Implementarea protecției datelor

Introducere în laborator

În acest laborator, veți învăța despre backup-ul și recuperarea mașinilor virtuale Azure. Veți învăța să creați un seif de servicii de recuperare și o politică de backup pentru mașinile virtuale Azure. Veți afla despre recuperarea în caz de dezastru cu Azure Site Recovery.

Acest laborator necesită un abonament Azure. Tipul de abonament poate afecta disponibilitatea funcțiilor din acest laborator. Puteți modifica regiunile, dar pașii sunt scriși folosind **East US** și **West US** .

Timp estimat: 50 de minute

Scenariu de laborator

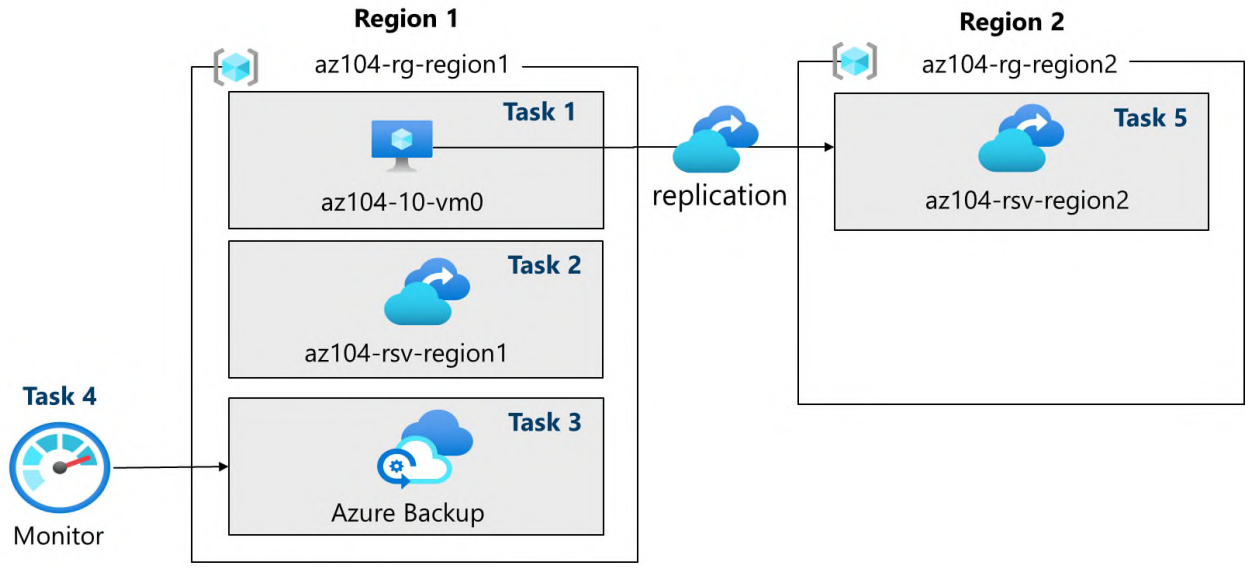
Organizația dumneavoastră evaluează modul de a face backup și de a restaura mașinile virtuale Azure după pierderi accidentale sau rău intenționate de date. În plus, organizația dorește să exploreze utilizarea Azure Site Recovery pentru scenarii de recuperare în caz de dezastru.

Competențe profesionale

- Sarcina 1: Utilizați un șablon pentru a furniza o infrastructură.
- Sarcina 2: Creați și configurați un seif Recovery Services.
- Sarcina 3: Configurați backup-ul la nivel de mașină virtuală Azure.
- Sarcina 4: Monitorizarea Azure Backup.
- Sarcina 5: Activarea replicării mașinii virtuale.

Timp estimat: 40 de minute

Diagramă de arhitectură



Sarcina 1: Utilizarea unui șablon pentru a furniza o infrastructură

În această sarcină, veți utiliza un șablon pentru a implementa o mașină virtuală. Mașina virtuală va fi utilizată pentru a testa diferite scenarii de backup.

1. Descărcați fișierele de laborator **\Allfiles\Lab10** .
2. Conectați-vă la **portalul Azure** - https://portal.azure.com.
3. Căutați și selectați Deploy a custom template.
4. Pe pagina de implementare personalizată, selectați **Creați-vă propriul șablon în editor** .
5. Pe pagina de editare a șablonului, selectați **Încărcare fișier** .
6. Localizați și selectați fișierul **\Allfiles\Lab10\az104-10-vms-edge-template.json** și selectați **Deschidere** .

Notă: Acordați-vă un moment pentru a examina șablonul. Implementăm o rețea virtuală și o mașină virtuală pentru a putea demonstra backup-ul și recuperarea.

7. **Salvați** modificările.
8. Selectați **Editare parametri** și apoi **Încărcare fișier** .
9. Încărcați și selectați fișierul **\Allfiles\Lab10\az104-10-vms-edge-parameters.json** .
10. **Salvați** modificările.

11. Folosiți următoarele informații pentru a completa câmpurile de implementare personalizată, lăsând toate celelalte câmpuri cu valorile lor implicite:

Setare	**Valoare**
Abonament	Abonamentul dvs. Azure
Grup de resurse	az104-rg-region1(Dacă este necesar, selectați **Creare nou**)
Regiune	**Estul SUA**
Nume de utilizator	**administrator local**
Parolă	Furnizați o parolă complexă

12. Selectați **Revizuire + Creare** , apoi selectați **Creare** .

Notă: Așteptați implementarea șablonului, apoi selectați **Accesați resursa** . Ar trebui să aveți o mașină virtuală într-o rețea virtuală.

Sarcina 2: Crearea și configurarea unui seif Recovery Services

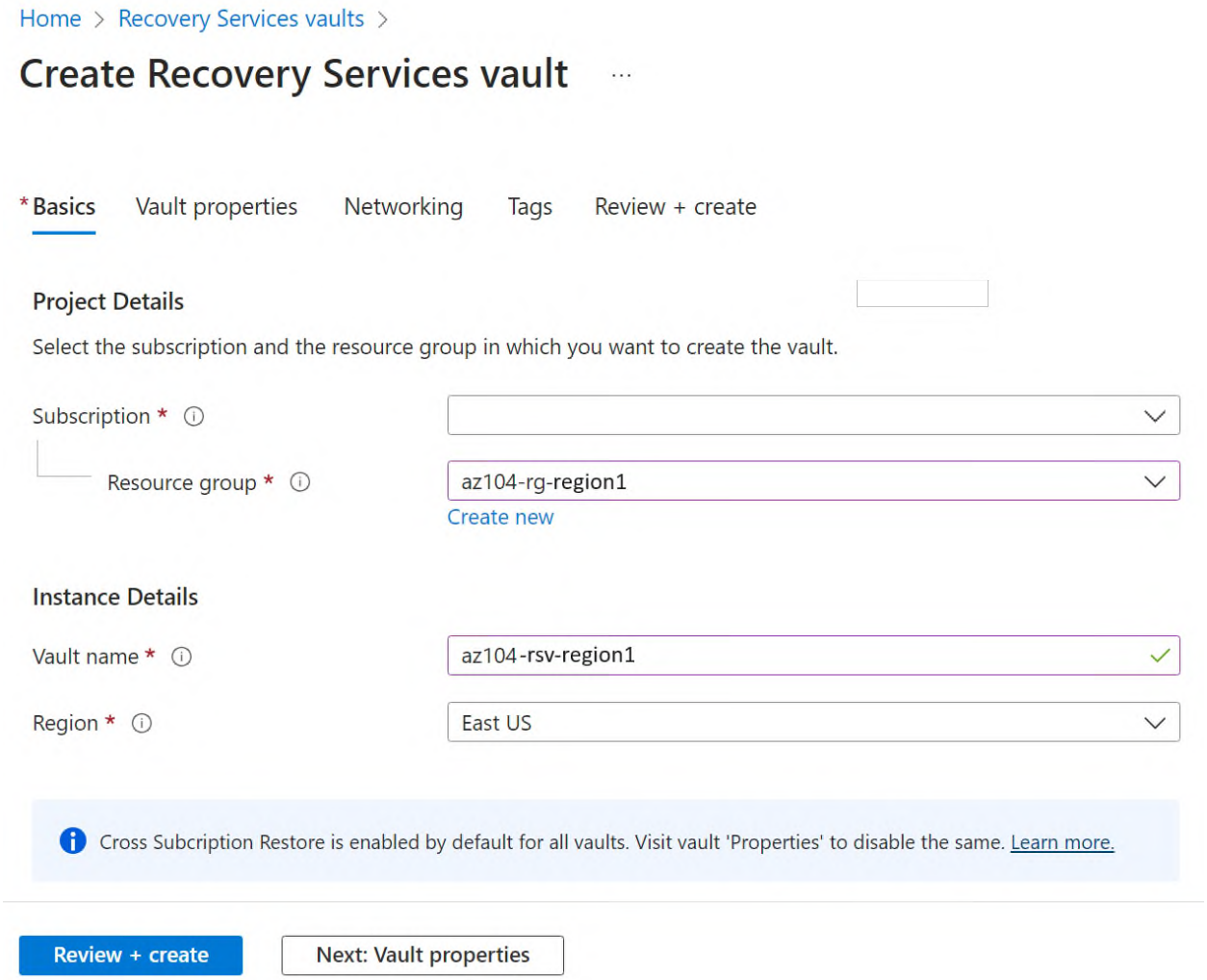
În această sarcină, veți crea un seif Recovery Services. Un seif Recovery Services oferă spațiu de stocare pentru datele mașinii virtuale.

1. În portalul Azure, căutați și selectați Recovery Services vaults, apoi, pe lama **Recovery Services vaults** , faceți clic pe **+ Creare** .
2. Pe blade-ul **seifului Create Recovery Services** , specificați următoarele setări:

Setări	**Valoare**
Abonament	numele abonamentului dvs. Azure
Grup de resurse	az104-rg-region1
Numele seifului	az104-rsv-region1

Setări	Valoare
Regiune	**Estul SUA**

3. **Notă** : Asigurați-vă că specificați aceeași regiune în care ați implementat mașinile virtuale în sarcina anterioară.



4.
5. Faceți clic **pe Revizuire + Creare** , asigurați-vă că validarea a trecut cu succes, apoi faceți clic pe **Creare** .

Notă : Așteptați finalizarea implementării. Implementarea ar trebui să dureze câteva minute.

6. Când implementarea este finalizată, faceți clic **pe Accesați resursa** .
7. În secțiunea **Setări** , faceți clic pe **Proprietăți** .

8. Selectați linkul **Actualizare** de sub eticheta **Configurare copie de rezervă** .
9. În lama **Configurare copie de rezervă** , examinați opțiunile pentru **Tip replicare stocare** . Lăsați setarea implicită **Geo-redundant** și închideți lama.

Notă : Această setare poate fi configurată numai dacă nu există elemente de rezervă.

Știați că... Opțiunea Cross Region Restore vă permite să restaurați datele într-o regiune secundară, asociată cu Azure.

10. Selectați linkul **Actualizare** de sub **Setări de securitate > Ștergere soft și** eticheta setări de securitate.
11. În lama **Setări de securitate** , rețineți că **Ștergerea soft (pentru sarcini de lucru care rulează în Azure)** este **activată** . Observați că **perioada de păstrare a ștergerii soft** este **de 14** zile.

Știați că... Azure are două tipuri de seifuri: seifuri pentru servicii de recuperare și seifuri pentru copii de rezervă. Principala diferență constă în sursele de date care pot fi copiate de rezervă. Aflați mai multe despre diferențe .

Sarcina 3: Configurarea copiei de rezervă la nivel de mașină virtuală Azure

În această sarcină, veți implementa o copie de rezervă la nivel de mașină virtuală Azure. Ca parte a unei copii de rezervă a mașinii virtuale, va trebui să definiți politica de copiere de rezervă și retenție care se aplică copiei de rezervă. Mașinile virtuale diferite pot avea atribuite politici diferite de copiere de rezervă și retenție.

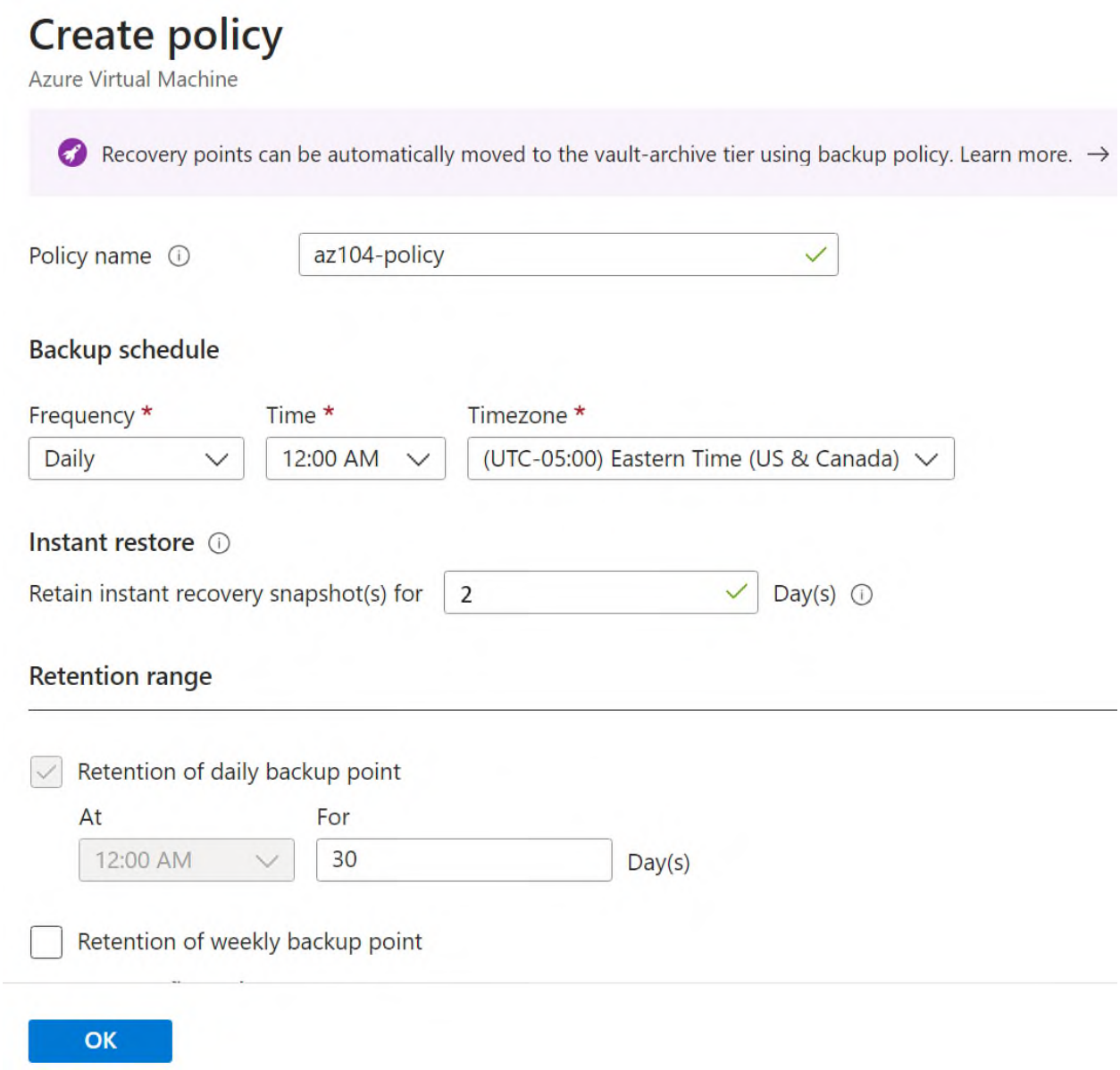
Notă : Înainte de a începe această sarcină, asigurați-vă că implementarea inițiată în prima sarcină a acestui laborator s-a finalizat cu succes.

1. În lama seifului Recovery Services, faceți clic pe **Prezentare generală** , apoi pe **+ Copiere de rezervă** .
2. În lama **Obiectiv de rezervă** , specificați următoarele setări:

Setări	**Valoare**
Unde rulează sarcina ta de lucru?	**Azure** (observați celelalte opțiuni)
Ce vrei să faci backup?	**Mașină virtuală** (observați celelalte opțiuni)

3. Selectați **Copiere de rezervă** .
4. Observați că există două **subtipuri de politici** : **Îmbunătățită** și **Standard** . Examinați opțiunile și selectați **Standard** .
5. În **Politica de rezervă** , selectați **Creați o politică nouă** .
6. Definiți o nouă politică de backup cu următoarele setări (lăsați celelalte cu valorile lor implicite):

Setare	**Valoare**
Numele politicii	az104-backup
Frecvenţă	**Zilnic**
Timp	**00:00**
Fus orar	numele fusului orar local
Păstrați instantaneele de recuperare instantanee pentru	**2** zile



7.

8. Faceți clic pe **OK** pentru a crea politica, apoi, în secțiunea **Mașini virtuale** , selectați **Adăugare** (derulați în jos).
9. În lama **Selectare mașini virtuale** , selectați **az-104-10-vm0** , faceți clic pe **OK** , apoi, înapoi în lama **Copiere de rezervă** , faceți clic pe **Activare copie de rezervă** .

Notă : Așteptați ca backup-ul să fie activat. Acest lucru ar trebui să dureze aproximativ 2 minute.

10. După implementare, selectați **Accesați resursa** .
11. În secțiunea **Elemente protejate** , faceți clic pe **Elemente de rezervă** , apoi faceți clic pe intrarea **Mașină virtuală Azure** .

12. Selectați linkul **Vizualizare detalii** pentru **az104-10-vm0** și examinați valorile intrărilor **Preverificare copie de rezervă** și **Stare ultima copie de rezervă** .

Notă: Observați că copia de rezervă este în așteptare.

13. Selectați **Copiere de rezervă acum** , acceptați valoarea implicită din lista derulantă **Păstrare copie de rezervă până la** și faceți clic pe **OK** .

Notă : Nu așteptați finalizarea copiei de rezervă, ci treceți la următoarea sarcină.

Sarcina 4: Monitorizarea Azure Backup

În această sarcină, veți implementa un cont de stocare Azure. Apoi, veți configura seiful pentru a trimite jurnalele și metricile către contul de stocare. Acest depozit poate fi apoi utilizat cu Log Analytics sau alte soluții de monitorizare terțe.

1. Din portalul Azure, căutați și selectați Storage accounts.
2. Pe pagina Conturi de stocare, selectați **Creare** .
3. Folosește următoarele informații pentru a defini contul de stocare, apoi selectează **Revizuire + creare** .

Setări	**Valoare**
Abonament	*Abonamentul dumneavoastră*
Grup de resurse	**az104-rg-regiunea1**
Numele contului de stocare	Furnizați un nume unic la nivel global
Regiune	**Estul SUA**

4. Selectați **Creare** .

Notă : Așteptați finalizarea implementării. Ar trebui să dureze aproximativ un minut.

5. Căutați și selectați seiful Recovery Services.
6. În lama **Monitorizare** , selectați **Setări diagnosticare** , apoi selectați **Adăugare setare diagnosticare** .
7. Denumiți setarea Logs and Metrics to storage.
8. Bifați următoarele categorii de jurnale și metrici:

- **Date de raportare pentru backup-ul Azure**
- **Date suplimentare pentru joburile de backup Azure**
- **Date de alertă pentru backup Azure Addon**
- **Joburi de recuperare a site-urilor Azure**
- **Evenimente de recuperare a site-ului Azure**

9. În Detaliile destinației, bifați opțiunea **Arhivare într-un cont de stocare** .
10. În câmpul derulant Cont de stocare, selectați contul de stocare pe care l-ați implementat anterior în această activitate.
11. Selectați **Salvare** .
12. Reveniți la seiful Serviciilor de recuperare, în blade-ul **Monitorizare** selectați **Lucrări de backup** .
13. Localizați operațiunea de backup pentru mașina virtuală **az104-10-vm0** .
14. **Vizualizați detaliile** (derulați la dreapta pentru link) ale sarcinii de backup.

Sarcina 5: Activarea replicării mașinii virtuale

1. În portalul Azure, căutați și selectați Recovery Services vaults, apoi, pe lama **Recovery Services vaults** , faceți clic pe **+ Creare** .
2. Pe blade-ul **seifului Create Recovery Services** , specificați următoarele setări:

Setări	**Valoare**
Abonament	numele abonamentului dvs. Azure
Grup de resurse	az104-rg-region2(Dacă este necesar, selectați **Creare nou**)
Numele seifului	az104-rsv-region2
Regiune	**Vestul SUA**

3. **Notă** : Asigurați-vă că specificați o regiune **diferită** de mașina virtuală.
4. Faceți clic **pe Revizuire + Creare** , asigurați-vă că validarea a trecut cu succes, apoi faceți clic pe **Creare** .

Notă : Așteptați finalizarea implementării. Implementarea ar trebui să dureze câteva minute.

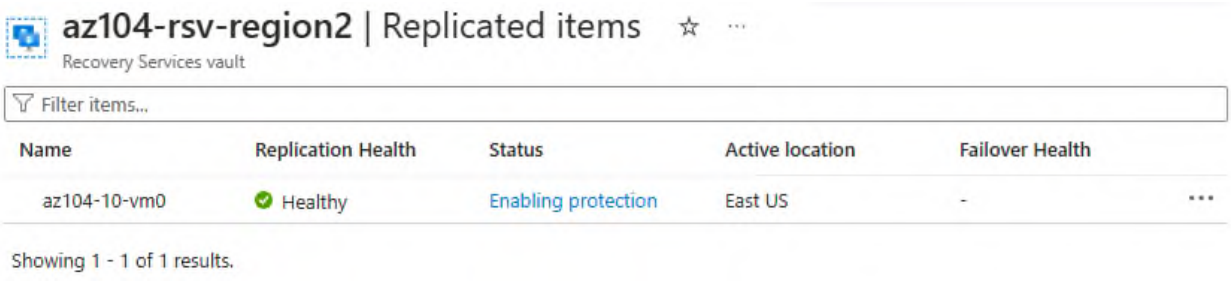
5. Căutați și selectați az104-10-vm0mașina virtuală.
6. În lama **Copiere de rezervă + Recuperare în caz de dezastru** , selectați **Recuperare în caz de dezastru** .
7. În fila **Elemente de bază** , observați **regiunea țintă** .
8. Selectați **Următorul: Setări avansate** . Selecțiile de resurse au fost făcute automat.
9. Derulați în jos și **creați** contul de automatizare.

Notă: Este important ca setările să fie completate, altfel validarea va eșua.

10. Selectați **Revizuire + Pornire replicare** și apoi **Activare replicare** .

Notă : Activarea replicării va dura 10-15 minute. Urmăriți mesajele de notificare din colțul din dreapta sus al portalului. În timp ce așteptați, luați în considerare consultarea linkurilor pentru instruirea în ritm propriu de la sfârșitul acestei pagini.

11. După ce replicarea este completă, căutați și localizați Seiful de servicii de recuperare, **az104-rsv-region2** . Este posibil să fie nevoie să **reîmprospătați** pagina.
12. În secțiunea **Elemente protejate** , selectați **Elemente reproduse** .
13. Verificați dacă mașina virtuală este afișată ca fiind sănătoasă pentru sănătatea replicării. Rețineți că starea va afișa sincronizarea (începând de la 0%) și, în final, va afișa **Protejată** după finalizarea sincronizării inițiale.



14. Selectați mașina virtuală pentru a vedea mai multe detalii.

Știați că... Este o practică bună să testați failover-ul unei mașini virtuale protejate .

Curățați-vă resursele

Dacă lucrați cu **propriul abonament,** acordați-vă un minut pentru a șterge resursele laboratorului. Acest lucru va asigura eliberarea resurselor și reducerea la minimum a

costurilor. Cea mai ușoară modalitate de a șterge resursele laboratorului este să ștergeți grupul de resurse ale laboratorului.

- În portalul Azure, selectați grupul de resurse, selectați **Ștergeți grupul de resurse** , **Introduceți numele grupului de resurse** , apoi faceți clic pe **Ștergeți** .
- Folosind Azure PowerShell, Remove-AzResourceGroup -Name resourceGroupName.
- Folosind interfața CLI, az group delete --name resourceGroupName.

Notă: Pentru a șterge un seif Azure Recovery Services, trebuie mai întâi să eliminați toate dependențele, cum ar fi elementele protejate, serverele de rezervă și conturile de stocare, să dezactivați caracteristicile de securitate, cum ar fi ștergerea soft, apoi să ștergeți seiful în sine. Este disponibil un exemplu de script PowerShell .

Extinde-ți cunoștințele cu Copilot

Copilot vă poate ajuta să învățați cum să utilizați instrumentele de scriptare Azure. Copilot vă poate ajuta, de asemenea, în domenii care nu au fost abordate în laborator sau în care aveți nevoie de mai multe informații. Deschideți un browser Edge și alegeți Copilot (dreapta sus) sau navigați la *copilot.microsoft.com* . Acordați câteva minute pentru a încerca aceste solicitări.

- Ce produse acceptă Azure Backup?
- Rezumați pașii pentru copierea de rezervă și restaurarea unei mașini virtuale Azure cu Azure Backup.
- Cum pot utiliza Azure PowerShell sau CLI pentru a verifica starea unei lucrări Azure Backup?
- Furnizați cel puțin cinci bune practici pentru configurarea copiilor de rezervă ale mașinilor virtuale Azure.

Învață mai multe cu instruire în ritm propriu

- Protejați-vă mașinile virtuale utilizând Azure Backup . Utilizați Azure Backup pentru a vă ajuta să protejați serverele locale, mașinile virtuale, SQL Server, partajările de fișiere Azure și alte sarcini de lucru.
- Protejați-vă infrastructura Azure cu Azure Site Recovery . Oferiți recuperare în caz de dezastru pentru infrastructura Azure prin personalizarea replicării, failover-ului și failback-ului mașinilor virtuale Azure cu Azure Site Recovery.

Concluzii cheie

Felicitări pentru finalizarea laboratorului. Iată principalele concluzii ale acestui laborator.

- Serviciul Azure Backup oferă soluții simple, sigure și rentabile pentru a face backup și a recupera datele.
- Azure Backup poate proteja resursele locale și în cloud, inclusiv mașinile virtuale și partajările de fișiere.
- Politicile Azure Backup configurează frecvența copiilor de rezervă și perioada de păstrare pentru punctele de recuperare.
- Azure Site Recovery este o soluție de recuperare în caz de dezastru care oferă protecție pentru mașinile și aplicațiile virtuale.
- Azure Site Recovery replică sarcinile de lucru pe un site secundar, iar în cazul unei întreruperi sau al unui dezastru, puteți face failover pe site-ul secundar și relua operațiunile cu un timp de nefuncționare minim.
- Un seif Recovery Services stochează datele de rezervă și minimizează cheltuielile generale de administrare.