



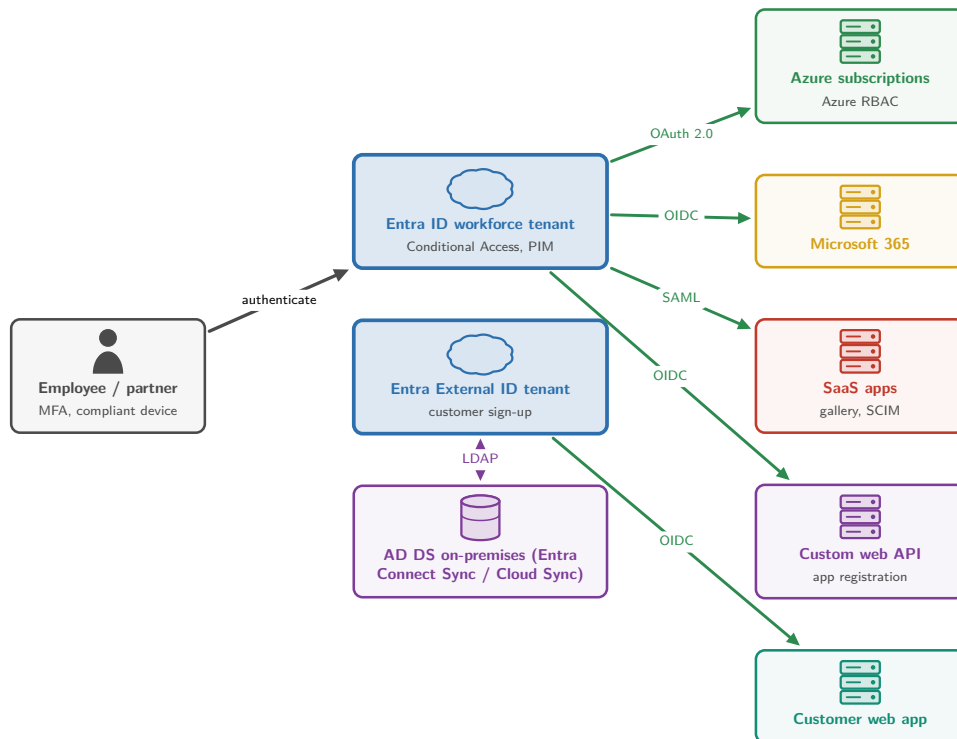
AZ-305 Domain 1a: Identity and Governance Design

AZ-305 skills outline, domain 1 (identity, governance), as of 2026 | Entra ID tenant and external identities, authentication and authorization design, managed identities, Key Vault, management groups, Azure Policy, RBAC, tagging, locks

AZ-305 Domain 1 Entra ID Azure Policy RBAC

Identity design: tenants, users, external identities

Domain 1 of AZ-305 (Design identity, governance and monitoring solutions) is the second-heaviest domain. Recall from AZ-104: a role assignment links a principal, a role and a scope; this sheet adds the **design choices**: how many tenants, which external identity model, which authentication method, which authorization scope and which guardrail.



One workforce tenant trusted by every Azure workload, federated outward

Need	Design	Why / limit
Partners use their own credentials on your apps	B2B collaboration (guest users, cross-tenant access settings)	guest authenticates at home; you apply your Conditional Access and access reviews
Consumers sign up with email, Google, Facebook	Entra External ID external tenant	Azure AD B2C stopped selling to new customers in May 2025; existing B2C tenants still supported
Two companies after a merger share apps	multitenant organisation, B2B direct connect (Teams shared channels), cross-tenant sync	keep separate tenants unless consolidation is a project
Hybrid sign-in for AD users	Password hash sync (recommended) or pass-through authentication; federation (AD FS) only if forced	PHS keeps cloud sign-in working when on-prem is down and enables leaked-credential detection
Cloud-only users	no sync; Entra ID native, password-less	fewest moving parts
Dev/test isolation	separate tenant only when directory-level settings must differ	every tenant = another identity boundary to secure

EXAM TIP

Keyword to answer: "external customers / social accounts" → Entra External ID (customer tenant). "partner employees" → B2B collaboration. "minimise on-premises dependency for authentication" → password hash sync. "must use the smart cards validated on-premises" → federation or certificate-based authentication.

🔍 Authentication and authorization design

CA

Conditional Access

if signal then grant control or block, per user and app

EXAMPLE

admins: phishing-resistant MFA from compliant device

NOT

Security defaults: one fixed MFA baseline, no exclusions

PIM

Privileged Identity Management

eligible, time-bound role activation with approval

EXAMPLE

Owner on prod for 2 h after approval

NOT

Access reviews: periodic recertification, no activation

MSI

Managed service identity (managed identity)

Azure-rotated identity for a resource

EXAMPLE

Function reads Key Vault with no secret

NOT

Service principal with a client secret you rotate

WIF

Workload identity federation

external OIDC token swapped for an Entra token

EXAMPLE

GitHub Actions deploys with azure/login, no secret

NOT

Publish profile or stored client secret

ABAC

Attribute-based access control

role assignment conditions on attributes

EXAMPLE

read blobs only where tag project=alpha

NOT

plain RBAC: scope only, no attribute filter

SCIM

System for Cross-domain Identity Management

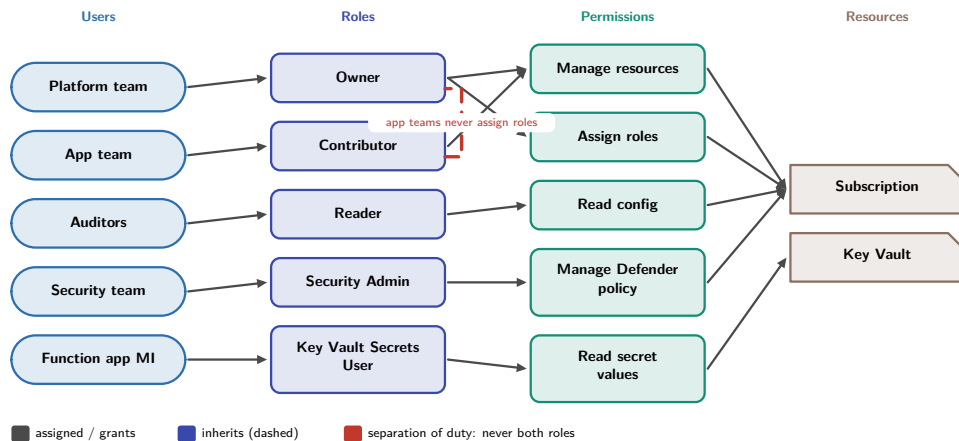
standard API to provision users into SaaS apps

EXAMPLE

Entra provisions Salesforce accounts

NOT

SAML: sign-in only, no account lifecycle



Azure RBAC: additive roles, inherited downward; separate duties for access management

Built-in role	Can do	Cannot do
Owner	everything, including role assignments	bypass Deny assignments or locks without removing them
Contributor	create and manage all resources	assign roles, manage Blueprints or policy assignments
Reader	view everything	read data-plane content (blob data, secret values)
User Access Administrator	manage role assignments	create resources
Role Based Access Control Administrator	assign roles, optionally constrained by conditions (allowed roles, principal types)	create resources; preferred over UAA for delegation

⚠️ Limits that bite

Up to 4,000 role assignments per subscription and 500 per management group (as of 2026, check the Azure subscription limits page); assign to **groups**, not users. Custom roles: 5,000 per tenant. A Deny assignment (from deployment stacks or managed apps) beats any allow.

System-assigned managed identity	User-assigned managed identity
created with the resource, deleted with it one resource only	standalone Azure resource with its own lifecycle shared by many resources (a VM scale set, many function apps)
role assignments recreated if resource is rebuilt	role assignments survive redeployments; pre-authorise before creation
simplest for a single app	AZ-305 favourite for scale-out, blue-green and federation (WIF)

🔒 Secrets, keys and certificates

Option	Key protection	Choose when
Key Vault Standard	software-protected keys, secrets, certificates	app secrets, TLS certificates, most CMK scenarios
Key Vault Premium	HSM-protected keys (FIPS 140 level 3 HSMs, multitenant)	regulation asks for HSM-backed keys
Managed HSM	single-tenant HSM pool, local RBAC, you own the security domain	full key-custody control, high throughput
Azure Payment HSM / Dedicated HSM path	physical HSM for payment processing	PCI PIN workloads only

Key Vault design baseline

✓ baseline / mandatory □ recommended – verify in your context

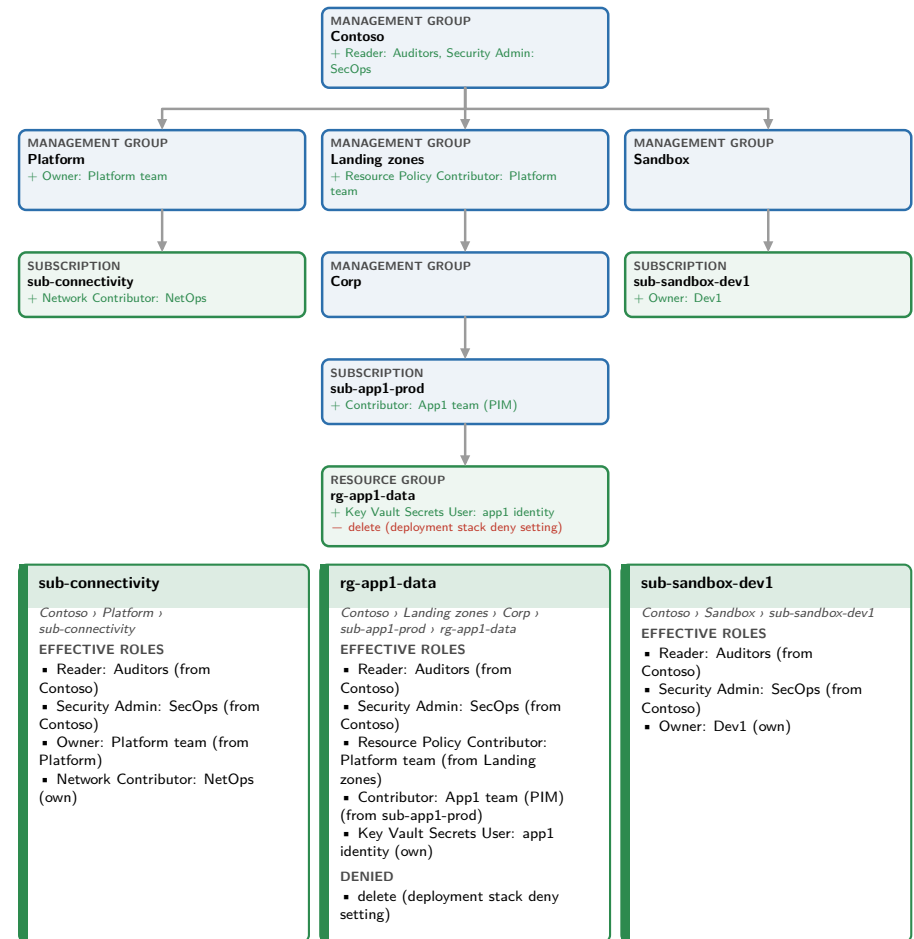
- ✓ Azure RBAC permission model (not legacy access policies) Key Vault Secrets User for apps, Key Vault Administrator for the platform team
- ✓ Soft delete (always on, 7-90 days retention, default 90) and purge protection on purge protection is required for CMK encryption of storage, SQL TDE and disks
- ✓ One vault per application per environment per region limits the blast radius and throttling scope
- **MUST** Private endpoint and public network access disabled

- ❑ **MUST** Diagnostic settings: AuditEvent to Log Analytics
- ❑ **SHOULD** Key rotation policy and certificate auto-renewal with an integrated CA

```
Grant a user-assigned identity read access to secrets (az CLI)
az identity create -g rg-app -n id-orders
PID=$(az identity show -g rg-app -n id-orders \
  --query principalId -o tsv)
KV=$(az keyvault show -n kv-orders-prod --query id -o tsv)
az role assignment create --assignee-object-id $PID \
  --assignee-principal-type ServicePrincipal \
  --role "Key Vault Secrets User" --scope $KV
```

Governance: hierarchy, policy, tags, locks

CUMULATIVE: assignments are inherited and add up down the tree; a deny blocks whatever is granted



Roles assigned higher up cannot be removed lower down; only a deny assignment or deny policy blocks them.

Management group design (Azure landing zone style): role assignments add up down the path

- **Depth** up to six levels of management groups below the tenant root (root and subscription level not counted); 10,000 management groups per tenant
- **Design rule** organise by policy and access needs (archetype: corp, online, sandbox), not by org chart; keep it flat (3-4 levels)
- **Subscription as a unit** scale, quota and billing boundary; one workload per subscription per environment is the landing-zone default (subscription vending)
- **Never assign at tenant root** except a few tenant-wide audit policies; use an intermediate root you control

Policy effect	What happens	Typical use
Deny	request rejected (HTTP 403) at create or update	allowed regions, no public IP on NICs
Audit / AuditIfNotExists	resource marked non-compliant, request allowed	first rollout of a new rule
Modify	adds, replaces or removes tags or properties; remediation task for existing	inherit a cost-center tag from the resource group
Append	adds fields at create or update	add an IP rule to a storage firewall
DeployIfNotExists (DINE)	deploys a related resource after the resource exists; needs a managed identity on the assignment	diagnostic settings to Log Analytics
DenyAction	blocks a specific action (delete) on matching resources	prevent deleting production databases
Disabled / Manual	rule off / attestation by a person	exemptions during migrations

Policy exemption — A scoped, time-limited waiver (Waiver or Mitigated category) for one assignment; prefer it to deleting the assignment.

Enforcement mode DoNotEnforce — Assignment evaluates and reports compliance but does not deny or deploy: the safe way to test a Deny policy at scale.

Azure Policy what resources may look like (properties)	vs	Azure RBAC who may do which action
Tell: Is it about the resource or the person?		
Resource lock CanNotDelete blocks delete, allows changes, applies to everyone	vs	Policy DenyAction blocks delete on resources matching a rule, at scale
Tell: One resource by hand, or every matching resource by rule?		
Tag name-value metadata for cost and ownership, not inherited by default	vs	Management group hierarchy that inherits policy and RBAC
Tell: Do you need inheritance of controls (MG) or reporting labels (tag)?		
Azure Blueprints deprecated, retirement announced for July 2026	vs	Template specs + deployment stacks + policy current way to stamp governed environments
Tell: AZ-305 2026 answers never pick Blueprints for new designs		

💡 **Worked example and myths**

How many role assignments does a group-based design save?

PROBLEM

120 engineers across 8 application subscriptions; each needs Contributor on 3 resource groups of their app and Reader on the subscription. Compare per-user and per-group assignments against the 4,000 per subscription limit.

GIVEN

- 15 engineers per subscription (120 / 8)
- per user: 3 Contributor + 1 Reader assignments
- per group: 1 Entra group per app team

1

Per-user assignments per subscription

15 users x (3 + 1) = 60 assignments

Why: each user needs one assignment per scope and role

2

Per-group assignments per subscription

1 group x (3 + 1) = 4 assignments

Why: membership changes happen in Entra, not in RBAC

3

Headroom vs limit

per user 60 / 4000 = 1.5 %; per group 4 / 4000 = 0.1 %

Why: the limit is not the issue here; auditability is

4

Joiner-mover-leaver cost

1 leaver = 4 role removals per-user vs 1 group removal

Why: access reviews run on the group, PIM for groups adds JIT

ANSWER

Group-based: 4 assignments per subscription instead of 60 (15x fewer), one change per leaver

CHECK

✓ 8 subscriptions x 4 = 32 assignments in total vs 480 per user

MYTH	FACT
✗ Owner of a subscription can always delete a locked resource	✓ The lock blocks the delete until someone removes the lock Owners and User Access Administrators can remove locks; that is an audited separate step.
✗ Reader can read the secrets in a Key Vault	✓ Reader is control-plane only Secret values need a data-plane role such as Key Vault Secrets User.
✗ Azure Policy Deny fixes existing resources	✓ Deny only blocks new creates and updates Existing resources show non-compliant; use Modify or DINE with a remediation task to fix them.
✗ Tags flow down from resource groups automatically	✓ Tags are not inherited unless a Modify policy copies them Use the built-in 'Inherit a tag from the resource group' policy.

🚩 Recap and self-test

Key takeaways

01 One workforce tenant
B2B for partners, External ID for customers

02 No secrets in code
managed identities, workload identity federation, Key Vault RBAC

03 Groups, PIM, conditions
assign roles to groups, eligible not permanent, constrained delegation

04 Flat MG hierarchy
by archetype; policy at MG, exemptions not deletions

05 Audit then Deny
DoNotEnforce first, remediation tasks for existing resources

Q1 A web app on a VM scale set must read Key Vault secrets and keep access after the scale set is rebuilt. Which identity?

A A user-assigned managed identity with Key Vault Secrets User: it survives the rebuild and is shared by all instances.

Q2 Which Entra ID licence is needed for PIM?

A Microsoft Entra ID P2 (or Entra ID Governance) for the users who use PIM.

Q3 Which policy effect deploys diagnostic settings on resources that lack them?

A DeployIfNotExists, with a managed identity on the assignment and a remediation task for existing resources.

Q4 How deep can management groups go?

A Six levels below the tenant root group (root and subscriptions not counted).

Q5 Customer-facing app with social sign-in, new design in 2026?

A Microsoft Entra External ID with an external (customer) tenant; B2C is closed to new customers.

Q6 Delegate role assignment to an app team without letting it grant Owner?

A Role Based Access Control Administrator with a condition restricting assignable roles (or PIM-managed).

Q7 CI/CD from GitHub Actions to Azure without a stored secret?

A Workload identity federation: federated credential on an app registration or user-assigned identity, azure/login with OIDC.

Q8 Key Vault setting required before storage accounts can use it for customer-managed keys?

A Soft delete and purge protection enabled.

Q9 Hybrid identity option that keeps cloud sign-in working if the datacentre is offline?

A Password hash synchronisation (with Entra Connect Sync or Cloud Sync).