Monitorowanie i kopie: Azure Monitor, KQL, alerty, Backup i Site Recovery

Poziom: średnio

Dotyczy: AZ-104, domena „Monitor and maintain Azure resources” (10 do 15%), Azure Monitor, Log Analytics, KQL, alerty i grupy akcji, Network Watcher Connection monitor, Azure Backup, Azure Site Recovery, Azure CLI 2.91, moduł Az

Czas: 4 dni po 1,5 do 2 godzin

Dni 22 do 25 programu: metryki i logi w Azure Monitor, obszar roboczy Log Analytics i zapytania KQL, reguły alertów z grupami akcji i regułami przetwarzania, Insights i Connection monitor, magazyny kopii z politykami oraz replikacja maszyny do drugiego regionu w Site Recovery. Najmniejsza domena egzaminu, ale jedyna, w której ćwiczymy odtwarzanie, a nie tylko tworzenie.

ZAŁOŻENIA SCENARIUSZA

monitorujemy zasoby laboratorium z poprzednich dni: `vm-lab-web01`, `vm-lab-web02`, `vm-lab-db01` i konto magazynu. Obszar roboczy `law-zielona-lab` stoi w `rg-lab-monitor`, magazyn kopii `rsv-lab-pl` w `polandcentral`, a magazyn Site Recovery `rsv-lab-se` z siecią `vnet-lab-dr` (10.32.64.0/20) w `swedencentral`. Kopie serwerów w serwerowni Zielonej (restic, `bkp01`, `bkp02`, Veeam) opisuje książka Kopie zapasowe, a monitorowanie serwerowni Zabbix na `mon01`; tu zostajemy w Azure.

Skróty użyte na tej stronie (16)

Skrót	Co znaczy
AKS	Azure Kubernetes Service: Kubernetes w chmurze Microsoftu, w którym płaszczyznę sterowania utrzymuje dostawca
AZ-104	numer egzaminu Microsoft Azure Administrator: egzamin, którego zdanie daje certyfikat Microsoft Certified: Azure Administrator Associate, ważny rok i odnawiany bezpłatną oceną online
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu

Skrót	Co znaczy
GRS	Geo-Redundant Storage: nadmiarowość w Azure, która dodatkowo kopiuje dane do drugiego, odległego regionu
GUID	Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
ITSM	IT Service Management: zarządzanie usługami IT, czyli prowadzenie IT jak zestawu usług dla reszty firmy, a nie tylko utrzymanie sprzętu; tak też nazywa się klasa programów do zgłoszeń, jak GLPI
KQL	Kusto Query Language: język zapytań do logów w Azure Monitor, Log Analytics i Microsoft Sentinel, zapisywany jako ciąg kroków po znaku |
LRS	Locally Redundant Storage: nadmiarowość w Azure, która trzyma trzy kopie danych w jednym centrum danych
RPO	Recovery Point Objective: ile danych wolno stracić przy awarii
RTO	Recovery Time Objective: jak długo wolno nie działać przy awarii
SMS	Short Message Service: krótka wiadomość tekstowa na telefon, która dociera także bez internetu
SQL	Structured Query Language: język zapytań do relacyjnych baz danych
VM	Virtual Machine: maszyna wirtualna
WWW	World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS
ZRS	Zone-Redundant Storage: nadmiarowość w Azure, która rozkłada kopie danych na kilka stref dostępności w jednym regionie

Fiszka

Komendy wykonujemy po `az account set --subscription zielona-lab`. Polecenia `az monitor log-analytics query` i `az monitor alert-processing-rule` pochodzą z rozszerzeń, które CLI instaluje przy pierwszym użyciu. Identyfikatory zasobów (`IdMaszyny`, `IdObszaru`, `IdKonta`) odczytujemy przez `az ... show --query id -o tsv`. Parametry sprawdziliśmy w pomocy Azure CLI 2.91.0, w dokumentacji rozszerzeń i modułu Az (19 października 2026).

◫◫ ZMIENIA SYSTEM

Utworzenie obszaru roboczego Log Analytics: az monitor log-analytics workspace create

```
az monitor log-analytics workspace create --resource-group rg-lab-monitor --name law-zielona-lab --location polandcentral --retention-time 30
```

Obszar roboczy to baza logów, do której piszą ustawienia diagnostyczne i agenci. W PowerShell: `New-AzOperationalInsightsWorkspace -ResourceGroupName rg-lab-monitor -Name law-zielona-lab -Location polandcentral -RetentionInDays 30`.

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Odczyt metryki maszyny: az monitor metrics list

```
az monitor metrics list --resource IdMaszyny --metrics "Percentage CPU" --interval PT5M --aggregation Average -o table
```

Metryki platformy są zbierane bez żadnej konfiguracji. W PowerShell: `Get-AzMetric -ResourceId IdMaszyny -MetricName "Percentage CPU" -TimeGrain 00:05:00`.

□□ **CPU** = Central Processing Unit: procesor · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Wysyłka logów konta magazynu do obszaru roboczego: az monitor diagnostic-settings create

```
az monitor diagnostic-settings create --name diag-blob --resource IdKonta/blobServices/default --workspace IdObszaru \
  --logs '[{"category":"StorageRead","enabled":true},{"category":"StorageWrite","enabled":true},{"category":"StorageDelete","enabled":true}]' \
  --metrics '[{"category":"Transaction","enabled":true}]'
```

Logi usługi blobów ustawiamy na zasobie `blobServices/default`, a nie na samym koncie. Trafiają do tabeli `StorageBlobLogs`. W PowerShell: `New-AzDiagnosticSetting -Name diag-blob -ResourceId NazwaZasobu -WorkspaceId IdObszaru -Log $logi`.

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Wysyłka dziennika aktywności subskrypcji do obszaru roboczego: az monitor diagnostic-settings subscription create

```
az monitor diagnostic-settings subscription create --name diag-aktywnosc --location
polandcentral --workspace IdObszaru \
  --logs
'[{"category":"Administrative","enabled":true},{"category":"Policy","enabled":true}]'
```

Dziennik aktywności (kto co utworzył, zmienił, usunął) trafia wtedy do tabeli `AzureActivity` i można go przeszukiwać KQL dłużej niż przez okres trzymany w samym portalu.

KQL = Kusto Query Language: język zapytań do logów w Azure Monitor, Log Analytics i Microsoft Sentinel, zapisywany jako ciąg kroków po znaku | · **az** = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Uruchomienie zapytania KQL w obszarze roboczym: az monitor log-analytics query

```
ID=$(az monitor log-analytics workspace show --resource-group rg-lab-monitor --name law-
zielona-lab --query customerId -o tsv)
az monitor log-analytics query --workspace "$ID" --analytics-query "AzureActivity |
summarize count() by Caller" --timespan P1D
```

Parametr `--workspace` przyjmuje identyfikator klienta obszaru (GUID z pola `customerId`), a nie identyfikator zasobu. W PowerShell: `Invoke-AzOperationalInsightsQuery -WorkspaceId $ID -Query "AzureActivity | summarize count() by Caller"`.

KQL = Kusto Query Language: język zapytań do logów w Azure Monitor, Log Analytics i Microsoft Sentinel, zapisywany jako ciąg kroków po znaku | · **GUID** = Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera · **az** = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Zapytanie: kto usuwał zasoby w ostatnim tygodniu

```
AzureActivity
| where TimeGenerated > ago(7d)
| where OperationNameValue endswith "/DELETE"
| where ActivityStatusValue == "Success"
```

```
| project TimeGenerated, Caller, ResourceGroup, OperationNameValue
| order by TimeGenerated desc
```

Pierwsze zapytanie, które uruchamiamy, gdy zasób zniknął. Kolumny `Caller` i `ResourceGroup` mówią kto i gdzie.

◫◫ ZMIENIA SYSTEM

Zapytanie: usunięte bloby w koncie magazynu

```
StorageBlobLogs
| where TimeGenerated > ago(1d)
| where OperationName == "DeleteBlob"
| project TimeGenerated, CallerIpAddress, Uri, StatusText
```

Wymaga ustawienia diagnostycznego z kategorią StorageDelete.

◫◫ TYLKO ODCZYT

Zapytanie: maszyny, które przestały wysyłać sygnał życia

```
Heartbeat
| summarize OstatniSygnal = max(TimeGenerated) by Computer
| where OstatniSygnal < ago(15m)
```

Tabela `Heartbeat` zapełnia się, gdy na maszynach działa agent Azure Monitor z regułą zbierania danych kierującą dane do obszaru.

◫◫ ZMIENIA SYSTEM

Utworzenie grupy akcji z powiadomieniem e-mail: az monitor action-group create

```
az monitor action-group create --resource-group rg-lab-monitor --name ag-lab-it --group-short-name labit \
  --action email zespol-it NazwaSkrzynki@zielona.example
```

Format akcji e-mail to `--action email NAZWA ADRES`. Ta sama grupa może dzwonić, wysyłać SMS, wywoływać webhook, Logic App albo runbook. W PowerShell: `New-AzActionGroup -Name ag-lab-it -ResourceGroupName rg-lab-monitor -Location global -GroupShortName labit -EmailReceiver $odbiorca`, gdzie `$odbiorca` tworzy `New-AzActionGroupEmailReceiverObject -Name zespol-it -EmailAddress NazwaSkrzynki@zielona.example`.

SMS = Short Message Service: krótka wiadomość tekstowa na telefon, która dociera także bez internetu · **az** = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie alertu metryki procesora: az monitor metrics alert create

```
az monitor metrics alert create --resource-group rg-lab-monitor --name alert-cpu-web01
--scopes IdMaszyny \
  --condition "avg Percentage CPU > 80" --window-size 5m --evaluation-frequency 1m --
severity 2 \
  --action IdGrupyAkcji --description "Procesor vm-lab-web01 powyzej 80 procent"
```

Okno 5 minut, sprawdzanie co minutę, ważność od 0 (krytyczna) do 4 (informacyjna). W PowerShell regułę tworzy `Add-AzMetricAlertRuleV2` z warunkiem z `New-AzMetricAlertRuleV2Criteria`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie alertu dziennika aktywności na usunięcie maszyny: az monitor activity-log alert create

```
az monitor activity-log alert create --resource-group rg-lab-monitor --name alert-
usuniecie-vm \
  --scope /subscriptions/IdSubskrypcji \
  --condition category=Administrative and
operationName=Microsoft.Compute/virtualMachines/delete \
  --action-group IdGrupyAkcji
```

Alert dziennika aktywności reaguje na operacje zarządzania, a nie na metryki.

az = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Wyciszenie powiadomień na okno serwisowe: az monitor alert-processing-rule create

```
az monitor alert-processing-rule create --resource-group rg-lab-monitor --name cisza-okno-serwisowe \
  --rule-type RemoveAllActionGroups --scopes /subscriptions/IdSubskrypcji/resourceGroups/rg-lab-obliczenia \
  --schedule-start-datetime '2026-10-27 18:00:00' --schedule-end-datetime '2026-10-27 20:00:00' \
  --schedule-time-zone 'Central European Standard Time' --description "Okno serwisowe laboratorium"
```

Reguła przetwarzania nie wyłącza alertów, tylko w podanym czasie nie wywołuje grup akcji. Drugi typ, `AddActionGroups`, dokłada grupę akcji do wszystkich alertów w zakresie. Polecenie pochodzi z rozszerzenia `alertsmanagement`, a nazwę strefy czasowej sprawdzamy na liście stref Windows.

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Utworzenie magazynu Recovery Services: az backup vault create

```
az backup vault create --resource-group rg-lab-obliczenia --name rsv-lab-pl --location polandcentral
```

Magazyn musi być w tym samym regionie co chronione maszyny. W PowerShell: `New-AzRecoveryServicesVault -Name rsv-lab-pl -ResourceGroupName rg-lab-obliczenia -Location polandcentral`.

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Ustawienie nadmiarowości magazynu przed pierwszą kopią: az backup vault backup-properties set

```
az backup vault backup-properties set --resource-group rg-lab-obliczenia --name rsv-lab-pl --backup-storage-redundancy LocallyRedundant
```

Dozwolone wartości to `GeoRedundant`, `LocallyRedundant` i `ZoneRedundant`. Ustawiamy je przed objęciem ochroną pierwszego elementu. W PowerShell: `Set-AzRecoveryServicesBackupProperty -Vault $magazyn -BackupStorageRedundancy LocallyRedundant`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Objęcie maszyny ochroną z polityką domyślną: az backup protection enable-for-vm

```
az backup protection enable-for-vm --resource-group rg-lab-obliczenia --vault-name rsv-lab-pl --vm vm-lab-db01 --policy-name DefaultPolicy
```

Listę polityk magazynu pokazuje `az backup policy list --resource-group rg-lab-obliczenia --vault-name rsv-lab-pl -o table`. W PowerShell: `Enable-AzRecoveryServicesBackupProtection -Policy $polityka -Name vm-lab-db01 -ResourceGroupName rg-lab-obliczenia -VaultId $magazyn.ID`.

az = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Kopia na żądanie: az backup protection backup-now

```
az backup protection backup-now --resource-group rg-lab-obliczenia --vault-name rsv-lab-pl \
  --container-name vm-lab-db01 --item-name vm-lab-db01 --backup-management-type AzureIaasVM --retain-until 30-11-2026
```

Data `--retain-until` ma format dzień-miesiąc-rok. Postęp pokazuje `az backup job list --resource-group rg-lab-obliczenia --vault-name rsv-lab-pl -o table`.

az = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Lista punktów odzyskiwania: az backup recoverypoint list

```
az backup recoverypoint list --resource-group rg-lab-obliczenia --vault-name rsv-lab-pl
\
  --container-name vm-lab-db01 --item-name vm-lab-db01 --backup-management-type
AzureIaasVM -o table
```

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Odtworzenie dysków maszyny z punktu odzyskiwania: az backup restore restore-disks

```
az backup restore restore-disks --resource-group rg-lab-obliczenia --vault-name rsv-lab-
pl \
  --container-name vm-lab-db01 --item-name vm-lab-db01 --rp-name NazwaPunktu \
  --storage-account NazwaKontaPosredniego --target-resource-group rg-lab-dr
```

Odtwarza dyski zarządzane do grupy `rg-lab-dr`, z których stawiamy nową maszynę albo podmieniamy dysk. Konto pośrednie służy do konfiguracji i szablonu maszyny.

□□ **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Utworzenie magazynu kopii (Backup vault): New-AzDataProtectionBackupVault

```
$ustawienie = New-AzDataProtectionBackupVaultStorageSettingObject -DataStoreType
VaultStore -Type LocallyRedundant
New-AzDataProtectionBackupVault -ResourceGroupName rg-lab-obliczenia -VaultName bv-lab-
pl -Location polandcentral -StorageSetting $ustawienie
```

Backup vault to drugi rodzaj magazynu, dla nowszych obciążeń: blobów, dysków zarządzanych, Azure Database for PostgreSQL i AKS. W Azure CLI odpowiadające polecenia są w rozszerzeniu `dataprotection`.

□□ **AKS** = Azure Kubernetes Service: Kubernetes w chmurze Microsoftu, w którym płaszczyznę sterowania utrzymuje dostawca · **CLI** = Command Line Interface: praca przez wpisywanie komend w terminalu

🖱️ KLIKAMY W INTERFEJSIE

Replikacja maszyny do drugiego regionu i test w portalu

```
Portal Azure → Virtual machines → vm-lab-db01 → Backup + disaster recovery → Disaster recovery
  Target region: Sweden Central → Review + Start replication
Portal Azure → Recovery Services vaults → rsv-lab-se → Replicated items → vm-lab-db01 → Test failover
Portal Azure → Recovery Services vaults → rsv-lab-se → Replicated items → vm-lab-db01 → Cleanup test failover
```

Test przełączenia uruchamiamy do sieci izolowanej, a po teście sprzątamy. Właściwe przełączenie (Failover), zatwierdzenie (Commit) i ponowna ochrona w drugą stronę (Re-protect) są na tym samym ekranie. W PowerShell test uruchamia `Start-AzRecoveryServicesAsrTestFailoverJob -ReplicationProtectedItem $element -Direction PrimaryToRecovery -AzureVMNetworkId IdSieciTestowej`.

🖼️ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Disaster recovery maszyny vm-lab-db01 z regionem docelowym Sweden Central, widoczne pola Target resource group (rg-lab-dr), Target virtual network (vnet-lab-dr) i przycisk Review + Start replication.

Dzień 22: Azure Monitor, metryki, logi i KQL

🎭 Z ŻYCIA WZIĘTE

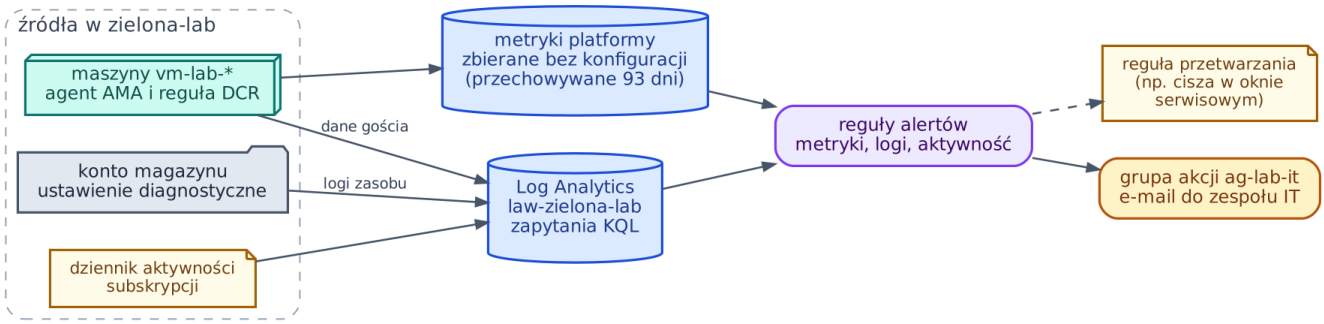
Poniedziałek, 8:10. Tomek zauważa, że w laboratorium nie ma konta magazynu, które w piątek służyło do ćwiczeń z prywatnym punktem końcowym. Nikt się nie przyznaje, a portal pokazuje dziennik aktywności tylko dla jednego zasobu naraz. Tomek uruchamia w `law-zielona-lab` zapytanie po `AzureActivity` z filtrem na usunięcia i po dwudziestu sekundach widzi siebie: piątkowe `az group delete` na `rg-lab-magazyn`. Zapisuje w dzienniku, że zanim zacznie szukać winnego, sprawdzi własne polecenia.

Cele egzaminu

- interpretacja metryk w Azure Monitor
- konfiguracja ustawień logów w Azure Monitor
- odpytywanie i analiza logów w Azure Monitor

Jak to działa

Azure Monitor zbiera dwa rodzaje danych. Metryki to liczby w czasie (procesor, transakcje, opóźnienie), zbierane automatycznie dla zasobów i przechowywane 93 dni. Logi to rekordy z wieloma polami (kto, co, z jakim wynikiem), które trzeba wysłać do obszaru roboczego Log Analytics ustawieniem diagnostycznym albo agentem.



Rysunek 1. Przepływ danych Azure Monitor w laboratorium: maszyny z agentem i regułą zbierania danych, konto magazynu z ustawieniem diagnostycznym i dziennik aktywności piszą do law-zielona-lab, metryki platformy zbierane są bez konfiguracji, a reguły alertów wywołują grupę akcji z e-mailem do zespołu IT (kliknięcie otwiera pełny rozmiar)

Źródło	Gdzie trafia domyślnie	Co trzeba zrobić, żeby było w Log Analytics
Metryki platformy	magazyn metryk, 93 dni	ustawienie diagnostyczne z kategorią metryk (opcjonalnie)
Logi zasobów (na przykład StorageRead)	nigdzie	ustawienie diagnostyczne na zasobie
Dziennik aktywności	portal, ograniczony okres	ustawienie diagnostyczne subskrypcji
Dane z wnętrza maszyny (zdarzenia, liczniki)	nigdzie	agent Azure Monitor (AMA) i reguła zbierania danych (DCR)

Pojęcie: KQL (Kusto Query Language). Język zapytań Log Analytics. Zapytanie zaczyna się od nazwy tabeli, a każdy kolejny krok po znaku `|` filtruje, wybiera kolumny albo grupuje. Najczęstsze operatory na egzaminie: `where`, `project`, `summarize ... by`, `order by`, `take`, `ago()`, `bin()`.

SQL	KQL
`SELECT kol1, kol2 FROM tabela`	`tabela \
`WHERE czas > NOW() - 1 dzień`	`\

SQL	KQL
`GROUP BY kol COUNT(*)`	`\`
`ORDER BY kol DESC`	`\`
`LIMIT 10`	`\`

Kto zna SQL ze stron o bazach danych w naszej bazie, czyta KQL bez trudu, tylko w odwrotnej kolejności: najpierw skąd, potem co.

Zadania laboratoryjne

1. Tworzymy `law-zielona-lab` z retencją 30 dni.
2. Włączamy ustawienie diagnostyczne usługi blobów konta i dziennika aktywności subskrypcji.
3. Na `vm-lab-web01` w portalu włączamy VM Insights (instaluje agenta i regułę zbierania danych) i po kwadransie sprawdzamy tabelę `Heartbeat`.
4. W Metrics explorer rysujemy wykres procesora obu maszyn WWW na jednym wykresie i przypinamy go do pulpitu.
5. Uruchamiamy trzy zapytania z Fiszki, zapisujemy je jako zapytania w obszarze roboczym.

Pułapki egzaminacyjne

- Logi zasobów nie są zbierane, dopóki nie ustawimy ustawienia diagnostycznego.
- Dane z wnętrza systemu (zdarzenia, dziennik systemowy) wymagają agenta, a nie ustawienia diagnostycznego.
- `az monitor log-analytics query` chce GUID obszaru (`customerId`), nie identyfikatora zasobu.
- Retencję ustawia się na obszarze (i tabelach), a nie w regule alertu.

Ćwiczenia

1. Napisz zapytanie KQL, które pokaże liczbę operacji w dzienniku aktywności z ostatnich 24 godzin w podziale na grupę zasobów, od największej.

Odpowiedź

```
AzureActivity
| where TimeGenerated > ago(24h)
| summarize Liczba = count() by ResourceGroup
| order by Liczba desc
```

Dzień 23: alerty, grupy akcji, reguły przetwarzania, Insights i Connection monitor

Z ŻYCIA WZIĘTE

Wtorek, 22:40. Telefon Tomka dzwoni dwanaście razy w ciągu godziny: alert procesora z `vm-lab-web01`, bo ćwiczeniowa pętla obciążająca została uruchomiona i zapomniana. Rano dokładamy regułę przetwarzania, która w oknie zaplanowanych prac nie wywołuje grup akcji, i zmieniamy alert, żeby sam się zamykał, gdy procesor spadnie. Tomek pyta jeszcze, czy można po prostu wyłączyć alert na noc. Można, ale reguła przetwarzania zostawia alert w historii, a wyłączenie nie.

Cele egzaminu

- konfiguracja reguł alertów, grup akcji i reguł przetwarzania alertów w Azure Monitor
- konfiguracja i interpretacja monitorowania maszyn, kont magazynu i sieci przy pomocy Azure Monitor Insights
- korzystanie z Azure Network Watcher i Connection monitor

Jak to działa

Rodzaj alertu	Na czym działa	Przykład
Metryki	metryka zasobu	procesor powyżej 80 procent przez 5 minut
Wyszukiwania w logach	wynik zapytania KQL	więcej niż 10 usuniętych blobów w godzinę
Dziennika aktywności	operacja zarządzania albo zdarzenie Service Health	usunięcie maszyny
Kondycji zasobu	stan zasobu zgłaszany przez platformę	maszyna niedostępna

Pojęcie: grupa akcji. Lista odbiorców i działań (e-mail, SMS, połączenie, powiadomienie w aplikacji, webhook, Logic App, runbook, Event Hub, ITSM) wielokrotnego użytku. Jedna grupa akcji obsługuje wiele reguł alertów.

Pojęcie: reguła przetwarzania alertów. Reguła nakładana na już wyzwolone alerty w zakresie: wycisza powiadomienia (usuwa grupy akcji) albo dokłada grupę akcji, stale albo według harmonogramu. Typowe użycie to okno serwisowe.

Insights to gotowe widoki dla typów zasobów: VM Insights (wydajność i mapa połączeń maszyn), Storage Insights (dostępność, opóźnienia, pojemność kont) i Network Insights (stan zasobów sieciowych w jednym miejscu). Connection monitor w Network Watcher mierzy stale połączenie

między punktami (maszyna, adres, port), z progami niepowodzeń i czasu odpowiedzi, i może wywołać alert.

Zadania laboratoryjne

1. Tworzymy grupę akcji `ag-lab-it` z e-mailem i testujemy ją w portalu (Test action group).
2. Tworzymy alert metryki procesora `vm-lab-web01` i obciążamy procesor, aż przyjdzie e-mail.
3. Tworzymy alert dziennika aktywności na usunięcie maszyny i usuwamy maszynę testową.
4. Tworzymy regułę przetwarzania z oknem na dziś wieczór i sprawdzamy, że alert jest w historii, a e-maila nie ma.
5. W Network Watcher tworzymy Connection monitor z `vm-lab-web01` do 10.32.32.4 na port 22 i oglądamy wykres opóźnień.
6. Przeglądamy Storage Insights konta laboratorium i Network Insights subskrypcji.

Pułapki egzaminacyjne

- Reguła przetwarzania nie zatrzymuje wyzwalania alertów, tylko powiadomienia.
- Alert metryki działa na metryce jednego typu zasobu w zakresie, alert logów na wyniku zapytania.
- Grupa akcji jest osobnym zasobem: zmiana adresu w grupie zmienia odbiorcę wszystkich reguł naraz.
- Connection monitor wymaga agenta albo rozszerzenia Network Watcher na maszynie źródłowej.

Ćwiczenia

1. W każdą sobotę od 6:00 do 8:00 trwa aktualizacja maszyn laboratorium. Alerty mają powstawać, ale bez powiadomień. Co konfigurujemy?

Odpowiedź

Regułę przetwarzania alertów typu RemoveAllActionGroups na zakresie grupy zasobów, z harmonogramem cotygodniowym (sobota, 6:00 do 8:00, strefa czasowa Europy Środkowej). Reguły alertów i grupy akcji zostają bez zmian.

Dzień 24: Azure Backup

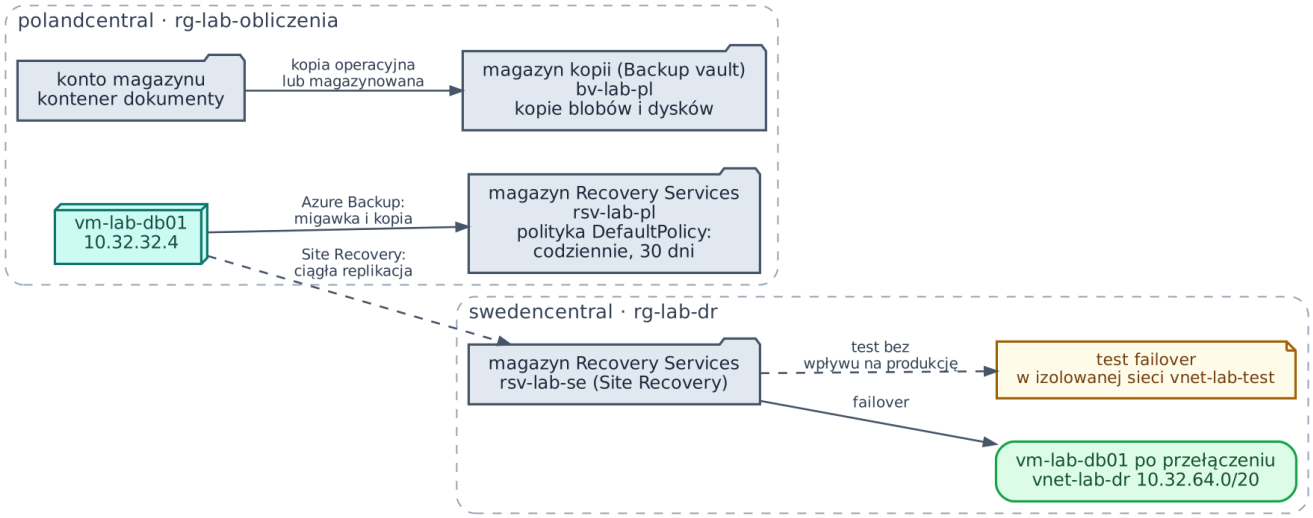
Z ŻYCIA WZIĘTE

Środa, 13:00. Pan Wojtek, audytor, pyta na przeglądzie, czy maszyny w Azure mają kopie i czy ktoś kiedyś coś z nich odtworzył. Tomek pokazuje magazyn `rsv-lab-pl`, politykę z codzienną kopią i zadanie odtworzenia dysków `vm-lab-db01` z wczoraj, zakończone powodzeniem po kilkunastu minutach. Pan Wojtek zapisuje w protokole, że w laboratorium test odtworzenia jest udokumentowany, i pyta, kiedy tak samo będzie z produkcją.

Cele egzaminu

- tworzenie magazynu Recovery Services
- tworzenie magazynu kopii (Backup vault)
- tworzenie i konfiguracja polityki kopii
- wykonywanie kopii i odtwarzania przy pomocy Azure Backup
- konfiguracja i interpretacja raportów i alertów kopii

Jak to działa



Rysunek 2. Kopie i odtwarzanie w laboratorium: vm-lab-db01 kopiowana do magazynu Recovery Services rsv-lab-pl, konto magazynu chronione w Backup vault bv-lab-pl, a ta sama maszyna replikowana Site Recovery do magazynu rsv-lab-se w swedencentral z testem przełączenia w izolowanej sieci (kliknięcie otwiera pełny rozmiar)

	Magazyn Recovery Services	Magazyn kopii (Backup vault)

Co chroni	maszyny Azure, SQL i SAP HANA w maszynach, Azure Files, serwery lokalne z agentem MARS	bloby, dyski zarządzane, Azure Database for PostgreSQL, AKS
Site Recovery	tak	nie
W CLI	`az backup`	rozszerzenie `dataprotection`
W PowerShell	`*-AzRecoveryServices*`	`*-AzDataProtection*`

> **Pojęcie: polityka kopii.** Harmonogram (codziennie, co tydzień, co kilka godzin w polityce rozszerzonej) i retencja punktów (dzienne, tygodniowe, miesięczne, roczne). Polityka domyślna `DefaultPolicy` dla maszyn ma kopię codzienną z retencją, którą sprawdzamy w portalu przy tworzeniu magazynu (w dokumentacji opisana jako 30 dni, do potwierdzenia dla naszej wersji).

Kopia maszyny ma dwa etapy: migawka dysków (z niej działa szybkie odtwarzanie, instant restore) i przeniesienie danych do magazynu. Nadmiarowość magazynu (LRS, ZRS, GRS) ustawiamy przed pierwszą kopią, a odtwarzanie do drugiego regionu (Cross Region Restore) wymaga GRS. Usunięte dane kopii są domyślnie chronione miękkim usuwaniem (czas sprawdzamy w ustawieniach magazynu).

Odtworzyć maszynę można na kilka sposobów: nowa maszyna, odtworzenie dysków (i własna maszyna z nich), zastąpienie dysków istniejącej maszyny albo odzyskanie pojedynczych plików przez zamontowanie punktu odzyskiwania. Raporty kopii (Backup reports) wymagają ustawienia diagnostycznego magazynu do obszaru Log Analytics, a alerty kopii idą przez Azure Monitor.

Zasady kopii w Zielonej (3-2-1-1-0, RPO, RTO) i to, czym różni się kopia od replikacji, opisuje strona Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje.

Zadania laboratoryjne

1. Tworzymy `rsv-lab-pl`, ustawiamy LRS, obejmujemy `vm-lab-db01` polityką `DefaultPolicy`.
2. Wykonujemy kopię na żądanie i śledzimy zadanie `az backup job list`.
3. Odtwarzamy dyski do `rg-lab-dr`, a w portalu odzyskujemy pojedynczy plik (File Recovery).
4. Tworzymy Backup vault `bv-lab-pl` w PowerShell i w portalu obejmujemy ochroną operacyjną kontener blobów konta.
5. Włączamy ustawienie diagnostyczne magazynu do `law-zielona-lab` i otwieramy Backup reports (dane pojawiają się z opóźnieniem).
6. Na koniec dnia: zatrzymujemy ochronę z usunięciem danych i sprawdzamy, czy miękkie usuwanie nie trzyma ich dalej, bo magazynu z danymi nie da się usunąć.

Pułapki egzaminacyjne

- Nadmiarowości magazynu nie zmienimy po objęciu ochroną pierwszego elementu.
- Magazyn Recovery Services musi być w regionie chronionych maszyn.
- Bloby i dyski chronimy w Backup vault, nie w Recovery Services vault.
- Magazynu z elementami w miękkim usunięciu nie da się usunąć, dopóki nie miną albo ich nie odzyskamy i usuniemy trwale.

Ćwiczenia

1. Maszyna w `polandcentral` ma być chroniona kopią z możliwością odtworzenia w drugim regionie, gdy cały region padnie. Jak ustawiamy magazyn?

Odpowiedź

Magazyn Recovery Services w `polandcentral` z nadmiarowością GRS i włączonym Cross Region Restore, ustawionymi przed pierwszą kopią. Uwaga: `polandcentral` jest regionem bez pary, więc dostępność GRS i regionu docelowego dla tego magazynu sprawdzamy w dokumentacji (do potwierdzenia). Jeżeli liczy się szybki powrót, a nie tylko dane, lepszą odpowiedzią jest Site Recovery.

Dzień 25: Site Recovery

> **Z ŻYCIA WZIĘTE**
>
> Czwartek, 9:00. Pan Zbigniew pyta, co się stanie z bazą w Azure, jeśli cały region będzie niedostępny przez dzień. Tomek pokazuje replikację `vm-lab-db01` do `swedencentral` i uruchamia test przełączenia do sieci `vnet-lab-test`: po kilkunastu minutach w Szwecji działa kopia maszyny, a oryginał w Polsce pracuje dalej. Pan Zbigniew pyta, czy test coś popsuł. Tomek pokazuje, że nie, i klika sprzątanie po teście.

Cele egzaminu

- konfiguracja Azure Site Recovery dla zasobów Azure
- przełączenie do regionu zapasowego przy pomocy Site Recovery

Jak to działa

> **Pojęcie: Azure Site Recovery.** Ciągła replikacja maszyn do innego regionu z możliwością przełączenia. Kopia zapasowa odpowiada na pytanie „jak odzyskać dane sprzed tygodnia”, a Site Recovery na pytanie „jak w godzinę uruchomić system gdzie indziej”.

Krok	Co robi	Wpływ na produkcję
Włączenie replikacji	tworzy w regionie docelowym grupę, sieć i dyski repliki	brak
Test failover	uruchamia kopię maszyny w izolowanej sieci	brak
Cleanup test failover	usuwa maszyny testowe	brak
Failover	uruchamia maszynę w regionie docelowym z wybranego punktu	produkcja przechodzi do regionu zapasowego
Commit	zatwierdza punkt odzyskiwania	brak odwrotu do innych punktów
Re-protect	odwraca replikację	przygotowanie do powrotu
Failback	przełączenie z powrotem	jak failover

Przy odzyskiwaniu między regionami magazyn Site Recovery stawiamy w regionie innym niż maszyna źródłowa, najlepiej w regionie docelowym (w laboratorium `rsv-lab-se` w `swedencentral`). Site Recovery umie też odzyskiwanie między strefami jednego regionu. Test zawsze uruchamiamy w sieci odizolowanej od produkcji, żeby kopia maszyny z tym samym adresem nie zderzyła się z oryginałem. Plany odzyskiwania (recovery plans) grupują maszyny i określają kolejność ich uruchamiania.

Zasady testów odtwarzania w Zielonej i dziennik testu opisuje strona Testy odtwarzania: plik, maszyna, baza i cała lokalizacja.

Zadania laboratoryjne

1. Tworzymy w `swedencentral` grupę `rg-lab-dr`, sieć `vnet-lab-dr` (10.32.64.0/20) i izolowaną `vnet-lab-test` (10.32.80.0/20, bez peeringu).
2. Włączamy replikację `vm-lab-db01` do `swedencentral` z ekranu Disaster recovery maszyny, magazyn `rsv-lab-se`.
3. Czekamy na stan „Protected”, uruchamiamy test failover do `vnet-lab-test`, logujemy się do kopii przez konsolę szeregową.
4. Sprzątamy test, a potem (opcjonalnie) wykonujemy pełny failover, commit i re-protect.
5. Wyłączamy replikację i usuwamy `rg-lab-dr` tego samego dnia: replikacja zużywa miejsce i transfer.

Pułapki egzaminacyjne

- Test failover nie wpływa na maszynę źródłową, failover tak.
- Przy odzyskiwaniu między regionami magazyn Site Recovery i jego grupa zasobów nie mogą być w regionie maszyny źródłowej (przy odzyskiwaniu między strefami mogą), a Microsoft zaleca region docelowy równy regionowi magazynu.
- Po failoverze trzeba wykonać re-protect, żeby mieć replikację w drugą stronę.
- Site Recovery to nie kopia zapasowa: usunięty plik zreplikuje się do regionu zapasowego.

Ćwiczenia

1. Po teście przełączenia zapomnieliśmy o sprzątaniu. Co zostaje i dlaczego to problem?

Odpowiedź

Zostaje działająca kopia maszyny w izolowanej sieci w regionie docelowym, z dyskami i kartą sieciową, rozliczana jak zwykła maszyna. Dopóki test nie jest posprzątany, Site Recovery nie pozwoli uruchomić kolejnego testu dla tego elementu. Dlatego po każdym teście wykonujemy Cleanup test failover.

Częste błędy

Objaw	Przyczyna	Co robimy
W Log Analytics brak tabeli `StorageBlobLogs`	ustawienie diagnostyczne na koncie, a nie na `blobServices/default`	ustawienie na zasobie usługi blobów
`Heartbeat` pusty	brak agenta lub reguły zbierania danych	VM Insights albo AMA z DCR
Zapytanie z CLI zgłasza zły obszar	podany identyfikator zasobu zamiast `customerId`	`az monitor log-analytics workspace show --query customerId`
Alert procesora nie wysyła e-maili	brak grupy akcji albo aktywna reguła przetwarzania	sprawdzamy akcje reguły i reguły przetwarzania
Nie da się zmienić nadmiarowości magazynu kopii	element już objęty ochroną	ustawienie przed pierwszą kopią, nowy magazyn
Magazynu kopii nie da się usunąć	elementy w miękkim usunięciu, aktywna replikacja	czekamy albo odzyskujemy i usuwamy trwale, wyłączamy replikację
Test failover się nie uruchamia	poprzedni test nieposprzątany	Cleanup test failover

Powiązane: Sieć: VNet, peering, trasy, NSG, Bastion, prywatne punkty końcowe, DNS i Load Balancer · Próbny egzamin AZ-104 i strategia na dzień egzaminu · Strategia kopii zapasowych

Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje · Testy odtwarzania: plik, maszyna, baza i cała lokalizacja · Azure Site Recovery dla Hyper-V bez VMM: replikacja, test, przełączenie i powrót

Źródła: Microsoft Learn: przewodnik do egzaminu AZ-104 (lista od 17 kwietnia 2026), dokumentacja `az monitor log-analytics query` (rozszerzenie, `--workspace` jako GUID, `--timespan`) i `az monitor alert-processing-rule` (rozszerzenie `alertsmanagement`, typy reguł, harmonogram); pomoc Azure CLI 2.91.0 (`az monitor log-analytics workspace create`, `metrics list`, `diagnostic-settings create` i `subscription create`, `action-group create` z formatem `--action email`, `metrics alert create`, `activity-log alert create`, `az backup vault create`, `vault backup-properties set`, `protection enable-for-vm`, `protection backup-now` z formatem daty, `policy list`, `recoverypoint list`, `restore restore-disks`, `job list`); dokumentacja modułu Az (`New-AzOperationalInsightsWorkspace`, `Invoke-AzOperationalInsightsQuery`, `Get-AzMetric`, `New-AzDiagnosticSetting`, `New-AzActionGroup`, `New-AzActionGroupEmailReceiverObject`, `Add-AzMetricAlertRuleV2`, `New-AzMetricAlertRuleV2Criteria`, `New-AzRecoveryServicesVault`, `Set-AzRecoveryServicesBackupProperty`, `Enable-AzRecoveryServicesBackupProtection`, `New-AzDataProtectionBackupVaultStorageSettingObject`, `New-AzDataProtectionBackupVault`, `Start-AzRecoveryServicesAsrTestFailoverJob`), stan na 19 października 2026.

Revision #4
Created 2026-10-18 23:00:26 UTC by Tomasz Konieczny
Updated 2026-11-01 18:03:22 UTC by Tomasz Konieczny