Лабораторна робота №7

РОБОТА З AZURE STORAGE ACCOUNT: AZURE BLOB STORAGE ТА AZURE FILES

Мета: ознайомитися зі службою Azure Storageта її ключовими компонентами – сховищами об'єктів Blob і файловими сховищами Azure Files. Навчитися створювати обліковий запис сховища, налаштовувати захист, життєвий цикл та політики збереження, працювати з контейнерами та файловими спільними ресурсами, обмежувати мережевий доступ до Storage Account і керувати доступом за допомогою SAS-посилань.

Хід роботи

1. Перевірити політику Allowed resource deployment regions та обрати один з регіонів.
2. У порталі Azure знайдіть Resource groups і створіть нову групу з ім'ям rg-sa-xxx-yyy-zzz, де:
   - xxx – скорочена назва обраного регіону;
   - yyy – ініціали студента;
   - zzz – номер варіанту.
3. В Azure Portal знайдіть **Storage accounts** і виберіть **+ Create**. На вкладці **Basics** заповніть:
   - **Subscription**: ваша навчальна підписка;
   - **Resource group**: rg-sa-xxx-yyy-zzz;
   - **Storage account name**: унікальне ім'я з 3–24 символів (літери та цифри);
   - **Region**: обраний регіон;
   - **Performance**: Standard;
   - **Redundancy**: Geo-redundant storage (GRS);
   - Увімкніть пункт

     «Make read access to data available in the event of regional unavailability»
4. На вкладці **Advanced** ознайомтесь з доступними параметрами та прийміть налаштування за замовчуванням. На вкладці **Networking** тимчасово

вимкніть **Public network access** (Inbound access), щоб обліковий запис був доступний лише через приватні мережі.

5. Прийміть стандартні налаштування вкладок **Data protection** та **Encryption** і натисніть **Review + create**, а після перевірки – **Create**. Дочекайтеся створення та відкрийте ресурс.
6. Перегляньте вкладку **Overview** новоствореного **Storage Account** – зверніть увагу, що обліковий запис підтримує **Blob containers**, **File shares**, **Queues** та **Tables**. Перейдіть у **Security + Networking** та оберіть **Networking**. Зверніть увагу, що **Public network access** вимкнено, як і було задано під час створення Storage Account. Оберіть **Manage** та змініть **Public network access** налаштування на **Enabled**, змініть на **Public network access scope** на **Enable from selected networks**. У полі **IPv4 Addresses**, оберіть **Add your client IPv4** address та збережіть зміни.
7. У розділі **Data management** відкрийте **Redundancy** і перегляньте інформацію про Primary та Secondary data center locations.
8. У Lifecycle management створіть правило **Movetocool**, яке переноситиме об’єкти Blob Cool access tier, якщо вони не змінювались 30 днів. Для решти параметрів залиште стандартні значення.
9. У **Data storage** > **Containers**, натисніть **+ Add container** і створіть контейнер **data**. Рівень публічного доступу залиште **Private**.
10. Відкрийте пункт **Access policy** для контейнера, оберіть **Add policy** та налаштуйте політику незмінності (**Immutable Blob Storage**):
    - **Policy type**: Time-based retention;
    - **Retention period**: 180 днів.
11. Поверніться на сторінку контейнера і натисніть **Upload**. Виберіть невеликий файл зі свого комп’ютера. У розділі Advanced встановіть:
    - **Blob type**: Block blob;
    - **Block size**: 4 MiB;
    - **Access tier**: Hot;
    - **Upload to folder**: securitytest;

- **Encryption scope**: залиште default.

Завантажте файл та переконайтеся, що він з’явився в контейнері.

12. Скопіювати URL-адресу завантаженого файлу (**Properties** > **URL**) і перевірте в режимі InPrivate: сторінка повинна повертати очікувану помилку **ResourceNotFound** або **PublicAccessNotPermitted**.

13. Щоб надати контрольований доступ, для файлу оберіть **Generate SAS** та встановити наступні параметри:

- **Signing key**: Key 1;
- **Permissions**: Read;
- **Start date**: попередній день;
- **Start time**: поточний час;
- **Expiry date**: наступний день;
- **Expiry time**: поточний час.

14. У своєму цьому ж Azure Storage Account перейти в **File shares** та натиснути **+ File share**. Дайте йому ім’я **share1**, залишити рівень доступу **Transaction optimized** та вимкніть резервне копіювання та натиснути **Create**.

15. Відкрити **Storage browser** та переконатись, що **share1** доступний. Створити всередині одну чи кілька папок та завантажити файл. Зверніть увагу, що наразі обмежень доступу немає.

16. Створити обмеження мережевого доступу до Storage Account.

Створіть віртуальну мережу: у порталі знайти **Virtual networks**, натиснути **+ Create**, обрати Resource group rg-sa-xxx-yyy-zzz, задайте ім’я **vnet1** і залишити параметри за замовчуванням. Після створення відкрити ресурс.

17. У розділі **Settings** обрати **Service endpoints**, натисніть **Add**, в полі **Service** обрати **Microsoft.Storage**, а в полі **Subnets** – **Default**. Натиснути **Add**.

18. Повернутись до сторінки Storage Account. У меню **Security + networking** відкрити **Networking**, натиснути **Manage** та змінити **Public network access** на **Enabled from selected networks**. Додати віртуальну мережу **vnet1** зі стандартною підмережею та видалити свою поточну IP-адресу зі списку дозволених. Зберегти зміни.

19. Оновити сторінку Storage browser та спробувати відкрити Container або File share з поточного комп'ютера. Очікуваний результат – помилка, оскільки дозволено доступ лише з мережі **vnet1**.

20. Створити **Virtual Machine** у тому ж регіоні, що і **vnet1**. В головному пошуку на Azure Portal знайти **Virtual Machine** та обрати опцію **Create**. Далі заповнити поля:

Basics (змінювати тільки вказані поля):

- **Subscription**: обрати підписку Azure for Students;
- **Resource group**: оберіть існуючу Resource group, де знаходяться Virtual Network **vnet1** та Storage Account;
- **Virtual machine name**: vm-xxx-yyy-zzz-001, де 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;
- **Region**: обрати серед доступних, що вказані в політиці регіонів, яка застосовується для навчальних Subscriptions Azure for Students;
- **Availability options**: No infrastructure redundancy required;
- **Security type**: Trusted launch virtual machines;
- **Image**: Ubuntu Server 24.04 LTS – x64 Gen2;
- **VM architecture**: x64;
- **Size:** Standard_B2s – 2 vcpus, 4GiB memory;
- **Username:** аналогічний username, як і в Azure Cloud Shell, типу ki251_mvv;
- **Password:** довільний безпечний пароль не менше 12 символів, що буде містити букви, цифри, спец.символи (у звіті не вказувати);
- **Public inbound ports:** Allow selected ports;
    - **Select inbounds ports:** SSH (22)**;**
- ***Усі інші поля залишити за замовчуванням***
- Перейти у вкладу **Review + Create** та після валідації натиснути **Create**.

21. Активувати **Service endpoint** для **Virtual Network**, що була створена в

процесі створення **Virtual Machine**. Перейти у **Resource group**, де знаходиться попередньо створена **Virtual Machine** та знайти **Virtual Network**, що було створено разом з **Virtual Machine**, перейти до її налаштувань (**Settings** > **Service endpoints**). Якщо **Virtual Machine** створено у тому ж регіоні, що й **Storage Account**, то у полі **Service** обрати **Microsoft.Storage**, якщо ж створено у іншому регіоні, то **Microsoft.Storage.Global**. В полі **Subnets** обрати єдину доступну **Subnet** та натиснути **Add**.

22. У налаштуваннях **Storage Account** змінити мережевий доступ, вказавши **Virtual Network**, в якій знаходиться **Virtual Machine**. Повернутись у налаштування раніше створеного **Storage Account, Security + Networking** > **Public network access** > **Manage**. У вкладці **Virtual Networks**, напроти **vnet1**, клікнути на еліпсис (…), обрати Remove та натиснути **Save**, зберігши зміни. Повернутись у **Security + Networking** > **Public network access** > **Manage** > **Virtual Networks** > **Add a virtual network** > **Add existing virtual network** та обрати наступне:

- **Subscription**: доступна Subscription Azure for Students;
- **Virtual networks**: обрати Virtual network, в якій знаходиться Virtual machine;
- **Subnets**: обрати єдину доступну Subnet у тій Virtual network.

Натиснути **Add** та зберегти зміни, натиснувши **Save**.

23. Підключитись локально або з Azure Cloud Shell по SSH до **Virtual Machine**. В глобальному пошуку Azure Portal знайти Virtual Machines та клікнути по доступній у списку **Virtual Machine**. На вкладці Overview знайти **Primary NIC public IP** та скопіювати цю адресу. Далі в терміналі виконати наступну команду:

```
ssh <ім’я користувача, яке було задано в пункті 20>@<попередньо скопійована публічна IP-адреса>
```

В результаті команда буде виглядати наступним чином:

```
ssh username@1.2.3.4
```

24. Підключившись до **Virtual Machine**, переконатись у наявному доступі до **Storage Account**. Виконати наступну команду, використовуючи у 13 пункті **SAS URL** (за необхідності його перегенерувати його):

```
curl -vOJ '<SAS URL>'
```

В результаті має бути отримано завантажений в поточній директорії Blob.

25. Порівняти SHA256 Hash Sum завантаженого файлу з файлом на локальній машині, який було завантажено в Azure Blob Storage.

Відобразити sha256 sum файлу, що було завантажено на віртуальній машині, виконавши наступну команду:

```
sha256sum <ім'я файлу, що було завантажено>
```

На локальній машині, якщо вона від управлінням Windows, можна використати командлет:

```
Get-FileHash <ім'я локальноно файлу> -Algorithm SHA256
```

Переконатись, що hash співпадає.

26. Підключити **File Share** до **Virtual Machine**. В Azure Portal в глобальному пошуку знайти **Storage Accounts** та клікнути по доступному **Storage Account**. Далі перейти у **Data storage** > **File shares**, де має бути попередньо створена **share1**. Клікнути по ній та далі обрати **Connect** > **Linux** > **Show Script**. Скопіювати значення згенерованого скрипту та виконати його в SSH-сесії підключення до **Virtual Machine**. Виконати команду `mount` та переконатись, що File Share було успішно підключено, знайшовши приблизно наступний вивід.

```
//sagwcmvv001.file.core.windows.net/share1 on /media/share1 type cifs
(rw,relatime,vers=3.1.1,cache=strict,upcall_target=app,username=sagwcmvv001,uid=0,noforceuid,gid=0,noforcegid,addr=20.209.177.70,file_mode=0755,dir_mode=0755,soft,persistenthandles,nounix,serverino,mapposix,mfsymlinks,reparse=nfs,nativesocket,symlink=mfsymlinks,rsize=1048576,wsize=1048576,bsize=1048576,retrans=1,echo_interval=60,nosharesock,actimeo=30,closetimeo=1)
```

З даного виводу можна побачити, що **File Share** було змонтовано у `/media/share1`.

27. Перейти за шляхом, куди було змонтовано **File Share** та створити файл з інформацією про операційну систему.

```
cd /media/share1 # шлях може відрізнятись
sudo bash -c 'printf
"Hostname: %s\nUsername: %s\nDistro: %s\nArchitecture: %s\nLocal
IP: %s\nPublic IP: %s\n" \
"$(hostname)" "$(whoami)" \
"$(. /etc/os-release 2>/dev/null && echo "$PRETTY_NAME")" \
"$(uname -m)" \
"$(hostname -I | awk '\''{print $1}'\'')" \
"$(curl -s ifconfig.me)" \
> os-info.txt'
```

28. Переконатись, що файл було завантажено до **File Share**. Оскільки, попередньо через мережеві обмеження доступ до Storage Account було дозволено лише з Virtual Network, де було розгорнуто Virtual Machine, для перевірки наявності файлу в File Share, необхідно дозволити доступ зі своєї IP-адреси. Для того, щоб надати необхідний дозвіл, в Azure Portal в глобальному пошуку знайти **Storage Accounts** та клікнути по доступному **Storage Account**. Далі у **Security + networking** > **Networking** > **Manage** > **IPv4 Addresses** > **Add your client IPv4 address** та зберегти зміни, клікнувши на **Save**.

29. Перейти у **Data storage** > **File shares** > **share1** > **Browse**, завантажити файл os-info.txt та переглянути його вміст.

30. Перевірити як впливає ротація Storage Account Access Keys на SAS tokens. Перейти у **Data storage** > **Containers** > **data** > **securitytest**, де має знаходитись один попередньо завантажений файл. Клікнути на **Upload**, обрати будь-який файл на комп'ютері, залишити усі параметри за замовчуванням та натиснути **Upload**, щоб завантажити його у Blob container.

31. Клікнути по будь-якому файлу у Blob container та обрати **Generate SAS**. Опціонально можна Expiry та розширити термін дії ключа, решту параметрів залишити за замовчуванням та клікнути **Generate SAS token and URL**, скопіювати згенероване значення з поля **Blob SAS URL**, відкрити нову анонімну вкладку у браузері та перевірити доступність Blob-об'єкту. Очікувано, Blob-об'єкт буде відкритий.

32. Обрати другий файл з Blob container та повторити дію з генерацією SAS token, але в якості **Signing key** вказати значення **Key 2**. Перевірити доступність Blob-об'єкту аналогічним чином, як і в пункті 31.

33. Уявімо ситуацію, що доступ до одного з ключів Storage Account Access key, який надає доступ до всього Storage Account та за відсутності обмежень доступу з авторизованих мереж є серйозним інцидентом безпеки. В такому випадку необхідно якомога швидше виконати його ротацію. Для цього потрібно на рівні Storage Account перейти у **Security + networking**, обрати та напроти **key1** та натиснути **Rotate key**.

34. Після ротації перевірити доступність Blob-об'єктів за їх SAS URL, що було згенеровано у пунктах 31 та 32. SAS URL, де в якості Signing key було використано **key1**, ротацію якого було виконано у пункті 33 більше не має працювати. SAS URL, де було використано **key2** має працювати. На практиці обидва ключі не використовуються одночасно, а один з ключів використовується, як проміжний, для виконання ротації.

35. Перевірити як працює Read-access geo-redundant storage (RA-GRS). Перейти у вкладку **Overview** Storage Account та переконатись, що він в полі **Replication** є саме значення **Read-access geo-redundant storage (RA-GRS)**. Далі перейти у **Data management** > **Redundancy**, обрати **View all** у полі **Storage endpoints**. Знайти значення **Secondary Blob Service Endpoint**. Можна побачити, що Secondary Blob Service Endpoint сформований наступним чином: `https://<accountname>-secondary.blob.core.windows.net`.

На основі цього, змінити SAS URL, що використовував key, щоб від використовував **Secondary Blob Service Endpoint** та використовуючи сторонній сервіс www.azurespeed.com/Azure/IPLookup, переконатись, що **Primary Blob Service Endpoint** та **Secondary Blob Service Endpoint** використовують різні регіони.

36. Іноді бувають випадки, коли для Blob-об'єктів потрібно надавати доступ без запитування автентифікації та авторизації прав. Тобто надати так званий Anonymous acces. Під час створення Storage Account Anonymous Access було

вимкнено. Увімкнути його, перейшовши в **Settings** > **Configuration**, обрати **Allow Blob anonymous access** на зберегти зміни, клікнувши **Save**. Після перейти у **Data storage** > **Containers** > **data**, де всередині має бути директорія **securitytest**. Клікнути на чекбокс, поруч з **securitytest** та обрати вгор**i Change access level** на **Anonymous**. Перейти у директорію **securitytest** та по черзі клікнути на Blob-об'єкти > **еліпсис** (…) > **Copy URL**. Перевірити доступ до обох файлів у приватній вкладці браузеру. Перевірити чи працюють раніше згенеровані SAS URL.

37. Перейти на рівень директорії **securitytest** > **еліпсис** (…) > **Copy URL**. Перевірити чи вдається отримати доступ до директорії у приватній вкладці браузеру.

38. Видалити усі ресурси, що було створено протягом даної лабораторної.

Контрольні запитання

1. Які основні типи сервісів містить Azure Storage Account та в чому різниця між Blob Storage і Azure Files?
2. Що таке GRS та RA-GRS у контексті відмовостійкості Storage Account? У чому відмінність між Primary та Secondary endpoints?
3. Навіщо у Storage Account можна вимикати або обмежувати Public network access? Які ризики виникають при відкритому доступі?
4. Поясніть призначення Service endpoints. Як вони забезпечують доступ до Storage Account лише з певної Virtual Network?
5. Що таке Lifecycle Management у Azure Blob Storage? Які сценарії вирішує правило автоматичного переміщення об’єктів, наприклад MoveToCool?
6. Що таке Immutable Blob Storage (політика незмінності) та які реальні проблеми безпеки вона допомагає вирішити?
7. У чому полягає різниця між публічним доступом до контейнера (Anonymous access) та доступом за допомогою SAS-URL? Коли який механізм доцільно використовувати?
8. Що таке Shared Access Signature (SAS), які основні параметри визначають його поведінку (permissions, start/expiry time, signing key)?
9. Як ротація Storage Account Access Keys впливає на раніше згенеровані SAS-посилання? Які SAS залишаться дійсними після ротації?
10. Яким чином можна перевірити доступ до Blob-об’єктів та File Share з Virtual Machine у тій самій Virtual Network, і чому доступ з локального комп’ютера після обмеження мережевих правил стає недоступним?