Практична робота №8

МОНІТОРИНГ ТА РЕЗЕРВНЕ КОПІЮВАННЯ РЕСУРСІВ AZURE: AZURE MONITOR, NETWORK WATCHER, APPLICATION INSIGHTS, AZURE BACKUP ТА AZURE SITE RECOVERY

Мета: ознайомитися з платформою Azure Monitor та навчитися збирати, аналізувати й візуалізувати метрики та журнали ресурсів Azure: налаштовувати diagnostic settings, будувати запити Kusto Query Language (KQL), використовувати Metrics explorer, Insights, Workbooks та Dashboards. Навчитися збирати дані гостьової операційної системи віртуальних машин за допомогою Azure Monitor Agent і data collection rules, створювати правила сповіщень на основі метрик, журналів та Activity log, налаштовувати action groups і alert processing rules. Набути навичок діагностики мережевого з'єднання за допомогою Azure Network Watcher та моніторингу вебзастосунків за допомогою Application Insights. Опанувати резервне копіювання та відновлення віртуальних машин, Azure Blob Storage та Azure App Service за допомогою Azure Backup, моніторинг резервного копіювання, а також налаштування аварійного відновлення віртуальних машин в іншому регіоні за допомогою Azure Site Recovery.

Теоретичні відомості

Azure Monitor: метрики та журнали

Azure Monitor – платформа збору, аналізу та реагування на телеметрію з ресурсів Azure, віртуальних машин, застосунків і локальної інфраструктури. Дані поділяються на два основні типи (табл. 1). **Метрики** (metrics) – числові значення, що збираються через рівні проміжки часу та зберігаються в базі даних часових рядів; вони придатні для швидкого відображення стану ресурсу та сповіщень майже в реальному часі. **Журнали** (logs) – записи подій з різним набором властивостей, що

зберігаються в таблицях Log Analytics workspace і аналізуються запитами KQL. Platform metrics збираються для ресурсів Azure автоматично й безкоштовно зберігаються 93 дні.

Таблиця 1

Основні джерела даних Azure Monitor

Джерело	Що містить	Як збирається
Platform metrics	Числові показники ресурсу (CPU, Transactions, Ingress тощо)	Автоматично, без налаштувань
Activity log	Операції рівня керування в підписці (створення, зміна, видалення ресурсів), події Service Health	Автоматично, зберігається 90 днів; для довшого зберігання – diagnostic setting підписки
Resource logs	Операції рівня даних усередині ресурсу (наприклад, читання та видалення blobs)	Лише після створення diagnostic setting
Дані гостьової ОС	Лічильники продуктивності, Syslog, Windows Event Log	Azure Monitor Agent та data collection rule
Дані застосунку	Запити, залежності, винятки, перевірки доступності	Application Insights (автоінструментування або SDK / OpenTelemetry)

Diagnostic setting визначає, які категорії resource logs і метрик ресурсу надсилаються та куди: до Log Analytics workspace, Storage Account (архівування), Event Hubs (передавання до зовнішніх систем) або партнерського рішення. Для кожного ресурсу можна створити до п’яти diagnostic settings. У режимі **Resource specific** кожна категорія записується до окремої таблиці (наприклад, `StorageBlobLogs`), у режимі **Azure diagnostics** – до загальної таблиці `AzureDiagnostics`; Microsoft рекомендує режим Resource specific.

Log Analytics workspace – сховище журналів Azure Monitor з власними налаштуваннями зберігання (за замовчуванням 30 днів для більшості таблиць, до 2 років інтерактивного зберігання й до 12 років разом із довгостроковим) та керуванням доступом. Оплата здійснюється переважно за обсяг завантажених даних, тому категорії журналів слід обирати свідомо. Запити пишуться мовою **Kusto Query Language (KQL)**:

запит починається з імені таблиці, далі оператори з’єднуються символом | (табл. 2).

Таблиця 2

Основні оператори KQL

Оператор	Призначення	Приклад
where	Фільтрація рядків	where TimeGenerated > ago(1h)
project	Вибір і перейменування стовпців	project TimeGenerated, StatusCode
summarize	Агрегування з групуванням	summarize count() by OperationName
bin()	Групування часу в інтервали	summarize avg(Val) by bin(TimeGenerated, 5m)
sort by / top	Сортування, перші N рядків	top 10 by TimeGenerated desc
extend	Обчислення нового стовпця	extend Sec = DurationMs / 1000
render	Візуалізація результату	render timechart

Metrics explorer будує графіки метрик з обраною агрегацією (Sum, Avg, Min, Max, Count), гранулярністю часу, фільтрами та розбиттям (**Apply splitting**) за вимірами (dimensions), наприклад за ім’ям API для Storage Account. Графіки метрик і результати запитів можна закріплювати на **Azure dashboards**. **Insights** – готові інтерактивні звіти для типів ресурсів (Storage insights, VM insights, Network insights), побудовані на **Workbooks** – гнучких звітах, що поєднують текст, запити KQL, метрики й параметри. Додатково в порталі доступні Azure Monitor dashboards with Grafana.

Сповіщення Azure Monitor

Alert rule складається з області (**Scope** – ресурс, Resource group або підписка), умови (**Condition** – сигнал, логіка та поріг), дій (**Actions** – action groups) та деталей (**Details** – ім’я, опис, серйозність від 0 – Critical до 4 – Verbose). Типи правил наведено в табл. 3. Сповіщення (alert) має стан умови (**Fired**, **Resolved**) та стан опрацювання користувачем (**New**, **Acknowledged**, **Closed**).

Таблиця 3

Типи правил сповіщень Azure Monitor

Тип	Сигнал	Приклад
Metric alert	Метрика ресурсу; статичний або динамічний поріг, вимірювання за вікном часу (lookback period)	Кількість транзакцій DeleteBlob > 0
Log search alert	Результат запиту KQL, що виконується з заданою періодичністю	Більше 10 помилок 404 за 5 хвилин
Activity log alert	Подія Activity log (адміністративна операція, Service Health, Resource Health)	Видалення віртуальної машини
Availability (Application Insights)	Результати перевірок доступності з кількох розташувань	Застосунок недоступний з двох розташувань

Action group – повторно використовуваний набір отримувачів і дій: сповіщення (email, SMS, push-сповіщення застосунку Azure, голосовий виклик, роль Azure Resource Manager) та дії (Azure Functions, Logic Apps, webhook, Automation runbook, ITSM, Event Hubs). Регіон action group зазвичай **Global**. **Alert processing rule** змінює обробку вже створених сповіщень: додає action groups до сповіщень в області або пригнічує (**Suppress notifications**) надсилання сповіщень, наприклад на час планового обслуговування; правила сповіщень при цьому продовжують спрацьовувати.

Моніторинг віртуальних машин

Для віртуальної машини Azure без додаткових налаштувань доступні метрики хоста (host metrics: Percentage CPU, Network In/Out, Disk Read/Write) та Activity log. Дані гостьової ОС (використання пам’яті та файлових систем, процеси, Syslog, Windows Event Log) збирає **Azure Monitor Agent (AMA)** – розширення віртуальної машини, що замінило виведений з експлуатації Log Analytics agent. Що саме збирати та куди надсилати, визначає **data collection rule (DCR)**; одну DCR можна пов’язати з багатьма машинами, а машина може мати кілька DCR. Увімкнення розширеного моніторингу (VM insights) у порталі встановлює AMA та

створює DCR автоматично. Доступні два варіанти: метрики OpenTelemetry, що зберігаються в Azure Monitor workspace (рекомендований і безкоштовний для стандартного набору лічильників), та класичні метрики на основі журналів у таблиці `InsightsMetrics` Log Analytics workspace. Наявність агента підтверджують записи таблиці `Heartbeat`, що надходять щохвилини.

Azure Network Watcher

Azure Network Watcher – набір засобів моніторингу та діагностики мереж IaaS, що автоматично вмикається в регіоні під час створення віртуальної мережі (ресурс `NetworkWatcher_<регіон>` у Resource group `NetworkWatcherRG`). Основні засоби наведено в табл. 4. NSG flow logs виводяться з експлуатації 30 вересня 2027 року, і створювати нові NSG flow logs уже неможливо; замість них використовуються virtual network flow logs.

Таблиця 4

Засоби Azure Network Watcher

Засіб	Призначення
IP flow verify	Перевіряє, чи дозволено пакет із заданими 5-tuple до або з віртуальної машини, і називає правило NSG, що прийняло рішення
NSG diagnostics	Показує результат обробки трафіку всіма NSG на шляху та ефективні правила
Next hop	Визначає тип і адресу наступного вузла маршруту та таблицю маршрутів, що застосовано
Connection troubleshoot	Разова перевірка TCP/ICMP-з'єднання від віртуальної машини до адреси чи URI з переліком вузлів і затримок
Connection monitor	Постійний моніторинг досяжності та затримки (RTT) між джерелами й призначеннями за протоколами TCP, ICMP або HTTP(S) з даними в Log Analytics та сповіщеннями
Topology	Візуальне подання ресурсів мережі та зв'язків між ними
Flow logs, Traffic analytics	Журналювання IP-трафіку віртуальної мережі та його аналітика

Application Insights

Application Insights – засіб моніторингу продуктивності застосунків (APM) у складі Azure Monitor. Ресурс Application Insights зберігає телеметрію в пов'язаному Log Analytics workspace (workspace-based). Для

App Service можна ввімкнути автоінструментування без зміни коду. Основні можливості: **Failures** (невдалі запити, винятки, коди відповіді), **Performance** (тривалість операцій і залежностей), **Live metrics** (потокові показники з затримкою близько секунди), **Application map** (залежності компонентів), **Availability** (перевірки доступності) та **Logs** (запити KQL до таблиць `requests`, `dependencies`, `exceptions`). **Standard test** надсилає HTTP(S)-запит до URL з кількох розташувань Azure, перевіряє код відповіді, сертифікат TLS і вміст; під час створення тесту автоматично створюється правило сповіщення. Класичні URL ping tests виведено з експлуатації 30 вересня 2026 року.

Azure Backup

Azure Backup – служба резервного копіювання, що зберігає точки відновлення (recovery points) у сховищах двох типів (табл. 5). **Backup policy** визначає розклад (щодня, щотижня або кілька разів на день), час, часовий пояс і терміни зберігання точок відновлення. Для віртуальних машин Azure резервна копія створюється за допомогою знімків дисків: спочатку точка відновлення доступна в рівні snapshot (instant restore, швидке відновлення), потім дані передаються до сховища (vault-standard). Віртуальні машини з типом безпеки Trusted launch захищаються з використанням політики **Enhanced** (у порталі), що також дозволяє створювати резервні копії кожні 4 години та зберігати знімки до 30 днів. Варіанти відновлення віртуальної машини: створення нової машини, заміна дисків наявної, відновлення дисків та відновлення окремих файлів (**File Recovery**) – для Linux порталом або Azure CLI генерується Python-скрипт, що підключає томи точки відновлення через iSCSI.

Таблиця 5

Типи сховищ Azure Backup

Характеристика	Recovery Services vault	Backup vault
Робочі навантаження	Віртуальні машини Azure, SQL Server і SAP HANA у віртуальних машинах, Azure Files, MARS-агент, Azure Site Recovery	Azure Blobs, Azure Disks, Azure Database for PostgreSQL, AKS, Azure Data Lake Storage
Надлишковість сховища	LRS, ZRS, GRS (за замовчуванням); змінюється, доки немає захищених елементів	LRS, ZRS, GRS
Soft delete	Видалені резервні копії зберігаються 14 днів (налаштовується до 180), можливий режим always-on	Аналогічно, 14 днів за замовчуванням
Додаткові можливості	Cross Region Restore, immutable vault, multi-user authorization	Immutable vault, multi-user authorization

Для Azure Blobs підтримуються **operational backup** (локальний захист у самому Storage Account на основі point-in-time restore, versioning і soft delete) та **vaulted backup** (копіювання даних до Backup vault із захистом від видалення облікового запису). Для vaulted backup керована ідентичність Backup vault отримує роль **Storage Account Backup Contributor** на захищеному та цільовому обліковому записі. Єдиний центр керування резервним копіюванням і аварійним відновленням у порталі – **Resiliency** (раніше Backup center, Business Continuity Center).

Моніторинг резервного копіювання включає перегляд **Backup jobs**, вбудовані сповіщення Azure Monitor про невдалі задачі (за замовчуванням увімкнені й надсилаються через alert processing rules та action groups), а також diagnostic settings сховища до Log Analytics workspace у режимі Resource specific (таблиці `CoreAzureBackup`, `AddonAzureBackupJobs` тощо), на яких побудовано **Backup reports** у Resiliency. Початкове надходження даних до звітів може тривати до 24 годин.

Azure Site Recovery

Azure Site Recovery (ASR) забезпечує аварійне відновлення (disaster recovery) шляхом безперервної реплікації віртуальних машин до іншого регіону Azure. Під час увімкнення реплікації створюються або обираються Recovery Services vault у цільовому регіоні, цільові Resource group, віртуальна мережа, cache storage account у вихідному регіоні та політика реплікації; на машину встановлюється розширення Mobility service. Точки відновлення бувають crash-consistent (за замовчуванням щоп'ять хвилин) та app-consistent. **Test failover** створює копію машини в ізольованій мережі цільового регіону без зупинки реплікації, після перевірки її видаляють операцією **Cleanup test failover**. Плановий чи аварійний **failover** переносить роботу до цільового регіону; далі виконуються **commit**, **re-protect** (реплікація у зворотному напрямку) та **failback**. Ключові показники – RPO (допустима втрата даних) і RTO (час відновлення).

Резервне копіювання Azure App Service

App Service підтримує резервне копіювання в цінових категоріях Basic, Standard, Premium та Isolated (у Basic – лише production slot). **Автоматичні резервні копії** створюються щогодини без налаштувань і зберігаються 30 днів на платформі. **Custom backups** зберігаються у вказаному контейнері Storage Account у вигляді ZIP-архіву та XML-файлу, виконуються на вимогу або за розкладом (не частіше ніж кожні 2 години) і можуть містити пов'язану базу даних. Відновлення можливе з перезаписом наявного застосунку, до іншого застосунку чи слоту, з відновленням або без відновлення конфігурації застосунку. Резервна копія не містить, зокрема, власних доменів, сертифікатів TLS, керованих ідентичностей і налаштувань масштабування.

Хід роботи

У завданнях використовуються такі позначення: **xxx** – скорочена назва обраного регіону серед доступних у політиці Allowed resource deployment regions відповідно до цього файлу; **yyy** – ініціали студента латинськими літерами; **zzz** – номер варіанту з трьох цифр (наприклад, для 15 варіанту – 015). Скорочення типів ресурсів в іменах відповідають рекомендаціям Cloud Adoption Framework. Імена Storage Account не можуть містити дефіси, тому мають вигляд `stmonxxxyyyzzz`; якщо ім'я зайняте, додається суфікс `rrr` з трьох випадкових символів a-z0-9. Усі ресурси створюються в Resource group `rg-mon-xxx-yyy-zzz` у регіоні, обраному в кроці 1.2, якщо не зазначено інше. Команди виконуються в Azure Cloud Shell (Bash), якщо не зазначено інше. Частина операцій (резервне копіювання, реплікація, надходження журналів) триває від кількох хвилин до години; під час очікування можна виконувати наступні завдання. Звіт має містити скріншоти та виведення команд, що підтверджують виконання кожного кроку.

Частина 1. Підготовка

1. Обрати регіони й розмір віртуальної машини та підготувати Subscription.
   1.1. Відкрити Azure Portal та Azure Cloud Shell (Bash). Виконати скрипт, який для кожного регіону з політики Allowed resource deployment regions виводить розміри віртуальних машин з не більше ніж 2 vCPU, доступні для підписки та з ненульовою

квотою сімейства (обсяг пам’яті та, у дужках, сімейство, використана кількість vCPU і ліміт):

```
REGIONS=$(az policy assignment show \
  --name sys.regionrestriction \
  --query "parameters.listOfAllowedLocations.value" -o tsv)
Q_USAGE="[?to_number(limit)>\`0\`] \
  .[name.value, currentValue, limit]"
Q_SKU="[?length(restrictions[?type=='Location'])==\`0\` \
  && capabilities[?name=='vCPUs' \
  && to_number(value)<=\`2\`]] \
  .[name, family, \
  capabilities[?name=='MemoryGB'].value|[0]]"

for L in $REGIONS; do
  echo "=== $L"
  az vm list-usage --location $L --query "$Q_USAGE" \
    -o tsv > ~/quota-$L.txt
  az vm list-skus --location $L \
    --resource-type virtualMachines \
    --query "$Q_SKU" -o tsv |
  while read SKU FAMILY MEM; do
    Q=$(grep -i "^$FAMILY[[:space:]]" ~/quota-$L.txt) &&
      echo "  $SKU  RAM=${MEM}GB  ($Q)"
  done
done
```

1.2. Обрати основний регіон і розмір з 2 vCPU та не менше 4 ГіБ пам’яті (наприклад, `Standard_B2ls_v2` або `Standard_B2als_v2`), а також цільовий регіон для Azure Site Recovery – інший регіон із переліку, у якому доступний той самий розмір. Не обирати розміри серій DC, EC та L. Обрані значення зафіксувати у звіті.

1.3. Задати змінні та зареєструвати resource providers, необхідні для практичної роботи (після перезапуску Cloud Shell змінні необхідно задати знову):

```
LOC=<основний регіон, наприклад francecentral>
LOC2=<цільовий регіон ASR, наприклад swedencentral>
SIZE=<обраний розмір, наприклад Standard_B2ls_v2>
SUFFIX=xxx-yyy-zzz
RG=rg-mon-$SUFFIX
SA=stmonxxxyyyzzz
VM=vm-$SUFFIX
RSV=rsv-$SUFFIX
for NS in Microsoft.Insights Microsoft.OperationalInsights \
    Microsoft.AlertsManagement Microsoft.Monitor \
    Microsoft.RecoveryServices Microsoft.DataProtection \
    Microsoft.Network Microsoft.Compute \
    Microsoft.Storage Microsoft.Web; do
  az provider register --namespace $NS
done
az group create --name $RG --location $LOC -o table
```

2. Створити Log Analytics workspace та action group.

2.1. У головному пошуку Azure Portal знайти **Log Analytics workspaces** та натиснути **Create**. Задати **Resource group** – `rg-mon-xxx-yyy-zzz`, **Name** – `log-xxx-yyy-zzz`, **Region** – основний регіон. Натиснути **Review + Create** та **Create**. Після створення переглянути в **Settings** > **Usage and estimated costs** > **Data Retention** період зберігання даних і зафіксувати його.

2.2. У головному пошуку знайти **Monitor**, перейти в **Alerts** > **Action groups** та натиснути **Create**. На вкладці **Basics** задати: **Resource group** – `rg-mon-xxx-yyy-zzz`; **Region** – **Global**; **Action group name** – `ag-ops-xxx-yyy-zzz`; **Display name** – `OpsTeam` (не більше 12 символів).

2.3. На вкладці **Notifications** обрати **Notification type** – **Email/SMS message/Push/Voice**, встановити прапорець **Email** та ввести студентську електронну пошту `@student.ztu.edu.ua`, натиснути **OK**; **Name** – `email-student`. Натиснути **Review +**

create та **Create**. Переконатися, що на пошту надійшов лист про додавання до action group.

Частина 2. Моніторинг Storage Account

3. Створити Storage Account та налаштувати diagnostic setting для Blob Storage.
   3.1. Створити Storage Account: **Resource group** – `rg-mon-xxx-yyy-zzz`; **Storage account name** – `stmonxxxyyyzzz`; **Region** – основний регіон; **Preferred storage type** – **Azure Blob Storage or Azure Data Lake Storage**; **Performance** – **Standard**; **Redundancy** – **Locally-redundant storage (LRS)**; інші параметри – за замовчуванням. Після створення призначити власному обліковому запису роль **Storage Blob Data Contributor** на Storage Account (**Access Control (IAM)** > **Add role assignment**).
   3.2. Перейти в **Data storage** > **Containers**, створити контейнер `images` та завантажити до нього три довільні зображення (можна використати скріншоти).
   3.3. Перейти в **Monitoring** > **Diagnostic settings**, обрати ресурс **blob** та натиснути **Add diagnostic setting**. Задати **Diagnostic setting name** – `diag-blob-xxx-yyy-zzz`; у **Logs** обрати **Category groups** – **audit** та **allLogs**; у **Metrics** – **Transaction**; у **Destination details** обрати **Send to Log Analytics workspace** та workspace `log-xxx-yyy-zzz`. Натиснути **Save**.
   3.4. Видалити один blob з контейнера `images` (обрати файл та натиснути **Delete**), а також відкрити й завантажити (**Download**) інший файл.

4. Проаналізувати журнали Blob Storage за допомогою KQL.
   4.1. Через 5–10 хвилин після кроку 3.4 перейти в Storage Account > **Monitoring** > **Logs**, закрити вікно з прикладами запитів і перемкнути редактор із **Simple mode** на **KQL mode**. Виконати запит, що виводить операції видалення blobs:

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

   4.2. Виконати запит, що підраховує операції за типами за останню годину, та відобразити результат у вигляді кругової діаграми:

```
StorageBlobLogs
| where TimeGenerated > ago(1h)
| summarize Operations = count() by OperationName
| render piechart
```

   4.3. Пояснити у звіті, чому значення `AuthenticationType` для операцій, виконаних у порталі, – `OAuth`, і чому до створення diagnostic setting записів у таблиці `StorageBlobLogs` немає.
5. Дослідити метрики та створити dashboard.
   5.1. У головному пошуку знайти **Dashboard hub**, натиснути **Create** > **Custom**, задати ім’я `Storage insights xxx-yyy-zzz`, не додаючи плиток, та натиснути **Save**.
   5.2. Повернутися до запиту з кроку 4.1 та натиснути **Save** > **Pin to dashboard** (або **Pin to** > **Azure dashboard**); обрати **Existing**, **Type** – **Private**, **Dashboard** – `Storage insights xxx-yyy-zzz` та натиснути **Pin**.
   5.3. Перейти в Storage Account > **Monitoring** > **Metrics** та задати: **Metric Namespace** – **Account**; **Metric** – **Transactions**; **Aggregation** – **Sum**. Натиснути на інтервал часу у верхньому правому куті та обрати **Time range** – **Last hour**, **Time granularity** – **1 minute**, **Show time as** – **UTC/GMT**.

5.4. Натиснути **Apply splitting** та задати **Values** – **API name**, **Limit** – `10`. Додати фільтр (**Add filter**) **Response type** = **Success**. Пояснити у звіті різницю між фільтром і розбиттям.

5.5. Натиснути **Save to dashboard** > **Pin to dashboard**, обрати **Existing**, **Type** – **Private**, dashboard `Storage insights xxx-yyy-zzz` та натиснути **Pin**.

5.6. Відкрити dashboard у **Dashboard hub**, натиснути **Edit**, змінити розміри плиток, додати плитку **Markdown** з короткою інформацією про призначення dashboard (ім'я студента, Storage Account, перелік показників) та натиснути **Save**.

6. Створити metric alert на видалення blobs.

6.1. У Metrics explorer (крок 5.3) натиснути **New alert rule**. На вкладці **Scope** переконатися, що обрано Storage Account `stmonxxxyyyzzz`.

6.2. На вкладці **Condition** задати: **Signal name** – **Transactions**; **Threshold** – **Static**; **Aggregation type** – **Total**; **Operator** – **Greater than**; **Threshold value** – `0`; у розділі **Split by dimensions** обрати **Dimension name** – **API name**, **Operator** – **=**, **Dimension values** – **DeleteBlob**; **Check every** – **1 minute**; **Lookback period** – **5 minutes**.

6.3. На вкладці **Actions** натиснути **Select action groups** та обрати `ag-ops-xxx-yyy-zzz`. На вкладці **Details** задати **Severity** – **2 - Warning**, **Alert rule name** – `alr-deleteblob-xxx-yyy-zzz`, **Alert rule description** – `A blob was deleted`. Натиснути **Review + create** та **Create**.

6.4. Через 5 хвилин після створення правила видалити ще один blob з контейнера `images`. Перейти в **Monitor** > **Alerts**, відкрити сповіщення, що спрацювало, переглянути його стан (**Fired**), серйозність і деталі умови, змінити **User response** на

Acknowledged. Перевірити пошту та додати до звіту скріншот листа.

7. Дослідити Storage insights та Workbooks.

   7.1. Перейти в Storage Account > **Monitoring** > **Insights** та переглянути вкладки **Overview**, **Failures**, **Performance**, **Availability** та **Capacity**. Зафіксувати кількість транзакцій та обсяг використаного сховища.

   7.2. У **Monitor** перейти в **Workbooks**, натиснути **New**, обрати **Add** > **Add query**, вибрати **Data source** – **Logs**, **Resource type** – **Log Analytics**, **Log Analytics workspace** – `log-xxx-yyy-zzz` та ввести запит:

```
StorageBlobLogs
| where TimeGenerated > ago(1d)
| summarize Requests = count()
    by bin(TimeGenerated, 15m), OperationName
| render timechart
```

   7.3. Натиснути **Run Query**, **Done Editing**, додати над запитом текстовий блок (**Add** > **Add text**) із заголовком звіту, натиснути **Save** та зберегти workbook з ім’ям `wb-storage-xxx-yyy-zzz` у Resource group `rg-mon-xxx-yyy-zzz`. Порівняти у звіті можливості dashboard та workbook.

Частина 3. Моніторинг віртуальної машини

8. Створити віртуальну машину Linux.

   8.1. У головному пошуку знайти **Virtual machines** та обрати **Create** > **Virtual machine**. На вкладці **Basics** задати: **Resource group** – `rg-mon-xxx-yyy-zzz`; **Virtual machine name** – `vm-xxx-yyy-zzz`; **Region** – основний регіон; **Availability options** – **No infrastructure redundancy required**; **Security type** – **Trusted launch virtual machines**; **Image** – **Ubuntu Server 24.04 LTS - x64 Gen2**; **Size** – розмір з кроку 1.2; **Authentication type** – **Password**; **Username** – ім’я користувача, аналогічне імені в Azure Cloud

Shell; **Password** – надійний пароль (у звіті не вказувати); **Public inbound ports** – **Allow selected ports**, **Select inbound ports** – **SSH (22)**.

8.2. На вкладці **Networking** залишити створення нової віртуальної мережі, публічної IP-адреси та NSG за замовчуванням. На вкладці **Monitoring** переконатися, що **Boot diagnostics** ввімкнено з managed storage account. Натиснути **Review + create** та **Create**.

8.3. Підключитися до віртуальної машини через SSH з Azure Cloud Shell та створити файл, який буде використано під час відновлення з резервної копії:

```
IP=$(az vm show -d -g $RG -n $VM --query publicIps -o tsv)
ssh $USER@$IP
echo "Важливі дані yyy, $(date)" | sudo tee /srv/report.txt
```

9. Увімкнути розширений моніторинг віртуальної машини.

9.1. Відкрити віртуальну машину та перейти в **Monitoring** > **Monitor** (або **Insights**). Переглянути доступні за замовчуванням графіки метрик хоста та натиснути **Configure** у повідомленні про ввімкнення розширеного моніторингу.

9.2. На сторінці **Configure monitor** залишити **OpenTelemetry metrics** та додатково обрати метрики на основі журналів (logs-based). Натиснути **Customize infrastructure monitoring**: для Azure Monitor workspace обрати **Create new** з ім’ям `amw-xxx-yyy-zzz`, для Log Analytics workspace – `log-xxx-yyy-zzz`; вимкнути **OpenTelemetry per process metrics** (тарифікується додатково) та зняти прапорець **Enable recommended alerts**. Натиснути **Review + Enable** та **Enable**.

9.3. Після завершення перейти у віртуальній машині в **Settings** > **Extensions + applications** та переконатися, що розширення **AzureMonitorLinuxAgent** має стан **Provisioning succeeded**. У

Monitor > **Settings** > **Data Collection Rules** знайти створену DCR та переглянути її **Data sources**, **Resources** і **Destinations**.

10. Налаштувати збирання Syslog за допомогою data collection rule.
    10.1. У **Monitor** > **Settings** > **Data Collection Rules** натиснути **Create**. На вкладці **Basics** задати **Rule Name** – `dcr-syslog-xxx-yyy-zzz`, **Resource Group** – `rg-mon-xxx-yyy-zzz`, **Region** – основний регіон, **Platform Type** – **Linux**.
    10.2. На вкладці **Resources** натиснути **Add resources** та обрати `vm-xxx-yyy-zzz`. На вкладці **Collect and deliver** натиснути **Add data source**, обрати **Data source type** – **Linux Syslog**, для **LOG_USER** встановити мінімальний рівень **LOG_INFO**, для решти facilities – **LOG_WARNING**. На вкладці **Destination** переконатися, що обрано **Azure Monitor Logs** та workspace `log-xxx-yyy-zzz`. Натиснути **Add data source**, **Review + create** та **Create**.
    10.3. Через 5 хвилин записати тестові повідомлення до Syslog у SSH-сеансі віртуальної машини та створити навантаження на процесор на 10 хвилин:

```
logger -p user.warning "pr8-test: повідомлення від yyy"
logger -p user.info "pr8-test: друге повідомлення"
for i in 1 2; do timeout 600 yes > /dev/null & done
```

11. Проаналізувати дані гостьової ОС у Log Analytics.
    11.1. Відкрити Log Analytics workspace `log-xxx-yyy-zzz` > **Logs** у режимі **KQL mode** та переконатися, що агент надсилає heartbeat:

```
Heartbeat
| where TimeGenerated > ago(30m)
| summarize Beats = count(), Last = max(TimeGenerated)
    by Computer, Category, OSType
```

11.2. Побудувати графік використання процесора за даними VM insights:

```
InsightsMetrics
| where TimeGenerated > ago(30m)
| where Name == "UtilizationPercentage"
| summarize avg(Val) by bin(TimeGenerated, 1m), Computer
| render timechart
```

11.3. Знайти тестові повідомлення Syslog:

```
Syslog
| where TimeGenerated > ago(30m)
| where SyslogMessage has "pr8-test"
| project TimeGenerated, Computer, Facility,
    SeverityLevel, SyslogMessage
```

11.4. Відкрити у віртуальній машині **Monitoring** > **Monitor** (**Insights**) та переглянути графіки в обох поданнях (на основі метрик OpenTelemetry та на основі журналів). Порівняти графік **Percentage CPU** у **Monitoring** > **Metrics** (метрика хоста) з даними гостьової ОС. Пояснити у звіті, чому метрики хоста не підтверджують, що збирання журналів налаштовано.

12. Створити Activity log alert та alert processing rule.

12.1. У **Monitor** > **Alerts** обрати **Create** > **Alert rule**. На вкладці **Scope** обрати Resource group `rg-mon-xxx-yyy-zzz`. На вкладці **Condition** натиснути **See all signals**, обрати **Signal type** – **Activity log**, сигнал **Delete Virtual Machine (Virtual Machines)** та натиснути **Apply**; **Event level** і **Status** – **All selected**.

12.2. На вкладці **Actions** обрати action group `ag-ops-xxx-yyy-zzz`. На вкладці **Details** задати **Resource group** – `rg-mon-xxx-yyy-zzz`, **Alert rule name** – `alr-vm-deleted-xxx-yyy-zzz`, **Alert rule description** – `A VM in the resource group was deleted`, **Region** – **Global**, встановити **Enable alert rule upon creation**. Натиснути **Review + create** та **Create**. Сповіщення буде перевірено в завданні 24.

12.3. У **Monitor** > **Alerts** обрати **Alert processing rules** та натиснути **Create**. На вкладці **Scope** обрати Resource group `rg-mon-xxx-yyy-zzz`. На вкладці **Rule settings** обрати **Suppress notifications**. На вкладці **Scheduling** обрати **At a specific time**, **Start** – сьогодні о 22:00, **End** – завтра о 07:00, **Time zone** – **(UTC+02:00) Kyiv** (якщо поточний час потрапляє в цей інтервал, змістити його, щоб сповіщення в завданні 24 не було пригнічено). На вкладці **Details** задати **Rule name** – `apr-maintenance-xxx-yyy-zzz`, **Description** – `Suppress notifications during planned maintenance`. Натиснути **Review + create** та **Create**.

Частина 4. Azure Network Watcher

13. Діагностувати мережевий трафік віртуальної машини.

13.1. У головному пошуку знайти **Network Watcher**, перейти в **Network diagnostic tools** > **IP flow verify** та задати: **Virtual machine** – `vm-xxx-yyy-zzz`; **Network interface** – мережевий інтерфейс машини; **Protocol** – **TCP**; **Direction** – **Inbound**; **Local port** – `22`; **Remote IP address** – `8.8.8.8`; **Remote port** – `60000`. Натиснути **Verify IP flow** та зафіксувати результат і правило NSG. Повторити перевірку для **Local port** – `80`.

13.2. Перейти в **Next hop** та задати: віртуальна машина `vm-xxx-yyy-zzz`, **Source IP address** – приватна IP-адреса машини, **Destination IP address** – `8.8.8.8`. Натиснути **Next hop** та зафіксувати **Next hop type** і **Route table ID**.

13.3. Перейти в **Connection troubleshoot** та задати: **Source type** – **Virtual machine**, **Virtual machine** – `vm-xxx-yyy-zzz`; **Destination type** – **Specify manually**, **URI, FQDN or IP address** – `www.microsoft.com`; **Preferred IP version** – **IPv4**; **Protocol** – **TCP**; **Destination port** – `443`. Натиснути **Run diagnostic tests** та

переглянути результат (**Reachable**), кількість переходів і затримку. Пояснити у звіті, у чому відмінність Connection troubleshoot від IP flow verify.

14. Налаштувати Connection monitor.
    14.1. У Network Watcher перейти в **Monitoring** > **Connection monitor** та натиснути **Create**. На вкладці **Basics** задати **Connection Monitor Name** – `cm-xxx-yyy-zzz`, **Region** – основний регіон; у **Workspace configuration** зняти прапорець використання workspace за замовчуванням та обрати `log-xxx-yyy-zzz`.
    14.2. На вкладці **Test groups** задати **Test group name** – `tg-web`. Натиснути **Add sources**, на вкладці **Azure endpoints** обрати `vm-xxx-yyy-zzz` та натиснути **Add endpoints**. Натиснути **Add destinations**, на вкладці **External Addresses** обрати **Add Endpoint** з іменем `microsoft` та адресою `www.microsoft.com`, натиснути **Add endpoints**.
    14.3. Натиснути **Add Test configuration** та задати **Test configuration name** – `https`, **Protocol** – **HTTP**, **Destination port** – `443`, **Test frequency** – **Every 30 seconds**; інші параметри за замовчуванням. Натиснути **Add Test configuration**, **Add Test Group**, перейти на вкладку **Create alert**, не створюючи сповіщення, та натиснути **Review + create** і **Create**. Під час створення на віртуальну машину автоматично встановлюється розширення Network Watcher.
    14.4. Через 10 хвилин відкрити монітор `cm-xxx-yyy-zzz` та переглянути стан тестів, відсоток невдалих перевірок (**Checks failed**) і **Round-trip time**. Перейти до топології тесту та зафіксувати переходи між джерелом і призначенням.

Частина 5. Application Insights та резервне копіювання App Service

15. Створити Application Insights та App Service.
    15.1. У головному пошуку знайти **Application Insights** та натиснути **Create**. Задати **Resource group** – `rg-mon-xxx-yyy-zzz`, **Name** – `appi-xxx-yyy-zzz`, **Region** – основний регіон, **Log Analytics Workspace** – `log-xxx-yyy-zzz`. Натиснути **Review + create** та **Create**.
    15.2. У головному пошуку знайти **App Services** та обрати **Create** > **Web App**. На вкладці **Basics** задати: **Resource group** – `rg-mon-xxx-yyy-zzz`; **Name** – `app-xxx-yyy-zzz`; **Publish** – **Code**; **Runtime stack** – **.NET 10 (LTS)**; **Operating System** – **Linux**; **Region** – основний регіон; **Linux Plan** – **Create new** з ім'ям `asp-xxx-yyy-zzz`; **Pricing plan** – **Basic B1** (категорія Free F1 не підтримує резервне копіювання).
    15.3. На вкладці **Monitor + secure** обрати **Enable Application Insights** – **Yes** та **Application Insights** – `appi-xxx-yyy-zzz`. Натиснути **Review + create** та **Create**. Після створення відкрити **Default domain** застосунку та переконатися, що відображається стандартна сторінка.
16. Дослідити невдалі запити, Live metrics та запити KQL в Application Insights.
    16.1. Відкрити **Application Insights** > **Investigate** > **Live metrics** у новій вкладці браузера. В Azure Cloud Shell згенерувати 100 запитів до неіснуючих сторінок застосунку та підрахувати отримані коди відповіді:

```
D=<Default domain застосунку>
for i in $(seq 1 100); do
  curl -s -o /dev/null -w "%{http_code}\n" \
    "https://$D/$RANDOM$RANDOM"
done | sort | uniq -c
```

16.2. Зафіксувати показники **Incoming Requests**, **Failed requests** та використання ресурсів сервера в Live metrics під час виконання запитів.

16.3. Через 3–5 хвилин перейти в **Investigate** > **Failures**, у розділі **Top 3 response codes** обрати **404**, відкрити один із запитів (**Drill into**) та зафіксувати інформацію про нього (URL, тривалість, роль, екземпляр).

16.4. Перейти в **Monitoring** > **Logs** та виконати запит, що групує запити за кодами відповіді:

```
requests
| where timestamp > ago(1h)
| summarize Requests = count() by resultCode
| render piechart
```

16.5. Відкрити **Queries hub**, обрати категорію **Performance** (або **Failures**), запит **Failed requests – top 10** та натиснути **Run**. На сторінці **Overview** відкрити **Application Dashboard** і додати його скріншот до звіту.

17. Налаштувати перевірку доступності застосунку.

17.1. В Application Insights перейти в **Investigate** > **Availability** та натиснути **Add Standard test**. Задати: **Test name** – `app-availability`; **URL** – `https://<Default domain застосунку>`; **Parse dependent requests** – вимкнено; **Enable retries for availability test failures** – увімкнено; **SSL certificate validity** – вимкнено; **Test frequency** – **5 minutes**; **Test locations** – три розташування; **Success criteria** – **HTTP response** `200`. Натиснути **Create**.

17.2. Через 10 хвилин переконатися, що на графіку **Availability** відображаються успішні перевірки. Перейти в **Monitoring** > **Alerts** > **Alert rules** Application Insights та переглянути автоматично створене правило сповіщення для тесту; додати до нього action group `ag-ops-xxx-yyy-zzz` (**Edit** > **Actions**).

17.3. Зупинити застосунок (**Overview** > **Stop**), зачекати 10–15 хвилин та зафіксувати невдалі перевірки на графіку Availability, сповіщення, що спрацювало, лист на пошті та зміни в Connection monitor (якщо до тестової групи `tg-web` додано адресу застосунку). Запустити застосунок (**Start**).

18. Налаштувати резервне копіювання App Service та відновити застосунок.

    18.1. У застосунку перейти в **Settings** > **Environment variables**, на вкладці **App settings** додати змінну `PR8_VERSION` зі значенням `1` та натиснути **Apply**.

    18.2. Перейти в **Settings** > **Backups** та переглянути автоматичні резервні копії. Натиснути **Configure custom backups**, обрати **Storage account** – `stmonxxxyyyzzz`, **Container** – **Create new** з ім'ям `appbackups` та натиснути **Configure**. Натиснути **Backup Now** та дочекатися стану **Succeeded**.

    18.3. Відкрити контейнер `appbackups` у Storage Account та переглянути створені файли резервної копії (ZIP та XML). Змінити значення `PR8_VERSION` у застосунку на `2`.

    18.4. У **Backups** натиснути **Restore**, обрати **Source** – **Custom Backup**, створену резервну копію, **Restore destination** – наявний застосунок `app-xxx-yyy-zzz` (production slot), встановити прапорець **Restore site configuration** та запустити відновлення. Після завершення переконатися, що значення `PR8_VERSION` – `1`. Пояснити у звіті різницю між автоматичними та custom backups.

Частина 6. Azure Backup та Azure Site Recovery

19. Створити Recovery Services vault та налаштувати резервне копіювання віртуальної машини.
    19.1. У головному пошуку знайти **Recovery Services vaults** та натиснути **Create**. Задати **Resource group** – `rg-mon-xxx-yyy-zzz`, **Vault name** – `rsv-xxx-yyy-zzz`, **Region** – основний регіон (має збігатися з регіоном віртуальної машини). Натиснути **Review + create** та **Create**.
    19.2. Відкрити сховище, перейти в **Settings** > **Properties** та в розділі **Backup Configuration** натиснути **Update**: переглянути **Storage replication type** (**Geo-redundant** за замовчуванням) та змінити його на **Locally-redundant**, щоб зменшити вартість; зберегти зміни. Переглянути **Security Settings** > **Soft Delete and security settings** та зафіксувати період зберігання видалених даних. Пояснити, чому тип реплікації можна змінити лише до захисту першого елемента.
    19.3. На сторінці **Overview** сховища натиснути **+ Backup**: **Where is your workload running?** – **Azure**; **What do you want to backup?** – **Virtual machine**; **Policy sub type** – **Enhanced** (обов'язково для віртуальних машин з типом безпеки Trusted launch). Натиснути **Backup**.
    19.4. У **Backup policy** обрати **Create a new policy**: **Policy name** – `pol-vm-daily`; **Frequency** – **Daily**, час `23:00`, **Timezone** – **(UTC+02:00) Kyiv**; **Retain instant recovery snapshot(s) for** – `1` день; **Retention of daily backup point** – `7` днів. Натиснути **OK**. У розділі **Virtual Machines** натиснути **Add**, обрати `vm-xxx-yyy-zzz`, натиснути **OK** та **Enable backup**.
    19.5. Після завершення перейти в **Protected items** > **Backup items** > **Azure Virtual Machine**, відкрити `vm-xxx-yyy-zzz` та натиснути

Backup now, залишивши термін зберігання за замовчуванням. Перейти в **Monitoring** > **Backup jobs**, відкрити задачу та стежити за підзадачами **Take Snapshot** і **Transfer data to vault**.

20. Налаштувати моніторинг резервного копіювання.
    20.1. У сховищі `rsv-xxx-yyy-zzz` перейти в **Monitoring** > **Diagnostic settings** та натиснути **Add diagnostic setting**. Задати **Diagnostic setting name** – `diag-rsv-xxx-yyy-zzz`, обрати категорії **Core Azure Backup Data**, **Addon Azure Backup Job Data**, **Addon Azure Backup Policy Data**, **Addon Azure Backup Protected Instance Data** та **Azure Backup Operations**, **Send to Log Analytics workspace** – `log-xxx-yyy-zzz`, **Destination table** – **Resource specific**. Натиснути **Save**.
    20.2. У головному пошуку знайти **Resiliency** та переглянути **Protection inventory** (захищені елементи), **Monitoring + Reporting** > **Jobs** та **Alerts**. Переглянути в **Alerts** > **Alert processing rules** правила, що визначають надсилання вбудованих сповіщень Azure Backup, та створити правило з **Scope** – Resource group `rg-mon-xxx-yyy-zzz`, **Filter** – **Monitor service** = **Azure Backup**, **Rule settings** – **Apply action group** `ag-ops-xxx-yyy-zzz`, **Rule name** – `apr-backup-xxx-yyy-zzz`.
    20.3. Через кілька годин (або наступного дня, до видалення ресурсів) виконати в Log Analytics workspace запит до таблиці задач резервного копіювання. Якщо записів ще немає, пояснити причину:

```
AddonAzureBackupJobs
| where TimeGenerated > ago(1d)
| project TimeGenerated, JobOperation, JobStatus,
    JobStartDateTime, JobDurationInSecs
```

21. Відновити файл з резервної копії віртуальної машини.
    21.1. Після завершення підзадачі **Take Snapshot** (крок 19.5) видалити файл `/srv/report.txt` у SSH-сеансі віртуальної машини.

21.2. В Azure Cloud Shell отримати ім’я останньої точки відновлення, згенерувати скрипт відновлення файлів (команда виводить ім’я файлу та пароль) і скопіювати скрипт на віртуальну машину:

```
B="--resource-group $RG --vault-name $RSV"
I="--container-name $VM --item-name $VM"
RP=$(az backup recoverypoint list $B $I \
  --query "[0].name" -o tsv)
az backup restore files mount-rp $B $I --rp-name $RP
SCRIPT=$(ls -t ${VM}_* | head -1)
scp $SCRIPT $USER@$IP:
```

21.3. У SSH-сеансі віртуальної машини запустити скрипт, погодитися на встановлення потрібних компонентів, ввести пароль з виведення попередньої команди та скопіювати файл з підключеного тому точки відновлення (точний шлях до тому виводить скрипт):

```
sudo python3 ./<ім’я скрипту>
ls ~/*/Volume*/srv/ 2>/dev/null
sudo cp <шлях до тому>/srv/report.txt /srv/
cat /srv/report.txt
```

21.4. У порталі відкрити елемент резервної копії віртуальної машини, обрати **File Recovery** та натиснути **Unmount Disks**, а у віртуальній машині виконати скрипт з параметром `clean` (`sudo python3 ./<ім’я скрипту> clean`). Пояснити у звіті, чому підключення до точки відновлення необхідно закривати.

22. Налаштувати vaulted backup Azure Blob Storage та відновити дані в інший Storage Account.

22.1. У **Resiliency** натиснути + **Configure protection**: **Resources managed by** – **Azure**, **Datasource type** – **Azure Blobs (Azure Storage)**, **Solution** – **Azure Backup**; натиснути **Continue**. На вкладці **Basics** для **Vault** обрати **Create vault**: **Resource group** – `rg-mon-xxx-yyy-zzz`, **Backup vault name** – `bvault-xxx-yyy-zzz`, **Region** – основний регіон, **Backup storage redundancy** – **Locally-redundant**; натиснути **Review + create** та **Create**.

22.2. На вкладці **Backup policy** обрати **Create new**: **Policy name** – `pol-blob-daily`; на вкладці **Schedule + retention** вимкнути **Operational backup**, залишити **Vaulted backup** з **Backup Frequency** – **Daily**, **Time** – `23:00`, **Timezone** – **(UTC+02:00) Kyiv** та терміном зберігання за замовчуванням. Натиснути **Review + create** та **Create**.

22.3. На вкладці **Datasources** натиснути **Add/Edit**, обрати Storage Account `stmonxxxyyyzzz` та у стовпці **Selected containers** переконатися, що обрано **Backup all containers**. Якщо перевірка повідомляє про відсутню роль, натиснути **Assign missing roles** (керованій ідентичності сховища буде призначено роль **Storage Account Backup Contributor**) та після поширення ролі – **Revalidate**. Натиснути **Next** та **Configure backup**.

22.4. Завантажити до контейнера `images` ще один файл. Перейти в `bvault-xxx-yyy-zzz` > **Manage** > **Backup instances**, відкрити екземпляр резервної копії та натиснути **Backup Now**. Після успішного завершення задачі (**Monitoring** > **Backup jobs**) видалити один файл з контейнера `images`.

22.5. Створити Storage Account `stmonxxxyyyzzzrst` з параметрами з кроку 3.1. Скопіювати **Object (principal) ID** керованої ідентичності Backup vault (**Settings** > **Identity**) та призначити їй роль **Storage Account Backup Contributor** на новому обліковому записі (**Access Control (IAM)** > **Add role assignment**, **Assign access to** – **User, group, or service principal**, пошук за Object ID).

22.6. У Backup vault відкрити екземпляр резервної копії, натиснути **Restore**, обрати точку відновлення, створену в кроці 22.4, та задати **Select option to restore the blobs** – **Restore all backed up containers**, **Target storage account** – `stmonxxxyyyzzzrst`.

Натиснути **Validate**, **Next** та **Restore**. Після завершення переконатися, що в цільовому обліковому записі з’явився контейнер з усіма файлами, включно з видаленим.

23. Налаштувати аварійне відновлення віртуальної машини за допомогою Azure Site Recovery.
    23.1. Відкрити віртуальну машину `vm-xxx-yyy-zzz`, перейти в **Backup + disaster recovery** > **Disaster recovery**. На вкладці **Basics** обрати **Target region** – цільовий регіон з кроку 1.2.
    23.2. Перейти на вкладку **Advanced settings** та переглянути параметри, що будуть створені автоматично: цільову підписку, Resource group і віртуальну мережу з суфіксом `-asr`, cache storage account, Recovery Services vault у цільовому регіоні та політику реплікації. Зафіксувати їх у звіті. Якщо перевірка вимагає Automation account для оновлення Mobility service, дозволити його створення.
    23.3. Натиснути **Review + Start replication** та **Start replication**. Через 15–30 хвилин відкрити **Disaster recovery** віртуальної машини та переконатися, що **Replication health** – **Healthy**, а стан реплікації – **Protected**. Зафіксувати RPO та останню точку відновлення.
    23.4. Натиснути **Test failover**, обрати точку відновлення **Latest processed (low RTO)** та віртуальну мережу Azure з суфіксом `-asr` у цільовому регіоні, натиснути **OK**. Після завершення задачі знайти тестову віртуальну машину з суфіксом `-test` у цільовому регіоні та переконатися, що вона запущена.
    23.5. Натиснути **Cleanup test failover**, у полі **Notes** вказати результат перевірки, встановити прапорець **Testing is complete** та натиснути **OK**. Після завершення натиснути **Disable Replication**, вказати причину та підтвердити вимкнення

реплікації. Пояснити у звіті відмінність між test failover та failover.

24. Перевірити спрацювання Activity log alert та видалити ресурси.
    24.1. У сховищі `rsv-xxx-yyy-zzz` вимкнути soft delete (**Properties** > **Security Settings** > **Update**, зняти **Enable soft delete**, **Update**). Відкрити елемент резервної копії віртуальної машини, натиснути **Stop backup**, обрати **Delete Backup Data**, ввести ім’я елемента та натиснути **Stop backup**. Аналогічно в `bvault-xxx-yyy-zzz` вимкнути soft delete (**Properties** > **Soft delete**) та зупинити захист екземпляра резервної копії з видаленням даних.
    24.2. Переконатися, що правило `alr-vm-deleted-xxx-yyy-zzz` увімкнене, та видалити віртуальну машину `vm-xxx-yyy-zzz` (**Delete**, підтвердити видалення). Через 5–15 хвилин перевірити пошту та відкрити сповіщення в **Monitor** > **Alerts**: переглянути його область, умову, операцію `Microsoft.Compute/virtualMachines/delete` та історію. Повторно виконати запит з кроку 11.1 та пояснити, чому дані, отримані до видалення машини, залишилися в workspace.
    24.3. Видалити Resource group `rg-mon-xxx-yyy-zzz`, Resource group з суфіксом `-asr` у цільовому регіоні та інші автоматично створені Resource groups (наприклад, з Automation account або Azure Monitor workspace, якщо вони з’явилися) і переконатися, що їх видалено:

```
az group delete --name $RG --yes
az group list --query "[].name" -o tsv
```

Контрольні запитання

1. Чим відрізняються метрики та журнали Azure Monitor? Які дані збираються автоматично, а для яких потрібні diagnostic settings, Azure Monitor Agent або Application Insights?
2. Що таке Log Analytics workspace і diagnostic setting? Чим відрізняються режими Resource specific та Azure diagnostics і які місця призначення підтримує diagnostic setting?
3. Які основні оператори KQL використовуються для фільтрації, агрегування та візуалізації даних? Наведіть приклад запиту до таблиці StorageBlobLogs.
4. Як працює Metrics explorer? Що означають агрегація, гранулярність часу, фільтр і розбиття (splitting) метрики? Чим dashboard відрізняється від workbook?
5. З яких компонентів складається alert rule? Порівняйте metric alerts, log search alerts та Activity log alerts і поясніть призначення action groups та alert processing rules.
6. Як збираються дані гостьової ОС віртуальної машини? Яку роль відіграють Azure Monitor Agent і data collection rules та чим відрізняються метрики OpenTelemetry і метрики VM insights на основі журналів?
7. Які засоби Azure Network Watcher використовуються для діагностики з'єднань? Чим відрізняються IP flow verify, Next hop, Connection troubleshoot та Connection monitor?
8. Які можливості надає Application Insights для моніторингу вебзастосунку? Як працює Standard availability test і які резервні копії підтримує Azure App Service?

9. Чим відрізняються Recovery Services vault і Backup vault? Що визначає backup policy, як відбувається резервне копіювання віртуальної машини та які варіанти відновлення доступні?
10. Як Azure Site Recovery забезпечує аварійне відновлення віртуальної машини? Чим відрізняються test failover та failover і що означають RPO та RTO?