

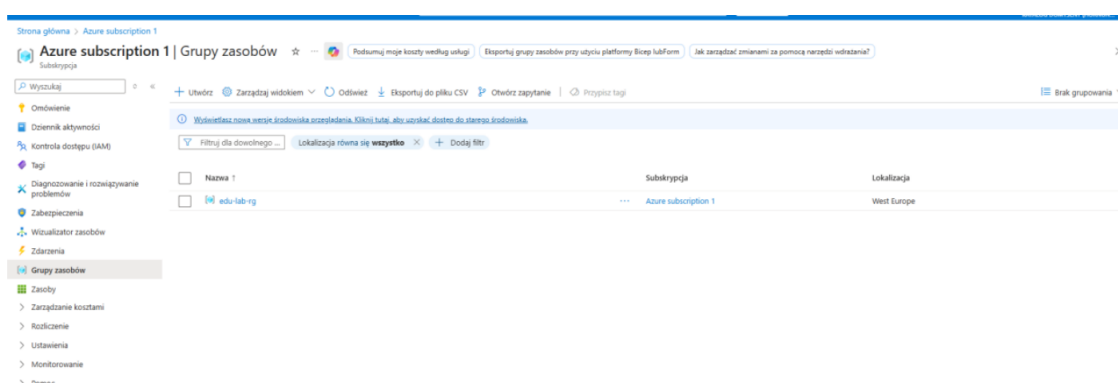
## 1. ETAP 1 — Wymagania wstępne i zakres konfiguracji

Upewnij się, że masz dostęp do subskrypcji, w której będą tworzone zasoby (np. „Azure subscription 1”) oraz uprawnienia pozwalające przypisywać role RBAC na poziomie subskrypcji (najczęściej Owner lub User Access Administrator).

Upewnij się, że masz uprawnienia w Microsoft Entra ID pozwalające utworzyć rejestrację aplikacji oraz nadać/zaakceptować uprawnienia Microsoft Graph (do „Grant admin consent” zwykle wymagane są uprawnienia administratora katalogu).

Przygotuj miejsce na bezpieczne zapisanie danych konfiguracyjnych (Tenant ID, Client ID, Client Secret Value, Subscription ID) – szczególnie „Client Secret Value” będzie widoczny tylko raz.

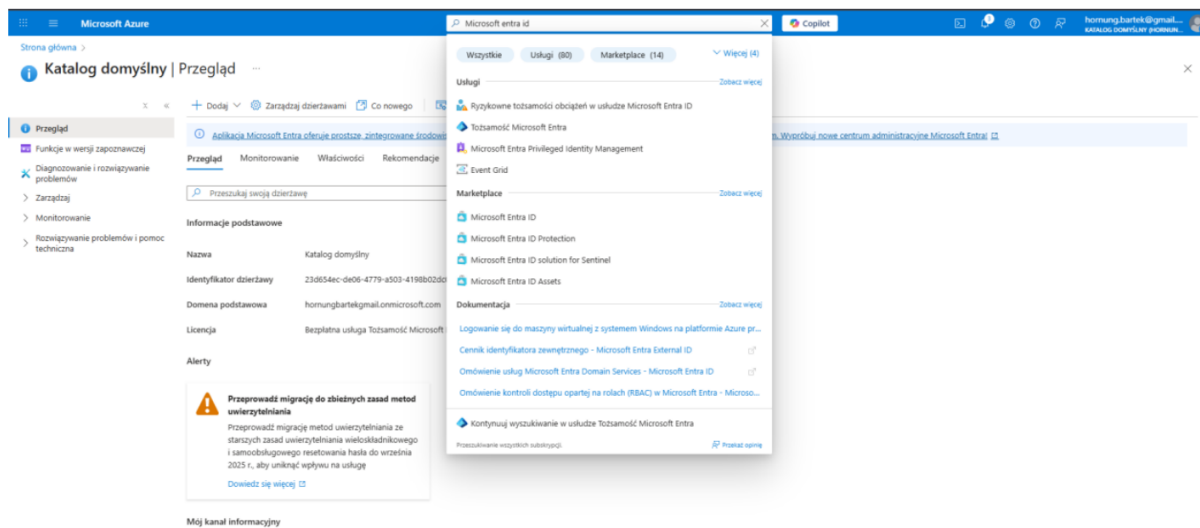
## 2. ETAP 2 — Utworzenie Resource Group dla zasobów adaptera



W Azure Portal wyszukaj „Grupy zasobów” i wybierz „Utwórz”.

- Ustaw parametry: Subskrypcja:
- „Azure subscription 1”, Grupa zasobów: „edu-lab-rg”, Region: „West Europe”.
- Kliknij „Przejrzyj i utwórz”, a następnie „Utwórz”.

## 3. ETAP 3 — Rejestracja aplikacji w Microsoft Entra ID (App Registration)



W Azure Portal wyszukaj „Microsoft Entra ID” (wynik typu „Usługa”), następnie przejdź do „Rejestracje aplikacji” i wybierz „Nowa rejestracja”.

W formularzu ustaw: Nazwa: „cloud-adapter-azure”, Obsługiwane typy kont: pierwsza opcja (konta tylko w tym katalogu / single-tenant), URI przekierowania: pozostaw puste.

Kliknij „Zarejestruj”, a następnie zanotuj z widoku „Przegląd” wartości: „Application (client) ID” oraz „Directory (tenant) ID”.

## 4. ETAP 4 — Utworzenie Client Secret dla aplikacji

W widoku aplikacji „cloud-adapter-azure” przejdź do: „Certyfikaty i tajne klucze”.

Kliknij „Dodaj wpis tajny klienta”, ustaw: Opis/Nazwa: „adapter-secret”, Wygasa: np. 12 miesięcy (lub zgodnie z polityką projektu), następnie kliknij „Dodaj”. Skopiuj natychmiast pole „Value” (to jest właściwy sekret używany przez adapter) i zapisz je bezpiecznie; „Secret ID” nie jest używany jako hasło.

## 5. ETAP 5 — Nadanie uprawnień Microsoft Graph dla aplikacji

> Group-OnPremisesSyncBehavior

▼ Group (1)

<input type="checkbox"/>	Group.Create ⓘ Create groups	Tak
<input type="checkbox"/>	Group.Read.All ⓘ Read all groups	Tak
<input checked="" type="checkbox"/>	Group.ReadWrite.All ⓘ Read and write all groups	Tak

> GroupMember

<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage all users' identities	Tak
<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Tak
<input type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	Tak
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Tak

W aplikacji „cloud-adapter-azure” przejdź do „Uprawnienia interfejsu API” i kliknij „Dodaj uprawnienie”, następnie wybierz „Microsoft Graph”.

Wybierz wyłącznie „Uprawnienia aplikacji” (nie „Delegowane”), a następnie dodaj: „User.ReadWrite.All” oraz „Group.ReadWrite.All”.

Strona główna > Katalog domyślny | Przegląd > cloud-adapter-azure

cloud-adapter-azure | Uprawnienia interfejsu API

Wyszukaj

Przegląd

Szybki start

Asystent integracji

Diagnostowanie i rozwiązywanie problemów

Zarządzaj

Znakowanie i właściwości

Authentication (Preview)

Certyfikaty i klucze tajne

Konfiguracja tokenu

Uprawnienia interfejsu API

Uwidocznij interfejs API

Role aplikacji

Właściciele

Role i administratorzy

Manifest

Pomoc techniczna i rozwiązywanie problemów

Edytuj uprawnienia do aplikacji. Użytkownicy będą musieli wyrazić zgodę nawet wtedy, gdy już ją wcześniej wyrazili.

Udzielenie zgody dla całej dzierżawy może spowodować wycofanie uprawnień, których udzielono już w całej dzierżawie dla tej aplikacji. Nie ma to wpływu na uprawnienia, które użytkownicy już udzieliłi we własnym in

Kolumna „Wymagana zgoda administratora” zawiera wartość domyślną dla organizacji. Jednak zgodę użytkownika można dostosować dla poszczególnych uprawnień, użytkowników lub aplikacji. Ta kolumna może nie będzie używana ta aplikacja. [Dowiedz się więcej](#)

Skonfigurowane uprawnienia

Aplikacje są autoryzowane do wywoływania interfejsów API po przyznaniu im uprawnień przez użytkowników/administratorów w ramach procesu wyrażania zgody. Lista skonfigurowanych uprawnień powinna zawierać wszystkie uprawnienia potrzebne aplikacji. [Dowiedz się więcej o uprawnieniach i zgodzie](#)

+ Dodaj uprawnienie ✓ Wyraż zgodę administratora dla katalogu Katalog domyślny

Interfejs API / Nazwa uprawnień	Typ	Opis	Wymagana zgoda a...	Stan
▼ Microsoft Graph (3)				
Group.ReadWrite.All	Aplikacja	Read and write all groups	Tak	⚠ Nie udzielono dla Katal...
User.Read	Delegowa...	Loguj się i odczytuj profil użytkownika	Nie	⚠ Nie udzielono dla Katal...
User.Read.All	Aplikacja	Read all users' full profiles	Tak	⚠ Nie udzielono dla Katal...

Aby wyświetlić uprawnienia ze zgodą dla poszczególnych aplikacji i zarządzać nimi, a także ustawienia zgody dzierżawy, wypróbuj [aplikację dla przedsiębiorstw](#).

Po dodaniu uprawnień kliknij „Wyraź zgodę administratora dla katalogu domyślnego” (Grant admin consent) i upewnij się, że uprawnienia mają status zatwierdzony.

Microsoft Azure

Strona główna > Katalog domyślny | Przegląd > cloud-adapter-azure

cloud-adapter-azure | Uprawnienia interfejsu API

Wyszukaj zasoby, usługi i dokumenty (G+/I)

Przegląd

Szybki start

Asystent integracji

Diagnozowanie i rozwiązywanie problemów

Zarządzaj

Znakowanie i właściwości

Authentication (Preview)

Certyfikaty i klucze tajne

Konfiguracja tokenu

**Uprawnienia interfejsu API**

Uwidocznij interfejs API

Rola aplikacji

Właściciele

Rola i administratorzy

Manifest

Pomyślnie udzielono zgody administratora na żądane uprawnienia.

Kolumna „Wymagana zgoda administratora” zawiera wartość domyślną dla organizacji. Jednak zgodę użytkownika można dostosować dla poszczególnych uprawnień, użytkowników lub aplikacji. [Dowiedz się więcej](#)

Skonfigurowane uprawnienia

Aplikacje są autoryzowane do wywoływania interfejsów API po przyznaniu im uprawnień przez użytkowników/administratorów w ramach procesu wyrażania zgody. Lista skonfigurowanych uprawnień powinna zawierać wszystkie uprawnienia potrzebne aplikacji. [Dowiedz się więcej o uprawnieniach i zgodzie](#)

+ Dodaj uprawnienie ✓ Wyraź zgodę administratora dla katalogu Katalog domyślny

Interfejs API / Nazwa uprawnień	Typ	Opis	Wymagana zgoda a...	Stan
▼ Microsoft Graph (3)				
Group.ReadWrite.All	Aplikacja	Read and write all groups	Tak	✓ Udzielono dla Katalog d...
User.Read	Delegowa...	Loguj się i odczytuj profil użytkownika	Nie	✓ Udzielono dla Katalog d...
User.ReadWrite.All	Aplikacja	Read and write all users' full profiles	Tak	✓ Udzielono dla Katalog d...

Aby wyświetlić uprawnienia ze zgodą dla poszczególnych aplikacji i zarządzać nimi, a także ustawienia zgody dzierżawy, wypróbuj [aplikację dla przedsiębiorstw](#).

## 6. ETAP 6 — Przypisanie ról RBAC na poziomie subskrypcji (dostęp do zasobów i kosztów)

Strona główna > Subskrypcje > Azure subscription 1

Subskrypcje

Katalog domyślny (homungbarke@gmail.com)

+ Dodaj Zarządzaj zasadami

Administratorzy globalni mogą zarządzać wszystkimi subskrypcjami na tej liście. [aktualizując ustawienia zasad tutaj.](#)

Wyświetli listę subskrypcji, dla których masz uprawnienia kontrolowania dostępu opartej na rolach do zarządzania zasobami platformy Azure. Aby wyświetlić subskrypcję, dla której masz dostęp do roli, kliknij tutaj.

Pokazywane są subskrypcje w katalogu Katalog domyślny. Nie widoczne subskrypcji? [Przełączanie katalogów](#)

Subskrypcje: Odfiltrowane (1 z 1)

Moja rola: wszystkie

Stan: wszystkie

Dodaj filtr

Nazwa subskrypcji: Azure subscription 1

Azure subscription 1 | Kontrola dostępu (IAM)

Wyszukaj

+ Dodaj Pobierz przypisanie ról Edycja kolumny Dodawanie Usunięcie Opinia

Wymagane akcje: Od 31 sierpnia 2024 r. zasoby Kluczowe role administratora platformy Azure (wraz z kluczowymi zasobami platformy Azure i usługą Azure Service Manager) zostaną wycofane i nie będą już obsługiwane. Jeśli nadal masz aktywne przypisanie ról w administratora lub administratora, natychmiast przekształć te role na usługi Azure RBAC. [Dowiedz się więcej](#)

Sprawdź dostęp Przypisanie ról Rola Przypisanie odmowy Administratorzy klasycznych

Mój dostęp

Wyświetl mój poziom dostępu do tego zasobu.

Wyświetl mój dostęp

Sprawdź dostęp

Przejrzyj poziom dostępu użytkownika, grupy, jednostki usługi lub tożsamości zarządzanej do tego zasobu. [Dowiedz się więcej](#)

Sprawdź dostęp

Udziel dostępu do tego zasobu

Udziel dostępu do zasobów przez przypisanie ról. [Dowiedz się więcej](#)

Dodaj przypisanie ról

Wyświetl dostęp do tego zasobu

Wyświetl przypisanie ról udzielające dostępu do tego i innych zasobów. [Dowiedz się więcej](#)

Wyświetl

Wyświetlanie przypisań odmowy

Wyświetl przypisanie ról, którym odmówiono dostępu do konkretnych akcji w tym zakresie. [Dowiedz się więcej](#)

Wyświetl

Tworzenie roli niestandardowej

Utwórz rolę niestandardową dla zasobów platformy Azure z własnym zestawem uprawnień, aby zaspokoić określone potrzeby Twojej organizacji. [Dowiedz się więcej](#)

Dodaj

Wejdź w subskrypcję (np. „Azure subscription 1”), następnie „Kontrola dostępu (IAM)” i wybierz „Dodaj przypisanie ról”.

Dodaj rolę „Contributor” dla tożsamości typu „Użytkownik, grupa lub podmiot usługi”,  
wyszukaj „cloud-adapter-azure” i wykonaj przypisanie.

Strona główna > Subskrypcje > Azure subscription 1 | Kontrola dostępu (IAM)

Subskrypcja

Wyszukaj

+ Dodaj Pobierz przypisanie ról Edycja kolumn Odwiesz Usual Opinia

Omówienie  
Dziennik aktywności  
Kontrola dostępu (IAM)  
Tagi  
Diagnostowanie i rozwiązywanie problemów  
Zabezpieczenia  
Wizualizator zasobów  
Zdarzenia  
Grupy zasobów  
Zasoby  
Zarządzanie kosztami  
Rozliczenie  
Ustawienia  
Monitorowanie  
Pomoc

Administrators globalni mogą zarządzać wszystkimi subskrypcjami na tej liście, aktualizując ustawienia zasad tutaj.

Wyświetlił listę subskrypcji, dla których masz uprawnienia kontroli dostępu oparte na rolach do zarządzania zasobami platformy Azure. Aby wyświetlić subskrypcję, dla której masz dostęp do rozliczeń, kliknij tutaj.

Pokazywane są subskrypcje w katalogu Katalog domyślny. Nie widzisz subskrypcji? Przeglądanie katalogów

Subskrypcje: **Odfiltrowane (1 z 1)**

Moje role == wszystkie

Stan == wszystkie

Dodaj filtr

Nazwa subskrypcji

Azure subscription 1

Definicja roli to kolekcja uprawnień. Możesz zastosować wbudowane role lub utworzyć własne role niestandardowe. [Dowiedz się więcej](#)

Wszystko Role funkcji zadania **Role administratorów uprzywilejowanych**

Wyszukaj według nazwy roli, opisu, uprawnień lub ...

Typ: Wszystkie Kategoria: Wszystkie

Nazwa	Opis	Typ	Kategoria	Szczegóły
Właściciel	Przyznaje pełen dostęp do zarządzania wszystkimi zasobami, w tym przypisywania ról w ramach...	BuiltInRole	Ogólne	<a href="#">Wyświetl</a>
Współautor	Zapewnia pełny dostęp do zarządzania wszystkimi zasobami, ale nie pozwala na przypisywanie...	BuiltInRole	Ogólne	<a href="#">Wyświetl</a>
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed...	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Administrator dostępu użytkowników	Umożliwia zarządzanie dostępem użytkowników do zasobów platformy Azure.	BuiltInRole	Ogólne	<a href="#">Wyświetl</a>
Administrator rezerwacji	Pozwala odczytywać i zarządzać wszystkimi rezerwacjami w dzierżawie	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Azure IoT Operations Onboarding	User can Azure arc connect and deploy Azure IoT Operations securely.	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Azure Resilience Management Drills ...	Administrator Role of Azure Resilience Management Drills Service	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Azure Resilience Management Drills ...	This Role grants permissions on the Chaos Subscription to create, read, and delete Resource G...	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Azure Resilience Management Drills ...	This role should be assigned at the Service Group Members scope to enable resource read acc...	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Azure Resilience Management Recov...	Administrator Role of Azure Resilience Management Recovery Service	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Azure Resilience Management Recov...	Contributor Role of Azure Resilience Management Recovery Service	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Role Based Access Control Administr...	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not all...	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Service Group Administrator	Role Definition for administrator of a Service Group	BuiltInRole	Brak	<a href="#">Wyświetl</a>
Service Group Contributor	Role Definition for contributor of a Service Group	BuiltInRole	Brak	<a href="#">Wyświetl</a>

Wyświetlane 1 — 14 z 14 wyników.

Powtórz procedurę dla roli „Cost Management Reader”, również przypisując ją do „cloud-adapter-azure”.

Strona główna > Subskrypcje > Azure subscription 1 | Kontrola dostępu (IAM)

Dodawanie przypisania roli

Rola Członkowie Warunki [Przejrzyj i przypisz](#)

Definicja roli to kolekcja uprawnień. Możesz zastosować wbudowane role lub utworzyć własne role niestandardowe. [Dowiedz się więcej](#)

Funkcja Copilot może pomóc w wybraniu roli

Role funkcji zadania Role administratorów uprzywilejowanych

Udział dostępu do zasobów platformy Azure na podstawie funkcji zadania, takiej jak możliwość tworzenia maszyn wirtualnych.

Wyszukaj

Typ: Wszystkie Kategoria: Wszystkie

Nazwa	Opis	Typ	Kategoria	Szczegóły
Cost Management — czytelnik	Może wyświetlać konfigurację i dane kosztów (np. budżety, operacje eksportu)	BuiltInRole	Zarządzanie i nadzór	<a href="#">Wyświetl</a>
Cost Management — współautor	Może wyświetlać koszty i zarządzać konfiguracją kosztów (np. budżetów, operacji eksportu)	BuiltInRole	Zarządzanie i nadzór	<a href="#">Wyświetl</a>

Na koniec w „Przypisanie ról” sprawdź czy obie role są widoczne na zakresie „Subskrypcja”.

Strona główna > Subskrypcje > Azure subscription 1 | Kontrola dostępu (IAM) > Dodawanie przypisania roli

Dodawanie przypisania roli

Rola Członkowie Warunki [Przejrzyj i przypisz](#)

Rola Cost Management — czytelnik

Zakres

Członkowie

Nazwa	Identyfikator obiektu	Typ
cloud-adapter-azure		Aplikacja

Opis Brak opisu

## 7. ETAP 7 — Utworzenie pliku .env (konfiguracja uruchomieniowa adaptera)

Utwórz plik „.env” w katalogu uruchomieniowym adaptera (zgodnie ze strukturą projektu) i przygotuj poniższe klucze.

Uzupełnij wartości na podstawie danych z poprzednich etapów: Tenant ID i Client ID z „Przegląd” aplikacji, Client Secret z pola „Value”, Subscription ID z widoku subskrypcji, Resource Group i region zgodnie z konfiguracją.

```
AZURE_TENANT_ID=<Directory (tenant) ID>
AZURE_CLIENT_ID=<Application (client) ID>
AZURE_CLIENT_SECRET=<Client Secret VALUE>
AZURE_SUBSCRIPTION_ID=<Subscription ID>
AZURE_DEFAULT_RESOURCE_GROUP=edu-lab-rg
AZURE_DEFAULT_REGION=westeurope
```