**Лабораторна робота №5**

# РОБОТА З МЕРЕЖЕВИМИ СЕРВІСАМИ AZURE: AZURE VIRTUAL NETWORK, NETWORK SECURITY GROUP, AZURE DNS, VIRTUAL NETWORK APPLIANCE, AZURE LOAD BALANCER, AZURE APPLICATION GATEWAY, AZURE NETWORK WATCHER

**Мета**: Ознайомитися з основними мережевими сервісами платформи Microsoft Azure та навчитися створювати, налаштовувати й аналізувати хмарну мережеву інфраструктуру. Дослідити принципи побудови віртуальних мереж (Virtual Network), створення підмереж (Subnets) і груп безпеки мережі (Network Security Group) для контролю трафіку. Навчитися налаштовувати службу Azure DNS для управління доменними іменами, розгортати віртуальні мережеві пристрої (Virtual Network Appliances), балансувати навантаження за допомогою Azure Load Balancer та Application Gateway, а також використовувати Azure Network Watcher для моніторингу, діагностики й аналізу мережевих з'єднань і трафіку.

## Хід роботи

1. Перевірити політику Allowed resource deployment regions та обрати один з регіонів. Створити Virtual Network з Subnet, використовуючи Azure Portal. В головному пошуку на Azure Portal знайти Virtual Networks та обрати опцію Create. У вкладці Basics заповнити поля Resource Group, Name, Region, де Resource Group буде називатись rg-vnet-xxx-yyy-zzz,, xxx – скорочена назва обраного, серед доступних в політиці, регіонів, яка застосовується для навчальних Subscriptions Azure for Students, відповідно до цього файлу, що містить відповідність між повною та скороченою назвою регіону, а yyy – ініціали студента, zzz – номер варіанту; Name – Campus1, Region – обраний попередньо зі списку доступних, регіон. У вкладці IP Addresses замінити попередньо заповнений адресний простір на 10.xxx.zzz.0/16, де xxx – сума усіх цифр номеру групи (наприклад, для групи КБ-22-1, сума рівна 2+2+1=5), а zzz – номер варіанту групи.

Додати дві Subnet. Перша Subnet буде мати назву Campus1-Floor1, та використовувати адресний простір 10.xxx.zzz+10.0/24, друга Subnet буде мати назву Campus1-Floor2, та адресний простір 10.xxx,zzz+20.0/24. Після натиснути Review + Create.

2. Після створення попередньої Virtual Network, переглянути її параметри за переконатись у наявності вказаних Subnet. Далі перейти в Automation, Export template. Після завершення генерації template, натиснути вгорі на кнопку Download. Розпакувати завантажений zip-архів на відкрити файл template.json. Замінити у ньому всі значення Campus1 на Campus2; 10.xxx.zzz.0/16 на 10.xxx.zzz+100.0/16; Campus1-Floor1 на Campus2-Floor1; 10.xxx.zzz+10.0/24 на 10.xxx.zzz+110.0/24; Campus1-Floor2 на Campus2-Floor2; 10.xxx.zzz+120.0/24 на 10.xxx.zzz+120.0/24 та зберегти зміни у файлі templates.json. У файлі parameters.json замінити Campus1 на Campus2 та зберегти зміни. В головному пошуку Azure Portal знайти Deploy a custom template, обрати Build your own template in the editor, далі Load file. Завантажити змінений файл template.json та натиснути Save. Обрати Edit parameters, потім Load file та завантажити змінений parameters.json і натиснути Save. Переконатись, що обрано Resource Group з першого завдання, натиснути Review + Create та знову Create.
3. Створити Application Security Group (ASG). В Azure Portal в пошуку знайти Application security groups. Натиснути Create та у вкладці Basics обрати доступну Subscription, попередньо створену Resource Group, попередньо обраний Region та вказати наступний Name: asg-campus-web-xxx-zzz, де xxx – номер групи (наприклад, для КБ-22-1 – 221), zzz – номер варіанту. Натиснути Review + Create та знову Create.
4. Створити Network security Group (NSG). В Azure Portal в пошуку знайти Network security groups. Натиснути Create та у вкладці Basics обрати доступну Subscription, попередньо створену Resource Group, попередньо обраний Region та вказати наступний Name: nsg-secure-xxx-zzz, де xxx – номер групи (наприклад, для КБ-22-1 – 221), zzz – номер варіанту. Натиснути Review + Create та знову Create. Перейти до новоствореної Network Security Group, далі в розділі Settings обрати Subnets та знайти кнопку Associate. У вікні вибору обрати Virtual Network – Campus1, Subnet – Campus1-Floor1 та зберегти зміни. Продовжити роботу з NSG, перейшовши в Settings > Inbound security rules та ознайомитись з існуючими правилами. Додати нове правило, яке дозволить вхідний трафік за портами 80 TCP та 443 TCP для усіх віртуальних машин, які потенційно можуть бути додані до

ASG, вказавши наступні параметри: Source: Application security group; Source application security groups: asg-campus-web-xxx-zzz; Source port ranges: *; Destination: Any; Service: Custom; Destination port ranges: 80,443; Protocol: TCP; Action: Allow; Priority: 100; Name: AllowCampusASG. Додати Outbound security rule, яке заборонить доступ до Інтернету з наступними параметрами: Source: Any; Source port ranges: *; Destination: Service tag; Destination service tag: Internet; Service: Custom; Destination port ranges: *; Protocol: Any; Action: Deny; Priority: 4096; Name: DenyFromCampusToInternetOutbound.

5. Виконати реєстрацію безкоштовного домену у доменній зоні pp.ua на ресурсі nic.ua, використовуючи довільне ім'я домену.
6. В головному пошуку на Azure Portal знайти DNS zones та обрати Create. У вкладці Basics вказати доступну Subscription, створити нову Resource Group, що буде називатись rg-dns-yyy-zzz, де yyy – ініціали студента, а zzz – номер варіанту, а в полі Name вказати ім'я домену. Після цього обрати Review + Create та ще раз натиснути Create. Після створення DNS Zone, всередині неї обрати DNS Management > Recordsets та зафіксувати значення запису @ типу NS. Значення будуть типу ns1-06.azure-dns.com., ns2-06.azure-dns.net., ns3-06.azure-dns.org., ns4-06.azure-dns.info.. Далі повернутись в налаштування домену на nic.ua, та вказати ці значення в якості кастомних NS servers та зберегти зміни. Для перевірки роботи змін, додати A-record у Recordsets, вказавши в полі Name yyy-zzz, де yyy – ініціали студента, а zzz – номер варіанту та в полі IP address – 127.0.0.1. Через певний час перевірити як ваша система розв'язує даний доменний запис, використовуючи nslookup. Виконати додаткову перевірку на сайті www.whatsmydns.net.
7. В головному пошуку на Azure Portal знайти Private DNS zones та обрати Create. Задати йому назву pvt. + назва створеного в пункті 5 домену. У вкладці Basics вказати доступну Subscription та Resource Group, створену в пункті 6. У вкладці Virtual Network Link задати довільну назву в полі Link name, вказати доступну Subscription, Resource Group з пункту 6 та обрати Virtual Network Campus2 та обрати опцію Enable auto registration. Після цього обрати Review + Create та ще раз натиснути Create.
8. Використовуючи Azure CLI, створити Network Peering між Campus1 та Campus2 та розгорнути віртуальні машини у цих мережах для перевірки роботи Network Peering (підказки будуть надані викладачем).

9. У створеній у пункті 7 Private DNS zone, додати довільний A-record, який буде посилатись на IP-адресу в мережі Campus2. Перевірити як розв'язується даний доменний запис в Azure Cloud Shell та у віртуальній машині, що була розгорнута в мережі Campus2. Зробити висновки по результатах тестування.
10. Виконати вправи на https://learn.microsoft.com/en-us/training/modules/control-network-traffic-flow-with-routes/3-exercise-create-custom-routes, https://learn.microsoft.com/en-us/training/modules/control-network-traffic-flow-with-routes/5-exercise-create-nva-vm, https://learn.microsoft.com/en-us/training/modules/control-network-traffic-flow-with-routes/6-exercise-route-traffic-through-nva.

**Контрольні запитання**

1. Що таке Azure Virtual Network і для чого вона використовується в хмарній інфраструктурі? Які параметри потрібно обов'язково вказати при її створенні?
2. Яка роль Subnet у віртуальній мережі Azure і чому важливо правильно планувати її адресний простір?
3. Поясніть, що таке Network Security Group (NSG). Які параметри визначають правило NSG, та як пріоритет впливає на обробку трафіку?
4. У чому відмінність між Application Security Group (ASG) та Network Security Group (NSG)? Коли доцільно використовувати ASG?
5. Навіщо створюється Azure DNS Zone? Яка різниця між публічною та приватною DNS зоною?
6. Що таке Virtual Network Peering? Які переваги він надає порівняно з традиційним маршрутизуванням?
7. Поясніть відмінність між Azure Load Balancer та Azure Application Gateway. На якому рівні моделі OSI працює кожен з них?
8. Для чого використовується Virtual Network Appliance (NVA)? Наведіть приклади сценаріїв, де її застосування є необхідним.
9. Що таке Azure Private DNS Zone, як вона пов'язана з Virtual Network, та навіщо використовується функція auto-registration?
10. Яким чином Azure Network Watcher допомагає у діагностиці мережевих з'єднань? Наведіть приклад інструмента (Connection Monitor, IP Flow Verify тощо) та його застосування.