Azure Fundamentals — Sesiunea 02

Identitate, Acces și Control în Cloud

Cine are voie să facă ce în Azure? Astăzi răspundem la întrebarea pe care puțini și-o pun la început — și care face diferența dintre un utilizator de cloud și un profesionist de cloud.

WEBINAR • SESIUNEA 02

AZURE FUNDAMENTALS

Dacă Azure este un mall...

Imaginați-vă un mall uriaș cu sute de magazine, zeci de etaje și mii de angajați. Cineva administrează întregul mall. Fiecare magazin are propriul manager. Angajații au acces doar la magazinul lor — nu la toate.

Fără control al accesului

Dacă oricine ar putea intra în orice magazin, ar putea modifica prețurile, muta marfa, accesa casa de marcat... mall-ul ar fi un haos total în câteva zile.

Același principiu în cloud

Dacă oricine ar putea face orice în subscripția Azure a companiei — crea servere, șterge baze de date, modifica rețele, accesa date sensibile — infrastructura ar fi vulnerabilă, costurile necontrolate, și securitatea inexistentă.

De aceea există **sisteme de identitate și control al accesului.** Și astăzi explorăm cum funcționează acestea în Azure.

Ierarhia Azure și Analogia Clădirii de Birouri

PARTEA ÎNTÂI

Înainte să vorbim despre acces și permisiuni, trebuie să înțelegem structura organizatorică a Azure. Cea mai bună analogie este o clădire de birouri modernă — **compania TechCorp** cu mai multe etaje, fiecare etaj aparținând unui departament.

Tenant (Organizația)

Clădirea în ansamblu. Entitatea care deține totul, care are identitatea proprie și există ca un tot unitar. Este instanța dedicată a Entra ID pentru compania voastră.

Subscription (Etajul)

Fiecare departament cu buget propriu, resurse proprii și responsabili proprii. IT cheltuiește pe servere, Marketing pe analytics, HR pe sisteme de personal.

Resource Group (Biroul)

Proiecte specifice, echipe specifice. Fiecare birou are conținut propriu și persoane responsabile. Containerul logic pentru resurse înrudite.

Resource (Obiectele)

Calculatoarele, imprimantele, dosarele din birouri — adică mașinile virtuale, bazele de date, storage-ul, rețelele. Resursele efective Azure.

Fiecare angajat are un **badge de acces** — un rol — care spune exact unde poate intra și ce poate face. Unii au acces la tot etajul, alții doar la birou, alții doar citesc documente. Unul singur are cheia tuturor ușilor: **administratorul clădirii.**

De ce companiile folosesc mai multe Subscription-uri?

Dacă ai o companie, de ce nu pui totul într-o singură Subscription? Pe termen scurt pare mai simplu. Pe termen lung este o problemă serioasă.

1 Separarea bugetelor

O Subscription este o entitate de billing separată. Cu Subscription-uri distincte, fiecare departament are propria factură, propriul buget, propriile limite de cheltuieli — vizibilitate financiară completă.

2 Separarea responsabilităților

Administratorul IT nu ar trebui să aibă acces automat la resursele HR — date de personal, contracte, salarii. Subscription-uri separate înseamnă că un accident în IT nu poate afecta datele HR.

3 Reducerea riscului

Dacă un incident de securitate compromite o Subscription, celelalte sunt izolate. Un atacator în Subscription-ul de Marketing nu ajunge automat la serverele de producție din IT.

4 Managementul limitelor Azure

Azure impune limite pe Subscription-uri pentru diverse resurse: numărul maxim de VM-uri, adrese IP publice, capacitate de rețea. Distribuind resursele, evitați atingerea acestor limite.

Concluzie: Mai multe Subscription-uri nu înseamnă complexitate inutilă. Înseamnă organizare profesională.

Microsoft Entra ID — Sistemul de Identitate al Azure

PARTEA A DOUA

Ajungem la fundamentul tehnic al tot ceea ce discutăm astăzi: **Microsoft Entra ID** — fost cunoscut ca Azure Active Directory (Azure AD). Microsoft a redenumit serviciul în 2023, dar în documentație și conversații tehnice veți întâlni ambele denumiri. Important: sunt **același serviciu.**

Ce este Entra ID?

Sistemul de management al identității și accesului în Azure. Locul unde există utilizatorii, grupurile, aplicațiile și regulile care determină cine poate face ce. Verifică identitatea și emite token-uri de autentificare.

Ce conține un Tenant?

Toți utilizatorii organizației, toate grupurile, toate aplicațiile înregistrate și toate politicile de securitate și acces. Identificat printr-un Tenant ID unic global și un domeniu de forma `numefirma.onmicrosoft.com`.

Cine există în Entra ID?

Orice persoană care accesează Azure — administrator, developer, sau stagiar — există ca utilizator sau invitat. Orice aplicație care accesează resurse programatic există ca Service Principal sau Managed Identity.

Analogia Bancară: Account, Tenant, Subscription

Aceasta este una din confuziile cele mai frecvente la juniori. O analogie simplă clarifică totul:

→ Account = Contul personal de bancă

Identitatea voastră. Emailul, credențialele, profilul vostru. Voi ca persoană. **Account-ul este cine sunteți.**

→ Tenant = Banca în sine

Instituția care gestionează toate conturile, verifică identitățile, aplică regulile. Poate fi ING, BCR, Raiffeisen — fiecare bancă este un Tenant separat. **Tenant-ul este organizația în care existați.**

→ Subscription = Produsele bancare

Contul de economii, contul curent, cardul de credit — fiecare este un container separat de resurse și billing. Puteți avea mai multe produse la aceeași bancă. **Subscription-ul este containerul de resurse pe care îl folosiți.**

Authentication vs. Authorization — Două Concepte Critice

🔑 Authentication

Dovedești cine ești. Procesul de verificare a identității. Introduci emailul și parola, sau codul MFA. Sistemul verifică că ești cine spui că ești.

Analogia: arăți buletinul la intrarea în clădire. Securitatea verifică că fotografia corespunde cu fața ta.

🛡️ Authorization

Dovedești ce ai voie să faci. După verificarea identității, sistemul verifică ce permisiuni ai. Poți accesa sala de conferințe? Poți intra în serverroom? Poți modifica setările de rețea?

Analogia: după ce ai arătat buletinul, primești un badge de acces. Badge-ul permite intrarea la etajele 3 și 4, dar nu la etajul 5.

Entra ID gestionează ambele. Verifică identitățile și emite token-uri care conțin informații despre ce are voie să facă utilizatorul respectiv. Chiar dacă cineva obține credențialele unui utilizator, daunele sunt limitate de permisiunile acelui utilizator.

Entra ID în Portal — Ce Vedeți în Practică

Overview

Tenant ID-ul, numele organizației, domeniul implicit, statistici despre utilizatori și aplicații active.

Users

Lista tuturor utilizatorilor din Tenant. Creați utilizatori noi, modificați profiluri, resetați parole, activați sau dezactivați conturi.

Groups

Organizați utilizatorii în grupuri. Atribuiți roluri grupurilor — nu individual — și adăugați utilizatori în grupuri. Angajatul nou primește automat toate permisiunile grupului.

Conditional Access

Politici complexe: accesul din afara rețelei de birou necesită MFA obligatoriu, sau accesul la portal doar de pe dispozitive corporate.

RBAC — Role-Based Access Control

PARTEA A TREIA

RBAC este mecanismul prin care Azure decide ce poate face o persoană sau un serviciu cu o resursă specifică. Se bazează pe **trei concepte simple** care combinate formează o Role Assignment.

Security Principal

Entitatea căreia îi atribuiți acces: utilizator individual, grup de utilizatori, aplicație, sau identitate gestionată de Azure.

Role Definition

Lista de permisiuni — ce acțiuni sunt permise și ce sunt interzise. Azure are zeci de roluri predefinite, de la roluri generale la roluri specifice fiecărui serviciu.

Scope

Nivelul la care se aplică rolul: Management Group, Subscription, Resource Group, sau resursă individuală. Cu cât scope-ul este mai larg, cu atât mai multe resurse sunt afectate.

Cele Trei Roluri Fundamentale

👑 Owner — Proprietarul

Control complet. Poate crea, modifica și șterge resurse. **Poate gestiona accesul** altor utilizatori — atribuie și revocă roluri. Poate face absolut orice în scope-ul respectiv.

🔧 Contributor — Colaboratorul

Poate crea, modifica și șterge resurse. **Nu poate gestiona accesul.** Nu poate da sau lua roluri altor utilizatori. Poate construi și poate distruge, dar nu controlează cine are acces.

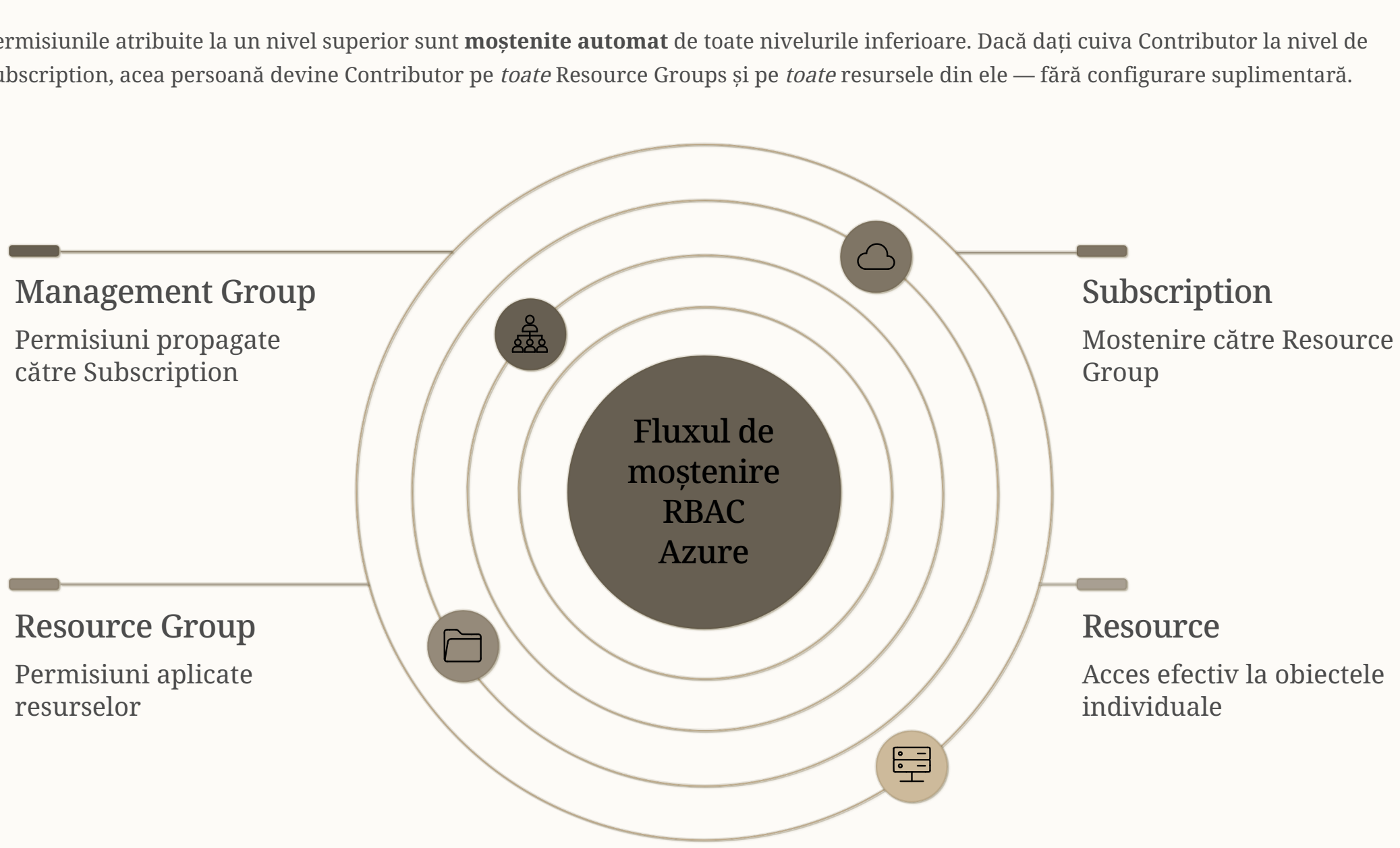
👁️ Reader — Cititorul

Poate vedea resursele, citi configurațiile, accesa log-urile. **Nu poate modifica nimic.** Rolul de observator — ideal pentru QA, audit, sau stagiari în explorare.

Diferența cheie Owner vs. Contributor: Owner poate da sau lua acces altora. Contributor nu poate. Managementul accesului rămâne în mâinile celor cu rol Owner sau cu roluri administrative dedicate.

Moștenirea Permisiunilor — Sabia cu Două Tăișuri

Permisiunile atribuite la un nivel superior sunt **moștenite automat** de toate nivelurile inferioare. Dacă dați cuiva Contributor la nivel de Subscription, acea persoană devine Contributor pe *toate* Resource Groups și pe *toate* resursele din ele — fără configurare suplimentară.



Aceasta simplifică managementul, dar impune prudență: un rol la nivel înalt moștenește la tot. De aceea atribuiți roluri la **cel mai jos nivel de scope necesar.**

Scenarii Practice — Cine Primește Ce Rol?

Persoană	Rol	Scope	Justificare
Ana — QA	Reader	Resource Group relevant	Verifică log-uri și status; nu creează, nu modifică nimic
Mihai — Developer	Contributor	RG de development al proiectului	Creează VM-uri și deploye aplicații; nu gestionează accesul colegilor
Andrei — Tech Lead	Owner	Subscription sau RG proiect	Responsabil pentru resurse, buget și accesul echipei
Maria — Intern	Reader	RG de development selectat	Explorare fără risc; prima săptămână, familiarizare cu platforma

Observați pattern-ul: **cu cât responsabilitatea este mai mare, cu atât rolul este mai larg — dar cu cât rolul este mai larg, cu atât scope-ul ar trebui să fie mai restricționat.**

Roluri Personalizate în Azure

Pe lângă rolurile predefinite, Azure permite crearea de **Custom Roles** — roluri create de voi, cu exact permisiunile pe care le specificați. De exemplu: un operator care poate porni și opri VM-uri, fără să poată crea sau șterge. Sau un rol care permite citirea log-urilor de securitate fără acces la datele aplicației. Dacă niciun rol predefinit nu se potrivește exact, nu sunteți obligați să dați un rol mai larg decât este necesar.

Least Privilege — Principiul Care Previne Catastrofele

PARTEA A PATRA

> "Orice utilizator, serviciu, sau proces ar trebui să aibă exact atâtea permisiuni câte are nevoie pentru a-și îndeplini rolul. **Nimic mai mult.**"

Sună simplu. Sună chiar evident. Și totuși este ignorat constant în practică — pentru că a respecta Least Privilege necesită efort: trebuie să înțelegi ce face fiecare persoană, ce resurse accesează, ce operațiuni efectuează. Este mult mai simplu să dai Owner la nivel de Subscription în treizeci de secunde. Dar acea decizie de treizeci de secunde poate costa compania mii de euro atunci când se materializează consecințele.

Povestea Internului cu Owner — O Lecție Reală

Ce s-a întâmplat

O companie mică angajează un intern. Managerul tehnic, grăbit, îl adaugă ca **Owner la nivel de Subscription.** Internul, entuziast, urmărește un tutorial de cleanup al resurselor neutilizate. Vede un Resource Group cu un nume similar celui pe care lucrează. Aplică tutorialul. Confirmă ștergerea.

Resource Group-ul șters conținea **baza de date de producție** a aplicației principale. Aplicația cade. Clienții nu pot accesa serviciul. Compania pierde ore de venituri și zile de muncă pentru recuperare din backup.

Cine este vinovat?

Internul nu a avut intenții rele. A crezut că face ceva util. A urmat instrucțiunile unui tutorial.

Managerul este vinovat. Cel care a dat Owner pe Subscription unui intern în prima săptămână, fără să înțeleagă implicațiile.

Ce ar fi trebuit să se întâmple

Dacă internul ar fi avut Contributor (sau Reader) pe un singur Resource Group de development — cel pe care lucra el — nu ar fi putut atinge nimic altceva. Greșeala nu ar fi avut niciun impact.

Least Privilege nu înseamnă că nu ai încredere în oameni. Înseamnă că accidentele sunt inevitabile și că minimizezi suprafața potențialului accident.

Cele Mai Frecvente Greșeli de Access în Companii

Toți au Owner pe Subscription

Toată echipa de development are Owner pe subscripția de producție. Convenabil pe termen scurt. Bombă cu ceas pe termen lung.

Accesul nu este revocat când oamenii pleacă

Un angajat pleacă. Contul Azure rămâne activ cu acces complet timp de săptămâni sau luni. Vulnerabilitate de securitate serioasă.

Accesul temporar devine permanent

Un consultant extern primește acces pentru un proiect de două luni. Proiectul se termină. Accesul nu este revocat. Consultantul are în continuare acces la resursele companiei.

Roluri la nivel greșit de scope

Un junior primește Contributor pe Subscription, când are nevoie doar de Contributor pe un singur Resource Group. Greșeală frecventă din grabă sau necunoaștere.

Nu există audit regulat al accesurilor

Nimeni nu verifică periodic cine are ce acces. Lista utilizatorilor cu acces crește în timp, fără să fie curățată. Oameni care au plecat din proiect — dar nu din firmă — au în continuare acces.

Concepte Avansate: PIM, Access Reviews, Managed Identities

Privileged Identity Management (PIM)

Roluri eligibile activate temporar, nu permanent. Un utilizator activează Owner pentru **două ore**, uneori cu justificare și aprobare managerială, apoi rolul expiră automat. Principiul **Just-in-Time Access.**

Access Reviews

Proces programat în care managerii confirmă periodic dacă accesul mai este necesar. Trimestrial, toți deținătorii de rol Owner sunt întrebați dacă mai au nevoie. Dacă nu răspund, accesul poate fi revocat automat.

Managed Identities

Identități gestionate automat de Azure pentru aplicații și scripturi — fără secrete pe care le gestionați voi. Azure rotește credențialele în fundal. **Best practice pentru aplicațiile Azure moderne.**

Exercițiu Practic — Azure Portal

PARTEA A CINCEA

Hai să vedem cum arată toate acestea în **Azure Portal.** Urmăriți pașii împreună, în timp real.

Pasul 1 — Explorați Microsoft Entra ID

01

Navigați la Entra ID

Deschideți bara de căutare de sus în Azure Portal și scrieți `Microsoft Entra ID`. Selectați serviciul din rezultate.

02

Explorați Overview

Vedeți **Tenant Name** (numele organizației), **Tenant ID** (un GUID unic lung), și **Primary Domain**. Acestea sunt datele de identitate ale organizației voastre.

03

Accesați Users

Faceți click pe **Users** în meniu. Vedeți contul vostru listat acolo. Aceasta este identitatea voastră în acest Tenant — utilizatorul cu care sunteți autentificat.

Pasul 2 — Creați Resource Group-ul Sesiunii

01

Deschideți Resource Groups

Reveniți la Azure Portal principal. Scrieți `Resource Groups` în bara de căutare și selectați serviciul.

02

Creați un Resource Group nou

Dați **Create**. La **Name**, scrieți `rg-s02-[prenumele vostru]`. La **Region**, selectați `West Europe`.

03

Finalizați crearea

Dați **Review and Create**, apoi **Create**. Așteptați notificarea de confirmare a creării cu succes.

Pasul 3 — Explorați Access Control (IAM)

01

Navigați la Access Control

Deschideți Resource Group-ul vostru. În meniul din stânga, găsiți și selectați **Access Control (IAM)** — Identity and Access Management.

02

Vizualizați Role Assignments

Dați click pe **Role Assignments**. Vedeți toți utilizatorii cu roluri pe acest Resource Group. Observați coloana **Scope** — dacă rolul este moștenit de la Subscription, veți vedea indicatorul de moștenire.

03

Explorați Add Role Assignment

Dați click pe **Add → Add Role Assignment**. Explorați wizard-ul: vedeți rolurile disponibile (Owner, Contributor, Reader și zeci altele). **Nu adăugăm niciun rol acum** — explorăm doar interfața. Dați Cancel.

Acum știți unde mergeți când trebuie să gestionați accesul pe o resursă. Panoul IAM este punctul central de control RBAC pentru orice resursă Azure.

Recap — Cinci Întrebări de Tip Examen

Să consolidăm sesiunea de astăzi. Acestea sunt întrebări pe care le-ați putea întâlni în examenul **AZ-900** sau în orice interviu tehnic Azure.

1

Ce este RBAC?

Role-Based Access Control — sistemul Azure prin care controlați cine poate face ce cu resursele. Se bazează pe atribuirea de roluri (seturi de permisiuni) utilizatorilor sau grupurilor, la niveluri de scope specifice. Combinarea Security Principal + Role Definition + Scope = Role Assignment.

2

Owner vs. Contributor — care este diferența?

Ambii pot crea, modifica și șterge resurse. Diferența esențială: **Owner poate gestiona accesul** — atribuie și revocă roluri altor utilizatori. **Contributor nu poate.** Contributor construiește. Owner construiește și controlează cine mai poate construi.

3

Authentication vs. Authorization?

Authentication = verificarea identității (dovedești cine ești). **Authorization** = verificarea permisiunilor (dovedești ce ai voie să faci). Authentication precede Authorization. Mai întâi confirmați identitatea, apoi sistemul verifică permisiunile.

4

Ce este un Tenant?

Instanța dedicată de **Microsoft Entra ID** pentru o organizație. Containerul care conține toți utilizatorii, toate grupurile și toate politicile de identitate și acces. O organizație are în mod normal un singur Tenant.

5

Ce înseamnă Least Privilege?

Orice utilizator sau serviciu primește **exact atâtea permisiuni câte are nevoie** pentru rolul său — nimic mai mult. Reduce suprafața potențialului incident la minimum. Dacă un cont este compromis sau dacă un utilizator face o greșeală, daunele sunt limitate de permisiunile acelui cont.

Tema pentru Acasă — Sesiunea 02

Tema de astăzi are **trei componente** și vă rog să le abordați serios. Scopul nu este să copiați din documentație — ci să asimilați conceptele și să le exprimați cu propriile cuvinte.

📝 Componenta 1 — Teoria

Scrieți în **5–7 propoziții** cu cuvintele voastre:

- Diferența dintre Tenant, Subscription și Account
- Ce este RBAC și cum funcționează
- Ce este Least Privilege și de ce contează

Nu copiați din documentație. Scrieți ca și cum ați explica unui coleg nou, în primul lui sprint.

🏢 Componenta 2 — Scenariul Aplicat

Sunteți responsabilul tehnic al unei firme mici cu **patru persoane**: un Developer, un QA, un Manager, și un Intern. Definiți:

- Ce rol primește fiecare?
- La ce nivel de scope?
- De ce acel rol și nu altul?

Există mai multe răspunsuri corecte. Ceea ce contează este argumentarea.

💭 Componenta 3 — Mini-Reflecția

Răspundeți în **3–5 propoziții** la această întrebare:

"De ce accesul prea mare este periculos chiar dacă ai deplină încredere în persoana respectivă?"

Aceasta nu este o întrebare cu răspuns tehnic. Este o întrebare de mentalitate. Reflectați sincer — nu există răspuns greșit dacă este gândit.

Privire spre Sesiunea 03

La sesiunea viitoare construim **al doilea strat al fundației Azure.** Dacă sesiunea de astăzi a transformat mentalitatea din perspectiva accesului, sesiunea viitoare o va face din perspectiva **organizării resurselor.**

1

Regiuni Azure

De ce contează unde se află resursele voastre și cum alegeți corect Region-ul pentru fiecare resursă.

2

Resource Groups în Detaliu

Nu doar ce sunt, ci cum se proiectează corect pentru a reflecta structura organizației și a proiectelor.

3

Naming Conventions

De ce juniorii care știu să numească resursele corect par deja mid-level. Standarde și pattern-uri reale din industrie.

4

Tag-uri Azure

Metadate care transformă organizarea haotică în organizare profesională. Billing, ownership, mediu — toate gestionate prin tag-uri.

Veți înțelege de ce organizarea resurselor nu este o preferință estetică, ci o **necesitate operațională.** Veți crea primul Resource Group cu naming consistent și tag-uri corecte.

Schimbarea de Mentalitate

> "Diferența nu este despre tehnic. Este despre **responsabilitate.**"

Perspectiva Utilizatorului

Ați venit la sesiunea unu și ați descoperit că puteți crea lucruri în cloud. Ați simțit accesibilitatea platformei, puterea de a crea servere și resurse cu câteva clickuri. **Știți cum.**

Perspectiva Profesionistului

Astăzi ați adăugat o perspectivă diferită. Nu toți au voie să creeze lucruri. Nu toți ar trebui să poată șterge orice. Accesul este controlat, structurat și deliberat. **Știți și cine, și de ce, și cu ce nivel de acces.**

Resursele cloud costă bani reali. Datele pe care le protejați aparțin unor oameni reali. Erorile — chiar și cele bine intenționate — au consecințe reale.

3	4	2
Roluri fundamentale	**Niveluri de scope**	**Concepte de identitate**
Owner, Contributor, Reader — fundația oricărei strategii RBAC	Management Group → Subscription → Resource Group → Resource	Authentication și Authorization — distincte, secvențiale, ambele critice

Un junior care înțelege Least Privilege, care știe să configureze RBAC corect, și care poate explica diferența dintre Tenant, Subscription și Account este un junior care **gândește ca un profesionist.** Mentalitatea corectă este fundația pe care restul se construiește. Ne vedem la Sesiunea 03!