



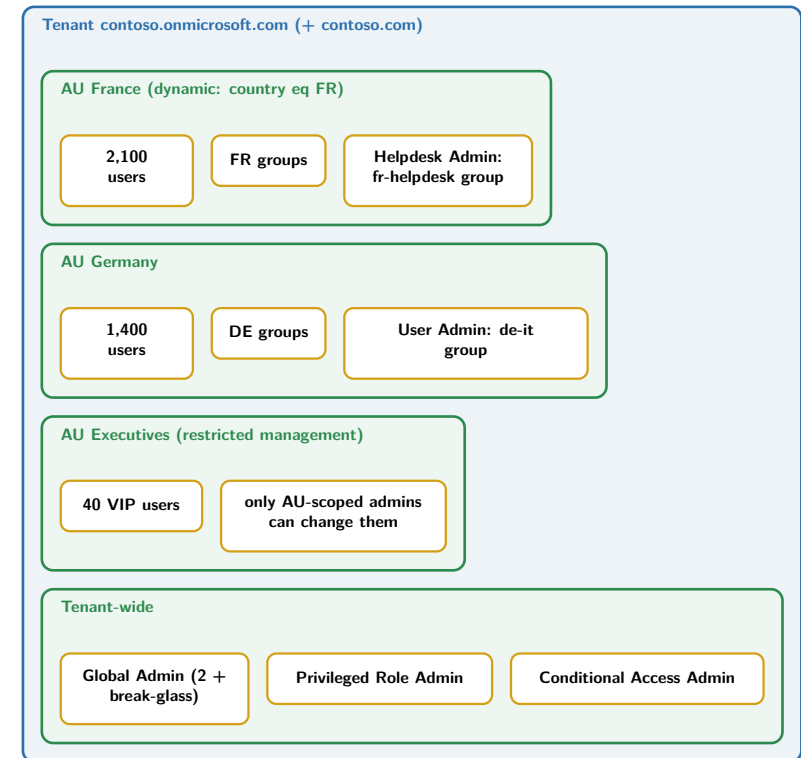
SC-300 Domain 1a: Tenant, Users, Groups and Roles

SC-300 skills measured, domain 1 Implement and manage user identities (20-25 %), as of 2026 | Tenant settings and custom domains, users and licences, group types and dynamic membership, administrative units, Entra built-in and custom roles, Graph PowerShell

SC-300 Domain 1 Entra ID Groups Administrative units

Tenant and domains

Setting	Where	Recommended
Custom domain	Entra admin center → Domain names → add, then TXT (or MX) record at your DNS host → Verify	make it primary for new users; one domain can be verified in one tenant only
Users can register applications	User settings	No: app registration through Application Developer role or a request process
Restrict non-admin users from creating tenants	User settings	Yes
Users can create security groups / M365 groups	Groups → General	restrict to a team, or use naming policy + expiration (P1)
Restrict access to the Entra admin center	User settings	Yes (a UI restriction only, not a security boundary: Graph still works)
Guest user access restrictions	External collaboration settings	guests limited to their own directory objects (sheet 02)



Administrative units carve the tenant for delegated administration; tenant-wide roles stay few

EXAM TIP

'Helpdesk in Paris must reset passwords only for French users' → **administrative unit** + Helpdesk Administrator **scoped to the AU**. 'Even Global Administrators must not modify the CEO's account except named admins' → **restricted management administrative unit**. Azure RBAC is never the answer for directory objects.

Users and licences

- **Sources** cloud-only (created in Entra), synchronised (from AD via Connect Sync / Cloud Sync: edit on-prem), guests (B2B invitations or redemption), provisioned from HR (Workday, SuccessFactors inbound provisioning)
- **Bulk operations** portal CSV for create, invite, delete; or Graph PowerShell / API for anything repeatable
- **Licences** set usage location first; prefer group-based licensing; check errors: CountViolation (not enough licences), MutuallyExclusiveViolation, DependencyViolation
- **Deleted users** soft-deleted for 30 days, restorable with memberships; permanently delete to free the UPN sooner
- **Attributes** custom security attributes (key-value, protected by their own roles) for ABAC and app filtering; directory extensions from sync

0

PS> New-MgUser

1

PS> New-MgUser -DisplayName 'Ana Silva' -UserPrincipalName ana@contoso.com

UPN on a verified custom domain

2

PS> New-MgUser -DisplayName 'Ana Silva' -UserPrincipalName ana@contoso.com -MailNickname ana_-AccountEnabled

required properties

3

PS> New-MgUser -DisplayName 'Ana Silva' -UserPrincipalName ana@contoso.com -MailNickname ana -AccountEnabled -PasswordProfile @{Password=\$p; ForceChangePasswordNextSignIn=\$true}

temporary password (or issue a Temporary Access Pass)

4

PS> New-MgUser -DisplayName 'Ana Silva' -UserPrincipalName ana@contoso.com -MailNickname ana -AccountEnabled -PasswordProfile @{Password=\$p; ForceChangePasswordNextSignIn=\$true} -UsageLocation FR -Department Sales

usage location before licensing; department drives dynamic groups

5

PS> Connect-MgGraph -Scopes 'User.ReadWrite.All'; New-MgUser -DisplayName 'Ana Silva' -UserPrincipalName ana@contoso.com -MailNickname ana -AccountEnabled -PasswordProfile @{Password=\$p; ForceChangePasswordNextSignIn=\$true} -UsageLocation FR -Department Sales

delegated scopes for the session

📄
 Worked example: group-based licensing errors

The tenant owns 500 Microsoft 365 E5 licences. Dynamic group 'Sales-E5' grows to 520 members after a reorganisation. Licences assigned = min(520, 500 - 0 already used elsewhere) = 500; **20 users** go into the CountViolation error state and have no E5 services. Fix: buy 20 more, or tighten the rule (exclude interns -and (user.employeeType -ne "Intern")), then **Reprocess** the group. Check with Get-MgGroup -Filter "hasMembersWithLicenseErrors eq true".

👤
 Groups and dynamic membership

Group type	Membership	Use for
Security group	assigned, dynamic user, dynamic device	app access, licences, CA policy targeting, Azure RBAC
Microsoft 365 group	assigned or dynamic user	Teams, SharePoint, shared mailbox; expiration and naming policy
Role-assignable group	assigned only, set at creation (isAssignableToRole)	hold Entra roles (with PIM for Groups); only Privileged Role Admin / Global Admin manage it
Mail-enabled security / distribution	Exchange-managed	mail flow, not managed in Entra

(user.<attribute> <operator> "<value>")

[-and|-or (<rule>)]

...

command

= type exactly

[optional]

= may be omitted

...

= repeat as needed

attribute

department, jobTitle, country, employeeType, accountEnabled, extension_<appid>_<name>, assignedPlans (multivalue)

operator

-eq, -ne, -startsWith, -contains, -match (regex), -in, -notin; multivalue: -any / -all

value

a string in double quotes, true/false, or a list ["FR","BE"] with -in

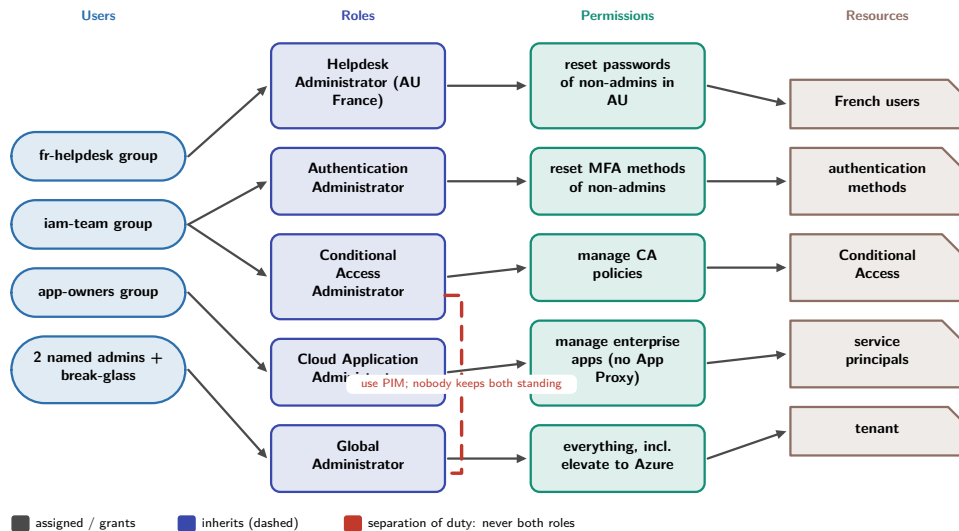
rule

another bracketed expression; -not negates

Dynamic membership rule, e.g. (user.department -eq "Sales") -and (user.accountEnabled -eq true)

- **Device rules** (device.deviceOSType -eq "Windows") -and (device.deviceOwnership -eq "Company"); a group is either user- or device-based
- **Multivalue** user.assignedPlans -any (assignedPlan.servicePlanId -eq "<guid>" -and assignedPlan.capabilityStatus -eq "Enabled")
- **Processing** changes can take minutes to hours in large tenants; use Validate rules on sample users; pause processing during big migrations
- **Limits to remember** dynamic groups and role-assignable groups cannot be the same group; nested groups do not inherit app assignments or group-based licences

Entra roles and delegation



Smallest role, narrowest scope, through groups and PIM

Need	Least-privileged Entra role
reset passwords of non-admin users	Helpdesk (Password) Administrator
reset passwords and MFA methods of any user including admins	Privileged Authentication Administrator
configure authentication methods policy	Authentication Policy Administrator
manage users and groups (not admins' passwords)	User Administrator
assign licences	License Administrator
register and manage app registrations and enterprise apps	Application Administrator (Cloud Application Administrator: no App Proxy)
manage Entra Connect / Cloud Sync, federation	Hybrid Identity Administrator
manage entitlement management, access reviews, lifecycle workflows	Identity Governance Administrator
read everything for audits	Global Reader



TIP

List members of a role with `Get-MgDirectoryRoleMember` or the role's Assignments blade; plan for fewer than 5 Global Administrators, all eligible through PIM except two cloud-only break-glass accounts with FIDO2 keys.

Self-check, recap and flashcards

Statement	True	False
1. A dynamic group can be role-assignable → Role-assignable groups need assigned membership.	☐	☒
2. Usage location must be set before assigning a licence → Services depend on the country.	☒	☐
3. Deleted users can be restored within 30 days → With group memberships and licences.	☒	☐
4. Helpdesk Administrator can reset a Global Administrator's password → Needs Privileged Authentication Administrator.	☐	☒
5. Restricting access to the Entra admin center blocks Graph access → It only hides the portal UI.	☐	☒
6. Administrative units can scope Helpdesk Administrator → Scoped role assignments on an AU.	☒	☐

Tick a box only when you could explain the point to someone else

- ☐ Verify custom domains, lock down user settings
- ☐ Dynamic groups for attributes, role-assignable groups for roles
- ☐ Least-privileged role, scoped, through PIM
- ☐ Group-based licensing with a usage location
- ☐ AUs to delegate, restricted AUs to protect VIPs

Q1 Which DNS record types verify a custom domain?

A TXT (preferred) or MX.

Q2 Which group property must be set at creation to assign Entra roles to a group?

A `isAssignableToRole = true` (role-assignable group).

Q3 Dynamic rule for enabled Sales users?

A `(user.department -eq "Sales") -and (user.accountEnabled -eq true)`.

Q4 Which licence do dynamic groups need?

A Microsoft Entra ID P1 for the members.

Q5 Which role resets MFA methods for non-admin users?

A Authentication Administrator.

Q6 Which role manages Entra Connect and federation settings?

A Hybrid Identity Administrator.

Q7 Group-based licence error for 'not enough licences'?

A CountViolation.

Q8 How long are deleted users kept?

A 30 days (soft delete).

Q9 Graph PowerShell cmdlet to sign in with scopes?

A `Connect-MgGraph -Scopes 'User.ReadWrite.All'`.