Лабораторна робота №8

МОНІТОРИНГ ХМАРНОЇ ІНФРАСТРУКТУРИ В AZURE

Мета: Ознайомитися з можливостями платформи Azure Monitor для збору, аналізу та візуалізації метрик і журналів у хмарному середовищі. Навчитися працювати зі стандартними та будувати запити за допомогою Kusto Query Language (KQL), аналізувати журнали роботи сервісів Azure та виявляти аномалії чи проблеми продуктивності. Опанувати створення правил сповіщень (Azure Monitor Alerts) на основі метрик, журналів і логічних умов, а також налаштовувати дії реагування через Action Groups. Дослідити механізми резервного копіювання ресурсів Azure за допомогою Azure Backup, навчитися створювати політики захисту, виконувати бекап та відновлення даних, а також перевіряти стан захищеності ресурсів.

Хід роботи

1. Перевірити політику Allowed resource deployment regions та обрати один з регіонів.
2. У глобальному пошуку Azure Portal знайти **Resource groups** та створити нову **Resource group** з ім’ям rg-sa-xxx-yyy-zzz, де:
   - xxx – скорочена назва обраного регіону;
   - yyy – ініціали студента;
   - zzz – номер варіанту.
3. Створити **Azure Storage Account**. В головному пошуку Azure Portal знайти **Storage Account** та обрати опцію **Create**. Далі заповнити поля:
   Basics (змінювати тільки вказані поля):
   - **Subscription**: навчальна підписка Azure for Students;
   - **Resource group**: обрати створену в пункті 2 Resource group;
   - **Storage account name**: унікальне ім’я з 3–24 символів (літери та цифри);
   - **Region**: обраний в пункті 1 регіон;

- **Performance**: Standard;
- **Redundancy**: Locally-redundant storage (LRS).

Залишити решту налаштувань за замовчуванням та натиснути **Review + Create** та **Create**.

4. Створити **Log Analytics Workspace**. У глобальному пошуку Azure Portal знайти **Log Analytics Workspaces** та створити новий. В процесі створення вказати наступні дані:
   - **Subscription**: навчальна підписка Azure for Students;
   - **Resource group**: обрати створену в пункті 2 Resource group;
   - **Name**: задаємо ім'я log-xxx-yyy-zzz, де
     - xxx – скорочена назва обраного регіону;
     - yyy – ініціали студента;
     - zzz – номер варіанту;
   - **Region**: обраний в пункті 1 регіон.

   Та натиснути **Review + Create** та **Create**.
5. Перейти в створений в пункті 3 **Storage Account** > **Data storage** > **Containers** та натиснути **Add container**, вказати **Name**: images та натиснути **Create**. Перейти в новостворений контейнер, натиснути Upload > Browse for files та обрати 3 випадкові зображення на комп'ютері (можна зробити три випадкові скріншоти).
6. Перевірити доступність одного з завантажених файлів. Клікнути правою кнопкою миші по одному з файлів в Container та обрати **Generate SAS** > **Generate SAS token and URL** та скопіювати **Blob SAS URL** та відкрити скопійоване посилання у новій вкладці браузеру.
7. Налаштувати відправку логів про події в Storage Account у Log Analytics Workspace. Перейти в створений в пункті 3 Storage Account > Monitoring > Diagnostic settings, обрати серед доступних опцій blob, клікнути далі на + Add diagnostic setting. Далі вказати наступне:
   - **Diagnostic setting name**: diag-blob-xxx-yyy-zzz, де
     - xxx – скорочена назва обраного регіону;

- yyy – ініціали студента;
- zzz – номер варіанту;

- **Logs**:
    - **Category groups**: audit, allLogs;
- **Destination details**: Send to Log Analytics workspace:
    - **Subscription**: Azure for Students;
    - **Log Analytics workspace**: обрати з випадаючого списку Log Analytics workspace, який було створено в пункті 4.

Зберегти зміни, натиснувши **Save** вгорі.

8. Видалити один Blob object з Blob container. Перейти в **Data storage** > **Containers**, обрати раніше створений контейнер **images**, клікнути по одному з об'єктів та натиснути **Delete**.
9. Створити Dashboard. Для цього в глобальному пошуку знайти **Dashboard hub** та натиснути **Create**. Обрати **Custom** та нічого не обираючи з Tile gallery та задати ім'я **Dashboard** на «**Storage insights**» на зберегти зміни, натиснувши **Save**.
10. Використовуючи Log Analytics Workspace, знайти отримати інформацію про операції DeleteBlob. Для цього перейти в створений в пункті 3 **Storage Account** > **Monitoring** > **Logs**. При заході в даний розділ Azure пропонує шаблони запитів, яке можна проігнорувати наразі та закрити вікно. Вгорі справа змінити тип відображення інтерфейсу із запитами з **Simple mode** на **KQL mode**, після чого в інтерфейсі появиться поле, де є можливість писати запити KQL. Вставити та виконати даний запит:

```
StorageBlobLogs
| where OperationName == "DeleteBlob"
| sort by TimeGenerated desc
| project AccountName, AuthenticationType, StatusCode, StatusText, ObjectKey
```

11. Azure дозволяє закріплювати результати виконання KQL-запитів на Dashboard. Результат виконання попереднього запиту закріпити на створений у пункті 9 Dashboard «Storage insights». Для цього вгорі справа

клікнути на Save > Pin to Azure Dashboard. У вікні, що відкрилось обрати:

- **Type**: Private;
- **Dashboard**: з випадаючого списку обрати Dashboard, який було створено в пункті 9 з назвою «Storage insights» та натиснути **Pin**.

12. Вивести інформацію про Ingress traffic в Storage Account. Для цього перейти в створений в пункті 3 **Storage Account** > **Monitoring** > **Metrics** та обрати наступне:
    - **Metric Namespace**: Account;
    - **Metric**: Ingress;
    - **Aggregation**: Sum.

    Змінити параметри відображення графіку, натиснувши вгорі справа на **Local Time: Last 24 hours (Automatic)** та обрати:
    - **Time rage**: Last hour;
    - **Time granularity**: з випадаючого списку обрати 1 min;
    - **Shot time as**: UTC/GMT.

    Для відображення інформації про Ingress traffic в розрізі API name, що використовувались, клікнути на Apply splitting та обрати:
    - **Values**: API name;
    - **Limit**: 20;
    - **Sort**: Ascending.
13. Додати на Dashboard «Storage insights» метрики, отримані з пункту 12. Для цього перебуваючи на цьому ж екрані, де було отримані в пункті 12 метрики, клікнути вгорі справа на **Save to dashboard** > **Pin to dashbord** та обрати у вкладці Existing:
    - **Type**: Private;
    - **Dashboard**: з випадаючого списку обрати Dashboard, який було створено в пункті 9 з назвою «Storage insights» та натиснути **Pin**.
14. Створити новий Alert rule, базуючись на основі метрик Storage Account. Знову ж таки, перебуваючи на екрані з метриками, що було отримано в путкні 12, клікнути вгорі справа на New alert rule та далі налаштувати

наступне:

- у вкладці **Scope** переконатись, що обрано Resource – Storage account, створений у пункті 3;
- у вкладці Condition вказати:
    - **Signal name**: Ingress;
    - **Threshold type**: Static;
    - **Aggregation type**: Total;
    - **Values is**: Greater than;
    - **Unit**: B;
    - **Threshold**: 1;
    - **Dimension name**: API name;
    - **Operator**: =;
    - **Dimension values**: DeleteBlob;
    - **Check every**: 5 minutes;
    - **Loopback perion**: 5 minutes;
- у вкладці **Actions** обрати **+ Create action group** і далі:
    - **Basics**:
    - **Subscription**: Azure for Students;
    - **Resource group**: створена у пункті 2 Resource group;
    - **Region**: Global;
    - Action group name: ag-email-xxx-yyy-zzz, де

    • xxx – скорочена назва обраного регіону;

    • yyy – ініціали студента;

    • zzz – номер варіанту;

    - **Display name**: Storage account Action group – Email;
    - **Notification**:
    - **Notification type**: Email/SMS message/Push/Voice;
    - **Email** та вказати студентську пошту @student.ztu.edu.ua і натиснути **OK**;
    - **Name**: Email alert;

    - Після цього настинути **Review + create** > **Create**. Після створення Action group має відбутись перенаправлення на подальшу конфігурацію алерту;
- у вкладці **Details** вказати:
    - **Severity**: 2 – Warning;
    - **Alert rule name**: DeleteBlob event alert;
    - **Alert rule description**: «This alert has been triggered because a Blob object was removed»;
- Натиснути **Review + create** > **Create**.

15. Перевірити роботу створеного алерту, повторивши пункт 8 з видаленням Blob object.
16. В глобальному пошуку Azure знайти **Monitor** > **Alerts**. Далі вгорі знайти **Alert rules** та клікнути по створеному в пункті 14 **DeleteBlob event alert** алерту. Далі перейти у **History** та переконатись, що там є подія, яка фіксує, що алерт спрацював. У випадку, якщо історія пуста, то перевірити попередні налаштування, усунути їх та відворити події, що призведуть до спрацювання алерту. Також перевірити вказану в 14 пункті електронну пошту, на яку мав прийти лист з детальним повідомленням про алерт.
17. Стилізувати наповнений у результаті виконання попередніх пунктів Dashboard. В глобальному пошуку Azure знайти **Dashboard hub** та клікнути по назві Dashboard з назвою «**Storage insights**». Довільно стилізувати його, змінити розмір блоків з даними, які на ньому є, додати блок Markdown, куди вписати будь-яку релевантну для цього Dashboard, інформацію, та зберегти зміни.
18. У глобальному пошуку Azure Portal знайти **Resource groups** та створити нову **Resource group** з ім’ям rg-webapp-xxx-yyy-zzz, де:
    - xxx – скорочена назва обраного регіону;
    - yyy – ініціали студента;
    - zzz – номер варіанту.

19. Створити App Service. В головному пошуку на Azure Portal знайти **App Services** та обрати опцію **Create** > **Web App**. Далі заповнити поля:
Basics (змінювати тільки вказані поля):
- **Subscription**: обрати підписку Azure for Students;
- **Resource group**: обрати створену в пункті 18 Resource group
- **Name**: app-linux-dotnet-xxx-yyy-zzz-001 (наприклад, app-linux-dotnet-frc-mvv-006-001), де
- xxx – скорочена назва обраного регіону;
- yyy – ініціали студента;
- zzz – номер варіанту. іціали студента

та вимкнути *Secure unique default hostname on*
- **Publish**: Code**;**
- **Runtime stack**: .NET 10 (LTS);
- **Operating system**: Linux;
- **Region**: обрати серед доступних, що вказані в політиці регіонів, яка застосовується для навчальних Subscriptions Azure for Students;
- **App Service Plan** обрати Create new та задати наступні значення:
    - **Name:** asp-linux-dotnet-xxx-yyy-zzz-001 (наприклад, asp-linux-php-frc-mvv-006-001), 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;
    - **Pricing plan**: обрати **Free F1 (Shared infrastructure)**;

Monitoring + secure:
- **Enable Application Insights**: Yes;
- Перейти у вкладу **Review + Create** та після валідації натиснути **Create**. Переконатись у тому, що додаток функціонує справно, перейшовши до новогостворeного **App Service** > **Overview** > **Browse**.

20. Згенерувати запити, що повернуть 404 HTTP response code – Not found. Для цього у вкладці Overview створеного у пункті 19 App service, скопіювати значення Default domain, відкрити нову вкладку браузеру, вставити скопійоване значення, перейти за даним посиланням та переконатись, що додаток працює. В Azure Cloud Shell, в середовищі PowerShell виконати наступну команду, яка згенерує 100 запитів, які мають згенерувати 100 помилок:

```
1..100 | %{$u="https://<Значення Default domain>/$(Get-Random -Maximum 99999999)"; "$u -> $((Invoke-WebRequest $u -Method Head -EA SilentlyContinue).StatusCode)"}
```

21. Знайти в Application Insights інформацію про згенеровані у пункті 20 запити , що повернули помилку. Перейти у створену в пункті 18 Resource group та знайти ресурс з типом **Application insigts**, перейти у пункт **Failures**. Перейти справа у розділ Top 3 response codes та клікнути по 404. У відкритому вікні мають відображатись усі 100 запитів, які мали повернути 404 HTTP response code. Клікнути по будь-якому запиту та зафіксувати отриману інформацію.
22. Отримати інформацію про використання ресурсів. В **Application Insights** > **Investigate > Live metrics** переглянути інформацію про поточне завантаження на App Service, його використання ресурсів. У сусідній вкладці браузеру зробити декілька запитів до App Service, щоб згенерувати події, що відобразяться у **Live metrics**. Результат зафіксувати.
23. Створити тест, щоб перевіряє доступність App Service. У Application Insigts > Investigate > Availability створити тест, клікнувши Add Standard test та вказати наступне:
    - **Test name**: App Service Availability Test;
    - **URL**: прописати https:// та вставити значення з Default domain App Service;
    - **Parse dependent requests**: uncheck;
    - **Enable retries for availability test failures**: check;
    - **Enable SSL certificate validity**: uncheck;
    - **Test frequence**: 5 minutes;
    - **Test locations**: встановити тільки один будь-який location.

    Решту значень залишити за замовчуванням та натиснути **Create**.
24. Перевірити Avaiability test, зачекавший 5хв, до виконання тесту. Після того, як на графіку Availability буде відображено одну успішну перевірку, зупинити App Service, зачекати ще 5хв та перевірити, що Availability test

буде вимкнено. У випадку, якщо обліковий запис Owner містить валідну пошту, то на неї також буде відправлено лист з інформацією про дану подію. Перейти у **Application Insights** > **Monitoring** > **Alerts** > **Alert rules** та переконатись у створених Alert rules, які було створено в процесі створення Avaiability test.

25. Переглянути Application Insigts Dashboard. Перейти у вкладку **Overview** на вгорі зліва знайти та клікнути на **Application Dashboard**.
26. Повернутись у Application Insigts, знайти **Monitoring** > **Logs**. Вгорі справа клікнути на **Queries hub** > **Perfomance** > **Failed requests – top 10** > **Run**. Зафіксувати результат виконання запиту.
27. Створити Backup vault для Azure Blob Storage. В глобальному пошуку Azure знайти Resiliency. Натиснути вгорі зліва **+ Configure protection** та обрати наступне:
    - **Resources managed by**: Azure;
    - **Resources managed by**: Azure Blobs (Azure Storage);
    - **Solution**: Azure Backup;

    Натиснути Continue та у далі налаштувати наступне:

    Basics:

    - **Datasource type**: Azure Blobs (Azure Storage);
    - Vault: Create Vault та далі налаштувати наступне:
        - **Subscription**: Azure for Students;
        - **Resource group**: обрати Resource group, яку було створено у пункті 2;
        - **Backup vault name**: vault-xxx-yyy-zzz, де
            - xxx – скорочена назва обраного регіону;
            - yyy – ініціали студента;
            - zzz – номер варіанту.
        - **Region**: обрати регіон, в якому знаходиться раніше створений Storage Account;
        - **Backup storage redundancy**: Locally-redundant.

Решту параметрів залишити за замовчування та натиснути **Review + Create** > **Create**.

Після повернутись у налаштування бекапів Azure Blob Storage та у вкладці **Backup policy** обрати Create new:

- **Basics:**
  - **Policy name**: daily;
- Schedule + retention
  - **Operation backup**: uncheck;
  - **Backup Frequency**: Daily;
  - **Time**: 00:00;
  - **Timezone**: обрати часову зону за Києвом

Натиснути **Review + Create** > **Create.**

Після повернутись у **Datasource** клікнути **+ Add/Edit** та обрати створений у пункті 3, Storage Account. Натиснути **Assign missing roles** для виправлення помилки валідації ролі, якої не вистачає користувачеві (Storage Account Backup Contributor). У колонці Selected containers натиснути на Change та переконатись, що там обрати Backup all containers. Далі натиснути **Next** та **Configure backup**.

28. Переконатись, що у створеному у пункті 3 Storage Account в Blob container є 1 Blob object. Завантажити 1 або більше або Blob objects у даний Blob container images. Далі щоб не очікувати коли створиться перший бекап, запустити задачу по створенню бекапу. Для цього, перейти у **Resource group**, де було розміщено Backup vault та обрати **Manage** > **Backup instances** та клікнути по Backup instance, який доступний там та натиснути вгорі Backup Now.
29. Повторити пункт 8 та видили один випадковий Blob object з контейнеру Objects.
30. Повторити пункт 3 та створити Storage Account з довільним ім’ям.
31. Підготувати процес відновлення бекапу, надавши необхідні права для Backup Vault. Перейти у **Managed** > **Identity** за скопіювати значення **Object (principal) ID**. Перейти до створеного у пункті 30 **Storage**

Account > **Access Control (IAM)** > **Add** > **Add role assignment** та обрати **Storage Account Backup Contributor** роль. У **Assign access** to обрати **User, group, or service principal**, **+ select memebers** та в поле пошуку вставити значення скопійованого **Object (principal) ID**. Обрати запропоноване значення зі списку та натиснути **Next** > **Review + Assign**.

32. Перейти у Backup vault > Backup items та обрати доступний Backup item там. Обрати Restore > Restore point та обрати Restore point, який було створено у пункті 29. Далі у Restore parameters обрати наступне:
    - **Select option to restore the blobs**: Restore all backed up containers;
    - **Target Subscription**: Azure for Students;
    - **Target storage Account**: якщо список пустий, то за потреби створити новий Storage Account з параметрами за замовчуванням;

    Завершити процедуру відновлення, натиснувши **Next** > **Review and restore**.
33. Дочекатись виконання процесу відновлення бекапу, та перейти у створений у пункті 30, Storage Account та переконатись, що там появився відновлений Blob container та раніше видалений Blob object.
34. У наявних Backup vault, зупинити бекапи та видалити усі наявні бекапи. У **Properties** > **Soft delete** обрати **Update** та зняти галочку на **Enable Soft Delete** й натиснути **Update**. Перейти у Backup instances, обрати доступний **Backup item** > **Stop Backup** та обрати наступне:
    - **Stop backup level**: Delete Backup Data;
    - **Type the name of Backup Instance**: вказати назву Storage Account, бекап якого зупиняється;
    - **Reason: Others;**
    - **Comment**: вказати будь-що.

    Та натиснути **Stop backup**. Це необхідний крок, перед видаленням усіх ресурсів.
35. Видалити усі створені в процесі лабораторної, ресурси.

Контрольні запитання

1. Які типи даних збирає Azure Monitor, та в чому різниця між метриками і логами?
2. Для чого використовується Log Analytics Workspace і які типи даних можуть у нього надходити від сервісів Azure?
3. Що таке Kusto Query Language (KQL)? Які його можливості у контексті аналізу журналів і пошуку подій у StorageBlobLogs?
4. Навіщо налаштовуються Diagnostic Settings у Storage Account, та які типи логів можуть бути передані в Log Analytics Workspace?
5. Як працює Azure Monitor Metrics? Які параметри необхідно задати, щоб відобразити Ingress трафік у Storage Account із розбиттям за API name?
6. Що таке Azure Monitor Alert Rule, з яких основних компонентів воно складається (Scope, Condition, Actions, Details) і як працюють Action Groups?
7. Яким чином можна перевірити спрацювання алерту DeleteBlob event alert та де переглянути історію його спрацьовувань?
8. У чому полягає призначення Application Insights? Яку інформацію можна отримати в розділах Failures, Live Metrics та Availability?
9. Які кроки потрібно виконати, щоб налаштувати Availability Test для вебзастосунку, і як інтерпретувати результати роботи тесту після зупинки App Service?
10. Що таке Azure Backup Vault, як створюється політика резервного копіювання для Blob Storage, та як відбувається процес відновлення даних у новий Storage Account?