Disaster Recovery & Business Continuity în Azure

Ghid complet zero-to-hero: Azure Site Recovery, Azure Backup, storage geo-redundant, RTO vs RPO, arhitecturi cross-region, Front Door și Traffic Manager.

WEBINAR · CURS PRACTIC

Public țintă: Junior cloud engineers, administratori Azure, ingineri de infrastructură, ingineri de platformă și profesioniști care vor să treacă de la teorie la design și execuție practică.

Obiectivele cursului

La finalul acestui webinar, fiecare cursant va fi capabil să:

1

Explice diferențele

Să distingă clar între high availability, backup și disaster recovery — trei concepte frecvent confundate în practică.

2

Definească RTO și RPO

Să definească Recovery Time Objective și Recovery Point Objective pentru orice workload, pornind de la cerințele de business.

3

Aleagă modelul corect

Să selecteze modelul potrivit de protecție (backup, ASR, geo-redundanță, active-active, active-passive) în funcție de context și buget.

4

Implementeze din portal

Să configureze din Azure Portal un scenariu coerent de continuitate operațională, de la vault la test failover.

Agenda webinarului

01

De ce contează DR și Business Continuity

Diferența dintre HA, Backup și DR. Analogii practice și întrebări de business.

02

Concepte fundamentale: RTO, RPO, failover, failback

Definiții, tabele de implicații tehnice și modele de cost.

03

Serviciile Azure și rolul fiecăruia

ASR, Backup, GRS/GZRS, Front Door, Traffic Manager — când și cum le combini.

04

Azure Site Recovery — deep dive

Deploy pas cu pas, recovery plans, test failover, checklist pre-activare.

05

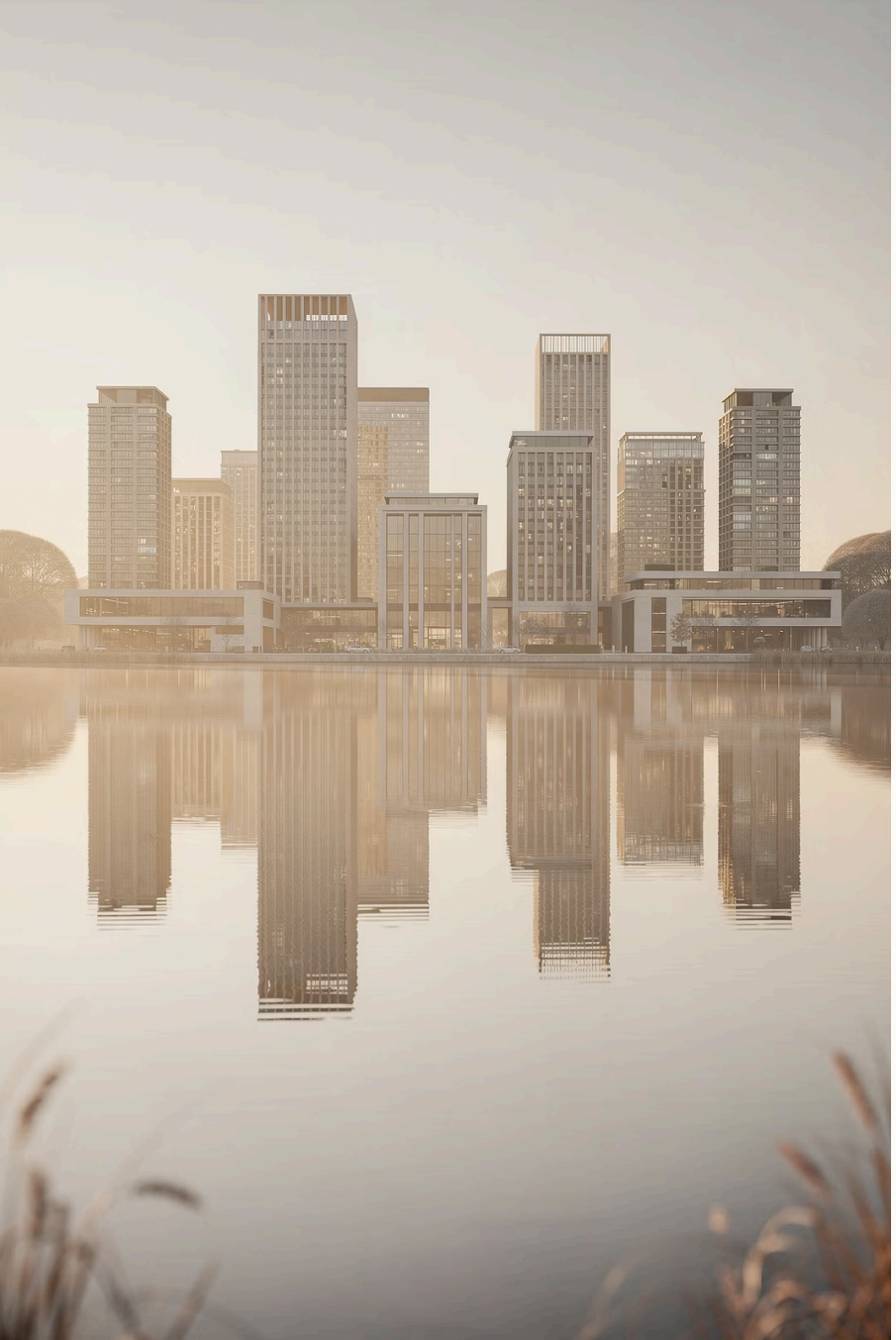
Azure Backup și politici de protecție

Vault, policy, redundanță, soft delete, restore test.

06

Arhitecturi cross-region, Front Door, Traffic Manager, Runbooks, Labs

Active-active vs active-passive, deploy Front Door/TM, greșeli frecvente, checklist arhitect.



CAPITOL 1

De ce contează Disaster Recovery și Business Continuity

Multe echipe confundă trei lucruri complet diferite: reziliența locală, backup-ul și recuperarea în caz de dezastru. Înțelegerea diferenței este primul pas spre un design matur.

Trei concepte diferite, adesea confundate

High Availability

O mașină virtuală cade și pornește rapid pe alt host. Reducerea downtime-ului la nivel local sau zonal. **Analogie:** airbag și ABS pe aceeași mașină.

Backup

Ai o copie a datelor de ieri. Copie de siguranță pentru restaurare la un punct în timp. **Analogie:** copii ale documentelor importante într-un seif.

Disaster Recovery

Un întreg serviciu, o regiune sau un datacenter devine indisponibil și tu poți continua serviciul într-o altă locație. **Analogie:** muți întreaga operațiune într-un alt sediu dacă primul este închis.

Business Continuity

Capacitatea business-ului de a continua funcțiile critice în orice condiții.

Notă practică

Un plan bun nu începe cu portalul Azure. Începe cu întrebări de business: **ce trebuie să supraviețuiască, cât de repede, cu câtă pierdere de date și cu ce buget?**

CAPITOL 2

Concepte fundamentale: RTO, RPO, failover, failback

Recovery Point Objective (RPO)

Cantitatea maximă de date pe care organizația acceptă să o piardă. Răspunde la întrebarea: **câtă dată poți pierde?**

Recovery Time Objective (RTO)

Timpul maxim acceptat până când serviciul revine într-o stare funcțională. Răspunde la întrebarea: **cât timp poți sta indisponibil?**

Backup zilnic

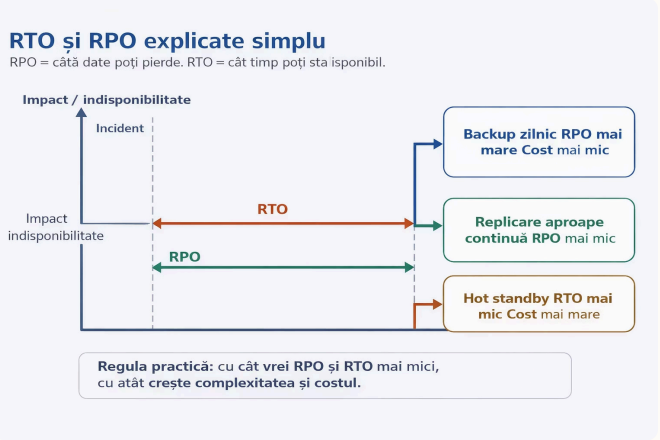
RPO mai mare · Cost mai mic

Replicare aproape continuă

RPO mai mic · Cost mediu

Hot standby

RTO mai mic · Cost mai mare



Regula practică: Cu cât vrei RPO și RTO mai mici, cu atât crește complexitatea și costul.

Failover, Failback și modele de standby

Failover

Mutarea operațiunii din locația primară în cea secundară, fie planificat, fie la incident.

Failback

Revenirea controlată în locația inițială după stabilizarea incidentului.

Test Failover

Exercițiu controlat fără impact major asupra producției, folosit pentru validarea procedurilor.

Active-Active

Ambele regiuni procesează trafic. Cost mai mare, RTO foarte bun.

Active-Passive

Regiunea secundară stă în așteptare. Cost mai mic, activare la incident.

Ținte de business și implicații tehnice

Fiecare obiectiv de business se traduce direct într-o decizie de arhitectură și cost. Tabelul de mai jos ilustrează câteva exemple reprezentative:

Țintă de business	**Exemplu**	**Implicație tehnică**
RPO = 24h	Poți pierde modificările din ultima zi	Backup periodic; de regulă nu este suficient doar pentru aplicații critice
RPO = 15 min	Date aproape la zi	Replicare frecventă sau servicii geo-redundante
RTO = 8h	Sistemul poate fi offline o parte din zi	Warm standby sau restore orchestrat
RTO = 15 min	Aproape fără întrerupere	Arhitectură multi-region, trafic și date pregătite

CAPITOL 3

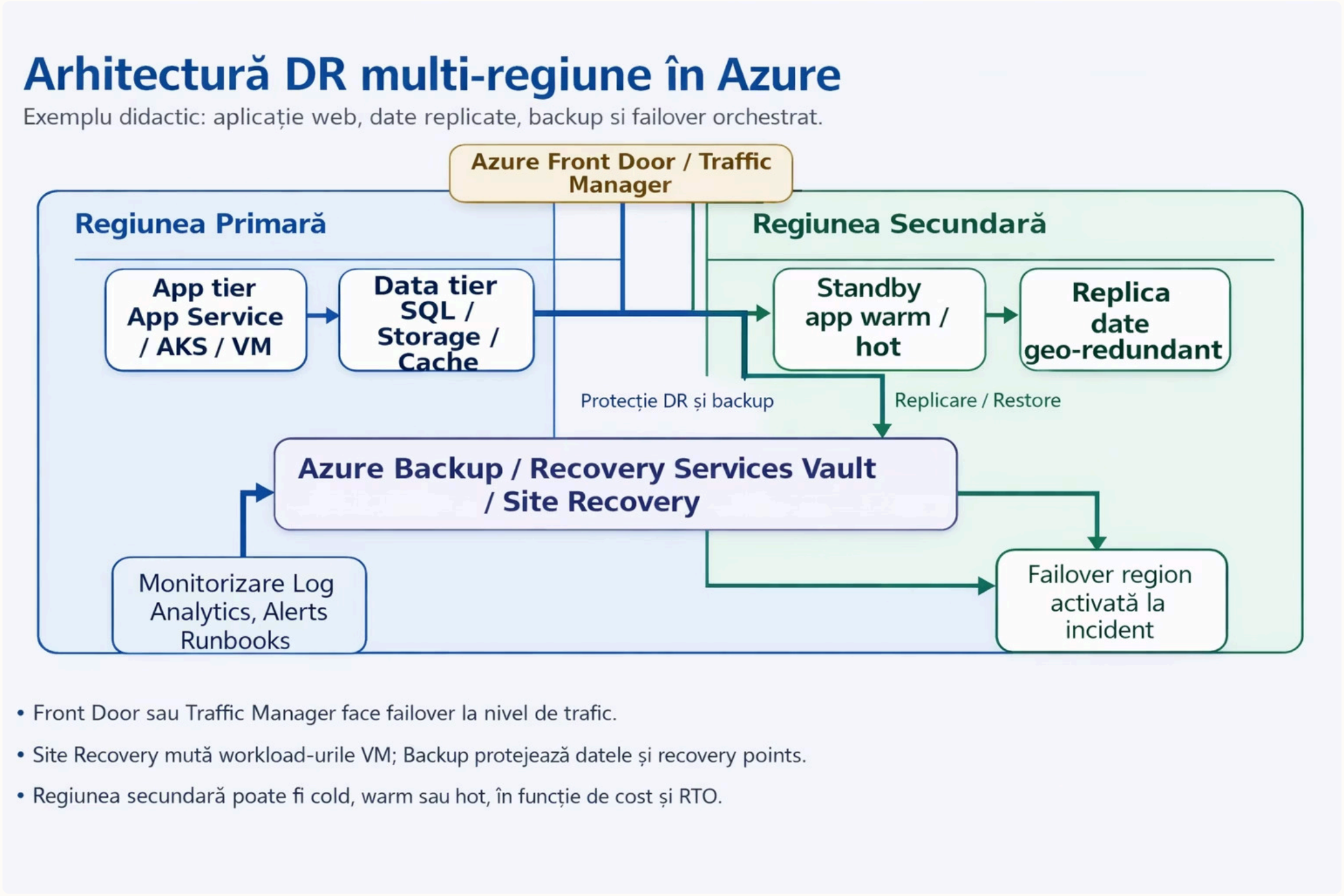
Cum se leagă serviciile Azure între ele

Azure nu are un singur produs care rezolvă tot. Ai nevoie de o combinație de servicii, fiecare cu rolul lui precis. **Regula simplă:** Site Recovery mută workload-uri VM. Backup recuperează date sau mașini la un punct în timp. Front Door și Traffic Manager mută traficul. Storage geo-redundant protejează datele. Toate se completează, nu se exclud reciproc.

Serviciu / Componentă	Ce rezolvă	Când îl alegi
Azure Site Recovery	Replicare și failover pentru VM-uri și servere	Când vrei DR orchestrat pentru mașini virtuale
Azure Backup	Backup și restore pe puncte de timp	Când ai nevoie de retenție, restaurare și protecție la ștergere/ransomware
GRS / GZRS storage	Redundanță a datelor în regiune pereche	Pentru date și backup-uri care trebuie să supraviețuiască unei regiuni
Azure Front Door	Failover și distribuție trafic HTTP/HTTPS la nivel global	Pentru aplicații web și API-uri globale
Azure Traffic Manager	Failover DNS și routing la nivel de endpoint	Pentru servicii care nu depind de reverse proxy L7
Load Balancer / App Gateway	Distribuție trafic într-o regiune	Nu sunt substitut pentru DR cross-region

Arhitectură DR multi-regiune în Azure

Exemplu didactic: aplicație web cu date replicate, failover și failback orchestrat între două regiuni Azure.



Front Door / Traffic Manager

Face failover la nivel de trafic între regiuni.

Site Recovery

Mută workload-urile VM; Backup protejează datele și recovery points.

Regiunea secundară

Poate fi cold, warm sau hot, în funcție de cost și RTO.

CAPITOL 4

Azure Site Recovery (ASR) — Deep Dive

Azure Site Recovery este serviciul Azure folosit pentru orchestrarea replicării, failover-ului și failback-ului pentru Azure VMs, mașini on-premises și alte scenarii suportate. Pentru workload-uri hostate în VM-uri, este piesa centrală a DR-ului.

Ce face concret ASR și când îl alegi

Ce face ASR

- Configurează replicare din sursă către o locație secundară
- Menține recovery points și permite test failover
- Orchestrează failover planificat sau neplanificat
- Poate automatiza ordinea de pornire a workload-urilor și scripts

Când ASR este alegerea corectă

- Aplicația rulează pe Azure VM sau pe servere on-premises și trebuie mutată într-o regiune secundară
- Vrei secvențiere de recovery și recovery plans
- Ai nevoie de testare periodică a DR-ului fără a reconstrui manual întregul mediu

Ce NU trebuie să ceri de la ASR

- Nu este înlocuitor pentru backup pe termen lung
- Nu este soluția nativă pentru PaaS web globale (acolo contează Front Door și replicarea de date)
- Nu reduce la zero nevoia de documentare, runbooks și ownership

Deploy Azure Site Recovery din Azure Portal — Pas cu pas

1

Recovery Services Vault

Creezi sau alegi un Recovery Services vault în **regiunea țintă de DR**.

2

Scenariu de replicare

În vault, deschizi Site Recovery și selectezi scenariul, de exemplu **Azure to Azure** pentru VMs din altă regiune.

3

Validare permisiuni

Validezi permisiunile, subscription-ul sursă și **regiunea țintă**.

4

Configurare target

Alegi resource group-ul de target, rețeaua țintă, subnet-ul și opțional setările de capacity reservation sau availability.

5

Replication policy

Configurezi frecvența recovery points, retention și **app-consistent snapshots** unde este cazul.

6

Activare și test failover

Activezi replication pentru VM-urile selectate. Aștepți starea **Protected** și rulezi un test failover către o rețea izolată.

Notă practică: Insistă pe rețea izolată pentru test failover. Vrei să validezi recovery fără să intri accidental în coliziune cu producția.

Checklist pre-activare ASR — Ce verifică un inginer

Înainte de activarea replicării, un inginer trebuie să valideze fiecare element din tabelul de mai jos. Un failover fără conectivitate sau fără identitate configurată corect este inutil.

Verificare	De ce contează	Exemplu
Target VNet/Subnet	VM-ul recuperat trebuie să pornească într-un spațiu IP valid	10.20.0.0/16 cu subnet dedicat aplicației
NSG și UDR	Recovery fără conectivitate nu ajută	Permiți acces către DB, DNS, jump host
Ordine de pornire	Aplicația pornește doar dacă dependențele există	DB înainte de app
Identity și secrete	Serviciul trebuie să se poată autentifica după failover	Managed identity, Key Vault, DNS
Licensing / sizing	Secundarul trebuie să suporte load-ul minim acceptat	Warm standby la 50% din capacitate

CAPITOL 5

Azure Backup și politicile de protecție

Azure Backup răspunde la o întrebare diferită față de ASR: **cum restaurez datele sau mașina la un punct în timp?** Nu mută în mod implicit traficul web și nu ține loc de orchestrare DR, dar este o piesă critică în continuitate. Greșeala clasică este să configurezi backup și să nu faci niciodată restore test. **Un backup neverificat este doar o speranță, nu o garanție.**

Recovery Services Vault și elementele esențiale ale unei policy

Rolul vault-ului

Recovery Services vault centralizează policy-urile, retenția și punctele de restaurare. Este piesa de bază pentru protecția mașinilor virtuale și scenarii clasice de backup în Azure.

Elemente esențiale într-o policy de backup

- Frecvența backup-ului
- Retenția zilnică, săptămânală, lunară, anuală
- Tipul de redundanță al datelor de backup
- Soft delete, protecție la ștergere și controlul accesului
- Teste periodice de restore

Deploy backup din portal — pași practici

1. Creezi un Recovery Services vault în regiunea principală
2. Alegi redundanța potrivită (ex. GRS pentru reziliență regională)
3. Din vault selectezi Backup, apoi tipul de workload (Azure VM, SQL in Azure VM, Files etc.)
4. Configurezi backup policy: oră, frecvență, retention
5. Selectezi resursele protejate și activezi backup
6. Validezi restore points și efectuezi restaurări de test

Backup vs Site Recovery — Când folosești ce

Întrebare	Azure Backup	Azure Site Recovery
Vreau copie la puncte de timp	✅ Da	Parțial, prin recovery points operaționale
Vreau failover orchestrat	❌ Nu	✅ Da
Vreau retenție luni/ani	✅ Da	❌ Nu acesta este scopul principal
Vreau testarea mutării workload-ului	Indirect, prin restore	✅ Da, prin test failover

Concluzie: Backup și Site Recovery nu se exclud — se completează. Un design matur le folosește pe amândouă cu roluri clare.

CAPITOL 6

Strategii de redundanță pentru date și storage

Nu toate datele se protejează la fel. Pentru unele workload-uri, principalul risc este ștergerea accidentală. Pentru altele, este pierderea unei întregi regiuni. Aici intervin modelele de redundanță de storage și replicarea serviciilor de date.

LRS

Copie locală în aceeași locație. Cost minim, protecție limitată.

ZRS

Copie între zone din aceeași regiune. Bun pentru reziliență zonală.

GRS / GZRS

Copie asincronă într-o regiune pereche. Bun pentru scenarii de DR regional.

Cross-Region Restore

Pentru backup-uri și servicii suportate, restaurare în regiunea secundară.

Notă practică: Dacă ai un fișier important într-un storage account cu geo-redundanță, datele sunt protejate la nivel de replicare. Dar aplicația care le folosește ar putea totuși să fie indisponibilă. Pentru DR complet, trebuie să te uiți separat la compute, trafic, identitate, DNS și date.

Protecție recomandată pe tip de workload

Tip workload	Protecție minimă	Protecție recomandată
Documente / fișiere	Backup + soft delete	GRS/GZRS + backup + restore test
Bază de date critică	Backup automat	HA nativ + geo-redundanță + plan de failover
VM aplicație business	Backup zilnic	ASR + backup + validare aplicație
Site public global	Load balancer local	Front Door + date replicate + secundar pregătit

CAPITOL 7

Arhitecturi Cross-Region: Active-Active vs Active-Passive

Aici se joacă mare parte din cost. Cu cât vrei recuperare mai rapidă și experiență mai bună pentru utilizatori, cu atât trebuie să pregătești mai mult secundarul.

Active-Passive

- Regiunea principală deservește traficul
- Regiunea secundară este pregătită minimal sau moderat
- Failover doar la incident
- Cost mai mic, operare mai simplă
- RTO poate fi mai mare

Potrivit pentru: payroll intern, portal de raportare, aplicații non-critice.

Active-Active

- Ambele regiuni procesează trafic sau sunt pregătite să o facă instant
- RTO redus semnificativ
- Necesită design de date, consistență și observabilitate mai bune
- Cost și complexitate mai ridicate

Potrivit pentru: checkout, e-commerce, servicii publice critice.

Notă practică: Nu există un răspuns universal. Alegerea depinde de RTO/RPO aprobate de business și de bugetul disponibil.

CAPITOL 8

Azure Front Door și Traffic Manager pentru Disaster Recovery

Aceste două servicii se ocupă de **trafic**, nu de backup-ul datelor. Mulți juniori se blochează aici: dacă pui Front Door în față, nu ai rezolvat automat replicarea bazei de date sau mutarea VM-urilor. Traficul și datele sunt responsabilități separate.

Front Door vs Traffic Manager — Când alegi ce

Criteriu	Front Door	Traffic Manager
Nivel	HTTP/HTTPS global entry point	DNS-based routing
Failover	Rapid, pe baza health probes și origin groups	Depinde și de TTL/cache DNS
WAF / TLS / caching	Da	Nu
Tip scenarii	Web apps, APIs	Mai general, inclusiv endpoint-uri non-Azure

Când alegi Azure Front Door

- Aplicații web și API-uri HTTP/HTTPS
- Routing și health probes la nivel global
- Ai nevoie de WAF, TLS termination, caching sau layer 7 intelligence
- Active-active sau active-passive pentru aplicații web

Când alegi Azure Traffic Manager

- Failover DNS între endpoint-uri
- Serviciile pot fi Azure sau externe
- Nu ai nevoie de reverse proxy global layer 7
- Tolerezi comportamentul specific DNS caching

Deploy Azure Front Door din portal — Pași clari

1

Creare profil

Creezi un Azure Front Door profile, de regulă **Standard sau Premium**.

2

Endpoint public

Creezi un endpoint public care va fi punctul de intrare global.

3

Origin group

Definești un origin group cu **origin-ul primar și cel secundar**.

4

Health probes și load balancing

Configurezi health probes și regulile de load balancing între origini.

5

Route

Configurezi route-ul pentru hostname și paths.

6

Test failover

Testezi oprirea controlată a origin-ului primar și observi direcționarea către secundar.

Deploy Traffic Manager din portal — Pași clari

1

Creare profil

Creezi un **Traffic Manager profile** în Azure Portal.

2

Routing method

Alegi routing method, de exemplu **Priority** pentru failover clasic.

3

DNS și monitor

Configurezi DNS name, TTL și **monitor settings** pentru health check.

4

Endpoint-uri

Adaugi **endpoint-ul primar și secundar** cu prioritățile corespunzătoare.

5

Test indisponibilitate

Verifici monitor health și execuți un **test de indisponibilitate** pentru a valida failover-ul DNS.

CAPITOL 9

Runbooks, Monitorizare și Guvernare Operațională

Tehnologia singură nu livrează continuitate. Ai nevoie de monitoring, alertare, roluri clare și proceduri executabile sub presiune. Un plan bun de DR nu înseamnă doar tehnologie — înseamnă roluri clare, decizie de activare, teste recurente, proceduri de comunicare și evidență a dependențelor.

Ciclul unui plan de Disaster Recovery

1

1. Definești obiectivele

RTO, RPO, impact business, servicii critice

2

2. Protejezi

Backup, ASR, replicare, monitorizare

3

3. Testezi

Test failover, runbook, roluri și acces

4

4. Declanșezi

Decizie formală, comunicare, failover

5

5. Operezi în DR

Validare aplicație, DNS/traffic, monitoring

6

6. Failback

Revenire controlată, sincronizare, lessons learned

Instrumente de monitorizare și guvernare

Azure Monitor și Alert Rules

Monitorizare continuă a sănătății aplicației și a stării replicării. Alerte proactive înainte ca incidentul să escaladeze.

Log Analytics

Corelarea incidentelor din multiple surse. Vizibilitate unificată asupra întregului stack.

Action Groups

Notificare automată către echipa on-call la declanșarea alertelor critice.

Runbooks și Checklist-uri

Proceduri aprobate pentru failover și failback, executabile sub presiune, fără ambiguitate.

Exerciții recurente

Nu doar un test anual formal. Exerciții periodice pentru validarea procedurilor și a echipei.

CAPITOL 10

Exemple reale de use cases

Teoria prinde sens când o aplici pe scenarii concrete. Iată trei exemple reprezentative care acoperă cele mai frecvente situații întâlnite în practică.

Use Case 1 — Aplicație internă pe două VM-uri și SQL

Compute — VM-urile aplicației

Protejate cu **Azure Site Recovery**. Replicare configurată către regiunea secundară, test failover periodic, recovery plan cu ordine de pornire definită.

Date — Baza de date SQL

Protejată prin **mecanismul nativ de backup** sau prin backup și restaurare în regiunea secundară. Geo-redundanță activată pentru datele critice.

Trafic

Mutat prin **Traffic Manager** sau DNS operațional la momentul failover-ului. Simplu, fără overhead de layer 7.

Use Case 2 — Portal public multi-region

Trafic global

Azure Front Door în față, cu health probes, WAF și routing inteligent. Failover automat la nivel de trafic HTTP/HTTPS.

Compute

Două **App Services sau două clusteri AKS** în regiuni diferite, pregătite să preia traficul instant.

Date

Date replicate sau serviciu PaaS cu capabilități native de failover (ex. Azure SQL cu geo-replication).

Observabilitate

Observabilitate unificată și **runbooks clare** pentru activare, operare în DR și failback controlat.

Use Case 3 — On-premises către Azure

Rolul ASR în scenariul on-premises

Dacă sursa este on-premises, **Azure Site Recovery** te ajută să ridici workload-urile în Azure. ASR acționează ca mecanism de replicare și orchestrare a failover-ului din datacenter-ul propriu către cloud.

Ce trebuie să verifici atent

- **Conectivitate** — ExpressRoute sau VPN între on-premises și Azure
- **IP addressing** — evitarea conflictelor de adresare între rețelele sursă și țintă
- **DNS** — rezoluție corectă după failover
- **Acces operator** — jump host, bastion sau acces securizat în Azure
- **Proceduri de failback** — revenirea controlată on-premises după stabilizare

CAPITOL 11

Laborator didactic recomandat

Fiecare laborator este conceput pentru a traduce teoria în practică. Cursanții lucrează în Azure Portal și produc un rezultat verificabil la finalul fiecărui exercițiu.

Exercițiu	Obiectiv	Rezultat așteptat
Lab 1 — RTO/RPO workshop	Traduci cerințe business în obiective tehnice	Fiecare echipă definește țintele și justifică costul
Lab 2 — Azure Backup	Configurezi un vault și policy, apoi rulezi restore test	Cursantul demonstrează restore point și verificare
Lab 3 — ASR pentru VM	Activezi replicare și test failover către rețea izolată	Workload-ul pornește în regiunea secundară
Lab 4 — Front Door / Traffic Manager	Simulezi indisponibilitatea regiunii primare	Traficul ajunge în secundar
Lab 5 — Runbook de failback	Documentezi pașii de revenire	Checklist clar și ordonat

CAPITOL 12

Greșeli frecvente în proiectele de DR

Cunoașterea greșelilor comune este la fel de valoroasă ca și cunoașterea bunelor practici. Iată cele mai frecvente capcane întâlnite în proiectele reale de DR.

Top greșeli — Ce să eviți

- [ ] **Backup confundat cu Disaster Recovery**

  Backup-ul restaurează date la un punct în timp. DR mută întregul serviciu. Sunt complementare, nu interschimbabile.

- [ ] **Identitate, DNS și secrete uitate**

  Se uită de identitate, DNS, Key Vault, secrete și dependențe externe. Un VM pornit fără autentificare funcțională este inutil.

- [ ] **Testare doar a infrastructurii**

  Se testează doar infrastructura, nu și funcționalitatea aplicației. Un VM pornit nu înseamnă o aplicație funcțională.

- [ ] **Lipsa ownership-ului de activare**

  Nu există ownership pentru activarea oficială a planului. Cine decide că se face failover? Cine apasă butonul?

- [ ] **RTO de minute cu buget de laborator**

  Se proiectează RTO de minute cu buget de laborator. RTO mic costă. Dacă bugetul nu susține arhitectura, RTO-ul nu este realist.

- [ ] **Failback nedocumentat**

  Nu se documentează failback-ul. Echipa știe să plece în DR, dar nu și să revină controlat. Failback-ul neplanificat poate cauza pierderi de date.

CAPITOL 13

Checklist de design pentru arhitect sau inginer cloud

Folosește acest checklist ca instrument de validare înainte de a considera un design de DR matur și gata de producție.

Workload-uri critice identificate

Știm exact ce workload-uri sunt critice și avem o listă aprobată de business?

RTO și RPO aprobate

Avem RTO și RPO aprobate formal de business, nu doar estimate tehnic?

Protecție separată pe piloni

Avem protecție separată pentru compute, date și trafic — nu o soluție unică pentru toate?

Test failover executat recent

Am executat cel puțin un test failover în ultimele 6-12 luni?

Runbook de failback și owner

Avem runbook de failback documentat și un owner operațional desemnat?

Restore test pentru backup-uri

Am testat restore pentru backup-urile critice? Un backup neverificat nu este o garanție.

CAPITOL 14

Concluzie

Un program matur de Disaster Recovery în Azure nu se construiește doar din butoane din portal. Se construiește din obiective clare, design corect, roluri clare, disciplină de testare și alegerea potrivită a serviciilor.

Mesajul central al cursului

Site Recovery

Pentru mutarea workload-urilor VM între regiuni, cu orchestrare, recovery plans și test failover.

Azure Backup

Pentru protecția punctelor de timp, retenție pe termen lung și restaurare la incident de date.

Storage geo-redundant

Pentru date care trebuie să supraviețuiască pierderii unei întregi regiuni Azure.

Front Door / Traffic Manager

Pentru failover de trafic la nivel global, independent de mutarea datelor și a compute-ului.

> **DR nu este doar tehnologie.** Este o combinație de arhitectură, operațiuni, securitate, networking, ownership și exercițiu practic.

Temă recomandată: Luați o aplicație simplă cu web + DB și descrieți, într-o singură pagină, ce faceți pentru compute, pentru date, pentru trafic și pentru testare DR. Dacă nu puteți răspunde clar la toate patru, designul nu este încă matur.