Designing Access Control Strategy with Microsoft Entra & Azure RBAC

Implementing Least Privilege at Enterprise Scale

PerparimLabs

The Access Control Challenge

Modern enterprises face identity sprawl across hybrid and multicloud environments.

Multiple teams, roles, and resources increase the risk of privilege misuse.

To achieve Zero Trust, access must be **granular, auditable, and role-based.**

Goal: Align Entra ID and Azure RBAC for unified access governance.

PerparimLabs

Access Control Models

Three foundational models:

DAC (Discretionary Access Control) – User-defined permissions.

MAC (Mandatory Access Control) – Centralized, system-enforced policies.

RBAC (Role-Based Access Control) – Role defines access, not identity.

Azure and Entra ID leverage RBAC as the foundation for scalable access management.

Azure Role-Based Access Control (RBAC)

RBAC grants access by **assigning roles to users, groups, or service principals.**

Each role defines allowed actions (read/write/delete) on Azure resources.

Access is inherited from higher scopes → lower scopes.

- *Scopes:* Management Group → Subscription → Resource Group → Resource

Permissions flow downward through inheritance, simplifying governance while maintaining least privilege.

PerparimLabs

Built-in vs Custom Roles

Built-in roles:	Owner – Full access + delegate permissions	Contributor – Modify resources, no role assignment	Reader – View-only access
Custom roles:	Fine-tuned to meet specific business or compliance needs	JSON-defined actions and scopes	

Custom roles bridge the gap between least privilege and operational flexibility.

Privileged Access Management

Integrate **Microsoft Entra Privileged Identity Management (PIM)** for JIT access.

Enforce **MFA**, **approval workflows**, and **time-bound assignments.**

Audit all privileged activities for compliance.

🔐 *PIM ensures that admin access is elevated only when required.*

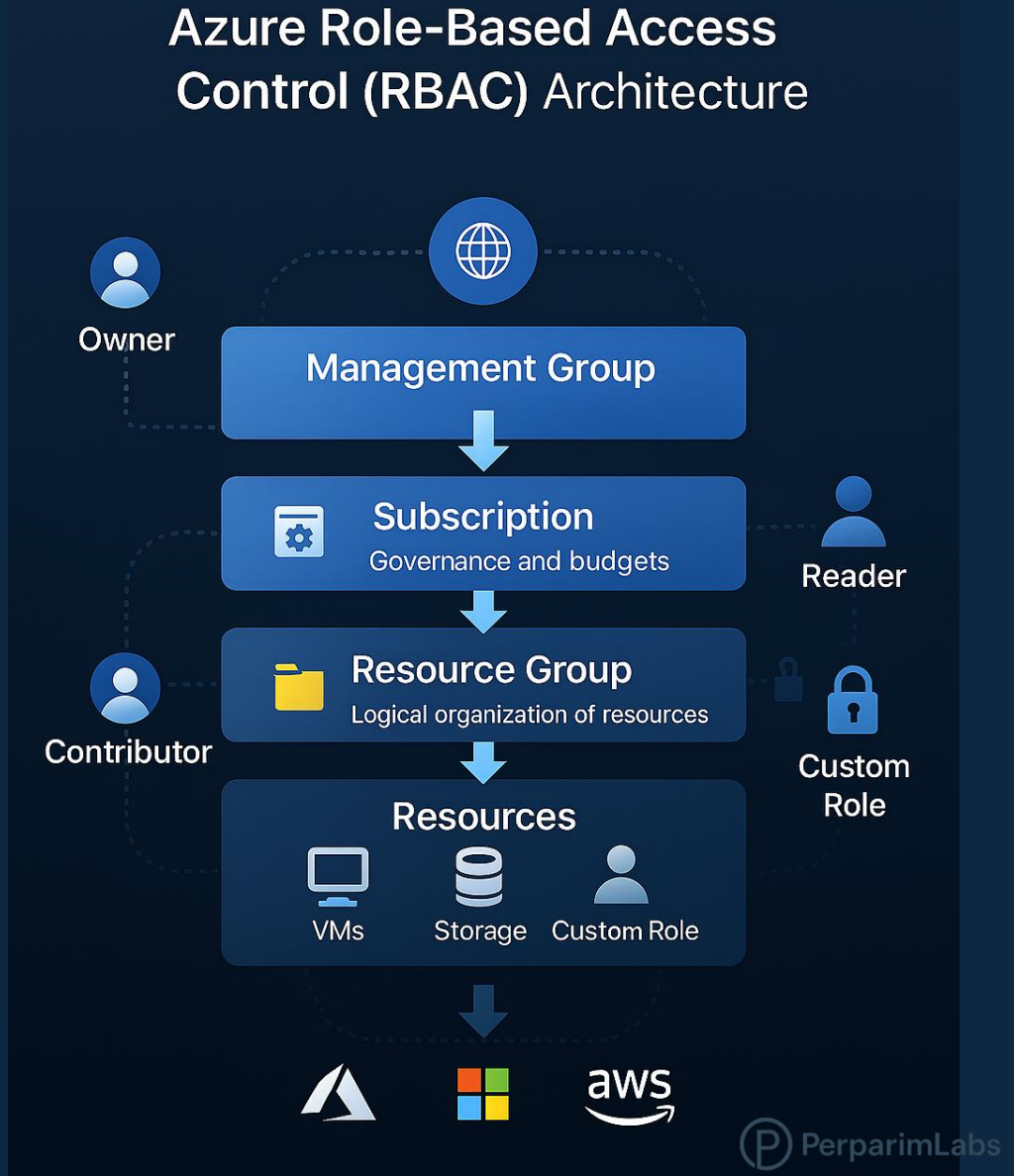
PerparimLabs

Azure RBAC Architecture Diagram

RBAC Inheritance and Role Scope Visualization

- Show inheritance flow from **Management Group → Subscription → Resource Group → Resources**
- Side roles (Owner, Contributor, Reader, Custom Role)
- Reinforce multi-cloud scope (Azure, Microsoft 365, AWS

🧭 *Represents how least privilege is enforced through hierarchy and role assignment.*



Key Takeaways

- ✅ **Implement** RBAC for unified access control
- ✅ **Use** PIM for on-demand privilege elevation
- ✅ **Create** custom roles for compliance-driven access
- ✅ **Apply** the **Enterprise Access Model** to align control layers
- ✅ **Continuously audit**, review, and refine access

PerparimLabs