Azure Active Directory & Zero Trust Architecture

Microsoft Entra ID deep dive pentru cursuri Azure

Conditional Access, PIM, managed identities, passwordless și aplicarea principiilor Zero Trust în implementări reale Azure

VERSIUNE 2026

PORTAL.AZURE.COM & MICROSOFT ENTRA ADMIN CENTER

Obiective de învățare

Ghid complet zero-to-hero în limba română. Material didactic pentru ingineri cloud la început de drum, administratori Azure și arhitecți care vor să construiască implementări moderne, sigure și ușor de operat.

01

Autentificare vs. autorizare

Să înțelegi clar diferența dintre autentificare, autorizare, identitate și controlul privilegiilor.

02

Roluri și identități

Să știi când folosești Microsoft Entra roles, Azure RBAC, service principals și managed identities.

03

Conditional Access

Să poți construi politici Conditional Access din portal și să le testezi în report-only înainte de enforce.

04

PIM & Just-in-Time

Să implementezi PIM pentru acces just-in-time și să reduci standing privilege pentru rolurile sensibile.

05

Passwordless rollout

Să proiectezi un rollout passwordless realist, inclusiv Temporary Access Pass pentru onboarding.

06

Zero Trust în scenarii reale

Să aplici principiile Zero Trust în scenarii reale Azure: Portal, AKS, App Service, Key Vault, Storage, SQL și admin access.

De ce identitatea este atât de importantă

În trecut, multe organizații tratau rețeaua ca pe o clădire de birouri. Dacă ai trecut de poarta principală, presupunerea era că ești de încredere. Astăzi, modelul acesta nu mai funcționează bine. Utilizatorii lucrează de acasă, folosesc SaaS, deschid aplicații din browser și accesează API-uri care nu locuiesc toate în același subnet.

> **Analogia aeroportului:** Nu este suficient să fii în parcarea aeroportului ca să poți urca în avion. Treci prin verificarea identității, control de securitate, verificare a biletului, eventual control suplimentar dacă apar factori de risc. Conditional Access și PIM fac exact acest lucru pentru accesul digital: verifică cine ești, din ce context vii și cât privilegiu ai nevoie chiar acum.

Schimbarea de mentalitate pentru junior cloud engineers: Securitatea modernă nu înseamnă doar VNet, NSG și firewall. Înseamnă decizii de acces luate dinamic, bazate pe identitate, dispozitiv, risc, aplicație, rol și comportament.

Ce este Microsoft Entra ID și cum se leagă de Azure

Microsoft Entra ID

Fostul Azure Active Directory, este serviciul de identitate și access control al ecosistemului Microsoft. Stochează utilizatori, grupuri, aplicații, enterprise applications, device identities, metode de autentificare și politicile de acces.

Când te conectezi în Azure Portal, în Microsoft 365 sau într-o aplicație enterprise federată, Entra ID face autentificarea și emite tokenul.

Răspunde la: "Cine ești?" și "În ce condiții te las să intri?"

Azure RBAC

Intervine după autentificare și decide ce ai voie să faci pe resursele Azure.

Răspunde la: "Ce ai voie să faci după ce ai intrat?"

Separarea esențială

Entra ID = **identitate și autentificare** Azure RBAC = **autorizare pe resurse** Managed Identity = **identitate fără secrete pentru workload-uri**

Comparație: Entra Roles, Azure RBAC, Service Principals, Managed Identities

Concept	La ce folosește	Unde se aplică	Când îl alegi
Roluri Microsoft Entra	Administrare identitate și tenant	Entra admin center / tenant	Când administrezi identitatea, users, groups, CA, PIM
Azure RBAC	Autorizare pe resurse Azure	Subscription / RG / resource	Când dai acces la VM, Storage, Key Vault, AKS, RG
Service Principal	Identitate pentru aplicații	Entra + aplicații	Când o aplicație externă are nevoie de identitate; mai multă grijă la secrete/certificate
Managed Identity	Identitate gestionată de platformă	Resurse Azure suportate	Prima alegere pentru workload-uri Azure deoarece evită secretele manuale

Ideea centrală: Entra ID spune "cine ești", Azure RBAC spune "ce poți face", managed identity este felul preferat în Azure de a oferi unei resurse o identitate fără secrete.

Obiecte și concepte importante în Entra ID

Tenant

Instanța ta logică de identitate. O organizație poate avea unul sau mai multe tenants.

User

Identitatea unei persoane. Poate fi cloud-only, sincronizată din AD sau invitată B2B.

Group

Folosit pentru a grupa utilizatori și a simplifica assignment-urile.

App Registration

Definiția logică a unei aplicații care vrea să folosească identitatea Microsoft.

Service Principal

Instanța acelei aplicații într-un tenant; identitatea pe care o vede organizația ta.

Managed Identity

O formă specială de service principal, gestionată de Azure pentru o resursă suportată.

Enterprise Application

Reprezentarea unei aplicații folosite în tenant pentru SSO, provisioning și policy.

Conditional Access

Motorul de policy care decide dacă și cum se acordă acces.

PIM

Control pentru privilegii administrative just-in-time și governance al rolurilor sensibile.

CAPITOL 3

Zero Trust pe înțelesul tuturor

Zero Trust nu este un singur produs și nici un singur buton din portal. Este un mod de a proiecta securitatea pe baza a trei idei simple.

> **Analogia hotelului modern:** Chiar dacă ai intrat în recepție, nu poți deschide orice cameră. Cardul tău este verificat pentru o anumită ușă, într-un anumit interval de timp, iar camerele tehnice au acces separat și mai strict. Exact așa ar trebui tratat și accesul în cloud.

În Azure, Zero Trust se traduce în mod practic prin: MFA și metode phishing-resistant, Conditional Access, PIM pentru roluri privilegiate, RBAC minim necesar, identități gestionate pentru workload-uri, acces privat către servicii și monitorizare puternică a semnalelor de autentificare și autorizare.

Cele trei principii Zero Trust

🔍 Verifică explicit

Folosești semnale precum identitatea utilizatorului, rolul, riscul, dispozitivul, locația, aplicația și sensibilitatea resursei înainte să permiți accesul. Nicio decizie de acces nu se ia implicit.

🔒 Acordă minimul necesar

Nu oferi Owner sau Global Administrator pentru orice nevoie. Dai exact cât trebuie, la nivelul de scope potrivit și pe durata potrivită. Privilegiul excesiv este un risc, nu un confort.

⚠️ Presupune că există deja o breșă

Segmentezi accesul, monitorizezi, faci review-uri și construiești astfel încât compromiterea unei identități să nu însemne compromiterea întregii organizații.

Model didactic: verifică explicit, acordă minimul necesar, presupune că există deja o breșă.

Zero Trust aplicat în Azure: arhitectura de ansamblu

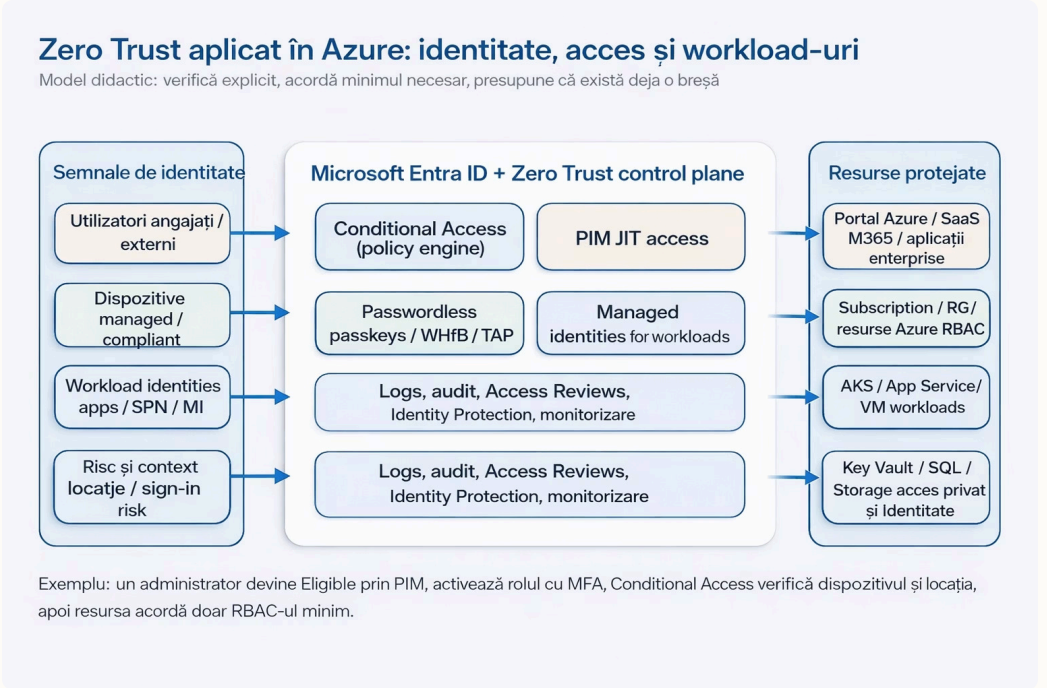
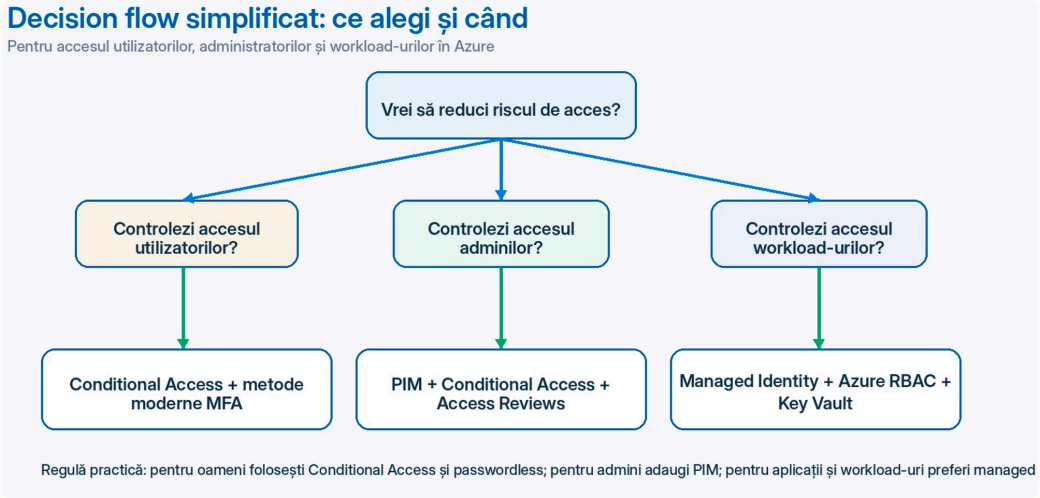


Diagrama ilustrează arhitectura Zero Trust în Azure, organizată în trei componente principale: **Semnale de identitate** (utilizatori, dispozitive, workload identities, risc și context), **Microsoft Entra ID + Zero Trust control plane** (Conditional Access, PIM JIT, Passwordless, Managed Identities, Logs & monitorizare) și **Resurse protejate** (Portal Azure/SaaS/M365, Subscription/RBAC, AKS/App Service/VM, Key Vault/SQL/Storage).

> **Exemplu practic:** Un administrator devine Eligible prin PIM, activează rolul cu MFA, Conditional Access verifică dispozitivul și locația, apoi resursa acordă doar RBAC-ul minim.

Decision Flow: ce alegi și când



Accesul utilizatorilor

Conditional Access + metode moderne MFA

Accesul adminilor

PIM + Conditional Access + Access Reviews

Accesul workload-urilor

Managed Identity + Azure RBAC + Key Vault

Regulă practică: pentru oameni folosești Conditional Access și passwordless; pentru admini adaugi PIM; pentru aplicații și workload-uri preferi managed identity.

CAPITOL 4

Conditional Access în profunzime

Conditional Access este policy engine-ul Zero Trust al Microsoft Entra. Politicile sunt în esență reguli de tip **if-then**: dacă un anumit user sau workload încearcă să acceseze o resursă într-un anumit context, atunci aplică grant controls sau session controls.

Cele mai comune semnale sunt: utilizator sau grup, aplicație sau cloud resource, device platform, locație, client app, sign-in risk, user risk, authentication strength și filtre pentru workload identities. Puterea reală nu vine doar dintr-un singur semnal, ci din **combinarea lor într-o politică coerentă**.

> **Best practice:** Începe cu **report-only**. Astfel vezi în jurnale cine ar fi fost blocat sau cine ar fi fost forțat să facă MFA, fără să strici producția în prima zi.

Componentele unei politici Conditional Access

Componentă	Rol
Assignments	Cui se aplică și ce resurse acoperă: users, groups, workload identities, cloud apps, actions.
Conditions	Context suplimentar: locație, platformă, client app, sign-in risk, device filter etc.
Grant controls	Ce trebuie să se întâmple: require MFA, require compliant device, require authentication strength, block access.
Session controls	Ce se întâmplă după autentificare: sign-in frequency, app enforced restrictions, CAE și alte limite de sesiune.
Policy state	Disabled, Report-only sau On.

Politici Conditional Access recomandate pentru orice organizație

→ MFA pentru administratori privilegiați

Require MFA sau authentication strength phishing-resistant pentru toți administratorii privilegiați, fără excepție.

→ Blocare legacy authentication

Blocare sau restricționare pentru legacy authentication și protocoale care ocolesc controalele moderne.

→ Compliant device pentru date sensibile

Require compliant device pentru aplicații sau date sensibile. Dispozitivele negestionate nu ar trebui să acceseze resurse critice.

→ Politici separate pentru workload identities

Fără a presupune că serviciile pot face MFA ca un om. Workload identities au propriile controale.

→ Named locations și politici bazate pe risc

Politici pentru scenarii din afara țării sau din rețele nesigure, bazate pe locație sau risc.

→ Exclude-uri controlate strict

Un set de exclude-uri foarte bine controlate, doar pentru break-glass accounts și conturi de urgență.

Cum creezi o politică Conditional Access din portal — pas cu pas

1

Navighează la Conditional Access

Intră în Microsoft Entra admin center → Protection → Conditional Access → Policies → New policy.

2

Alege un nume clar

Exemplu: `CA - Admins - Require MFA` sau `CA - Storage - Require compliant device`. Naming consistent ajută la audit.

3

Selectează Users / Workload identities

Cine intră în scope. Folosește grupuri dedicate, nu selecții haotice user-cu-user.

4

Target resources

Alege aplicațiile sau acțiunile. Multe organizații aleg All resources și rafinează cu excepții bine justificate.

5

Conditions

Setezi contextul relevant: locații, platforme, client apps, filters, risk.

6

Grant controls

Require MFA, authentication strength, compliant device sau block access. Gândește-te la AND versus OR pentru politici complexe.

7

Report-only → validare → On

Pune politica în Report-only, validează rezultatele în sign-in logs, apoi comută pe On când ești sigur de impact.

Capcane frecvente în Conditional Access

⛔ Politici puternice direct pe All users fără test pilot

Să aplici politici puternice direct pe All users fără test pilot și fără conturi break-glass este cel mai rapid mod de a te bloca singur afară din tenant.

⛔ Amestecarea politicilor pentru oameni cu workload identities

Un serviciu nu poate satisface aceleași controale interactive ca un utilizator uman. Politicile trebuie separate clar.

⛔ Ignorarea diferenței autentificare vs. autorizare

Conditional Access îți decide intrarea; RBAC decide operațiile după intrare. Confundarea lor duce la găuri de securitate.

⛔ Lipsa monitorizării în sign-in logs

O politică bună este una observabilă, nu doar una bifată în portal. Urmărește workbook-urile și alertele regulat.

CAPITOL 5

Privileged Identity Management (PIM)

PIM există pentru a reduce **standing privilege**. În loc să ții un om permanent Owner, Privileged Role Administrator sau Global Administrator, îl faci **Eligible** și îi permiți activarea rolului doar când are nevoie, pentru o durată limitată și cu controale suplimentare.

> **Analogia cheii de la camera tehnică:** Nu o ții tot timpul în buzunarul tuturor. Ea stă într-un seif, iar cine o ia trebuie să lase urme: cine e, de ce are nevoie, pentru cât timp și cine aprobă.

Pentru organizații mature, PIM este una dintre cele mai valoroase investiții. Scade riscul, ajută auditul, reduce blast radius-ul și face mult mai clar cine a avut acces privilegiat și când.

Termeni esențiali în PIM

Eligible

Persoana are dreptul să activeze rolul, dar nu îl deține activ tot timpul. Starea implicită recomandată pentru admini.

Active

Rolul este activ chiar acum. Ar trebui să fie starea excepțională, nu cea permanentă.

Activation

Procesul prin care utilizatorul cere și obține rolul pentru o perioadă determinată.

Approval

Un approver trebuie să valideze cererea înainte de activare. Adaugă un strat de control uman.

Access Review

Revizuire periodică a accesului pentru a elimina privilegiile care nu mai sunt necesare.

JIT

Just-in-time access; primești privilegiu doar când chiar ai nevoie de el, nu permanent.

Cum activezi PIM și configurezi un rol — pas cu pas

1

Navighează la PIM

Intră în Microsoft Entra admin center → Identity Governance → Privileged Identity Management.

2

Alege tipul de rol

Alege dacă lucrezi cu Microsoft Entra roles, Azure resources sau Groups.

3

Selectează rolul sensibil

De exemplu: Global Reader, Security Administrator sau Contributor pe o subscription.

4

Configurează ca Eligible

Configurează assignment-ul ca Eligible, nu Active, pentru utilizatorii normali de administrare.

5

Setează controalele de activare

Activation duration, require MFA on activation, ticket info sau justification și approvers dacă e nevoie.

6

Adaugă Access Reviews

Pentru a forța recertificarea periodică a accesului și a elimina privilegiile expirate.

7

Monitorizează

Verifică activity history și alerts pentru a vedea dacă există roluri prea largi sau activări neobișnuite.

PIM + Conditional Access = combinația corectă

De ce să le combini?

O practică excelentă este ca activarea rolului prin PIM să forțeze reevaluarea Conditional Access. Astfel un admin nu doar cere rolul, ci îl activează într-un context controlat.

În felul acesta reduci riscul unui token vechi sau al unui context nesigur care ar putea fi exploatat.

Ce verifică combinația?

- MFA la momentul activării rolului PIM
- Dispozitiv de încredere și compliant
- Locație acceptată conform politicii
- Sign-in risk scăzut sau acceptabil
- Justificare și ticket number (opțional)
- Aprobare din partea unui approver desemnat

Niciun strat nu este singurul gardian. PIM + CA + RBAC + monitorizare = apărare în adâncime.

CAPITOL 6

Managed Identities pentru workload-uri

Managed identity este modul preferat în Azure pentru a da unei resurse o identitate fără să salvezi manual parole, client secrets sau certificate în config files. Azure creează și gestionează identitatea pentru resursă, iar aplicația obține tokenul din platformă.

> **Analogia badge-ului:** În loc să-i dai aplicației o cheie fizică și să te rogi să nu o piardă, îi dai un badge emis și rotit de clădire, iar badge-ul poate fi revocat și controlat central.

Acesta este unul dintre cele mai importante pattern-uri de securitate pentru **App Service, Function App, VM, AKS, Automation Accounts** și alte resurse care consumă Key Vault, Storage, SQL sau API-uri protejate de Entra.

System-assigned vs. User-assigned Managed Identity

System-assigned

Legată de o singură resursă. Dacă ștergi resursa, dispare și identitatea. Este simplă și foarte bună pentru **majoritatea scenariilor**.

- Lifecycle legat de resursă
- Nu poate fi partajată
- Ideal pentru resurse independente
- Configurare simplă din portal

User-assigned

Identitate separată, independentă de resursa care o folosește. Poate fi atașată la mai multe resurse. Utilă când vrei **reuse, lifecycle separat sau permisiuni partajate controlat**.

- Lifecycle independent
- Poate fi partajată între resurse
- Ideal pentru integrări shared
- Administrare centralizată

Deploy din portal: App Service + Managed Identity + Key Vault

01

Activează System-assigned Identity

Deschide App Service-ul în Azure Portal → Identity → System assigned = On și salvează. Azure creează automat identity principal-ul în Entra ID.

02

Acordă acces în Key Vault

Mergi în Key Vault → Access control (IAM) sau modelul de access policy folosit de organizația ta. Atribuie rolul minim necesar, de exemplu `Key Vault Secrets User`, la scope-ul corect.

03

Folosește DefaultAzureCredential în cod

În cod folosește `DefaultAzureCredential` sau SDK-ul potrivit pentru a cere token și a accesa secretul fără a pune nimic sensibil în appsettings.

04

Testează și verifică logs

Testează din aplicație și verifică în diagnostic logs și activity logs că accesul este acordat corect și că nu există erori de autorizare.

Regulă de aur: Nu da Administrator dacă aplicația trebuie doar să citească un secret. Principiul minimului necesar se aplică și pentru managed identities.

Bune practici pentru Managed Identities

System-assigned pentru resurse unice

Alege system-assigned când identitatea aparține clar unei singure resurse și nu trebuie partajată.

User-assigned pentru resurse partajate

Alege user-assigned când mai multe resurse trebuie să partajeze aceeași identitate controlat.

Roluri minime

Folosește grupuri și roluri minime. Evită Contributor sau Owner fără justificare clară pentru identity-urile de workload.

Evită secretele long-lived

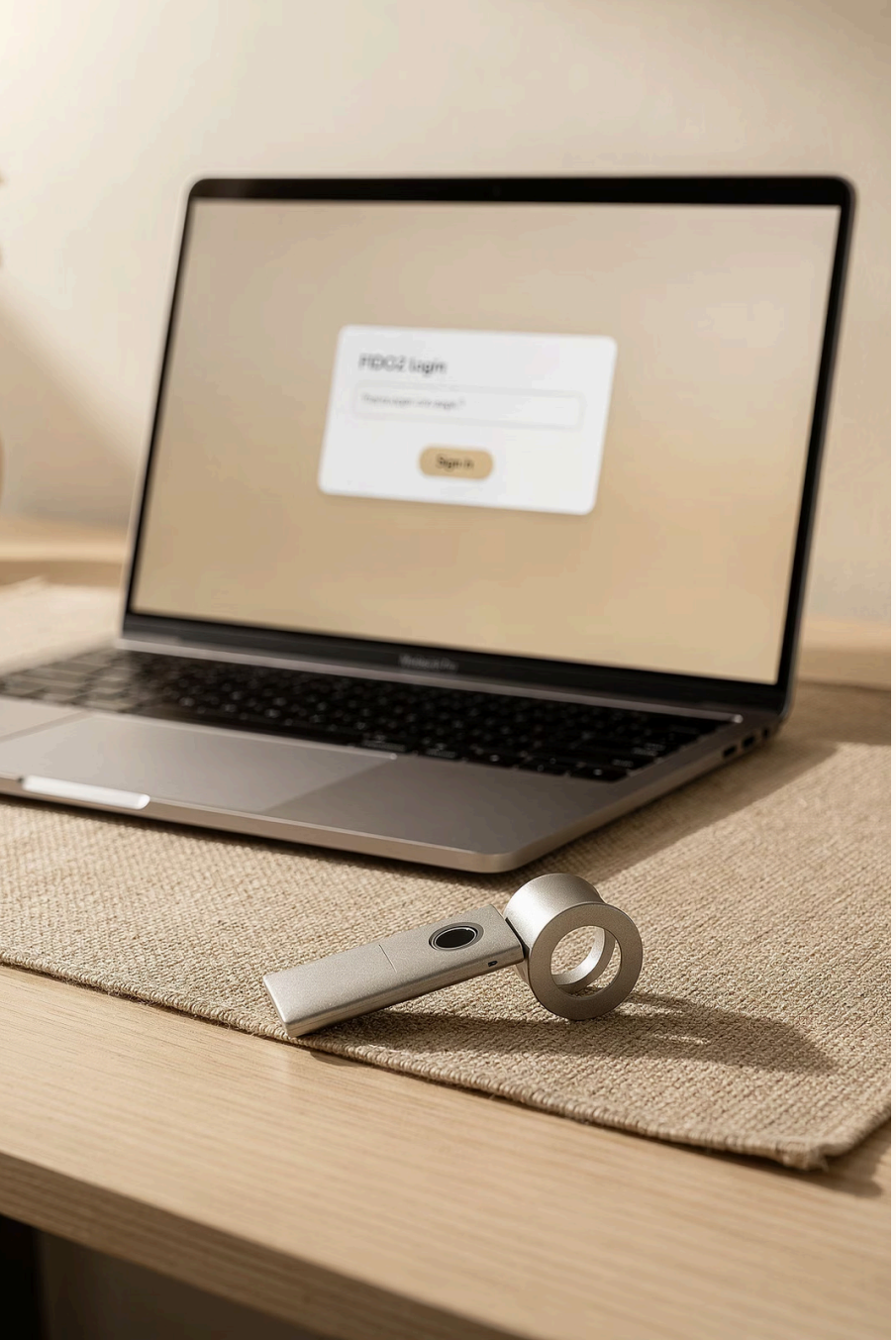
Evită secretele lung-lived în pipelines și aplicații atunci când o managed identity poate rezolva scenariul.

Separă prod de non-prod

Separă identitățile de producție de cele non-producție; nu reutiliza aceeași identitate peste tot.

Monitorizează role assignments

Monitorizează role assignments și privilegii excesive acordate identity-urilor de workload în mod regulat.



CAPITOL 7

Passwordless și phishing-resistant authentication

Passwordless nu înseamnă doar confort. Înseamnă reducerea dependenței de parole, care pot fi phishing-uite, reutilizate sau slabe. În Entra ID, metodele moderne includ **Windows Hello for Business, passkeys/FIDO2 security keys** și **Temporary Access Pass** pentru onboarding și recovery.

> Parola este ca un cod scris pe un bilețel pe care îl poți dicta la telefon. O metodă phishing-resistant este mai aproape de o cheie criptografică legată de dispozitivul tău și de o confirmare biometrică locală.

Strategia practică de rollout passwordless

Pilot cu IT și security champions

Începe cu un pilot: IT, security champions și câțiva utilizatori din business care pot oferi feedback real.

Activează metodele în Entra

Activează metodele suportate în Entra Authentication Methods și definește ce grupuri au voie să le folosească.

Configurează Temporary Access Pass

Configurează TAP pentru onboarding și recovery controlat. TAP este etapa de bootstrap, nu metoda permanentă.

Comunică experiența de înrolare

Comunică foarte clar experiența de înrolare, device requirements și ce faci dacă utilizatorul își schimbă telefonul sau pierde cheia FIDO2.

Migrare treptată spre phishing-resistant

Mută treptat grupurile critice spre metode phishing-resistant și redu dependența de metode slabe precum SMS acolo unde organizația permite.

Temporary Access Pass (TAP) — pași din portal

Ce este TAP?

Temporary Access Pass este un cod cu durată limitată, generat de un administrator, care permite unui utilizator să se autentifice și să înroleze o metodă puternică de autentificare fără a folosi parola.

Este etapa de **bootstrap**, nu o metodă permanentă de lucru zilnic.

Pași din portal

1. În Entra admin center mergi la Protection → Authentication methods → Temporary Access Pass.
2. Enable politica pentru grupul pilot și configurează lifetime, one-time use și alte setări potrivite politicii interne.
3. Pentru un utilizator, deschide profilul său și generează un TAP când trebuie să își înroleze o metodă nouă sau și-a pierdut credentialele puternice.
4. Folosește TAP ca etapă de bootstrap, nu ca metodă permanentă de lucru zilnic.

CAPITOL 8

Zero Trust într-o implementare reală Azure

Să luăm un exemplu realist: o echipă administrează un **AKS, un App Service, un Key Vault și un Storage Account**.

Administratori → PIM

Administratorii folosesc PIM pentru Contributor sau AKS RBAC Admin, activând rolul doar când au nevoie, cu MFA și justificare.

Acces la portal → Conditional Access

Conditional Access cere MFA și dispozitiv compliant pentru portal și pentru resurse sensibile.

App Service → Managed Identity

App Service folosește system-assigned managed identity pentru a citi secrete din Key Vault, fără secrete în config.

AKS → Workload Identity

AKS folosește workload identity sau alte mecanisme moderne compatibile pentru acces controlat la servicii Azure.

Storage & Key Vault → Private + RBAC minim

Storage și Key Vault sunt accesate privat și cu RBAC minim. Private endpoints reduc suprafața de atac.

Zero Trust înseamnă că niciun strat nu este singurul gardian; fiecare verifică partea lui.

Design recomandat pentru roluri și privilegii

Rol / identitate	Model recomandat
Break-glass accounts	Foarte puține, excluse controlat din unele politici, monitorizate sever și protejate offline.
Administratori uzuali	Eligibili în PIM, MFA obligatoriu la activare, role assignment la scope minim.
Developeri	Acces pe dev/test, Contributor doar unde e nevoie, fără Owner implicit pe subscription.
Workload App Service	System-assigned managed identity, rol Key Vault Secrets User, fără secret în config.
Workload shared integration	User-assigned MI doar dacă mai multe resurse chiar au nevoie de aceeași identitate și același lifecycle.

CAPITOL 9

Monitorizare, audit și operațiuni

Identitatea trebuie tratată ca un **sistem operațional**, nu doar ca o configurare inițială. Asta înseamnă să urmărești sign-in logs, audit logs, activări PIM, role assignments și modificări de politică.

În practică, echipele bune construiesc **workbook-uri și alerte** pentru: tentative de acces blocate de Conditional Access, activări PIM neobișnuite, creșteri de sign-in risk, schimbări ale metodei de autentificare și role assignments privilegiate la scope mare.

Ce ar trebui să urmărească un inginer cloud sau identity admin

→ Roluri mari active permanent

Conturi cu roluri mari active permanent în loc de eligibile prin PIM. Acesta este un semn clar de standing privilege necontrolat.

→ Politici CA neevaluate

Politici Conditional Access care există, dar nu sunt niciodată evaluate pentru aplicațiile critice. O politică neevaluată nu protejează nimic.

→ Identități cu roluri excesive

Service principals și managed identities cu roluri excesive, precum Contributor sau Owner fără justificare clară.

→ Utilizatori cu metode slabe

Utilizatori care încă depind de metode slabe de autentificare, deși organizația a făcut rollout passwordless.

→ Excepții vechi nejustificate

Excepții vechi care au rămas în politici și nu mai sunt justificate. Tratează-le ca security debt și curăță-le periodic.

CAPITOL 10

Compararea controalelor: când folosești ce

Control	Ce face	Îl alegi când	Nu uita
Conditional Access	Controlează condițiile de acces la autentificare și sesiune	Când vrei MFA, compliant device, auth strength, blocare după context	Nu înlocuiește RBAC și nu acordă permisiuni pe resurse
PIM	Reduce standing privilege și forțează JIT	Când ai roluri privilegiate administrative sau acces sensibil temporar	Nu înlocuiește Conditional Access; le combini
Azure RBAC	Spune ce acțiuni poți face pe resurse Azure	Pentru VM, Storage, AKS, KV, subscription, RG etc.	Nu decide metoda de autentificare
Managed Identity	Dă identitate unei resurse Azure fără secrete	Pentru workload-uri care accesează alte resurse	Nu este pentru oameni și nu rezolvă governance singur
Passwordless	Îmbunătățește puternic autentificarea utilizatorului	Pentru a reduce parolele și phishing-ul	Trebuie planificate onboarding-ul și recovery

CAPITOL 11

Laborator practic recomandat pentru curs

Acest laborator este potrivit pentru o sesiune de **90-120 de minute** și îi ajută pe studenți să lege teoria de portal.

Scenariu: un tenant de test cu câțiva utilizatori, un grup de administratori, un App Service, un Key Vault și o subscription lab.

1

Creează grupuri pilot

Creează un grup pilot pentru Conditional Access și un grup separat pentru administratori eligibili în PIM.

2

Politică CA în report-only

Configurează o politică Conditional Access în report-only care cere MFA pentru grupul admin la All resources.

3

Testează sign-in și verifică logs

Generează un test sign-in și verifică rezultatul în sign-in logs pentru a vedea impactul politicii.

4

Configurează PIM

Configurează PIM pentru un rol Azure pe subscription sau RG și testează activarea cu justificare și MFA.

5

Managed Identity + Key Vault

Activează system-assigned managed identity pe un App Service și acordă-i acces minim în Key Vault.

6

TAP + Passwordless (opțional)

Configurează Temporary Access Pass pentru un user pilot și pornește înrolarea unei metode passwordless.

7

Recapitulare finală

Cere studenților să explice în propriile cuvinte diferența dintre Conditional Access, PIM și RBAC.

CAPITOL 12

Troubleshooting: probleme frecvente și cum le gândești

Problemă	Cum o abordezi
Politica Conditional Access nu pare să se aplice	Verifică dacă userul sau aplicația este în scope, dacă există exclude-uri, dacă politica e doar report-only și dacă tokenul vechi mai este valid.
Un admin are acces prea mare	Verifică dacă rolul este Active în loc de Eligible, dacă există assignment-uri directe în afara PIM și la ce scope a fost acordat rolul.
Aplicația nu poate citi secretul din Key Vault	Verifică dacă identity-ul este activat, dacă rolul RBAC este corect, dacă e vorba de access policy model versus RBAC model și dacă rețeaua/PE permit accesul.
Passwordless rollout are rezistență din partea utilizatorilor	Ai nevoie de pilot, comunicare, TAP pentru bootstrap și instrucțiuni foarte simple de recovery.
Există prea multe excepții în politici	Curăță periodic excepțiile și tratează-le ca debt de securitate, nu ca soluție permanentă.

CAPITOL 13

Best Practices de reținut

Identitatea ≠ rețeaua

Nu confunda identitatea cu rețeaua. Zero Trust începe adesea cu identitatea, nu cu firewall-ul.

Group-based assignments

Folosește group-based assignments și naming clar pentru politici și roluri. Evită selecțiile haotice user-cu-user.

Report-only → pilot → enforce

Începe cu report-only și cu pilot controlat, apoi mergi spre enforce. Nu aplica politici puternice direct în producție.

PIM pentru roluri mari

Aplică PIM pentru roluri mari și evită standing privilege. Eligible este starea normală, Active este excepția.

Managed identities pentru workload-uri

Preferă managed identities pentru workload-uri Azure în locul secretelor manuale în config files.

Metode phishing-resistant

Mergi către metode phishing-resistant acolo unde business-ul și dispozitivele permit. Redu dependența de SMS și parole.

Review regulat

Fă review regulat la policies, role assignments și excepții. Tratează excepțiile vechi ca security debt.

Combină controalele

Combină: Conditional Access + PIM + RBAC + private access + monitorizare. Niciun strat nu este singurul gardian.

CAPITOL 14

Mini-glosar pentru studenți

Authentication

Procesul prin care dovedești cine ești.

Authorization

Procesul prin care sistemul decide ce ai voie să faci.

MFA

Mai mult de un factor de autentificare.

Phishing-resistant

Metodă de autentificare mult mai greu de furat sau redirecționat prin phishing.

PIM

Serviciu pentru acces privilegiat just-in-time și governance al rolurilor sensibile.

Managed Identity

Identitate a unei resurse Azure, gestionată de platformă, fără secrete manuale.

RBAC

Model de autorizare bazat pe roluri și scope pe resurse Azure.

Conditional Access

Motorul de politici Zero Trust din Entra pentru decizii de acces.

TAP

Temporary Access Pass; folosit pentru onboarding și recovery la metode passwordless.

JIT

Just-in-time access; primești privilegiu doar când chiar ai nevoie de el.

Concluzie

> Dacă ar fi să reții doar o singură idee, aceasta este: în Azure modern, **identitatea este una dintre cele mai importante suprafețe de securitate și de operațiuni**. Nu este un subiect doar pentru echipa de identity; este un subiect pentru orice cloud engineer.

Când stăpânești Entra ID, Conditional Access, PIM, managed identities și passwordless, nu doar că securizezi mai bine platforma, ci și **simplifici foarte mult modul în care aplicațiile și oamenii lucrează în cloud**.

Acesta este tipul de cunoaștere care face diferența dintre a ști să creezi resurse în Azure și a ști să operezi Azure într-un mod **matur, enterprise și rezilient**.

🔐 Identitatea = noul perimetru

Securitatea modernă pornește de la identitate, nu de la rețea.

🏗️ Controalele se combină

CA + PIM + RBAC + Managed Identity + Monitorizare = Zero Trust real.

🚀 Operare matură

Cunoașterea identității diferențiază un inginer cloud junior de unul senior.