

# Manual Azure Storage - Ediția Gamificată

## (Partea a III-a)



### Despre Acest Manual (Partea a III-a)

Bun venit la a treia parte a aventurii tale în Azure! Ai învățat despre fundamente și ai stăpânit serviciile de calcul. Acum, este timpul să explorezi fundația pe care se construiește totul: **stocarea (storage)**. Fiecare aplicație, fiecare mașină virtuală, fiecare bucată de informație are nevoie de un loc unde să existe. În acest manual, vei deveni un gardian al datelor, învățând cum să le stochezi, să le gestionezi și să le protejezi în Azure.

#### Ce vei învăța:

- Azure Storage Accounts - Concepte și tipuri
- Cele patru servicii de stocare: Blob, File, Queue, Table
- Securizarea accesului: Access Keys, SAS Tokens, RBAC
- Redundanță și protecție: LRS, ZRS, GRS, GZRS
- Laborator practic: Upload în Blob Storage

#### Sistem de Gamification:

- 🎮 XP Points** - Câștigă experiență pentru fiecare capitol și laborator
- 🏆 Achievement-uri Noi** - Deblochează medalii pentru competențe de stocare
- ⭐ Nivele de Dificultate** - De la Beginner la Advanced
- 🎯 Laborator Hands-on** - Construiește infrastructură reală în Azure

Total XP Posibil (Partea a III-a): 850 puncte

# CAPITOLUL 8: Stocarea în Azure - Fundația Datelor Tale

---

**Tema Gamification:** “Gardianul Datelor”

**Nivel:** Intermediate (★★)

Bun venit la a treia parte a aventurii tale în Azure! Ai învățat despre fundamente și ai stăpânit serviciile de calcul. Acum, este timpul să explorezi fundația pe care se construiește totul: **stocarea (storage)**. Fiecare aplicație, fiecare mașină virtuală, fiecare bucată de informație are nevoie de un loc unde să existe. În acest capitol, vei deveni un gardian al datelor, învățând cum să le stochezi, să le gestionezi și să le protejezi în Azure. La final, vei debloca achievement-ul **Data Guardian!**

## 8.1 Azure Storage Accounts: Seiful Tău Digital

Totalul în lumea stocării Azure începe cu un **Storage Account**. Acesta este un container de nivel superior care îți oferă un spațiu de nume unic în Azure pentru a-ți stoca și accesa datele. Gândește-te la el ca la un seif digital masiv, care conține diferite tipuri de compartimente pentru diferite tipuri de date.

***Analogie:** Un Storage Account este ca un depozit uriaș. În interiorul acestui depozit, ai diferite zone: o zonă pentru paleți cu marfă vrac (Blob), o zonă cu rafturi pentru dosare (File), o zonă pentru corespondență și mesagerie (Queue) și o zonă de arhivare cu index (Table). Tu deții întregul depozit și decizi ce și cum stochezi în fiecare zonă.*

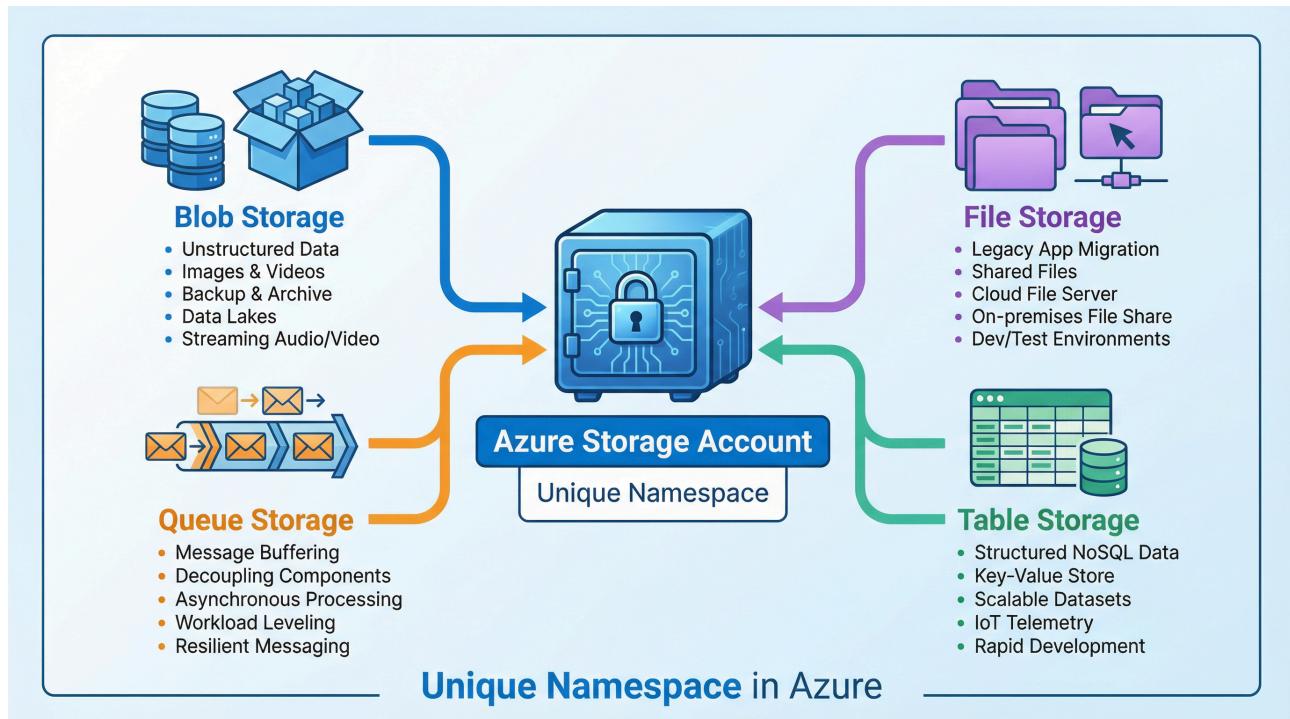
Un Storage Account este resursa fundamentală care găzduiește unul sau mai multe dintre cele patru servicii de bază de stocare Azure.

### Caracteristici Cheie:

- **Unique Namespace:** Fiecare Storage Account are un nume unic global în Azure (ex: mystorageaccount.blob.core.windows.net ).
- **Scalabilitate:** Poate stoca de la câțiva megabytes la petabytes de date.
- **Durabilitate:** Datele sunt replicate automat pentru protecție.
- **Accesibilitate:** Datele sunt accesibile de oriunde prin HTTP/HTTPS.

## 8.2 Cele Patru Servicii Fantastice de Stocare

Un cont de stocare de tip **General Purpose v2 (GPv2)**, cel mai comun și recomandat tip, îți oferă acces la patru servicii distincte, fiecare cu un scop precis:



Serviciu	Tip de Date	Ideal pentru...	Analogie
<b>Blob Storage</b>	Obiecte (fișiere mari, nestructurate)	Imagini, video, backup-uri, fișiere de log, date pentru analiză Big Data.	Un container maritim unde poți arunca orice, de la o mașină la cutii cu documente.
<b>File Storage</b>	Partajări de fișiere (File Shares)	Partajări de fișiere în rețea (SMB/NFS), migrarea aplicațiilor legacy care folosesc file shares.	Un dulap cu dosare, organizat și accesibil de mai mulți utilizatori simultan.
<b>Queue Storage</b>	Mesaje	Comunicare asincronă între componentele unei aplicații, procesare de sarcini în background.	O bandă de transport la poștă, unde pachetele (mesajele) stau la coadă pentru a fi procesate.
<b>Table Storage</b>	Date structurate NoSQL	Stocarea de date structurate, dar flexibile (ex: date de la senzori IoT, profiluri de utilizator).	Un tabel uriaș, dar fără o schemă fixă, unde fiecare rând poate avea coloane diferite.

## Blob Storage: Inima Stocării de Obiecte

Blob (Binary Large Object) Storage este cel mai utilizat serviciu. Este optimizat pentru a stoca cantități masive de date nestructurate. Există trei tipuri de blob-uri:

- **Block Blobs:** Compuse din blocuri, ideale pentru fișiere mari precum video sau backup-uri. Pot stoca până la aproximativ 190 TB.
- **Append Blobs:** Optimizate pentru operațiuni de adăugare, perfecte pentru fișiere de log. Fiecare append blob poate avea până la 195 GB.
- **Page Blobs:** Optimizate pentru operațiuni de citire/scriere aleatorii, folosite pentru a stoca discurile virtuale (VHD) ale mașinilor virtuale. Pot stoca până la 8 TB.

## File Storage: Partajări în Cloud

Azure Files oferă partajări de fișiere complet gestionate în cloud, accesibile prin protocolul **SMB (Server Message Block)** sau **NFS (Network File System)**. Este perfect pentru scenarii de migrare “lift-and-shift” unde aplicațiile existente se bazează pe partajări de fișiere.

## Queue Storage: Mesageria Simplă

Queue Storage oferă mesagerie asincronă între componentele aplicației. Este ideal pentru decuplarea componentelor și pentru procesarea de sarcini în background. Fiecare mesaj poate avea până la 64 KB, iar o coadă poate conține milioane de mesaje.

## Table Storage: NoSQL pentru Toți

Table Storage este un magazin de date NoSQL pentru date structurate. Este ideal pentru stocarea de seturi mari de date structurate, dar flexibile, cum ar fi datele de la senzori IoT sau profilurile de utilizator. Este mai ieftin decât bazele de date SQL tradiționale și este extrem de scalabil.

---

## ★ QUIZ TIME! ★

1. Ce este un Azure Storage Account?
  - a) Un tip de mașină virtuală.
  - b) Un container de nivel superior care găzduiește serviciile de stocare Azure.
  - c) O bază de date SQL.

2. Ce serviciu de stocare ai folosi pentru a crea o partajare de fișiere accesibilă prin protocolul SMB?
  - a) Blob Storage
  - b) File Storage
  - c) Queue Storage
3. Pentru ce scenariu este ideal Queue Storage?
  - a) Stocarea de fișiere video.
  - b) Găzduirea unui site web static.
  - c) Decuplarea componentelor unei aplicații pentru procesare asincronă.
4. Ce tip de blob este optimizat pentru fișiere de log?
  - a) Block Blob
  - b) Page Blob
  - c) Append Blob
5. Care este cel mai comun și recomandat tip de Storage Account pentru majoritatea scenariilor?
  - a) BlobStorage
  - b) FileStorage
  - c) General Purpose v2 (GPv2)

(Răspunsuri la finalul manualului)

---

Ai înțeles elementele de bază. Acum ești gata să înveți cum să-ți protejezi datele și să le faci ultra-rezistente.

 Achievement Deblocat: Data Guardian 

+200 XP

---

## CAPITOLUL 9: Securitate și Redundanță în Stocare

---

**Tema Gamification:** “Arhitectul Invincibil”

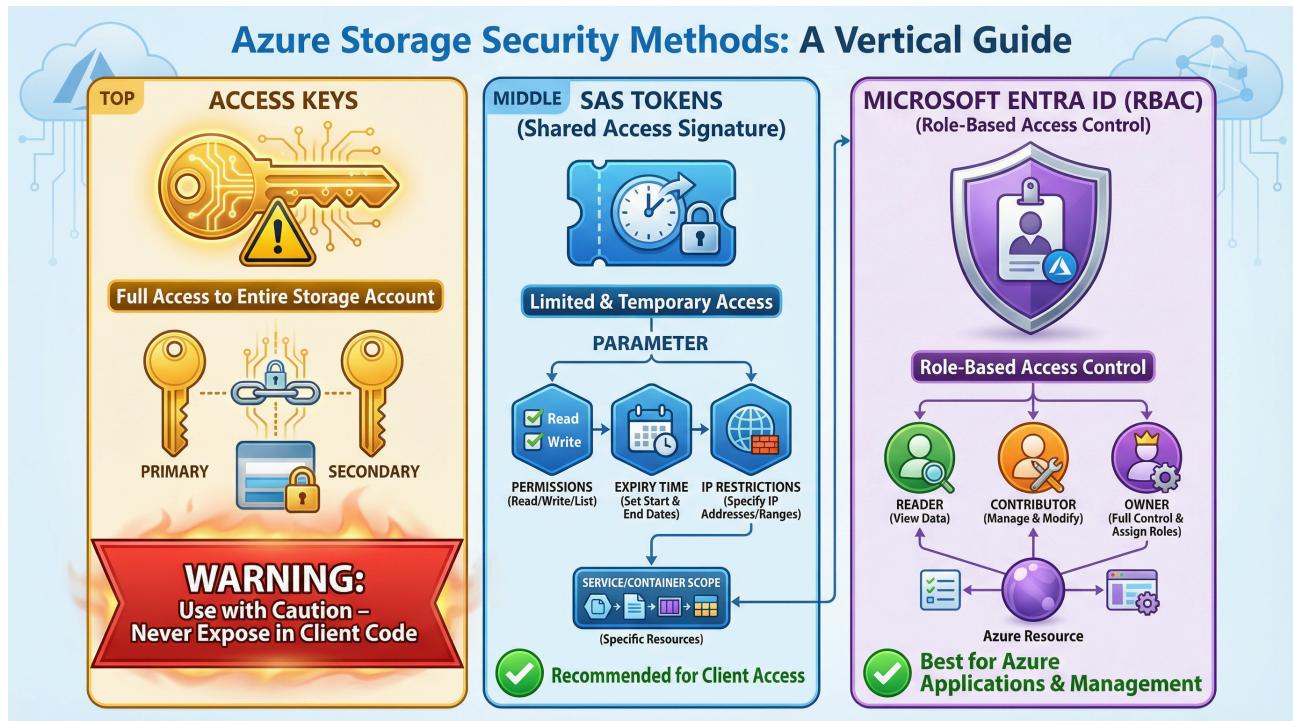
**Nivel:** Intermediate-Advanced (

Ca un gardian al datelor, datoria ta nu este doar să le stochezi, ci și să le protejezi. În acest capitol, vei învăța cele două arte esențiale ale protecției datelor: **securitatea** (cine are acces) și **redundanța** (cum supraviețuiesc datele în caz de dezastru).

Stăpânirea acestor concepte te va transforma într-un arhitect a cărui fortăreață de date este aproape impenetrabilă și îți va aduce achievement-ul **Fortress Architect**.

## 9.1 Securizarea Accesului la Date

Există mai multe strategii pentru a controla accesul la datele tale din Storage Account, de la cea mai puternică și periculoasă la cea mai granulară și sigură.



### 1. Storage Account Access Keys:

- **Ce sunt?** Două chei (primară și secundară) care oferă acces de administrator la **întregul** cont de stocare.
- **Analogie:** Sunt cheile de la intrarea principală a depozitului tău. Oricine le are, are control total.
- **Putere:** Acces complet la toate serviciile (Blob, File, Queue, Table) și toate operațiunile (citire, scriere, ștergere).
- **Best Practice:** Folosește-le doar pentru managementul inițial sau pentru scenarii limitate. **Nu le expune niciodată** în codul unei aplicații client (ex: JavaScript în browser)! Rotește-le regulat pentru securitate.

### 2. Shared Access Signatures (SAS):

- **Ce sunt?** Un URI care conține un token ce acordă acces limitat și temporar la resursele de stocare.

- **Analogie:** Este un card de acces temporar, programat să funcționeze doar pentru o anumită ușă (ex: un container de blob-uri), pentru o anumită perioadă de timp (ex: 15 minute) și doar pentru anumite acțiuni (ex: doar citire).
- **Putere:** Poți specifica:
  - **Permisiuni:** Citire, scriere, ștergere, listare.
  - **Timp:** Data și ora de început și de expirare.
  - **Resurse:** La nivel de serviciu, container sau blob individual.
  - **Restricții IP:** Doar anumite adrese IP pot folosi token-ul.
- **Best Practice:** Aceasta este metoda preferată pentru a acorda acces clienților sau serviciilor la resursele tale, fără a expune cheile principale. Folosește **User Delegation SAS** (bazat pe Entra ID) pentru securitate maximă.

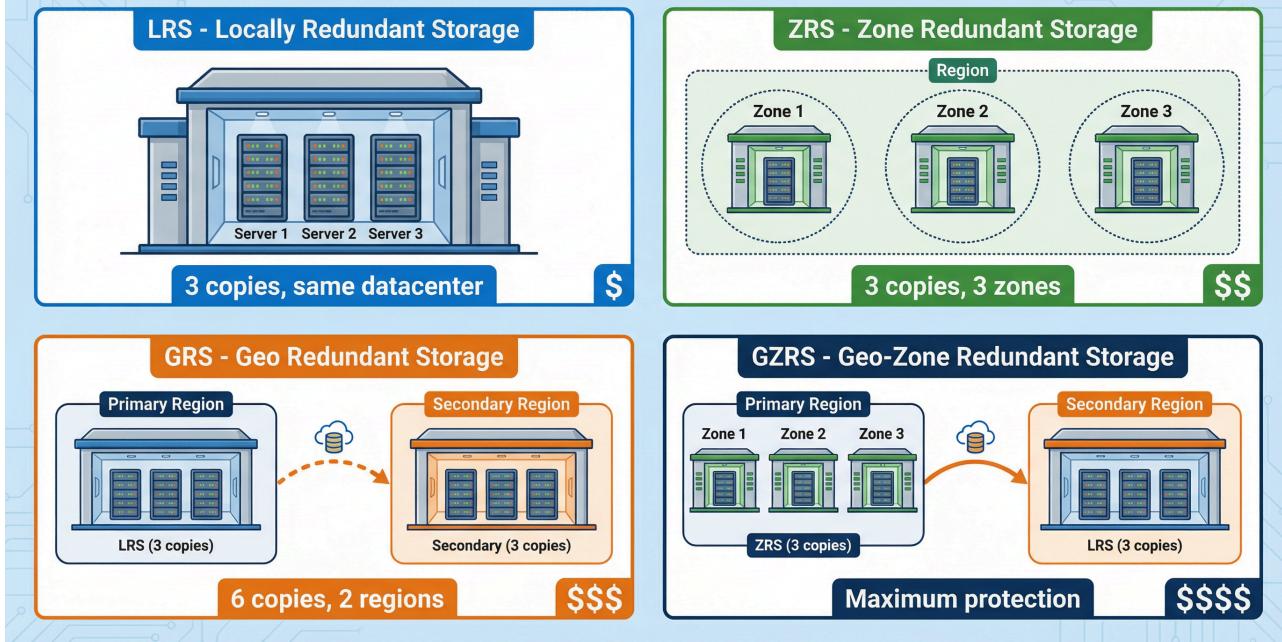
### **3. Microsoft Entra ID (fostul Azure Active Directory) și RBAC:**

- **Ce este?** Integrarea cu sistemul de identitate și acces al Azure. Poți acorda permisiuni utilizatorilor, grupurilor sau serviciilor folosind **Role-Based Access Control (RBAC)**.
- **Analogie:** Este un sistem de securitate centralizat cu paznici și carduri de identitate, unde fiecare angajat are un rol bine definit (ex: “cititor de blob-uri”, “contributor la cozi”).
- **Putere:** Roluri predefinite precum:
  - **Storage Blob Data Reader:** Citire blob-uri.
  - **Storage Blob Data Contributor:** Citire, scriere, ștergere blob-uri.
  - **Storage Account Contributor:** Management la nivel de cont.
- **Best Practice:** Folosește Entra ID pentru a gestiona accesul la nivel de management și pentru aplicațiile care rulează în Azure (folosind Managed Identities). Este cea mai sigură și mai ușor de gestionat metodă pentru scenarii enterprise.

## **9.2 Redundanța: Planul de Rezervă al Datelor Tale**

Redundanța se referă la stocarea mai multor copii ale datelor tale pentru a le proteja împotriva defecțiunilor hardware sau a dezastrelor. Azure oferă mai multe niveluri de redundanță, fiecare cu un grad diferit de protecție și cost.

## AZURE STORAGE REDUNDANCY OPTIONS: DATA AVAILABILITY & DURABILITY



### Redundanță în Regiunea Primară:

- **Locally-Redundant Storage (LRS):**

- **Ce face?** Creează 3 copii ale datelor tale în același centru de date, dar pe rack-uri hardware diferite.
- **Protejează împotriva:** Defecțiunilor unui disc, a unui server sau a unui rack.
- **Nu protejează împotriva:** Unui dezastru la nivel de centru de date (incendiu, inundație, cutremur).
- **Durabilitate:** 11 nines (99.99999999%) pe parcursul unui an.
- **Cost:** Cel mai scăzut.
- **Caz de utilizare:** Date de dezvoltare, testare sau date care pot fi ușor recreate.

- **Zone-Redundant Storage (ZRS):**

- **Ce face?** Creează 3 copii ale datelor tale, distribuite sincron în 3 Zone de Disponibilitate diferite în aceeași regiune.
- **Protejează împotriva:** Defecțiunilor la nivel de centru de date (zonă). Dacă o zonă întreagă devine indisponibilă, datele tale rămân accesibile din celelalte două zone.
- **Nu protejează împotriva:** Unui dezastru care afectează întreaga regiune.

- **Durabilitate:** 12 nines (99.999999999%).
- **Cost:** Mediu.
- **Caz de utilizare:** Date de producție care necesită disponibilitate ridicată.

### **Redundanța Geo-spațială (între Regiuni):**

- **Geo-Redundant Storage (GRS):**

- **Ce face?** Este LRS (3 copii în regiunea primară) **plus** o replicare asincronă a datelor într-o a doua regiune, la sute de kilometri distanță. În regiunea secundară, datele sunt de asemenea replicate local (LRS).
- **Protejează împotriva:** Unui dezastru regional. Dacă întreaga regiune primară devine indisponibilă, datele tale sunt în siguranță în regiunea secundară.
- **Acces:** În mod implicit, datele din regiunea secundară nu sunt accesibile pentru citire decât dacă se face un **failover** (comutare) la regiunea secundară. Pentru acces de citire permanent, vezi RA-GRS.
- **Durabilitate:** 16 nines (99.999999999999%).
- **Cost:** Ridicat.
- **Caz de utilizare:** Date critice de producție care necesită protecție împotriva dezastrelor regionale.

- **Read-Access Geo-Redundant Storage (RA-GRS):**

- **Ce face?** Este GRS **plus** acces de citire la datele din regiunea secundară, fără a fi nevoie de failover.
- **Avantaj:** Poți citi datele din regiunea secundară pentru a reduce latența pentru utilizatorii din acea zonă geografică sau pentru a avea o copie de siguranță accesibilă în orice moment.
- **Cost:** Similar cu GRS.
- **Caz de utilizare:** Aplicații cu utilizatori globali sau scenarii de disaster recovery unde vrei acces imediat la datele de backup.

- **Geo-Zone-Redundant Storage (GZRS):**

- **Ce face?** Este ZRS (3 copii în 3 zone în regiunea primară) **plus** o copie asincronă a datelor într-o a doua regiune (unde este replicată cu LRS).

- **Este cea mai rezistentă opțiune**, combinând protecția la nivel de zonă cu cea la nivel de regiune.
- **Durabilitate:** 16 nines.
- **Cost:** Foarte ridicat.
- **Caz de utilizare:** Date ultra-critice care necesită nivelul maxim de protecție.

- **Read-Access Geo-Zone-Redundant Storage (RA-GZRS):**

- **Ce face?** Este GZRS **plus** acces de citire la regiunea secundară.
- **Cea mai completă opțiune** pentru disponibilitate și durabilitate maximă.

Opțiune	Copii	Locație	Protecție Maximă	Durabilitate	Cost
LRS	3	Același centru de date	Defecțiune server/rack	11 nines	\$
ZRS	3	3 zone de disponibilitate	Defecțiune centru de date	12 nines	\$\$
GRS	6	2 regiuni diferite	Dezastru regional	16 nines	\$\$\$
RA-GRS	6	2 regiuni + read access	Dezastru regional + HA	16 nines	\$\$\$
GZRS	6	3 zone în reg. 1 + reg. 2	Dezastru regional + zonal	16 nines	
RA-GZRS	6	3 zone + reg. 2 + read	Protecție maximă	16 nines	

**Best Practice:** Alege nivelul de redundanță în funcție de criticitatea datelor tale. Pentru date de dezvoltare, LRS este suficient. Pentru date de producție critice, GRS sau GZRS sunt esențiale. Evaluează întotdeauna raportul cost-beneficiu.

### 9.3 Encryption: Protecția Invizibilă

Pe lângă controlul accesului și redundanță, Azure Storage oferă și **criptare automată**:

- **Data at Rest:** Toate datele stocate în Azure sunt criptate automat folosind **AES-256**, unul dintre cele mai puternice standarde de criptare. Nu trebuie să faci nimic pentru a activa acest lucru.

- **Data in Transit:** Datele sunt criptate în timpul transferului folosind **HTTPS/TLS**. Asigură-te că aplicațiile tale folosesc întotdeauna HTTPS pentru a accesa Storage Account-ul.
  - **Customer-Managed Keys:** Pentru un control și mai mare, poți folosi propriile chei de criptare, gestionate în **Azure Key Vault**.
- 

## ★ QUIZ TIME! ★

1. Care este cea mai sigură metodă de a acorda unui utilizator acces temporar pentru a încărca un fișier într-un container de blob-uri?
  - a) A-i da una dintre cheile de acces ale contului de stocare.
  - b) A crea un Shared Access Signature (SAS) cu permisiuni de scriere și o durată limitată.
  - c) A-l face proprietar al contului de stocare.
2. Ce opțiune de redundanță te protejează împotriva unui dezastru care afectează un întreg centru de date, dar nu și întreaga regiune?
  - a) LRS
  - b) ZRS
  - c) GRS
3. Care este diferența fundamentală între GRS și LRS?
  - a) GRS folosește 4 copii, LRS folosește 3.
  - b) GRS replică datele într-o a doua regiune geografică, LRS nu.
  - c) GRS este mai ieftin decât LRS.
4. Ce înseamnă RBAC în contextul securității Azure?
  - a) Redundant Access to Blobs and Containers
  - b) Role-Based Access Control
  - c) Rapid Backup and Copy
5. Care este cea mai rezistentă și durabilă opțiune de redundanță oferită de Azure Storage?
  - a) LRS
  - b) ZRS
  - c) GZRS

(Răspunsuri la finalul manualului)

---

Excelent! Acum ştii cum să-ţi construieşti fortăreaţa de date, folosind atât ziduri de securitate, cât şi planuri de evacuare în caz de dezastru.

 Achievement Deblocat: Fortress Architect 

+300 XP

---

## CAPITOLUL 10: Laborator Practic - Upload în Blob Storage

---

**Tema Gamification:** “Primul Artefact”

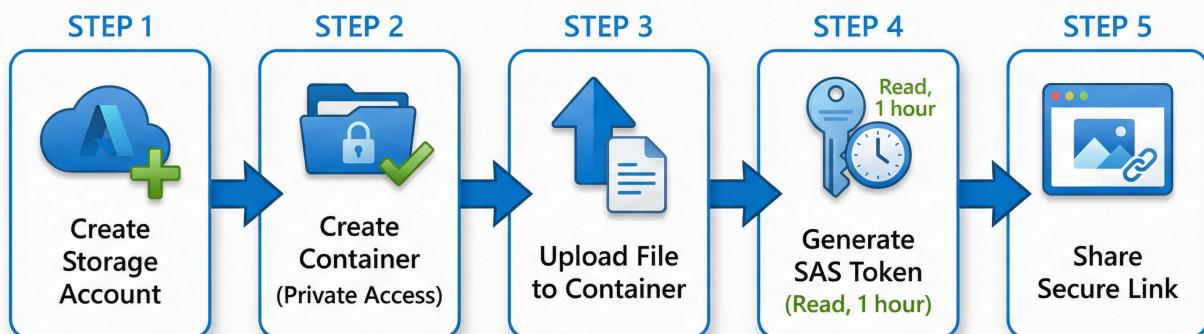
**Nivel:** Beginner-Intermediate (★)

Teoria este importantă, dar practica este cea care consolidează cunoştinţele. În acest laborator final, vei aplica tot ce ai învățat despre stocare și securitate pentru a îndeplini o sarcină fundamentală: încărcarea unui fișier în Azure Blob Storage. Acesta este primul tău “artefact” digital stocat în cloud și îți va aduce achievement-ul **Blob Uploader**.

### 10.1 Obiectivul Laboratorului

Vei crea un cont de stocare, vei configura un container de blob-uri, vei încărca un fișier și apoi vei genera un link securizat (SAS token) pentru a-l partaja.

---



**Lab Complete - Your First Artifact in the Cloud!**

## 10.2 Pașii Laboratorului

**Challenge:** “Urcă Artefactul” (350 XP)

Urmează cu atenție pașii de mai jos în Azure Portal.

### Pasul 1: Creează un Storage Account

1. În Azure Portal, căută “Storage accounts” și apasă “Create”.
2. **Resource Group:** Creează unul nou, numit `Storage-Lab-RG`.
3. **Storage account name:** Alege un nume unic global, cu litere mici și cifre (ex: `storagelab + initialele tale + anul curent`, ex: `storagelabxy2026`). Numele trebuie să aibă între 3 și 24 de caractere.
4. **Region:** Alege o regiune apropiată de tine (ex: West Europe).
5. **Performance:** Lasă Standard (suficient pentru majoritatea cazurilor).
6. **Redundancy:** Alege Locally-redundant storage (LRS) pentru acest laborator, fiind cea mai ieftină opțiune.
7. Apasă “Review” și apoi “Create”. Așteaptă câteva minute până se finalizează crearea (vei primi o notificare).

### Pasul 2: Creează un Container

1. Mergi la resursa Storage Account pe care tocmai ai creat-o (poți apăsa pe “Go to resource” din notificare).
2. În meniul din stânga, sub secțiunea “Data storage”, selectează **Containers**.
3. Apasă pe butonul “+ Container” din partea de sus.
4. **Name:** Dă-i un nume, de exemplu `imagini` sau `documente`. Numele trebuie să fie cu litere mici.
5. **Public access level:** Alege `Private (no anonymous access)`. Aceasta este setarea cea mai sigură și înseamnă că nimeni nu poate accesa fișierele fără permisiune.
6. Apasă “Create”.

### Pasul 3: Încarcă un Fișier (Blob)

1. Intră în containerul `imagini` pe care l-ai creat (apasă pe numele lui).
2. Apasă pe butonul “Upload” din partea de sus.

3. În panoul care apare în dreapta, apasă pe iconița de folder (sau zona de drag-and-drop) pentru a selecta un fișier de pe computerul tău. Alege o imagine mică (ex: un screenshot, o poză).
4. Poți lăsa celelalte setări la valorile implicite.
5. Apasă pe butonul “Upload” din partea de jos a panoului.

Felicitări! Tocmai ai încărcat primul tău blob în Azure. Fișierul tău este acum stocat în siguranță, cu 3 copii, într-un centru de date Azure.

#### Pasul 4: Generează un Shared Access Signature (SAS)

Acum, să partajăm în mod securizat fișierul.

1. În containerul `imagini`, vei vedea fișierul pe care l-ai încărcat. Apasă pe numele fișierului pentru a-i vedea proprietățile.
2. În pagina blob-ului, în tab-urile de sus, selectează **Generate SAS**.
3. În noul panou, configurează token-ul:
  - **Signing key:** Lasă `Key 1` (sau `Account key`).
  - **Permissions:** Bifează doar **Read** (citire). Nu vrem să permitem modificarea sau ștergerea.
  - **Start and expiry date/time:** Setează data de expirare la **1 oră** de acum (sau mai mult, dacă vrei să testezi mai târziu).
  - **Allowed IP addresses:** Lasă gol pentru a permite accesul de oriunde (sau introdu IP-ul tău pentru restricție suplimentară).
4. Apasă pe “Generate SAS token and URL”.
5. Azure va genera două câmpuri. Copiază valoarea din câmpul **Blob SAS URL** (este un link complet, gata de folosit).

#### Pasul 5: Testează Link-ul

1. Deschide un nou tab în browser (sau un browser în mod incognito/private pentru a testa fără autentificare Azure).
2. Lipește link-ul SAS URL pe care l-ai copiat în bara de adrese și apasă Enter.
3. Ar trebui să poți vedea imaginea sau să o descarci. Dacă încerci să accesezi același link după o oră (sau după timpul de expirare pe care l-ai setat), nu va mai funcționa și vei primi o eroare de autentificare!

## Pasul 6: Curățenie (Foarte Important!)

**ATENȚIE:** Nu uita să ștergi Resource Group-ul Storage-Lab-RG după ce termini pentru a elimina toate resursele și a opri orice cost potențial.

1. În Azure Portal, căută “Resource groups”.
  2. Găsește Storage-Lab-RG și apasă pe el.
  3. Apasă pe butonul “Delete resource group” din partea de sus.
  4. Confirmă ștergerea scriind numele grupului de resurse și apasă “Delete”.
- 

## ★ QUIZ TIME! ★

1. Care este primul pas în utilizarea Azure Storage?
  - a) Crearea unui container.
  - b) Crearea unui Storage Account.
  - c) Încărcarea unui fișier.
2. Ce nivel de acces public este cel mai sigur pentru un container?
  - a) Public
  - b) Blob
  - c) Private
3. Ce informații NU poți specifica atunci când generezi un SAS token?
  - a) Permișunile (citire, scriere).
  - b) Data de expirare.
  - c) Nivelul de redundanță (LRS, GRS).
4. De ce este important să ștergi Resource Group-ul după un laborator?
  - a) Pentru a elibera numele unic al contului de stocare.
  - b) Pentru a opri toate costurile asociate cu resursele create.
  - c) Pentru a reseta permisiunile.
5. Ce se întâmplă dacă încerci să accesezi un SAS URL după data sa de expirare?
  - a) Primești o eroare de autentificare (403 Forbidden sau similar).
  - b) Ești redirecționat către Azure Portal.
  - c) Link-ul continuă să funcționeze.

(Răspunsuri la finalul manualului)

---

Misiune îndeplinită, Gardian al Datelor! Ai stocat și ai partajat în mod securizat primul tău artefact digital în vastul univers Azure.

**Achievement Deblocat: Blob Uploader**

+350 XP



## SECȚIUNEA FINALĂ (Partea a III-a)

### Răspunsuri Quiz-uri

#### Capitolul 8:

1. b) Un container de nivel superior care găzduiește serviciile de stocare Azure.
2. b) File Storage
3. c) Decuplarea componentelor unei aplicații pentru procesare asincronă.
4. c) Append Blob
5. c) General Purpose v2 (GPv2)

#### Capitolul 9:

1. b) A crea un Shared Access Signature (SAS) cu permisiuni de scriere și o durată limitată.
2. b) ZRS
3. b) GRS replică datele într-o a doua regiune geografică, LRS nu.
4. b) Role-Based Access Control
5. c) GZRS

#### **Capitolul 10:**

1. b) Crearea unui Storage Account.
  2. c) Private
  3. c) Nivelul de redundanță (LRS, GRS).
  4. b) Pentru a opri toate costurile asociate cu resursele create.
  5. a) Primești o eroare de autentificare (403 Forbidden sau similar).
-

## Glosar de Termeni (Partea a III-a)

Termen	Definiție
<b>Access Tier</b>	Nivel de acces (Hot, Cool, Archive) care optimizează costul în funcție de frecvența accesării.
<b>Append Blob</b>	Tip de blob optimizat pentru operațiuni de adăugare, ideal pentru log-uri.
<b>Blob</b>	Binary Large Object. Un fișier de orice tip stocat în Azure.
<b>Block Blob</b>	Tip de blob compus din blocuri, ideal pentru fișiere mari.
<b>Container</b>	Un folder logic pentru a grupa blob-uri într-un Storage Account.
<b>Entra ID</b>	Serviciul de identitate și acces al Microsoft (fostul Azure Active Directory).
<b>GRS</b>	Geo-Redundant Storage. 3 copii în regiunea primară + 3 copii într-o regiune secundară.
<b>GZRS</b>	Geo-Zone-Redundant Storage. ZRS în regiunea primară + LRS în regiunea secundară.
<b>LRS</b>	Locally-Redundant Storage. 3 copii în același centru de data center.
<b>Page Blob</b>	Tip de blob optimizat pentru operațiuni de citire/scriere aleatorii, folosit pentru VHD-uri.
<b>RA-GRS</b>	Read-Access Geo-Redundant Storage. GRS cu acces de citire la regiunea secundară.
<b>RBAC</b>	Role-Based Access Control. Metodă de a acorda permisiuni bazată pe roluri definite în Entra ID.
<b>SAS</b>	Shared Access Signature. Un URI securizat care acordă acces limitat și temporar la resurse.
<b>Storage Account</b>	Resursa fundamentală care conține toate serviciile de stocare Azure.
<b>ZRS</b>	Zone-Redundant Storage. 3 copii distribuite în 3 zone de disponibilitate diferite.

## Resurse pentru Aprofundare (Storage)

### Documentație Oficială Microsoft:

- [Azure Storage Documentation](#)
- [Azure Blob Storage Documentation](#)
- [Azure Files Documentation](#)
- [Azure Storage Security Guide](#)

### Certificări Recomandate:

- **AZ-104: Azure Administrator** - Include management de Storage Accounts
- **AZ-204: Azure Developer** - Focus pe integrarea cu Storage Services
- **AZ-305: Azure Solutions Architect** - Design de soluții de stocare scalabile

### Hands-on Labs:

- [Microsoft Learn - Store data in Azure](#)
  - [Upload, download, and manage data with Azure Storage Explorer](#)
- 

## Tabelul Final de Achievement-uri (Partea a III-a)

Achievement	Descriere	XP
<b>Data Guardian</b>	Completează Capitolul 8 și înțelege Storage Services	200
<b>Fortress Architect</b>	Completează Capitolul 9 și stăpânește securitatea	300
<b>Blob Uploader</b>	Completează Laboratorul și încarcă primul blob	350
<b>Storage Expert</b>	Finalizează totul cu 90%+ media	200

**Total XP Posibil (Partea a III-a):** 1,050 XP (850 XP din capitole + 200 XP bonus pentru Storage Expert)

---

## Mesaj Final (Partea a III-a)

Felicitări pentru finalizarea acestui modul! Ai explorat fundația oricărei soluții cloud: stocarea. Acum știi cum să alegi serviciul potrivit pentru datele tale, cum să le securizezi și cum să te asiguri că supraviețuiesc oricărui dezastru. Aceste competențe sunt esențiale pentru orice profesionist în cloud.

Continuă să experimentezi. Creează diferite tipuri de conturi de stocare, explorează Azure Files și încearcă să trimiți un mesaj printr-o coadă (Queue). Cu cât exercezi mai mult, cu atât vei deveni un arhitect mai bun.

**Drumul tău în Azure continuă!** 