Лекція 2. Концепція забезпечення високої надійності застосунків Microsoft Azure.

Тема 1. Регіони та зони доступу. Пари регіонів.

Тема 2. Віртуальні машини - основні налаштування.

Тема 3. Azure Cloud Shell – інструкції для створення віртуальної машини.

Тема 4. Віртуальні машини - «домени збою» і «домени оновлення».

Тема 5. Система доменних імен - Azure DNS.

Azure Регіони - 58 регіонів в 140 країнах

Azure global infrastructure experience (microsoft.com)

Постачальник хмарних служб та сервісів мають потужності в різних регіонах для забезпечення вимог щодо місця розташування даних користувачів. Чим ближче розташовані до користувачів хмарні сервіси/дані тим краще. Наприклад, користувачі «хмарних сервісів» з Канада, мають вимоги щоб їх дані знаходились в Канаді.
Azure включає 58 регіонів в 140 країнах.
Регіон – це група «доступних зон» (Availability Zone AZ) в яких знаходяться центри обробки даних.
Azure Availability Zone відноситься до поняття, яке використовується в хмарних сервісах Microsoft Azure для означення ізольованих локацій всередині регіону Azure. Кожна зона складається з одного або кількох дата-центрів, які оснащені незалежною електрикою, охолодженням та мережевою інфраструктурою. Це дозволяє виключити спільні точки відмови та забезпечує високий рівень доступності та надійності сервісів, розміщених в хмарі. Availability Zone застосовуються для реалізації стратегій відновлення після збоїв та забезпечення високої доступності критичних додатків.
Категорії регіонів

1. Рекомендовані регіони –регіони, в яких доступні майже всі сервіси Azure (підтримують 3 доступні зони)
2. Альтернативні – регіони з функціями «аварійного відновлення» (не підтримують різні доступні зони).

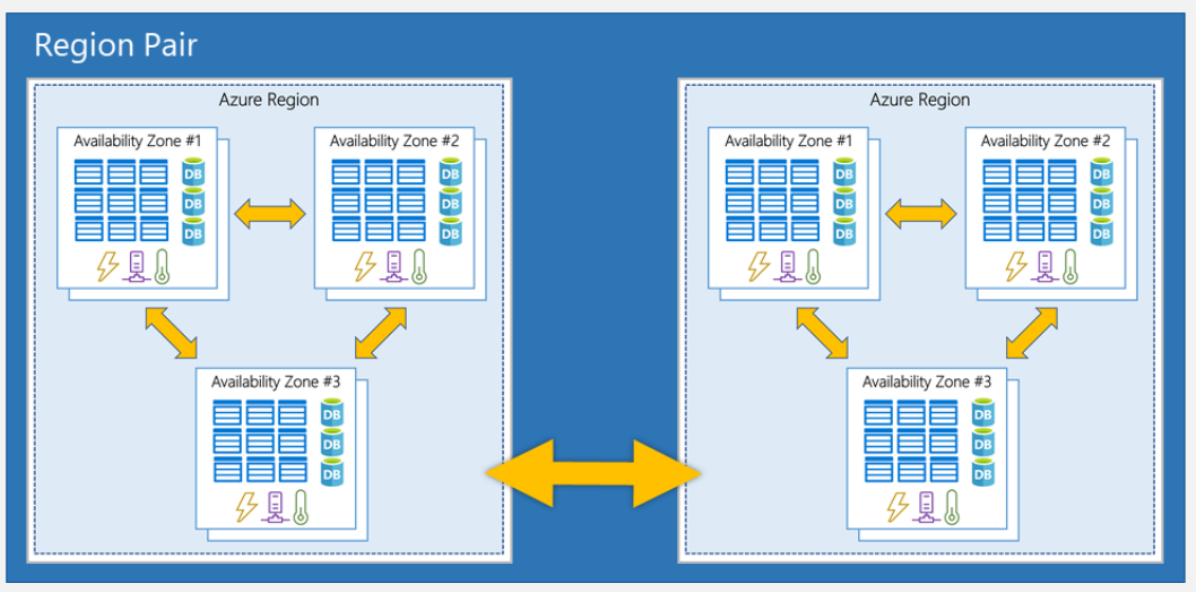
Кожен регіон «дублюється» (дзеркальна копія) іншим регіоном, який знаходиться на відстані 1287.48 км (800 miles). Таким чином, у випадку необхідності аварійного відновленні – використовуються регіон – «дублер».

Region Pairs

- At least 300 miles of separation between region pairs.
- Automatic replication for some services.
- Prioritized region recovery in the event of outage.
- Updates are rollout sequentially to minimize downtime.

Web Link: https://aka.ms/PairedRegions

Region	Region
North Central US	South Central US
East US	West US
West US 2	West Central US
US East 2	Central US
Canada Central	Canada East
North Europe	West Europe
UK West	UK South
Germany Central	Germany Northeast
South East Asia	East Asia
East China	North China
Japan East	Japan West
Australia Southeast	Australia East
India South	India Central
Brazil South (Primary)	South Central US



Azure Sovereign Regions (US Government services)

Meets the security and compliance needs of US federal agencies, state and local governments, and their solution providers.

Azure Government:

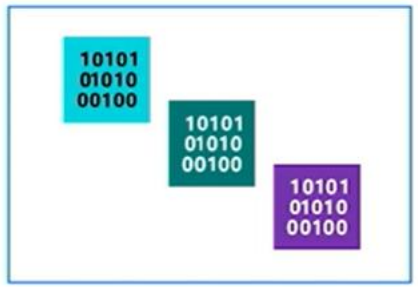
- Separate instance of Azure
- Physically isolated from non-US government deployments
- Accessible only to screened, authorized personnel

Azure Sovereign region - для US Government services, також відомий як Azure Government, - це окремий регіон Microsoft Azure, спеціально розроблений для задоволення вимог урядових організацій Сполучених Штатів. Цей регіон хмарних сервісів має покращені заходи безпеки та відповідність федеральним стандартам, серед яких:

- Фізична та логічна ізоляція даних: Azure Government забезпечує окремі центри даних, що не є доступними для загального хмарного сервісу Azure.
- Операції у Azure Government відповідають таким стандартам як FedRAMP High, CJIS, IRS 1075, DoD L4 (та частково L5) та інші. Це забезпечує високий рівень захисту даних, який вимагають урядові організації.
- Доступ до Azure Government можуть мати тільки американські громадяни, які пройшли перевірку особи, та експлуатація даного хмарного сервісу знаходиться повністю на території США.

Azure Sovereign Regions (Azure China)

Microsoft is China's first foreign public cloud service provider, in compliance with government regulations.

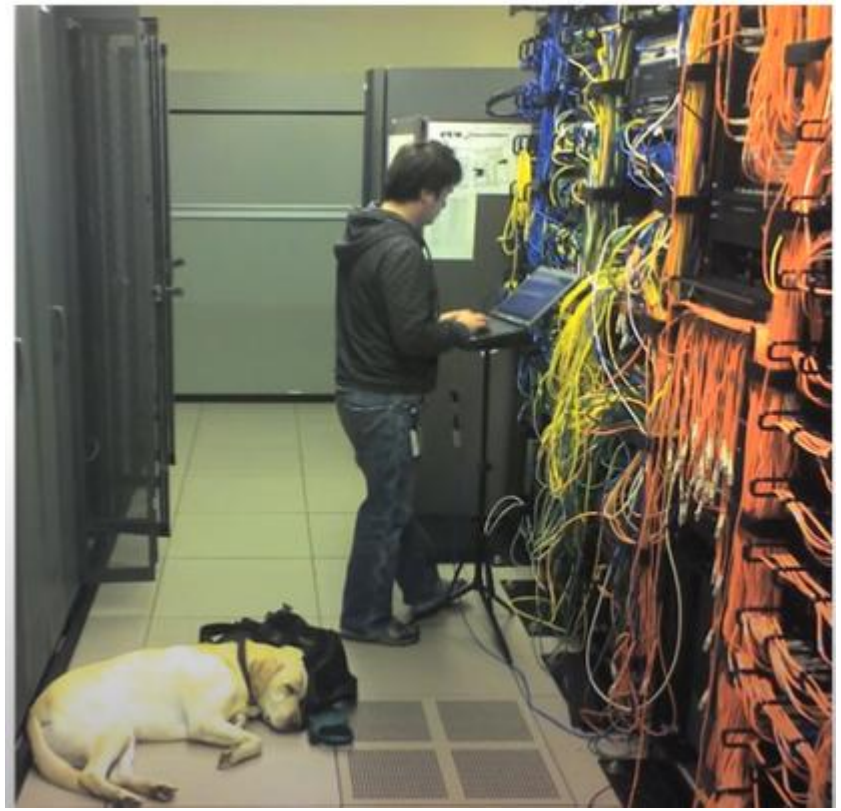


Azure China features:

- Physically separated instance of Azure cloud services operated by 21Vianet
- All data stays within China to ensure compliance

Azure China Region - це спеціальний регіон Microsoft Azure, який відповідає специфічним вимогам Китайських законів про кібербезпеку та захист даних. Цей регіон керується місцевим оператором 21Vianet, який є єдиним повноцінним постачальником сервісів від Microsoft Azure в Китаї. Це забезпечує, що дані зберігаються на території Китаю, що є вимогою місцевого законодавства.

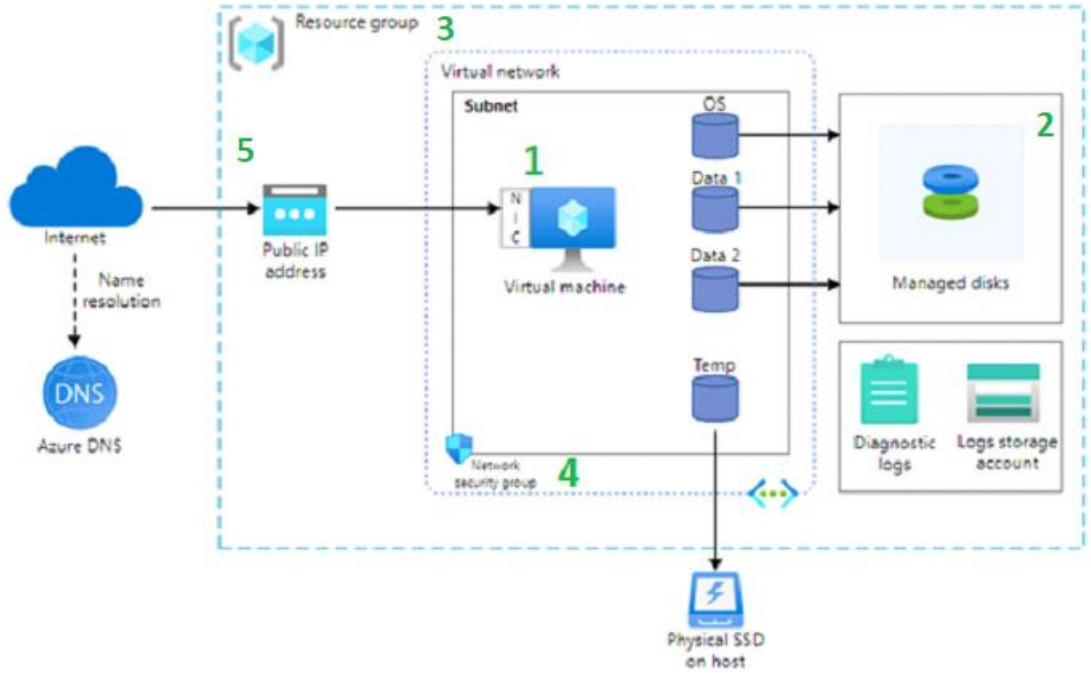
Служби Azure – базові, основні, стратегічні



«Доступна зона» - місце розташування будівлі де знаходяться центри обробки даних – 100 серверів та комп. В рекомендовану регіоні доступні до 3-х «зон».

- *Базові служби:* доступні у всіх рекомендованих та альтернативних регіонах, коли регіон стане загальнодоступним або протягом 90 днів після того, як нова базова служба стане загальнодоступною. Приклад, Azure Backup, Azure Cosmos DB, Azure DNS, Azure ExpressRoute, бази даних Azure, ВМ.
- *Основні служби:* доступні у всіх регіонах, що рекомендуються, протягом 90 днів після загальної доступності регіону. На основі попиту, деякі основі служби можуть бути розгорнуті в альтернативних регіонах. Приклад, Служба керування Azure API, Пакетна служба Azure, База даних Azure для MySQL, База даних Azure для PostgreSQL, Брандмауер Azure, Реєстр контейнерів Azure, Примірники контейнерів Azure, т.п.
- *Стратегічні служби*: Доступність на основі попиту в різних регіонах, приклад База даних Azure для MariaDB, Машинне навчання Azure, Рішення Azure VMware, Azure Analysis Services

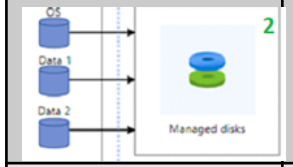
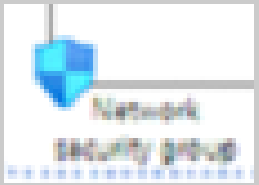
Віртуальні машини Azure



Віртуальна машина (1), віртуальні жорсткі диски (2), Віртуальна мережа (3), групи безпеки мережі (4), загальнодоступна IP-адреса (5)

- Віртуальні машини (ВМ) Azure - це масштабовані хмарні обчислювальні ресурси на вимогу. Вони аналогічні ВМ, розміщеним у Windows Hyper-V. У них є процесор, пам'ять, сховище та мережеві ресурси. ВМ - призначені для полегшення процесу міграції існуючих Windows Server додатків в "хмару" структуру. ***На відміну від перенесення сервісів і окремих компонентів, ВМ дозволяє перенести додаток цілком (lift and shift)***, і бере на себе відповідальність за надання сервісів автоматичного управління, оновлення та відмовостійкості.

Створення віртуальної машини Azure

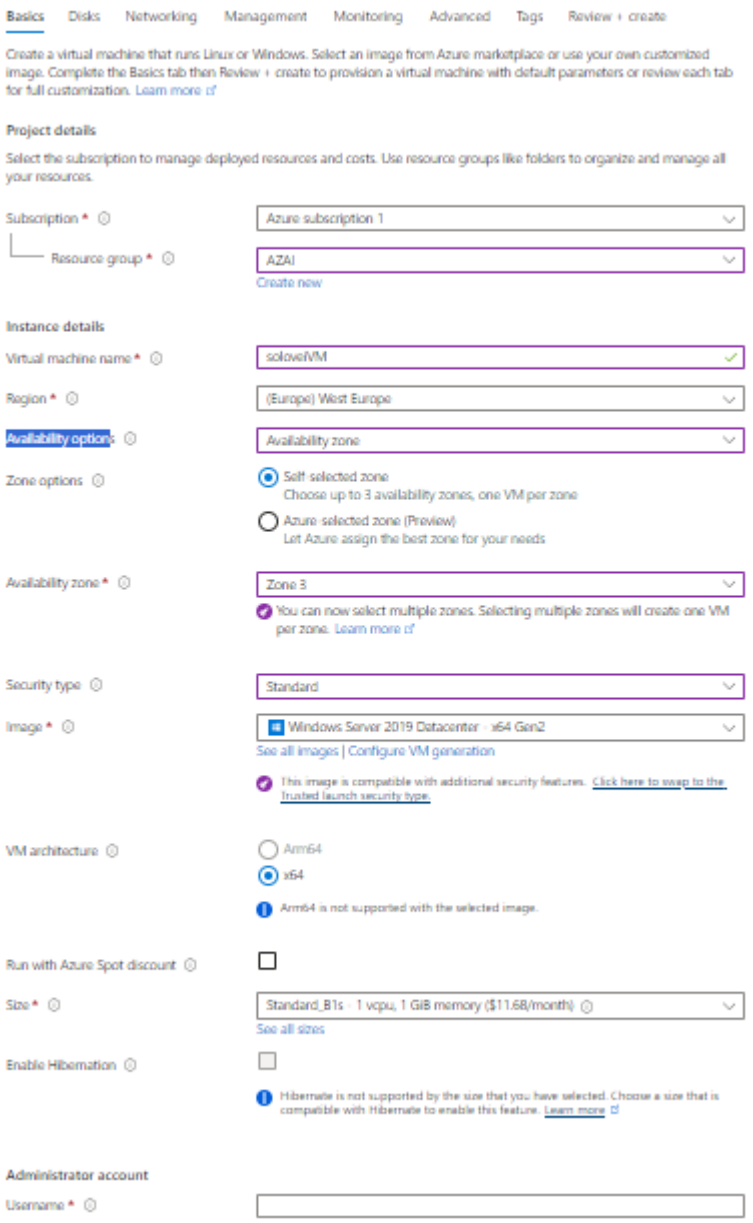
	При створенні ВМ необхідно визначити її регіон; розмір; архітектуру; базову операційну систему (Windows, Linux та інші); вибрати варіанти сховища.
	Вибрати варіант сховища, для зберігання операційної системи, додатків та даних.
	Налаштувати віртуальну мережу для забезпечення ізоляції.
	Налаштувати групи безпеки - основний інструмент, призначений для застосування та контролю правил мережевого трафіку на рівні мережі. Групи безпеки мережі — це додатковий рівень безпеки, який виступає як програмний брандмауер, який фільтрує вхідний та вихідний трафік у віртуальній мережі.

Розміри ВМ

- Розміри віртуальних машин згруповані за категоріями, починаючи із серії B для найпростішого тестування та закінчуючи серією H для складних обчислювальних завдань.
- Розмір віртуальної машини слід вибирати відповідно до необхідного робочого навантаження.
- Розмір віртуальної машини можна змінити після створення, але для цього необхідно спочатку завершити її роботу, тому краще відразу вибрати правильний розмір, якщо це можливо.

Задачі	Можливий розмір
Загальне використання обчислень або веб-сайтів: тестування та розробка, невеликі та середні бази даних або веб-сервери з низьким та середнім трафіком.	B, Dsv3, Dv3, DSv2, Dv2
Складні обчислювальні завдання: веб-сервери із середнім трафіком, мережні пристрої, пакетні процеси та сервери програм.	Fsv2 Fs, F
Використання великого обсягу пам'яті. Сервери реляційних баз даних, кеші середнього та великого обсягу, а також аналітика, що виконується в пам'яті.	Esv3, Ev3, M, GS, G, DSv2, Dv2
Зберігання та обробка даних: бази даних SQL та NoSQL, яким потрібна висока пропускна спроможність диска та операції вводу-виводу.	Ls
Ресурсоємне малювання зображень або редагування відео, а також навчання моделей та формування висновків за допомогою глибокого навчання	NV, NC, NCv2, NCv3 та ND
Високопродуктивні обчислення (HPC): якщо вам потрібні найшвидші та найпотужніші віртуальні машини ЦП з додатковими мережевими інтерфейсами з високою пропускною здатністю	H

ВМ – ***основні*** налаштування



Група, ім'я, Регіон

- Availability options – опція для управління рівнем доступності ВМ.

1) Availability zone – надається фізично відокремлена зона в межах регіону. Доступні 3 зони, кожна зона має окреме джерело живлення, мережу та охолодження.
2) VM Scale sets – дозволяє створювати групи ВМ із збалансованим навантаженням.

3) Availability sets – дозволяє групувати ВМ для забезпечення збалансованого навантаження.

Рекомендовано створювати завжди 2 ВМ

- Security type – тип безпеки, за замовчення визначено Trusted Launch VM – забезпечую захист від атак. Основою TL є Secure Boot – для всіх компонентів ВМ запитує сертифікат видавця, у разі не отримання – зупиняє інсталяцію ВМ.

2) Confidential VM - забезпечує додатковий захист на рівні обладнання.

- Image – дозволяє вибрати операційну систему
- Size - обчислювальна потужність, пам’ять і ємність зберігання.
- Administrator account – username/user password для ВМ.
- Public inbound ports – визначає порти ВМ, які доступні з Інтернету.

ВМ – ***основні*** налаштування

OS disk size - розмір диску в ГБ
OS disk type - Доступні варіанти включають жорсткі диски (HDD) або сучасні твердотільні накопичувачі (SSD).
За умовчанням для віртуальної машини Windows створюються два віртуальні жорсткі диски:
Диск операційної системи. Це основний диск або C, максимальна ємність якого становить 2048 ГБ.
Тимчасовий диск. Він призначений для тимчасового зберігання ОС чи додатків. Він має букву D: за замовчуванням, а його розмір залежить від розміру віртуальної машини, тому це ідеальне розташування для файлу підкачки Windows.

	Ultra Disk	Premium SSD v2	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	SSD	HDD
Рекомендовано для умов:	інтенсивні навантаження вводу виводу. Важкі транзакції.	низької затримки та високої пропускної здатності	Навантаження з високою продуктивністю	Веб - сервери	підтримка резервного копіювання
Max disk size	65,536 GiB	65,536 GiB	32,767 GiB	32,767 GiB	32,767 GiB

Key management – визначити набір ключів шифрування диска. За замовченням - Platform-managed keys – ключі шифрування керовані платформою.
Customer-managed keys - шифрування диску на основі власних ключів.

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

The configuration of this virtual machine and its attached disk(s) does not allow for the disk(s) to utilize their full throughput performance. The current virtual machine size supports 23 MBps. The total for disk(s) attached to virtual machine 'soloveiVM' is 100 MBps. You can change the virtual machine size to support additional disk(s) throughput. Learn more

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ☐

Encryption at host is not registered for the selected subscription.
Learn more about enabling this feature

OS disk

OS disk size: Image default (127 GiB)

OS disk type *: Standard SSD (locally-redundant storage)

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Delete with VM ☑

Key management: Platform-managed key

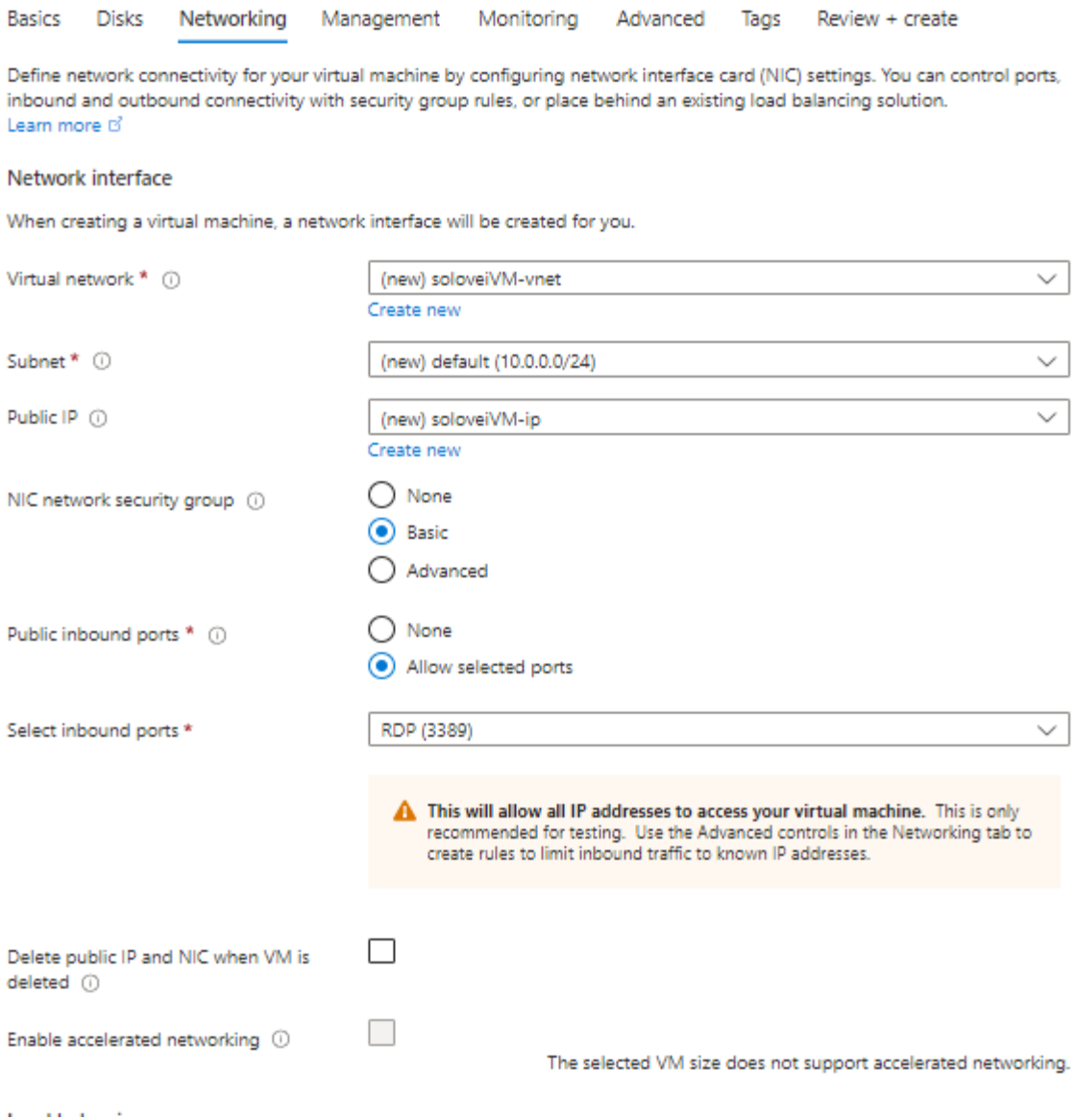
Enable Ultra Disk compatibility ☐

Data disks for soloveiVM

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM

Віртуальна мережа (Virtual network)



Віртуальна мережа Azure — це служба, яка дозволяє багатьом типам ресурсів Azure (в тому числі віртуальній машині) безпечно взаємодіяти з іншими, Інтернетом і локальними сетями.

Основні сценарії, які можна виконати за допомогою віртуальної мережі.

- Обмін даних через Інтернет – можливо за допомогою Public IP.
- Взаємодія з локальними ресурсами - – за протоколами Point-to-site virtual private network (VPN), Site-to-site VPN, Azure ExpressRoute
- Фільтрація мережевого трафіку – через створення груп безпеки. Група безпеки мережі містить правила безпеки, які дозволяють або забороняють вхідний мережевий трафік до віртуальної машини або вихідний мережевий трафік від віртуальної машини. рекомендується пов’язувати групу безпеки мережі з окремими підмережами (Subnet), а не з окремими мережевими інтерфейсами в підмережі, коли це можливо.
- Маршрутизация сетевого трафика.

Віртуальна мережа – Мережа основні налаштування

- Virtual networks - віртуальні мережі логічно ізольовані одна від одної. Для їх налаштувати необхідно визначити діапазони IP-адрес, підмережі, таблиці маршрутів, шлюзи та параметри безпеки
- Subnet - це діапазон IP-адрес у вашій віртуальній мережі, який можна використовувати для ізоляції віртуальних машин одна від одної.
- Network Interface (NIC) network security group - складається з правил, які забороняють чи дозволяють вхідний мережевий трафік до ВМ або вихідний мережевий трафік від ВМ.
- Public inbound ports - За замовчуванням доступ до віртуальної машини обмежено. Якщо вибрати "Allow selected ports" - тоді вхідний трафік стане можливим.
- Load balancing - механізм балансування навантажень для ВМ, які включені в поол.

Загальнодоступні та приватні IP-адреси

- Загальнодоступні та приватні IP-адреси використовуються в Azure для обміну даними між ресурсами. Обмін даними між ресурсами може відбуватися у приватній віртуальній мережі Azure та в загальнодоступний Інтернет.
- Префікси загальнодоступної IP-адреси — це резервовані діапазони IP-адрес в Azure. Префікси загальнодоступних IP-адрес складаються з адрес IPv4 і
- IPv6.
- Доступні такі розміри префіксів загальнодоступних IP-адрес:
- /28 (IPv4) або /124 (IPv6) = 16 адрес
- /29 (IPv4) або /125 (IPv6) = 8 адрес
- /30 (IPv4) або /126 (IPv6) = 4 адреси
- /31 (IPv4) або /127 (IPv6) = 2 адреси
- Розмір префікса визначається як розмір маски безкласової міждоменної.
- маршрутизації (CIDR).

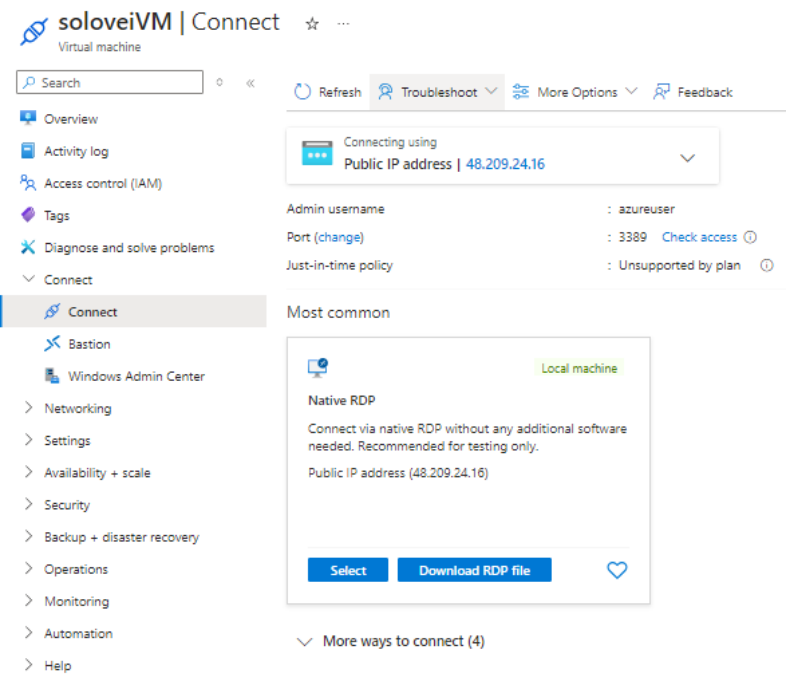
Пріоритети правил

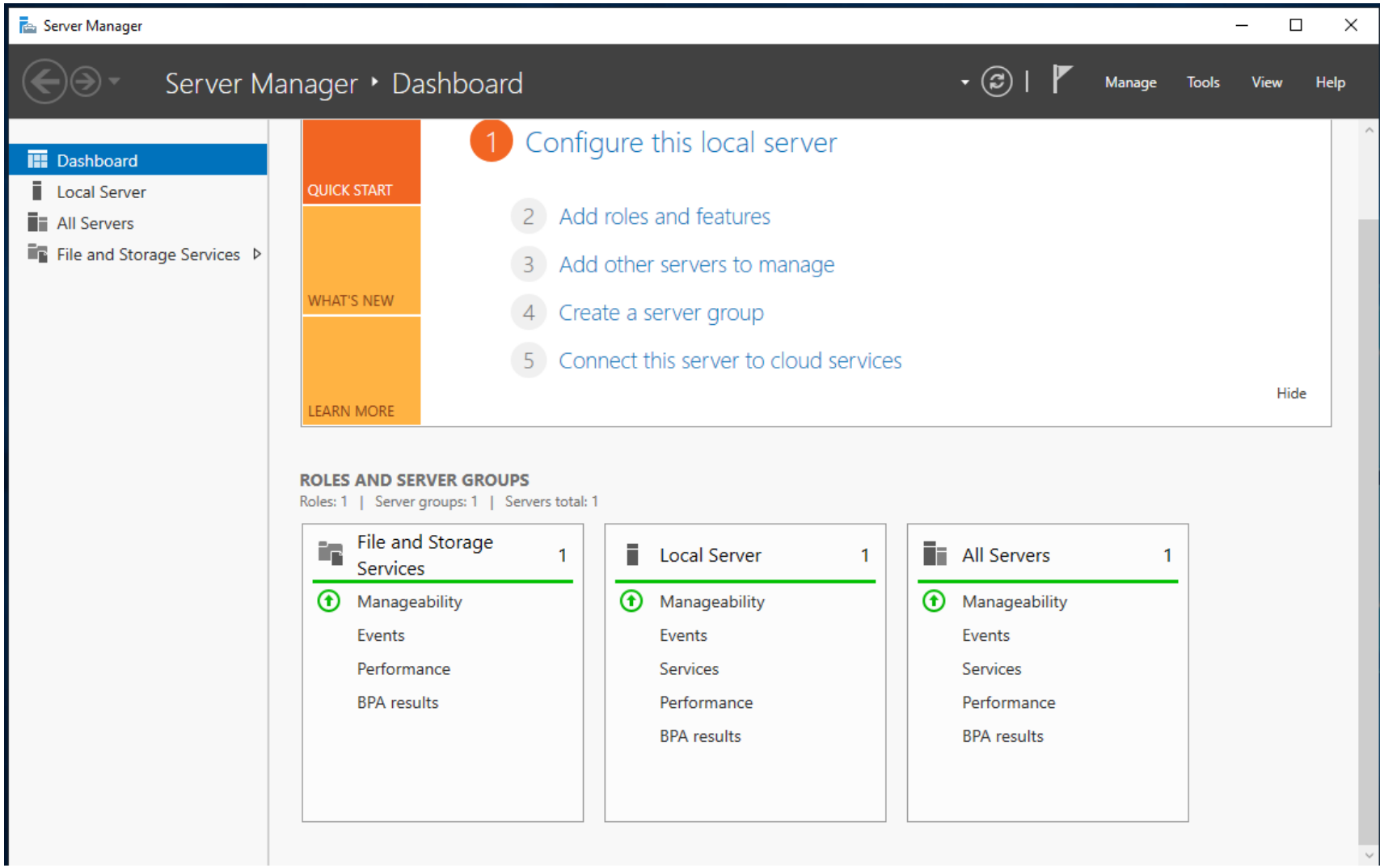
- Правила оцінюються в порядку пріоритету, починаючи з найнижчого пріоритетного правила. Забороняюче правило завжди зупиняє оцінку. Наприклад, якщо вихідний запит заблоковано правилом інтерфейсу мережі, правила для підмережі не перевіряються. Щоб проходження трафіку через групу безпеки було дозволено, він повинен проходити через усі застосовні групи.
- ***Останнє правило - це завжди правило Заборонити все. Це правило за умовчанням, додане до кожної групи безпеки для вхідного та вихідного трафіку з пріоритетом 65500***

Підключення до ВМ Azure

- Після створення ВМ – до неї необхідно підключитись. Існує кілька варіантів вибору.
  - Протокол віддаленого робочого столу (RDP)
  - Користувальницькі скрипти;
  - Користувальницькі образи віртуальних машин (з встановленим програмним забезпеченням).
- Протокол віддаленого робочого стола (RDP) забезпечує віддалене підключення до інтерфейсу користувача комп'ютерів Windows. RDP дозволяє увійти на віддалений фізичний або віртуальний комп'ютер Windows і керувати цим комп'ютером.
- Для підключення протоколу RDP потрібен клієнт RDP. Корпорація Майкрософт надає клієнтам RDP такі операційні системи:
  - Windows (вбудований);
  - macOS;
  - iOS
  - Android.
- Щоб підключитися до віртуальної машини Azure за допомогою клієнта RDP, вам знадобиться:
  - загальнодоступна IP-адреса віртуальної машини (або приватна адреса, якщо налаштовано підключення віртуальної машини до вашої мережі);
  - Номер порту
- Ви можете ввести ці відомості в клієнт RDP або завантажити попередньо налаштований файл RDP.
- Файл RDP - це текстовий файл, який містить набір пар "ім'я-значення", які визначають параметри з'єднання для клієнта RDP для підключення до віддаленого комп'ютера за допомогою протоколу віддаленого робочого столу.

Для підключення до *створеної* ВМ необхідно отримати RDP file. При вдалому підключенні ви зможете відкрити Server Manager, який треба налаштувати





Web-Internet Information Services (IIS) — це веб-сервер від компанії Microsoft, який входить до складу операційних систем Windows. IIS забезпечує платформу для розміщення та управління веб-сайтами, веб-додатками та послугами.

Основні компоненти IIS:
Веб-сервер: Основна функція IIS — це обробка запитів HTTP і HTTPS. Веб-сервер приймає запити від клієнтів (наприклад, веб-браузерів) і повертає відповідний контент, такий як HTML-сторінки, зображення або інші дані.

FTP-сервер: IIS може також функціонувати як FTP-сервер, забезпечуючи передачу файлів через протокол FTP.

Служби безпеки: IIS підтримує різні методи автентифікації та авторизації для захисту ресурсів веб-сайту. Це включає Windows-аутентифікацію, базову автентифікацію, сертифікати SSL/TLS для захищеного з'єднання тощо.

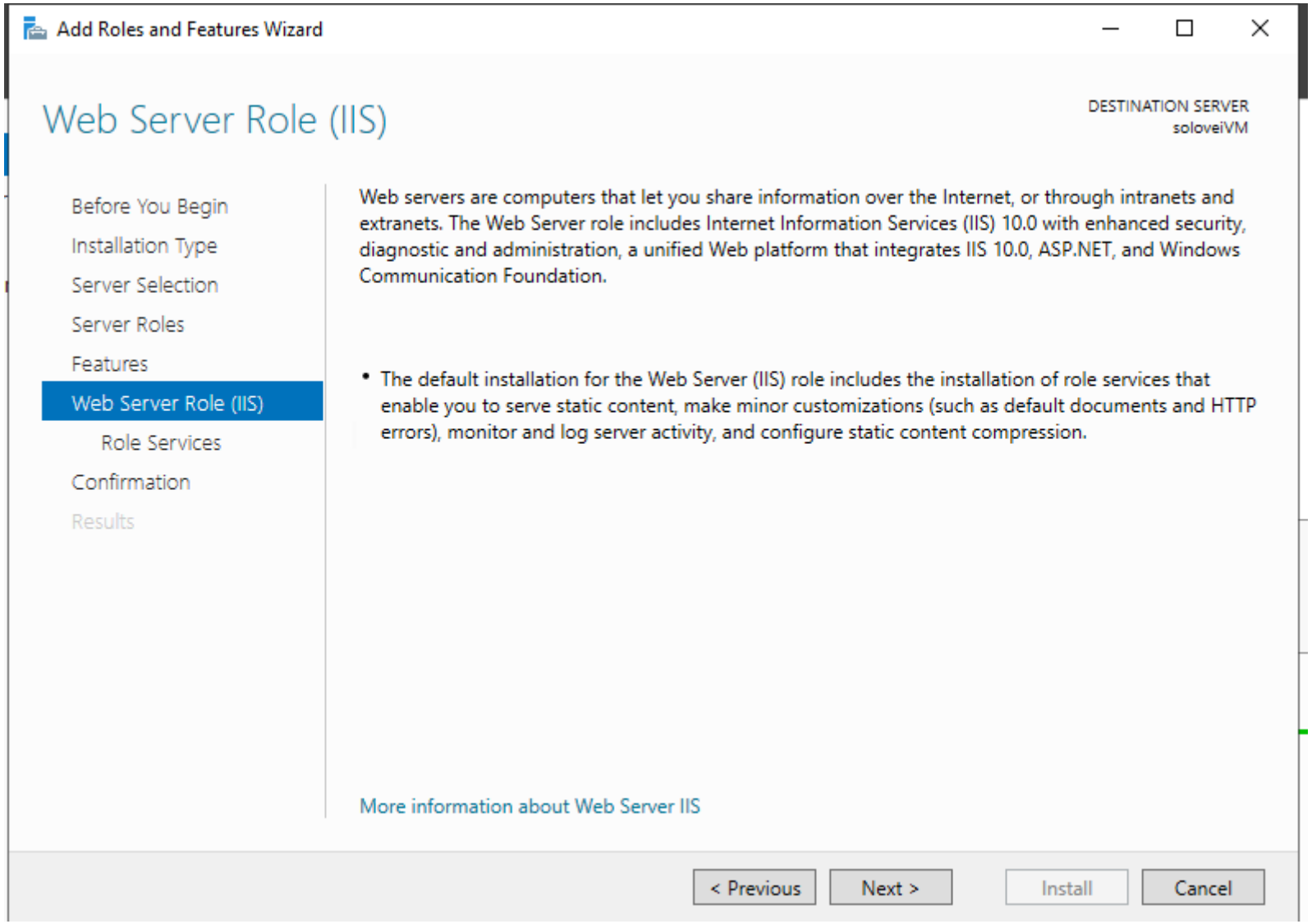
Розширюваність: IIS підтримує модулі, які дозволяють розширювати функціональні можливості сервера. Наприклад, це можуть бути модулі для обробки запитів ASP.NET, PHP, CGI, і інші.

Управління сайтами: IIS надає інтерфейс для управління веб-сайтами та додатками, де можна створювати нові сайти, налаштовувати зони видимості, обмеження доступу, налаштовувати обробку помилок і так далі.

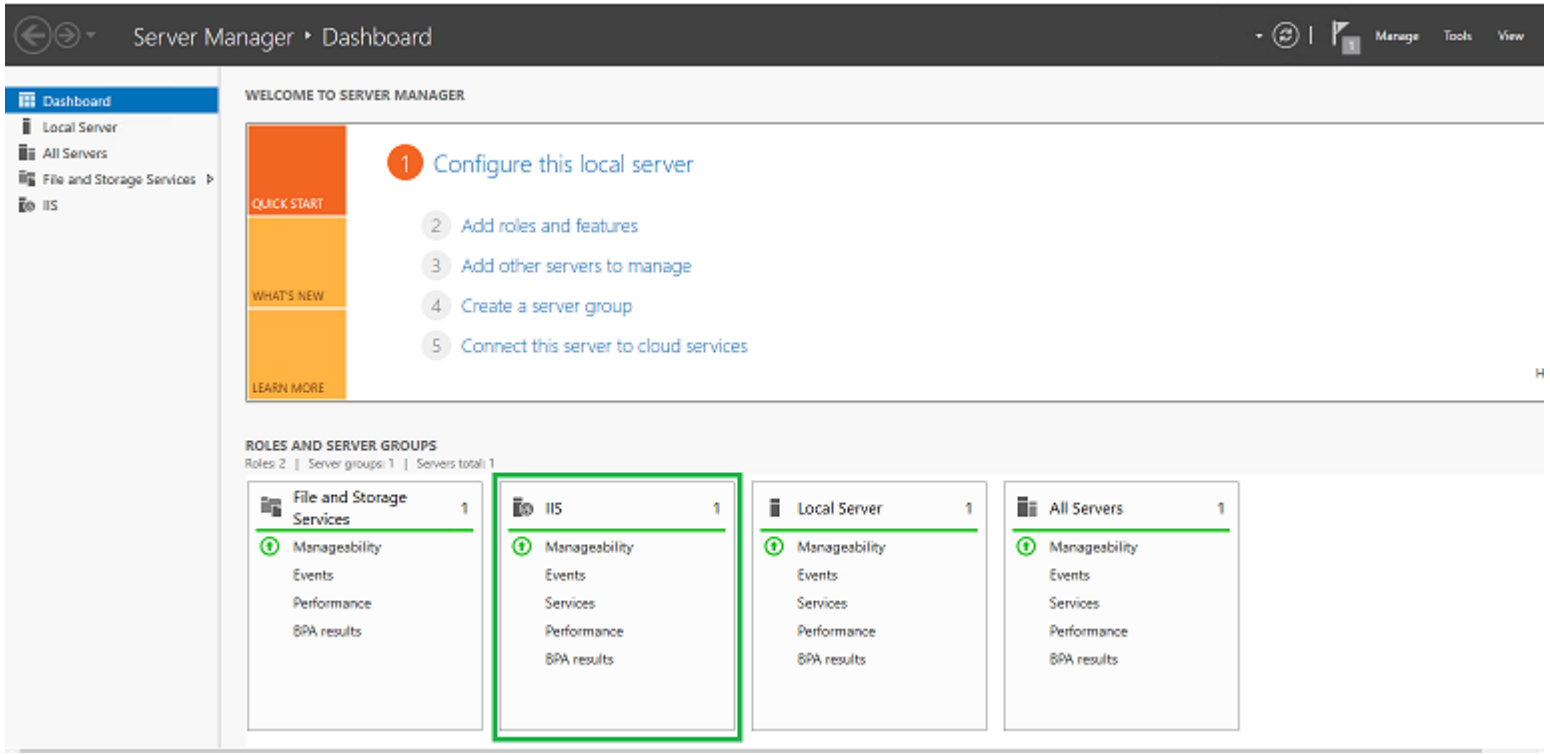
Логи та моніторинг: IIS надає інструменти для ведення логів і моніторингу активності на сервері. Це дозволяє адміністраторам відстежувати доступ до ресурсів, виявляти та усувати можливі проблеми.

Налаштування Web-Internet Information Services (IIS) на ВМ

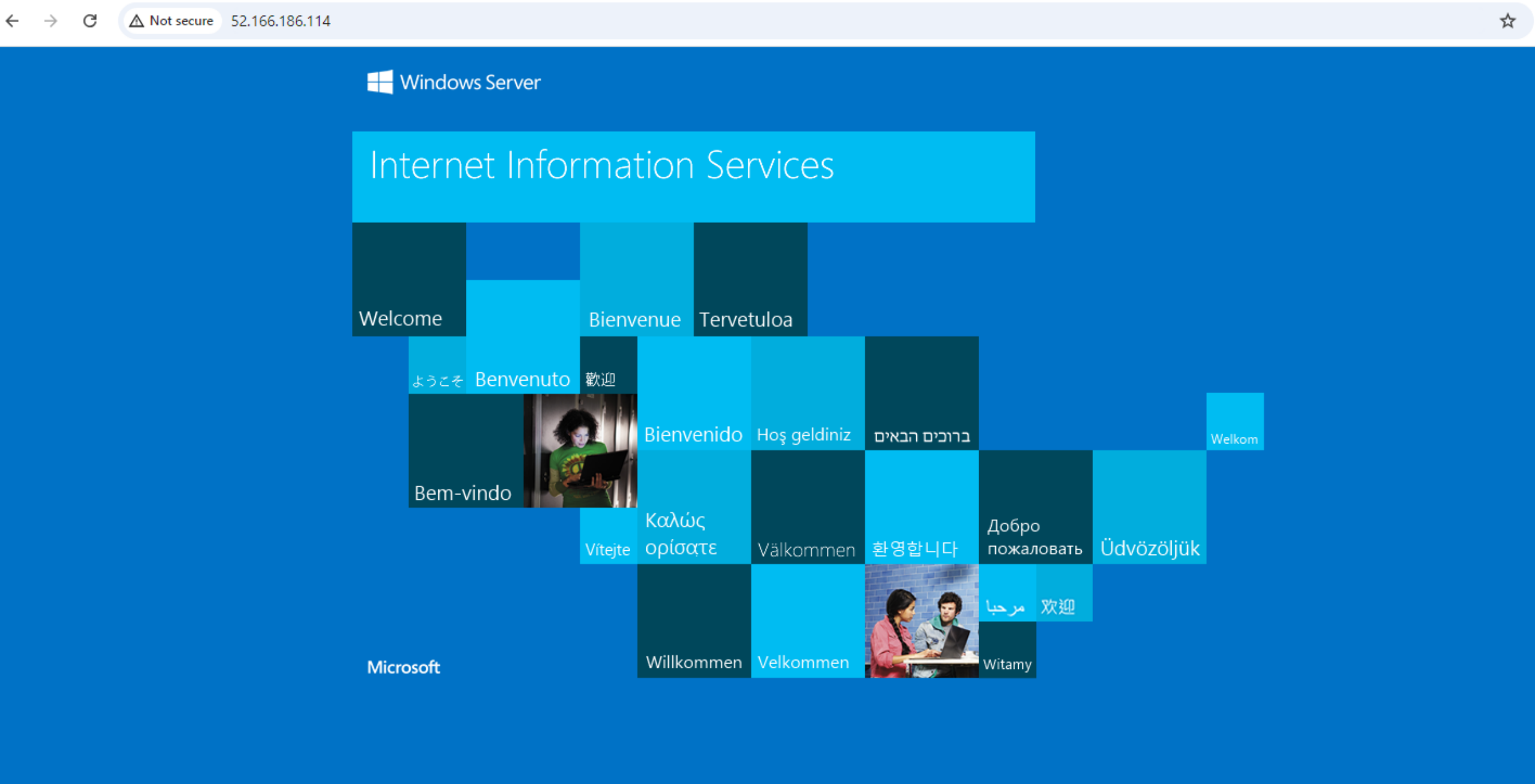
Server Manager/Add Roles and Features/Web Server Role



Після вдалого розгортання серверу, його буде додано до списку серверів.



Відкриємо Default Web site page



Відкриття портів у віртуальних машинах Azure

Нові віртуальні машини заблоковано за замовчуванням.

Програми можуть виконувати вихідні запити, але дозволено лише вхідний трафік із віртуальної мережі (наприклад, інші ресурси у тій самій локальній мережі) та Azure Load Balancer (перевірка проб).

Щоб налаштувати конфігурацію для підтримки FTP, потрібно виконати два кроки.

При створенні віртуальної машини можна відкрити кілька поширених портів (RDP, HTTP, HTTPS і SSH). Проте, якщо потрібно внести інші зміни до брандмауера, необхідно внести їх самостійно.

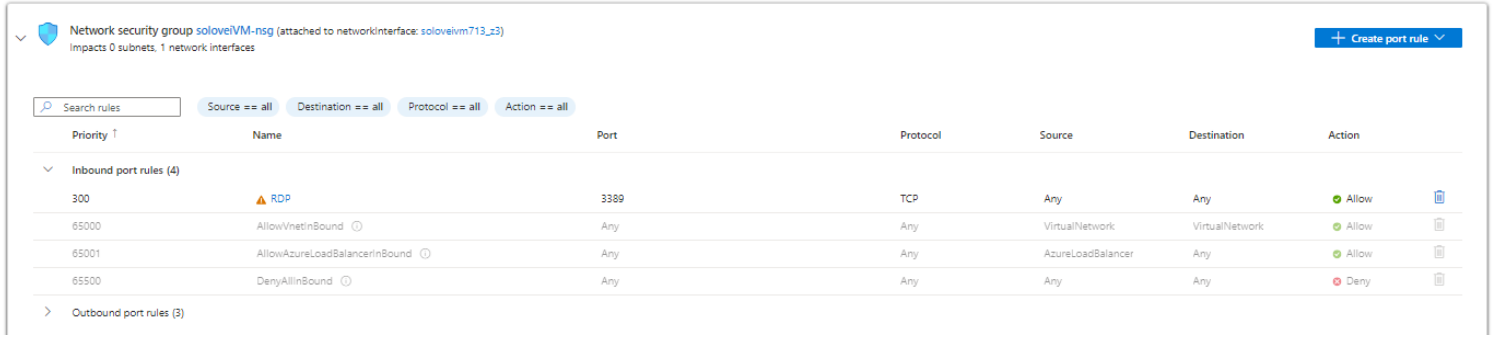
Ця процедура складається з двох етапів:

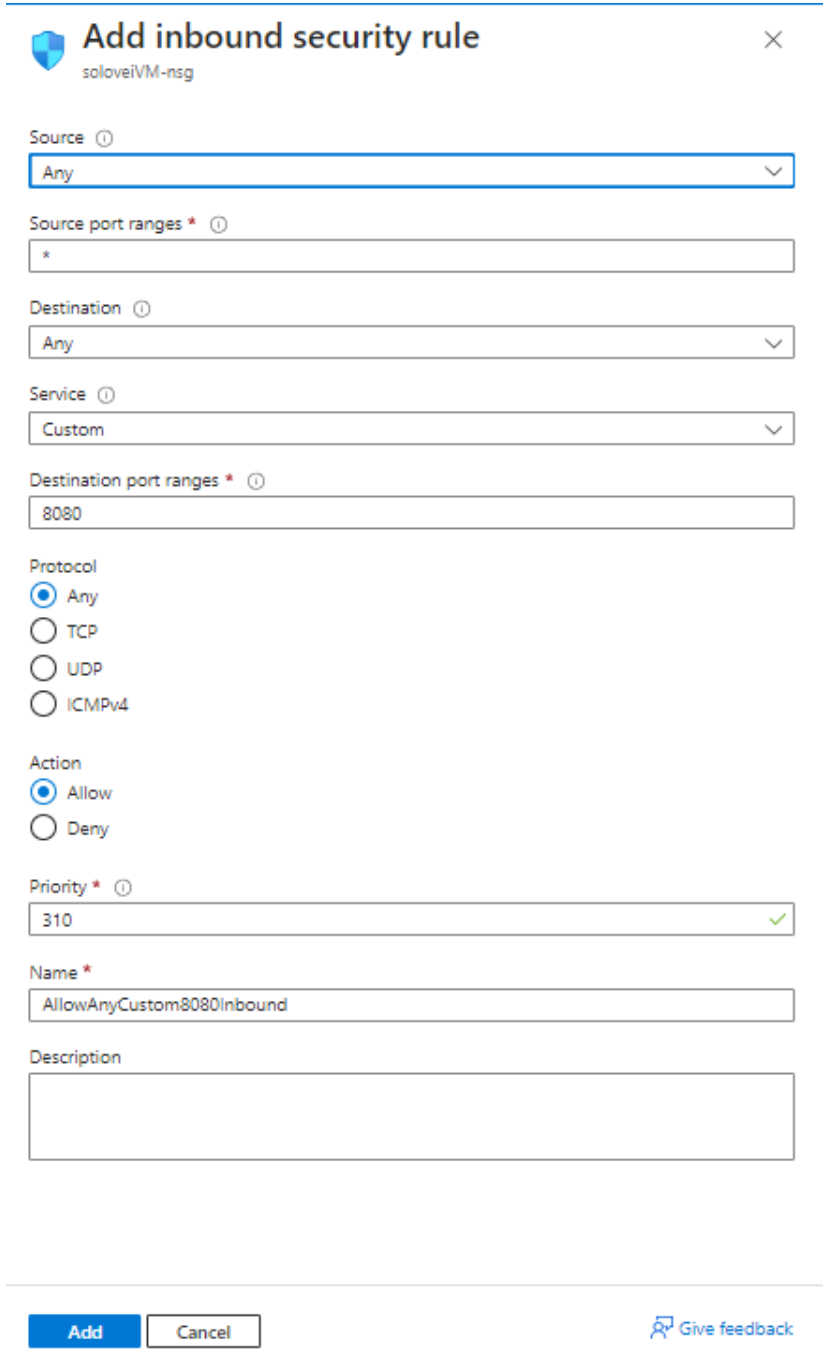
- ✓ Створіть групу безпеки мережі.
- ✓ Створіть правило вхідного трафіку, яке дозволяє трафік через порт 20 та 21 для активної підтримки FTP.

Відкриємо Default Web site page

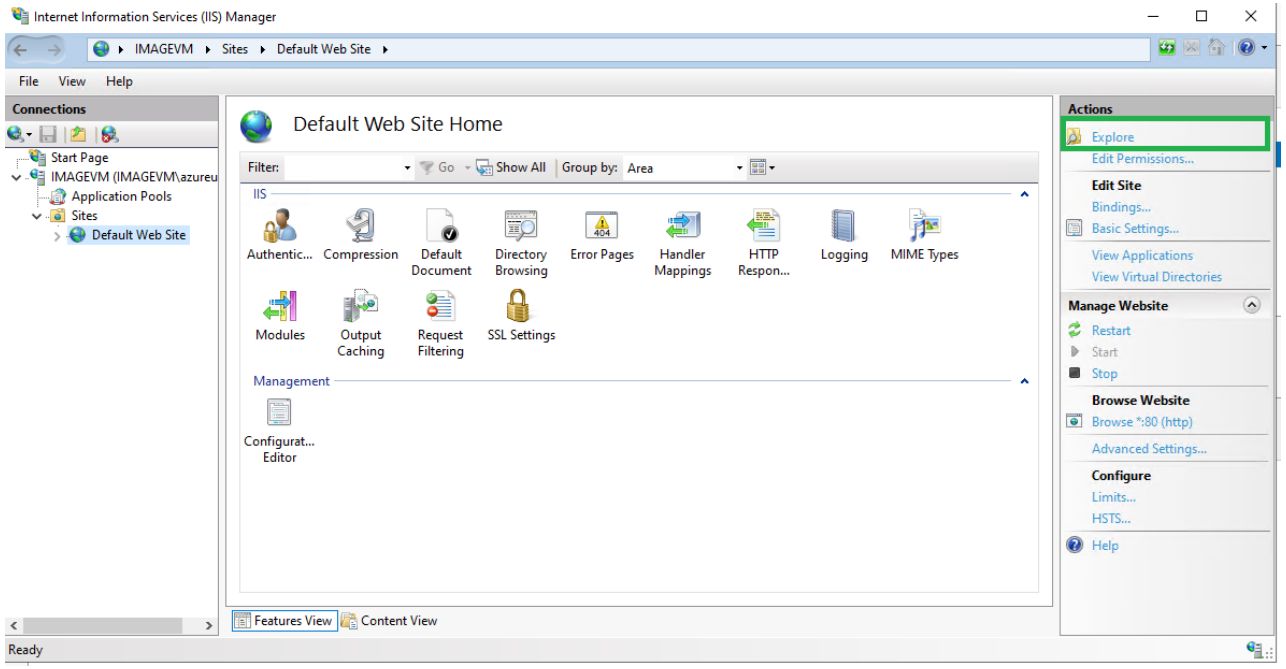
Для *створеної* ВМ група безпеки закриває всі порти.

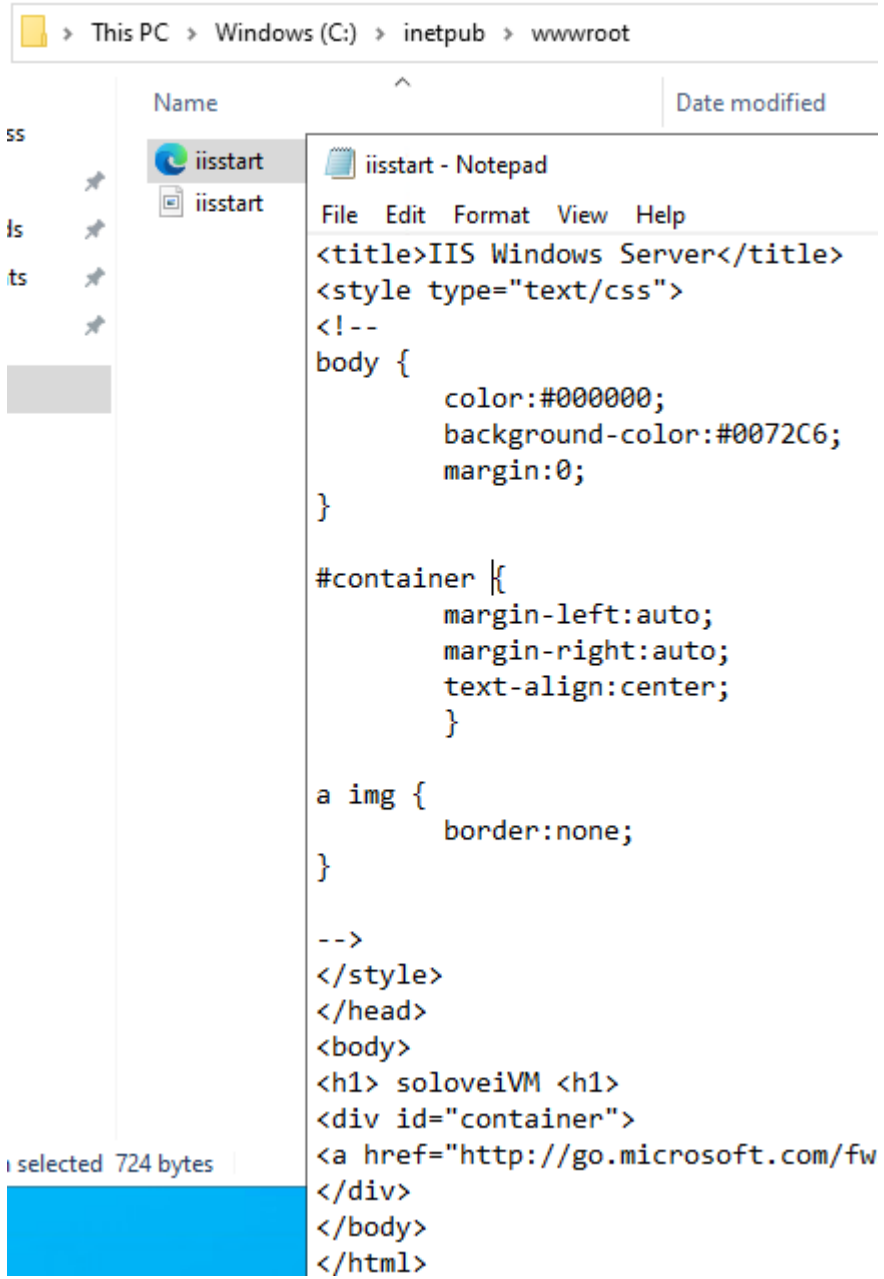
Для отримання трафіку – відкриємо порти – 8080.





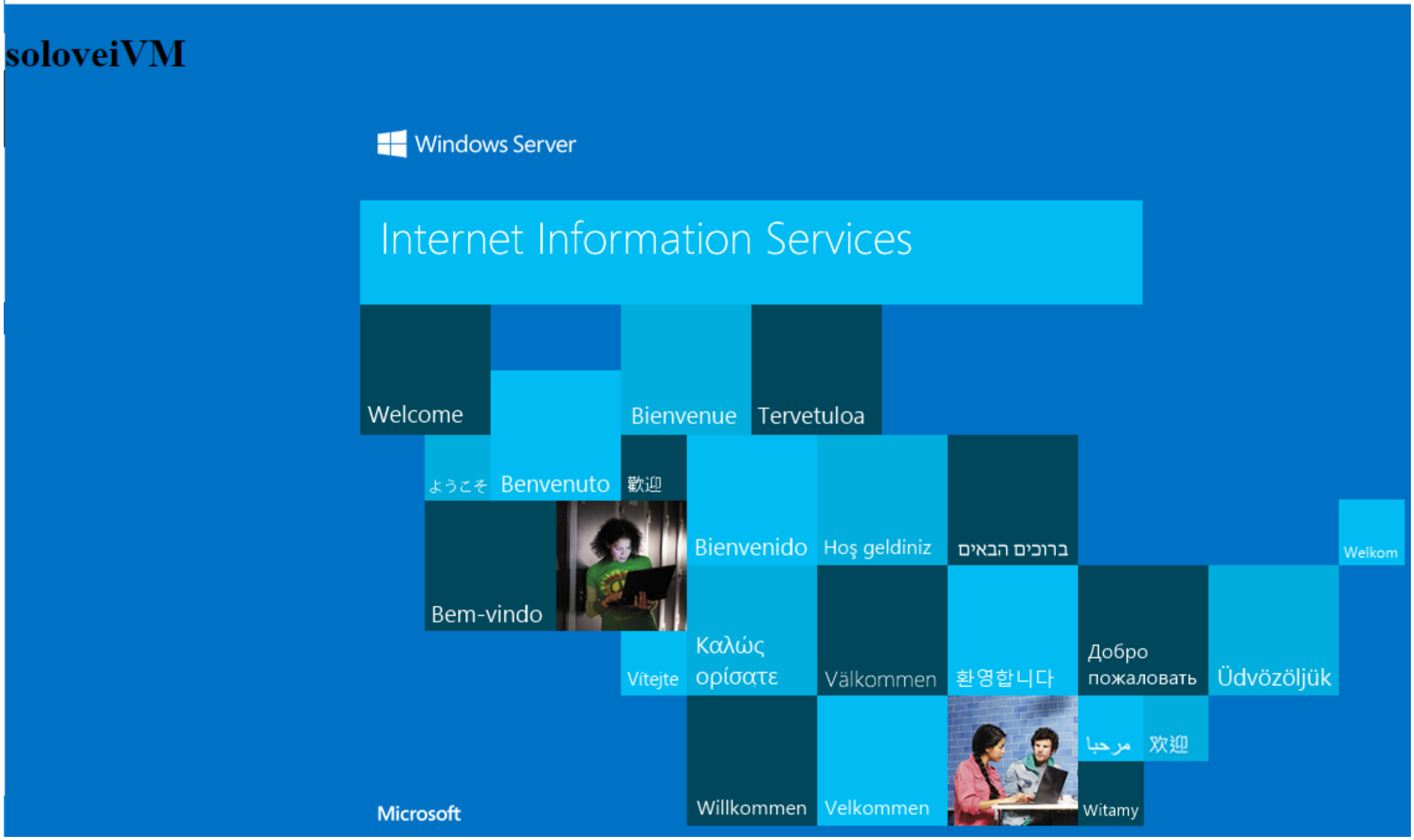
Додамо ім'я ВМ на default web site home page виконаємо кроки – IIS Manager, Explore.





Not secure 52.166.186.114

soloveiVM



Azure Cloud Shell – Azure CLI

Azure Cloud Shell - це браузерна оболонка, призначена для розробки та адміністрування ресурсів Azure. Azure CLI використовується для створення ресурсів Azure та керування ними з командного рядка або за допомогою скриптів.

Оскільки Cloud Shell створена для інтерактивних сеансів, оболонки автоматично завершують роботу після 20 хвилин бездіяльності.

Azure Cloud Shell виконується в Azure Linux, дистрибутиві Linux корпорації Майкрософт для продуктів та служб на межі хмарної інфраструктури.

Корпорація Майкрософт внутрішньо компілює всі пакети, що входять до репозиторій Azure Linux, щоб захиститися від атак ланцюжка поставок.

Azure Cloud Shell дозволяє створити та розгорнути ВМ за допомогою низки команд.

Azure Cloud Shell – команди для створення ВМ

1. Робота починається зі створення групи ресурсів за допомогою команди ***az group create***.

```
resourcegroup="myResourceGroupCLI"
location="westus3"
az group create --name $resourcegroup --location $location
```

У прикладі створюється група ресурсів з ім'ям myResourceGroup в розташуванні "Західна частина США 3".

1. Командою az vm create – створюється ВМ.

```
vmname="myVM"
username="azureuser"
az vm create \
    --resource-group $resourcegroup \
    --name $vmname \
    --image Win2022AzureEditionCore \
    --public-ip-sku Standard \
    --admin-username $username
```

У прикладі створюємо ВМ з ім’ям myVM та ім'ям адміністратора – azureuser. Якщо ВМ - ну створено, то про це з’явиться повідомлення та publicIpAddress.

Створення ВМ – cloud shell

```
$grp="VMdemo"
$location="westeurope"
$vnetName="VNET"
$subnetName="SUBNET_1"
$vmName="Demo_VM1"
$vmName="Demo_VM2"
$avset ="AVSET"

# CREATE RESOURCE GROUP
az group create --name $grp --location $location

# CREATE VIRTUAL NETWORK
az network vnet create --address-prefixes 10.0.0.0/16 --name $vnetName --resource-group $grp

# CREATING SUBNET
az network vnet subnet create -g $grp --vnet-name $vnetName -n $subnetName --address-
prefixes 10.0.0.0/24

# CREATING VMs
az vm create --resource-group $grp --name $vmName --vnet-name $vnetName --subnet
$subnetName --admin-username azureuser --admin-password Hello@12345#

#open ports
az vm open-port --port 80 --resource-group $grp --name $vmName

#install web server IIS
az vm run-command invoke -g $grp -n $vmName --command-id RunPowerShellScript --scripts
"Install-WindowsFeature -name Web-Server -IncludeManagementTools"

#az group delete --name $grp
```

Azure Marketplace містить багато образів, які можна використовувати для створення віртуальних машин. На попередніх кроках віртуальна машина створювалася за допомогою Windows Server 2016 Datacenter. На цьому кроці модуль PowerShell використовується для пошуку інших образів Windows на сайті Marketplace, які можна використовувати для створення віртуальних машин. Цей процес полягає в пошуку відомостей про видавця, пропозицію, номер SKU та (необов'язково) номер версії для ідентифікації образу.
Get-AzVMImagePublisher -Location "westeurope"

Список пропозицій образів, використовуючи команду Get-AzVMImageOffer. Ця команда повертає список, відфільтрований за вказаним видавцем Microsoft Windows Server.

```
Get-AzVMImageOffer `
   -Location "westeurope" `
   -PublisherName "MicrosoftWindowsServer"
```

Команда Get-AzVMImageSku відфільтрує список на ім'я видавця та назву пропозиції, відобразивши список імен образів.

```
Get-AzVMImageSku -Location "westeurope" -PublisherName "MicrosoftWindowsServer" -Offer "WindowsServer"
```

Ці відомості можна використовувати для розгортання віртуальної машини з урахуванням конкретного образу

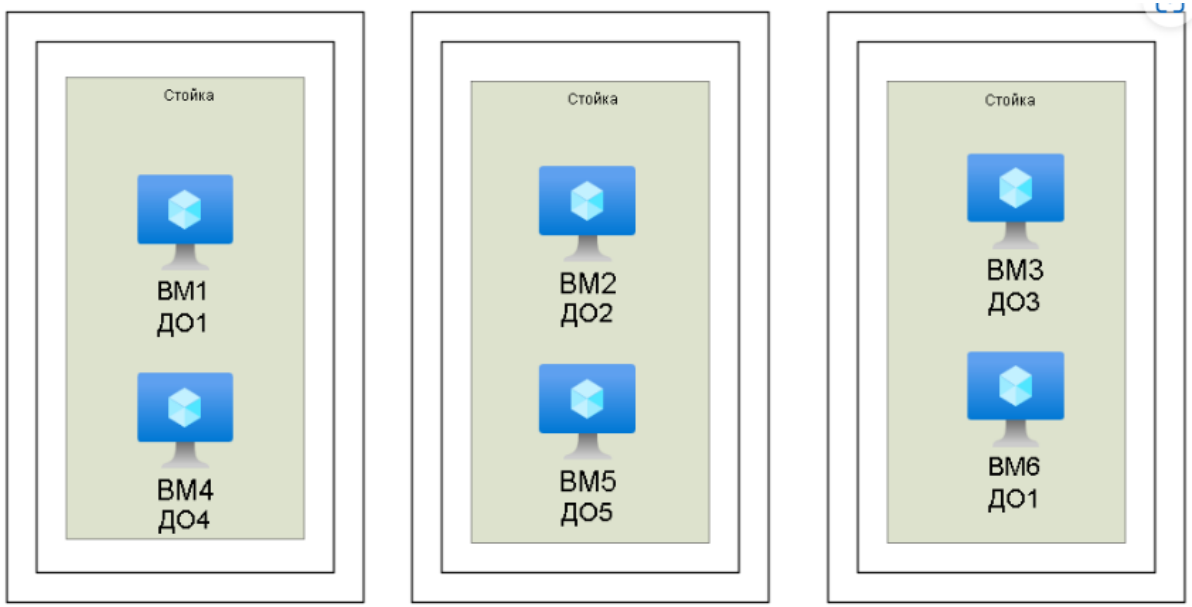
```
az vm create --resource-group VMdemo --name MyVM --image Win2019Datacenter --admin-username azureuser --admin-password
Hello@12345# --size Standard_DS1_v2

$grp = "VMdemo"
$vmname = "MyVM“

#open ports
az vm open-port --port 80 --resource-group $grp --name $vmName

az vm run-command invoke -g $grp -n $vmName --command-id RunPowerShellScript --scripts "Install-WindowsFeature -name Web-Server -
IncludeManagementTools“
```

Azure *«Availability sets»* ***- «домени збою» і «домени оновлення»***

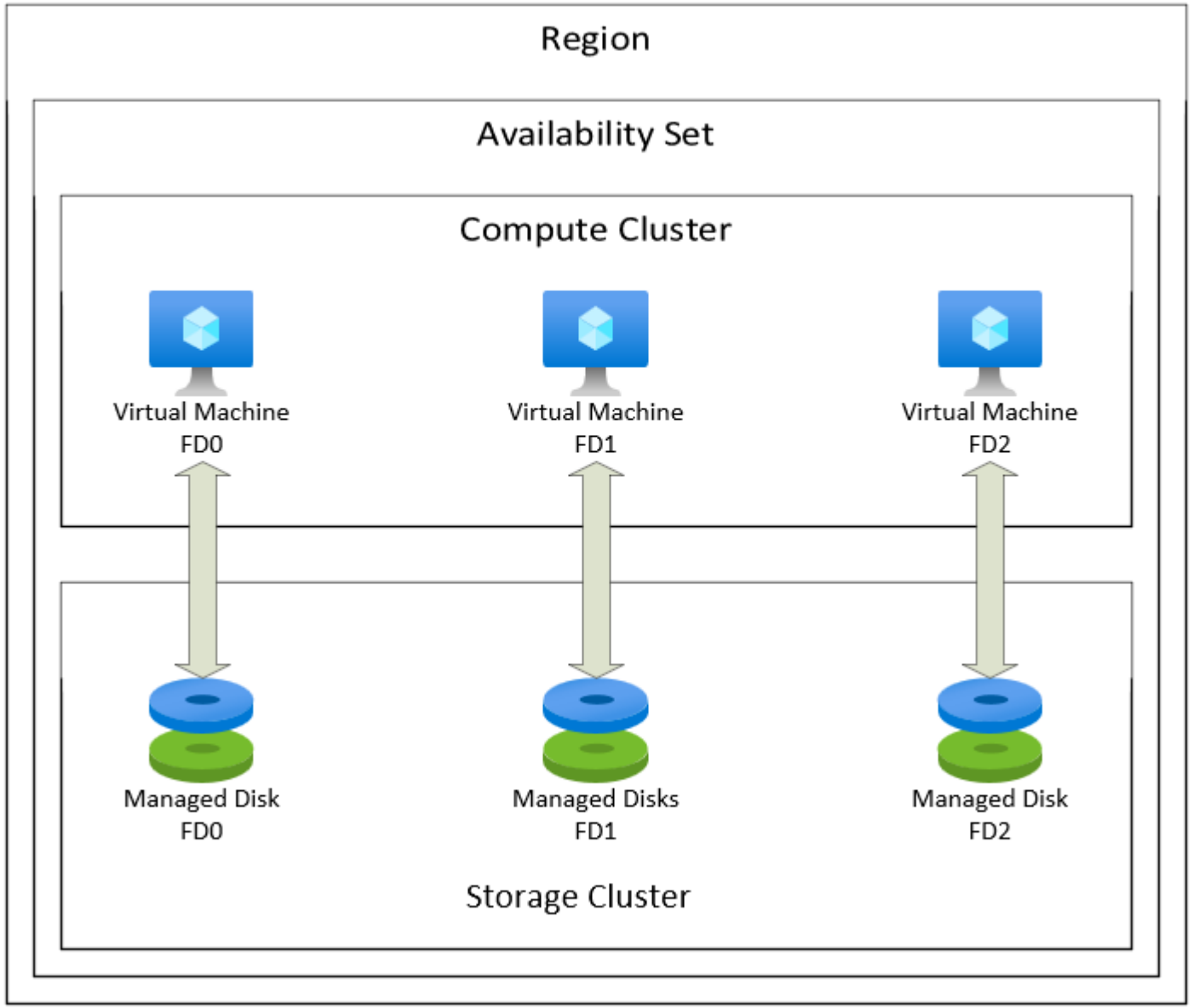


Наприклад, для 6 ВМ з 5 доменами оновлення шоста віртуальна машина поміщається в той же домен оновлення, що й перша віртуальна машина, таким чином, коли ДО1 – перезавантажується, то ВМ1 та ВМ2 не доступні, але ВМ3, ВМ4, ВМ5 – працюють, відповідно при завантаженні ДО2 – не доступна тільки ВМ2.
Це рішення забезпечує високу доступність ВМ в хмарі Azure.

- «Доступна зона» є комбінацією «доменів збою» і «доменів оновлення». Для кожної зони доступності можна настроїти до 3 доменів збою та 20 доменів оновлення. Ці конфігурації не можна змінити після створення групи доступності.
- Домени збою визначають групу віртуальних машин, які спільно використовують спільне джерело живлення та мережний комутатор.
- Домени оновлення – це групи віртуальних машин та базове фізичне обладнання, яке може бути перезавантажено одночасно.

Availability sets— це логічне групування віртуальних машин, яке дозволяє Azure зрозуміти, як ваша програма створена для забезпечення резервування та доступності. Рекомендовано створювати дві або більше віртуальних машин у межах набору доступності, щоб забезпечити високу доступність програми та відповідати 99,95% Azure SLA.
За певних обставин дві віртуальні машини в одному наборі доступності можуть спільно використовувати домен помилки.
Спільний домен помилки може бути спричинений виконанням наступної послідовності під час розгортання віртуальних машин:

Розгорніть першу віртуальну машину.
Зупинити/звільнити першу віртуальну машину.
Розгорніть другу віртуальну машину.
За цих обставин диск ОС другої віртуальної машини може бути створений у тому самому домені помилки, що й перша віртуальна машина, тому дві віртуальні машини будуть у тому самому домені помилки. Щоб уникнути цієї проблеми, не треба зупиняти/звільняти віртуальні машини між розгортаннями.



Availability sets

```
az vm availability-set create --name
                              --resource-group
                              [--location]
                              [--no-wait]
                              [--platform-fault-domain-count]
                              [--platform-update-domain-count]
                              [--ppg]
                              [--tags]
                              [--unmanaged]
                              [--validate]
```

az vm availability-set create -n MyAvSet -g $grp --platform-fault-domain-count 2 --platform-update-domain-count 2

```
az vm availability-set delete [--availability-set-name]
                              [--ids]
                              [--resource-group]
                              [--subscription]
```

Azure DNS

Система доменних імен – це ієрархія доменів. Ієрархія починається з root домену, ім'я якого просто ".". Нижче наведені домени верхнього рівня, такі як com, net, org або ukjp. Під доменами верхнього рівня знаходяться домени другого рівня, наприклад, org.uk або co.jp. Ці домени в ієрархії DNS глобально розподілені на серверах DNS по всьому світу.

Домени DNS в Azure DNS розміщуються в глобальній мережі DNS-серверів Azure, В Azure DNS мережа організована таким чином, що на кожен запит DNS відповідає найближчий доступний DNS-сервер.

При створенні контейнера на порталі Azure для нього автоматично створюється IP-адреси. Загальнодоступна IP-адреса використовується для віддаленого доступу. Хоча портал не створює повне доменне ім'я або повне доменне ім'я, його варто додати після створення.

Реєстратор доменних імен - це організація, яка дозволяє придбати доменне ім'я, наприклад, company.com. Купуючи доменне ім'я, ви отримуєте право керувати ієрархією DNS під цим ім'ям, наприклад, налаштувати перенаправлення на веб-сайт вашої компанії при введенні адреси www.company.com. Реєстратор може розмістити домен на власних серверах імен від вашого імені або дозволить вказати альтернативні сервери доменних імен.

Зона DNS

Зона DNS використовується для розміщення записів DNS певного домену. Щоб розмістити домен в Azure DNS, необхідно створити зону DNS. Кожен запис DNS для вашого домену створюється всередині цієї зони DNS.

Наприклад, домен company.com може містити декілька записів DNS, включаючи mail.company.com (поштовий сервер) і www.company.com (для веб-сайту).

При створенні зони DNS в Azure DNS враховуйте таке.

- ✓ Ім'я зони має бути унікальним у межах групи ресурсів, а зона не має існувати. В іншому випадку операція завершиться помилкою.
- ✓ Це ж ім'я зони можна використовувати повторно в іншій групі ресурсів або іншій підписці Azure.
- ✓ Якщо кільком зонам надано одне й те саме ім'я, кожному примірнику призначаються різні адреси серверів доменних імен. За допомогою реєстратора доменних імен можна налаштувати лише один набір адрес.

Типи та набори записів

Типи записів

Кожний запис DNS має ім'я та тип. Записи поділяються на різні типи в залежності від даних, які вони містять. Найбільш поширений тип - запис A, який зіставляє ім'я з IPv4-адресою. Інший поширений тип - запис MX, який зіставляє ім'я з поштовим сервером.

Azure DNS підтримує всі загальні типи записів DNS: A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV та TXT. Зверніть увагу, що записи SPF представлені у вигляді записів TXT.

Набори записів

У деяких випадках необхідно створити кілька записів DNS із заданим ім'ям та типом. Наприклад, припустимо, що веб-сайт www.company.com розміщується за двома різними IP-адресами. Для цього веб-сайту потрібно два різні записи A — по одній для кожної IP-адреси: Ось приклад набору записів:

```
www.contoso.com.        3600    IN    A    134.170.185.46
www.contoso.com.        3600    IN    A    134.170.188.221
```

Типи та набори записів

Azure DNS керує всіма записами DNS за допомогою наборів записів. Набір записів (також називається набором записів ресурсів) – це колекція записів DNS у зоні, які мають одне ім'я та належать до одного типу. Більшість наборів записів містять один запис. Проте трапляються й набори з кількома записами (як у прикладі вище).

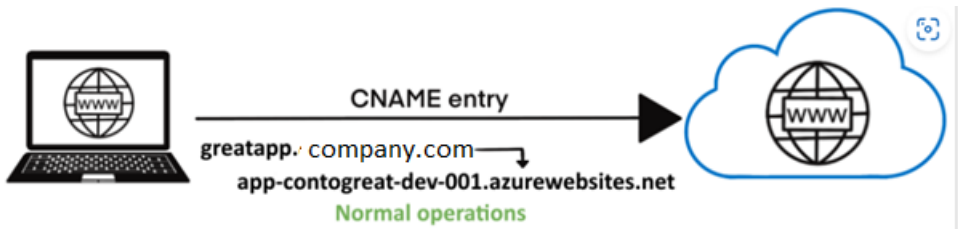
Наприклад, припустимо, що ви вже створили в зоні company.com запис A www, що вказує на IP-адресу 134.170.185.46 (перший запис вище). Щоб створити другий запис, не потрібно створювати додатковий набір записів — слід додати запис до вже наявного набору записів.

Набір записів типу SOA та CNAME є винятками. За стандартами DNS декілька записів з тим самим ім'ям для цих типів не допускаються, тому такі набори записів можуть містити лише один запис.

Захоплення піддомену

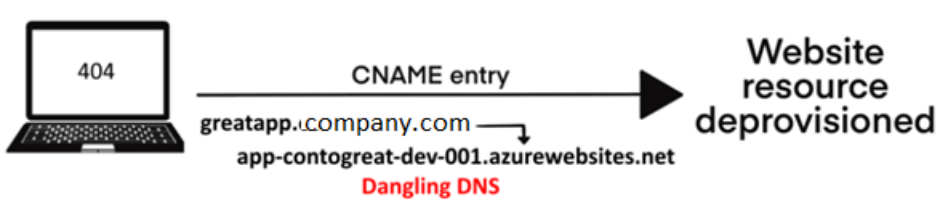
Захоплення піддоменів — поширена та серйозна загроза для організацій, які регулярно створюють та видаляють безліч ресурсів. Захоплення піддомену може відбутися, якщо у вас є запис DNS, що вказує на відкликаний ресурс Azure. Такі записи DNS називаються недійсними. Записи CNAME особливо вразливі до цієї загрози. Захоплення піддоменів дозволяє зловмисникам перенаправляти трафік, призначений для домену організації на сайт, що виконує шкідливі дії. Поширений сценарій для захоплення піддомену:

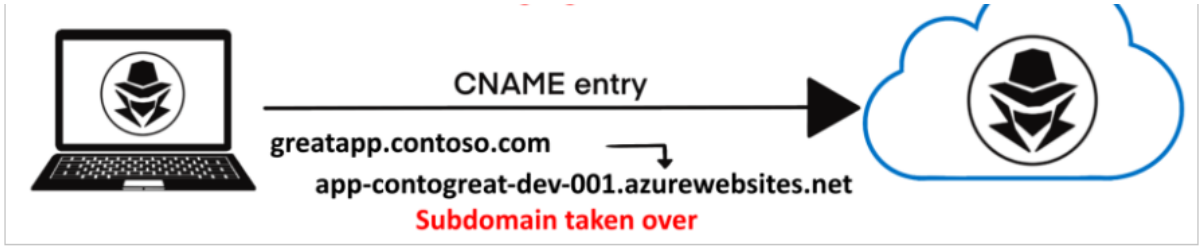
СТВОРІННЯ: Ви підготуєте ресурс Azure з повним доменним ім'ям (FQDN) app-contogreat-dev-001.azurewebsites.net. Ви призначаєте запис CNAME в зоні DNS з піддоменом greatapp.company.com, який надсилає трафік до ресурсу Azure.



Захоплення піддомену - ВІДГУК

Ресурс Azure буде відкликаний або видалений після того, як у ньому зникне потреба.





На цьому етапі запис CNAME greatapp.company.com необхідно видалити із зони DNS. Якщо запис CNAME не видалити, він оголошується як активний домен, але не надсилає трафік до активного ресурсу Azure. Це визначення "висячих" dns-записів.

Висячий піддомен (greatapp.company.com) тепер вразливий і може бути перепризначений іншому ресурсу підписки Azure.

ЗАХОПЛЕННЯ:

Використовуючи загальнодоступні методи та засоби, зловмисник виявляє "висячий" піддомен. Зловмисник готує ресурс Azure з тим самим повним доменним ім'ям раніше керованого вами ресурсу. У цьому прикладі app-contogreat-dev-001.azurewebsites.net.

Трафік, що відправляється в піддомен greatapp.company.com, тепер направляється в ресурс шкідливого суб'єкта, де вони керують вмістом.

Питання

1. Що таке регіон Azure, і чому їх географічне розташування важливе для продуктивності та відповідності вимогам?
2. Чим відрізняються зони доступу (Availability Zones) від регіонів, і які гарантії відмовостійкості вони надають?
3. Яку роль відіграють пари регіонів (Region Pairs) та які переваги забезпечують у сценаріях аварійного відновлення?
4. Які ключові параметри потрібно визначити під час створення віртуальної машини в Azure (наприклад, розмір, OS, диск, мережа)?
5. Чим відрізняються типи дисків Standard HDD, Standard SSD та Premium SSD, і як вибір впливає на продуктивність?
6. Які параметри безпеки (SSH, паролі, мережеві правила) необхідно враховувати під час розгортання VM?
7. Які інструменти доступні в Azure Cloud Shell і чим відрізняються Bash та PowerShell режими?
8. Які основні команди Azure CLI використовують для створення віртуальної машини через Cloud Shell?
9. Чому Azure Cloud Shell вважається зручним інструментом для автоматизації та навчання адмініструванню Azure?
10. Що таке Fault Domain (домени збою) та як вони захищають VM від одночасного апаратного збою?
11. Яку роль виконують Update Domains (домени оновлення) та чому вони важливі під час планових оновлень інфраструктури?
12. Як Availability Set використовує Fault та Update Domains для підвищення доступності додатків?
13. Які типи DNS-зон підтримує Azure DNS та для чого використовується кожна з них?
14. Як працює делегування DNS-зони між реєстратором домена та Azure DNS?
15. Які переваги надає Azure DNS порівняно з традиційними DNS-серверами, зокрема у масштабованих хмарних системах?