

AZ-104

Administer Identity



AZ-104 Course Outline

01: Administer Identity
02: Administer Governance and Compliance



AAA

Tods

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

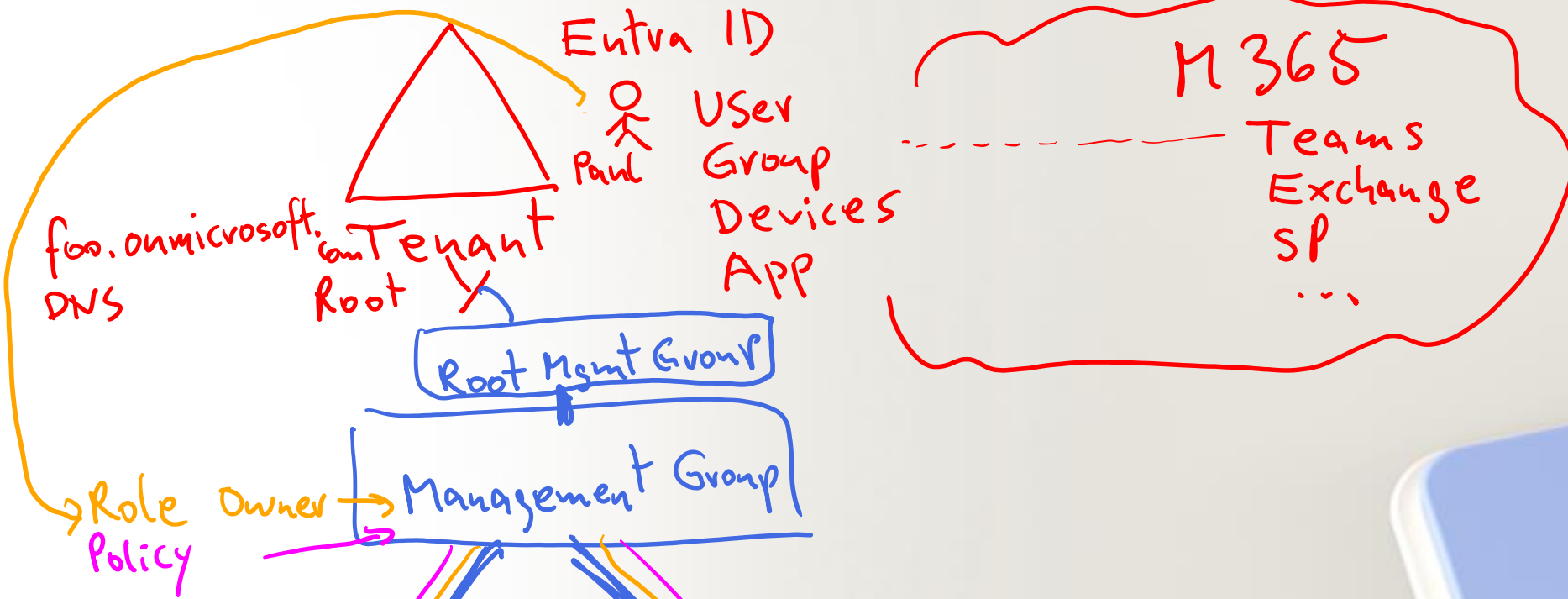
09: Administer PaaS Compute Options

10: Administer Data Protection

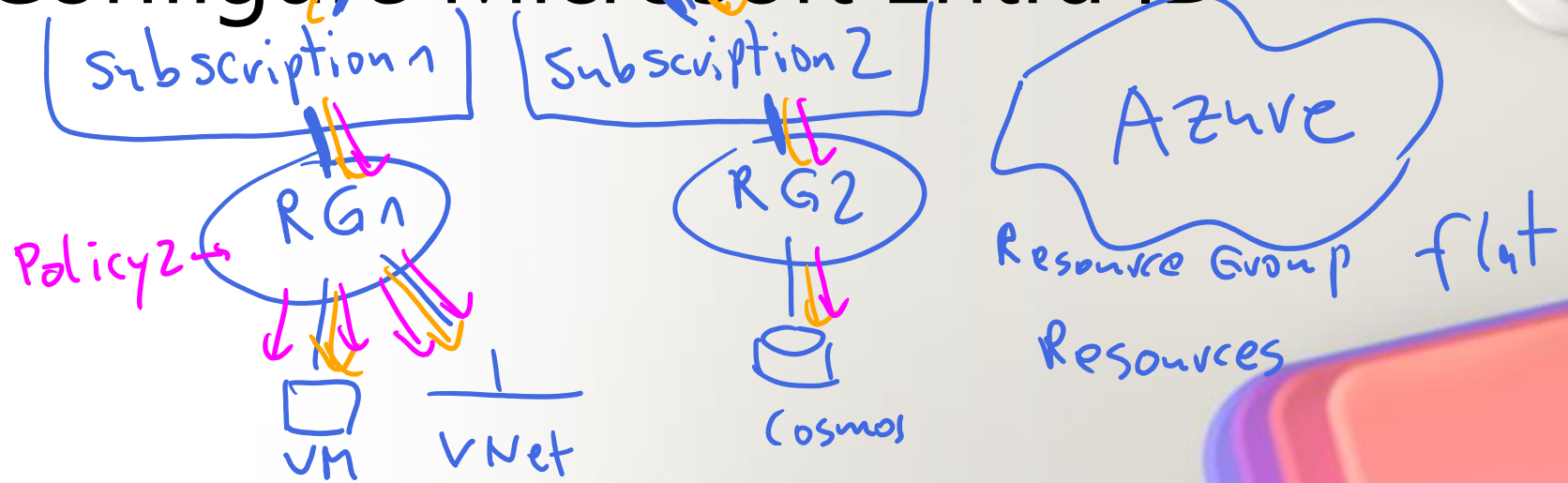
11: Administer Monitoring

Learning Objectives

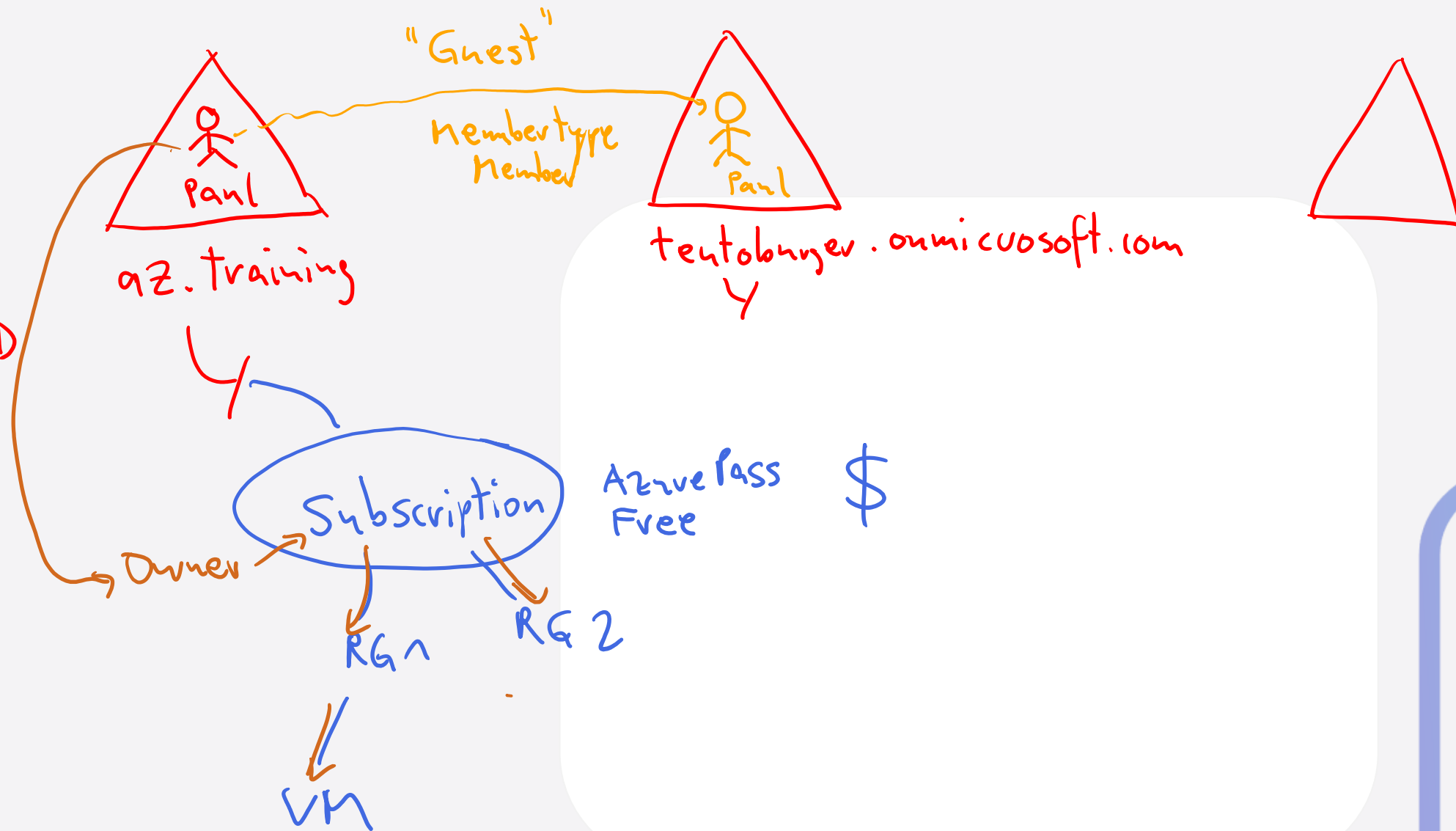
- [Configure Microsoft Entra ID](#)
- [Configure User and Group Accounts](#)
- [Lab 01 - Manage Microsoft Entra ID Identities](#)



Configure Microsoft Entra ID



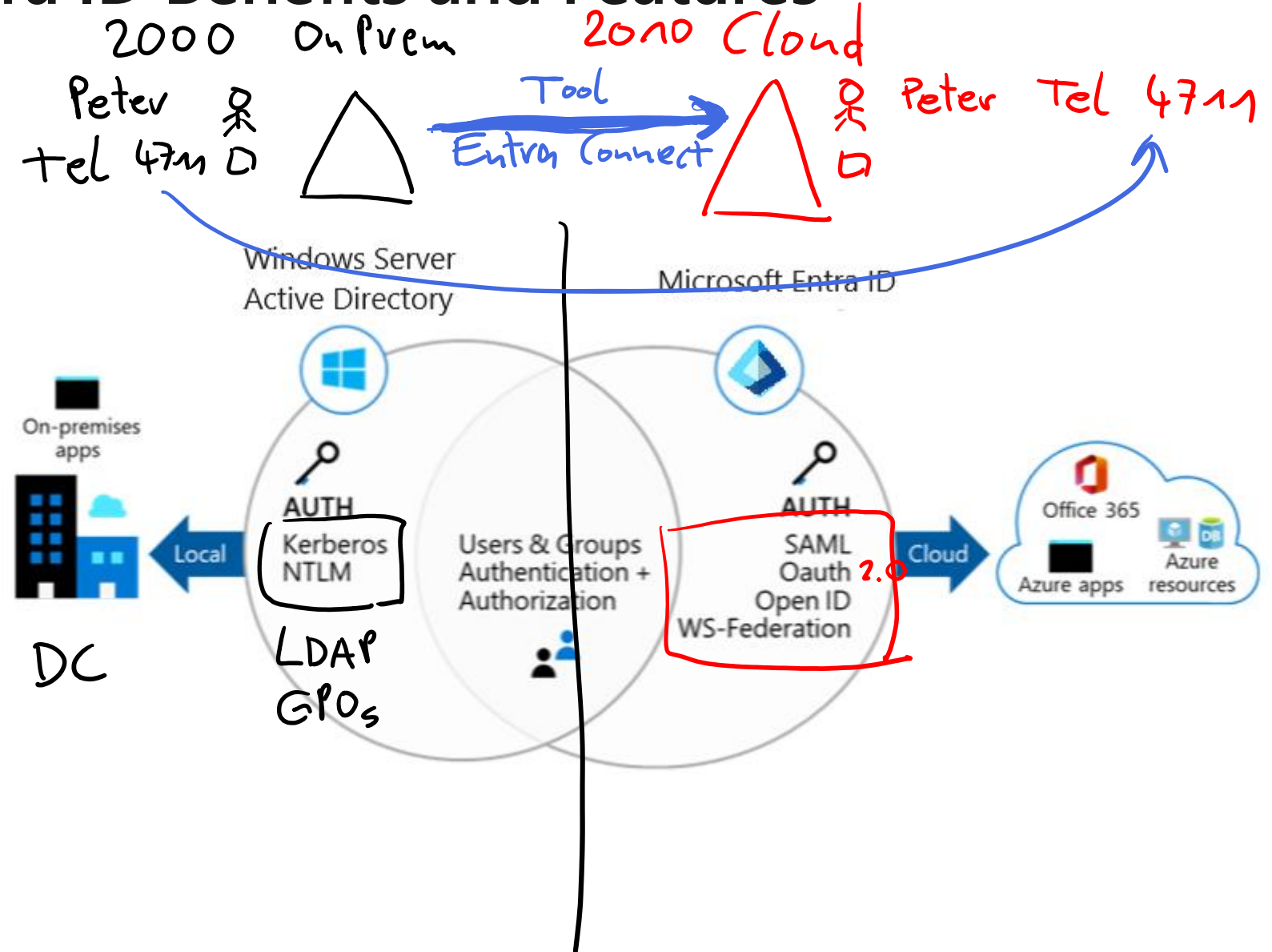
Tenants
= Directory
= Instanz von EntraID



Describe Microsoft Entra ID 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 Microsoft Entra ID Concepts

Concept	Description
Identity <i>PK ID</i>	An object that can be authenticated
Account <i>Tel</i>	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	<p>A dedicated and trusted instance. 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 can be created• Microsoft Entra ID is the underlying product providing the identity service• The term <i>Tenant</i> means a single instance representing a single organization• The terms <i>Tenant</i> and <i>Directory</i> are often used interchangeably
Azure subscription	Used to pay for <u>Azure</u> cloud services

Compare Microsoft Entra ID to Active Directory Domain Services



Microsoft Entra ID is primarily an identity solution



Queried using the REST API over HTTP and HTTPS



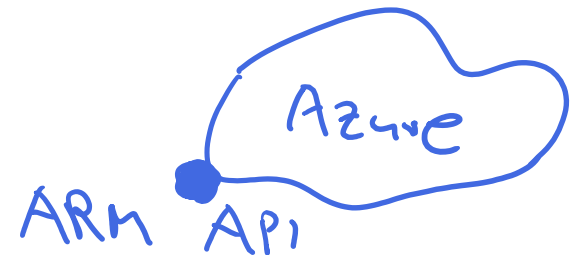
Uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization)



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



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



MSAL
(old)

Microsoft
Graph

API

OAuth

AD-DS

Kerberos

LDAP

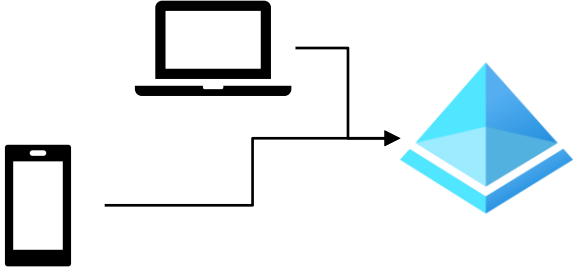
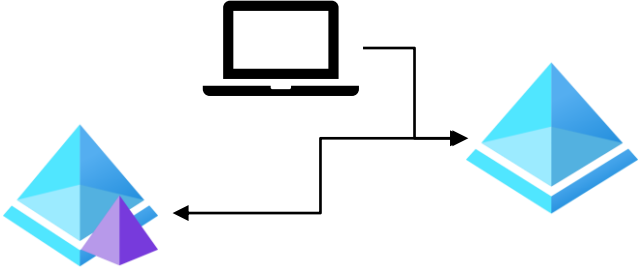
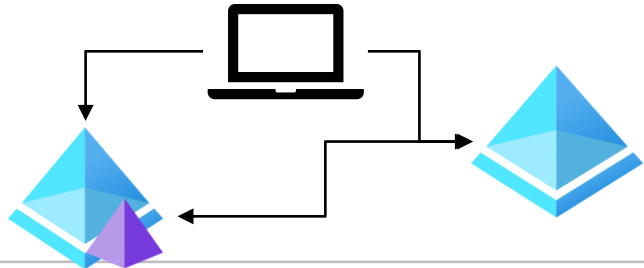
GPO

SKU

Select Microsoft Entra Plans & Pricing (examples)

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 (<u>sign-in risk, user risk</u>)			✓✓	
Automated user and group provisioning to apps		✓	✓	✓
Privileged identity management (PIM)			✓	✓

Configure Device Identities (optional)

Registered devices	Joined devices	Hybrid joined devices
		
<ul style="list-style-type: none">• Supports Bring Your Own Device• Registered devices sign-in using a Microsoft account• Attached to an account granting access to resources• Control using Mobile Device Management (MDM) tools like Microsoft Intune• OS – Windows 10+, iOS, Android, and MacOS	<ul style="list-style-type: none">• Intended for cloud-first or cloud-only organizations• Organization-owned devices• Joined only to Azure - organizational account required• Can use Conditional Access policies• OS – Windows 10+ devices	<ul style="list-style-type: none">• You have Win32 apps deployed to these devices• You want to continue to use Group Policy to manage the device• You want to use existing image solutions to deploy devices• OS - Windows 7+ devices

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
mitanic (Default 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



Create User Accounts

 **Users** | All users

Microsoft

All users

Deleted users


Password reset


User settings


Diagnose and solve problems


+ New user


+ New guest user






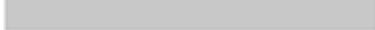


 Bulk operations

 Refresh

 Reset password

 Multi-Factor Authentication

 Delete user

Name	User principal name	↑↓	User type	Directory synced
 Retail Crisis Notifications	 @microsoft.com		Member	Yes
 Rumon Sinha	 @microsoft.onmicrosoft.com		Guest	No
 Momir Radojkovic	 @microsoft.onmicrosoft.com		Guest	No
 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](#)

- 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
- Microsoft 365 groups

Assignment Types

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

Assigned Gr

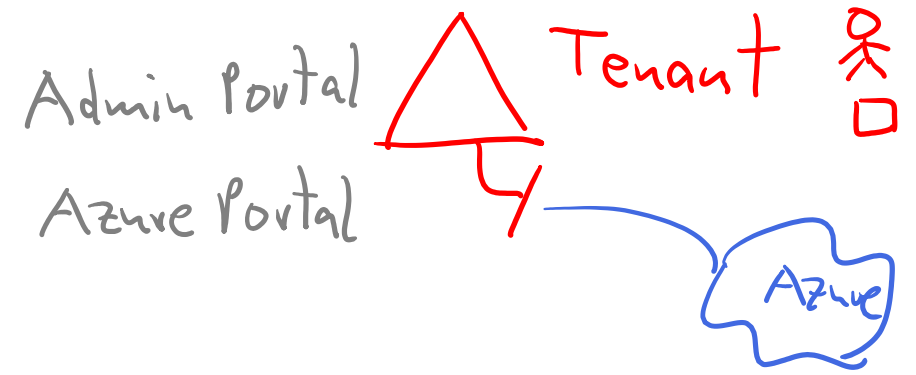
Assign Licenses to Users and Groups

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)

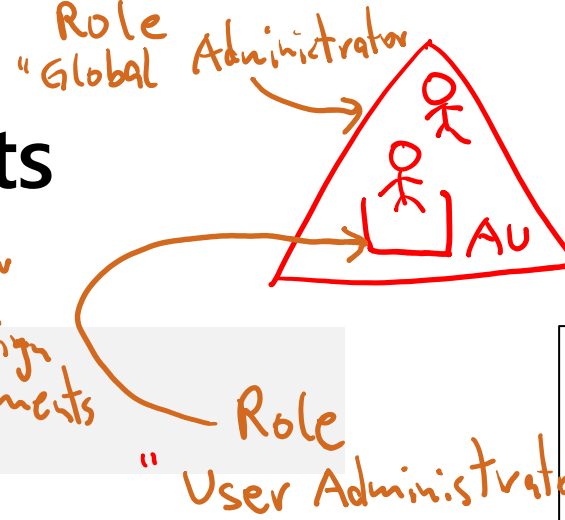
- Microsoft paid cloud services require licenses
- Licenses are assigned to those who need access to the services
- Each user or group requires a separate paid license
- Administrators use management portals and PowerShell cmdlets to manage licenses



- ☐ 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

Create Administrative Units

Tenant

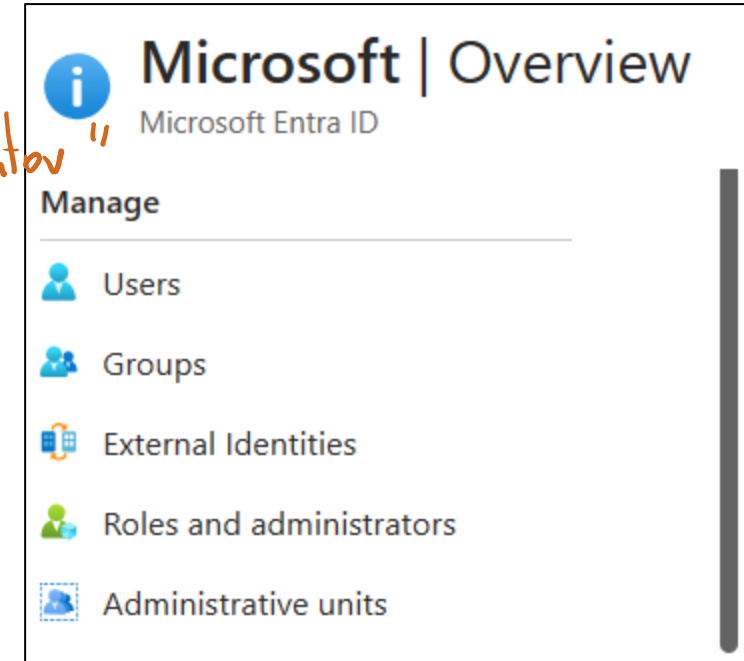


Create an administrative unit

Populate the administrative unit with users or groups

Create a role with appropriate permissions scoped to the administrative unit

Add IT members to the role



Microsoft Entra ID P1 or P2
Privileged Role Administrator or
Global Administrator

Lab 01 - Manage Microsoft Entra ID Identities



Lab 01 – Manage Microsoft Entra ID Identities



To allow Contoso users to authenticate, you have been tasked to:

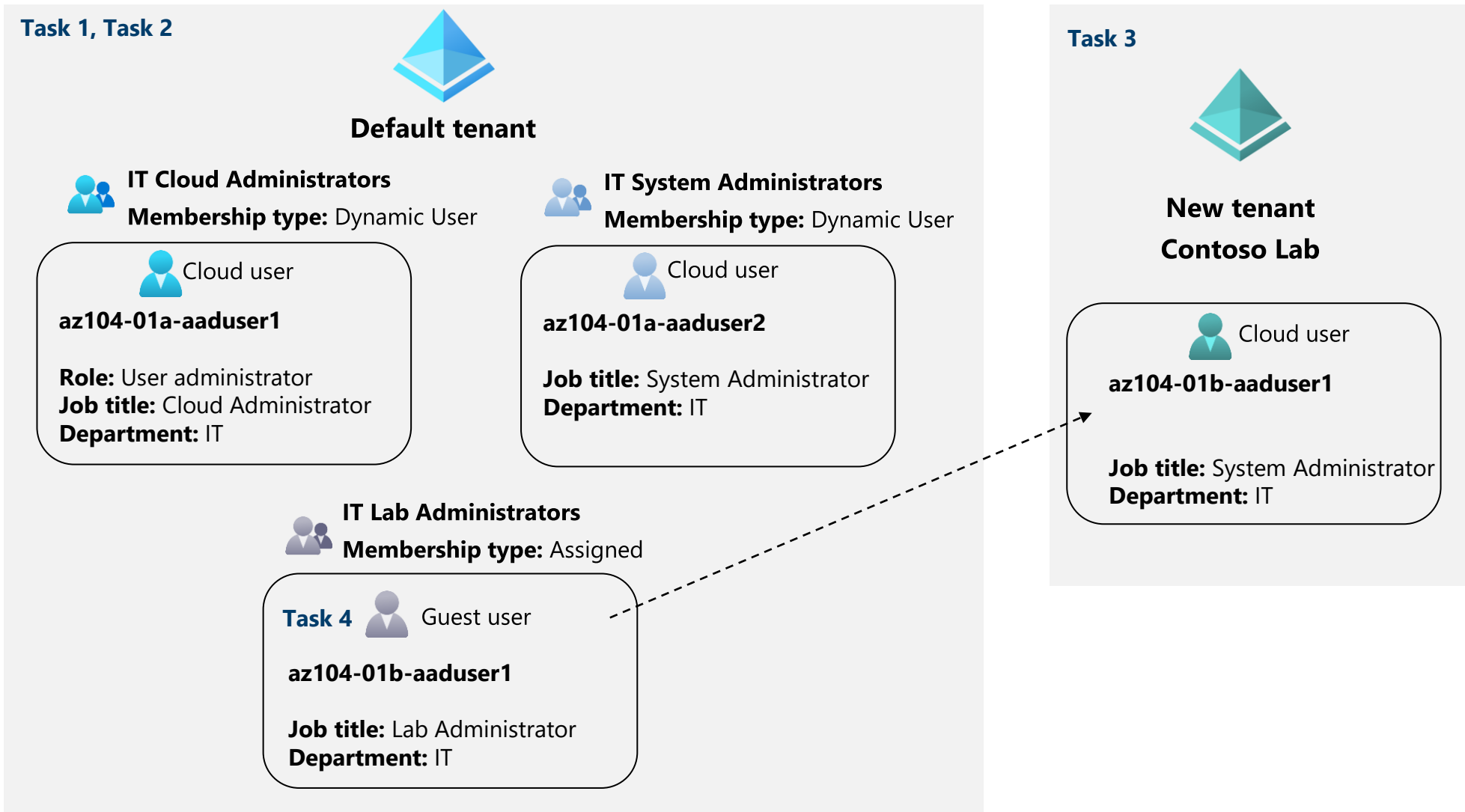
- Provision users and group accounts.
- Update membership of the groups automatically based on the user job titles.
- Create a test tenant with a test user account and grant that account limited permissions to resources in the Contoso Azure subscription.

Objectives

- **Task 1:** Create and configure users
- **Task 2:** Create groups with assigned and dynamic membership
- **Task 3:** Create a tenant
- **Task 4:** Manage guest users

Next slide for an architecture diagram ➡

Lab 01 – Architecture diagram



End of presentation

