# Tożsamość i ład: Entra ID, RBAC, Azure Policy, blokady, tagi i koszty

**Poziom: średnio**

**Dotyczy: AZ-104, domena „Manage Azure identities and governance” (20 do 25%), Microsoft Entra ID, Azure RBAC, Azure Policy, Azure CLI 2.91, moduł Az**

**Czas: 6 dni po 1,5 do 2 godzin**

*Dni 2 do 7 programu: użytkownicy i grupy w Entra ID, role Azure i ich zakresy, grupy zarządzania i subskrypcje, Azure Policy, blokady i tagi oraz koszty. To największa obok obliczeń domena egzaminu i fundament reszty: bez niej nie nadamy nikomu prawa do maszyny ani nie zatrzymamy kogoś, kto chce postawić zasób w złym regionie.*

**ZAŁOŻENIA SCENARIUSZA**

ćwiczymy w dzierżawie laboratorium „Zielona Lab” (`azlab.zielona.example`) i subskrypcji `zielona-lab` ze strony Plan 4 tygodni i laboratorium Azure w Zielonej. Grupy dynamiczne, licencjonowanie grupowe i samoobsługowe resetowanie hasła wymagają licencji Entra ID P1, więc w dzierżawie laboratorium włączamy wersję próbną Entra ID P2 albo pakietu Microsoft 365 z P1 (dostępność wersji próbnej do potwierdzenia w centrum administracyjnym). Produkcyjna dzierżawa Zielonej z Entra Connect jest opisana w książce Intune.

**Skróty użyte na tej stronie (9)**

| Skrót | Co znaczy |
|---|---|
| **AD** | Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie |
| **AZ-104** | numer egzaminu Microsoft Azure Administrator: egzamin, którego zdanie daje certyfikat Microsoft Certified: Azure Administrator Associate, ważny rok i odnawiany bezpłatną oceną online |
| **B2B** | business to business: sprzedaż i systemy skierowane do innych firm, nie do klientów indywidualnych |
| **CLI** | Command Line Interface: praca przez wpisywanie komend w terminalu |

| Skrót | Co znaczy |
|---|---|
| **GUID** | Globally Unique Identifier: unikalny w skali globalnej identyfikator obiektu, tu konkretnego protektora klucza BitLockera |
| **IAM** | Identity and Access Management: zarządzanie tożsamościami i uprawnieniami (w AWS: użytkownicy, role, polityki) |
| **RBAC** | Role-Based Access Control: uprawnienia nadawane rolom, a role ludziom |
| **SSPR** | Self-Service Password Reset: samoobsługowe resetowanie hasła w Microsoft Entra ID, bez dzwonienia do działu IT |
| **UPN** | User Principal Name: login w formie adresu, np. jan.nowak@zielona.example |

# Fiszka

Komendy `az` wykonujemy po `az login` i `az account set --subscription zielona-lab`, komendy Az po `Connect-AzAccount`. Do tworzenia użytkowników i nadawania ról potrzebujemy w laboratorium roli Global Administrator w Entra ID i Owner w subskrypcji. Nazwy `NazwaUzytkownika`, `IdSubskrypcji`, `IdObiektu` zastępujemy własnymi. Parametry sprawdziliśmy w pomocy Azure CLI 2.91.0 i w dokumentacji modułu Az (19 października 2026).

**□□ ZMIENIA SYSTEM**

## Utworzenie użytkownika w Entra ID: az ad user create

```
az ad user create --display-name "Ola Test" --user-principal-name
ola.test@azlab.zielona.example \
  --password "HasloTymczasowe" --force-change-password-next-sign-in true
```

Tworzy konto chmurowe. Wymagane są trzy parametry: nazwa wyświetlana, nazwa główna użytkownika (UPN) i hasło.

□□ **UPN** = User Principal Name: login w formie adresu, np. jan.nowak@zielona.example · **az** = Azure CLI: narzędzie chmury Microsoftu

**□□ ZMIENIA SYSTEM**

## Utworzenie użytkownika w PowerShell: New-AzADUser

```
$haslo = Read-Host -AsSecureString "Haslo tymczasowe"
New-AzADUser -DisplayName "Marek Test" -UserPrincipalName
marek.test@azlab.zielona.example `
  -MailNickname marek.test -Password $haslo -ForceChangePasswordNextLogin
```

W module Az parametr `-MailNickname` jest wymagany, w Azure CLI nie. Hasło przekazujemy jako `SecureString`, nie zwykłym tekstem.

**CLI** = Command Line Interface: praca przez wpisywanie komend w terminalu

**ZMIENIA SYSTEM**

## Utworzenie grupy zabezpieczeń: az ad group create

```
az ad group create --display-name gr-lab-operatorzy --mail-nickname gr-lab-operatorzy --
description "Operatorzy laboratorium AZ-104"
```

Grupa o członkostwie przypisanym. Grupę dynamiczną tworzymy w portalu (fiszka niżej), bo `az ad group create` nie ma parametru reguły członkostwa.

**az** = Azure CLI: narzędzie chmury Microsoftu · **AZ-104** = numer egzaminu Microsoft Azure Administrator: egzamin, którego zdanie daje certyfikat Microsoft Certified: Azure Administrator Associate, ważny rok i odnawiany bezpłatną oceną online

**TYLKO ODCZYT**

## Dodanie użytkownika do grupy: az ad group member add

```
az ad group member add --group gr-lab-operatorzy --member-id $(az ad user show --id
ola.test@azlab.zielona.example --query id -o tsv)
```

Parametr `--member-id` przyjmuje identyfikator obiektu, a nie UPN, dlatego pobieramy go wewnętrzną komendą `az ad user show`. W PowerShell: `Add-AzADGroupMember -TargetGroupDisplayName gr-lab-operatorzy -MemberUserPrincipalName ola.test@azlab.zielona.example`.

**UPN** = User Principal Name: login w formie adresu, np. jan.nowak@zielona.example · **az** = Azure CLI: narzędzie chmury Microsoftu

**TYLKO ODCZYT**

## Utworzenie grupy dynamicznej, gościa i licencji w centrum Entra

```
Microsoft Entra admin center → Entra ID → Groups → New group
  Membership type: Dynamic User → Add dynamic query
Microsoft Entra admin center → Entra ID → Users → New user → Invite external user
Microsoft Entra admin center → Entra ID → Users → (użytkownik) → Licenses → Assignments
Microsoft Entra admin center → Entra ID → Password reset → Properties → Self service
password reset enabled: Selected
```

Reguła grupy dynamicznej ma postać `(user.department -eq "Magazyn")`. Gość dostaje typ użytkownika Guest i zaproszenie e-mailem. Licencji nie przypiszemy użytkownikowi bez ustawionej lokalizacji użycia (Usage location).

**◫ ZRZUT EKRANU DO UZUPEŁNIENIA**

Zrzut do uzupełnienia: ekran New group w centrum Microsoft Entra z typem członkostwa Dynamic User i edytorem reguły, widoczna reguła `(user.department -eq "Magazyn")` i przycisk Validate Rules.

**◫ ZMIENIA SYSTEM**

## Nadanie roli na zakresie grupy zasobów: az role assignment create

```
az role assignment create --assignee ola.test@azlab.zielona.example --role "Virtual
Machine Contributor" \
  --scope /subscriptions/IdSubskrypcji/resourceGroups/rg-lab-obliczenia
```

Parametr `--scope` decyduje, gdzie rola działa: grupa zarządzania, subskrypcja, grupa zasobów albo pojedynczy zasób. Role nadajemy grupom, nie pojedynczym osobom, a tu pojedyncze konto jest tylko do ćwiczenia.

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

**◫ ZMIENIA SYSTEM**

## Nadanie roli w PowerShell: New-AzRoleAssignment

```
New-AzRoleAssignment -SignInName marek.test@azlab.zielona.example -RoleDefinitionName
Reader -ResourceGroupName rg-lab-siec
```

Dla grupy zamiast `-SignInName` podajemy `-ObjectId` grupy.

**TYLKO ODCZYT**

## Sprawdzenie wszystkich przypisań osoby, także odziedziczonych: az role assignment list

```
az role assignment list --assignee ola.test@azlab.zielona.example --all --include-inherited --include-groups -o table
```

Bez `--all` polecenie pokazuje tylko przypisania na poziomie subskrypcji, a bez `--include-inherited` i `--include-groups` pominie role z wyższych zakresów i z grup. To dokładnie ta sama pułapka, co w pytaniach „dlaczego użytkownik ma dostęp”.

Przykład:

```
Principal                        Role                        Scope
--------------------------------  ---------------------------
-----------------------------------------------------------
ola.test@azlab.zielona.example    Virtual Machine Contributor
/subscriptions/.../resourceGroups/rg-lab-obliczenia
gr-lab-operatorzy                 Reader                      /subscriptions/...
```

(identyfikator subskrypcji w kolumnie Scope skrócony do kropek)

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

**TYLKO ODCZYT**

## Podgląd uprawnień roli wbudowanej: az role definition list

```
az role definition list --name "Virtual Machine Contributor" --query "[].permissions[].actions" -o json
```

Pokazuje listę akcji, na które rola pozwala. W PowerShell: `Get-AzRoleDefinition -Name "Virtual Machine Contributor"`.

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

**ZMIENIA SYSTEM**

## Utworzenie grupy zarządzania: az account management-group create

```
az account management-group create --name mg-lab --display-name "Zielona Lab"
```

Nowa grupa trafia pod główną grupę dzierżawy (Tenant root group), chyba że podamy `--parent`. W PowerShell: `New-AzManagementGroup -GroupName mg-lab -DisplayName "Zielona Lab"`.

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

□□ **TYLKO ODCZYT**

## Przeniesienie subskrypcji do grupy zarządzania: az account management-group subscription add

```
az account management-group subscription add --name mg-lab --subscription zielona-lab
```

Subskrypcja ma zawsze dokładnie jednego rodzica. W PowerShell: `New-AzManagementGroupSubscription -GroupName mg-lab -SubscriptionId IdSubskrypcji`.

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

□□ **TYLKO ODCZYT**

## Znalezienie definicji zasady po nazwie: az policy definition list

```
az policy definition list --query "[?displayName=='Allowed locations'].name" -o tsv
```

Zwraca nazwę (identyfikator) wbudowanej definicji „Allowed locations”. Nazwę wyświetlaną zawsze sprawdzamy po angielsku, bo tak jest zapisana w definicji.

Przykład:

```
e56962a6-4747-49cd-b67b-bf8b01975c4c
```

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

□□ **ZMIENIA SYSTEM**

## Przypisanie zasady dozwolonych regionów: az policy assignment create

```
az policy assignment create --name dozwolone-regiony --display-name "Tylko polandcentral
i swedencentral" \
  --policy e56962a6-4747-49cd-b67b-bf8b01975c4c \
  --scope /providers/Microsoft.Management/managementGroups/mg-lab \
  --params '{"listOfAllowedLocations":{"value":["polandcentral","swedencentral"]}}'
```

Parametr definicji nazywa się `listOfAllowedLocations`. Ta zasada nie obejmuje samych grup zasobów ani zasobów globalnych, więc grupę w innym regionie nadal da się utworzyć. W PowerShell zasadę przypisuje `New-AzPolicyAssignment -Name NazwaPrzypisania -PolicyDefinition $definicja -Scope NazwaZakresu -PolicyParameterObject @{...}`.

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

□□ **TYLKO ODCZYT**

## Sprawdzenie zgodności z zasadami: az policy state summarize

```
az policy state summarize --resource-group rg-lab-obliczenia
```

Podsumowuje zasoby niezgodne z przypisanymi zasadami. Ocena po nowym przypisaniu nie jest natychmiastowa, więc wynik sprawdzamy po kilku, kilkunastu minutach (dokładny czas sprawdzamy w dokumentacji Azure Policy).

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

□□ **ZMIENIA SYSTEM**

## Założenie blokady przed usunięciem: az lock create

```
az lock create --name blokada-siec --lock-type CanNotDelete --resource-group rg-lab-siec
--notes "Siec laboratorium, nie kasowac"
```

`CanNotDelete` pozwala czytać i zmieniać, ale nie usuwać. `ReadOnly` blokuje także zmiany. W PowerShell: `New-AzResourceLock -LockName blokada-siec -LockLevel CanNotDelete -ResourceGroupName rg-lab-siec`.

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

□□ **TYLKO ODCZYT**

## Usunięcie blokady: az lock delete

```
az lock delete --name blokada-siec --resource-group rg-lab-siec
```

Bez tego kroku wieczorne `az group delete` zakończy się błędem. Blokady zakładać i zdejmować mogą tylko role z prawem `Microsoft.Authorization/locks/*`, czyli Owner i User Access Administrator.

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

**ZMIENIA SYSTEM**

## Dopisanie tagu bez kasowania istniejących: az tag update --operation Merge

```
az tag update --resource-id /subscriptions/IdSubskrypcji/resourceGroups/rg-lab-obliczenia \
  --operation Merge --tags dzial=it centrum-kosztow=lab
```

`Merge` dokłada tagi, `Replace` zastępuje wszystkie, `Delete` usuwa podane. W PowerShell: `Update-AzTag -ResourceId IdZasobu -Tag @{dzial='it'} -Operation Merge`.

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

**TYLKO ODCZYT**

## Przeniesienie zasobu do innej grupy zasobów: az resource move

```
az resource move --destination-group rg-lab-magazyn --ids IdZasobu
```

Zasób zmienia grupę (i identyfikator), ale nie region. Na czas przenoszenia obie grupy są zablokowane dla zmian. W PowerShell: `Move-AzResource -DestinationResourceGroupName rg-lab-magazyn -ResourceId IdZasobu`.

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

**TYLKO ODCZYT**

## Zalecenia kosztowe Azure Advisor: az advisor recommendation list

```
az advisor recommendation list --category Cost -o table
```

Kategorie to Cost, HighAvailability, OperationalExcellence, Performance i Security. W PowerShell: `Get-AzAdvisorRecommendation`.

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

**KLIKAMY W INTERFEJSIE**

### Budżet i analiza kosztów w portalu

```
Portal Azure → Cost Management + Billing → Cost Management → Budgets → Add
Portal Azure → Cost Management + Billing → Cost Management → Cost analysis → Group by: Resource group
```

Budżet zakładamy na subskrypcję albo grupę zasobów, z progiem rzeczywistym albo prognozowanym. Fiszka z budżetem w PowerShell stoi na stronie planu.

# Dzień 2: Entra ID, użytkownicy, grupy, licencje i goście

**Z ŻYCIA WZIĘTE**

Wtorek, 9:00. Tomek tworzy w laboratorium trzy konta testowe i jedną grupę „Magazyn”, do której ręcznie dopisuje Marka Testa. Pytamy, co się stanie, gdy w październiku przyjdzie nowy magazynier: Tomek odpowiada, że go dopisze. Zamieniamy grupę na dynamiczną z regułą po dziale i ustawiamy dział w profilu nowego konta. Po kilku minutach konto samo pojawia się w grupie, a Tomek zapisuje w dzienniku, że grupy dynamiczne wymagają licencji P1 dla każdego użytkownika, który z nich korzysta.

## Cele egzaminu

- tworzenie użytkowników i grup
- zarządzanie właściwościami użytkowników i grup
- zarządzanie licencjami w Microsoft Entra ID
- zarządzanie użytkownikami zewnętrznymi
- konfiguracja samoobsługowego resetowania hasła (SSPR)

# Jak to działa

> **Pojęcie: dzierżawa (tenant).** Jedna instancja Microsoft Entra ID dla jednej organizacji: własna lista użytkowników, grup i aplikacji, z identyfikatorem w postaci GUID i domeną początkową `NazwaTenanta.onmicrosoft.com`. Subskrypcja Azure ufa dokładnie jednej dzierżawie, a jedna dzierżawa może mieć wiele subskrypcji.

> **Pojęcie: grupa dynamiczna.** Grupa, której członków wylicza reguła na podstawie atrybutów (na przykład działu), a nie lista wpisana ręcznie. Do zwykłej grupy dopisujemy członków, do dynamicznej nie da się dopisać nikogo ręcznie.

| Rodzaj | Kto w niej jest | Licencja | Typowe pytanie egzaminu |
|---|---|---|---|
| Grupa zabezpieczeń, członkostwo przypisane | osoby dopisane ręcznie | Free | komu nadać rolę |
| Grupa zabezpieczeń, dynamiczna | wyliczani z reguły | P1 | jak samo dopisywać nowych pracowników |
| Grupa Microsoft 365 | osoby ze wspólną skrzynką i witryną | Free | nadawanie ról Azure: zwykle grupa zabezpieczeń |

Samoobsługowe resetowanie hasła (SSPR) dla kont chmurowych wymaga według tabeli licencji Microsoftu Microsoft 365 Business Standard, Business Premium albo Entra ID P1 lub P2. Entra ID Free pozwala tylko zmienić znane hasło. Zapis zresetowanego hasła z powrotem do lokalnego Active Directory (writeback) wymaga P1, P2 albo Business Premium.

Goście (B2B) to konta z innych dzierżaw albo adresy zewnętrzne, zaproszone do naszej dzierżawy. Mają typ użytkownika Guest i domyślnie ograniczone prawa w katalogu, ale role Azure nadajemy im tak samo jak pracownikom.

# Zadania laboratoryjne

1. Tworzymy konta `ola.test`, `marek.test` i `kasia.test` w domenie `azlab.zielona.example`, pierwsze dwa w CLI, trzecie w portalu. Kasi ustawiamy dział `Handel`, Markowi `Magazyn`.
2. Tworzymy grupę `gr-lab-operatorzy` (przypisaną) i dodajemy do niej Olę.
3. Tworzymy grupę dynamiczną `gr-lab-magazyn` z regułą `(user.department -eq "Magazyn")` i sprawdzamy, że Marek pojawił się w niej sam.
4. Ustawiamy Kasi lokalizację użycia `Poland` i przypisujemy jej licencję wersji próbnej. Potem przenosimy licencję na grupę `gr-lab-operatorzy` (licencjonowanie grupowe).
5. Zapraszamy gościa z adresem skrzynki testowej i sprawdzamy jego typ użytkownika.

6. Włączamy SSPR dla grupy `gr-lab-operatorzy` z jedną metodą uwierzytelniania i sprawdzamy reset hasła Oli w oknie prywatnym przeglądarki.

# Pułapki egzaminacyjne

- Do grupy dynamicznej nie dodamy nikogo ręcznie. Gdy pytanie mówi „dodaj użytkownika do grupy” i grupa jest dynamiczna, odpowiedzią jest zmiana atrybutu użytkownika albo reguły.
- Licencja nie zostanie przypisana bez lokalizacji użycia.
- SSPR włączone dla grupy „Selected” obejmuje tylko tę grupę. Administratorzy mają osobne, zawsze włączone zasady resetu.
- Rola Azure (RBAC) i rola Entra (na przykład User Administrator) to dwa osobne systemy. Rola Owner w subskrypcji nie pozwala tworzyć użytkowników w Entra ID.

# Ćwiczenia

1. Nowy pracownik magazynu ma automatycznie dostać dostęp do maszyn w `rg-lab-obliczenia`. Co konfigurujemy, w jakiej kolejności?

**Odpowiedź**

Grupę dynamiczną z regułą po dziale (`user.department -eq "Magazyn"`), a potem rolę Azure (na przykład Virtual Machine Contributor) przypisaną tej grupie na zakresie `rg-lab-obliczenia`. Nowe konto z działem Magazyn trafi do grupy samo, a rola przyjdzie z grupy. Grupa dynamiczna wymaga licencji P1.

1. Ola zapomniała hasła i nie widzi linku resetu, choć SSPR jest włączone. Gdzie szukamy przyczyny?

**Odpowiedź**

Sprawdzamy, czy SSPR obejmuje grupę, w której jest Ola (ustawienie Selected), czy Ola ma licencję z SSPR i czy zarejestrowała metodę uwierzytelniania wymaganą przez zasady. Gdy jest kontem synchronizowanym z AD, reset wymaga dodatkowo zapisu zwrotnego, czyli P1 i konfiguracji w Entra Connect.

# Dzień 3: role Azure i ich zakresy

**Z ŻYCIA WZIĘTE**

Środa, 14:20. Marek Test ma rolę Reader na subskrypcji i Virtual Machine Contributor na `rg-lab-obliczenia`, a mimo to nie może podłączyć nowej maszyny do sieci `vnet-lab-app`. Tomek podejrzewa błąd Azure, a my pokazujemy mu zakres: sieć leży w `rg-lab-siec`, gdzie Marek ma tylko Reader. Virtual Machine Contributor pozwala zarządzać maszynami, ale do podłączenia karty do podsieci potrzebne jest prawo dołączenia do sieci w jej grupie. Tomek nadaje Markowi rolę Network Contributor na samej podsieci i notuje: zakres liczy się tam, gdzie leży zasób.

# Cele egzaminu

- zarządzanie wbudowanymi rolami Azure
- przypisywanie ról na różnych zakresach
- interpretacja przypisań dostępu

# Jak to działa

**Pojęcie: przypisanie roli.** Trójka: kto (użytkownik, grupa, tożsamość zarządzana albo jednostka usługi), jaka rola (lista dozwolonych akcji) i gdzie (zakres). Przypisanie na wyższym zakresie dziedziczy się w dół, a uprawnienia z wielu przypisań się sumują.

| Rola wbudowana | Co może | Czego nie może |
|---|---|---|
| Owner | wszystko, łącznie z nadawaniem ról | nic w swoim zakresie |
| Contributor | tworzyć i zmieniać wszystkie zasoby | nadawać ról, zakładać blokad |
| Reader | oglądać wszystko | niczego zmienić |
| User Access Administrator | zarządzać dostępem (role, blokady) | zmieniać samych zasobów |
| Role Based Access Control Administrator | nadawać role, z możliwością ograniczenia warunkami | zarządzać zasobami |
| Virtual Machine Contributor | zarządzać maszynami | logować się do maszyn, zarządzać siecią i kontem magazynu, do których maszyna jest podłączona |
| Storage Blob Data Reader | czytać dane blobów | zarządzać kontem |

Rozróżnienie płaszczyzny zarządzania i płaszczyzny danych wraca w magazynie: Contributor na koncie magazynu może odczytać klucze konta i przez nie dostać się do danych, a rola Storage Blob Data Reader daje dostęp do danych przez Entra ID bez kluczy.

Rola Global Administrator w Entra ID nie daje automatycznie praw do subskrypcji. Może je sobie nadać przez ustawienie „Access management for Azure resources”, które przypisuje jej rolę User Access Administrator na zakresie głównym. Robimy to tylko w awarii i zaraz cofamy.

# Zadania laboratoryjne

1. Nadajemy grupie `gr-lab-operatorzy` rolę Reader na subskrypcji, a Oli rolę Virtual Machine Contributor na `rg-lab-obliczenia`.
2. W portalu sprawdzamy dostęp Oli: grupa zasobów → Access control (IAM) → Check access. Porównujemy z wynikiem `az role assignment list --assignee ... --all --include-inherited --include-groups`.
3. Logujemy się jako Ola w oknie prywatnym i próbujemy utworzyć konto magazynu w `rg-lab-obliczenia`: ma się nie udać, bo Virtual Machine Contributor nie obejmuje kont magazynu.
4. Usuwamy przypisanie Oli: `az role assignment delete --assignee ola.test@azlab.zielona.example --role "Virtual Machine Contributor" --resource-group rg-lab-obliczenia`.

# Pułapki egzaminacyjne

- Najmniejsze uprawnienie: gdy pytanie pyta o rolę „z najmniejszymi uprawnieniami”, Owner prawie nigdy nie jest dobrą odpowiedzią, a Contributor nie nada nikomu roli.
- Przypisanie na grupie zarządzania obejmuje wszystkie subskrypcje pod nią, także te dodane później.
- Odmowa (deny assignment) wygrywa z przypisaniem roli, ale samodzielnie jej nie tworzymy: zakładają ją usługi Azure, na przykład zarządzane aplikacje.
- Zmiana członkostwa w grupie działa od następnego tokenu, więc test robimy po ponownym zalogowaniu.

# Ćwiczenia

1. Użytkownik ma Contributor na subskrypcji i Reader na `rg-lab-siec`. Czy może usunąć sieć w `rg-lab-siec`?

**Odpowiedź**

Tak. Uprawnienia z przypisań się sumują, a Contributor odziedziczony z subskrypcji obejmuje też `rg-lab-siec`. Reader niczego nie odbiera. Zatrzymać usunięcie mogłaby tylko blokada `CanNotDelete` albo odmowa.

1. Kierownik projektu ma nadawać role współpracownikom w `rg-lab-obliczenia`, ale nie zmieniać zasobów. Jaką rolę dostaje i na jakim zakresie?

**Odpowiedź**

User Access Administrator albo Role Based Access Control Administrator na zakresie `rg-lab-obliczenia`. Druga pozwala dodatkowo ograniczyć warunkiem, jakie role wolno nadawać. Owner dałby za dużo, bo pozwala też zmieniać zasoby.

# Dzień 4: grupy zarządzania, subskrypcje i grupy zasobów

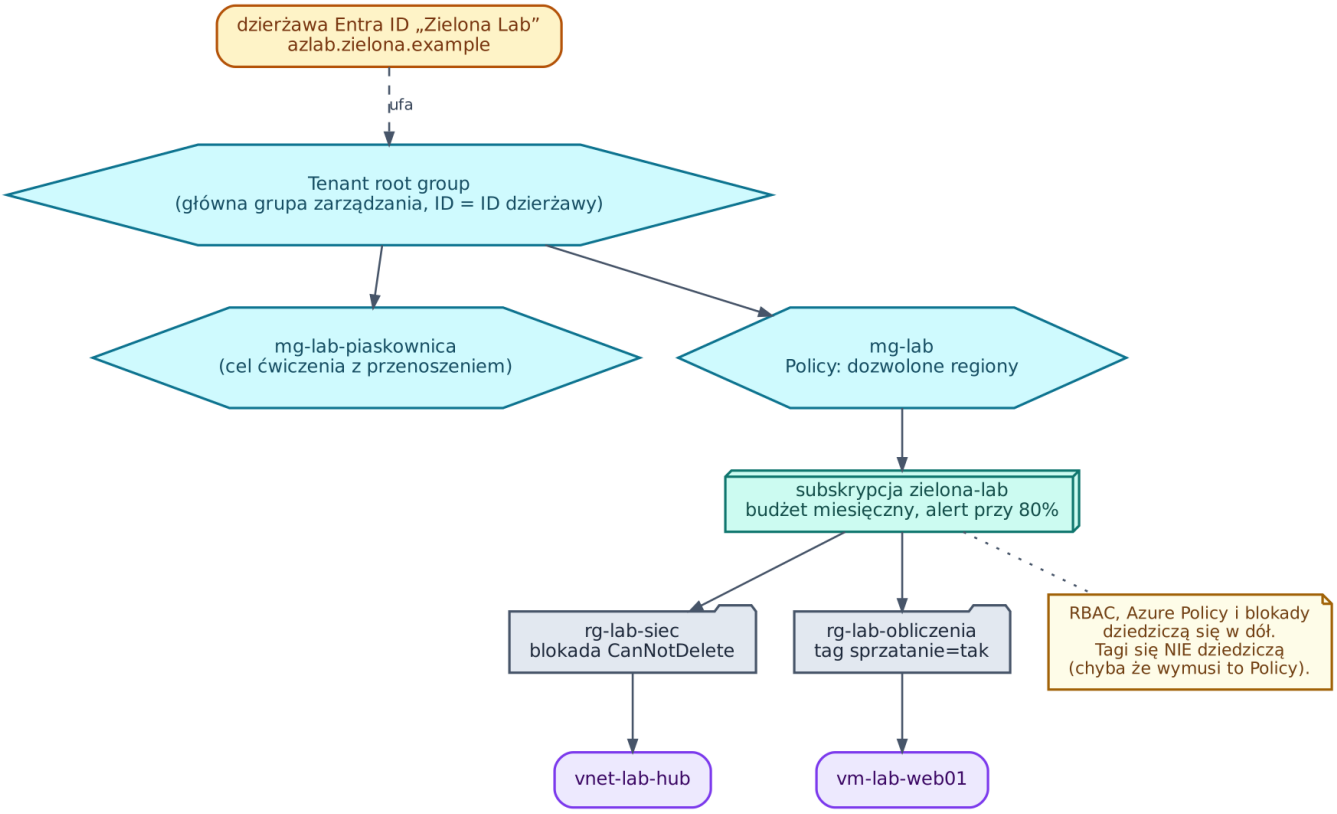
> **Z ŻYCIA WZIĘTE**
>
> Czwartek, 11:00. Pan Zbigniew pyta, czy laboratorium Tomka nie wymiesza się z tym, co w Azure stoi naprawdę. Pokazujemy mu rysunek z dwoma piętrami: grupa zarządzania `mg-lab` ma zasadę regionów, pod nią subskrypcja `zielona-lab` z budżetem, a pod subskrypcją grupy zasobów z blokadą i tagami. Pan Zbigniew pyta jeszcze, czy da się na górze ustawić jedną zasadę dla wszystkich przyszłych subskrypcji. Odpowiadamy, że właśnie po to są grupy zarządzania.

## Cele egzaminu

- zarządzanie grupami zasobów
- zarządzanie subskrypcjami
- konfiguracja grup zarządzania

## Jak to działa

Zasoby Azure żyją w czteropiętrowej hierarchii: grupa zarządzania, subskrypcja, grupa zasobów, zasób. Na każdym piętrze można przypisać role, zasady i blokady, a wszystko to dziedziczy się w dół.




*Rysunek 1. Hierarchia w dzierżawie laboratorium: Tenant root group, grupy mg-lab i mg-lab-piaskownica, subskrypcja zielona-lab, grupy zasobów z blokadą i tagiem oraz zasoby; RBAC, Policy i blokady dziedziczą się w dół, tagi nie (kliknięcie otwiera pełny rozmiar)*

> **Pojęcie: grupa zarządzania (management group).** Kontener na subskrypcje i inne grupy zarządzania, służący do nadawania ról i zasad wielu subskrypcjom naraz. Według dokumentacji Microsoftu jedna dzierżawa może mieć 10 000 grup zarządzania, drzewo ma do sześciu poziomów (nie licząc poziomu głównego i subskrypcji), a każda grupa i subskrypcja ma jednego rodzica.

| Poziom | Co tu nadajemy | Uwagi z dokumentacji |
|---|---|---|
| Tenant root group | zasady i role dla całej organizacji | ID równe ID dzierżawy, nie da się jej usunąć ani przenieść; nowe subskrypcje trafiają tu domyślnie |
| Grupa zarządzania | zasady dla gałęzi organizacji | do sześciu poziomów |
| Subskrypcja | budżet, limity, rozliczenie | ufa jednej dzierżawie Entra ID |
| Grupa zasobów | role zespołu, blokady, cykl życia | zasób należy do dokładnie jednej grupy; grupa ma region tylko dla swoich metadanych |
| Zasób | wyjątki | identyfikator zawiera subskrypcję i grupę |

Przeniesienie zasobu do innej grupy albo subskrypcji zmienia jego identyfikator, więc skrypty i alerty, które go używały, trzeba poprawić. Nie każdy zasób da się przenieść, a niektóre wymagają przeniesienia razem z zależnymi (na przykład maszyna z dyskami i kartą sieciową). Listę sprawdzamy w dokumentacji „Move operation support for resources”.

# Zadania laboratoryjne

1. Tworzymy grupy zarządzania `mg-lab` i `mg-lab-piaskownica`, przenosimy `zielona-lab` do `mg-lab`.
2. W portalu sprawdzamy, kto ma dostęp do głównej grupy: nikt domyślnie, Global Administrator po podniesieniu uprawnień.
3. Tworzymy konto magazynu w `rg-lab-obliczenia` i przenosimy je do `rg-lab-magazyn`, potem sprawdzamy, że zmienił się identyfikator zasobu, a region został ten sam.
4. Przenosimy subskrypcję do `mg-lab-piaskownica` i z powrotem, obserwując, które zasady i role znikają razem z rodzicem.

# Pułapki egzaminacyjne

- Region grupy zasobów nie ogranicza regionu zasobów w niej.
- Usunięcie grupy zasobów usuwa wszystkie zasoby w niej, niezależnie od ich regionu.
- Przeniesienie zasobu nie zmienia regionu. Do zmiany regionu służą inne narzędzia (Azure Resource Mover albo ponowne wdrożenie).
- Grupa zarządzania nie zawiera zasobów bezpośrednio, tylko subskrypcje i inne grupy.

# Ćwiczenia

1. Zasada przypisana na `mg-lab` blokuje region `westeurope`. Subskrypcja zostaje przeniesiona do `mg-lab-piaskownica`, gdzie zasady nie ma. Co dzieje się z maszyną, która już stoi w `westeurope`?

**Odpowiedź**

Nic się z nią nie dzieje. Zasada z efektem Deny działa przy tworzeniu i zmianie zasobów, a istniejące zasoby oznacza tylko jako niezgodne. Po przeniesieniu subskrypcja przestaje dziedziczyć zasadę, więc nowe zasoby w `westeurope` dadzą się utworzyć.

# Dzień 5: Azure Policy, blokady i tagi

> **Z ŻYCIA WZIĘTE**
>
> Piątek, 15:50. Tomek w ostatniej chwili przed weekendem próbuje usunąć `rg-lab-siec`, żeby zacząć od zera, i dostaje błąd o blokadzie, którą sam założył rano. Kilka minut później Ola, testując swoje uprawnienia, próbuje utworzyć maszynę w `westeurope` i dostaje odmowę z nazwą zasady „Tylko polandcentral i swedencentral”. Tomek mówi, że Azure dziś mu wszystko blokuje. Odpowiadamy, że tak miało być: blokada chroni przed pomyłką, a zasada przed złym regionem.

## Cele egzaminu

- wdrażanie zasad Azure Policy i zarządzanie nimi
- konfiguracja blokad zasobów
- nadawanie tagów zasobom i zarządzanie nimi

## Jak to działa

> **Pojęcie: Azure Policy.** Usługa, która przy tworzeniu i zmianie zasobów sprawdza ich właściwości z regułami i, zależnie od efektu, odmawia, dopisuje coś albo tylko raportuje. RBAC mówi, kto może coś zrobić, a Policy, jaki ma być wynik.

| Efekt | Co robi | Przykład w laboratorium |
|---|---|---|
| Deny | odmawia utworzenia albo zmiany | regiony spoza listy |
| Audit | przepuszcza, oznacza jako niezgodne | konta magazynu bez minimalnej wersji TLS |
| Modify | dopisuje lub zmienia właściwości, na przykład tagi | dziedziczenie tagu z grupy zasobów |
| Append | dodaje pola przy tworzeniu | dodatkowe reguły sieciowe |
| DeployIfNotExists | wdraża brakujący zasób, na przykład ustawienie diagnostyczne | wysyłka logów do `law-zielona-lab` |
| AuditIfNotExists | raportuje brak zasobu powiązanego | brak rozszerzenia na maszynie |

| Efekt | Co robi | Przykład w laboratorium |
|---|---|---|
| Disabled | wyłącza zasadę bez usuwania przypisania | test |

> **Pojęcie: inicjatywa (policy set).** Zestaw kilku definicji zasad przypisywany razem, na przykład wszystkie zasady jednego standardu. Efekty Modify i DeployIfNotExists potrzebują tożsamości zarządzanej przypisania, bo to ona wprowadza zmiany, a dla istniejących zasobów trzeba uruchomić zadanie naprawy (remediation).

> **Pojęcie: blokada (lock).** Ustawienie na subskrypcji, grupie albo zasobie, które zatrzymuje usunięcie (`CanNotDelete`) albo każdą zmianę (`ReadOnly`) niezależnie od ról. Blokada dziedziczy się w dół i działa na płaszczyźnie zarządzania, a nie na danych: blokada na koncie magazynu nie chroni pojedynczych blobów.

`ReadOnly` ma skutki uboczne, o które egzamin lubi pytać. Na koncie magazynu blokuje odczyt kluczy (to operacja POST, traktowana jak zmiana), a na grupie zasobów blokuje dokładanie nowych zasobów i zmianę skalowania.

> **Pojęcie: tag.** Para nazwa i wartość na zasobie, grupie albo subskrypcji, służąca do opisu i rozliczeń. Tagi nie dziedziczą się z grupy zasobów na zasoby. Dziedziczenie wymusza się zasadą z efektem Modify, na przykład wbudowaną „Inherit a tag from the resource group if missing”.

# Zadania laboratoryjne

1. Przypisujemy „Allowed locations” na `mg-lab` z listą `polandcentral` i `swedencentral` (fiszka). Po kilku minutach próbujemy utworzyć sieć w `westeurope`: oczekujemy odmowy.
2. Przypisujemy na subskrypcji wbudowaną zasadę wymagającą tagu `sprzatanie` na grupach zasobów (szukamy jej w portalu po słowie „Require a tag on resource groups”) i próbujemy utworzyć grupę bez tagu.
3. Przypisujemy „Inherit a tag from the resource group if missing” dla tagu `projekt` z tożsamością zarządzaną i uruchamiamy zadanie naprawy dla istniejących zasobów.
4. Zakładamy blokadę `CanNotDelete` na `rg-lab-siec`, próbujemy usunąć sieć, potem zdejmujemy blokadę.
5. Zakładamy blokadę `ReadOnly` na koncie magazynu i próbujemy odczytać klucze `az storage account keys list`. Zapisujemy w dzienniku komunikat błędu i zdejmujemy blokadę.

# Pułapki egzaminacyjne

- „Allowed locations” nie dotyczy grup zasobów. Do regionów grup jest osobna wbudowana zasada.
- Contributor nie założy ani nie zdejmie blokady, Owner i User Access Administrator tak.
- Blokada `CanNotDelete` na grupie nie przeszkadza w dodawaniu zasobów, `ReadOnly` przeszkadza.
- Zasada z efektem Deny nie usuwa istniejących niezgodnych zasobów, tylko je raportuje.
- Tag na grupie zasobów nie pojawia się automatycznie na zasobach w niej.

# Ćwiczenia

1. Na grupie `rg-lab-obliczenia` jest blokada `ReadOnly`. Ola z rolą Contributor próbuje zatrzymać maszynę. Co się stanie i dlaczego?

**Odpowiedź**

Zatrzymanie (dealokacja) się nie uda, bo to operacja zapisu na płaszczyźnie zarządzania, a `ReadOnly` blokuje wszystkie zmiany niezależnie od roli. Rola Contributor nie pozwala też zdjąć blokady, musi to zrobić Owner albo User Access Administrator.

1. Każdy zasób w subskrypcji ma mieć tag `centrum-kosztow` taki sam jak jego grupa zasobów, także zasoby utworzone przed wprowadzeniem zasady. Co robimy?

**Odpowiedź**

Przypisujemy zasadę z efektem Modify „Inherit a tag from the resource group if missing” (albo wariant zastępujący tag) z tożsamością zarządzaną, a dla istniejących zasobów uruchamiamy zadanie naprawy. Same tagi się nie dziedziczą.

# Dzień 6: koszty, budżety i Azure Advisor

**□□ Z ŻYCIA WZIĘTE**

> Poniedziałek, 8:30. Pan Zbigniew dostał prognozę wydatków na Azure i pyta, który projekt najwięcej kosztuje. Tomek otwiera analizę kosztów, grupuje po tagu `projekt` i widzi, że połowa kosztu laboratorium nie ma żadnego tagu. Zakładamy budżet na grupę zasobów z alertem prognozowanym i zasadę wymagającą tagu. Tydzień później pan Zbigniew dostaje raport, w którym każdy wiersz ma nazwę projektu.

# Cele egzaminu

- zarządzanie kosztami przy pomocy alertów, budżetów i zaleceń Azure Advisor

# Jak to działa

> **Pojęcie: budżet.** Kwota na okres (miesiąc, kwartał, rok) przypisana do zakresu, na przykład subskrypcji albo grupy zasobów, z progami powiadomień. Próg może dotyczyć kosztu rzeczywistego albo prognozowanego. Budżet tylko powiadamia, chyba że jego próg wywołuje grupę akcji, która coś automatyzuje.

| Narzędzie | Na jakie pytanie odpowiada |
|---|---|
| Cost analysis | ile kosztuje i co, w podziale na grupy, tagi, usługi |
| Budżety | kiedy przekroczymy kwotę |
| Alerty kosztów | anomalie i progi budżetów |
| Azure Advisor | co wyłączyć, zmniejszyć albo zarezerwować, żeby płacić mniej |
| Kalkulator cen | ile będzie kosztować, zanim postawimy |

Advisor pokazuje zalecenia w pięciu kategoriach: koszty, niezawodność (w CLI `HighAvailability`), doskonałość operacyjna, wydajność i bezpieczeństwo. Typowe zalecenie kosztowe to maszyna z niskim wykorzystaniem procesora do zmniejszenia albo wyłączenia.

# Zadania laboratoryjne

1. Zakładamy budżet na grupę `rg-lab-obliczenia` w portalu z dwoma progami: 50 procent kosztu rzeczywistego i 100 procent prognozowanego.
2. W Cost analysis grupujemy koszt po grupie zasobów i po tagu `projekt`, zapisujemy widok.
3. Uruchamiamy `az advisor recommendation list --category Cost -o table` i porównujemy z portalem.
4. Sprawdzamy, czy maszyny z poprzednich dni są zdealokowane, a nie tylko zatrzymane.

# Pułapki egzaminacyjne

- Budżet nie zatrzymuje zasobów sam z siebie.
- Dane kosztowe nie są natychmiastowe, więc alert budżetu przychodzi z opóźnieniem (konkretne opóźnienie sprawdzamy w dokumentacji Cost Management).
- Zalecenia Advisora są podpowiedziami, nic nie zmieniają same.
- Tagi pomagają w rozliczeniach tylko wtedy, gdy są na zasobach, a nie tylko na grupie.

# Ćwiczenia

1. Pan Zbigniew chce dostać e-mail, gdy przewidywany koszt miesiąca w laboratorium przekroczy kwotę budżetu, jeszcze zanim to się stanie. Co ustawiamy?

**Odpowiedź**

Budżet miesięczny na subskrypcji `zielona-lab` (albo na grupie) z progiem typu prognozowanego (Forecasted) na 100 procent i adresem pana Zbigniewa. Próg rzeczywisty wysłałby wiadomość dopiero po przekroczeniu.

# Dzień 7: powtórka tygodnia 1

Rano wracamy do czystej subskrypcji: zdejmujemy blokady, usuwamy przypisania testowe i grupy zasobów z tagiem `sprzatanie=tak`. Grupy zarządzania, zasady na `mg-lab` i budżet zostają, bo przydadzą się do końca programu.

Mini sprawdzian, dziesięć pytań na 15 minut, bez dokumentacji:

1. Jakie trzy elementy składają się na przypisanie roli?
2. Która rola może nadawać role, ale nie zmieniać zasobów?
3. Czy przypisanie na grupie zarządzania obejmuje subskrypcję dodaną do niej jutro?
4. Jaka licencja jest potrzebna do grup dynamicznych?
5. Czym różni się blokada `CanNotDelete` od `ReadOnly`?
6. Kto może zdjąć blokadę?
7. Który efekt zasady dopisze brakujący tag?
8. Czy tag na grupie zasobów pojawia się na zasobach?
9. Co robi przeniesienie zasobu z identyfikatorem i regionem?
10. Czy budżet wyłączy maszynę?

**Odpowiedzi**

1. Kto, jaka rola, na jakim zakresie. 2. User Access Administrator albo Role Based Access Control Administrator. 3. Tak, dziedziczenie działa dla obecnych i przyszłych dzieci. 4. Entra ID P1 (albo wyższa). 5. `CanNotDelete` pozwala zmieniać, ale nie usuwać, `ReadOnly` blokuje także zmiany. 6. Owner albo User Access Administrator (prawo `Microsoft.Authorization/locks/*`). 7. Modify (albo Append przy tworzeniu). 8. Nie, chyba że wymusi to zasada. 9. Identyfikator się zmienia, region nie. 10. Nie, budżet tylko powiadamia.

Każdą złą odpowiedź zapisujemy w dzienniku błędów z przyczyną: nie wiedziałem, pomyliłem pojęcia albo nie doczytałem pytania.

# Częste błędy

| Objaw | Przyczyna | Co robimy |
|---|---|---|
| `az ad group member add` zgłasza nieprawidłowy identyfikator | podany UPN zamiast identyfikatora obiektu | `az ad user show --id NazwaUPN --query id -o tsv` |
| Użytkownik ma rolę, a portal mówi o braku uprawnień | stary token po zmianie członkostwa w grupie albo zły zakres | ponowne logowanie, Check access w IAM na właściwym zasobie |
| `az role assignment list` nie pokazuje roli, którą użytkownik ma | brak `--all`, `--include-inherited` albo `--include-groups` | polecenie z trzema parametrami |
| Zasada nie blokuje nowego zasobu | ocena jeszcze nie objęła przypisania albo zły zakres | odczekać, sprawdzić `az policy assignment list --scope NazwaZakresu` |
| Grupa w niedozwolonym regionie powstała mimo zasady | „Allowed locations” nie obejmuje grup zasobów | osobna zasada regionów dla grup |
| Usunięcie grupy kończy się błędem | blokada na grupie albo zasobie | `az lock list --resource-group NazwaGrupy`, zdjęcie blokady |
| Licencja nie daje się przypisać | brak lokalizacji użycia albo brak wolnych licencji | ustawić Usage location, sprawdzić liczbę licencji |

**Powiązane:** Plan 4 tygodni i laboratorium Azure w Zielonej · Magazyn: konta, nadmiarowość, SAS, Blob, Azure Files i zabezpieczenia · Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy · Zasady zgodności i dostęp warunkowy · Azure: podstawy operacyjne

**Źródła:** Microsoft Learn: przewodnik do egzaminu AZ-104 (lista od 17 kwietnia 2026), „Management groups overview” (10 000 grup, sześć poziomów, jeden rodzic, Tenant root group), „Licensing requirements for Microsoft Entra self-service password reset” (P1, Business Standard i Premium, writeback); pomoc Azure CLI 2.91.0 (`az ad user create`, `az ad group create`, `az ad group member add`, `az role assignment create` i `list`, `az role definition list`, `az account management-group create` i `subscription add`, `az policy definition list`, `az policy assignment create`, `az`

`policy state summarize`, `az lock create` i `delete`, `az tag update`, `az resource move`, `az advisor recommendation list`); dokumentacja modułu Az (`New-AzADUser`, `Add-AzADGroupMember`, `New-AzRoleAssignment`, `Get-AzRoleDefinition`, `New-AzManagementGroup`, `New-AzManagementGroupSubscription`, `New-AzPolicyAssignment`, `New-AzResourceLock`, `Update-AzTag`, `Move-AzResource`, `Get-AzAdvisorRecommendation`), stan na 19 października 2026; dev.classmethod.jp, wpis o zasadzie „Allowed locations” (identyfikator definicji i parametr `listOfAllowedLocations`).

---

Revision #3
Created 2026-10-18 23:00:18 UTC by Tomasz Konieczny
Updated 2026-10-26 14:27:15 UTC by Tomasz Konieczny