**Create users and groups in Azure active directory**

User accounts

* Default set of permissions upon creation
* Different levels of users; admin, member, then guest(invitation)

Roles

* Admin; create, edit, assign admin roles to other users, reset passwords, manage license
* Member; default permission like edit profile information, handle internal organization stuff but not meant to assign other roles to members.
* Guest; restricted access, member users have default permission to invite guest users but can be removed by admin

**Manage app and resource**

Azure AD Roles

* Roles to manage resources like users, groups, billing, licensing

Role-based access

* Manage access to azure services such as vms, sql, and storage

Access rights; provide access rights to single user or groups

* Direct assignment,
* Group assignment, any member in this group inherit those rights
* Rule-based assignment, based on rules and requirements for the group

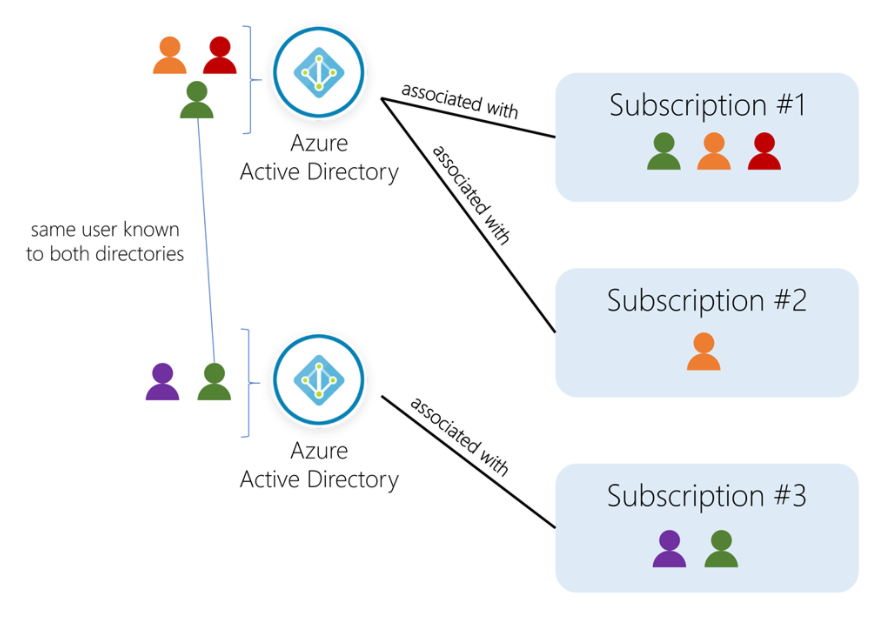
**Collaboration using B2B**

Guest user access

* Azure AD b2b
* Invite using email, direct link. Once accepted they’re then granted access to resources
* Why b2b? because you don’t have the responsibility of managing and authenticating guest users in detail.

**Manage Users and Groups**

* Each subscription has a single owner responsible for charges and resources
* Users can be added to multiple subscriptions



* You can switch directories if you have the **Directory + subscription** button in the portal header

**Sample Questions**

True or False, an organization can have more than one Azure AD directory.

True

Correct. While a single directory is created for the organization initially, more can be created to divide the security across boundaries.

An Azure AD directory can be associated with multiple subscriptions, but a subscription is always tied to a single directory.

An Azure subscription is a billing entity and security boundary

Azure AD defines users as

* Cloud identities, admin accounts that you manage yourself
* Directory-sync identities, on premises active directory. Can occur through **Azure AD Connect**
* Guest users, invited users that exist externally.

Create, add user using CLI

# Create a password object

$PasswordProfile = New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile

# Assign the password

$PasswordProfile.Password = "<Password>"

# Create the new user

New-AzureADUser -AccountEnabled $True -DisplayName "Abby Brown" -PasswordProfile $PasswordProfile -MailNickName "AbbyB" -UserPrincipalName "AbbyB@contoso.com"

* Can also use CSV file to add users

Groups

* Security group, most common group used to manage members and shared access to resources. Required is Azure AD admin
* Microsoft 365 group, provides collaboration and access to shared mailbox. Available to all users and groups

Create group command

New-AzureADGroup -Description "Marketing" -DisplayName "Marketing" -MailEnabled $false -SecurityEnabled $true -MailNickName "Marketing"

Built in roles

* Owner, full access, right to delegate access
* Contributor, create and manage, but cant grant access
* Reader, only view resources

Role definition

