Implementarea rețelelor virtuale

Introducere în laborator

Acest laborator este primul dintre cele trei laboratoare care se concentrează pe rețelele virtuale. În acest laborator, veți învăța elementele de bază ale rețelelor virtuale și ale subrețelelor. Veți învăța cum să vă protejați rețeaua cu grupuri de securitate de rețea și grupuri de securitate de aplicații. De asemenea, veți afla despre zonele și înregistrările DNS.

Acest laborator necesită un abonament Azure. Tipul de abonament poate afecta disponibilitatea funcțiilor din acest laborator. Puteți schimba regiunea, dar pașii sunt scrișI folosind **East US** .

Timp estimat: 50 de minute

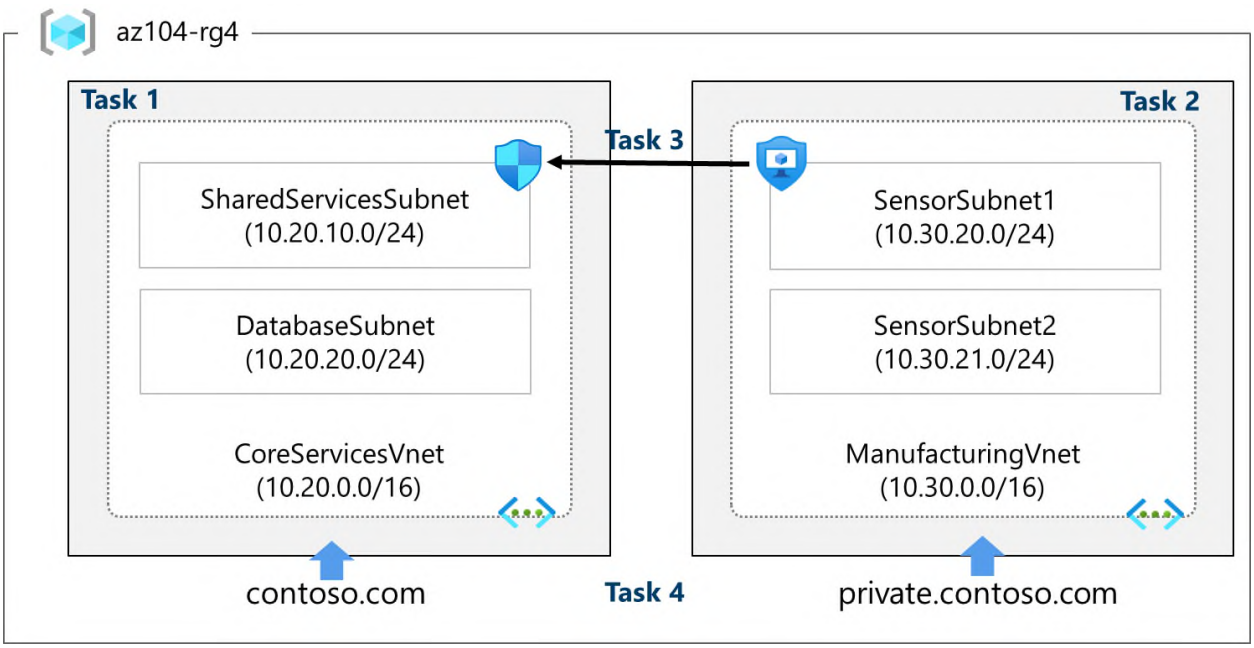
Scenariu de laborator

Organizația dumneavoastră globală intenționează să implementeze rețele virtuale. Scopul imediat este de a acomoda toate resursele existente. Cu toate acestea, organizația se află într-o fază de creștere și dorește să se asigure că există capacitate suplimentară pentru această creștere.

Rețeaua virtuală CoreServicesVnet are cel mai mare număr de resurse. Se anticipează o creștere semnificativă, așadar este necesar un spațiu de adrese mare pentru această rețea virtuală **.**

Rețeaua virtuală ManufacturingVnet conține sisteme pentru operațiunile unităților de producție. Organizația anticipează un număr mare de dispozitive conectate interne de la care sistemele sale pot prelua date **.**

Diagramă de arhitectură



Aceste rețele și subrețele virtuale sunt structurate într-un mod care să permită resursele existente, permițând în același timp creșterea proiectată. Să creăm aceste rețele și subrețele virtuale pentru a pune bazele infrastructurii noastre de rețea.

Știați că?: Este o practică bună să evitați suprapunerea intervalelor de adrese IP pentru a reduce problemele și a simplifica depanarea. Suprapunerea este o problemă în întreaga rețea, fie în cloud, fie local. Multe organizații proiectează o schemă de adresare IP la nivel de întreprindere pentru a evita suprapunerea și a planifica creșterea viitoare.

Competențe profesionale

- Sarcina 1: Creați o rețea virtuală cu subrețele utilizând portalul.
- Sarcina 2: Creați o rețea virtuală și subrețele folosind un șablon.
- Sarcina 3: Creați și configurați comunicarea între un Grup de Securitate a Aplicațiilor și un Grup de Securitate a Rețelei.
- Sarcina 4: Configurați zonele DNS Azure publice și private.

Sarcina 1: Crearea unei rețele virtuale cu subrețele utilizând portalul

Organizația planifică o creștere semnificativă a serviciilor de bază. În această sarcină, creați rețeaua virtuală și subrețelele asociate pentru a acomoda resursele existente și creșterea planificată. În această sarcină, veți utiliza portalul Azure.

1. Conectați-vă la **portalul Azure** - https://portal.azure.com.

2. Căutați și selectați Virtual Networks.
3. Selectați **Creare** pe pagina Rețele virtuale.
4. Finalizați fila **Noțiuni de bază** pentru CoreServicesVnet.

Opţiune	**Valoare**
Grup de resurse	az104-rg4(dacă este necesar, creați unul nou)
Nume	CoreServicesVnet
Regiune	(SUA) **Estul SUA**

5. Accesați fila **Adrese IP** .

Opţiune	**Valoare**
Spațiul de adrese IPv4	Înlocuiți spațiul de adrese IPv4 prepopulat cu 10.20.0.0/16(separați intrările)

6. Selectați **+ Adăugați o subrețea** . Completați informațiile despre nume și adresă pentru fiecare subrețea. Asigurați-vă că selectați **Adăugați** pentru fiecare subrețea nouă.

Notă: Asigurați-vă că ștergeți subrețeaua implicită - fie înainte, fie după crearea celorlalte subrețele.

Subrețea	**Opţiune**	**Valoare**
Subrețea de servicii partajate	Numele subrețelei	SharedServicesSubnet
	Adresă de pornire	10.20.10.0
	Dimensiune	/24
Subrețea de baze de date	Numele subrețelei	DatabaseSubnet
	Adresă de pornire	10.20.20.0

Subrețea	Opţiune	Valoare
	Dimensiune	/24

Notă: Fiecare rețea virtuală trebuie să aibă cel puțin o subrețea. Rețineți că vor fi întotdeauna rezervate cinci adrese IP, așa că luați în considerare acest aspect în planificarea dvs.

7. Pentru a finaliza crearea CoreServicesVnet și a subrețelelor asociate, selectați **Revizuire + creare** .
8. Verificați dacă configurația a trecut validarea, apoi selectați **Creare** .
9. Așteptați implementarea rețelei virtuale, apoi selectați **Accesați resursa** .
10. Acordați-vă un minut pentru a verifica **spațiul de adrese** și **subrețelele** . Observați celelalte opțiuni din lamina **Setări** .
11. În secțiunea **Automatizare** , selectați **Export șablon** , apoi așteptați generarea șablonului.
12. **Descărcați** șablonul.
13. Navigați pe mașina locală la folderul **Descărcări** și **extrageți toate** fișierele din fișierul zip descărcat.
14. Înainte de a continua, asigurați-vă că aveți fișierul **template.json** . Veți folosi acest șablon pentru a crea ManufacturingVnet în sarcina următoare.

Sarcina 2: Crearea unei rețele virtuale și a subrețelelor folosind un șablon

În această sarcină, creați rețeaua virtuală ManufacturingVnet și subrețelele asociate. Organizația anticipează creșterea birourilor de producție, astfel încât subrețelele sunt dimensionate pentru creșterea preconizată. Pentru această sarcină, utilizați un șablon pentru a crea resursele.

1. Localizați fișierul **template.json** exportat în sarcina anterioară. Ar trebui să fie în folderul **Descărcări** .
2. Editați fișierul folosind editorul ales. Multe editore au o funcție *de modificare a tuturor aparițiilor* . Dacă utilizați Visual Studio Code, asigurați-vă că lucrați într-o **fereastră de încredere** și nu în **modul restricționat** . Consultați diagrama arhitecturii pentru a verifica detaliile.

Efectuați modificări pentru rețeaua virtuală ManufacturingVnet

1. Înlocuiți toate aparițiile lui **CoreServicesVnet** cu ManufacturingVnet.
2. Înlocuiți toate aparițiile lui **10.20.0.0** cu 10.30.0.0.

Efectuați modificări pentru subrețelele ManufacturingVnet

1. Schimbați toate aparițiile lui **SharedServicesSubnet** în SensorSubnet1.
2. Schimbați toate aparițiile lui **10.20.10.0/24** în 10.30.20.0/24.
3. Schimbați toate aparițiile lui **DatabaseSubnet** în SensorSubnet2.
4. Schimbați toate aparițiile lui **10.20.20.0/24** în 10.30.21.0/24.
5. Citiți din nou fișierul și asigurați-vă că totul arată corect. Folosiți diagrama arhitecturii pentru numele resurselor și adresele IP.
6. Asigurați-vă că **salvați** modificările.

Notă: Există fișiere șablon completate în directorul fișierelor de laborator.

Faceți modificări la fișierul de parametri

1. Localizați fișierul **parameters.json** exportat în sarcina anterioară. Ar trebui să fie în folderul **Descărcări** .
2. Editați fișierul folosind editorul ales.
3. Înlocuiți singura apariție a lui **CoreServicesVnet** cu ManufacturingVnet.
4. **Salvați** modificările.

Implementați șablonul personalizat

1. În portal, căutați și selectați Deploy a custom template.
2. Selectați **Creați-vă propriul șablon în editor** , apoi **Încărcați fișierul** .
3. Selectați fișierul **template.json** cu modificările de producție, apoi selectați **Salvare** .
4. Selectați **Editare parametri** , apoi **Încărcare fișier** .
5. Selectați fișierul **parameters.json** cu modificările de producție, apoi selectați **Salvare** .
6. Asigurați-vă că este selectat grupul de resurse **az104-rg4 .**
7. Selectați **Revizuire + creare** , apoi **Creare** .

8. Așteptați implementarea șablonului, apoi confirmați (în portal) că au fost create rețeaua virtuală de producție și subrețelele.

Notă: Dacă trebuie să implementați de mai multe ori, este posibil să constatați că unele resurse au fost finalizate cu succes, iar implementarea eșuează. Puteți elimina manual aceste resurse și încerca din nou.

Sarcina 3: Crearea și configurarea comunicării între un Grup de Securitate a Aplicațiilor și un Grup de Securitate a Rețelei

În această sarcină, creăm un Grup de Securitate a Aplicațiilor și un Grup de Securitate a Rețelei. NSG-ul va avea o regulă de securitate de intrare care permite traficul de la ASG. NSG-ul va avea, de asemenea, o regulă de ieșire care refuză accesul la internet.

Creați Grupul de Securitate a Aplicațiilor (ASG)

1. În portalul Azure, căutați și selectați Application security groups.
2. Faceți clic **pe Creare** și furnizați informațiile de bază.

Setare	**Valoare**
Abonament	*abonamentul dumneavoastră*
Grup de resurse	**az104-rg4**
Nume	asg-web
Regiune	**Estul SUA**

3. Faceți clic **pe Revizuire + creare** , apoi, după validare, faceți clic **pe Creare** .

Notă: În acest moment, ar trebui să asociați ASG-ul cu o mașină (sau mașini) virtuală (virtual). Aceste mașini vor fi afectate de regula NSG de intrare pe care o creați în sarcina următoare.

Creați Grupul de Securitate a Rețelei și asociați-l cu CoreServicesVnet

1. În portalul Azure, căutați și selectați Network security groups.

Notă: Puteți găsi această resursă și utilizând meniul portalului Azure (pictograma din stânga sus). Selectați **Creare resursă** , apoi, în lama **Rețea** , selectați **Grup de securitate rețea** .

1. Selectați **+ Creare** și furnizați informații în fila **Noțiuni de bază** .

Setare	**Valoare**
Abonament	*abonamentul dumneavoastră*
Grup de resurse	**az104-rg4**
Nume	myNSGSecure
Regiune	**Estul SUA**

2. Faceți clic **pe Revizuire + creare** , apoi, după validare, faceți clic **pe Creare** .
3. După ce NSG-ul este implementat, faceți clic **pe Accesați resursa** .
4. Sub **Setări,** faceți clic **pe Subrețele** și apoi **pe Asociare** .

Setare	**Valoare**
Rețea virtuală	**CoreServicesVnet (az104-rg4)**
Subrețea	**Subrețea de servicii partajate**

5. Faceți clic pe **OK** pentru a salva asocierea.

Configurați o regulă de securitate de intrare pentru a permite traficul ASG

1. Continuați să lucrați cu grupul dvs. de securitate (NSG). În zona **Setări** , selectați **Reguli de securitate de intrare** .
2. Revizuiți regulile implicite de intrare. Observați că accesul este permis doar altor rețele virtuale și sisteme de echilibrare a încărcării.
3. Selectați **+ Adăugați** .
4. În lama **Adăugare regulă de securitate de intrare** , utilizați următoarele informații pentru a adăuga o regulă de port de intrare. Această regulă permite traficul ASG. Când ați terminat, selectați **Adăugare** .

Setare	Valoare
Sursă	**Grupul de securitate al aplicațiilor**
Grupuri de securitate ale aplicațiilor sursă	**asg-web**
Intervale de porturi sursă	*
Destinaţie	**Orice**
Serviciu	**Personalizat** (observați celelalte opțiuni ale dvs.)
Intervale de porturi de destinație	**80.443**
Protocol	**TCP**
Acţiune	**Permite**
Prioritate	**100**
Nume	AllowASG

Configurați o regulă NSG de ieșire care refuză accesul la internet

1. După ce ați creat regula NSG de intrare, selectați **Reguli de securitate pentru ieșire** .
2. Observați regula **AllowInternetOutBound** . De asemenea, observați că regula nu poate fi ștearsă și prioritatea este 65001.
3. Selectați **+ Adăugare** și apoi configurați o regulă de ieșire care refuză accesul la internet. Când ați terminat, selectați **Adăugare** .

Setare	Valoare
Sursă	**Orice**

Setare	Valoare
Intervale de porturi sursă	*
Destinaţie	**Etichetă de serviciu**
Etichetă de serviciu de destinație	**Internet**
Serviciu	**Personalizat**
Intervale de porturi de destinație	*
Protocol	**Orice**
Acţiune	**Refuza**
Prioritate	**4096**
Nume	DenyInternetOutbound

Sarcina 4: Configurarea zonelor DNS Azure publice și private

În această sarcină, veți crea și configura zone DNS publice și private.

Configurați o zonă DNS publică

Puteți configura Azure DNS pentru a rezolva numele de gazdă din domeniul public. De exemplu, dacă ați achiziționat numele de domeniu contoso.xyz de la un registrator de nume de domeniu, puteți configura Azure DNS pentru a găzdui contoso.comdomeniul și a rezolva www.contoso.xyz la adresa IP a serverului web sau a aplicației web.

1. În portal, căutați și selectați DNS zones.
2. Selectați **+ Creați** .
3. Configurați fila Noțiuni **de bază** .

Proprietate	Valoare
Abonament	**Selectați-vă abonamentul**

Proprietate	Valoare
Grup de resurse	**az104-rg4**
Nume	contoso.com(dacă este rezervat, modificați numele)
Regiune	**Estul SUA** (consultați pictograma informativă)

4. Selectați **Revizuire + creare** , apoi **Creare** .
5. Așteptați implementarea zonei DNS, apoi selectați **Accesați resursa** .
6. În lama **Prezentare generală,** observați numele celor patru servere de nume DNS Azure atribuite zonei. **Copiați** una dintre adresele serverului de nume. Veți avea nevoie de ea într-un pas viitor.
7. Extindeți lama **Gestionare DNS** și selectați **Seturi de înregistrări** . Faceți clic pe **+Adăugare** .

Proprietate	Valoare
Nume	**www**
Tip	**O**
TTL	**1**
Adresă IP	**10.1.1.4**

Notă: Într-un scenariu real, ar trebui să introduceți adresa IP publică a serverului web.

1. Selectați **Adăugare** și verificați dacă domeniul dvs. are un set de înregistrări A numit **www** .
2. Deschideți o linie de comandă și executați următoarea comandă. Dacă ați modificat numele de domeniu, faceți o ajustare.

nslookup www.contoso.com <name server name>

3. Verificați dacă numele de gazdă www.contoso.com se rezolvă la adresa IP pe care ați furnizat-o. Aceasta confirmă că rezoluția numelui funcționează corect.

Configurați o zonă DNS privată

O zonă DNS privată oferă servicii de rezoluție a numelor în cadrul rețelelor virtuale. O zonă DNS privată este accesibilă numai din rețelele virtuale la care este conectată și nu poate fi accesată de pe internet.

1. În portal, căutați și selectați Private dns zones.
2. Selectați **+ Creați** .
3. În fila **Noțiuni de bază** din secțiunea Creare zonă DNS privată, introduceți informațiile așa cum sunt listate în tabelul de mai jos:

Proprietate	**Valoare**
Abonament	**Selectați-vă abonamentul**
Grup de resurse	**az104-rg4**
Nume	private.contoso.com(ajustați dacă a trebuit să redenumiți)
Regiune	**Estul SUA**

4. Selectați **Revizuire + creare** , apoi **Creare** .
5. Așteptați implementarea zonei DNS, apoi selectați **Accesați resursa** .
6. Observați că în lama **Prezentare generală** nu există înregistrări de server de nume.
7. Extindeți lama **Gestionare DNS** și apoi selectați **Legături de rețea virtuală** . Configurați legătura.

Proprietate	**Valoare**
Numele linkului	manufacturing-link
Rețea virtuală	ManufacturingVnet

8. Selectați **Creare** și așteptați crearea linkului.
9. Din lama **DNS Management,** selectați **+ Recordsets** . Acum ar trebui să adăugați o înregistrare pentru fiecare mașină virtuală care necesită suport pentru rezoluția numelor private.

Proprietate	Valoare
Nume	**senzorvm**
Tip	**O**
TTL	**1**
Adresă IP	**10.1.1.4**

Notă: Într-un scenariu real, ar trebui să introduceți adresa IP pentru o anumită mașină virtuală de producție.

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.

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.

- Distribuiți cele mai bune 10 practici pentru implementarea și configurarea unei rețele virtuale în Azure.
- Cum utilizez comenzile Azure PowerShell și Azure CLI pentru a crea o rețea virtuală cu o adresă IP publică și o subrețea.

- Explicați regulile de intrare și ieșire ale grupului Azure Network Security și modul în care sunt utilizate acestea.
- Care este diferența dintre Azure Network Security Groups și Azure Application Security Groups? Partajați exemple despre când se utilizează fiecare dintre aceste grupuri.
- Oferiți un ghid pas cu pas despre cum să depanați orice probleme de rețea cu care ne confruntăm la implementarea unei rețele pe Azure. De asemenea, împărtășiți procesul de gândire utilizat pentru fiecare pas al depanării.

Învață mai multe cu instruire în ritm propriu

- Introducere în rețelele virtuale Azure . Proiectarea și implementarea infrastructurii de bază a rețelelor Azure, cum ar fi rețele virtuale, IP-uri publice și private, DNS, peering de rețele virtuale, rutare și Azure Virtual NAT.
- Proiectați o schemă de adresare IP . Identificați capacitățile de adresare IP private și publice ale Azure și ale rețelelor virtuale locale.
- Securizați și izolați accesul la resursele Azure utilizând grupuri de securitate de rețea și puncte finale de serviciu . Grupurile de securitate de rețea și punctele finale de serviciu vă ajută să vă securizați mașinile virtuale și serviciile Azure împotriva accesului neautorizat la rețea.
- Găzduiți-vă domeniul pe Azure DNS . Creați o zonă DNS pentru numele domeniului. Creați înregistrări DNS pentru a mapa domeniul la o adresă IP. Testați dacă numele domeniului se rezolvă la serverul web.

Concluzii cheie

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

- O rețea virtuală este o reprezentare a propriei rețele în cloud.
- La proiectarea rețelelor virtuale, este o practică bună să se evite suprapunerea intervalelor de adrese IP. Acest lucru va reduce problemele și va simplifica depanarea.
- O subrețea este un interval de adrese IP din rețeaua virtuală. Puteți împărți o rețea virtuală în mai multe subrețele pentru organizare și securitate.
- Un grup de securitate de rețea conține reguli de securitate care permit sau resping traficul de rețea. Există reguli implicite de intrare și ieșire pe care le puteți personaliza în funcție de nevoile dvs.

- Grupurile de securitate ale aplicațiilor sunt utilizate pentru a proteja grupuri de servere cu o funcție comună, cum ar fi serverele web sau serverele de baze de date.
- Azure DNS este un serviciu de găzduire pentru domenii DNS care oferă rezoluție de nume. Puteți configura Azure DNS pentru a rezolva numele de gazdă din domeniul public. De asemenea, puteți utiliza zone DNS private pentru a atribui nume DNS mașinilor virtuale (VM) din rețelele virtuale Azure.