Protera

WHITE PAPER

Azure Landing Zones
Part 2

Author:
Eric MacDonald
VP of Cloud Transformation

TABLE OF CONTENTS

Protera

Identity & Access Command Structure

(Tenants, RBAC, PIM, Break-Glass, Automation)

When deploying an Azure Landing Zone (ALZ), identity and access form the foundation of every control plane. Every subscription, network, and policy relies on who can authenticate and what they can authorize. Microsoft's Cloud Adoption Framework (CAF) defines identity and access management as a core design area for both platform and application landing zones.

This guide expands beyond Microsoft Learn to include deeper implementation notes, role-scoping logic, automation patterns, and operational governance you can apply in enterprise environments.

1. Identity & Access — your first design area

Identity must be the first design decision, not an afterthought. The CAF identity design area emphasizes that every other control plane—networking, security, monitoring—depends on a well-defined identity boundary. Microsoft Learn: Identity and access management in Azure landing zones →

Key recommendations:

- Establish your tenant strategy, directory services, and hybrid identity plan before building landing zones.
- Align your management-group hierarchy to identity scopes.
- Treat identity as code—automated, auditable, and versioned.

2. Tenant model & multi-tenant considerations

Microsoft recommends a single Microsoft Entra tenant for most organizations. This simplifies collaboration, governance, and monitoring. Only consider multiple tenants for regulatory isolation, mergers/acquisitions, or sovereign boundaries.

Reference: Azure landing zones and multiple Entra tenants

If you do deploy multiple tenants:

- Create one landing-zone hierarchy per tenant (Root → Platform MG → Landing-Zones MG).
- Establish cross-tenant governance and identity provisioning automation (for shared services, monitoring, or billing).
- Recognize that certain Azure services and policies do not span tenants natively — plan isolation deliberately.

3. Hybrid identity & directory services

Most enterprises still operate hybrid identity. CAF recommends using Microsoft Entra ID as the primary control plane, synchronizing from on-prem AD only as needed.

Reference: Hybrid identity with Active Directory and Microsoft Entra ID in Azure landing zones Best practices:

- Use Microsoft Entra Connect Cloud Sync where possible — lighter, more resilient than legacy AD Connect.
- If you must extend on-prem AD, isolate it inside the Platform Identity subscription.
- Consider Microsoft Entra Domain Services (AAD DS) if apps require Kerberos/LDAP but you want to retire on-prem AD.
- Protect sync connectors and domain controllers with network isolation and Defender for Identity.

---

4. RBAC vs. Microsoft Entra roles

A core mistake is mixing up tenant-wide and resource-scoped roles.

Reference: Landing-zone identity and access management

Role type	Scope	Typical usage
Microsoft Entra role	Tenant-wide	Manage users, apps, licenses (e.g., Global Admin, Privileged Role Admin)
Azure RBAC role	Management Group / Subscription / RG / Resource	Manage Azure resources (e.g., Owner, Contributor, Reader, custom)

Best practices:

- Use groups for assignments, not individuals.
- Avoid standing Owner roles — prefer Contributor + PIM.
- Document each RBAC scope: MG → Subscription → RG → Resource.
- Keep role definitions in version control as JSON for auditability.

---

5. Privileged Identity Management (PIM)

Static privileged access is one of the highest risks in Azure. Enable just-in-time (JIT) elevation using Microsoft Entra PIM for both directory and Azure roles.

Reference: Entra PIM Overview

PIM configuration checklist:

- Require MFA on elevation.
- Define approval workflows for Tier 0 roles.
- Limit activation durations (e.g., 4 hours).
- Stream PIM logs to Log Analytics for alerting.
- Run monthly access reviews for all eligible assignments.
- Remove unused eligible roles after 90 days.

For automation, use Microsoft Graph API or Azure CLI in your landing-zone pipelines to pre-configure PIM settings when new subscriptions are created.

6. Break-Glass / Emergency Access Accounts

Every tenant needs at least two emergency accounts to avoid lock-out.

Guidance:

- Assign only the Global Administrator role.
- Store credentials offline (sealed vault).
- Exclude from Conditional Access policies that might block sign-in.
- Monitor sign-ins — send alerts on any use.
- Test quarterly to ensure credentials and MFA methods still function.

Emergency accounts should never be used for daily administration.

7. Privileged Access Workstations (PAWs)

Control not just who administers Azure, but from where.

PAW design:

- Dedicated, hardened devices for Tier 0/1 admins.
- No internet browsing or email access.
- Enforce Conditional Access: only PAW devices may access privileged roles.
- Integrate with Defender for Endpoint for posture compliance.

Deploy PAWs via Microsoft Intune with compliance and Conditional Access policies attached

---

8. Tiered Access Model (Tier 0 → Tier 2)

CAF and Zero Trust guidance recommend tiering your control planes.

Tier	Scope	Controls	Review
Tier 0	Entra tenant, Root MG, Identity sub	Entra Connect, PIM, break-glass accounts	Global diagnostics, deny public IP
Tier 1	Platform subs (connectivity, mgmt, security)	Hub VNet, VPN, ExpressRoute, Azure Firewall	NSG flow logs required, deny wildcard rules
Tier 2	Application subs (dev/test/prod)	Log Analytics, Update Manager, Backup Vault	All diagnostics to central LA workspace

Reference: Identity & access management design area – separation of duties

Use Conditional Access policies aligned to these tiers to enforce risk-based MFA, compliant device checks, and limited geographic access.

---

9. Platform vs. Application Landing Zones — Delegation Model

Separation of duties is central to landing-zone identity design.

Reference: Landing-zone identity & access management

- Platform landing zones: contain shared services (Entra Connect, DNS, Log Analytics, Defender, Key Vault). Platform team holds Owner/Contributor; application teams have Reader only.
- Application landing zones: isolated per workload or BU; teams receive Contributor on their subscriptions only.
- Use management groups to cascade policies and RBAC boundaries.
- Avoid cross-scope ownership: app teams shouldn't control platform subscriptions.

This structure enforces least privilege and blast-radius containment.

---

10. Conditional Access Policies

Conditional Access is your Zero Trust enforcement engine.

Reference: Overview of Conditional Access in Microsoft Entra ID

Recommendations:

- Require MFA for all admins and privileged roles.
- Block legacy authentication protocols.
- Require compliant or hybrid-joined devices.
- Implement session controls (sign-in frequency, persistent browser session).
- Exclude emergency accounts from CA policies that might block them.

Use Named Locations for corporate networks and risk-based policies (integrated with Microsoft Entra ID Protection).

---

11. Monitoring & Logging

Identity without monitoring is blind.

Logging essentials:

- Stream Entra sign-in, audit, and PIM activation logs to Log Analytics.

Set alerts for:

- Break-glass sign-in activity.
- Privileged role activations after hours.
- Dormant privileged accounts.
- Guest accounts gaining elevated access.
- Integrate Defender for Identity alerts for hybrid AD.
- Centralize dashboards at the Management subscription level.

12. Identity Lifecycle & Access Reviews

Reference: Manage access reviews in Microsoft Entra ID

Lifecycle automation:

- Joiner–Mover–Leaver (JML) automation via HR/SCIM integration.
- Access Reviews every quarter for privileged roles and critical groups.
- Revoke inactive accounts automatically after review expiration.
- Version-control all role assignments and reviews (Git).
- Periodically audit Entra role assignments and RBAC drift.

---

13. Application Identity & Access

Applications are also principals. Treat them with the same governance rigor.
Reference: Application identity and access management

Key practices:

- Use Managed Identities (system or user-assigned) for workloads — never store credentials.
- Assign RBAC roles directly to managed identities, scoped per subscription/environment.
- Separate identities per environment (dev/test/prod).
- Disable unused service principals automatically after 90 days.
- Centralize app registrations in the Platform Identity subscription for visibility.

---

14. Automation: Identity as Code

Scale requires automation. Treat identity as code just like infrastructure.
Reference: CAF – Platform Automation Design Area

Automation patterns:

- Deploy PIM and RBAC configuration via Bicep or Terraform.
- Include role assignments, Conditional Access, and diagnostic settings in pipelines.
- Block manual role assignment changes with Azure Policy.
- Implement a subscription-vending pipeline that applies identity baselines automatically.
- Integrate with GitHub Actions or Azure DevOps for change control and audit trail.

Field kits and references

1. Identity & Access (CAF) learn.microsoft.com/identity-access
2. Landing-zone IAM learn.microsoft.com/identity-access-landing-zones
3. Hybrid Identity learn.microsoft.com/identity-access-active-directory-hybrid-identity
4. Multi-Tenant Design learn.microsoft.com/multi-tenant/overview
5. Application Identity learn.microsoft.com/identity-access-application-access
6. Conditional Access learn.microsoft.com/entra/identity/conditional-access/overview
7. PIM Overview learn.microsoft.com/azure/active-directory/privileged-identity-management/pim-configure

Next steps

In Part 3, we'll cover Networking and Connectivity — the backbone of your landing zone: hub-spoke architecture, ExpressRoute and VPN integration, hybrid DNS, and network segmentation guardrails.

Until then, review your current Entra tenant:

- Audit standing admin roles.
- Validate PIM enforcement.
- Confirm break-glass readiness.
- Test Conditional Access tiers.

Each of these actions reinforces the foundation your landing zone relies on.

Learn More

Protera.com