Implementarea conectivității inter-site-uri

Introducere în laborator

În acest laborator veți explora comunicarea între rețele virtuale. Veți implementa peering-ul de rețea virtuală și veți testa conexiunile. De asemenea, veți crea o rută personalizată.

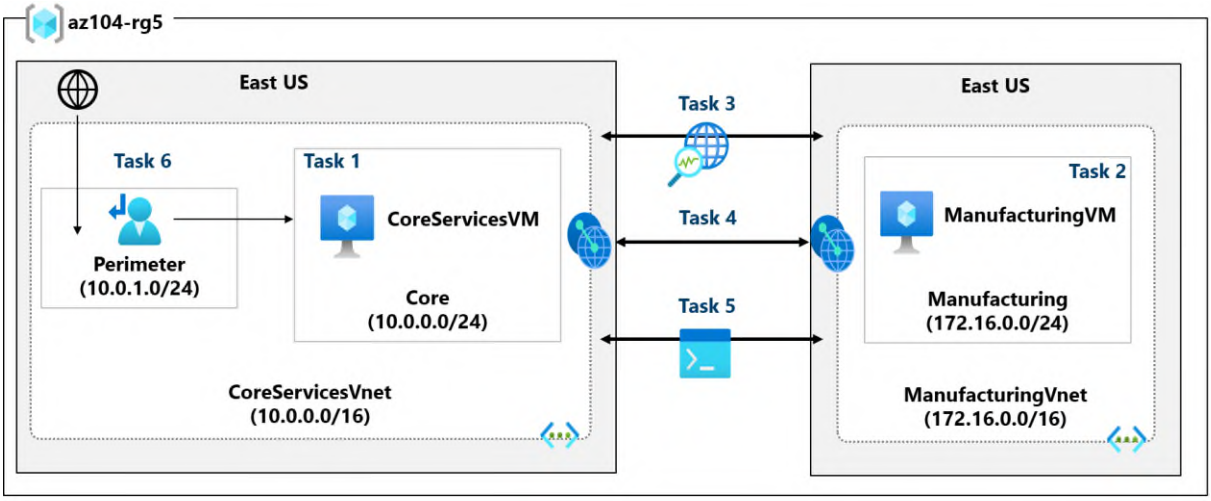
Acest laborator necesită un abonament Azure. Tipul de abonament poate afecta disponibilitatea funcțiilor din acest laborator. Puteți schimba regiunea, dar pașii sunt scrișI folosind **East US** .

Timp estimat: 50 de minute

Scenariu de laborator

Organizația dvs. segmentează aplicațiile și serviciile IT de bază (cum ar fi DNS și serviciile de securitate) de alte părți ale afacerii, inclusiv departamentul de producție. Cu toate acestea, în anumite scenarii, aplicațiile și serviciile din zona de bază trebuie să comunice cu aplicațiile și serviciile din zona de producție. În acest laborator, configurați conectivitatea între zonele segmentate. Acesta este un scenariu comun pentru separarea producției de dezvoltare sau separarea unei filiale de alta.

Diagramă de arhitectură



Competențe profesionale

- Sarcina 1: Crearea unei mașini virtuale într-o rețea virtuală.
- Sarcina 2: Creați o mașină virtuală într-o altă rețea virtuală.
- Sarcina 3: Utilizați Network Watcher pentru a testa conexiunea dintre mașinile virtuale.

- Sarcina 4: Configurați peering-urile de rețele virtuale între diferite rețele virtuale.
- Sarcina 5: Utilizați Azure PowerShell pentru a testa conexiunea dintre mașinile virtuale.
- Sarcina 6: Creați un traseu personalizat.

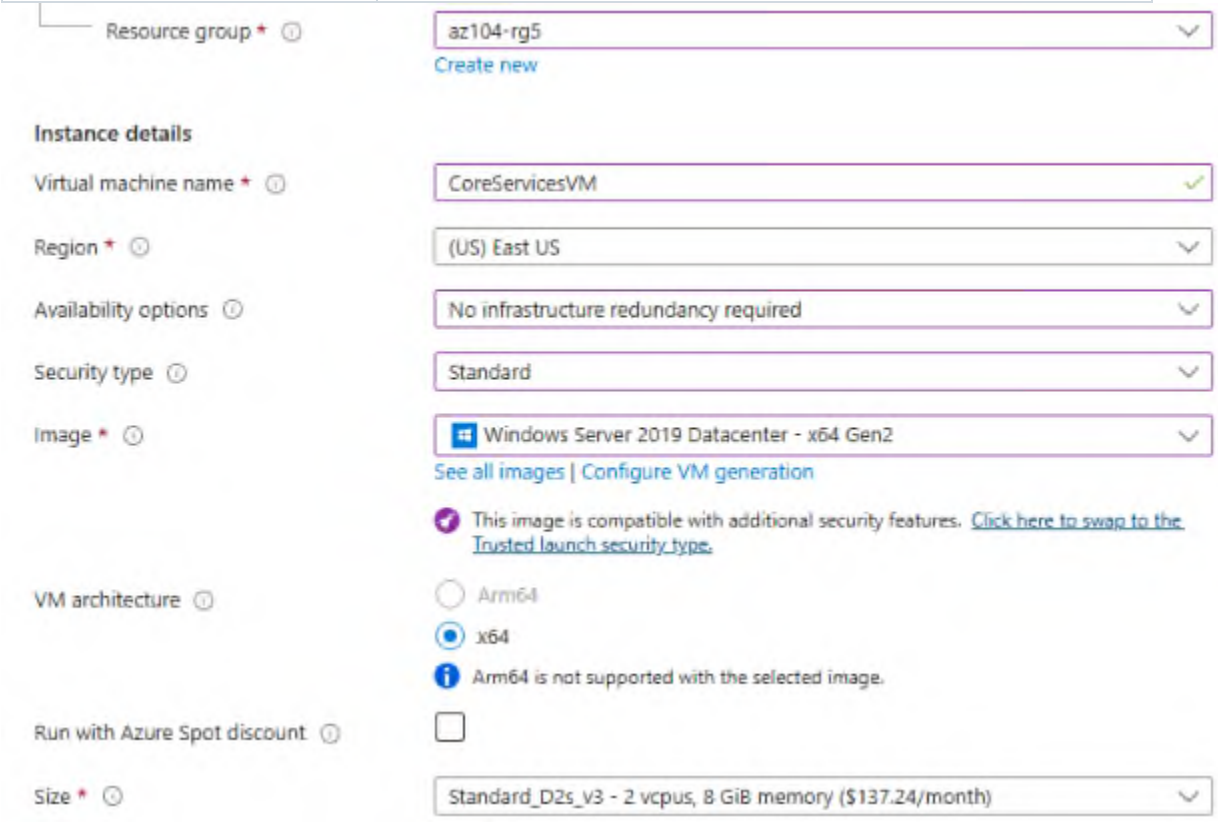
Sarcina 1: Crearea unei mașini virtuale și a unei rețele virtuale pentru servicii principale

În această sarcină, creați o rețea virtuală de servicii principale cu o mașină virtuală.

1. Conectați-vă la **portalul Azure** - https://portal.azure.com.
2. Căutați și selectați Virtual Machines.
3. Din pagina mașini virtuale, selectați **Creare** , apoi selectați **Mașină virtuală** .
4. În fila Noțiuni de bază, utilizați următoarele informații pentru a completa formularul, apoi selectați **Următorul: Discuri >** . Pentru orice setare nespecificată, păstrați valoarea implicită.

Setare	**Valoare**
Abonament	*abonamentul dumneavoastră*
Grup de resurse	az104-rg5(Dacă este necesar, **Creați nou** .)
Numele mașinii virtuale	CoreServicesVM
Regiune	**(SUA) Estul SUA**
Opțiuni de disponibilitate	Nu este necesară redundanța infrastructurii
Tip de securitate	**Standard**
Imagine (Vezi toate imaginile)	**Windows Server 2025 Datacenter - x64 Gen2** (observați celelalte opțiuni)

Setare	Valoare
Dimensiune	**Standard_DS2_v3**
Nume de utilizator	localadmin
Parolă	**Furnizați o parolă complexă**
Porturi publice de intrare	**Nici unul**

5. 

6. În fila **Discuri** , alegeți setările implicite și apoi selectați **Următorul: Rețea >** .
7. Pe fila **Rețea** , pentru Rețea virtuală, selectați **Creare nouă** .
8. Folosiți următoarele informații pentru a configura rețeaua virtuală, apoi selectați **OK** . Dacă este necesar, eliminați sau înlocuiți informațiile existente.

Setare	Valoare
Nume	CoreServicesVnet(Creați sau editați)
Interval de adrese	10.0.0.0/16
Nume subrețea	Core
Interval de adrese de subrețea	10.0.0.0/24

9. Selectați fila **Monitorizare** . Pentru Diagnosticare pornire, selectați **Dezactivare** .
10. Selectați **Revizuire + creare** , apoi selectați **Creare** .
11. Nu trebuie să așteptați crearea resurselor. Continuați cu sarcina următoare.

Notă: Ați observat că în această sarcină ați creat rețeaua virtuală odată cu crearea mașinii virtuale? De asemenea, puteți crea infrastructura rețelei virtuale, apoi adăuga mașinile virtuale.

Sarcina 2: Creați o mașină virtuală într-o altă rețea virtuală

În această sarcină, creați o rețea virtuală de servicii de producție cu o mașină virtuală.

1. Din portalul Azure, căutați și navigați la **Mașini virtuale** .
2. Din pagina mașini virtuale, selectați **Creare** , apoi selectați **Mașină virtuală** .
3. În fila Noțiuni de bază, utilizați următoarele informații pentru a completa formularul, apoi selectați **Următorul: Discuri >** . Pentru orice setare nespecificată, păstrați valoarea implicită.

Setare	Valoare
Abonament	*abonamentul dumneavoastră*
Grup de resurse	az104-rg5
Numele mașinii virtuale	ManufacturingVM
Regiune	**(SUA) Estul SUA**

Setare	Valoare
Tip de securitate	**Standard**
Opțiuni de disponibilitate	Nu este necesară redundanța infrastructurii
Imagine (Vezi toate imaginile)	**Windows Server 2025 Datacenter - x64 Gen2**
Dimensiune	**Standard_DS2_v3**
Nume de utilizator	localadmin
Parolă	**Furnizați o parolă complexă**
Porturi publice de intrare	**Nici unul**

4. În fila **Discuri** , alegeți setările implicite și apoi selectați **Următorul: Rețea >** .
5. Pe fila Rețea, pentru Rețea virtuală, selectați **Creare nouă** .
6. Folosiți următoarele informații pentru a configura rețeaua virtuală, apoi selectați **OK** . Dacă este necesar, eliminați sau înlocuiți intervalul de adrese existent.

Setare	Valoare
Nume	ManufacturingVnet
Interval de adrese	172.16.0.0/16
Nume subrețea	Manufacturing
Interval de adrese de subrețea	172.16.0.0/24

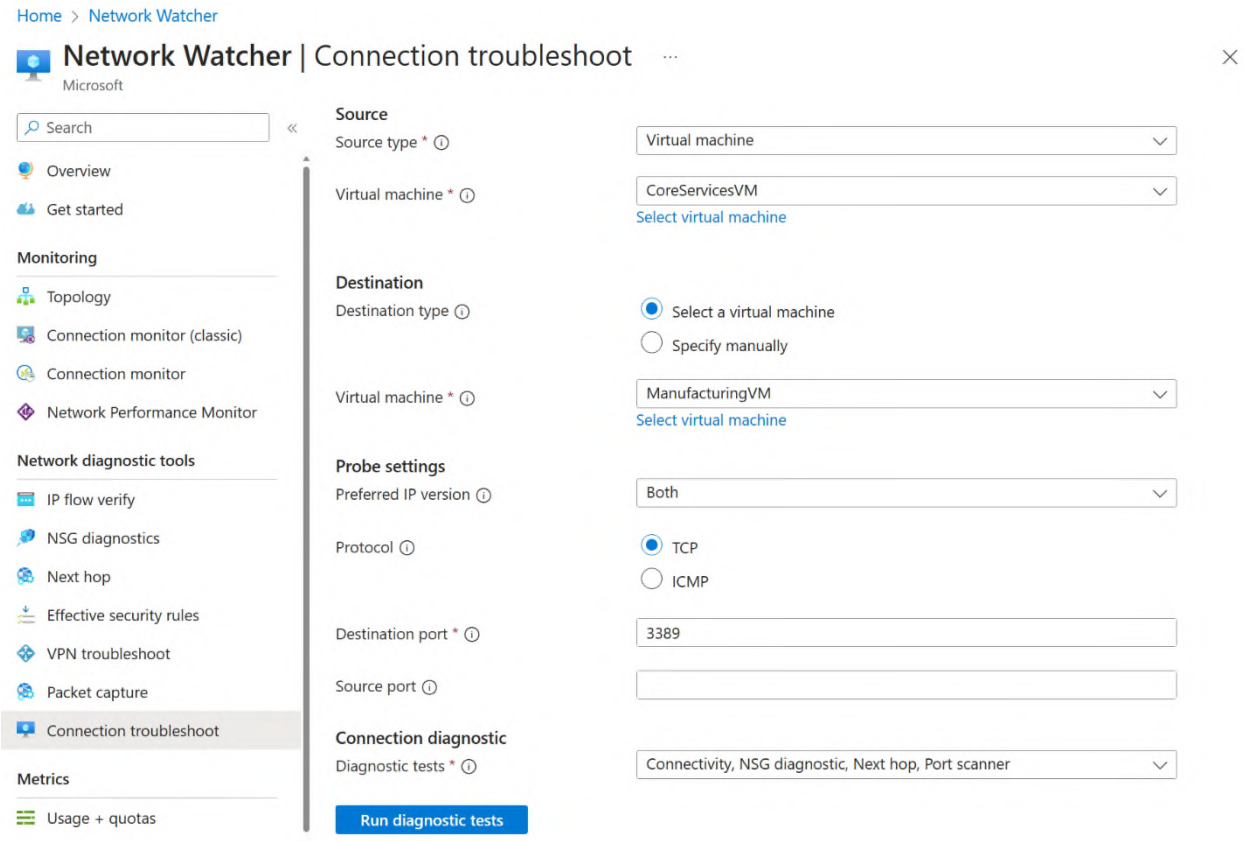
7. Selectați fila **Monitorizare** . Pentru Diagnosticare pornire, selectați **Dezactivare** .
8. Selectați **Revizuire + creare** , apoi selectați **Creare** .

Sarcina 3: Utilizarea Network Watcher pentru a testa conexiunea dintre mașinile virtuale

În această sarcină, verificați dacă resursele din rețelele virtuale peer-up pot comunica între ele. Network Watcher va fi utilizat pentru a testa conexiunea. Înainte de a continua, asigurați-vă că ambele mașini virtuale au fost implementate și rulează.

1. Din portalul Azure, căutați și selectați Network Watcher.
2. Din Network Watcher, în meniul Instrumente de diagnosticare a rețelei, selectați **Depanare conexiune** .
3. Folosiți următoarele informații pentru a completa câmpurile de pe pagina **Depanare conexiune** .

Domeniu	**Valoare**
Tipul sursei	**Mașină virtuală**
Mașină virtuală	**CoreServicesVM**
Tipul destinației	**Selectați o mașină virtuală**
Mașină virtuală	**ManufacturingVM**
Versiune IP preferată	**Ambele**
Protocol	**TCP**
Portul de destinație	3389
Port sursă	*Necompletat*
Teste de diagnostic	*Valori implicite*

4. 

5. Selectați **Executare teste de diagnosticare** .

Notă : Este posibil să dureze câteva minute până când rezultatele sunt returnate. Selecțiile de pe ecran vor fi inactive în timp ce rezultatele sunt colectate. Observați că **testul de conectivitate** arată **Inaccesibil** . Acest lucru are sens deoarece mașinile virtuale se află în rețele virtuale diferite.

Sarcina 4: Configurarea peering-urilor de rețea virtuală între rețele virtuale

În această sarcină, creați o rețea virtuală de peering pentru a permite comunicațiile între resursele din rețelele virtuale.

1. În portalul Azure, selectați CoreServicesVnetrețeaua virtuală.
2. În CoreServicesVnet, sub **Setări** , selectați **Peerings** .
3. Pe CoreServicesVnet, sub Peerings (Conexiuni de asociere), selectați **+ Add (Adăugare)** . Dacă nu este specificat, se va alege valoarea implicită.

Parametru	Valoare
Numele legăturii de peering	ManufacturingVnet-to-CoreServicesVnet
Rețea virtuală	**ManufacturingVnet (az104-rg5)**
Permiteți accesul la „ManufacturingVnet” către „CoreServicesVnet”	selectat (implicit)
Permiteți ca „CoreServicesVnet” să primească trafic redirecționat de la „ManufacturingVnet”	selectat
Numele legăturii de peering	CoreServicesVnet-to-ManufacturingVnet
Permiteți „ManufacturingVnet” să acceseze „CoreServicesVnet”	selectat (implicit)
Permiteți ca „ManufacturingVnet” să primească trafic redirecționat de la „CoreServicesVnet”	selectat

4. Faceți clic **pe Adăugare** .
5. În CoreServicesVnet, sub Peerings (Peeringuri), verificați dacă este listat peeringul **CoreServicesVnet-to-ManufacturingVnet** . Reîmprospătați pagina pentru a vă asigura că **starea Peering** este **Connected (Conectat)** .
6. Comutați la **ManufacturingVnet** și verificați dacă este listată conexiunea **ManufacturingVnet-to-CoreServicesVnet** peering. Asigurați-vă că **starea Peering** este **Conectat** . Poate fi necesar să **reîmprospătați** pagina.

Sarcina 5: Utilizarea Azure PowerShell pentru a testa conexiunea dintre mașinile virtuale

În această sarcină, retestează conexiunea dintre mașinile virtuale din rețele virtuale diferite.

Verificați adresa IP privată a CoreServicesVM

1. Din portalul Azure, căutați și selectați CoreServicesVMmașina virtuală.
2. În lama **Prezentare generală** , în secțiunea **Rețea** , înregistrați **adresa IP privată** a mașinii. Aveți nevoie de aceste informații pentru a testa conexiunea.

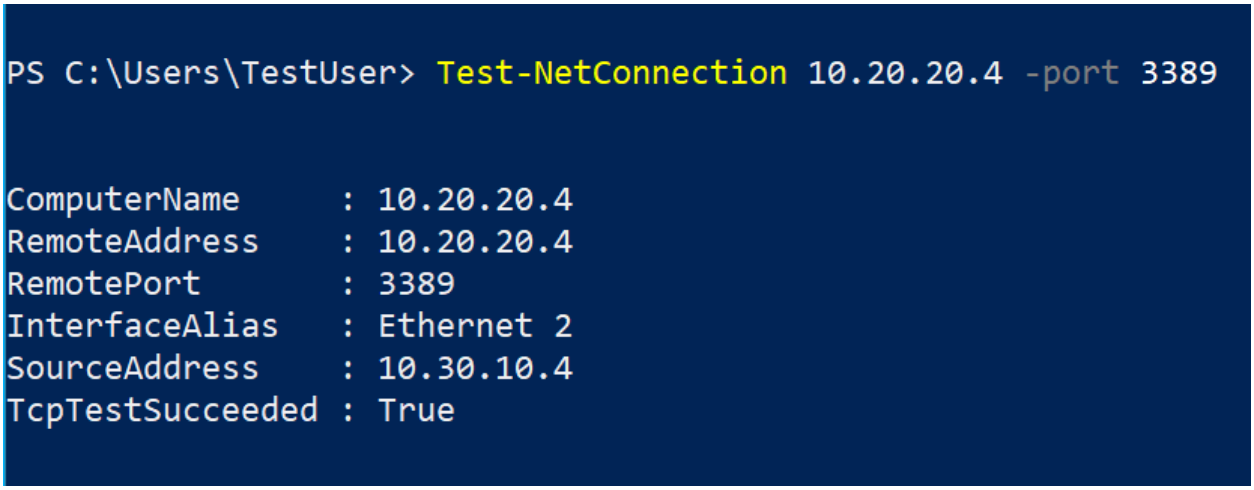
Testați conexiunea la CoreServicesVM din ManufacturingVM .

Știați că...? Există multe modalități de a verifica conexiunile. În această sarcină, utilizați **comanda Executare** . De asemenea, puteți continua să utilizați Network Watcher. Sau puteți utiliza o conexiune Desktop la distanță pentru a accesa mașina virtuală. După conectare, utilizați **test-connection** . Pe măsură ce aveți timp, încercați RDP.

1. Treceți la ManufacturingVMmașina virtuală.
2. În lama **Operațiuni** , selectați lama **comenzii Executare** .
3. Selectați **RunPowerShellScript** și executați comanda **Test-NetConnection** . Asigurați-vă că utilizați adresa IP privată a **CoreServicesVM** .

Test-NetConnection <CoreServicesVM private IP address> -port 3389

4. Este posibil să dureze câteva minute până când scriptul expiră. Partea de sus a paginii afișează un mesaj informativ *Execuție script în curs...*
5. Conexiunea de testare ar trebui să reușească deoarece a fost configurată peering-ul. Numele computerului și adresa la distanță din această imagine pot fi diferite.



Sarcina 6: Creați un traseu personalizat

În această sarcină, doriți să controlați traficul de rețea între subrețeaua perimetrală și subrețeaua internă a serviciilor principale. Un dispozitiv de rețea virtuală va fi instalat în subrețeaua perimetrală și tot traficul ar trebui să fie direcționat către aceasta.

1. Căutați selectați CoreServicesVnet.
2. Selectați **Subrețele** și apoi **+ Subrețea** . Asigurați-vă că selectați **Adăugare** pentru a salva modificările.

Setare	**Valoare**
Nume	perimeter
Adresă de pornire	10.0.1.0/24

3. În portalul Azure, căutați și selectați Route tables, selectați **+ Creare** .
4. Introduceți următoarele detalii, selectați **Revizuire + creare** , apoi selectați **Creare** .

Setare	**Valoare**
Abonament	abonamentul dumneavoastră
Grup de resurse	az104-rg5
Regiune	**Estul SUA**
Nume	rt-CoreServices
Propagarea rutelor gateway	**Nu**

5. După ce tabela de rutare este implementată, căutați și selectați **Tabele de rutare** .
6. Selectați resursa (nu caseta de selectare) **rt-CoreServices**
7. Extindeți **Setări,** apoi selectați **Rute** și apoi **+ Adăugare** . Creați o rută de la un viitor dispozitiv virtual de rețea (NVA) la rețeaua virtuală CoreServices.

Setare	**Valoare**
Numele rutei	PerimetertoCore
Tipul destinației	**Adrese IP**

Setare	Valoare
Adresele IP de destinație	10.0.0.0/16(rețea virtuală de servicii de bază)
Tipul următorului salt	**Aparat virtual** (observați celelalte opțiuni)
Adresa următoarei etape	10.0.1.7(viitor NVA)

8. Selectați **Adăugare** . Ultimul lucru de făcut este să asociați ruta cu subrețeaua.
9. Selectați **Subrețele** și apoi **+ Asociare** . Finalizați configurarea.

Setare	Valoare
Rețea virtuală	**CoreServicesVnet (az104-rg5)**
Subrețea	**Nucleu**

Notă : Ați creat o rută definită de utilizator pentru a direcționa traficul din DMZ către noul NVA.

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.

- Cum pot utiliza comenzile Azure PowerShell sau Azure CLI pentru a adăuga o rețea virtuală peering între vnet1 și vnet2?
- Creați un tabel care să evidențieze diverse instrumente de monitorizare Azure și de la terți acceptate pe Azure. Evidențiați când să utilizați fiecare instrument.
- Când aș crea o rută de rețea personalizată în Azure?

Învață mai multe cu instruire în ritm propriu

- Distribuiți-vă serviciile în rețele virtuale Azure și integrați-le utilizând peering-ul de rețele virtuale . Utilizați peering-ul de rețele virtuale pentru a permite comunicarea între rețele virtuale într-un mod sigur și cu complexitate minimă.
- Gestionați și controlați fluxul de trafic în implementarea Azure cu rute . Aflați cum să controlați traficul rețelei virtuale Azure prin implementarea de rute personalizate.

Concluzii cheie

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

- În mod implicit, resursele din rețele virtuale diferite nu pot comunica.
- Peering-ul de rețele virtuale vă permite să conectați fără probleme două sau mai multe rețele virtuale în Azure.
- Rețelele virtuale peered apar ca una singură în scopuri de conectivitate.
- Traficul dintre mașinile virtuale din rețelele virtuale peerizate utilizează infrastructura backbone Microsoft.
- Rutele definite de sistem sunt create automat pentru fiecare subrețea dintr-o rețea virtuală. Rutele definite de utilizator suprascriu sau se adaugă la rutele implicite ale sistemului.
- Azure Network Watcher oferă o suită de instrumente pentru monitorizarea, diagnosticarea și vizualizarea indicatorilor și jurnalelor pentru resursele Azure IaaS.