

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

GRID-системи та хмарні технології

Методичні вказівки
до виконання лабораторних робіт 1 – 7
для підготовки здобувачів другого (магістерського) рівня
вищої освіти за спеціальністю
121 «Інженерія програмного забезпечення»

Київ 2024

УДК 004.042

G10

Укладач О.Л. Соловей, канд. техн. наук.

Рецензент: О.А. Поплавський, канд. техн. наук, доцент.

Відповідальна за випуск Т.А. Гончаренко, канд. техн. наук,
доцент.

*Затверджено на засіданні кафедри інформаційних технологій,
протокол № 9 від 27 березня 2024 року.*

В авторській редакції.

GRID-системи та хмарні технології : методичні вказівки до
G10 виконання лабораторних робіт / уклад. О.Л. Соловей. – Київ :
КНУБА, 2024. – 40 с.

Містять теоретичні відомості і рекомендації щодо виконання лабораторних робіт та вимоги до оформлення звіту з дисципліни “GRID-системи та хмарні технології”. Спрямовані на організацію самостійної роботи студентів.

Призначено для підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 121 «Інженерія програмного забезпечення» для практичного використання під час виконання лабораторних робіт.

Зміст

Загальні положення	4
Лабораторна робота №1	5
Лабораторна робота №2	9
Лабораторна робота №3	14
Лабораторна робота №4	18
Лабораторна робота №5	24
Лабораторна робота №6	30
Лабораторна робота №7	34
Література.	40

Загальні положення

Лабораторні роботи є логічним продовженням лекційного курсу з дисципліни «GRID-системи та хмарні технології» і є перехідною ланкою від теоретичного курсу до набуття практичних навичок роботи з хмарними технологіями платформи Azure.

Метою курсу є навчити студентів використовувати основні прийоми створення розподілених застосунків з урахуванням сучасних концепцій і тенденцій розвитку хмарних технологій.

Під час вивчення курсу студенти набувають знань та умінь фахового використання Грід-технології для вирішення складних науково-практичних завдань.

Кожна лабораторна робота містить наступні види робіт:

- аналіз умови задачі;
- виконання задачі у хмарному середовищі Azure;
- демонстрацію виконаного завдання;
- відповіді на контрольні запитання;
- складання і захист звіту.

Завершивши вивчення дисципліни, здобувач повинен вміти створювати віртуальні машини (ВМ) на платформі Microsoft Azure за допомогою Azure Services та Azure Cloud Shell; підключатись до віртуальної мережі Azure методом «точка – мережа»; створювати канали ExpressRoute для підключень між локальною мережею та «хмарою» Майкрософт; отримувати зображення Докера та розгортати екземпляр контейнера в Azure за допомогою порталу Azure; повинен вміти працювати зі сховищами даних Azure та вміти працювати з Azure Data Factory.

Лабораторна робота №1.

Створення віртуальної машини (ВМ) на платформі Microsoft Azure за допомогою Azure Services та Azure Cloud Shell

Мета роботи: здобути навички створення ВМ на порталі Azure за допомогою Azure Services та Azure Cloud.

Завдання

1. Створити віртуальну машину на порталі Azure.
2. Підключитися до віртуальної машини за допомогою протоколу віддаленого робочого столу (remote desktop protocol - RDP).
3. Створіть другу віртуальну машину на порталі Azure за допомогою Azure Cloud Shell.
4. Оформити звіт, який включає знімок екрана з результатом, отриманим на кожному кроці виконання лабораторної роботи; відповіді на контрольні запитання.

Теоретичні відомості

Віртуальні машини (ВМ) Azure – це масштабовані хмарні обчислювальні ресурси, призначені для полегшення процесу міграції існуючих Windows Server додатків у «хмару». Створення віртуальної машини на порталі Azure пов'язано з вивченням її конфігурації, а саме: регіону, розміру, типу сховища даних, конфігурації мережі, правил груп безпеки.

Регіон – це група «доступних зон», в яких знаходяться центри обробки даних. До рекомендованих регіонів належать регіони, в яких доступні майже всі сервіси Azure (такі регіони підтримують три різні доступні зони). Альтернативні регіони – це регіони з функціями «аварійного відновлення» (не підтримують різні доступні зони).

Розміри віртуальних машин згруповані за категоріями, починаючи із серії «В» для найпростішого тестування та закінчуючи серією «Н» 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.

За умовчанням для віртуальної машини Windows створюються два віртуальні жорсткі диски:

1) диск операційної системи – це основний диск, або C, з максимальною ємністю 2048 ГБ;

2) тимчасовий диск – цей диск призначений для тимчасового зберігання ОС чи додатків, позначається літерою D і, за замовчуванням, його розмір залежить від розміру віртуальної машини.

Під час створення віртуальної машини можна вибрати існуючу віртуальну мережу у вибраному регіоні або створити нову. Створення мережі разом із віртуальною машиною – найпростіший варіант, але в більшості ситуацій він неідеальний. Найкраще спланувати вимоги до мережі для всіх компонентів архітектури і створити структуру віртуальної мережі окремо. Після цього можна створити віртуальні машини та помістити їх у вже створені віртуальні мережі.

Віртуальна мережа необхідна для:

- 1) обміну даними між ресурсами Azure;
- 2) взаємодії із локальними ресурсами;
- 3) фільтрування мережного трафіку;
- 4) маршрутизації мережевого трафіку;
- 5) інтеграції зі службами Azure.

Azure Cloud Shell – призначена для створення ресурсів Azure та керування ними з командного рядка або за допомогою скриптів. Оскільки Cloud Shell створена для інтерактивних сеансів, оболонка автоматично завершує роботу після 20 хвилин бездіяльності. Azure Cloud Shell дозволяє створити та розгорнути ВМ за допомогою низки команд.

Хід роботи

1. Зайдіть на портал Azure – <https://portal.azure.com>
2. Створіть віртуальну мережу – визначте ім'я вузла «Бастіон»; початкова адреса – залиште за замовчуванням 10.0.0.0; розмір підмережі – залиште за замовчуванням /24(256 адресів).
3. Створіть віртуальну машину – у колонці «Усі служби», в меню порталу знайдіть і виберіть «Віртуальні машини», натисніть «Створити» та виберіть «Віртуальна машина Azure» зі спадного списку.
4. На вкладці «Основні» введіть інформацію з рис. 1. 1.

Settings	Values
Subscription	Use default supplied
Resource group	Нова група має назву вашого прізвища
Virtual machine name	myVM
Region	(US) East US
Availability options	No infrastructure redundancy options required
Image	Windows Server 2019 Datacenter - Gen2
Size	Standard D2s v3
Administrator account username	azureuser
Administrator account password (type in carefully!)	Pa\$\$w0rd1234
Inbound port rules -	**Allow select ports **
Select inbound ports	RDP (3389) and HTTP (80)

Рис. 1. 1. Інформація у процесі створення VM

5. Перейдіть на вкладку «Мережа» та визначте наступні параметри:
 - 1) визначте створену вами віртуальну мережу;
 - 2) визначте підмережу;
 - 3) в розділі «Вибрати входні порти» визначте HTTP (80) і RDP (3389).
6. Перейдіть на вкладку «Керування» та в її розділі «Моніторинг» виберіть таке налаштування – «вимкнути діагностику завантаження». Залиште решту значень за замовчуванням, а потім натисніть кнопку «Переглянути + створити» внизу сторінки.
7. Після проходження перевірки натисніть кнопку «Створити».
8. «Перейти до ресурсу», коли розгортання машини закінчиться успішно, натисніть «Підключити» та виберіть RDP зі спадного списку.
9. На сторінці «Підключення до віртуальної машини» збережіть параметри за замовчуванням для з'єднання із загальнодоступною IP-адресою через порт 3389 і натисніть «Завантажити файл RDP».
10. Відкрийте завантажений файл RDP (розташований у нижній лівій частині вашої лабораторної машини) і натисніть «Підключитися», коли з'явиться запит.
11. У вікні безпеки Windows увійдіть, використовуючи облікові дані адміністратора, які ви використовували під час створення віртуальної машини azureuser, і пароль Pa\$\$w0rd1234.

12. На порталі Azure відкрийте Azure Cloud Shell за допомогою значка у верхньому правому куті порталу Azure.



13. У вікні «Welcome to Azure Cloud Shell» виберіть «Cloud Shell».

14. У вікні «You have no storage mounted» натисніть «Advanced settings» і заповніть як показано нижче. Поле «storage account» має включати ваше прізвище.

* Subscription: Azure subscription 1

* Cloud Shell region: West Europe

[Hide advanced settings](#)

☐ Show VNET isolation settings

* Resource group: ☒ Create new ☐ Use existing

* Storage account: ☒ Create new ☐ Use existing

* File share: ☒ Create new ☐ Use existing

vm_group

cloudshellsolovei

shellstorage

[Further information about Cloud Shell storage and VNET isolation.](#)

Create storage Close

15. Отримуйте підтвердження в PowerShell: «Welcome to Azure Cloud Shell».

```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

MOTD: SqlServer has been updated to Version 22!

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/olha> 
```

16. Створіть віртуальну машину через набір команд New-AzVm - ResourceGroupName «myRGPS» – Name «myVMPS» – Location «East US» – VirtualNetworkName «myVnetPS» – SubnetName «mySubnetPS» – SecurityGroupName «myNSGPS» – PublicIpAddressName «myPublicIpPS».

17. Коли буде запропоновано, введіть ім'я користувача (azureuser) і пароль (Pa\$\$w0rd1234). Процес створення ресурсів для віртуальної машини буде розпочато і закінчено повідомленням «ProvisioningState: Succeeded».

18. Після створення віртуальної машини закрийте панель Cloud Shell сеансу PowerShell. На порталі Azure знайдіть віртуальні машини та переконайтеся, що ВМ запущено. Це може зайняти кілька хвилин.

Home > Virtual machines EPAM

+ Create Switch to classic Reservations Manage view Refresh Export to CSV Open query Assign tags Start Restart Stop Delete Services Maintenance

Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all Add filter

Showing 1 to 1 of 1 records. No grouping List view

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
myVMPS	Virtual machine	Azure subscription 1	myRGPS	West US	Running	Windows	Standard_D2s_v3	13.91.135.70	1

19. На порталі Azure відкрийте Azure Cloud Shell, клацнувши значок у верхньому правому куті порталу Azure. Отримайте інформацію про вашу віртуальну машину, включаючи назву, групу ресурсів, розташування та статус, виконавши команду: `Get-AzVM – name myVMPS – status | Format – Table – autosize`.

Контрольні запитання

1. Яка роль віртуальної машини Azure?
2. Що означає термін «доступна зона»?
3. На які категорії поділяються регіони Azure?
4. Поясніть, для чого використовують «домени збою» та «домени оновлення»?
5. Поясніть, за яким принципом визначається розмір ВМ Azure?
6. Поясніть конфігурацію сховищ ВМ Azure за замовченням.

Лабораторна робота №2.

Підключення до віртуальної мережі Azure методом «точка – мережа»

Мета роботи: здобути навички створення підключення до віртуальної мережі Azure методом «точка – мережа».

Завдання

1. Створити віртуальну мережу з VPN-шлюзом та виконати підключення «віддаленого робочого місця» до віртуальної машини в хмарному середовищі Azure методом «точка-мережа».
2. Оформити звіт, який включає знімок екрана з результатом, отриманим на кожному кроці виконання лабораторної роботи; відповіді на контрольні запитання.

Теоретичні відомості

Локальний комп'ютер можна підключити до віртуальної мережі за допомогою з'єднання типу «точка – мережа», через створення VPN-шлюзу. Конфігурація з'єднання типу «точка – мережа» представлена на рис. 2. 1 і складається з Azure VPN, Client VPN або OnPrem VPN – для встановлення віртуального приватного мережевого з'єднання; P2S VPN Tunnel, IPsec/IKEv2 VPN Tunnel – шлюзів для передачі даних; Radius Server, Domain Server – сервери, дані з яких використовують під час виконання аутентифікації клієнтів.

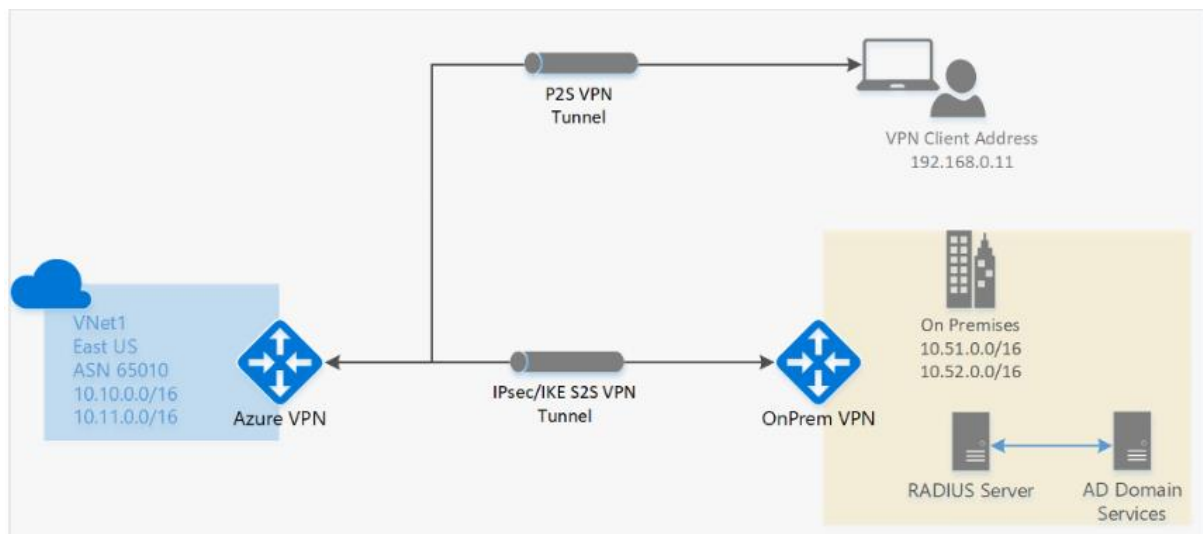


Рис. 2. 1. Конфігурація з'єднання типу «точка – мережа»

Обмін даними між комп'ютером та віртуальною мережею здійснюється через Інтернет за допомогою зашифрованого тунелю. Підключення типу «точка – мережа» можливе за одним із протоколів: OpenVPN – на основі SSL/TLS, підключення дозволяє трафіку проходити через брандмауер – порт 443; SSTP (Secure Socket Tunneling Protocol) – підключення за протоколом TLS (Transport Layer Security), підходить тільки для пристроїв Windows; IPsec/IKEv2 VPN – рішення VPN на основі стандартів Ipsec (IP Security – на відміну від SSL та TLS, працюють на мережевому рівні; IKE (Internet Key Exchange) – стандартний протокол набору протоколів IPsec, який використовується для забезпечення безпеки взаємодії у віртуальних приватних мережах). IKEv2 VPN використовують для пристроїв – на платформі Mac.

На момент встановлення підключення типу «точка – мережа» дані клієнта перевіряються VPN-шлюзом. Аутентифікація клієнтів виконується трьома способами:

- 1) перевірка сертифікату Azure клієнта;
- 2) перевірка дійсного облікового запису клієнта Azure, тобто перевірка Microsoft Entra ID;
- 3) перевірка облікового домену організації. Для перевірки облікового запису домену організації – додатково використовується сервер RADIUS, який інтегрований з сервером Azure з обліковими записами доменів організації.

Вимоги до конфігурації клієнта залежать від налаштувань VPN-клієнта, в табл. 2. 1 наведено конфігурації для способів аутентифікації способами 1– 2.

Таблиця 2. 1.

Вимоги до конфігурації клієнта

Спосіб аутентифікації	Тип тунелю	Файлова конфігурація	Налаштування VPN-клієнта
Сертифікат Azure	IKEv2, SSTP	Windows	власний VPN-клієнт
Сертифікат Azure	OpenVPN	Windows	Клієнт OpenVPN VPN-клієнт Azure
Сертифікат Azure	IKEv2, OpenVPN	macOS-iOS	macOS-iOS
Сертифікат Azure	IKEv2, OpenVPN	Linux	Linux
Microsoft Entra ID	OpenVPN (SSL)	Windows	Windows
Microsoft Entra ID	OpenVPN (SSL)	macOS	macOS

Хід роботи

1. Зайдіть на портал Azure – <https://portal.azure.com>.
2. Створіть віртуальну мережу, зазначивши необхідні параметри: «ім'я», «регіон», «IP-адреса».

Create virtual network ...

[Basics](#) [Security](#) [IP addresses](#) [Tags](#) [Review + create](#)

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual network name

Region ⓘ *

[Previous](#) [Next](#) [Review + create](#)

3. Створіть VPN-шлюз, зазначивши необхідні параметри: «підписку», «групу», «ім'я», «регіон», «тип шлюзу», «номер SKU», «віртуальну мережу», «діапазон адреси підмережі», вкажіть загальнодоступну IP-адресу, яка буде зв'язуватись з VPN-шлюзом.

Create virtual network gateway ...

[Basics](#) [Tags](#) [Review + create](#)

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group ⓘ

Instance details

Name * ✓

Region *

Gateway type * ⓘ ☒ VPN ☐ ExpressRoute

SKU * ⓘ

Generation ⓘ

Virtual network * ⓘ [Create virtual network](#)

Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range * ⓘ ✓
10.1.255.0 - 10.1.255.31 (32 addresses)

4. Визначте пул IP адрес – на сторінці «Конфігурація» додайте діапазон приватних IP адрес, які ви хочете використовувати. VPN-клієнт буде отримувати IP-адресу зі вказаного пулу. Мінімальне значення для налаштування маски – 29 біт у режимі «активний — пасивний» і 28 біт у режимі «активний – активний».

5. Визначте тип тунелю та спосіб аутентифікації.

The screenshot shows the Azure portal interface for configuring a Virtual Network Gateway (VNet1GW) for point-to-site connections. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Settings. Under Settings, the Configuration section is expanded, showing the Point-to-site configuration page. The main configuration area includes a search bar, a toolbar with Save, Discard, Delete, and Download VPN client buttons, and three configuration fields: Address pool (172.16.201.0/24), Tunnel type (IKEv2 and OpenVPN (SSL)), and Authentication type (Azure certificate). The Address pool field has a green checkmark, and the Tunnel type field is highlighted with a red box.

6. Перевірте VPN підключення – для цього виконайте команду `ipconfig/all`. В отриманій відповіді – перевірте, що отримана IP-адреса – це одина з IP адрес із визначеного вами пулу IP адрес.

```
PPP adapter VNet1:
  Connection-specific DNS Suffix .:
  Description.....: VNet1
  Physical Address.....:
  DHCP Enabled.....: No
  Autoconfiguration Enabled.....: Yes
  IPv4 Address.....: 172.16.201.3(Preferred)
  Subnet Mask.....: 255.255.255.255
  Default Gateway.....:
  NetBIOS over Tcpip.....: Enabled
```

7. Перевірте VPN підключення до ВМ, яку ви створили в лабораторній роботі №1. Для цього використовуйте підключення типу RDP.

Далі, для підключення «віддаленого робочого місця», введіть *IP адресу ВМ*.

Контрольні запитання

1. За якими протоколами можливе підключення «точка - мережа»?
2. Під час підключення «мережа – мережа» в чому різниця налаштувань VPN-тунелю: «активний – резервний» та «активний – активний»?
3. У яких випадках рекомендовано використовувати конфігурацію паралельного підключення?
4. В якому порядку оброблюються правила підмережевого інтерфейсу та інтерфейсу мережі для вхідного та вихідного трафіків?

Лабораторна робота №3.

Створення каналу ExpressRoute для підключень між локальною мережею та «хмарою» Майкрософт

Мета роботи: здобути навички створення каналу ExpressRoute для підключень локальною мережі до віртуальної мережі Azure.

Завдання

Створити канал ExpressRoute для підключень між локальною мережею та «хмарою» Майкрософт. Оформити звіт, який включає знімок екрана з результатом, отриманим на кожному кроці виконання лабораторної роботи; відповіді на контрольні запитання.

Теоретичні відомості

Канал ExpressRoute дозволяє підключення локальної мережі до Майкрософт «хмарних» послуг, таких як Office 365, Dynamics 365 та інші через партнерів. Архітектура з'єднання каналом ExpressRoute визначає наступні компоненти: партнери встановлюють підключення до кінцевої точки розташування ExpressRoute шляхом пірингу локальних мереж із віртуальними – ці з'єднання називають ExpressRoute Circuit (рис. 3. 1). ExpressRoute Circuit – забезпечує фізичне підключення для передачі даних через «прикордонні» канали постачальника (Partner Edge) на

«прикордонні» канали Майкрософт (Microsoft Edge). «Прикордонні» канали Майкрософт надають доступ в область Microsoft.

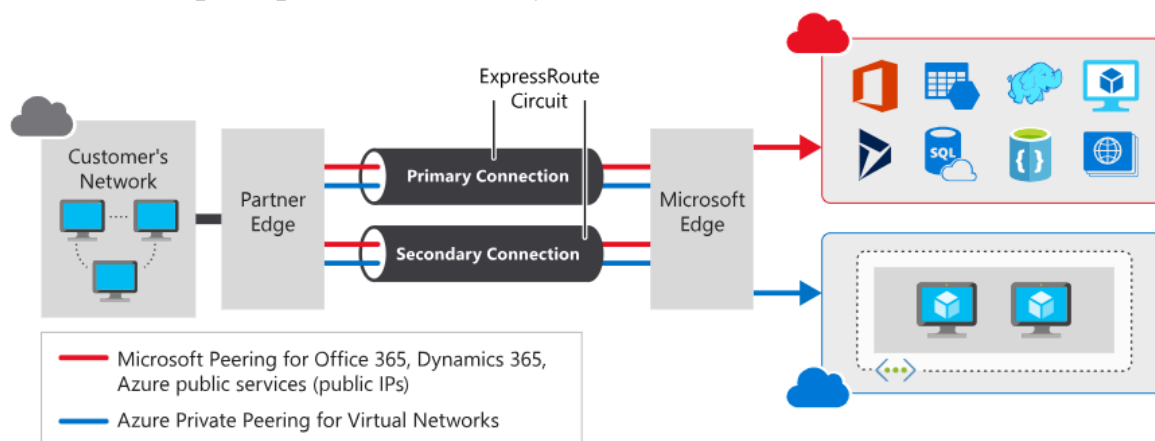


Рис. 3. 1. Архітектура з'єднання каналом ExpressRoute

Канал ExpressRoute є логічним зв'язком між локальною інфраструктурою та «хмарою» Майкрософт через постачальника послуг зв'язку. Канал, який однозначно ідентифікується стандартним GUID, називається ключем служби (s-key).

Ключ служба – це єдиний фрагмент інформації, який передається між Майкрософт постачальником послуг підключення та локальною мережею у разі співвідношення між каналом ExpressRoute і ключем 1:1. Канали ExpressRoute можуть підтримувати три незалежних типу пірингу: приватний і Microsoft Azure, загальний. Кожен канал має фіксовану пропускну здатність (50 Мбіт/с, 100 Мбіт/с, 200 Мбіт/с, 500 Мбіт/с, 5 Гбіт/с, 10 Гбіт/с) і підтримується з постачальником підключенням та піринговим розташуванням. Вибрана пропускну здатність поширюється на всі пірингові канали. Кількість префіксів IPv4, IPv6 та діапазон IP адрес залежно від типу пірингу наведено в табл. 3. 1.

Таблиця 3. 1

Кількість префіксів IPv4, IPv6 та діапазон IP адрес залежно від типу пірингу

	Приватний	Microsoft Azure	Загальний
Кількість префіксів IPv4, для одного пірингу	400 за замовчування	200	200
Кількість префіксів IPv6,	100	200	-

для одного пірингу			
--------------------	--	--	--

Закінчення таблиці 3. 1

Діапазон IP адрес	допустима IP-адреса у глобальній мережі	Загальнодоступні IP-адреси	Загальнодоступні IP-адреси
IP-протокол	IPv4, IPv6	IPv4, IPv6	IPv4

Хід роботи

1. Зайдіть на портал Azure – <https://portal.azure.com>.
2. Створіть канал ExpressRoute, визначивши необхідні параметри: «групу ресурсів», «ім'я», «регіон». Перейдіть в розділ конфігурації і вкажіть: «тип порту», «постачальника послуги», «розташування пірингу», виберіть «стандартний» SKU, модель оплати послуги – «з врахуванням трафіку».

Create ExpressRoute

Basics **Configuration** Tags Review + create

ExpressRoute circuits can connect to Azure through a service provider or directly to Azure at a global peering location. [Learn more about circuit types](#)

Port type * ☒ Provider ☐ Direct

Create new or import from classic * ☒ Create new ☐ Import

Provider *

Peering location *

Bandwidth *

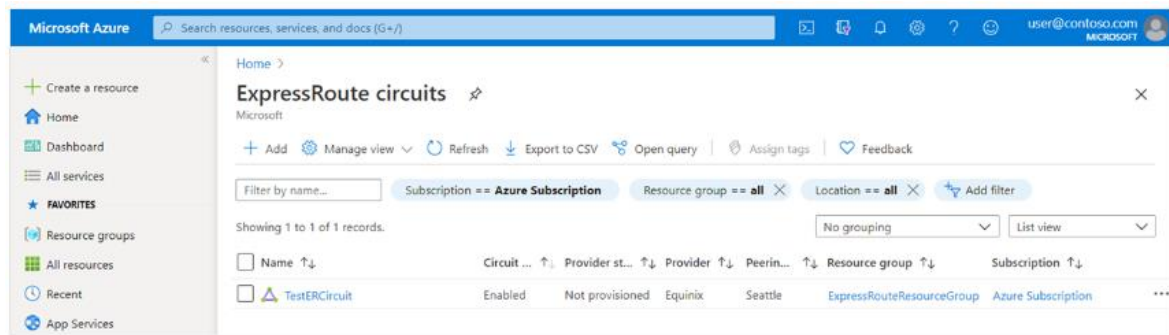
SKU * ☐ Standard ☒ Premium

Billing model * ☐ Metered ☒ Unlimited

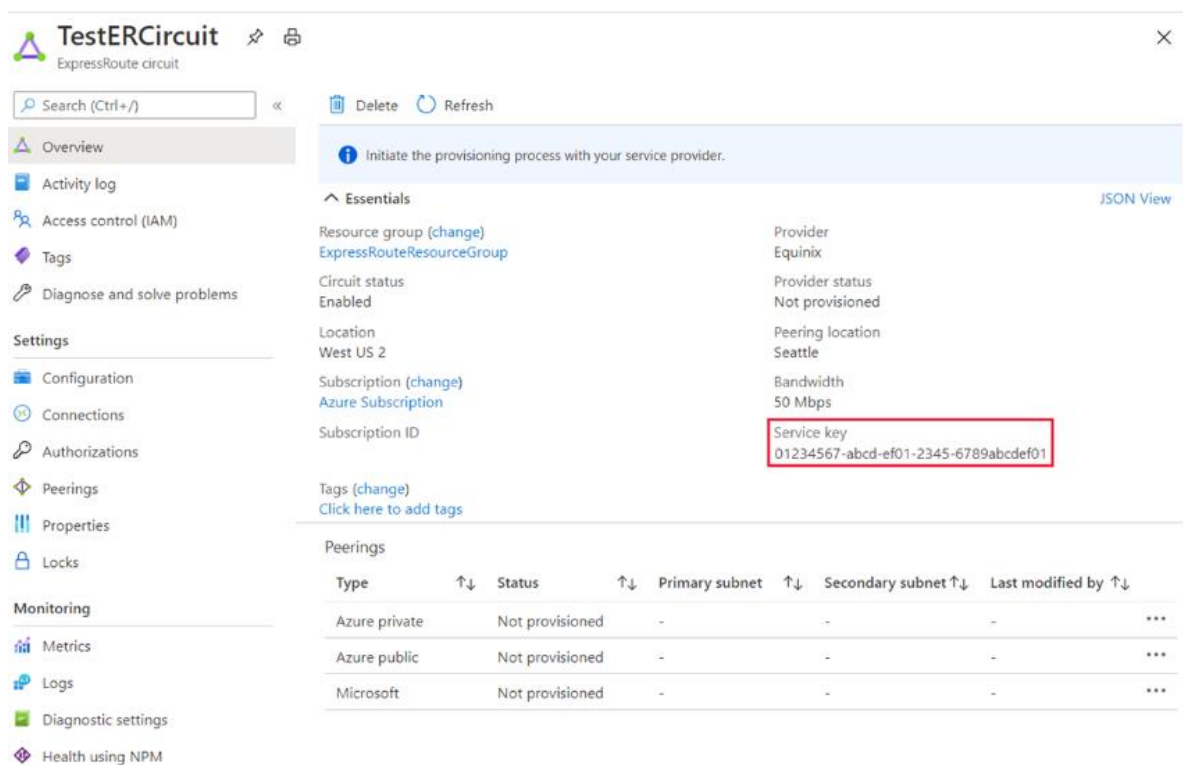
Allow classic operations ☐ Yes ☒ No

Review + create < Previous Next : Tags >

3. Створіть канал, натиснувши «Review+Create».
4. Перевірте, що канал створено, – для цього перейдіть до розділу «ExpressRoute» circuits.



5. Оберіть створений вами канал і перевірте, що для нього визначений Security ID, – цей ключ передається постачальнику для отримання послуг ExpressRoute.



Контрольні запитання

1. Поясніть відмінності в конфігурації типів пірингу?
2. Наведіть розміри префіксів загальнодоступних IP-адрес?
3. З чого складається архітектура паралельного підключення типу «точка – мережа» і ExpressRoute?
4. Які типи «ExpressRoute» з'єднання вам відомі?
5. Які переваги «ExpressRoute» з'єднання?

Лабораторна робота №4.

Отримання зображення Докера та розгортання екземпляра контейнера в Azure за допомогою порталу Azure

Мета роботи: здобути навички отримання зображення Докера та розгортання екземпляра контейнера в Azure за допомогою порталу Azure.

Завдання

1. Отримати зображення Докера.
2. Розгорнути екземпляр контейнера в Azure за допомогою порталу Azure.
3. Оформити звіт, який включає знімок екрана з результатом отриманим на кожному кроці виконання лабораторної роботи; відповіді на контрольні запитання.

Теоретичні відомості

Архітектура контейнеру Docker в хмарному середовищі Azure складається з Docker Hub, Docker Host (Докер Вузол) та контейнерів (рис. 4. 1).

Сервер Docker – це керуюча програма, яка називається `dockerd`, що відповідає на запити клієнта за допомогою REST API Docker та може взаємодіяти з іншими програмами, а також відповідає за відстеження життєвого циклу контейнерів.

Docker Hub – це реєстр контейнерів Docker. *Реєстри Docker* – це репозиторії, які служать для зберігання та розповсюдження створюваних образів контейнерів. Docker Hub є загальнодоступним реєстром Docker, який використовується за умовчанням для керування зображеннями контейнера.

Зображення контейнера – це пакет, що містить програмне забезпечення, бібліотеки, конфігураційні файли і т.п. Під час запуску він стає контейнером. Зображення контейнера є незмінним. Єдиний спосіб змінити зображення – створити нове.

Докер файл – це текстовий файл, який включає інструкції щодо компіляції та запуску зображення Докера.

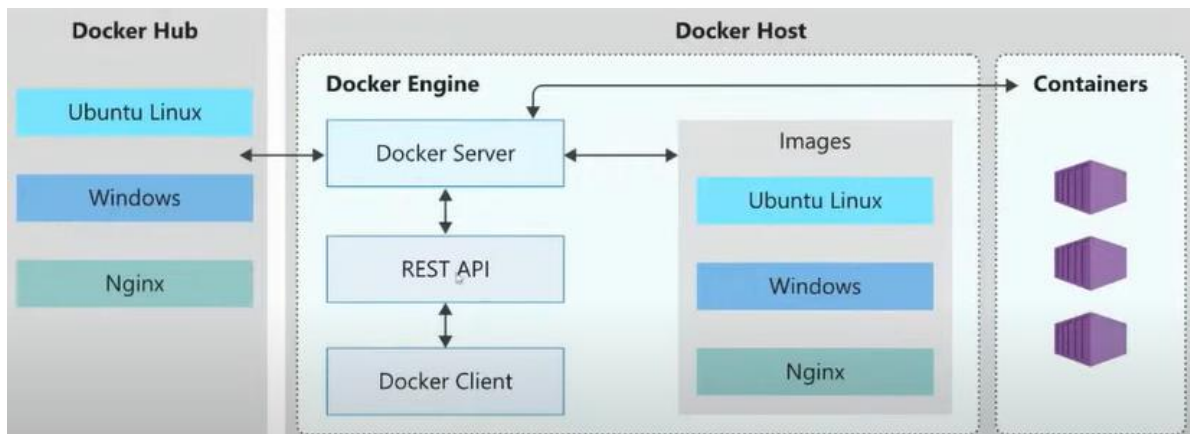


Рис. 4. 1. Архітектура контейнеру Docker в хмарному середовищі Azure

Під час розгортання контейнеру в Azure вказується джерело зображення в конфігурації розгортання або шаблонах. Потім середовище виконання контейнера (наприклад, Docker) використовує цю інформацію, щоб отримати вказане зображення контейнера з джерела та запустити його як контейнер у вашому середовищі Azure.

Хоча контейнер використовує ядро операційної системи сервера, але не отримує необмежений доступ до ядра. Натомість контейнер отримує ізольоване, а в деяких випадках віртуалізоване уявлення системи.

Наприклад, контейнер може звертатися до віртуалізованої версії файлової системи та реєстру, але будь-які зміни стосуються лише контейнера та видаляються під час його зупинки. Щоб зберегти дані, контейнер може підключити постійне сховище.

У табл. 4. 1 наведено типи програм, які не можна перемістити в контейнер Windows. В табл. 4. 2, навпаки, визначені типи програм «ідеальні» для контейнеризації.

Таблиця 4. 1

Типи програм, які не можна перемістити в контейнер Windows

Типи програм	Причини
Додатки, для яких потрібні можливості робочого столу	Контейнери не підтримують графічний інтерфейс користувача (GUI), навіть якщо в самому додатку немає графічного інтерфейсу користувача, але є установник, який його використовує
Програми, що використовують	Оскільки протокол віддаленого робочого столу (RDP) призначений для створення

протокол віддаленого робочого столу (RDP)	інтерактивного візуального сеансу, обмеження графічного інтерфейсу користувача, описане вище, застосовується і до нього
Програми з базами даних	Контейнери не передбачають збереження даних. Такі типи програм можна контейнеризувати лише в тому випадку, якщо ви ізолюєте потрібні дані з одного сеансу в наступному та зберігаєте їх у постійному сховищі
Програми, які використовують .NET Framework версії 2.0 або пізнішої	Для підтримки .NET Framework потрібні певні образи контейнерів, при цьому підтримуються лише пізніші версії, а версії, які передують 2.0, не підтримуються в принципі

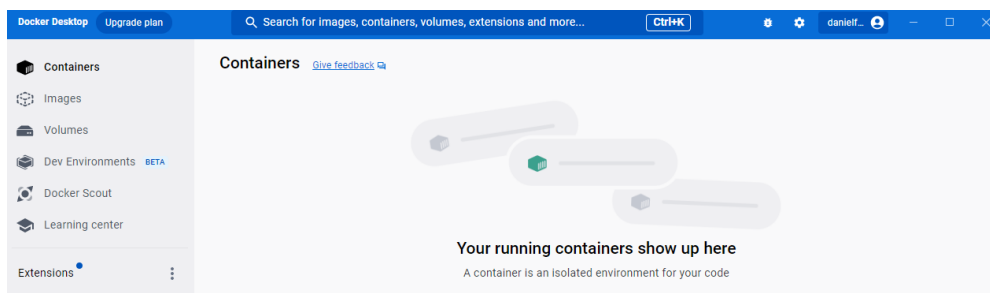
Таблиця 4. 2

Типи програм, які «ідеальні» для контейнеризації

Типи програм	Причини
Консольні програми	Консольні програми, які не мають обмежень за графічним інтерфейсом користувача
Служби Windows	Оскільки це фонові процеси, які не потребують прямої взаємодії з користувачем
Веб-програми	Веб-програми по суті є фоновими службами, які прослуховують певний порт, і тому є відмінними кандидатами для контейнеризації, бо вони можуть використовувати переваги масштабованості, пропоновані контейнерами

Хід виконання роботи

1. Розгорніть Docker на своєму комп'ютері.



2. Увійдіть на портал Azure – <https://portal.azure.com>.
3. Створіть екземпляр контейнера – на вкладці «Основи» (Basics), вкажіть необхідні параметри для контейнера. (Ім'я контейнера має включати ваше прізвище; Мережа – порт – 80, порт протокол – TCP).

Basics Networking Advanced Tags Review + create

Azure Container Instances (ACI) allows you to quickly and easily run containers on Azure without managing servers or having to learn new tools. ACI offers per-second billing to minimize the cost of running containers on the cloud.
[Learn more about Azure Container Instances](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ
[Create new](#)

Container details

Container name * ⓘ filatovcontainer ✓

Region * ⓘ (US) East US

Availability zones (Preview) ⓘ None

SKU Standard

4. Натисніть «Перевірити+Створити», щоб розпочати процес автоматичної перевірки. Після завершення перевірки натисніть «Створити».

✓ Validation passed

Basics Networking Advanced Tags Review + create

Basics

Subscription	Azure subscription 1
Resource group	
Region	East US
Container name	filatovcontainer
SKU	Standard
Image type	Public
Image	mcr.microsoft.com/azuredocs/aci-helloworld:latest
OS type	Linux
Memory (GiB)	1.5
Number of CPU cores	1
GPU type (preview)	None
GPU count	0

Networking

Networking type	Public
Ports	80 (TCP)
DNS name label scope reuse	Any reuse (unsecure)

Create < Previous Next > [Download a template for automation](#)

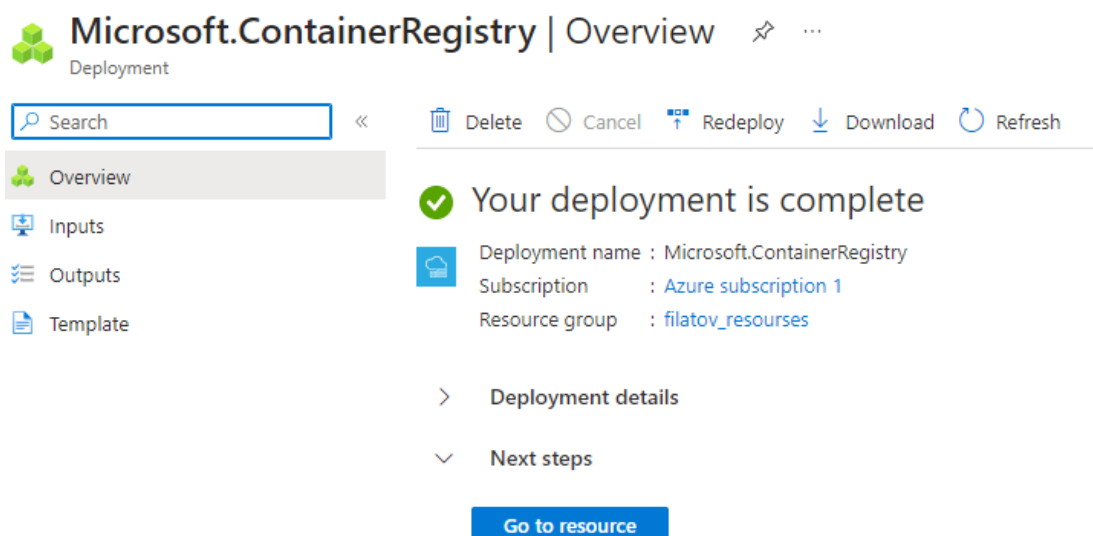
5. «Перейдіть до ресурсу», скопіюйте IP адресу та виконайте в новому браузері – маєте побачити привітання «Welcome to Azure Container Instances»!

6. Перегляньте DockerFile, для цього в PowerShell виконайте наступні команди, `git clone https://github.com/Azure-Samples/aci-helloworld.git`. Зайдіть в папку – **Cd aci-helloworld**. Виконайте команду – **Code**.

```
PS /home/azuresdk/aci-helloworld> git clone https://github.com/Azure-Samples/aci-helloworld.git
fatal: destination path 'aci-helloworld' already exists and is not an empty directory.
PS /home/azuresdk/aci-helloworld> Cd aci-helloworld
PS /home/azuresdk/aci-helloworld> code .
PS /home/azuresdk/aci-helloworld>
```

FILES	Dockerfile
4 .git - branches - hooks - info - logs - objects - refs - config - description - HEAD - index - packed-refs - app .gitignore - Dockerfile	<pre> 1 FROM node:8.9.3-alpine 2 RUN mkdir -p /usr/src/app 3 COPY ./app/* /usr/src/app/ 4 WORKDIR /usr/src/app 5 RUN npm install 6 CMD node /usr/src/app/index.js 7</pre>

7. Створіть «Реєстр Контейнерів». Для цього на панелі «Усі служби» знайдіть і виберіть «Реєстр Контейнерів» (container registry) і натисніть «Створити».



8. Перейдіть до ресурсу та в меню Налаштування («Settings») активуйте параметр «Адміністратор» (Admin user), в результаті відобразиться ім'я користувача та пароль для реєстру контейнерів. Запишіть Ім'я реєстру (Registry name), Сервер входу (Login server), Ім'я користувача (user name) та Пароль (password) для реєстру контейнерів.

Registry name	filatovregistry	
Login server	filatovregistry.azurecr.io	
Admin user ⓘ	☒	
Username	filatovregistry	
Name	Password	Regenerate
password	AOz0pPrAUHTwUDLjzi4ePpBwTlplUrtITwvXFMf62W+ACRD...	
password2	A/hE8E07FS5DWBSE9OXD/AVeOHVBdArsu9x7YkfS0c+ACR...	

9. В PowerShell виконайте наступні команди, попередньо замінивши <registry-name> на ваше ім'я реєстру.

```
docker tag reservationsystem:latest <registry-name>.azurecr.io/reservationsystem:latest
```

10. Перевірити, що «зображення» створене, введіть команду.

Docker image ls

11. В результаті на екрані відобразиться

REPOSITORY	TAG	IMAGE ID
CREATED	SIZE	
reservationsystem	latest	a56281e7038f 4
minutes ago	1.76GB	
<registry-name>.azurecr.io/reservationsystem		latest
a56281e7038f	4 minutes ago	1.76GB

12. Вкажіть сервер входу, виконавши команду – docker login <login-server>.

13. Поверніться на портал Azure – <https://portal.azure.com>.

14. Перейдіть до вашого ресурсу «Реєстр Контейнерів» і зайдіть в меню репозиторій – маєте побачити зображення «reservationsystem».

Контрольні запитання

1. Що таке Докер? З яких компонентів складається архітектура Докера?
2. Для чого призначений екземпляр контейнера?
3. Чи треба робити зміни в коді програмного доданку під час його контейнеризації? Якщо ні, то яка технологія це забезпечує?
4. У чому принципова різниця між ВМ і контейнерами?
5. Чи можна контейнеризувати доданок із графічним інтерфейсом? Доданок з базою даних?
6. Які програми є «ідеальними» для контейнеризації?
7. Чим відрізняються зона DNS від домену DNS?
8. Що означає захоплення піддомену? Як уникнути захоплення піддомену?

Лабораторна робота №5. Робота зі сховищами даних Azure

Мета роботи: здобути навички роботи зі сховищами даних Azure.

Завдання

1. Створити обліковий запис сховища Azure.
2. Побудувати процес відправки даних протоколом HTTP у хмарне сховище та збереження отриманих даних у хмарному сховищі.
3. Оформити звіт, який включає знімок екрана з результатом, отриманим на кожному кроці виконання лабораторної роботи; відповіді на контрольні запитання.

Теоретичні відомості

Azure об'єднує чотири служби сховища даних: BLOB-об'єкти Azure; файли Azure; черги Azure; таблиці Azure. Об'єднання служб даних в обліковий запис зберігання дозволяє керувати ними як групою. Параметри, які вказуються під час створення облікового запису, або зміни, які вносяться після створення, застосовуються до всіх служб облікового запису. Під час видалення облікового запису зберігання видаляються всі дані, що зберігаються всередині.

Обліковий запис зберігання визначає політику, яка застосовується до всіх служб сховища в обліковому записі. Так, параметр «реплікація» – визначає стратегію копіювання даних для захисту від збоїв обладнання та стихійних лих. Мінімальна реплікація називається локально надлишковим сховищем (LRS), що забезпечує захист від збоїв обладнання, але не від події, здатної вивести з ладу весь центр обробки даних. Більш надійна альтернатива – геонадлишкове сховище (GRS), при цьому налаштуванні копіювання даних виконується в різні центри обробки даних по всьому світу.

Параметр «рівень доступу» визначає, як швидко дані можуть бути отримані з «хмарного» сховища.

«Гарячий рівень доступу» оптимізовано для зберігання даних, до яких часто звертаються або які часто змінюють. «Холодний рівень доступу» оптимізовано для зберігання даних, до яких рідко звертаються або змінюють. «Гарячий рівень доступу» підтримується лише для великих двійкових об'єктів, він задається за замовчуванням.

Параметр «Потрібне безпечне переміщення» визначає прийом запитів лише від безпечних з'єднань, при цьому будь-які запити, виконані за протоколом HTTP, будуть відхилені. У разі включення зворотного видалення великих об'єктів для облікового запису зберігання необхідно вказати термін зберігання віддалених об'єктів у діапазоні від 1 до 365 днів.

Термін зберігання показує, як довго дані залишаються доступними після видалення або перезапису. Годинник для зберігання запускається в момент видалення або перезапису об'єкта.

Azure Logic Apps – це застосунок, який дозволяє автоматизувати робочі процеси та інтегрувати різні програми, служби та системи в хмарних і локальних середовищах. Logic Apps легко інтегрується з іншими службами хмарного середовища Azure, такими як функції Azure, службова шина Azure, база даних SQL Azure тощо, це дозволяє створювати складні робочі процеси, поєднуючи потужність кількох компонентів Azure.

Створення складного робочого процесу в застосунку Azure Logic Apps починається з визначення способу, яким буде ініційовано початок робочого циклу, тобто триггеру. Тригер представляє подію або умову, яка запускає робочий процес, наприклад, тригери типу: «Коли надходить електронний лист», «Коли новий елемент додається до списку SharePoint» або «Коли надходить запит HTTP» – починають робочий цикл, як тільки відбулась визначена подія. Наступними елементами робочого циклу є дії та з'єднувачі, які визначають сам процес та його кінцевий результат.

Хід виконання роботи

1. Увійдіть на портал Azure.
2. На панелі «Усі служби» знайдіть і виберіть «Служба сховища» (Storage Account) і натисніть «Створити».

The screenshot shows the 'Create new storage account' form in the Azure portal. At the top, there are two dropdown menus: 'Subscription' (selected: 'Azure subscription 1') and 'Resource group' (selected: '(New) filatov_resources', with a 'Create new' link below it). Below these is the 'Instance details' section. It includes a text input for 'Storage account name', a dropdown for 'Region' (selected: '(US) East US', with a 'Deploy to an edge zone' link below it), a radio button selection for 'Performance' (selected: 'Standard: Recommended for most scenarios (general-purpose v2 account)', with 'Premium: Recommended for scenarios that require low latency.' as an alternative), and a dropdown for 'Redundancy' (selected: 'Geo-redundant storage (GRS)', with a checked checkbox for 'Make read access to data available in the event of regional unavailability.' below it).

3. Надайте основні відомості для створення нової служби сховища (storage account name – має включати ваше прізвище). В розділі «Безпека» («Security») виберіть «Enable storage account key access»; в розділі – «Мережі» («Network connectivity») виберіть «Enable public access from all networks».

Security

Configure security settings that impact your storage account.

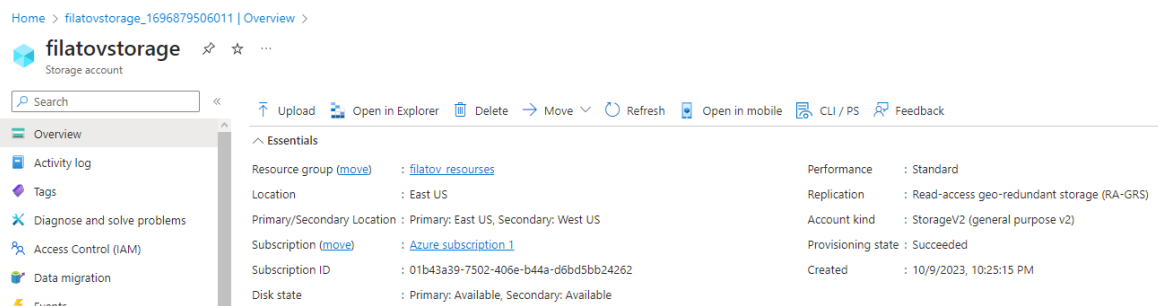
Require secure transfer for REST API operations ☒

Allow enabling anonymous access on individual containers ☐

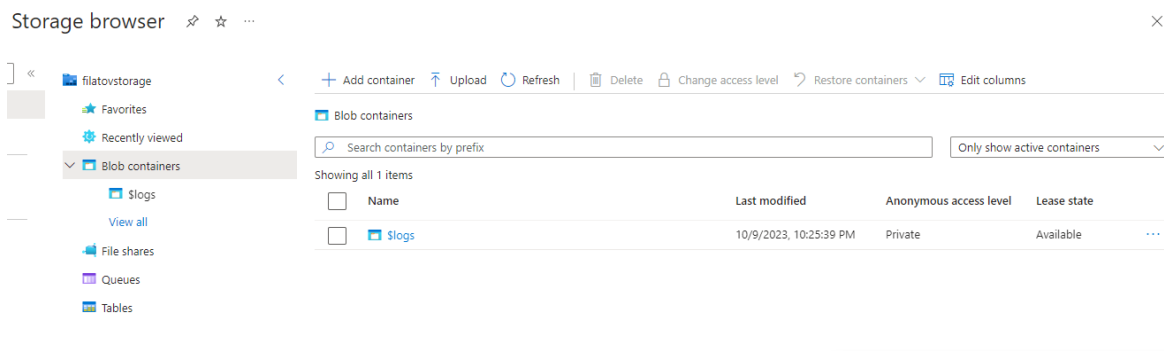
Enable storage account key access ☒

Default to Azure Active Directory authorization in the Azure portal ☐

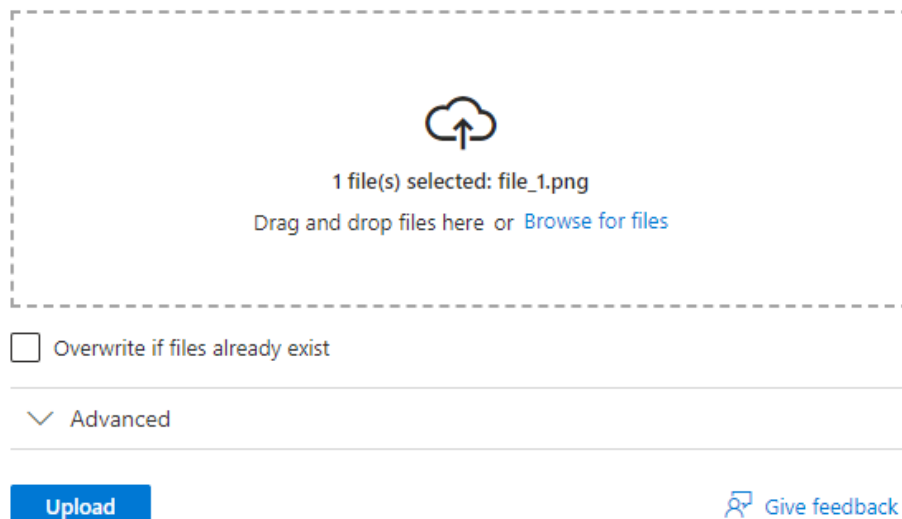
4. Натисніть «Переглянути та створити», щоб розпочати процес автоматичної перевірки. Після завершення розгортання перейдіть за посиланням «Перейти до ресурсу».



5. Перейдіть до меню «Storage Browser/Blob containers».



6. Створіть власний Blob Container, визначне рівень доступу – «anonymous read access for containers and blobs». Завантажте файл у створений контейнер.



1 file(s) selected: file_1.png

Drag and drop files here or [Browse for files](#)

☐ Overwrite if files already exist

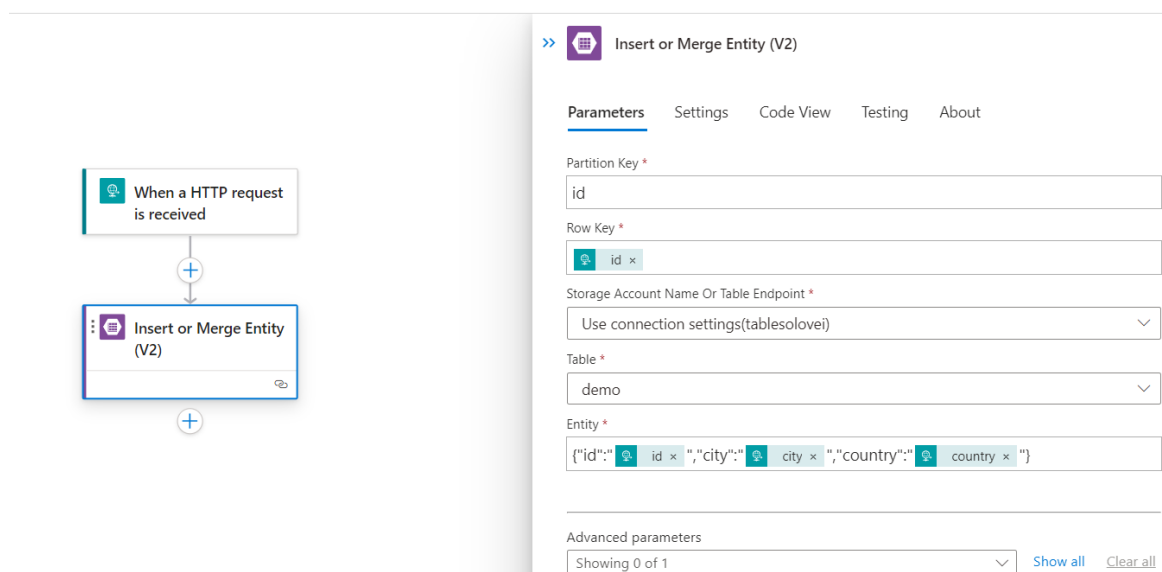
Advanced

Upload [Give feedback](#)

7. Скопіюйте URL адресу завантаженого файлу та виконайте її в новому вікні браузера – файл має стати доступний для читання та скачування.

8. Створить власну таблицю в «Службі сховища», яка має включати, щонайменше 3 рядки.

9. Створить процес в Logic Apps конструкторі - додайте метод «When a HTTP request is received» та визначте схему JSON, яка буде описувати ваш файл з даними, METHOD=POST. Додайте метод «Insert or Merge Entity» та визначте всі обов'язкові поля (рис. 5. 1).



When a HTTP request is received

Insert or Merge Entity (V2)

Insert or Merge Entity (V2)

Parameters Settings Code View Testing About

Partition Key *

id

Row Key *

id x

Storage Account Name Or Table Endpoint *

Use connection settings(tableslovei)

Table *

demo

Entity *

{"id": "id x", "city": "city x", "country": "country x"}

Advanced parameters

Showing 0 of 1 [Show all](#) [Clear all](#)

Рис. 5. 1. Приклад для визначення методу «Insert or Merge Entity»

10. Збережіть створений процес. Після збереження скопіюйте HTTP POST URL.

11. Відкрийте Postman Web та заповніть всі дані для нового POST request. (рис. 5. 2). Натисніть «Send» та впевнитесь, що Status = 202.

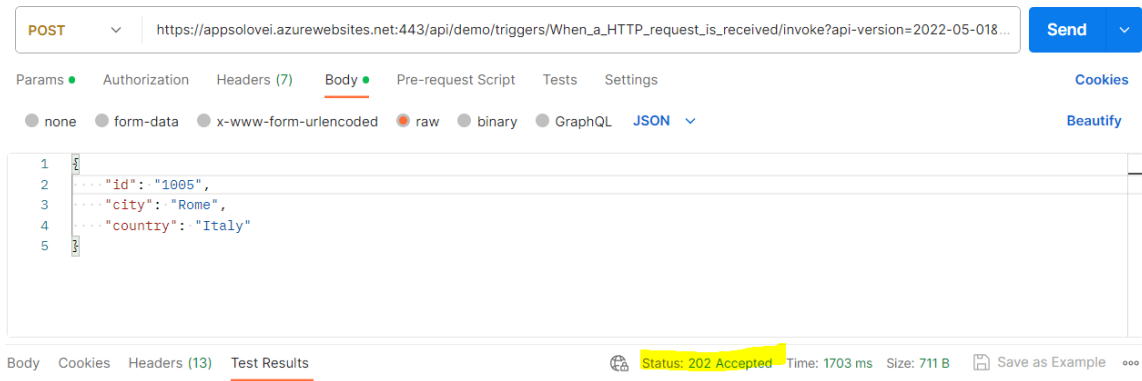


Рис. 5. 2. Приклад для визначення методу POST в Postman Web

12. Відкрийте Logic Apps Azure Overview Run History та перевірте, що процес виконано без помилок (рис. 5. 3).

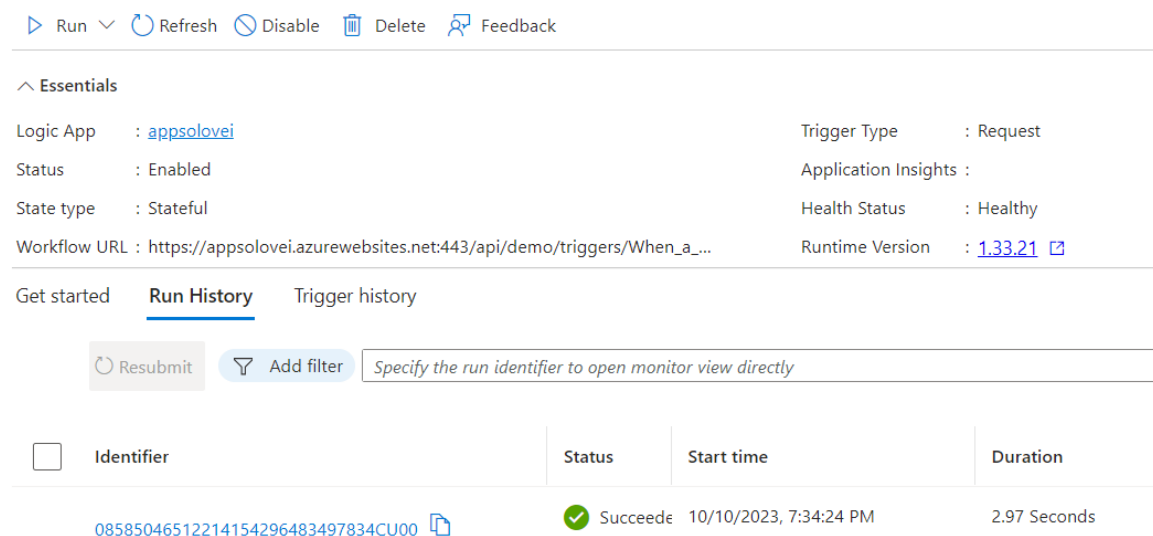


Рис. 5. 3. Перевірка статусу виконаного процесу в Logic Apps Azure Overview Run History

13. Перейдіть до сховища даних, перевірте, чи запис додано, чи оновлено (рис. 5. 4).

☐ Advanced filters

Showing all 3 items

☐	PartitionKey	RowKey	Timestamp	city	country
☐	id	1	2023-10-10T11:50:15.93...	London	UK
☐	id	1005	2023-10-10T16:34:26.74...	Rome	Italy
☐	id	2	2023-10-10T11:52:20.87...	Paris	France

Рис. 5. 4. У базу даних додано новий запис з RowKey=1005

Контрольні запитання

1. Які 4 служби об'єднує сховище Azure?
2. Який параметр облікового запису зберігання визначає які служби даних можна використовувати у вашому обліковому записі зберігання?
3. Які типи стратегій копіювання даних для захисту від збоїв обладнання та стихійних лих включають параметр облікового запису зберігання? У чому різниця між типами?
4. Які доступні рівні доступу до даних в обліковому записі зберігання? Коли треба застосовувати якій рівень?
5. Які три параметри застосовуються до самого облікового запису, а не до даних у ньому?
6. Протягом якого терміну можна відновити видалені дані, якщо при створенні облікового запису було визначено термін зворотного видалення 7 днів?
7. Є два відеофайли, які зберігаються як великі двійкові об'єкти. Один із відеофайлів критично важливий, інший відеофайл – ні. Скільки облікових записів зберігання вам потрібно створити і з якими типами стратегії копіювання даних для захисту від збоїв?

Лабораторна робота №6.

Робота з Azure Cosmos DB

Мета роботи: здобути навички роботи з Azure Cosmos DB за допомогою мови запитів SQL і клієнтських бібліотек для .NET, JavaScript, Python і Java.

Завдання

Визначити рівень споживання ресурсів під час роботи з таблицями Azure Cosmos DB.

Теоретичні відомості

Azure Cosmos DB – це платформа баз даних, яка є сукупністю логічно взаємопов'язаних баз даних, розподілених у комп'ютерній мережі. Програмні доданки працюють з базами даних Azure Cosmos DB за допомогою інтерфейсів (API), які розроблені також для таких баз даних, як MongoDB, PostgreSQL, Apache Cassandra, Apache Gremlin.

Залежно від типу бази даних інтерфейси зберігають дані в різних форматах, так:

- API для MongoDB зберігає дані у структурі документа у форматі BSON (Binary JSON);
- API для Cassandra зберігає дані у схемі, орієнтованій на стовпці;
- API для Gremlin дозволяє зберігати дані у вигляді ребер та вершин;
- API для таблиць зберігає дані у форматі «ключ-значення».

Azure Cosmos DB пропонує доступ до даних зі швидким відгуком під час читання та запису на глобальному рівні. Для забезпечення такого рівня доступності дані копіюються між регіонами.

Копіювання розподілених баз даних для забезпечення високого рівня їх доступності та низької затримки передбачає компроміс між узгодженістю читання та такими параметрами, як доступність, час затримки та пропускна спроможність. Такий підхід пов'язаний з проблемою забезпечення узгодженості даних. Наприклад, для копіювання даних з регіону US до регіону India потрібно 2 хв, протягом цього часу користувач з регіону US буде читати дані, які відрізняються від даних, доступних для регіону India, тобто дані будуть неузгоджені. Для забезпечення узгодженості даних Azure Cosmos DB пропонує п'ять чітко визначених рівнів «узгодженості даних» від сильних до слабких:

1. Рівень узгодженості «Суворий» (Strong).
2. Обмежений із запізненням (Bounded staleness).
3. Сеанс (Session).
4. Узгодженість префіксів (Consistent prefix).
5. Рівень узгодженості «Підсумковий» (Eventual).

Таким чином, під час роботи з даними, які зберігаються в Azure Cosmos DB, важливо визначити, який із визначених типів «узгодженості даних» підтримується для того, щоб правильно оцінювати очікувану «неузгодженість».

Для оцінювання завантаженості CPU під час роботи з Azure Cosmos DB використовують міру «одиниця запиту» за секунду (оз/с). 1 оз/с потрібна для читання 1кБ даних з Azure Cosmos DB. На рівень споживання ресурсів під час роботи з Azure Cosmos DB впливають наступні фактори:

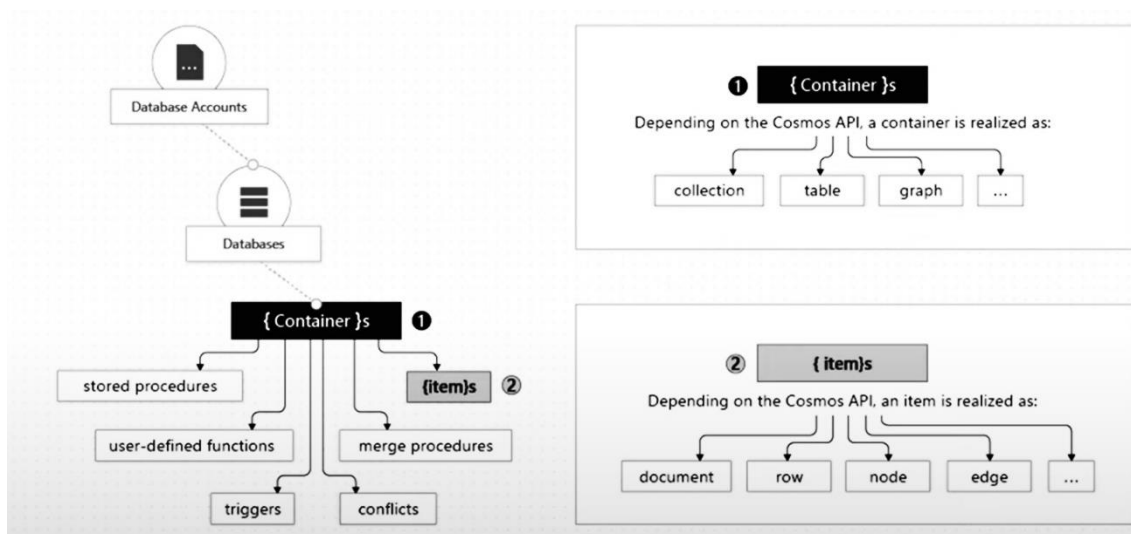
1) Розмір елемента. У міру збільшення розміру елемента число оз/с, необхідне для читання чи запису елемента, також збільшується.

2) Індексація елементів. За замовчуванням кожен елемент у таблиці Azure Cosmos DB автоматично індексується, таким чином зменшення кількості індексованих елементів сприяє зменшенню оз/с.

3) Узгодженість даних. «Суворий» рівень узгодженості потребує приблизно вдвічі більше оз/с під час виконання операцій читання порівняно з іншими рівнями узгодженості.

4) Типи операцій читання та шаблони запитів. Чинники, що впливають на вартість операцій запитів, такі: кількість результатів запиту; кількість предикатів; характер предикатів; кількість функцій, що визначаються користувачем; розмір вихідних даних; розмір результуючого набору; проекції.

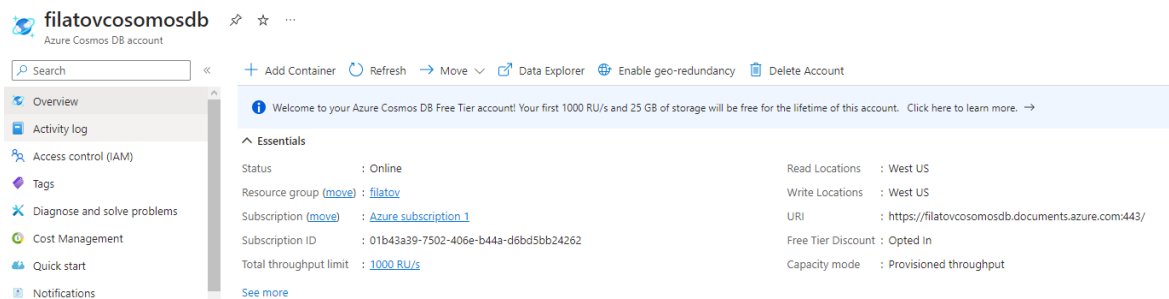
Структура бази даних Azure Cosmos DB представлена контейнерами, де кожен контейнер складається з даних, процедур, функції та тригерів.



Дані одного контейнера розподіляються по різних «логічних секціях» для забезпечення масштабування даних. Логічні секції формуються з урахуванням значення ключа секції, який є у кожного елемента у контейнері. Усі елементи у логічній секції мають однакове значення ключа секції. Крім ключа секції, кожен елемент в контейнері також має ідентифікатор, який є унікальним в межах логічної секції. Поєднання ключа секції та ідентифікатора елемента створює індекс, що однозначно визначає елемент.

Хід виконання

1. Створіть обліковий запис Azure Cosmos DB.



2. Виділіть один об'єкт, який є частиною вашого програмного доданка з предмету «Системна інженерія програмного забезпечення» і опишіть його властивості за допомогою JSON документа. (1 JSON має включати не менше 3-х секцій, кожна з яких включає більш ніж один об'єкт).

3. За допомогою однієї з клієнтських бібліотек створіть базу даних Cosmos DB та контейнер.

Взаємодія з Cosmos DB починається з екземпляра класу CosmosClient. Для створення екземпляра об'єкта клієнту потрібен обліковий запис та відповідно заповнити змінні середовища в файлі конфігурації. Провести перевірку клієнта можливо, якщо передавати облікові дані в ClientSecretCredential або використовувати DefaultAzureCredential:

```

from azure.cosmos import CosmosClient
from azure.identity import ClientSecretCredential, DefaultAzureCredential

import os
url = os.environ['ACCOUNT_URI']
tenant_id = os.environ['TENANT_ID']
client_id = os.environ['CLIENT_ID']
client_secret = os.environ['CLIENT_SECRET']

# Using ClientSecretCredential
aad_credentials = ClientSecretCredential(
    tenant_id=tenant_id,
    client_id=client_id,
    client_secret=client_secret)

# Using DefaultAzureCredential (recommended)
aad_credentials = DefaultAzureCredential()

client = CosmosClient(url, aad_credentials)

```

Після перевірки CosmosClient можна працювати з будь-яким ресурсом в облікового запису. Наведений нижче фрагмент коду створює базу даних API SQL, яка використовується за умовчанням, якщо під час виклику `create_database` не вказано API.

```

from azure.cosmos import CosmosClient, exceptions
import os

URL = os.environ['ACCOUNT_URI']
KEY = os.environ['ACCOUNT_KEY']
client = CosmosClient(URL, credential=KEY)
DATABASE_NAME = 'testDatabase'
try:
    database = client.create_database(DATABASE_NAME)
except exceptions.CosmosResourceExistsError:
    database = client.get_database_client(DATABASE_NAME)

```

Для створення контейнера з параметрами за замовчуванням необхідно скористатись методом

container = database.create_container (id=CONTAINER_NAME, partition_key=PartitionKey (path="/productName")).

4. Завантажте JSON документ; визначте ключ контейнера.
5. Визначте ОЗ/с, необхідні для виконання SQL запитів:
 - 1) читання з фільтром;
 - 2) читання з 2-х таблиць;
 - 3) оновлення значень.

Контрольні запитання

1. Що означає узгодженість даних?
2. Які типи узгодженості даних підтримує Azure Cosmos DB?

3. Що означає, коли для типу узгодженості даних «Обмежена із запізненням» обрано інтервал часу $T=10$ с ?
4. Який об'єм даних можна прочитати, витративши 100 ОЗ/с.
5. Яким чином Cosmos DB забезпечує горизонтальне масштабування?
6. Наведіть приклад, коли невдало визначений ключ секції призводить до зниження продуктивності бази даних.

Лабораторна робота №7.

Робота з Azure Data Factory

Мета роботи: здобути навички роботи з компонентами Azure Data Factory для організації процесу отримання, перетворення та завантаження даних в хмарному середовищі Azure.

Завдання

1. Створіть процес вилучення, перетворення та завантаження (Extract, Transform, Load – ETL) даних в Azure Data Factory.
2. Оформити звіт, який включає знімок екрана з результатом, отриманим на кожному кроці виконання лабораторної роботи; відповіді на контрольні запитання.

Теоретичні відомості

Фабрика даних Azure – це керована хмарна служба, створена для реалізації складних гібридних ETL процесів. До ключових компонентів Фабрики даних Azure належать:

- 1) конвеєр;
- 2) дії;
- 3) набори даних, які визначають тип даних, для яких створюється ETL процес;
- 4) пов'язані служби, які визначають способи підключення до джерел та сховищ даних.

Зазначені компоненти для реалізації процесу ETL застосовуються наступним чином: компонент конвеєр об'єднує логічну групу дії, які

можуть бути пов'язані послідовно або виконуватись паралельно і незалежно одна від одної. На рис. 7. 1 схематично представлено конвеєр, який об'єднує послідовні дії копіювання даних з одного сховища (зелений колір) в інше (синій колір).

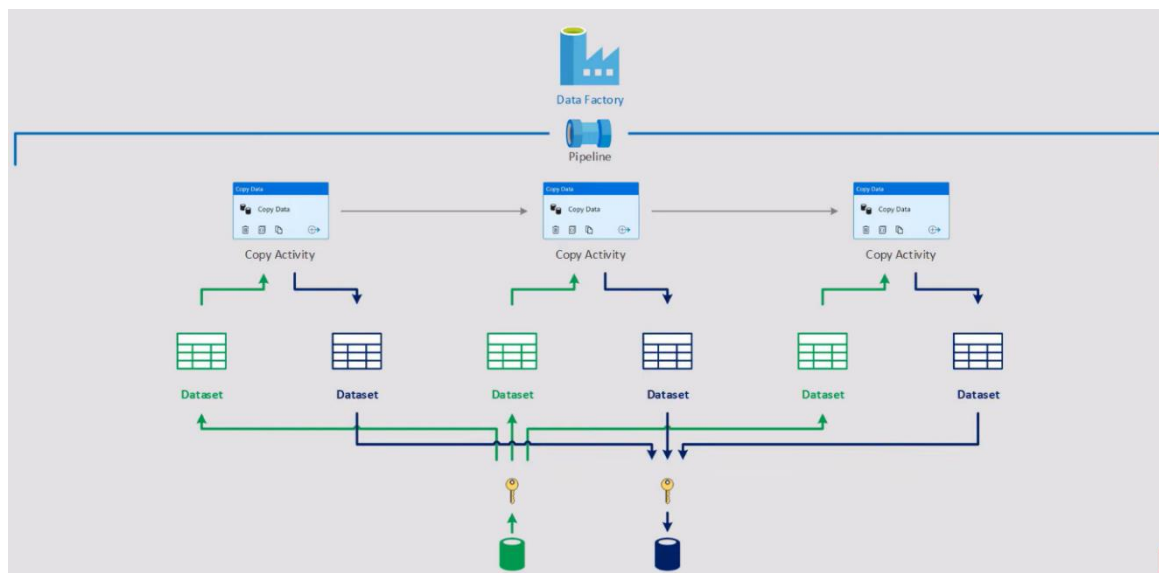


Рис. 7. 1. Конвеєр який об'єднує послідовні дії копіювання даних

Дії для копіювання даних використовують для копіювання даних між локальними та хмарними сховищами, відповідно до процесу:

- 1) отримання даних з джерела даних;
- 2) виконання дій серіалізації або десеріалізації, стиснення або розпакування, співставлення стовпців тощо;
- 3) запис даних до приймача або цільового сховища даних.

Налаштування правил відмовостійкості для дії копіювання визначаються відповідно до табл. 7. 1.

Таблиця 7. 1

Налаштування правил відмовостійкості для дії копіювання

Тип відмовостійкості	Збій виникає у випадку, коли	Управління
fileMissing	дані копіюються з файлу, який видаляється іншими доданками	True: інші файли копіюються, окрім того, який видаляється. False: копіювання даних зупиняється

fileForbidden	дані копіюються з файлу, який вимагає вищого рівня дозволів, ніж у налаштованого підключення.	True: необхідно скопіювати решту файлів, пропускаючи ці. False: ви повинні перервати копіювання у разі виникнення проблеми з дозволами для папок або файлів
dataInconsistency	під час копіювання неузгоджених даних між вихідним та цільовим сховищами	True: необхідно скопіювати решту даних, пропускаючи неузгоджені. False: Необхідно перервати копіювання у разі виявлення неузгоджених даних
invalidFileName	під час копіювання, якщо імена файлів неприпустимі для цільового сховища	True: потрібно скопіювати інші файли, пропускаючи файли з неприпустимими іменами. False: необхідно перервати копіювання у разі виявлення неприпустимих імен файлів

Потоки даних дозволяють реалізовувати логіку перетворення даних без написання коду. Потоки даних створюються так само, як конвеєри та набори даних. Створений потік даних складається з 3-х складових:

- панель управління,
- граф потоку даних,
- панель конфігурації.

Потік зазвичай починається з визначення джерела, за необхідності можна додати будь-яку кількість джерел. Всі додані джерела з'єднуються за допомогою перетворення з'єднання, пошуку або об'єднання.

Тип джерела визначається параметром «Набір даних» або «Вбудований набір даних».

Об'єкти «Набір даних» – це сутності, які багаторазово використовуються, також в інших потоках даних і діях, таких як копіювання.

Об'єкти «Набір даних» особливо корисні під час використання фіксованої схеми. Вбудовані набори даних рекомендуються під час використання гнучких схем, одноразових екземплярів або параметризованих джерел. Панель конфігурації визначає схему вихідних даних та правила трансформації даних.

Хід виконання роботи

1. Створіть XML-документ для опису компонент користувацького інтерфейсу програмного доданка з дисципліни «Системна інженерія програмного забезпечення» (приклад у табл. 7. 2.) та завантажте в Azure Blob Storage.

Таблиця 7. 2

Фрагмент XML-документ для опису компонент користувацького інтерфейсу

```
<form>
info= «Main form»/>
  <description info= «Booking a room in hotel»/>
  <content info= «Content of main form»>
    <inputField name= «Text_input» lable= «Enter name»
type= «text»/>
    <inputField name= «Text_input» lable= «Enter
surname» type= «text»/>
    <inputField name="Date_input" lable="Enter start
date" type="date"/>
    <inputField name="Date_input" lable="Enter end
date" type="date"/>
    <inputField name="Text_input" lable="E-mail"
type="text"/>
    <inputField name="Number_input" lable="Enter
phone number" type="number"/>
    <inputField name="Button" lable="Submit"
type="submit"/>
  </content>
</form>
```

2. Створіть таблиці в Azure SQL database для збереження даних XML- документу, окремо в 2-х таблицях: в 1-шу таблицю треба

завантажити дані 1-го рівня ієрархії XML-документу; в 2-гу – 2-го рівня ієрархії XML-документу (в таблиці 2 наведено приклад SQL команд для створення таблиць)

Таблиця 2

Команди для створення таблиць в Azure SQL database

```
CREATE TABLE input_fields (  
  id INT NOT NULL IDENTITY(1,1),  
  name VARCHAR(40) NOT NULL,  
  label VARCHAR(40) NOT NULL,  
  type VARCHAR(40) NOT NULL,  
  PRIMARY KEY (id)  
);
```

```
CREATE TABLE form_description (  
  id INT NOT NULL IDENTITY(1,1),  
  info VARCHAR(40) NOT NULL,  
  PRIMARY KEY (id)  
);
```

3. За допомогою потоку перетворення даних в Azure Data Factory завантажте XML- документ з Azure Blob Storage, виконайте «нормалізацію» даних XML- документу та збережіть в підготовлених таблицях Azure SQL database. (приклад створено потоку в Azure Data Factory наведено на рис. 1).

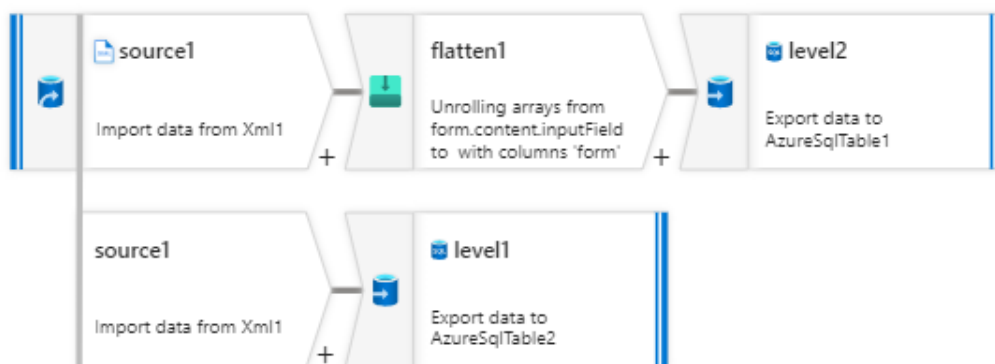


Рис. 1. Схема потоку даних для реалізації процесу ETL

Контрольні запитання

1. Які ключові компоненти включено в Azure Data Factory?

2. Коли варто використовувати дію «Копіювання даних», а коли «Потік перетворення даних»?

3. Який параметр конфігурації дії копіювання треба використовувати для запобігання збою при копіюванні даних, при умові, що збій виник коли «Файли, які копіюються службою, видаляються іншими додатками»?

4. Яку функцію «Потоку перетворення даних» треба використовувати для зміни типу стовбця?

5. Які типи з'єднань підтримуються Azure Data Factory для об'єднання даних з різних джерел?

Список літератури

1. Sreeram PK. Azure Serverless Computing Cookbook: Build and monitor Azure applications hosted on serverless architecture using Azure functions. Packt Publishing Ltd; 2020 Jun 19. <https://www.packtpub.com/en-ua/product/azure-serverless-computing-cookbook-9781800206601?type=print>
2. Seara DA, Milano F, Dominici D. Microsoft Azure Data Solutions-An Introduction. Microsoft Press; 2021 Jul 14. <https://www.oreilly.com/library/view/microsoft-azure-data/9780137252725/>
3. L'Esteve RC. The Definitive Guide to Azure Data Engineering: Modern ELT, DevOps, and Analytics on the Azure Cloud Platform. Apress; 2021. <https://www.oreilly.com/library/view/the-definitive-guide/9781484271827/>
4. Seara DA, Milano F. Exam Ref DP-900 Microsoft Azure Data Fundamentals. Microsoft Press; 2021 Mar 12. <https://www.oreilly.com/library/view/exam-ref-dp-900/9780137252145/>
5. Хмарні технології [Електронний ресурс]. – Режим доступу: <http://j.parus.ua/ua/358>.
6. Корольова Ю.І. Переваги та недоліки використання 88 хмарних технологій підприємствами України [Електронний ресурс]. – Режим доступу: <http://www.bsfa.edu.ua/files/konf2013/62.p.df>.
7. Юрчишин В.Я. Хмарні та ґрід-технології [Електронний ресурс]. – Режим доступу: <https://ela.kpi.ua/server/api/core/bitstreams/6db9b134-8c26-4687-9f98-7d3c8e85096e/content> .

Навчально-методичне видання

GRID-системи та хмарні технології

Методичні вказівки
до виконання лабораторних робіт 1 – 7
для підготовки здобувачів другого (магістерського) рівня
вищої освіти за спеціальністю
121 «Інженерія програмного забезпечення»

Укладач **Соловей** Ольга Леонідівна

Випусковий редактор *Л.С. Тавлуй*
Комп'ютерне верстання *Л.В. Лабунець*

Підписано до друку 24.10.2024. Формат 60 x 84_{1/16}
Ум. друк. арк. 2,32. Обл.-вид. арк. 2,5.
Електронний документ. Вид. № 130/III-24.

Видавець і виготовлювач:
Київський національний університет будівництва і архітектури

Проспект Повітряних Сил, 31, Київ, Україна, 03037

Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи ДК № 808 від 13.02.2002

