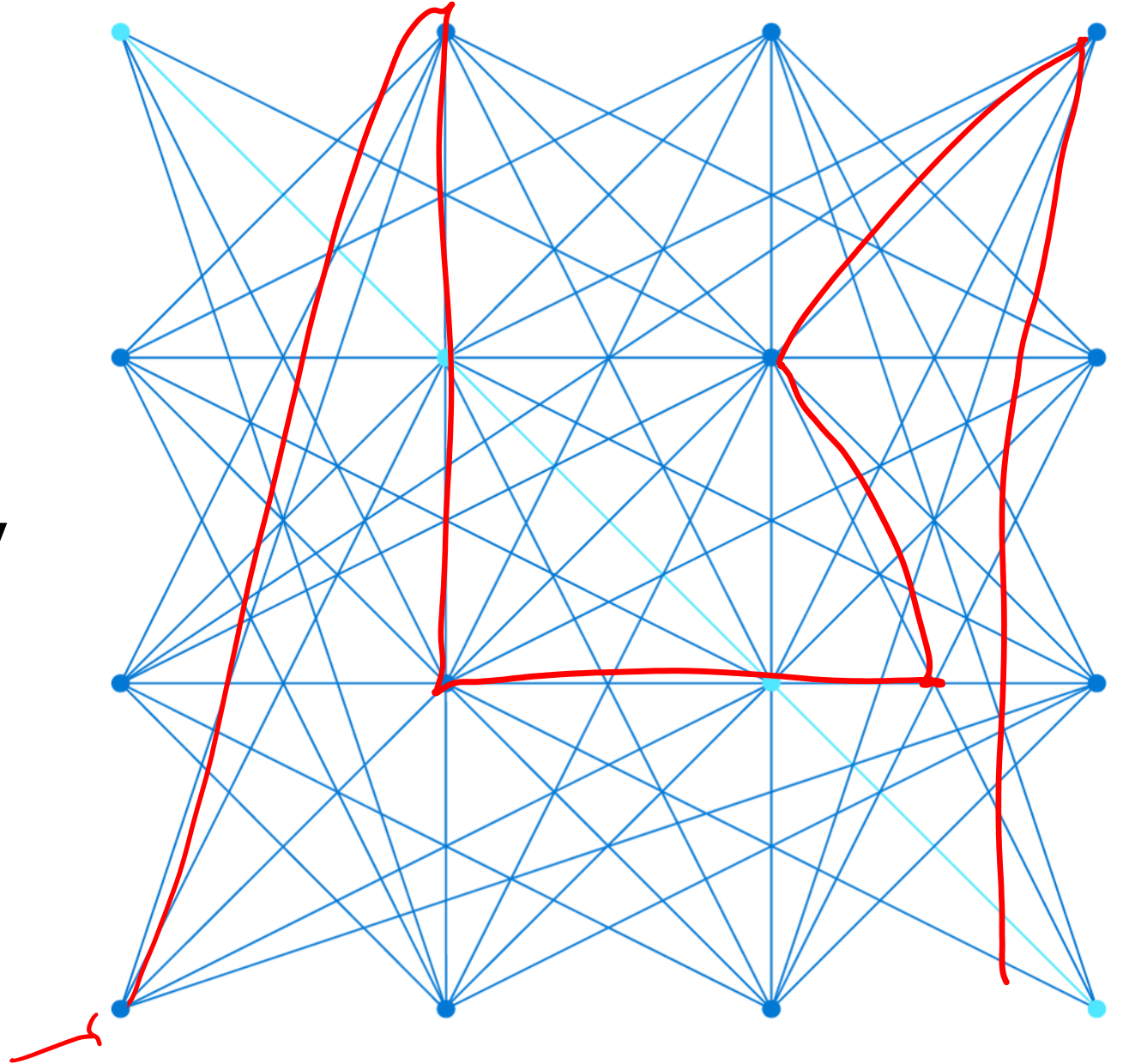
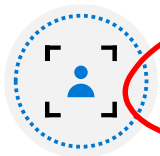
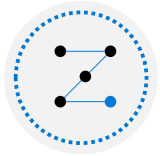

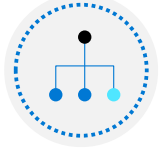
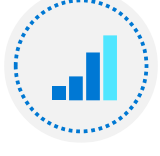

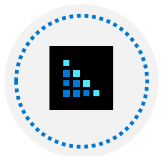
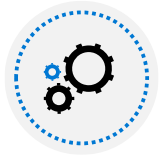


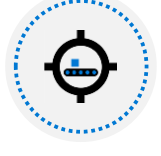


AZ-104

Administer Identity



About this course: Course Outline

-  01: Administer Identity *Entra ID*
AAA Authentication
-  02: Administer Governance and Compliance *Policies Roles RBAC*
-  03: Administer Azure Resources *Portal*
-  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

Administer Identity Introduction

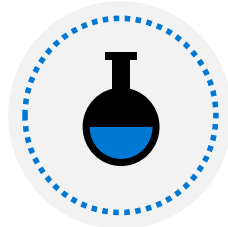
Entra ID



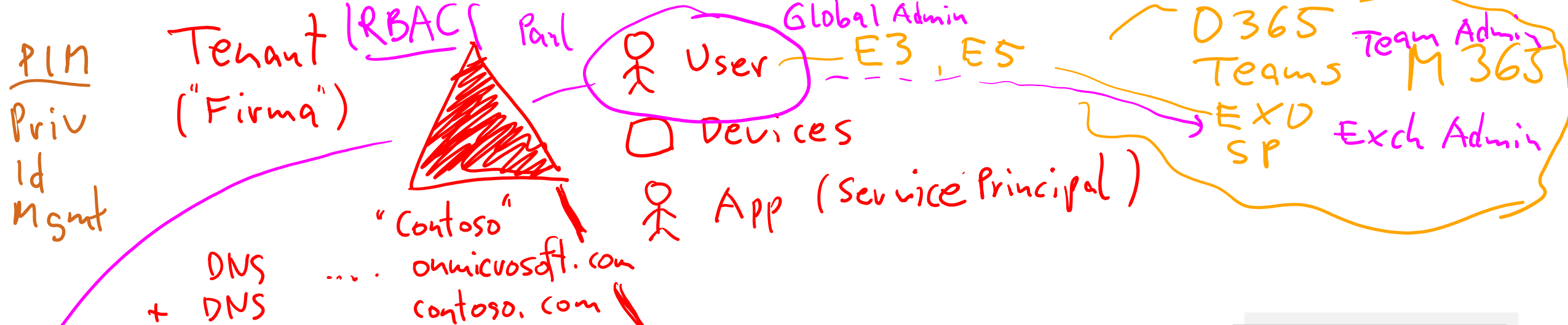
[Configure Azure Active Directory](#)



[Configure User and Group Accounts](#)

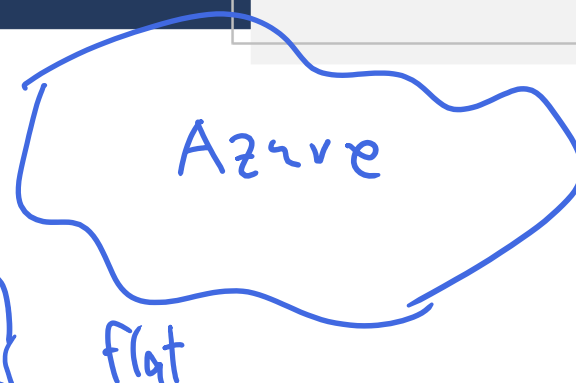
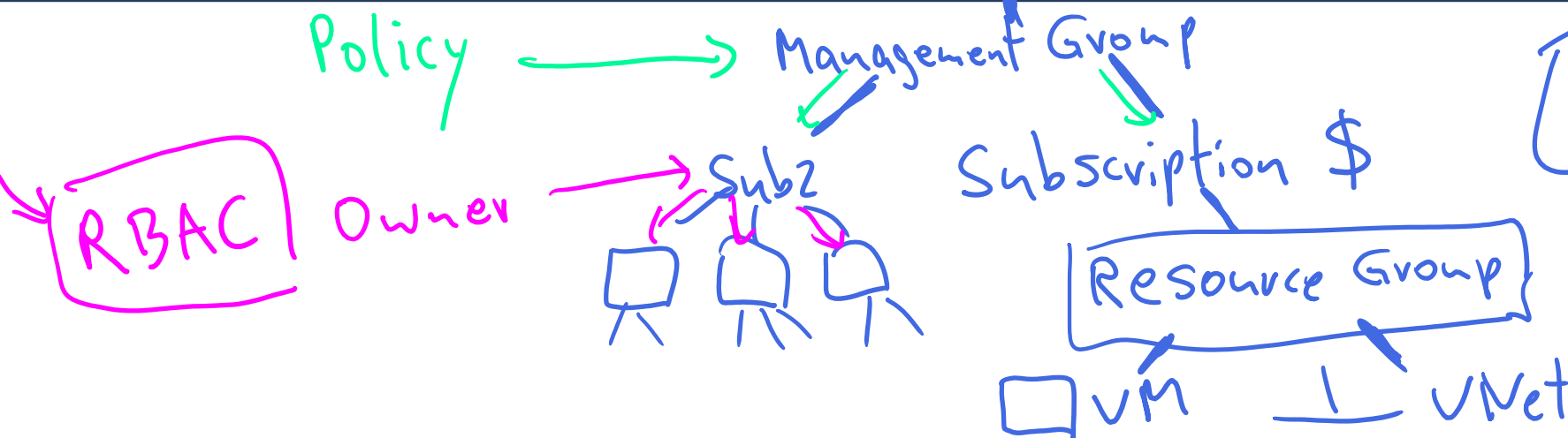
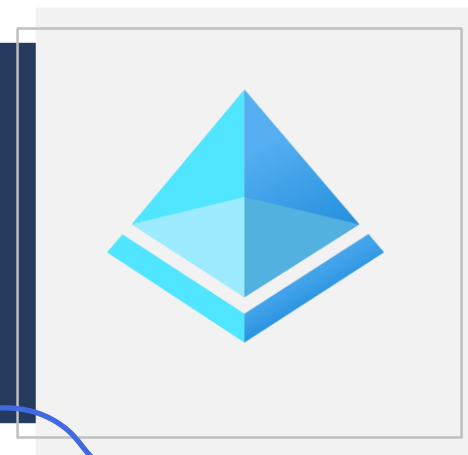


[Lab 01 - Manage Azure Active Directory Identities](#)

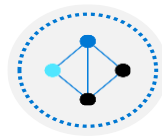


Configure Azure Active Directory

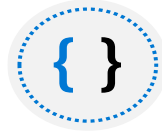
Root Management Group



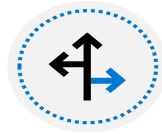
Configure Azure Active Directory Introduction



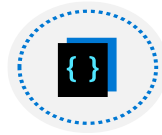
Describe Azure Active Directory Benefits and Features



Compare AD DS to Azure Active Directory

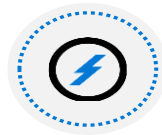


Describe Azure AD Concepts



Select Azure AD Editions

Free
0365 (Free)
P1
P2



Implement Azure AD Device Identities (optional)



Implement Self-Service Password Reset

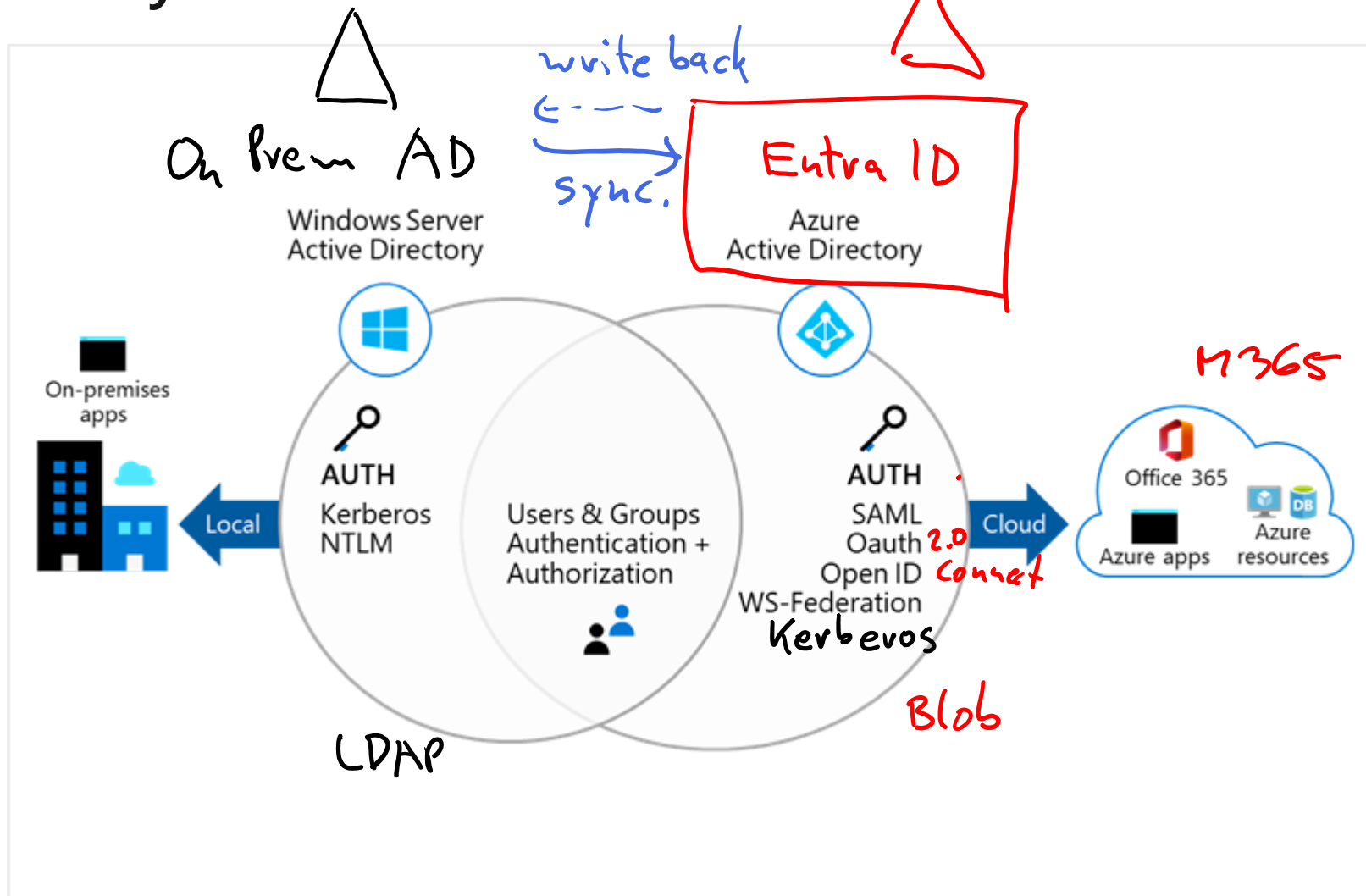


Summary and Resources

Describe Azure Active Directory Benefits and Features

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



Describe Azure AD Concepts

Concept	Description
Identity	An object that can be authenticated
Account	An identity that has data associated with it
Azure AD account	An identity created through Azure AD or another Microsoft cloud service
Azure AD tenant/directory	<p>A dedicated and trusted instance of Azure AD, a Tenant is automatically created when your organization signs up for a Microsoft cloud service subscription</p> <ul style="list-style-type: none">• Additional instances of Azure AD can be created• Azure AD is the underlying product providing the identity service• The term <i>Tenant</i> means a single instance of Azure AD representing a single organization• The terms <i>Tenant</i> and <i>Directory</i> are often used interchangeably
Azure subscription	Used to pay for Azure cloud services

On Prem

Compare AD DS to Azure Active Directory



Azure AD is primarily an 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)

Select Azure Active Directory Editions

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	<u>500,000 objects</u>	No object limit	No object limit	No object limit
Single Sign-On	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Premium Features			X	X
Hybrid Identities (full capabilities)			X	X
Advanced Group Management			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

PIM
Access Package

Implement 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

Save Discard

Diagnose and solve problems

Manage

- 1 Properties
- 2 **Authentication methods**
- 3 Registration
- Notifications
- Customization
- On-premises integration

Activity

- Audit logs
- Usage & insights

Troubleshooting + Support

- New support request

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

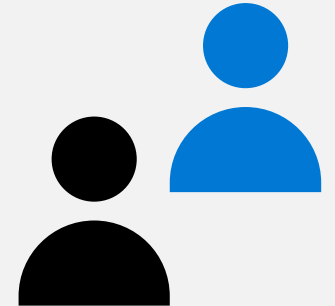
Number of questions required to reset ⓘ

3 4 5

Select security questions

5 security questions selected

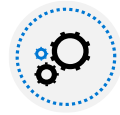
Configure User and Group Accounts



Configure User and Group Accounts Introduction



Create User Accounts



Manage User Accounts



Create Bulk Accounts (optional)



Create Group Accounts



Assign Licenses to Users and Groups (extra topic)



Create Administrative Units (optional)

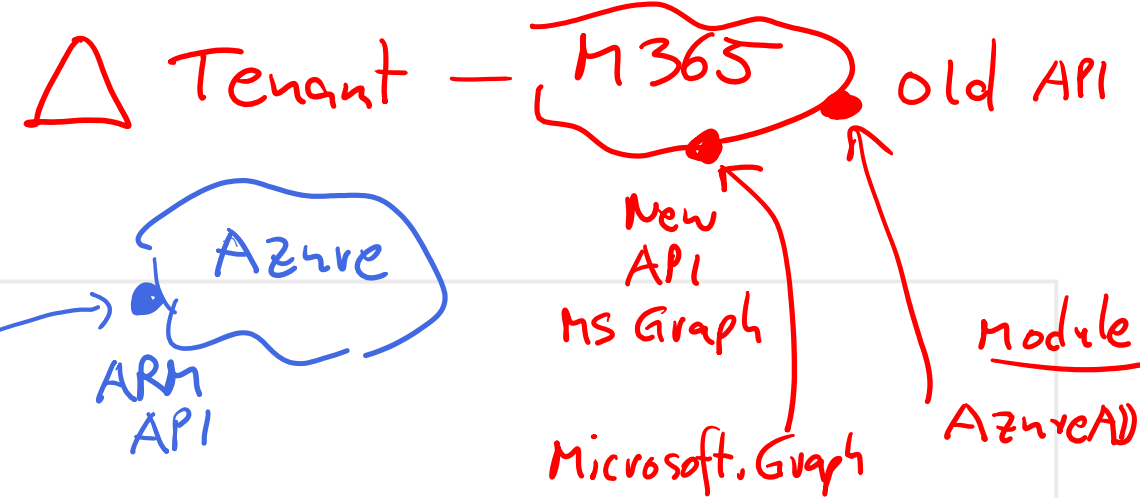


Demonstration – Users and Groups



Summary and Resources

PowerShell



Create User Accounts

module (az)
az.compute
az.*

Users | All users
Microsoft - Azure Active Directory

+ New user + New guest user Bulk operations Refresh Reset password Multi-Factor Authentication Delete user

	Name	User principal name	↑↓	User type	Directory synced
C	Retail Crisis Notifications	@microsoft.com		Member	Yes
S	Rumon Sinha	@microsoft.onmicrosoft.com		Guest	No
R	Momir Radojkovic	@microsoft.onmicrosoft.com		Guest	No
-N	Mika Robertson	@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

[+ 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](#)

B2B
Guest

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

+

Add filters

	Name	↑ ↓	Group Type	Membership Type
<input type="checkbox"/>	<div>MA</div> Managers		Security	Assigned
<input type="checkbox"/>	<div>VM</div> Virtual Machine Administrators		Security	Assigned
<input type="checkbox"/>	<div>VN</div> Virtual Network Administrators		Security	Assigned

Group Types

- Security groups ID
- Microsoft 365 groups ID + more

Assignment Types

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

Assign Licenses to Users and Groups

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

- Azure AD comes as a free service
- Gain additional Azure AD 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



Determine domain information



Explore user accounts

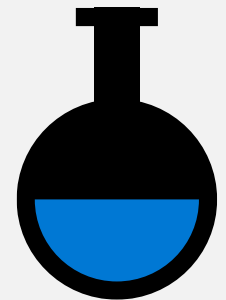


Explore group accounts



Explore PowerShell for group management

Lab 01 - Manage Azure Active Directory Identities



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:

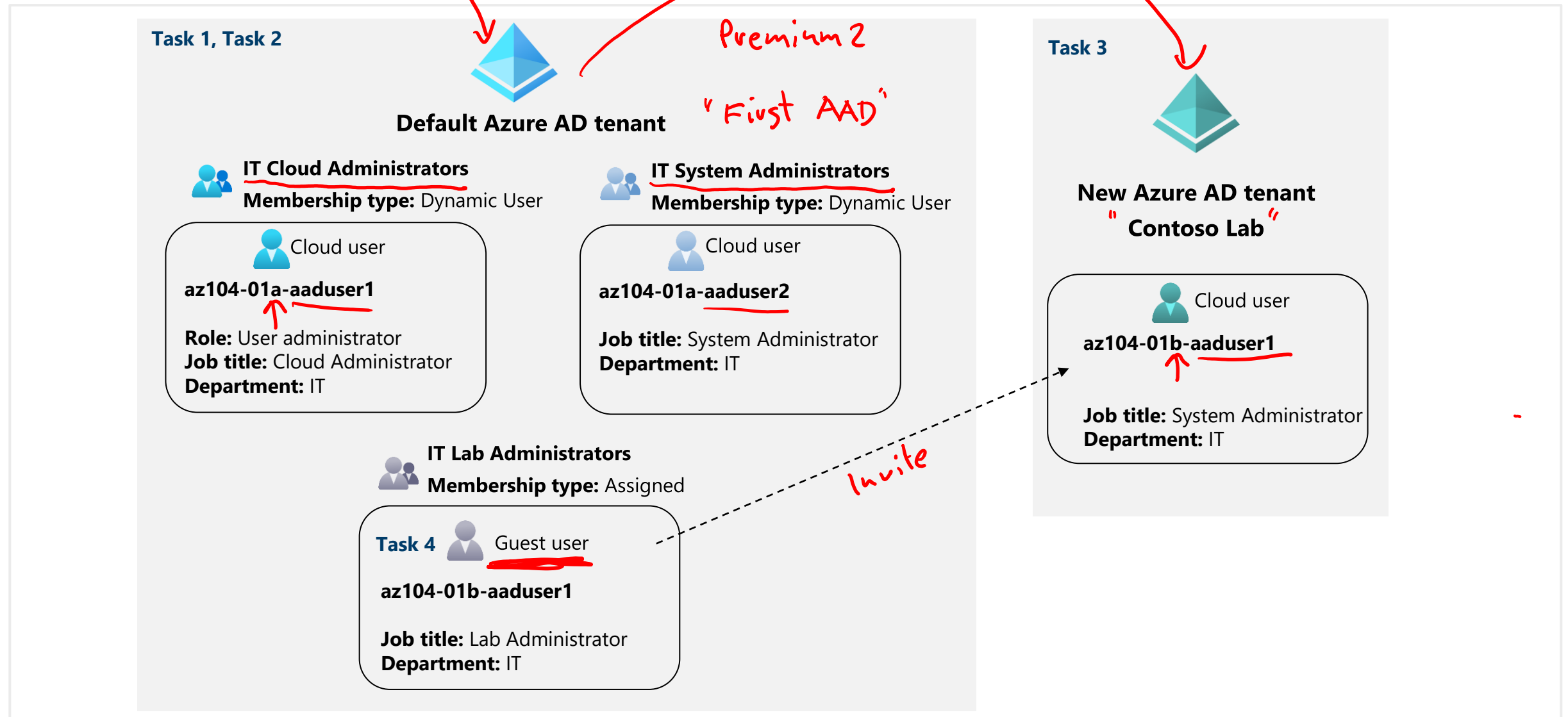
Create an Azure
Active Directory (AD)
tenant

Task 4:

Manage Azure AD
guest users

Next slide for an architecture diagram 

Lab 01 – Architecture diagram



End of presentation

