Magazyn: konta, nadmiarowość, SAS, Blob, Azure Files i zabezpieczenia

Poziom: średnio

Dotyczy: AZ-104, domena „Implement and manage storage” (15 do 20%), konta magazynu ogólnego przeznaczenia v2, Blob Storage, Azure Files, AzCopy, Azure Storage Explorer, Azure CLI 2.91, moduł Az

Czas: 4 dni po 1,5 do 2 godzin

Dni 8 do 11 programu: konto magazynu i jego nadmiarowość, zapora i szyfrowanie, klucze i tokeny SAS, kontenery blobów z warstwami, cyklem życia, wersjami i miękkim usuwaniem, wreszcie udziały Azure Files z migawkami. Wracamy tu przy każdym pytaniu „kto i jak dostaje się do danych w koncie”.

ZAŁOŻENIA SCENARIUSZA

konta laboratorium stoją w grupie `rg-lab-magazyn`. Konto podstawowe jest w `polandcentral`, a konto do ćwiczeń z nadmiarowością geograficzną i replikacją obiektów w `swedencentral`, bo `polandcentral` jest według Microsoftu regionem bez pary i dostępność GRS sprawdzamy tam osobno (do potwierdzenia). Publiczne adresy biura Zielonej (203.0.113.10) i magazynu (203.0.113.40) służą tylko jako przykład reguł zapory; produkcyjne archiwum kopii opisuje strona Zimne archiwum w chmurze: Azure Blob Storage i Amazon S3 Glacier.

Skróty użyte na tej stronie (21)

Skrót	Co znaczy
ACL	Access Control List: lista, kto ma jakie prawa do pliku lub zasobu
AD DS	Active Directory Domain Services: rola Windows Server uruchamiająca właściwą usługę katalogową Active Directory na kontrolerze domeny
AZ-104	numer egzaminu Microsoft Azure Administrator: egzamin, którego zdanie daje certyfikat Microsoft Certified: Azure Administrator Associate, ważny rok i odnawiany bezpłatną oceną online

Skrót	Co znaczy
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
GiB	gibibajt: 1024 MiB, czyli około 1,07 GB; tej jednostki używa dokumentacja MailCow przy wymaganiach pamięci
GRS	Geo-Redundant Storage: nadmiarowość w Azure, która dodatkowo kopiuje dane do drugiego, odległego regionu
GZRS	Geo-Zone-Redundant Storage: nadmiarowość w Azure łącząca strefy dostępności w regionie głównym z kopią w drugim regionie
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
LRS	Locally Redundant Storage: nadmiarowość w Azure, która trzyma trzy kopie danych w jednym centrum danych
NFS	Network File System: udostępnianie katalogów po sieci w świecie Linuksa
NTFS	New Technology File System: system plików Windows z wbudowanymi uprawnieniami ACL na poziomie pliku i folderu
RA-GRS	Read-Access Geo-Redundant Storage: nadmiarowość GRS z możliwością odczytu danych z regionu dodatkowego
RA-GZRS	Read-Access Geo-Zone-Redundant Storage: nadmiarowość GZRS z możliwością odczytu danych z regionu dodatkowego
SAS	Serial Attached SCSI: złącze i magistrala dyskowa w serwerach, następca równoległego SCSI, pozwala podłączyć wiele dysków i macierzy przez jeden kontroler z większą przepustowością niż SATA; w Azure także Shared Access Signature: podpisany adres z tokenem, który daje czasowy dostęp do danych w koncie magazynu
SKU	Stock Keeping Unit: oznaczenie pozycji handlowej, na przykład konkretnej licencji lub modelu
SMB	Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
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`. Nazwę konta (`NazwaKonta`) wybieramy sami: od 3 do 24 znaków, tylko małe litery i cyfry, unikatowa w całym Azure. Polecenia

danych (kontenery, bloby) uruchamiamy z `--auth-mode login`, czyli tożsamością Entra ID, a nie kluczem konta, co wymaga roli danych, na przykład Storage Blob Data Contributor. Parametry sprawdziliśmy w pomocy Azure CLI 2.91.0 i w dokumentacji modułu Az (19 października 2026).

◫◫ ZMIENIA SYSTEM

Utworzenie konta magazynu: az storage account create

```
az storage account create --name NazwaKonta --resource-group rg-lab-magazyn --location
polandcentral \
  --sku Standard_LRS --kind StorageV2 --access-tier Hot --min-tls-version TLS1_2 \
  --allow-blob-public-access false --https-only true
```

Bez `--sku` CLI 2.91 wybiera `Standard_RAGRS`, co w regionie bez pary może się nie udać, dlatego SKU podajemy zawsze. W PowerShell: `New-AzStorageAccount -ResourceGroupName rg-lab-magazyn -Name NazwaKonta -Location polandcentral -SkuName Standard_LRS -Kind StorageV2 -MinimumTlsVersion TLS1_2 -AllowBlobPublicAccess $false`.

◫◫ **CLI** = Command Line Interface: praca przez wpisywanie komend w terminalu · **SKU** = Stock Keeping Unit: oznaczenie pozycji handlowej, na przykład konkretnej licencji lub modelu · **az** = Azure CLI: narzędzie chmury Microsoftu

◫◫ ZMIENIA SYSTEM

Zmiana nadmiarowości konta: az storage account update --sku

```
az storage account update --name NazwaKonta --resource-group rg-lab-magazyn --sku
Standard_GRS
```

Przejście między LRS a GRS lub RA-GRS robimy zmianą SKU. Przejście na nadmiarowość strefową (ZRS, GZRS) to konwersja, której warunki sprawdzamy w dokumentacji „Change how a storage account is replicated”.

◫◫ **LRS** = Locally Redundant Storage: nadmiarowość w Azure, która trzyma trzy kopie danych w jednym centrum danych · **GRS** = Geo-Redundant Storage: nadmiarowość w Azure, która dodatkowo kopiuje dane do drugiego, odległego regionu · **RA-GRS** = Read-Access Geo-Redundant Storage: nadmiarowość GRS z możliwością odczytu danych z regionu dodatkowego · **SKU** = Stock Keeping Unit: oznaczenie pozycji handlowej, na przykład konkretnej licencji lub modelu · **ZRS** = Zone-Redundant Storage: nadmiarowość w Azure, która rozkłada kopie danych na kilka stref dostępności w jednym regionie · **GZRS** = Geo-Zone-Redundant Storage: nadmiarowość w Azure łącząca strefy dostępności w regionie głównym z kopią w drugim regionie · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Dodanie publicznego adresu do zapory konta: az storage account network-rule add

```
az storage account network-rule add --resource-group rg-lab-magazyn --account-name NazwaKonta --ip-address 203.0.113.10
```

Reguły IP dotyczą adresów publicznych. Adresu prywatnego z naszej sieci tu nie wpisujemy: dla sieci wirtualnej dodajemy regułę podsieci (`--vnet-name` i `--subnet`), co wymaga punktu końcowego usługi `Microsoft.Storage` w tej podsieci.

□□ **IP** = Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection) · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Zamknięcie konta dla wszystkich spoza reguł: az storage account update --default-action Deny

```
az storage account update --name NazwaKonta --resource-group rg-lab-magazyn --default-action Deny --bypass AzureServices
```

Od tej chwili wejdą tylko adresy i podsieci z reguł oraz zaufane usługi Azure. Kolejność ma znaczenie: najpierw reguły, potem odmowa. W PowerShell: `Update-AzStorageAccountNetworkRuleSet -ResourceGroupName rg-lab-magazyn -Name NazwaKonta -DefaultAction Deny -Bypass AzureServices`.

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

□□ TYLKO ODCZYT

Odnowienie klucza dostępu: az storage account keys renew

```
az storage account keys renew --resource-group rg-lab-magazyn --account-name NazwaKonta --key key2
```

Konto ma dwa klucze, żeby zmieniać je po kolei: aplikacje przełączamy na `key1`, odnawiamy `key2`, potem odwrotnie. Odnowienie klucza unieważnia wszystkie tokeny SAS podpisane tym kluczem. W PowerShell: `New-AzStorageAccountKey -ResourceGroupName rg-lab-magazyn -Name NazwaKonta -KeyName key2`.

□□ **SAS** = Serial Attached SCSI: złącze i magistrala dyskowa w serwerach, następca równoległego SCSI, pozwala podłączyć wiele dysków i macierzy przez jeden kontroler z większą przepustowością niż SATA; w Azure także Shared Access Signature: podpisany adres z tokenem, który daje czasowy dostęp do danych w koncie magazynu · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ ZMIENIA SYSTEM

Utworzenie kontenera: az storage container create

```
az storage container create --name dokumenty --account-name NazwaKonta --auth-mode login
```

Kontener jest prywatny, o ile nie podamy `--public-access`. Na koncie z `--allow-blob-public-access false` dostępu publicznego i tak się nie włączy.

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

□□ ZMIENIA SYSTEM

Utworzenie zasady przechowywanej na kontenerze: az storage container policy create

```
az storage container policy create --container-name dokumenty --name odczyt-tydzien \
  --permissions rl --expiry 2026-11-30T23:59:00Z --account-name NazwaKonta --account-key
KluczKonta
```

> **Pojęcie: zasada przechowywana (stored access policy).** Zapisane na kontenerze uprawnienia i termin, do których odwołuje się token SAS. Zmiana albo usunięcie zasady zmienia albo unieważnia wszystkie tokeny z niej wydane, bez odnawiania klucza. Zasada przechowywana działa z SAS usługi podpisanym kluczem konta, stąd `--account-key` zamiast `--auth-mode login`.

□□ **SAS** = Serial Attached SCSI: złącze i magistrala dyskowa w serwerach, następca równoległego SCSI, pozwala podłączyć wiele dysków i macierzy przez jeden kontroler z większą przepustowością niż SATA; w Azure także Shared Access Signature: podpisany adres z tokenem, który daje czasowy dostęp do danych w koncie magazynu · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Wygenerowanie tokenu SAS z zasady przechowywanej: az storage container generate-sas

```
az storage container generate-sas --name dokumenty --policy-name odczyt-tydzien \
  --account-name NazwaKonta --account-key KluczKonta --https-only -o tsv
```

Wynikiem jest ciąg zapytania doklejany do adresu kontenera. Uprawnienia i termin pochodzą z zasady. W PowerShell: `New-AzStorageContainerSASToken -Name dokumenty -Policy odczyt-tydzien -Context $kontekst`.

SAS = Serial Attached SCSI: złącze i magistrala dyskowa w serwerach, następca równoległego SCSI, pozwala podłączyć wiele dysków i macierzy przez jeden kontroler z większą przepustowością niż SATA; w Azure także Shared Access Signature: podpisany adres z tokenem, który daje czasowy dostęp do danych w koncie magazynu · **az** = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Wygenerowanie SAS delegowanego przez użytkownika: az storage blob generate-sas --as-user

```
az storage blob generate-sas --account-name NazwaKonta --container-name dokumenty --name NazwaPliku \
  --permissions r --expiry 2026-10-26T12:00:00Z --auth-mode login --as-user --https-only --full-uri
```

SAS delegowany przez użytkownika jest podpisany kluczem uzyskanym z Entra ID, a nie kluczem konta, więc rotacja kluczy konta go nie dotyczy. Microsoft zaleca go jako najbezpieczniejszy rodzaj SAS dla blobów.

SAS = Serial Attached SCSI: złącze i magistrala dyskowa w serwerach, następca równoległego SCSI, pozwala podłączyć wiele dysków i macierzy przez jeden kontroler z większą przepustowością niż SATA; w Azure także Shared Access Signature: podpisany adres z tokenem, który daje czasowy dostęp do danych w koncie magazynu · **az** = Azure CLI: narzędzie chmury Microsoftu

OSTROŻNIE · NIEODWRACALNE

Włączenie miękkiego usuwania i wersji blobów: az storage account blob-service-properties update

```
az storage account blob-service-properties update --account-name NazwaKonta --resource-group rg-lab-magazyn \
  --enable-delete-retention true --delete-retention-days 14 \
  --enable-container-delete-retention true --container-delete-retention-days 14 \
  --enable-versioning true
```

Miękkie usuwanie blobów i kontenerów oraz wersjonowanie włączamy osobnymi parametrami. W PowerShell: `Enable-AzStorageBlobDeleteRetentionPolicy -ResourceGroupName rg-lab-magazyn -StorageAccountName NazwaKonta -RetentionDays 14` i `Update-AzStorageBlobServiceProperty -ResourceGroupName rg-lab-magazyn -StorageAccountName NazwaKonta -IsVersioningEnabled $true`.

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

□□ TYLKO ODCZYT

Odzyskanie usuniętego blobu: az storage blob undelete

```
az storage blob undelete --account-name NazwaKonta --container-name dokumenty --name NazwaPliku --auth-mode login
```

Działa w okresie miękkiego usuwania. Listę usuniętych blobów pokazuje `az storage blob list --container-name dokumenty --include d --account-name NazwaKonta --auth-mode login`.

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

□□ ZMIENIA SYSTEM

Ustawienie reguły cyklu życia: az storage account management-policy create

```
az storage account management-policy create --account-name NazwaKonta --resource-group rg-lab-magazyn --policy @cykl-zycia.json
```

Reguła przenosi bloby między warstwami i usuwa je po czasie liczonym od modyfikacji albo ostatniego dostępu. Plik niżej.

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

□□ PLIK KONFIGURACYJNY

Reguła cyklu życia dla kontenera dokumenty: cykl-zycia.json

```
{
  "rules": [
    {
      "enabled": true,
```

```
      "name": "dokumenty-cool-archive-usun",
      "type": "Lifecycle",
      "definition": {
        "filters": {
          "blobTypes": ["blockBlob"],
          "prefixMatch": ["dokumenty/"]
        },
        "actions": {
          "baseBlob": {
            "tierToCool": { "daysAfterModificationGreaterThan": 30 },
            "tierToArchive": { "daysAfterModificationGreaterThan": 180 },
            "delete": { "daysAfterModificationGreaterThan": 730 }
          },
          "version": {
            "delete": { "daysAfterCreationGreaterThan": 90 }
          }
        }
      }
    }
  ]
}
```

Prefiks zaczyna się od nazwy kontenera. Bloby przenoszone do Archive potrzebują konta z LRS, GRS albo RA-GRS (ZRS i GZRS nie obsługują warstwy Archive), o czym więcej na stronie o zimnym archiwum.

□□ **LRS** = Locally Redundant Storage: nadmiarowość w Azure, która trzyma trzy kopie danych w jednym centrum danych · **GRS** = Geo-Redundant Storage: nadmiarowość w Azure, która dodatkowo kopiuje dane do drugiego, odległego regionu · **RA-GRS** = Read-Access Geo-Redundant Storage: nadmiarowość GRS z możliwością odczytu danych z regionu dodatkowego ·**ZRS** = Zone-Redundant Storage: nadmiarowość w Azure, która rozkłada kopie danych na kilka stref dostępności w jednym regionie · **GZRS** = Geo-Zone-Redundant Storage: nadmiarowość w Azure łącząca strefy dostępności w regionie głównym z kopią w drugim regionie

□□ ZMIENIA SYSTEM

Utworzenie zasady replikacji obiektów: az storage account or-policy create

```
az storage account or-policy create --account-name NazwaKontaDocelowego --resource-group
rg-lab-magazyn \
  --source-account NazwaKontaZrodlowego --destination-account NazwaKontaDocelowego \
  --source-container dokumenty --destination-container dokumenty-kopia
```

Replikacja obiektów asynchronicznie kopiuje bloby blokowe między kontami, także w innych regionach. Wymaga wersjonowania na obu kontach i kanału zmian (change feed) na koncie źródłowym.

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

□□ TYLKO ODCZYT

Wysłanie katalogu do kontenera: azcopy copy --recursive

```
azcopy login
azcopy copy '/srv/eksport/dokumenty'
'https://NazwaKonta.blob.core.windows.net/dokumenty' --recursive
```

`azcopy login` loguje przez Entra ID. Zamiast logowania można dokleić token SAS do adresu. Opcja `--block-blob-tier` wysyła od razu do wybranej warstwy.

□□ **SAS** = Serial Attached SCSI: złącze i magistrala dyskowa w serwerach, następca równoległego SCSI, pozwala podłączyć wiele dysków i macierzy przez jeden kontroler z większą przepustowością niż SATA; w Azure także Shared Access Signature: podpisany adres z tokenem, który daje czasowy dostęp do danych w koncie magazynu · **azcopy** = od Azure i copy: narzędzie wiersza poleceń do szybkiego kopiowania dużych ilości plików do i z Azure Storage, z możliwością wznowienia zadań

□□ OSTROŻNIE · NIEODWRACALNE

Utworzenie udziału Azure Files: az storage share-rm create

```
az storage share-rm create --resource-group rg-lab-magazyn --storage-account NazwaKonta
--name dzial-it --quota 100 --access-tier TransactionOptimized
```

Udział SMB o limicie 100 GiB. Polecenia `share-rm` idą przez płaszczyznę zarządzania (Azure Resource Manager), więc działają z rolą na koncie, bez klucza. W PowerShell: `New-AzRmStorageShare -ResourceGroupName rg-lab-magazyn -StorageAccountName NazwaKonta -Name dzial-it -QuotaGiB 100`.

□□ **SMB** = Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy · **GiB** = gibibajt: 1024 MiB, czyli około 1,07 GB; tej jednostki używa dokumentacja MailCow przy wymaganiach pamięci · **az** = Azure CLI: narzędzie chmury Microsoftu

◫◫ OSTROŻNIE · NIEODWRACALNE

Utworzenie migawki udziału: az storage share-rm snapshot

```
az storage share-rm snapshot --resource-group rg-lab-magazyn --storage-account
NazwaKonta --name dzial-it
```

Migawka to stan udziału tylko do odczytu, z której odtwarzamy pojedyncze pliki. W Windows widać ją jako „Poprzednie wersje”.

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

◫◫ OSTROŻNIE · NIEODWRACALNE

Włączenie miękkiego usuwania udziałów: az storage account file-service-properties update

```
az storage account file-service-properties update --account-name NazwaKonta --resource-
group rg-lab-magazyn \
  --enable-delete-retention true --delete-retention-days 14
```

Usunięty udział wraca przez `az storage share-rm restore` z parametrem `--deleted-version`, który odczytujemy z `az storage share-rm list --include-deleted`. W PowerShell: `Update-AzStorageFileServiceProperty -ResourceGroupName rg-lab-magazyn -StorageAccountName NazwaKonta -EnableShareDeleteRetentionPolicy $true -ShareRetentionDays 14`.

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

◫◫ KLIKAMY W INTERFEJSIE

Dostęp do udziału przez tożsamość i szyfrowanie w portalu

```
Portal Azure → Konto magazynu → Data storage → File shares → Identity-based access →
Configure
Portal Azure → Konto magazynu → Security + networking → Encryption → Encryption type
```

Pierwszy ekran wybiera źródło tożsamości dla SMB: lokalne AD DS, Microsoft Entra Domain Services albo Microsoft Entra Kerberos. Drugi przełącza klucze szyfrowania między zarządzanymi przez Microsoft a własnymi w Key Vault.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Identity-based access konta laboratorium z trzema źródłami tożsamości (AD DS, Microsoft Entra Domain Services, Microsoft Entra Kerberos), żadne niewłączone, i sekcja Default share-level permissions.

SMB = Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy · **AD DS** = Active Directory Domain Services: rola Windows Server uruchamiająca właściwą usługę katalogową Active Directory na kontrolerze domeny

Dzień 8: konto magazynu, nadmiarowość, szyfrowanie i zapora

Z ŻYCIA WZIĘTE

Poniedziałek, 9:30. Tomek zakłada pierwsze konto bez parametru `--sku`, a polecenie po kilku sekundach kończy się błędem o niedostępnej nadmiarowości w regionie. Sprawdzamy w pomocy CLI: domyślny SKU to `Standard_RAGRS`, a `polandcentral` jest regionem bez pary. Tomek powtarza polecenie z `Standard_LRS` i zapisuje w dzienniku dwie rzeczy: SKU podajemy zawsze, a ćwiczenia z GRS robimy w `swedencentral`.

Cele egzaminu

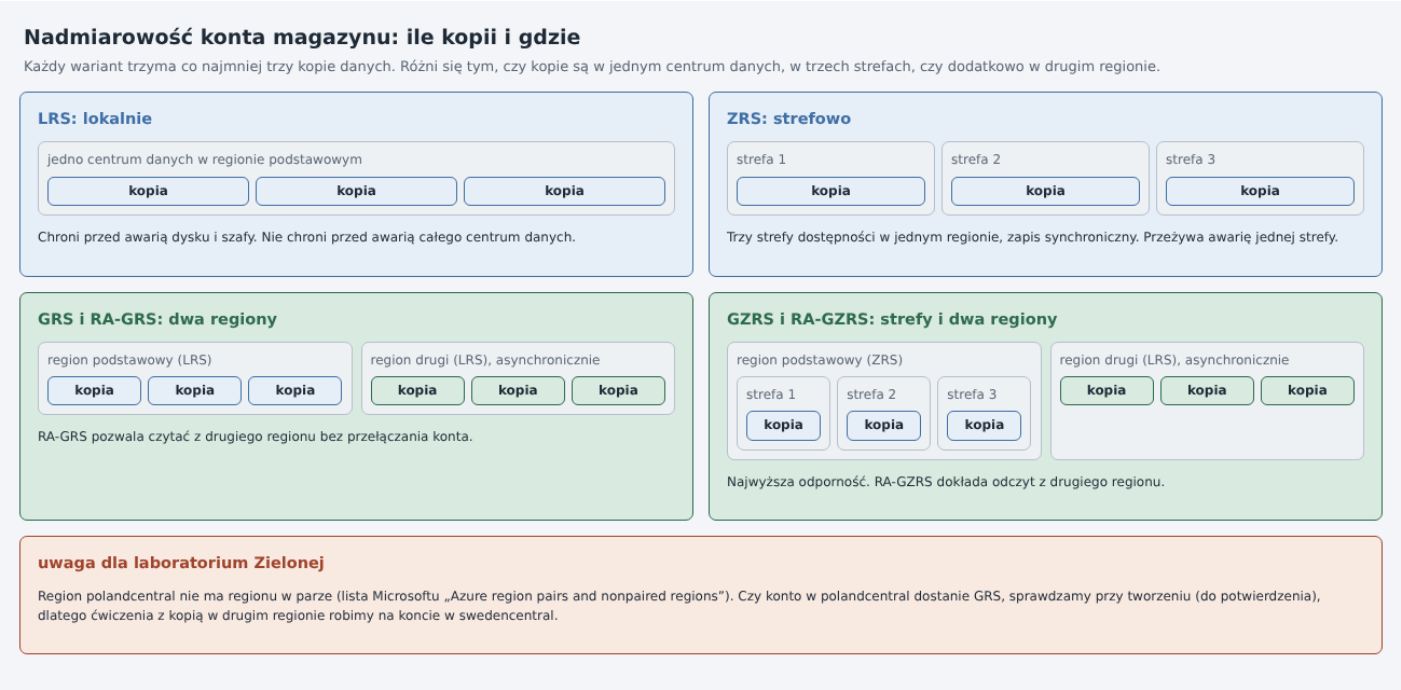
- tworzenie i konfiguracja kont magazynu
- konfiguracja nadmiarowości Azure Storage
- konfiguracja szyfrowania konta
- konfiguracja zapór i sieci wirtualnych dla Azure Storage

Jak to działa

Pojęcie: konto magazynu (storage account). Kontener najwyższego poziomu dla danych w Azure Storage, z jedną nazwą w całym Azure i punktami końcowymi dla blobów, plików, kolejek i tabel, na przykład `https://NazwaKonta.blob.core.windows.net`. Na koncie

ustawiamy nadmiarowość, sieć, szyfrowanie i domyślną warstwę dostępu.

Rodzaj konta	Do czego	Uwagi
Standard, ogólnego przeznaczenia v2 (StorageV2)	bloby, pliki, kolejki, tabele	domyślny wybór, wszystkie warstwy Blob
Premium, bloby blokowe	bloby o niskim opóźnieniu	dyski SSD, bez warstw Cool i Archive
Premium, udziały plików	Azure Files o wysokiej wydajności	SMB i NFS
Premium, bloby stronicowe	dyski niezarządzane, starsze scenariusze	rzadko na egzaminie



Rysunek 1. Nadmiarowość konta magazynu: LRS trzy kopie w jednym centrum danych, ZRS w trzech strefach, GRS i RA-GRS z kopią w drugim regionie, GZRS i RA-GZRS ze strefami i drugim regionem; polandcentral jest regionem bez pary (kliknięcie otwiera pełny rozmiar)

Wariant	Kopie	Przeżywa	Odczyt z drugiego regionu
LRS	3 w jednym centrum danych	awarię dysku, szafy	nie
ZRS	3 w trzech strefach	awarię strefy	nie
GRS	LRS plus LRS w drugim regionie	awarię regionu (po przełączeniu)	nie
RA-GRS	jak GRS	jak GRS	tak, stale

Wariant	Kopie	Przeżywa	Odczyt z drugiego regionu
GZRS	ZRS plus LRS w drugim regionie	awarię strefy i regionu	nie
RA-GZRS	jak GZRS	jak GZRS	tak, stale

Dane w Azure Storage są zawsze szyfrowane w spoczynku. Domyślnie kluczami zarządzanymi przez Microsoft, a na żądanie kluczami klienta w Azure Key Vault. Szyfrowanie infrastruktury (drugą warstwę) włączamy tylko przy tworzeniu konta parametrem `--require-infrastructure-encryption`.

Zapora konta ma domyślną akcję (Allow albo Deny), reguły adresów publicznych, reguły podsieci i wyjątki dla zaufanych usług Azure. Prywatne punkty końcowe opisujemy na stronie o sieci, bo egzamin trzyma je w domenie sieci.

Zadania laboratoryjne

1. Tworzymy konto LRS w `polandcentral` i konto GRS w `swedencentral`, oba z TLS 1.2 i bez publicznego dostępu do blobów.
2. Zmieniamy konto w `swedencentral` z GRS na RA-GRS i odczytujemy jego drugi punkt końcowy `az storage account show --name NazwaKonta --query secondaryEndpoints`.
3. Dodajemy regułę IP 203.0.113.10, ustawiamy domyślną odmowę, a potem próbujemy wylistować kontenery z Cloud Shell. Zapisujemy, co się stało, i dodajemy własny adres publiczny.
4. W portalu oglądamy ustawienie szyfrowania i sprawdzamy, które opcje da się zmienić po utworzeniu konta, a które nie.

Pułapki egzaminacyjne

- RA-GRS i RA-GZRS dają odczyt z drugiego regionu zawsze, GRS i GZRS dopiero po przełączeniu konta.
- Warstwa Archive działa tylko na kontach LRS, GRS i RA-GRS.
- Reguła sieci wirtualnej w zaporze konta wymaga punktu końcowego usługi w podsieci, a prywatny punkt końcowy nie wymaga reguły w zaporze.
- Domyślna akcja Deny bez reguły dla własnego adresu odcina także portal i Cloud Shell od danych.

Ćwiczenia

1. Aplikacja w Zielonej ma czytać dokumenty nawet wtedy, gdy region podstawowy jest niedostępny, bez żadnego działania administratora. Który wariant nadmiarowości wybieramy i dlaczego nie GRS?

Odpowiedź

RA-GRS albo RA-GZRS. Oba udostępniają stały punkt końcowy do odczytu w drugim regionie. Przy GRS kopia w drugim regionie istnieje, ale czytać z niej można dopiero po przełączeniu konta (failover), co wymaga działania i trwa.

1. Konto ma domyślną akcję Deny i regułę dla podsieci `snet-web`. Maszyna w tej podsieci nadal dostaje odmowę. Co sprawdzamy?

Odpowiedź

Czy podsieć `snet-web` ma punkt końcowy usługi `Microsoft.Storage` (bez niego reguła podsieci nie działa) i czy ruch idzie do publicznego punktu końcowego konta, a nie przez inną drogę, na przykład serwer pośredniczący. Sprawdzamy też, czy reguła dotyczy właściwej sieci i podsieci.

Dzień 9: klucze, SAS, zasady przechowywane i tożsamość

> **Z ŻYCIA WZIĘTE**
>
> Wtorek, 13:10. Ola prosi o link, przez który klient przez tydzień pobierze paczkę z kontenera `dokumenty`. Tomek generuje SAS podpisany kluczem konta, ważny siedem dni, a po godzinie Ola pisze, że link trafił do niewłaściwej osoby. Jedyna droga cofnięcia takiego tokenu to odnowienie klucza, a z tego klucza korzystają jeszcze dwie aplikacje. Następny link Tomek wydaje już z zasady przechowywanej, którą da się usunąć jednym poleceniem.

Cele egzaminu

- tworzenie i używanie tokenów SAS
- konfiguracja zasad przechowywanych
- zarządzanie kluczami dostępu
- konfiguracja dostępu przez tożsamość do Azure Files

Jak to działa

> **Pojęcie: SAS (Shared Access Signature).** Podpisany ciąg doklejany do adresu zasobu, który daje ograniczony dostęp: określone uprawnienia, czas, opcjonalnie adresy IP i tylko HTTPS. Kto ma link, ten ma dostęp, więc SAS traktujemy jak hasło.

Rodzaj SAS	Czym podpisany	Zakres	Jak cofnąć
Delegowany przez użytkownika	kluczem delegowania z Entra ID	bloby (i Data Lake)	odwołanie kluczy delegowania albo zmiana roli
Usługi	kluczem konta	jedna usługa: blob, plik, kolejka albo tabela	usunięcie zasady przechowywanej albo odnowienie klucza
Konta	kluczem konta	wiele usług i operacje na poziomie usługi	tylko odnowienie klucza

Zasada przechowywana może stać za SAS usługi. Microsoft pozwala na nie więcej niż pięć takich zasad na kontenerze, udziale, kolejce albo tabeli. Klucze konta dają pełny dostęp do wszystkich danych, dlatego zalecaną drogą jest Entra ID z rolami danych, a w nowych kontach można wręcz wyłączyć autoryzację kluczem (`--allow-shared-key-access false`).

Azure Files przez SMB może uwierzytelniać tożsamością z lokalnego AD DS, z Microsoft Entra Domain Services albo przez Microsoft Entra Kerberos dla tożsamości hybrydowych. Dostęp ma dwa piętra: rola na poziomie udziału (Storage File Data SMB Share Reader, Contributor albo Elevated Contributor) i uprawnienia NTFS na katalogach i plikach, takie same jak na `fs01`.

Zadania laboratoryjne

1. Tworzymy zasadę przechowywaną `odczyt-tydzien` (`rl`, tydzień), wydajemy z niej SAS i pobieramy plik `curl` z adresem z tokenem.
2. Usuwamy zasadę `az storage container policy delete --container-name dokumenty --name odczyt-tydzien --account-name NazwaKonta --account-key KluczKonta` i sprawdzamy, że link przestał działać.
3. Wydajemy SAS delegowany przez użytkownika na jeden plik, ważny dwie godziny.
4. Odnawiamy `key2` i sprawdzamy, który z tokenów przestał działać.
5. W portalu oglądamy ekran dostępu przez tożsamość dla Azure Files i opisujemy w dzienniku, jakie role i uprawnienia NTFS dostałby dział IT Zielonej.

Pułapki egzaminacyjne

- SAS konta nie da się cofnąć inaczej niż odnowieniem klucza.
- SAS delegowany przez użytkownika działa tylko dla blobów, a nie dla Azure Files przez SMB.
- Odnowienie klucza unieważnia SAS podpisane tym kluczem, a nie tym drugim.

- Rola Reader na koncie nie daje dostępu do danych przez Entra ID, potrzebna jest rola danych.

Ćwiczenia

1. Partner ma przez miesiąc dopisywać pliki do kontenera `przyjecia`, a my chcemy móc w każdej chwili odebrać mu dostęp bez wpływu na inne aplikacje. Co wydajemy?

Odpowiedź

SAS usługi powiązany z zasadą przechowywaną na kontenerze `przyjecia`, z uprawnieniami dodawania i zapisu (na przykład `acw`) i terminem w zasadzie. Odebranie dostępu to usunięcie albo zmiana zasady, bez odnawiania klucza, którego używają inne aplikacje. Alternatywą jest SAS delegowany przez użytkownika, ale jego cofnięcie dotyczy wszystkich kluczy delegowania danej tożsamości.

1. Użytkownik z rolą Storage File Data SMB Share Contributor nie może zapisać pliku w katalogu udziału. Gdzie szukamy przyczyny?

Odpowiedź

W uprawnieniach NTFS katalogu. Rola na poziomie udziału pozwala wejść do udziału z prawem zapisu, ale ostateczne prawa do katalogów i plików wyznaczają listy ACL NTFS, jak na zwykłym serwerze plików.

Dzień 10: Blob, warstwy, cykl życia, wersje i replikacja obiektów

Z ŻYCIA WZIĘTE

Środa, 16:05. Pani Halina pyta, czy da się odzyskać skan umowy, który przed chwilą „chyba skasowała” z folderu w portalu dokumentów, a który pod spodem leży w kontenerze `dokumenty`. Tomek sprawdza `az storage blob list --include d` i widzi plik z oznaczeniem usunięcia sprzed dziesięciu minut. Jedno `az storage blob undelete` i plik wraca. Pani Halina pyta, jak długo to działa, a Tomek odpowiada, że w laboratorium czternaście dni, bo tyle ustawiliśmy.

Cele egzaminu

- tworzenie i konfiguracja kontenera w Azure Blob Storage
- konfiguracja warstw magazynu
- konfiguracja miękkiego usuwania blobów i kontenerów
- konfiguracja zarządzania cyklem życia blobów
- konfiguracja wersjonowania blobów
- konfiguracja replikacji obiektów
- zarządzanie danymi przy pomocy Azure Storage Explorer i AzCopy

Jak to działa

> **Pojęcie: warstwa dostępu.** Ustawienie blobu decydujące o cenie przechowywania, cenie odczytu i czasie dostępu. Pełną tabelę warstw z minimalnymi czasami przechowywania (Cool 30 dni, Cold 90 dni, Archive 180 dni) i opisem rehydratacji mamy na stronie Zimne archiwum w chmurze: Azure Blob Storage i Amazon S3 Glacier, więc tu jej nie powtarzamy.

Mechanizm	Przed czym chroni	Ważne szczegóły
Miękkie usuwanie blobów	usunięcie i nadpisanie blobu	okres ustawiany w dniach; `undelete`
Miękkie usuwanie kontenerów	usunięcie całego kontenera	osobny parametr
Wersjonowanie	nadpisanie, z dostępem do każdej poprzedniej wersji	każda zmiana tworzy wersję i kosztuje miejsce
Migawka blobu	stan z chwili wykonania	ręcznie, tylko do odczytu
Niezmienność	usunięcie i zmiana w okresie retencji	opisana na stronie o archiwum
Replikacja obiektów	utrata regionu albo konta, kopia do innej aplikacji	asynchroniczna, wymaga wersjonowania i kanału zmian

Reguły cyklu życia działają raz na dobę, więc efekt nowej reguły może pojawić się dopiero po około dobie (dokładny czas sprawdzamy w dokumentacji). Warunek `daysAfterLastAccessTimeGreaterThan` wymaga włączonego śledzenia ostatniego dostępu (`--enable-last-access-tracking`).

Azure Storage Explorer to bezpłatna aplikacja na komputer do przeglądania kont, kontenerów, udziałów i kolejek, z logowaniem Entra ID albo SAS. AzCopy to narzędzie wiersza poleceń do kopiowania dużych ilości danych, także między kontami bez pobierania na dysk.

Zadania laboratoryjne

1. Tworzymy kontener `dokumenty`, wysyłamy do niego katalog przez AzCopy, a potem przeglądamy go w Storage Explorer.
2. Włączamy miękkie usuwanie blobów i kontenerów (14 dni) oraz wersjonowanie. Nadpisujemy plik dwa razy i przywracamy wersję pierwszą w portalu.
3. Usuwamy plik i odzyskujemy go `az storage blob undelete`.
4. Wdrażamy regułę z pliku `cykl-zycia.json` i sprawdzamy ją `az storage account management-policy show --account-name NazwaKonta --resource-group rg-lab-magazyn`.
5. Na koncie w `swedencentral` tworzymy kontener `dokumenty-kopia`, włączamy wersjonowanie na obu kontach i kanał zmian na źródłowym, a potem zasadę replikacji obiektów.

Pułapki egzaminacyjne

- Wersjonowanie i miękkie usuwanie to dwie różne rzeczy: pytanie o „przywrócenie poprzedniej treści pliku” wskazuje wersjonowanie, o „odzyskanie usuniętego pliku” miękkie usuwanie (albo wersje, jeśli włączone).
- Replikacja obiektów nie działa bez wersjonowania na obu kontach i kanału zmian na źródłowym.
- Reguła cyklu życia nie przenosi do Archive na koncie ZRS.
- Blob w Archive trzeba najpierw rehydratować, zanim da się go odczytać.

Ćwiczenia

1. Dokumenty mają być w warstwie Hot przez 30 dni od ostatniej modyfikacji, potem w Cool, po roku w Archive, a po siedmiu latach usuwane. Co ustawiamy i na jakim koncie?

Odpowiedź

Regułę cyklu życia z akcjami `tierToCool` po 30 dniach, `tierToArchive` po 365 dniach i `delete` po 2555 dniach od modyfikacji, na koncie z nadmiarowością LRS, GRS albo RA-GRS (Archive nie działa na ZRS i GZRS).

1. Dlaczego po dodaniu reguły cyklu życia bloby nie przeszły do Cool w ciągu godziny?

Odpowiedź

Bo zarządzanie cyklem życia uruchamia się raz na dobę i nowa reguła zaczyna działać z opóźnieniem. Sprawdzamy też, czy filtr prefiksu zaczyna się od nazwy kontenera i czy bloby są blokowe.

Dzień 11: Azure Files, migawki i miękkie usuwanie

> **Z ŻYCIA WZIĘTE**
>
> Czwartek, 10:40. Dział IT Zielonej rozważa przeniesienie części udziałów z `fs01` do Azure Files, a Tomek dostaje zadanie postawienia testowego udziału `dzial-it`. Po godzinie ktoś kasuje przez pomyłkę cały udział z portalu. Tomek odnajduje go na liście usuniętych udziałów, przywraca z wersji usuniętej, a pojedynczy nadpisany plik wyciąga z migawki porannej. Zapisuje, że miękkie usuwanie udziałów chroni cały udział, a migawka pojedyncze pliki.

Cele egzaminu

- tworzenie i konfiguracja udziału w Azure Files
- konfiguracja migawek i miękkiego usuwania dla Azure Files

Jak to działa

> **Pojęcie: Azure Files.** Udziały plików w chmurze dostępne przez SMB (Windows, Linux, macOS) albo NFS (konta premium), montowane jak zwykły udział sieciowy. Udział ma limit rozmiaru (quota) i warstwę: Transaction optimized, Hot albo Cool na kontach standardowych, Premium na kontach plikowych.

Ochrona	Zakres	Odtwarzanie
Migawka udziału	cały udział z chwili wykonania, tylko do odczytu	pojedyncze pliki albo cały udział
Miękkie usuwanie udziałów	usunięty udział	`az storage share-rm restore` w okresie retencji
Azure Backup dla Azure Files	migawki według harmonogramu z retencją	opisane na stronie o kopiach

Port 445 bywa blokowany przez dostawców internetu i sieci firmowe, więc montowanie udziału SMB z biura często wymaga VPN albo prywatnego punktu końcowego. Do synchronizacji udziału z serwerem lokalnym służy Azure File Sync (usługa synchronizacji, grupa synchronizacji, punkt końcowy w chmurze i na serwerze, warstwowanie do chmury). Na liście umiejętności z 17 kwietnia 2026 roku File Sync nie występuje, więc znamy go na poziomie pojęć.

Zadania laboratoryjne

1. Tworzymy udział `dzial-it` (100 GiB) i montujemy go z maszyny `vm-lab-web01` poleceniem podanym w portalu (Connect).
2. Włączamy miękkie usuwanie udziałów (14 dni), robimy migawkę, nadpisujemy plik i odtwarzamy go z migawki.
3. Usuwamy udział, odszukujemy go `az storage share-rm list --storage-account NazwaKonta --include-deleted` i przywracamy z `--deleted-version`.
4. Sprzątamy: `az group delete --name rg-lab-magazyn --yes --no-wait`, chyba że konto ma posłużyć w dniu 19 do prywatnego punktu końcowego.

Pułapki egzaminacyjne

- Migawka udziału nie zastępuje miękkiego usuwania: po usunięciu udziału bez miękkiego usuwania jego migawki też znikają.
- Montowanie SMB z internetu wymaga otwartego portu 445 po drodze.
- NFS w Azure Files to konta premium i dostęp z sieci wirtualnej, bez uwierzytelniania tożsamością użytkownika.

Ćwiczenia

1. Pracownik nadpisał plik w udziale `dzial-it` wczoraj po południu. Jak odzyskamy wersję z rana, jeżeli codzienna migawka powstaje o 7:00?

Odpowiedź

Z migawki z 7:00: w portalu (udział → Snapshots) albo w Windows przez Poprzednie wersje, kopiując plik z migawki w miejsce bieżącego. Miękkie usuwanie udziału tu nie pomoże, bo udział nie został usunięty.

Częste błędy

Objaw	Przyczyna	Co robimy
Tworzenie konta kończy się błędem nadmiarowości	domyślny SKU `Standard_RAGRS` w regionie bez pary	podajemy `--sku` jawnie
`AuthorizationPermissionMismatch` przy `--auth-mode login`	brak roli danych (Storage Blob Data Reader albo Contributor)	nadajemy rolę danych na koncie albo kontenerze

Objaw	Przyczyna	Co robimy
Portal nie pokazuje kontenerów po ustawieniu Deny	brak reguły dla naszego adresu publicznego	dodajemy adres, potem odświeżamy
Link SAS przestał działać po rotacji	SAS podpisany odnowionym kluczem	nowy SAS albo SAS z zasady przechowywanej
Replikacja obiektów nie daje się utworzyć	brak wersjonowania albo kanału zmian	włączamy na obu kontach i na źródłowym
Blob nie wraca po `undelete`	miękkie usuwanie było wyłączone w chwili usunięcia albo minął okres	włączamy miękkie usuwanie z wyprzedzeniem
Montowanie udziału z biura nie działa	zablokowany port 445	VPN, prywatny punkt końcowy albo test z maszyny w Azure

Powiązane: Tożsamość i ład: Entra ID, RBAC, Azure Policy, blokady, tagi i koszty · Obliczenia: ARM i Bicep, maszyny wirtualne, dostępność, App Service i kontenery · Zimne archiwum w chmurze: Azure Blob Storage i Amazon S3 Glacier · Azure: podstawy operacyjne

Źródła: Microsoft Learn: przewodnik do egzaminu AZ-104 (lista od 17 kwietnia 2026), „Azure region pairs and nonpaired regions” (polandcentral bez pary), „Upload files to Azure Blob storage by using AzCopy” (`--recursive`, SAS w adresie, `--block-blob-tier`), strona o zimnym archiwum w tej bazie (warstwy, Archive tylko LRS, GRS i RA-GRS); pomoc Azure CLI 2.91.0 (`az storage account create`, `update`, `network-rule add`, `keys renew`, `blob-service-properties update`, `file-service-properties update`, `management-policy create`, `or-policy create`, `az storage container create`, `policy create`, `generate-sas`, `az storage blob generate-sas`, `undelete`, `list`, `az storage share-rm create`, `snapshot`, `restore`, `list`); dokumentacja modułu Az (`New-AzStorageAccount`, `Update-AzStorageAccountNetworkRuleSet`, `New-AzStorageAccountKey`, `New-AzStorageContainerSASToken`, `Enable-AzStorageBlobDeleteRetentionPolicy`, `Update-AzStorageBlobServiceProperty`, `New-AzRmStorageShare`, `Update-AzStorageFileServiceProperty`), stan na 19 października 2026.

Revision #3
Created 2026-10-18 23:00:20 UTC by Tomasz Konieczny
Updated 2026-10-26 14:27:17 UTC by Tomasz Konieczny