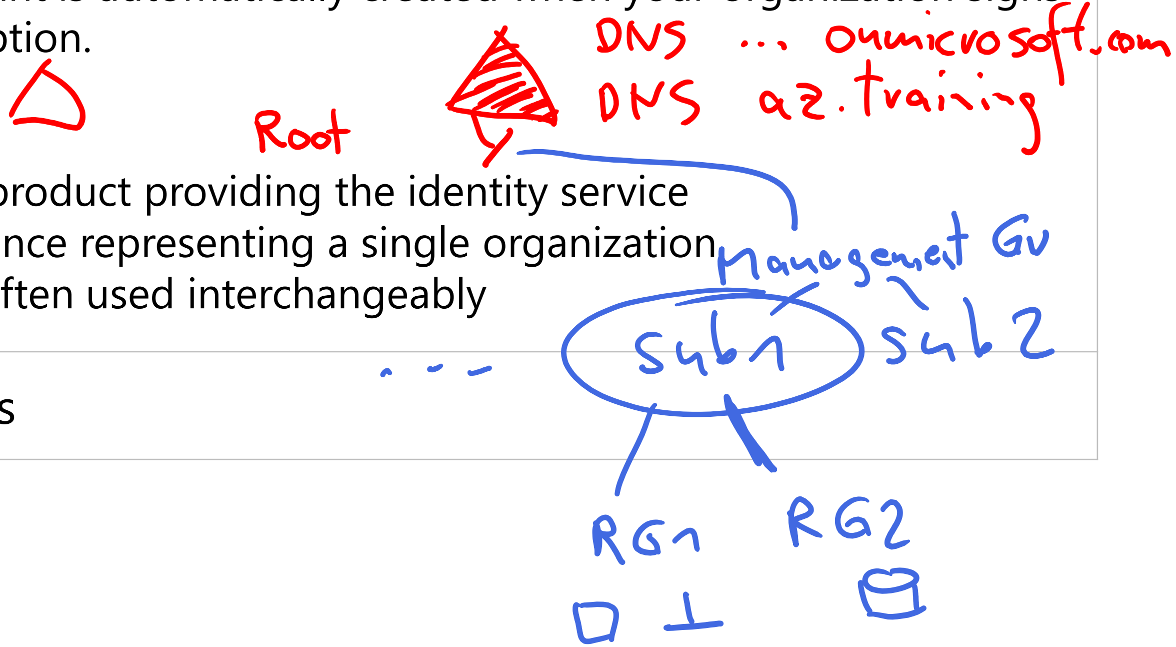
Open Auth 2.0
HTTP :443

Azure

- Configure access to applications, including single sign-on
- Manage and provision users and groups
- Providing an identity management solution, including federation
- Implement security features like multi-factor authentication and conditional access

Describe Microsoft Entra ID Concepts

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



AD - DS (DCs , GPOs)

Compare Microsoft Entra ID to Active Directory Domain Services

On Prem

- Microsoft Entra ID is primarily an identity solution

SKU

- Queried using the REST API over HTTP and HTTPS
- Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization)
- Includes federation services, and many third-party services (such as Facebook)
- Microsoft Entra ID users and groups are created in a flat structure, and there are no Organizational Units (OUs) or Group Policy Objects (GPOs)

X X

AU

Compare Microsoft Entra ID P1 and P2 plans

Lizenz
E3
E5

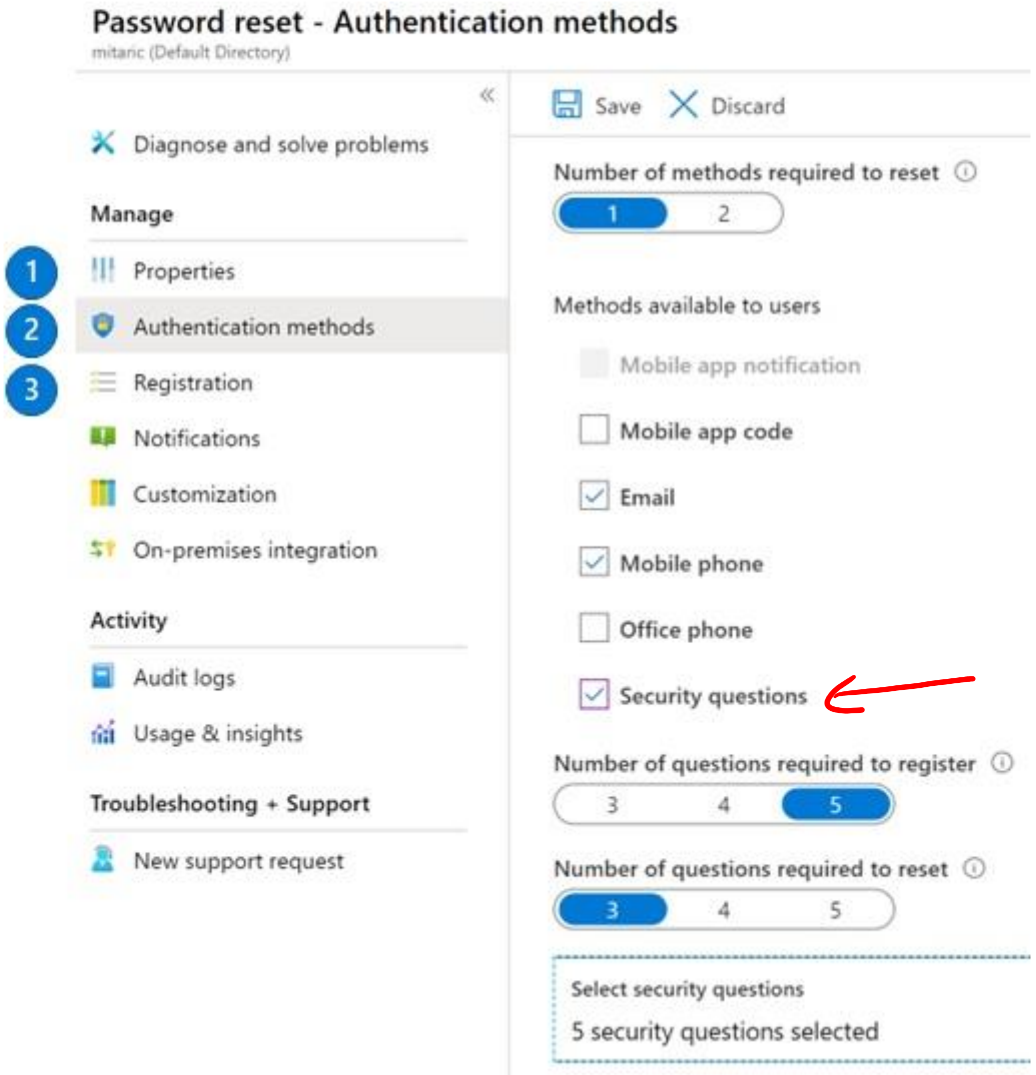
Feature	Free	P1	P2	Governance
Single Sign-On (unlimited)	✓	✓	✓	
Cloud and Federated authentication	✓	✓	✓	
Advanced group management		✓	✓	
Self-service account management portal	✓	✓	✓	
Multifactor authentication (MFA)	✓	✓	✓	
Conditional access		✓	✓	
Risk-based Conditional Access (sign-in risk, user risk)			✓	
Automated user and group provisioning to apps		✓	✓	✓
Privileged identity management (PIM)			✓	✓

What is self-service password reset in Microsoft Entra ID?

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)

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

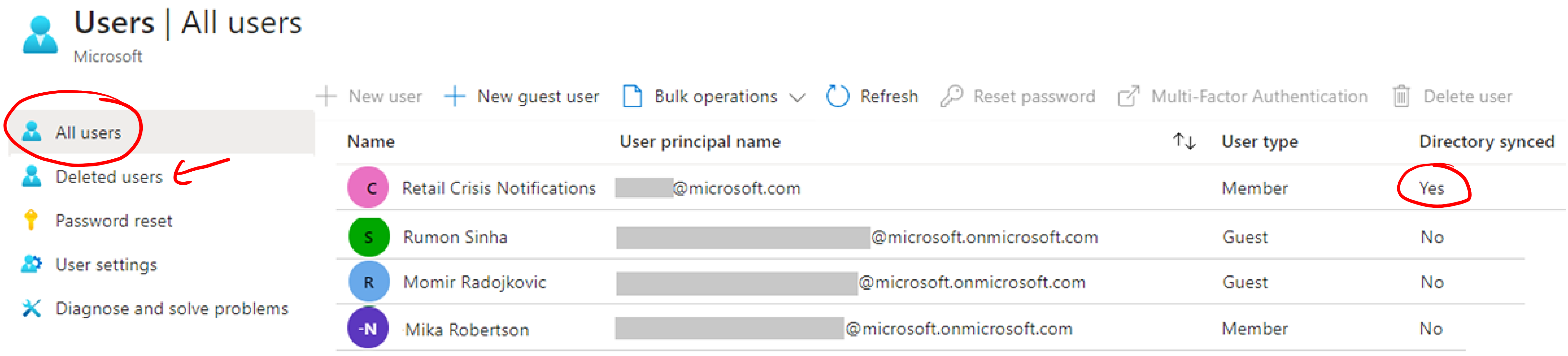
Learning Recap – Understand Microsoft Entra ID

Check your knowledge questions and additional study

- Understand Microsoft Entra ID
- Allow users to reset their password with self-service password reset
- Implement and manage hybrid identity

Configure User and Group Accounts

Create User Accounts



Name	User principal name	User type	Directory synced
Retail Crisis Notifications	[redacted]@microsoft.com	Member	Yes
Rumon Sinha	[redacted]@microsoft.onmicrosoft.com	Guest	No
Momir Radojkovic	[redacted]@microsoft.onmicrosoft.com	Guest	No
Mika Robertson	[redacted]@microsoft.onmicrosoft.com	Member	No

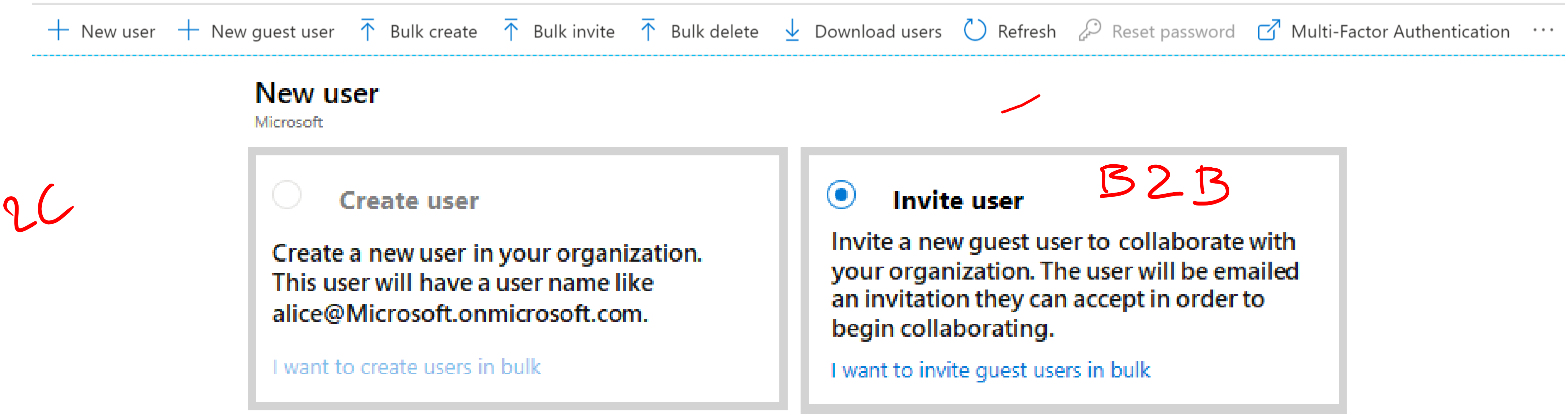
All users must have an account

The account is used for authentication and authorization

Each user account has additional properties

Manage User Accounts

IdP Authentication → Access Token → IdP Tenant ✓



+ New user   + New guest user   Bulk create   Bulk invite   Bulk delete   Download users   Refresh   Reset password   Multi-Factor Authentication   ···

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

B2C

B2B

Must be Global Administrator or User Administrator to manage users

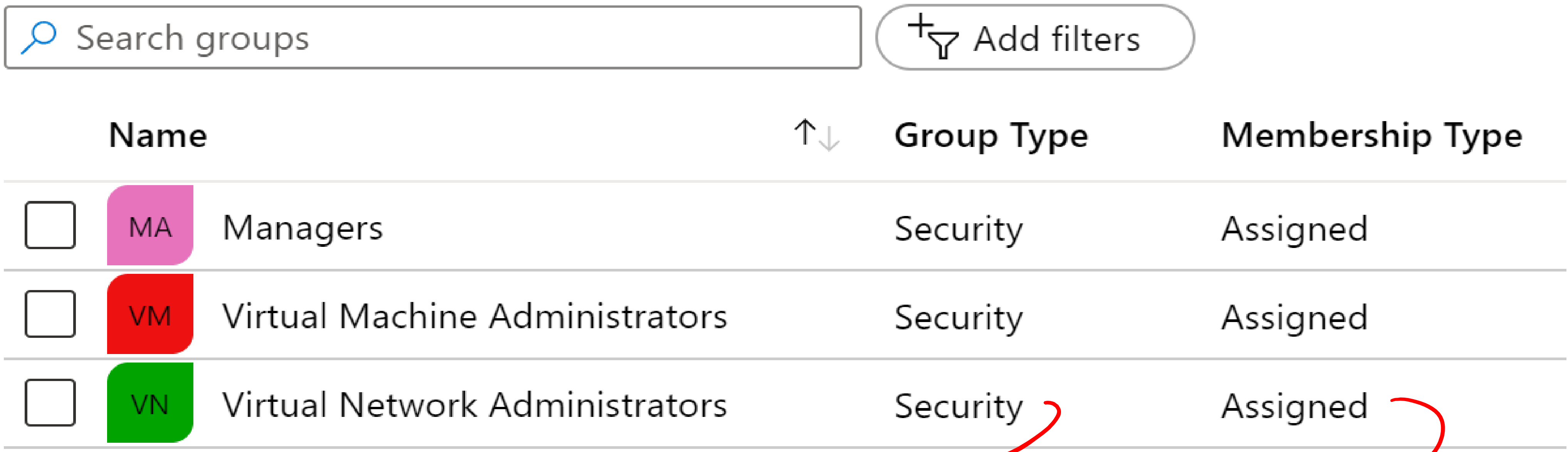
User profile (picture, job, contact info) is optional

Deleted users can be restored for 30 days

Sign in and audit log information is available

Create Group Accounts

3



	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

Membership Types

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

Assign Licenses to Users and Groups

Azure is a cloud service that provides many built-in services for free.

- Microsoft Entra ID comes as a free service
- Gain additional functionality with a P1 or P2 license

Additional Services (like O365 are paid cloud services)

- Microsoft paid cloud services require licenses
- Licenses are assigned to those who need access to the services
- Each user or group requires a separate paid license
- Administrators use management portals and PowerShell cmdlets to manage licenses

❑ View license plans and plan details

❑ Set the Usage Location parameter

❑ Assign licenses to users and groups

❑ Change license plans for users and groups

❑ Remove a license

Demonstration – Users and Groups

- Review license and domain information
- Explore user accounts
- Explore group accounts

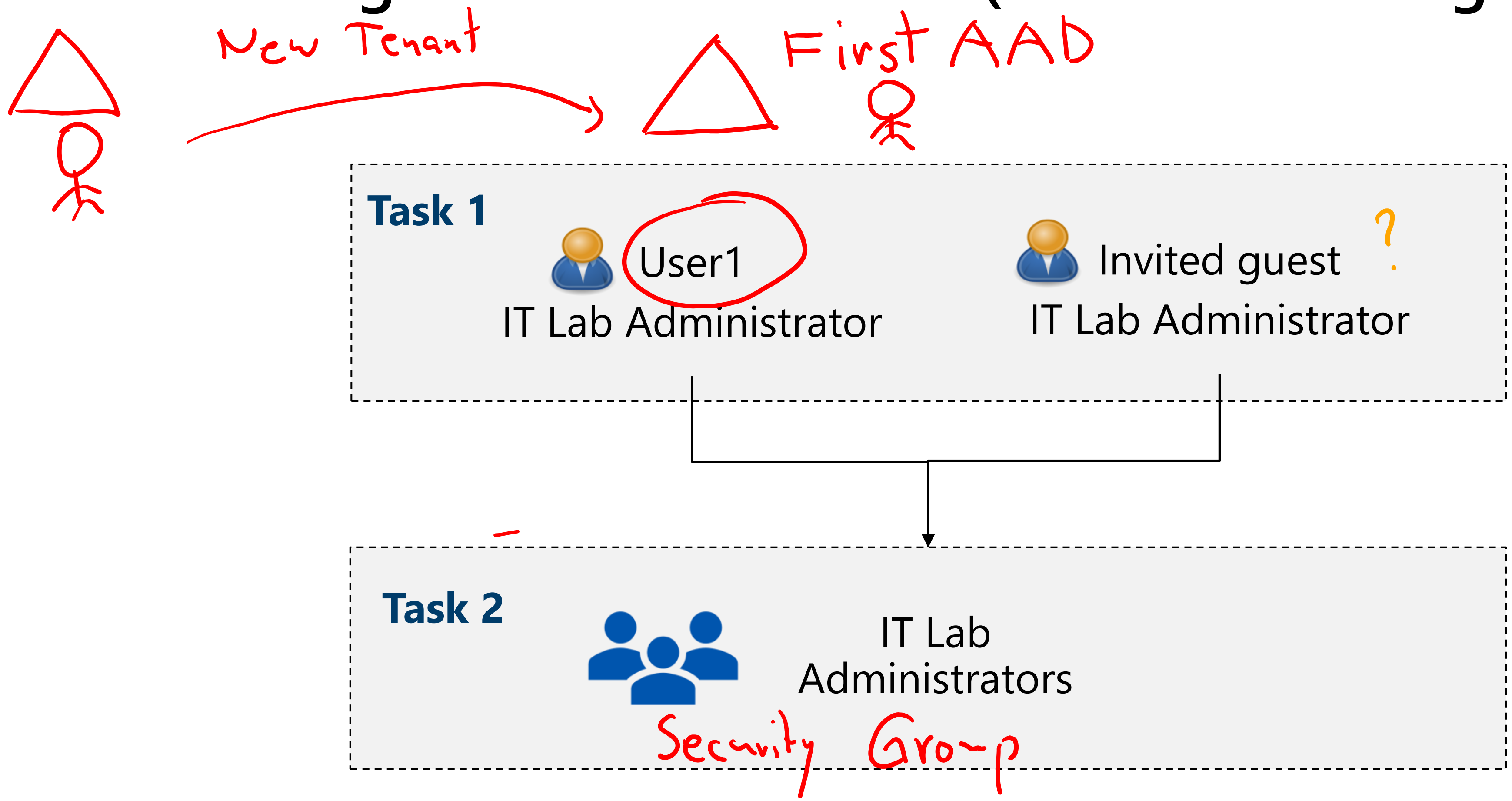
Learning Recap – Configure User and Group Accounts

Check your knowledge questions and additional study

- Create Azure users and groups in Microsoft Entra ID
- Manage users and groups

Lab – Manage Entra ID Identities

Lab 01 – Manage Entra ID Identities (architecture diagram)



New Tenant

First AAD

Task 1

User1

IT Lab Administrator

Invited guest ?

IT Lab Administrator

Task 2

IT Lab Administrators

Security Group

End of presentation