

MANUAL AZURE: IDENTITATE, SECURITATE ȘI MANAGEMENT

Partea a V-a: Gardianul Regatului

Bun Venit, Viitor Lord Comandant!

Ai ajuns la capitolul final al călătoriei tale în Azure! Până acum ai construit infrastructura (Compute), ai stocat datele (Storage) și ai conectat totul (Networking). Acum este timpul să înveți cum să **protejezi** și să **guvernezi** întregul regat digital.

În acest manual, vei descoperi:

- **Microsoft Entra ID:** Sistemul de identitate și acces
- **RBAC:** Controlul accesului bazat pe roluri
- **Azure Policy:** Legiuitorul regatului tău
- **Azure Monitor:** Ochiul atotvăzător
- **Cost Management:** Trezoreria sub control

Total XP disponibil în acest manual: 1,600 XP

Achievement-uri de deblocat: 5

Pregătește-te să devii un adevărat **Kingdom Commander!** 



CAPITOLUL 15: Microsoft Entra ID - Pașaportul Tău Digital în Cloud

Tema Gamification: “Gardianul Identității”

Nivel: Beginner-Intermediate (★★★)

Bun venit în centrul de comandă al securității! Orice fortăreață, oricât de bine construită, este vulnerabilă dacă nu știi cine intră și cineiese. În acest capitol, vei învăța despre **Microsoft Entra ID** (cunoscut anterior ca Azure Active Directory), serviciul care acționează ca un pașaport digital pentru toate resursele tale. Vei

descoperi cum să gestionezi utilizatori, grupuri și roluri pentru a te asigura că doar persoanele potrivite au accesul potrivit. Stăpânirea acestor concepte îți va aduce achievement-ul **Identity Guardian**!

15.1 Ce este Microsoft Entra ID?

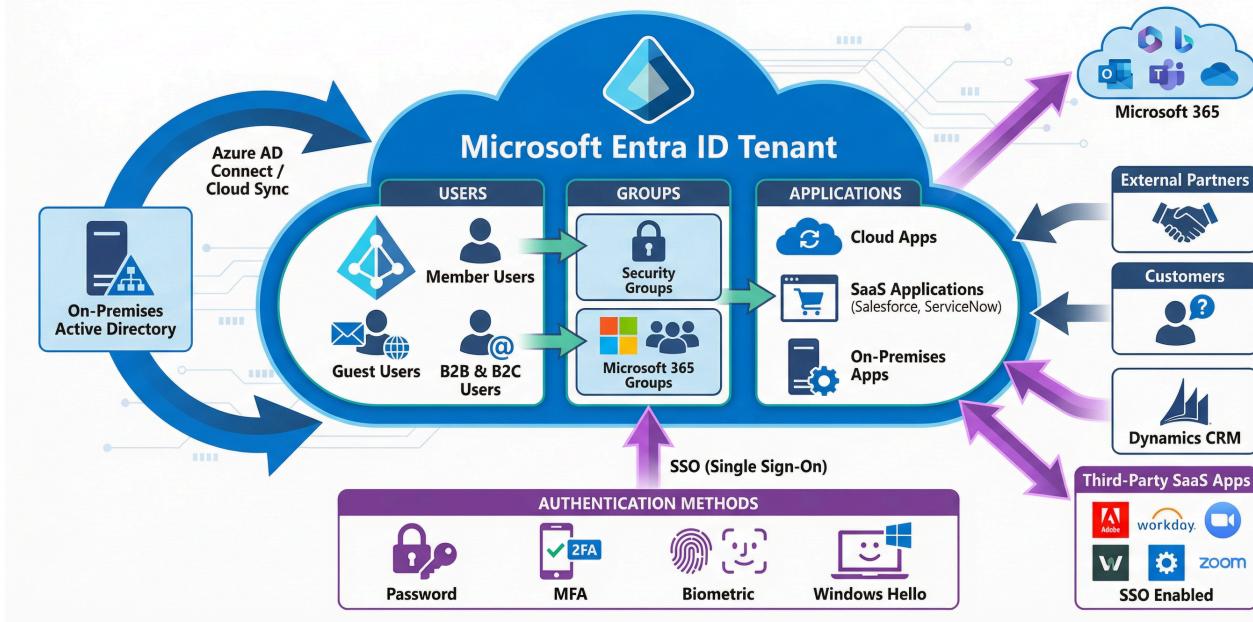
Microsoft Entra ID este un serviciu de management al identității și accesului (Identity and Access Management - IAM) bazat pe cloud. Este motorul care alimentează autentificarea și autorizarea pentru Azure, Microsoft 365, Dynamics 365 și mii de alte aplicații non-Microsoft (SaaS).

Analogie: Gândește-te la Entra ID ca la recepția unei clădiri de birouri globale. Fiecare angajat (utilizator) are un ecuson (identitate digitală). Când angajatul vrea să intre într-un birou (să acceseze o resursă), el prezintă ecusonul. Recepționerul (Entra ID) verifică dacă ecusonul este valid (autentificare) și dacă angajatul are permisiunea de a intra în acel birou specific (autorizare). Acest sistem funcționează nu doar pentru clădirea principală (Azure), ci și pentru birourile partenere din întreaga lume (alte aplicații cloud).

Ce face Entra ID?

- **Autentificare:** Verifică identitatea unui utilizator (ex: prin parolă, Multi-Factor Authentication - MFA, biometrie).
- **Single Sign-On (SSO):** Permite utilizatorilor să se autentifice o singură dată și să acceseze mai multe aplicații fără a se re-autentifica.
- **Managementul Utilizatorilor și Grupurilor:** Permite crearea și gestionarea conturilor de utilizator și gruparea lor logică.
- **Managementul Accesului la Aplicații:** Controlează cine are acces la ce aplicații.
- **Securitate:** Oferă funcționalități avansate precum Conditional Access, Identity Protection și managementul dispozitivelor.

Microsoft Entra ID (Azure AD) Architecture Overview



15.2 Utilizatori (Users)

Un **obiect de tip utilizator** reprezintă o identitate în Entra ID. Există mai multe tipuri de utilizatori:

- **Utilizatori Membri (Member Users):**
 - Sunt utilizatori nativi ai directorului tău (tenant).
 - De obicei, sunt angajații organizației tale.
 - Au un User Principal Name (UPN) de forma
nume.utilizator@domeniultau.onmicrosoft.com sau
nume.utilizator@domeniulcustom.com .
- **Utilizatori Invitați (Guest Users):**
 - Sunt utilizatori dintr-un alt director Entra ID sau cu orice alt cont de email (ex: Gmail, Yahoo).
 - Sunt invitați în directorul tău pentru a colabora la anumite proiecte sau resurse.
 - Au un UPN care reflectă identitatea lor externă, cu un format special (ex: john.doe_gmail.com#EXT#@domeniultau.onmicrosoft.com).
 - Au permișii limitate în mod implicit.

15.3 Grupuri (Groups)

Grupurile sunt colecții de utilizatori (sau alte obiecte, precum dispozitive sau chiar alte grupuri). Folosirea grupurilor simplifică enorm managementul accesului.

Best Practice: În loc să acorzi permisiuni direct utilizatorilor individuali, acordă permisiuni grupurilor. Când un utilizator nou are nevoie de aceleași permisiuni, pur și simplu îl adaugă în grupul respectiv. Când un utilizator părăsește organizația, îl scoți din grupuri, iar toate permisiunile sale sunt revocate automat. Aceasta este o abordare mult mai scalabilă și mai puțin predispusă la erori.

Tipuri de Grupuri:

- **Security Groups:**
 - Scopul principal este de a acorda permisiuni la resurse (ex: acces la un site SharePoint, la o aplicație sau la resurse Azure prin RBAC).
- **Microsoft 365 Groups:**
 - Sunt create pentru colaborare. Când creezi un grup Microsoft 365, primești automat o suita de resurse partajate: o căsuță de email partajată, un calendar, un site SharePoint, un planificator (Planner) etc.
 - Pot fi folosite și pentru securitate (orice grup Microsoft 365 poate acționa ca un grup de securitate).

Tipuri de Apartenență (Membership Types):

- **Assigned:** Administratorul adaugă și elimină manual membrii.
- **Dynamic User:** Membrii sunt adăugați sau eliminați automat pe baza unor reguli. De exemplu, poți crea un grup dinamic care conține toți utilizatorii din departamentul "Vânzări" (bazat pe atributul `department` al utilizatorului). *Necesită licență Entra ID P1 sau P2.*
- **Dynamic Device:** Similar cu Dynamic User, dar pentru dispozitive (ex: toate dispozitivele cu Windows 11).

15.4 Roluri Administrative în Entra ID

Acestea sunt roluri care acordă permisiuni pentru a gestiona **resursele din interiorul Entra ID**. Nu trebuie confundate cu rolurile RBAC pentru resursele Azure (despre care vom vorbi în capitolul următor).

Exemple de Roluri Administrative Comune:

- **Global Administrator:** “Regele” directorului. Are permisiuni complete asupra tuturor aspectelor din Entra ID și Azure. De folosit cu maximă precauție!
- **User Administrator:** Poate crea și gestiona utilizatori și grupuri, reseta parole etc.
- **Helpdesk Administrator:** Poate reseta parolele pentru utilizatorii non-administratori.
- **Billing Administrator:** Poate gestiona abonamentele, facturile și plățile.
- **Security Administrator:** Poate gestiona funcționalitățile de securitate, precum Identity Protection și Conditional Access.

Principiul Privilegiului Minim (Principle of Least Privilege): Acordă utilizatorilor doar permisiunile de care au absolută nevoie pentru a-și îndeplini sarcinile, și nimic mai mult. Nu acorda rolul de Global Administrator decât dacă este strict necesar. Folosește roluri mai specifice, precum User Administrator sau Helpdesk Administrator.

★ QUIZ TIME! ★

1. Care este principalul scop al Microsoft Entra ID?
 - a) Stocarea fișierelor în cloud.
 - b) Managementul identității și accesului (IAM).
 - c) Rularea de mașini virtuale.
2. Ce tip de utilizator ai crea pentru un consultant extern care are nevoie de acces temporar la un proiect?
 - a) Member User
 - b) Guest User
 - c) Service Principal
3. Care este cea mai bună practică pentru acordarea de permisiuni?
 - a) Acordarea permisiunilor direct utilizatorilor individuali.
 - b) Acordarea permisiunilor grupurilor și adăugarea utilizatorilor în acele grupuri.
 - c) Acordarea rolului de Global Administrator tuturor utilizatorilor.
4. Ce tip de grup adaugă automat membri pe baza unui atribut, cum ar fi departamentul?

- a) Assigned Security Group
 - b) Microsoft 365 Group
 - c) Dynamic User Group
5. Ce rol administrativ are permisiuni complete asupra întregului director Entra ID?
- a) User Administrator
 - b) Global Administrator
 - c) Security Administrator

(Răspunsuri la finalul manualului)

Ai învățat cum să gestionezi identitățile, pașapoartele digitale ale cloud-ului tău. Ești acum pregătit să înveți cum să folosești aceste identități pentru a controla accesul la resursele Azure.

 Achievement Deblocat: Identity Guardian 
+250 XP

CAPITOLUL 16: Role-Based Access Control (RBAC) - Cheile Regatului Tău Azure

Tema Gamification: “Maestrul Cheilor”

Nivel: Intermediate (

Ai creat identitățile, dar acum trebuie să decizi ce uși pot deschide acestea în regatul tău Azure. În acest capitol, vei învăța despre **Role-Based Access Control (RBAC)**, sistemul de autorizare care îți permite să acorzi permisiuni granulare la resursele Azure. Vei învăța cum să folosești roluri pentru a defini “ce se poate face” și scope-uri pentru a defini “unde se poate face”. Stăpânirea RBAC este esențială pentru securitate și îți va aduce achievement-ul **Key Master!**

16.1 Ce este Azure RBAC?

Azure Role-Based Access Control (RBAC) este un sistem de autorizare construit pe **Azure Resource Manager (ARM)** care oferă un management detaliat al accesului la resursele Azure. Cu RBAC, poți acorda exact permisiunile de care utilizatorii au nevoie pentru a-și face treaba, conform principiului privilegiului minim.

Analogie: Dacă *Entra ID* este serviciul care emite pașapoarte (identități), RBAC este sistemul care emite vize și chei. Un pașaport dovedește cine ești. O viză (rolul) specifică ce ai voie să faci într-o anumită țară (ex: turist, muncitor, diplomat). Cheia (scope-ul) îți dă acces doar la o anumită clădire sau cameră din acea țară (ex: un hotel, o sală de conferințe).

16.2 Cele Trei Componente ale unei Atribuirile de Rol (Role Assignment)

O atribuire de rol (role assignment) este procesul prin care acorzi acces. Aceasta are trei componente fundamentale:

1. Security Principal (Cine?):

- Obiectul care solicită accesul. Poate fi:
 - Un **User** (un angajat, un dezvoltator).
 - Un **Group** (un grup de administratori, un grup de dezvoltatori).
 - Un **Service Principal** (o identitate pentru o aplicație sau un script automatizat).
 - O **Managed Identity** (o identitate gestionată de Azure pentru servicii Azure, cum ar fi o mașină virtuală care trebuie să acceseze un Key Vault).

2. Role Definition (Ce?):

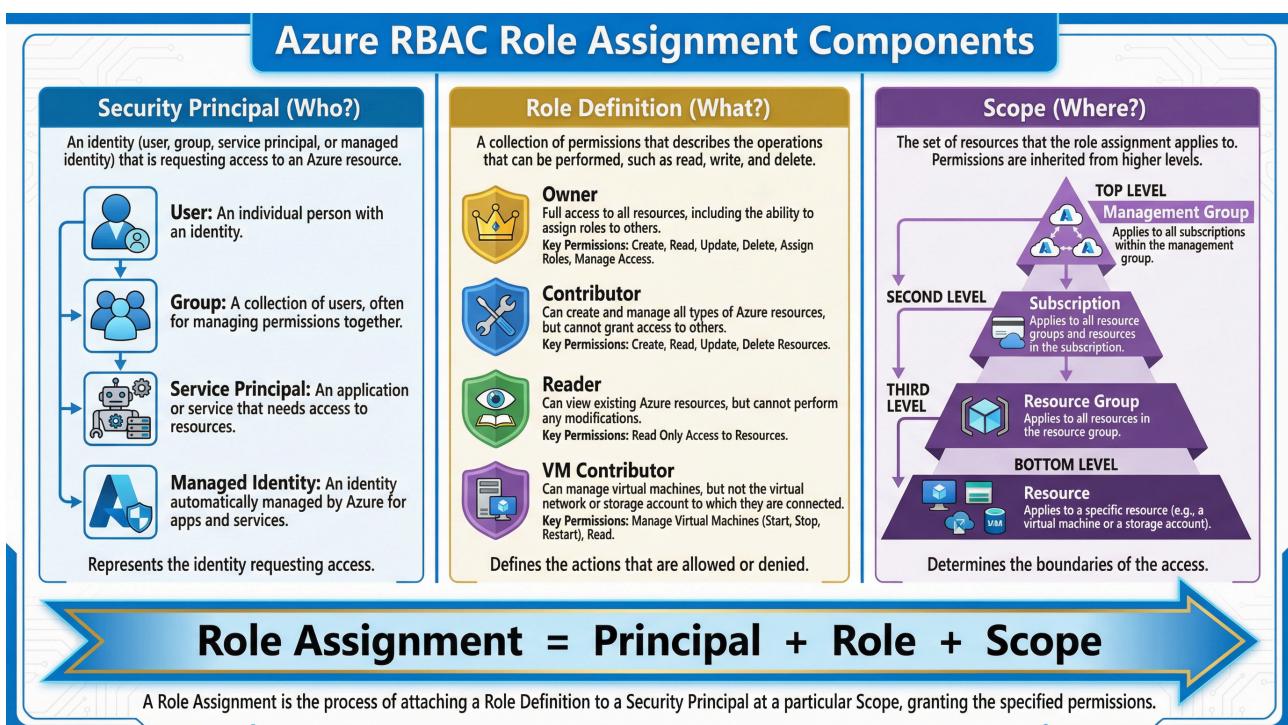
- O colecție de permisiuni. Un rol definește acțiunile care pot fi efectuate, cum ar fi `read`, `write`, `delete`.
- Acțiunile sunt de forma `Microsoft.Compute/virtualMachines/start/action` (permisiunea de a porni o mașină virtuală).
- Există sute de **roluri predefinite (built-in roles)**, cum ar fi:
 - **Owner:** Are control total asupra tuturor resurselor, inclusiv dreptul de a acorda acces altora.
 - **Contributor:** Poate crea și gestiona toate tipurile de resurse Azure, dar nu poate acorda acces altora.
 - **Reader:** Poate vizualiza resursele Azure, dar nu le poate modifica.

- **Virtual Machine Contributor:** Poate gestiona mașini virtuale, dar nu și rețea virtuală sau contul de stocare la care sunt conectate.
- Poți crea și **roluri personalizate (custom roles)** dacă cele predefinite nu sunt suficiente.

3. Scope (Unde?):

- Nivelul la care se aplică permisiunile. Scope-ul în Azure are o structură ierarhică, de la larg la specific:
 - **Management Group:** La cel mai înalt nivel, pentru a aplica permisiuni la mai multe abonamente.
 - **Subscription:** La nivel de abonament, pentru a aplica permisiuni la toate resursele din acel abonament.
 - **Resource Group:** La nivel de grup de resurse, pentru a aplica permisiuni la toate resursele dintr-un grup.
 - **Resource:** La nivelul unei resurse individuale (ex: o singură mașină virtuală).

Moștenirea Permisiunilor: Permisiunile sunt moștenite de la scope-urile părinte la cele copil. Dacă acorzi rolul de **Reader** la nivel de abonament, acel utilizator va putea vedea **toate** grupurile de resurse și resursele din acel abonament. Dacă acorzi rolul de **Contributor** la nivel de grup de resurse, utilizatorul poate gestiona **toate** resursele din acel grup, dar nu și din alte grupuri de resurse.



16.3 Cum funcționează RBAC?

Când un utilizator încearcă să acceseze o resursă, Azure Resource Manager (ARM) verifică toate atribuirile de rol care se aplică acestui utilizator (direct sau prin grupuri) la scope-ul resursei respective (și la toate scope-urile părinte).

RBAC este un **model aditiv**. Asta înseamnă că permisiunile efective ale unui utilizator sunt **suma** tuturor permisiunilor acordate prin diferitele sale roluri.

Exemplu:

- Ana este în grupul `Dev-Team`.
- Grupului `Dev-Team` i se acordă rolul de **Reader** la nivelul abonamentului `Production-Sub`.
- Anei i se acordă direct rolul de **Virtual Machine Contributor** la nivelul grupului de resurse `WebApp-RG` (care se află în `Production-Sub`).

Permisiunile efective ale Anei:

- Ea poate **vedea (Read)** toate resursele din întregul abonament `Production-Sub` (moștenit de la grup).
- Ea poate **gestiona (Contribute)** mașinile virtuale **doar** din grupul de resurse `WebApp-RG`.
- Ea nu poate gestiona alte tipuri de resurse (ex: baze de date) din `WebApp-RG` și nu poate gestiona nicio resursă din alte grupuri de resurse.

16.4 Best Practices pentru RBAC

- **Folosește Principiul Privilegiului Minim:** Acordă întotdeauna cel mai restrictiv rol care permite utilizatorului să-și facă treaba.
- **Acordă Roluri la Cel Mai Mic Scope Posibil:** În loc să acorzi rolul de `Contributor` la nivel de abonament, acordă-l la nivelul grupului de resurse specific unde utilizatorul trebuie să lucreze.
- **Folosește Grupuri:** Atribuie roluri grupurilor din Entitate ID, nu utilizatorilor individuali. Este mult mai ușor de gestionat pe termen lung.
- **Folosește Roluri Predefinite (Built-in):** Acestea sunt testate și menținute de Microsoft. Creează roluri personalizate doar atunci când este absolut necesar.

- **Evită Rolul de Owner:** Rolul de Owner este extrem de puternic. Limitează numărul de Owner-i la nivel de abonament la un minim absolut (ex: 2-3 persoane de încredere).
-

★ QUIZ TIME! ★

1. Care sunt cele trei componente ale unei atribuiri de rol RBAC?
 - a) User, Password, Scope
 - b) Security Principal, Role Definition, Scope
 - c) Role, Permission, Resource
2. Ce rol permite unui utilizator să creeze și să gestioneze resurse, dar NU să acorde acces altora?
 - a) Owner
 - b) Reader
 - c) Contributor
3. Dacă acorzi unui utilizator rolul de Reader la nivel de grup de resurse, ce va putea face acesta?
 - a) Va putea vedea toate resursele din întregul abonament.
 - b) Va putea vedea doar resursele din acel grup de resurse.
 - c) Va putea modifica resursele din acel grup de resurse.
4. Ce înseamnă că RBAC este un model “aditiv”?
 - a) Permișunile se anulează reciproc.
 - b) Permișunile efective sunt suma tuturor rolurilor atribuite.
 - c) Se aplică doar ultima regulă de permisiune.
5. Care este cea mai bună practică pentru a acorda acces unui nou dezvoltator care trebuie să lucreze la un proiect?
 - a) Să-i acorzi rolul de Owner la nivel de abonament.
 - b) Să-l adaugi într-un grup de dezvoltatori care are deja rolul de Contributor la grupul de resurse al proiectului.
 - c) Să-i atribui rolul de Contributor direct pe fiecare mașină virtuală.

(Răspunsuri la finalul manualului)

Ai devenit un maestru al cheilor! Știi cum să distribui accesul în mod sigur și eficient, asigurându-te că fiecare persoană are exact cheile de care are nevoie, și nimic mai mult. Acum ești gata să înveți cum să impui reguli la scară largă în întregul tău regat Azure.

 Achievement Deblocat: Key Master 

+300 XP

CAPITOLUL 17: Azure Policy - Legiuitorul Tărâmului Tău Azure

Tema Gamification: “Legiuitorul Suprem”

Nivel: Intermediate-Advanced (

Ai stabilit cine are acces și ce poate face. Dar cum te asiguri că toți constructorii din regatul tău respectă standardele? Cum previi construirea de castele (mașini virtuale) prea scumpe sau în regiuni interzise? Aici intervine **Azure Policy**, legiuitorul care impune reguli și asigură conformitatea la scară largă. Stăpânirea politicilor te va transforma într-un arhitect al guvernantei și îți va aduce achievement-ul **Supreme Lawmaker!**

17.1 Ce este Azure Policy?

Azure Policy este un serviciu în Azure care îți permite să creezi, să atribui și să gestionezi politici. Aceste politici impun reguli asupra resurselor tale, asigurându-se că acestea rămân conforme cu standardele tale corporative și cu acordurile de nivel de serviciu (SLA).

Analogie: Dacă RBAC se ocupă de “cine” poate face “ce”, Azure Policy se ocupă de “ce” poate fi creat și “cum”. Gândește-te la Azure Policy ca la codul de construcții al orașului tău Azure. Acesta nu se preocupă de cine este constructorul (RBAC se ocupă de asta), ci de faptul că orice clădire nouă trebuie să respecte anumite reguli: să nu depășească o anumită înălțime (cost), să fie construită doar în zonele aprobate (regiuni permise) și să aibă instalații de siguranță (tag-uri obligatorii).

De ce să folosești Azure Policy?

- **Guvernanță și Conformitate:** Asigură respectarea standardelor interne și a reglementărilor externe (ex: GDPR, ISO 27001).
- **Controlul Costurilor:** Previne crearea de resurse scumpe (ex: permite doar anumite SKU-uri de mașini virtuale).
- **Securitate:** Impune practici de securitate (ex: obligă criptarea conturilor de stocare).
- **Consistență:** Asigură că toate resursele sunt implementate într-un mod standardizat (ex: obligă adăugarea anumitor tag-uri pentru fiecare resursă).

17.2 Componentele Azure Policy

1. Policy Definition (Definiția Politicii):

- Este **regula** în sine, exprimată în format JSON.
- Conține o logică condițională (`if` și `then`).
- **Exemplu if :** `if` tipul resursei este `Microsoft.Compute/virtualMachines`
Și `if` locația resursei NU este în lista `['West Europe', 'North Europe']` ...
- **Exemplu then :** `...then` efectul este `Deny`.
- Azure oferă sute de **definiții predefinite (built-in)** pe care le poți folosi direct.

2. Policy Assignment (Atribuirea Politicii):

- Este procesul de **aplicare** a unei definiții de politică la un anumit **scope** (management group, abonament, grup de resurse).
- O singură definiție poate fi atribuită de mai multe ori la scope-uri diferite.

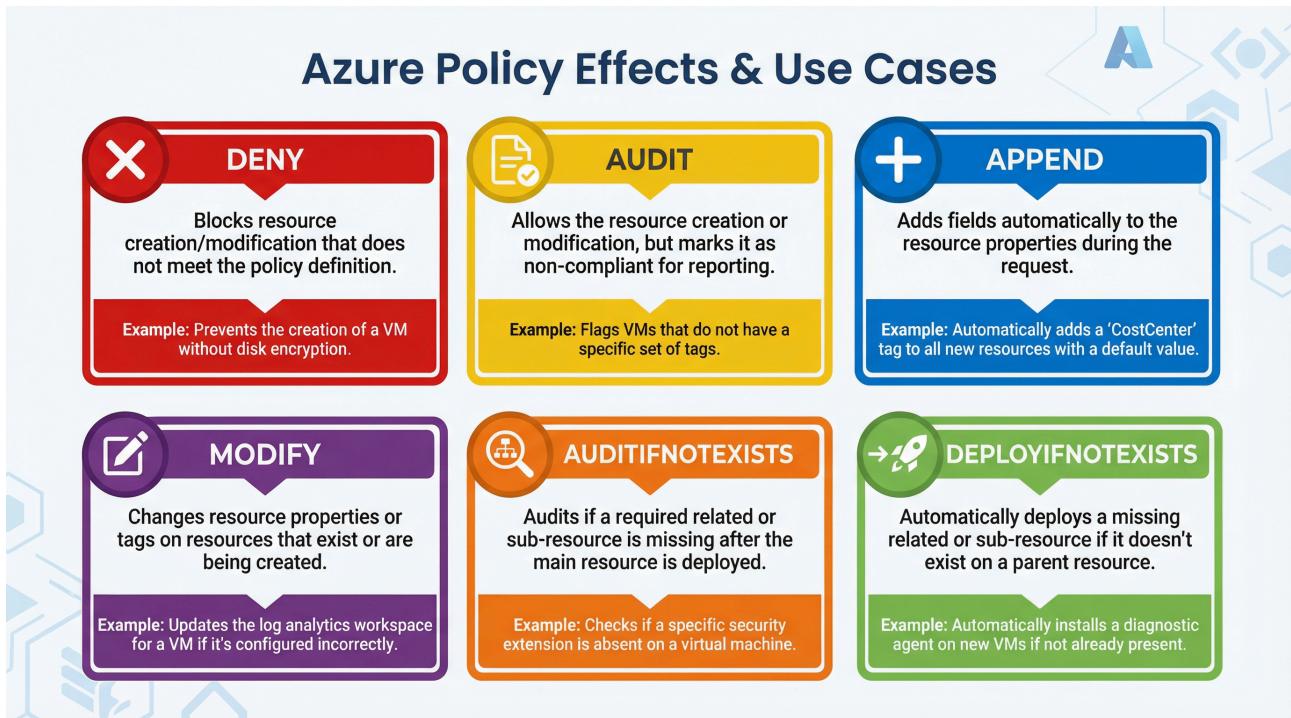
3. Initiative Definition (Inițiativa):

- Cunoscută și ca un **set de politici (policy set)**.
- Este o **colecție** de definiții de politici care sunt grupate pentru a atinge un obiectiv comun.
- **Exemplu:** O inițiativă numită “Conformitate ISO 27001” ar putea conține zeci de politici individuale legate de criptare, audit, acces la rețea etc.

- Atribui o inițiativă la un scope în același mod ca pe o politică individuală, simplificând managementul.

17.3 Efectele Politicilor (Policy Effects)

Efectul definește ce se întâmplă atunci când condiția unei politici este îndeplinită (când o resursă este neconformă).



- **Deny:** Blochează crearea sau modificarea resursei. Este cel mai restrictiv efect.
- **Audit:** Permite crearea/modificarea resursei, dar o marchează ca neconformă într-un raport de audit. Este util pentru a evalua impactul unei politici înainte de a o face restrictivă.
- **Append:** Adaugă câmpuri suplimentare la resursă în timpul creării (ex: adaugă automat un tag `CreatedBy` la toate resursele).
- **Modify:** Modifică proprietățile unei resurse (ex: adaugă sau modifică setările de diagnosticare pentru a trimite log-uri la un Log Analytics Workspace).
- **AuditIfNotExists:** Auditează dacă o resursă subordonată sau o proprietate lipsește (ex: verifică dacă o mașină virtuală are extensia de antivirus instalată).
- **DeployIfNotExists:** Implementează o resursă subordonată dacă aceasta lipsește (ex: implementează automat un agent de monitorizare pe toate mașinile virtuale noi).

- **Disabled:** Dezactivează politica fără a șterge atribuirea.

17.4 Evaluarea Conformității

Azure Policy evaluează resursele în diferite momente:

- La crearea sau actualizarea unei resurse.
- La atribuirea unei noi politici sau inițiative.
- Periodic (de obicei, la fiecare 24 de ore) pentru a verifica starea resurselor existente.

Portalul Azure oferă un dashboard de **Compliance** unde poți vedea starea de conformitate a tuturor resurselor tale, poți filtra după politici specifice și poți vedea exact ce resurse sunt neconforme și de ce.

Best Practice: Când implementezi o politică nouă și potențial restrictivă, începe întotdeauna cu efectul `Audit`. Las-o să ruleze pentru o perioadă, analizează raportul de conformitate pentru a vedea ce resurse ar fi afectate și comunică cu echipele responsabile. Doar după ce înțelegi pe deplin impactul, schimbă efectul în `Deny` sau `DeployIfNotExists`.

★ QUIZ TIME! ★

1. Care este principalul scop al Azure Policy?
 - Să acorde permisiuni utilizatorilor.
 - Să impună reguli de guvernanță și conformitate asupra resurselor.
 - Să monitorizeze performanța aplicațiilor.
2. Ce componentă Azure Policy reprezintă o colecție de politici grupate împreună?
 - Policy Definition
 - Policy Assignment
 - Initiative Definition
3. Ce efect de politică ai folosi pentru a bloca crearea de mașini virtuale în afara Europei?
 - Audit
 - Deny
 - Append

4. Care este cea mai bună practică atunci când implementezi o politică nouă și restrictivă?
 - a) Să o aplici imediat cu efectul `Deny` la nivel de abonament.
 - b) Să o aplici mai întâi cu efectul `Audit` pentru a evalua impactul.
 - c) Să o creezi, dar să o lași dezactivată.
5. Ce face efectul `DeployIfNotExists`?
 - a) Șterge resursele neconforme.
 - b) Trimit o alertă prin email.
 - c) Implementează o resursă necesară dacă aceasta lipsește.

(Răspunsuri la finalul manualului)

Ești acum un legiuitor! Știi cum să scrii și să implementezi legile care guvernează întregul tău ecosistem Azure, asigurând ordinea, securitatea și controlul costurilor. Următorul pas este să înveți cum să supraveghezi regatul și să reacționezi la evenimente.

 Achievement Deblocat: Supreme Lawmaker 

+350 XP

CAPITOLUL 18: Azure Monitor - Ochiul Atotvăzător al Regatului Tău

Tema Gamification: “Observatorul Cosmic”

Nivel: Intermediate (

Ai construit infrastructura, ai securizat-o și ai impus legi. Dar cum știi ce se întâmplă în regatul tău? Cum află dacă un server este suprasolicită sau dacă o eroare a apărut în miez de noapte? Aici intervine **Azure Monitor**, ochiul atotvăzător care colectează, analizează și acționează pe baza datelor de telemetrie din întregul tău mediu Azure. Înțelegerea acestui serviciu îți va oferi vizibilitate completă și îți va aduce achievement-ul **Cosmic Observer**!

18.1 Ce este Azure Monitor?

Azure Monitor este serviciul centralizat de monitorizare din Azure. Acesta colectează, analizează și acționează pe baza datelor de la resursele tale Azure, de la rețea on-premises și chiar din alte cloud-uri. Este o platformă complexă care oferă o imagine completă asupra performanței, sănătății și disponibilității aplicațiilor și infrastructurii tale.

Analogie: Gândește-te la Azure Monitor ca la camera de control a unei misiuni spațiale. Pe zeci de ecrane, vezi în timp real date despre viteză, consum de combustibil, temperatură, traекторie și starea de sănătate a astronauților. Această cameră de control (Azure Monitor) colectează date de la mii de senzori (resurse Azure) și le prezintă într-un mod care îți permite să vezi imaginea de ansamblu și să identifici problemele înainte ca acestea să devină catastrofale.

18.2 Cele Două Tipuri Fundamentale de Date: Metrics și Logs

Azure Monitor se bazează pe două tipuri principale de date:

1. Metrics (Date Metrice):

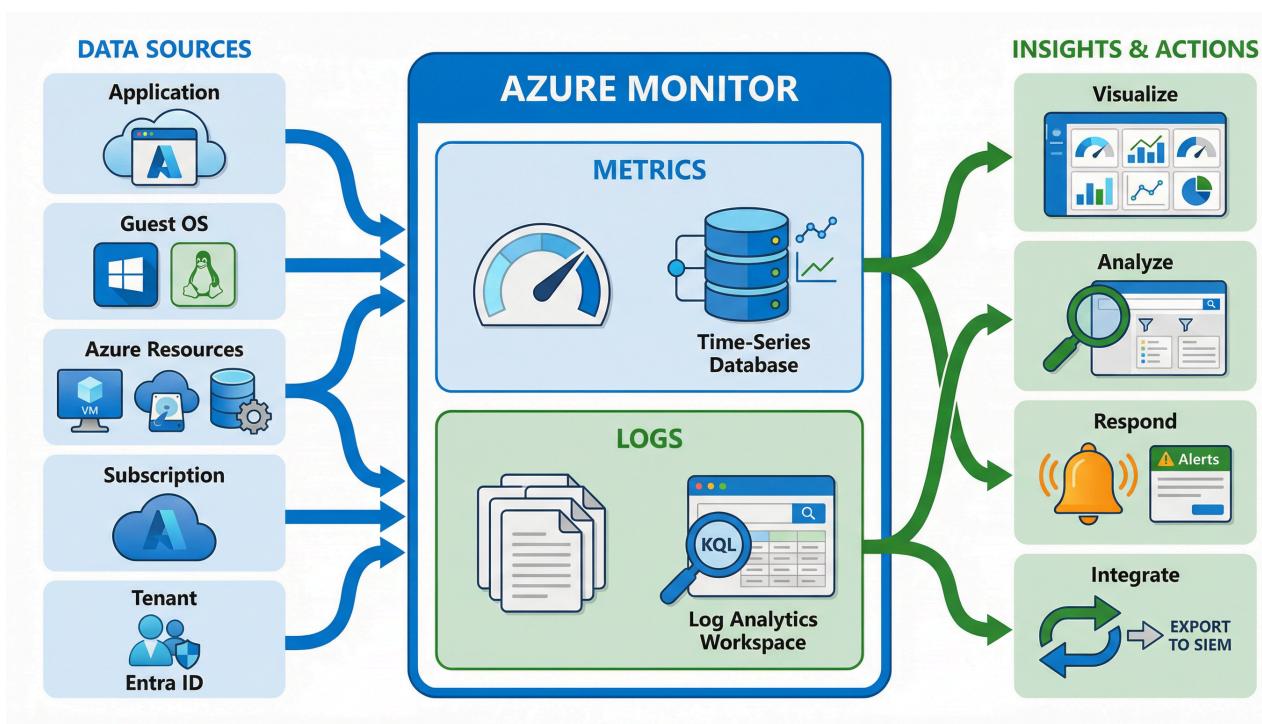
- Sunt valori **numerice**, dependente de timp, care descriu un anumit aspect al unui sistem la un moment dat.
- Sunt **ușoare** și colectate la intervale regulate (de obicei, la fiecare minut).
- Sunt ideale pentru alerte aproape în timp real.
- **Exemple:** Procentul de utilizare a procesorului (CPU), numărul de cereri pe secundă la o aplicație web, latența unui disc.
- **Analogie:** Metrics sunt ca și cum te-ai uitat la vitezometrul mașinii. Îți oferă o valoare numerică instantanee despre un anumit aspect.

2. Logs (Jurnale):

- Sunt înregistrări de evenimente care au avut loc. Conțin diferite tipuri de date organizate în înregistrări, fiecare cu proprietăți diferite.
- Sunt mai **bogate în context** decât datele metrice.
- Sunt colectate atunci când are loc un eveniment.

- Sunt ideale pentru analiză complexă, diagnosticare și investigarea cauzei rădăcină (root cause analysis).
- **Exemple:** Un log de la un server web care arată o eroare 500, un eveniment de securitate care indică o tentativă de autentificare eşuată, un log de la un firewall care arată traficul blocat.
- **Analogie:** Logs sunt ca și cum ai citi jurnalul de bord al mașinii după o călătorie. Îți oferă detalii despre fiecare eveniment: “La ora 10:05, motorul s-a supraîncălzit”, “La ora 10:10, s-a activat sistemul ABS”.

Caracteristică	Metrics	Logs
Format	Valori numerice	Înregistrări structurate/text
Scop	Alerte rapide, tendințe	Analiză profundă, diagnosticare
Colecțare	La intervale regulate	La apariția unui eveniment
Analiză	Grafice în timp real	Interrogări complexe (KQL)



18.3 De unde vin datele? Sursele de Date

Azure Monitor poate colecta date din mai multe surse:

- **Application:** Date despre performanță și funcționalitatea codului tău, colectate prin **Application Insights**.
- **Operating System (Guest OS):** Date de la sistemul de operare al mașinilor virtuale, colectate prin **Azure Monitor Agent**.
- **Azure Resources:** Date despre operațiunile unei resurse Azure (ex: un cont de stocare, o bază de date). Acestea sunt **Platform Logs**.
- **Azure Subscription:** Date despre managementul abonamentului, colectate din **Activity Log**.
- **Azure Tenant:** Date de la nivelul directorului, cum ar fi logurile de audit din Entra ID.

18.4 Activity Log și Diagnostic Settings

Activity Log:

- Este un jurnal la nivel de abonament care înregistrează toate evenimentele de management: **cine, ce și când** a făcut o acțiune la nivel de resurse Azure.
- Înregistrează fiecare operațiune de scriere (`PUT` , `POST` , `DELETE`) efectuată asupra resurselor tale.
- **Exemple:** Crearea unei mașini virtuale, ștergerea unui grup de resurse, actualizarea unei reguli de rețea.
- Este esențial pentru audit și investigarea modificărilor de infrastructură.

Diagnostic Settings:

- Acestea definesc **cum și unde** sunt trimise **Platform Logs** și **Metrics** de la o resursă specifică.
- Pentru fiecare resursă, trebuie să creezi o setare de diagnosticare pentru a exporta logurile sale interne.
- **Destinații Posibile:**
 - **Log Analytics Workspace:** Destinația principală pentru stocarea și analiza log-urilor folosind limbajul de interogare Kusto (KQL).
 - **Azure Storage Account:** Pentru arhivare pe termen lung, la cost redus.
 - **Azure Event Hubs:** Pentru a trimite datele către servicii externe (ex: un sistem SIEM precum Splunk sau QRadar) în timp real.

Best Practice: Configurează Diagnostic Settings pentru toate resursele critice pentru a trimite logurile către un Log Analytics Workspace centralizat. Acest lucru îți va oferi un singur loc unde poți interoga și corela date de la toate serviciile tale.

★ QUIZ TIME! ★

1. Care este diferența principală între Metrics și Logs?
 - a) Metrics sunt text, iar Logs sunt numere.
 - b) Metrics sunt valori numerice pentru alerte rapide, iar Logs sunt înregistrări detaliate pentru analiză.
 - c) Metrics sunt gratuite, iar Logs sunt scumpe.
2. Ce tip de dată ai folosi pentru a investiga cauza unei erori într-o aplicație?
 - a) Metrics
 - b) Logs
 - c) Activity Log
3. Ce înregistrează Activity Log-ul?
 - a) Performanța procesorului unei mașini virtuale.
 - b) Evenimentele de management la nivel de abonament (cine, ce, când).
 - c) Erorile din codul aplicației tale.
4. Ce trebuie să configurezi pentru a trimite logurile interne ale unei resurse (Platform Logs) către un spațiu de analiză?
 - a) O regulă de alertă.
 - b) O politică Azure.
 - c) O setare de diagnosticare (Diagnostic Setting).
5. Care este limbajul de interogare folosit pentru a analiza logurile într-un Log Analytics Workspace?
 - a) SQL
 - b) Python
 - c) KQL (Kusto Query Language)

(Răspunsuri la finalul manualului)

Ai devenit un observator vigilant. Știi cum să colectezi și să interpretezi semnalele din vastul tău univers Azure. Acum ești pregătit să înveți cum să acționezi automat pe baza

acestor semnale și cum să ții sub control costurile întregii operațiuni.

 Achievement Deblocat: Cosmic Observer 

+300 XP

CAPITOLUL 19: Alerte, Managementul Costurilor și Guvernanță

Tema Gamification: “Lordul Comandant al Regatului”

Nivel: Intermediate-Advanced (★★★★)

Ai identitate, ai chei, ai legi și ai ochi peste tot. Acum, în capitolul final al acestei serii, vei învăța cum să acționezi ca un adevărat Lord Comandant. Vei învăța cum să configurezi **alerte** pentru a fi notificat instantaneu despre probleme, cum să folosești **Azure Cost Management** pentru a ține trezoreria sub control și cum să combini toate aceste unelte pentru o guvernanță completă. Finalizarea acestui capitol îți va aduce cel mai înalt rang: **Kingdom Commander**.

19.1 Alertele în Azure Monitor

Colectarea datelor este inutilă dacă nu acționezi pe baza lor. **Alertele** din Azure Monitor te notifică proactiv atunci când datele tale de monitorizare indică o problemă, permitându-ți să o rezolvi înainte ca utilizatorii să o observe.

O regulă de alertă (**alert rule**) are trei componente principale:

1. **Target Resource (Tinta):** Resursa care este monitorizată (ex: o mașină virtuală, un cont de stocare).
2. **Condition (Condiția):** Logica ce este evaluată. Aceasta poate fi bazată pe:
 - **Metrics:** Ex: “Dacă procentul de utilizare a CPU este *mai mare de 90%* pentru o perioadă de *5 minute...*”
 - **Logs:** Ex: “Dacă numărul de rezultate al interogării KQL (Event | where EventLevelName == "Error") este *mai mare de 0* în ultimele *15 minute...*”
 - **Activity Log:** Ex: “Dacă evenimentul `Delete Virtual Machine` este detectat...”

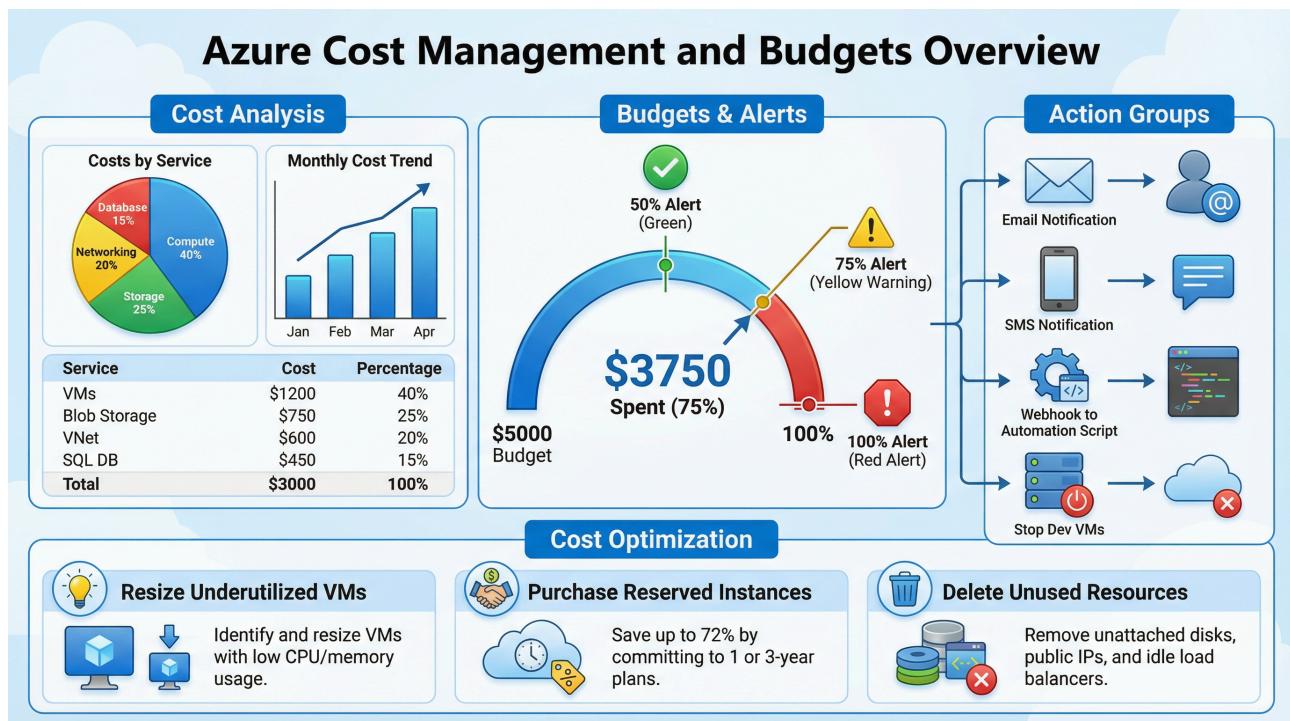
3. Action Group (Grupul de Acțiuni): Ce se întâmplă atunci când alerta se declanșează. Un grup de acțiuni poate conține una sau mai multe acțiuni, cum ar fi:

- **Notificări:** Trimiterea unui Email, SMS, notificare Push în aplicația Azure sau efectuarea unui apel vocal.
- **Acțiuni Automate:** Declanșarea unui Webhook, a unei funcții Azure (Azure Function), a unui Logic App, a unui runbook de Automation sau crearea unui ticket într-un sistem ITSM (ex: ServiceNow).

Analogie: O regulă de alertă este ca un senzor de fum. Tinta este camera. Condiția este “dacă se detectează fum”. Grupul de acțiuni este “pornește alarma sonoră (notificare) și activează sistemul de sprinklere (acțiune automată)”.

19.2 Azure Cost Management & Billing

Un regat, oricât de puternic, poate cădea dacă trezoreria se golește. **Azure Cost Management + Billing** este suita de unelte care te ajută să înțelegi, să monitorizezi și să optimizezi costurile cloud.



Componente Cheie:

- **Cost Analysis (Analiza Costurilor):**

- Un instrument interactiv pentru a explora și analiza costurile tale Azure.

- Poți vizualiza costurile după serviciu, locație, grup de resurse sau tag.
- Te ajută să înțelegi unde se duc banii și să identifici tendințe de cheltuieli.

- **Budgets (Bugete):**

- Îți permit să stabilești praguri de cheltuieli pentru un anumit scope (abonament, grup de resurse).
- Un buget **nu oprește** cheltuielile atunci când este atins. Este un instrument de monitorizare, nu de impunere.

- **Cost Alerts (Alerte de Cost):**

- Bugetele sunt folosite pentru a genera alerte. Poți configura alerte pentru a fi notificat când cheltuielile ating un anumit procent din buget (ex: 50%, 75%, 100%).
- Poți, de asemenea, să declanșezi grupuri de acțiuni automate, cum ar fi rularea unui script pentru a opri mașinile virtuale de dezvoltare în afara orelor de program.

- **Recommendations (Recomandări):**

- **Azure Advisor** este un consultant cloud personalizat care analizează configurația resurselor tale și oferă recomandări pentru a îmbunătăți disponibilitatea, securitatea, performanța și **costurile**.
- Recomandările de cost pot include: redimensionarea mașinilor virtuale subutilizate, achiziționarea de instanțe rezervate (Reserved Instances) pentru sarcini de lucru constant sau ștergerea resurselor neutilizate.

Best Practice: Implementează o strategie solidă de **tag-uri**. Tag-urile sunt perechi cheie-valoare pe care le atașezi resurselor (ex: `CostCenter:Marketing`, `Project:NewWebApp`, `Environment:Production`). Folosirea consistentă a tag-urilor îți permite să aloci costurile cu precizie în instrumentul de analiză a costurilor și să înțelegi care departament sau proiect generează cele mai mari cheltuieli.

19.3 Guvernanța Completă: Combinarea Uneltelor

Adevărată putere a guvernanței în Azure vine din combinarea tuturor conceptelor pe care le-ai învățat în această serie:

- 1. Identitate (Entra ID):** Stabilești cine sunt utilizatorii și îi organizezi în grupuri.
- 2. Acces (RBAC):** Atribui roluri acelor grupuri la scope-uri specifice, acordându-le permisiunile necesare conform principiului privilegiului minim.
- 3. Reguli (Azure Policy):** Implementezi politici pentru a te asigura că resursele create respectă standardele de securitate, conformitate și cost. De exemplu, o politică poate impune ca toate resursele să aibă un tag `CostCenter`.
- 4. Monitorizare (Azure Monitor):** Colecțezi log-uri și metriți de la toate resursele. Configurezi alerte pentru a fi notificat despre probleme de performanță, securitate sau erori.
- 5. Cost (Cost Management):** Creezi bugete pentru grupurile de resurse sau abonamente, bazându-te pe tag-ul `costCenter`. Configurezi alerte de buget pentru a notifica managerii de proiect când se apropiă de limita de cheltuieli.

Această abordare integrată îți oferă un control complet și proactiv asupra mediului tău Azure, de la identitate și acces, la conformitate, monitorizare și optimizare financiară.

★ QUIZ TIME! ★

1. Ce componentă a unei reguli de alertă definește ce se întâmplă când alerta se declanșează (ex: trimiterea unui email)?
 - a) Target Resource
 - b) Condition
 - c) Action Group
2. Ce se întâmplă atunci când un buget este atins în Azure Cost Management?
 - a) Toate resursele din scope-ul bugetului sunt opriate automat.
 - b) Se generează o alertă (dacă a fost configurată), dar cheltuielile continuă.
 - c) Se adaugă automat mai mulți bani în cont.
3. Ce instrument îți oferă recomandări personalizate pentru a reduce costurile, cum ar fi redimensionarea VM-urilor?
 - a) Azure Monitor
 - b) Azure Advisor
 - c) Azure Policy
4. Care este cea mai eficientă metodă pentru a aloca și a urmări costurile pe departamente sau proiecte?

- a) Crearea de abonamente separate pentru fiecare departament.
 - b) Utilizarea consistentă a tag-urilor (ex: CostCenter).
 - c) Trimiterea de email-uri lunare către fiecare departament.
5. Care este ordinea logică a implementării guvernantei?
- a) Costuri -> Reguli -> Identitate -> Acces -> Monitorizare
 - b) Identitate -> Acces -> Reguli -> Monitorizare -> Costuri
 - c) Monitorizare -> Costuri -> Acces -> Identitate -> Reguli

(Răspunsuri la finalul manualului)

Felicitări, Lord Comandant! Ai ajuns la finalul călătoriei tale de inițiere. Ai stăpânit arta identității, a accesului, a legilor, a supravegherii și a managementului trezoreriei. Ești acum echipat cu cunoștințele necesare pentru a guverna un mediu Azure în mod eficient, sigur și responsabil.

 Achievement Deblocat: Kingdom Commander 
+400 XP

SECȚIUNEA FINALĂ (Partea a V-a)

Răspunsuri Quiz-uri

Capitolul 15:

1. b) Managementul identității și accesului (IAM).
2. b) Guest User
3. b) Acordarea permisiunilor grupurilor și adăugarea utilizatorilor în acele grupuri.
4. c) Dynamic User Group
5. b) Global Administrator

Capitolul 16:

1. b) Security Principal, Role Definition, Scope
2. c) Contributor
3. b) Va putea vedea doar resursele din acel grup de resurse.

4. b) Permisunile efective sunt suma tuturor rolurilor atribuite.
5. b) Să-l adaugi într-un grup de dezvoltatori care are deja rolul de Contributor la grupul de resurse al proiectului.

Capitolul 17:

1. b) Să impună reguli de guvernanță și conformitate asupra resurselor.
2. c) Initiative Definition
3. b) Deny
4. b) Să o aplici mai întâi cu efectul Audit pentru a evalua impactul.
5. c) Implementează o resursă necesară dacă aceasta lipsește.

Capitolul 18:

1. b) Metrics sunt valori numerice pentru alerte rapide, iar Logs sunt înregistrări detaliate pentru analiză.
2. b) Logs
3. b) Evenimentele de management la nivel de abonament (cine, ce, când).
4. c) O setare de diagnosticare (Diagnostic Setting).
5. c) KQL (Kusto Query Language)

Capitolul 19:

1. c) Action Group
 2. b) Se generează o alertă (dacă a fost configurată), dar cheltuielile continuă.
 3. b) Azure Advisor
 4. b) Utilizarea consistentă a tag-urilor (ex: CostCenter).
 5. b) Identitate -> Acces -> Reguli -> Monitorizare -> Costuri
-

Glosar de Termeni (Partea a V-a)

Termen	Definiție
IAM	Identity and Access Management. Procesele și tehnologiile pentru gestionarea identităților digitale și a accesului acestora la resurse.
Entra ID	Serviciul de IAM bazat pe cloud de la Microsoft, cunoscut anterior ca Azure Active Directory.
Tenant	O instanță dedicată de Entra ID, reprezentând o organizație.
RBAC	Role-Based Access Control. Un sistem de autorizare care acordă acces la resursele Azure pe baza rolurilor.
Scope	Nivelul ierarhic (Management Group, Subscription, Resource Group, Resource) la care se aplică o atribuire de rol sau o politică.
Azure Policy	Un serviciu pentru crearea, atribuirea și gestionarea politicilor care impun reguli de guvernanță asupra resurselor.
Initiative	O colecție de definiții de politici grupate pentru a atinge un obiectiv comun.
Azure Monitor	Serviciul centralizat de monitorizare din Azure pentru colectarea, analiza și acțiunea pe baza datelor de telemetrie.
Metrics	Valori numerice, dependente de timp, care descriu un aspect al unui sistem.
Logs	Înregistrări de evenimente, bogate în context, stocate într-un Log Analytics Workspace și interogate cu KQL.
Activity Log	Un jurnal la nivel de abonament care înregistrează toate evenimentele de management.
Action Group	O colecție de notificări și acțiuni care sunt declanșate de o alertă.
Cost Management	Suita de unelte Azure pentru monitorizarea, analiza și optimizarea costurilor cloud.
Tag	O pereche cheie-valoare (metadată) care poate fi atașată resurselor Azure pentru a le organiza.

Resurse pentru Aprofundare (Identity, Security, Management)

Documentație Oficială Microsoft:

- [Microsoft Entra Documentation](#)
- [Azure RBAC Documentation](#)
- [Azure Policy Documentation](#)
- [Azure Monitor Documentation](#)
- [Microsoft Cost Management Documentation](#)

Certificări Recomandate:

- **AZ-900: Azure Fundamentals** - Acoperă toate aceste concepte la nivel de bază.
- **AZ-104: Azure Administrator** - Include managementul detaliat al tuturor acestor servicii.
- **AZ-500: Azure Security Engineer** - Certificare specializată pe securitate, cu focus pe Entra ID, RBAC și Policy.
- **SC-300: Identity and Access Administrator** - Certificare specializată pe Microsoft Entra ID.

Tabelul Final de Achievement-uri (Partea a V-a)

Achievement	Descriere	XP
🏆 Identity Guardian	Completează Capitolul 15 și înțelege Entra ID	250
🏆 Key Master	Completează Capitolul 16 și stăpânește RBAC	300
🏆 Supreme Lawmaker	Completează Capitolul 17 și înțelege Azure Policy	350
🏆 Cosmic Observer	Completează Capitolul 18 și înțelege Azure Monitor	300
🏆 Kingdom Commander	Completează Capitolul 19 și stăpânește alertele și costurile	400

Total XP Posibil (Partea a V-a): 1,600 XP

Mesaj Final (Seria Completă)

Felicitări, Maestru Azure!

Ai parcurs întreaga serie de manuale, de la fundamentele cloud-ului, la serviciile de calcul, stocare, rețelistică și, în final, la pilonii de identitate, securitate și guvernanță. Ai acumulat un total impresionant de **6,450 XP** și ai deblocat **28 de achievement-uri**, demonstrând o înțelegere cuprinzătoare a ecosistemului Azure.

Călătoria ta nu se termină aici. Cloud-ul este un domeniu în continuă evoluție, cu noi servicii și capabilități apărând constant. Folosește aceste manuale ca pe o fundație solidă, continuă să explorezi, să experimentezi în laboratoare și să te pregătești pentru certificări.

Ai demonstrat curiozitate, perseverență și dorință de a învăța. Acestea sunt cele mai importante calități ale unui profesionist cloud de succes. Mult succes în continuare în călătoria ta în Azure!

Drumul tău în Azure abia a început! 🚀