

Azure Active Directory

Jak zarządzać tożsamością oraz uprawnieniami dostępu do zasobów? Odpowiedzią na to pytanie jest usługa Azure Active Directory (AAD), dzięki której można konfigurować uwierzytelnianie użytkowników w chmurze, oraz mechanizm RBAC (ang. role-based access control — kontrola dostępu oparta na rolach) definiujący uprawnienia dostępu do zasobów.

Usługa Azure Active Directory

Azure Active Directory jest chmurową usługą katalogową, która umożliwia zarządzanie tożsamością i uprawnieniami dostępu użytkowników i aplikacji do zasobów. Często określa się ją mianem IaaS.

Usługa AAD umiejscowiona jest na szczycie hierarchii usług w chmurze Azure i jest bezpośrednio związana z podmiotem. Jeden podmiot może posiadać wiele subskrypcji, a w ramach każdej subskrypcji można tworzyć wiele grup obejmujących wiele zasobów.

W ramach jednego konta Azure można mieć dostęp do wielu odizolowanych od siebie podmiotów. Użytkownikowi po zalogowaniu jest przypisywany domyślny katalog i podmiot oraz przydzielany dostęp do zasobów powiązanych wyłącznie z danym podmiotem i jego subskrypcjami. Aby użytkownik mógł zarządzać zasobami innego podmiotu, musi zmienić katalog.

Usługa AAD jest oferowana w czterech warstwach cenowych:

- ☐ bezpłatnej,
- ☐ Office 365,
- ☐ PremiumP1,
- ☐ PremiumP2.

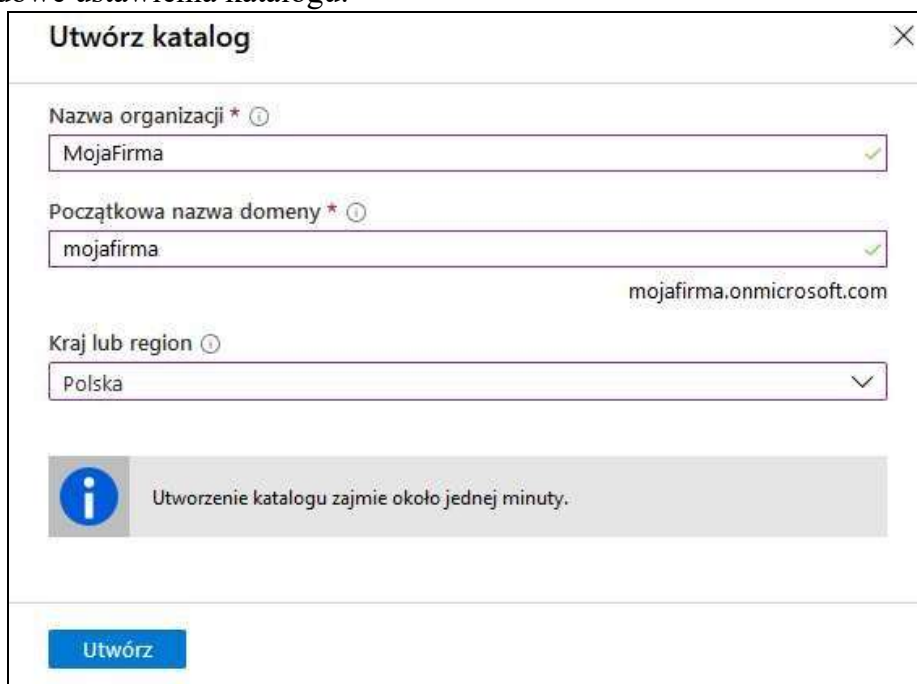
Warstwa Microsoft 365 oferuje m.in. możliwość zarządzania dostępem aplikacji chmurowych do zasobów, zarządzania tożsamością, definiowania grup, samodzielnego resetowania hasła i korzystania z usługi AAD Application Proxy.

W warstwach Premium dostępne są dodatkowe funkcjonalności korporacyjne, takie jak tworzenie dynamicznych grup, samodzielne zarządzanie grupami, zarządzanie tożsamością Microsoft (warstwa Premium P1). Warstwa Premium P2 zawiera wszystkie funkcjonalności warstwy P1, a ponadto ochronę tożsamości i zarządzanie uprzywilejowaną tożsamością.

Wykład skupia się na funkcjonalnościach oferowanych w bezpłatnej warstwie umożliwiającej tworzenie maksymalnie 500 000 obiektów katalogowych, zarządzanie

użytkownikami i ich grupami, synchronizowanie katalogu z lokalnym kontrolerem oraz tworzenie podstawowych raportów bezpieczeństwa. Warstwa ta w zupełności wystarczy do zapoznania się z podstawowymi widokami i samą usługą AAD. Funkcjonalności wszystkich warstw mogłyby być prawdopodobnie tematem osobnych wykładów i byłyby to w mojej ocenie materiały zbyt obszerny jak na nasze zajęcia.

Wprawdzie w ramach subskrypcji jest już dostępny jeden katalog (podmiot), warto jednak wiedzieć, jak się tworzy nowy. W tym celu kliknij ikonę Utwórz zasób, następnie sekcję Tożsamość i ikonę Azure Active Directory. W widoku, który się pojawi, wpisz nazwę organizacji i początkową nazwę domeny oraz wybierz kraj lub region. Początkowa nazwa domeny musi być unikatowa, ponieważ zostanie użyta do utworzenia pełnej nazwy w formacie nazwa_domeny.onmicrosoft.com. Tę nazwę będzie można później dostosować. Oto przykładowe ustawienia katalogu:




Utwórz katalog

Nazwa organizacji * ⓘ
MojaFirma ✓

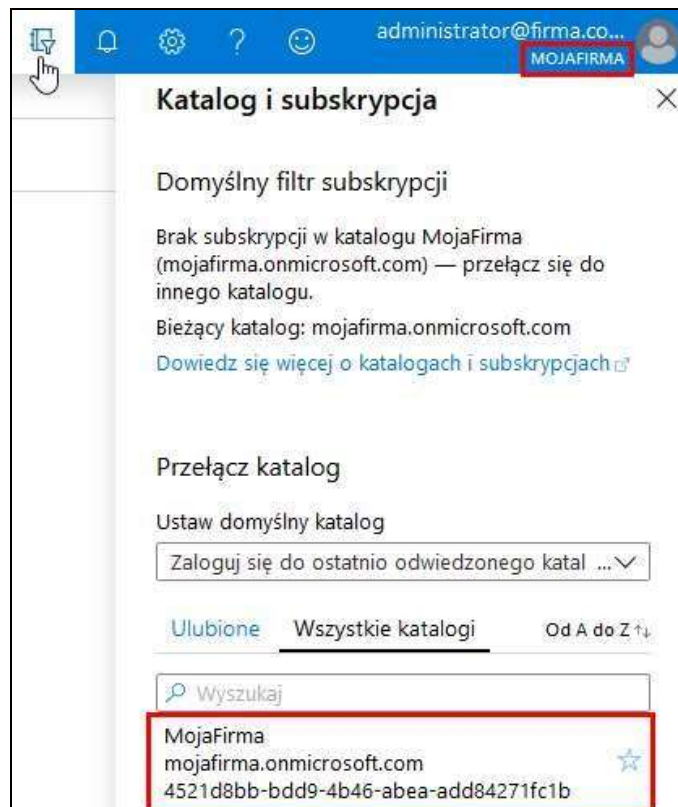
Początkowa nazwa domeny * ⓘ
mojafirma ✓
mojafirma.onmicrosoft.com

Kraj lub region ⓘ
Polska ▼

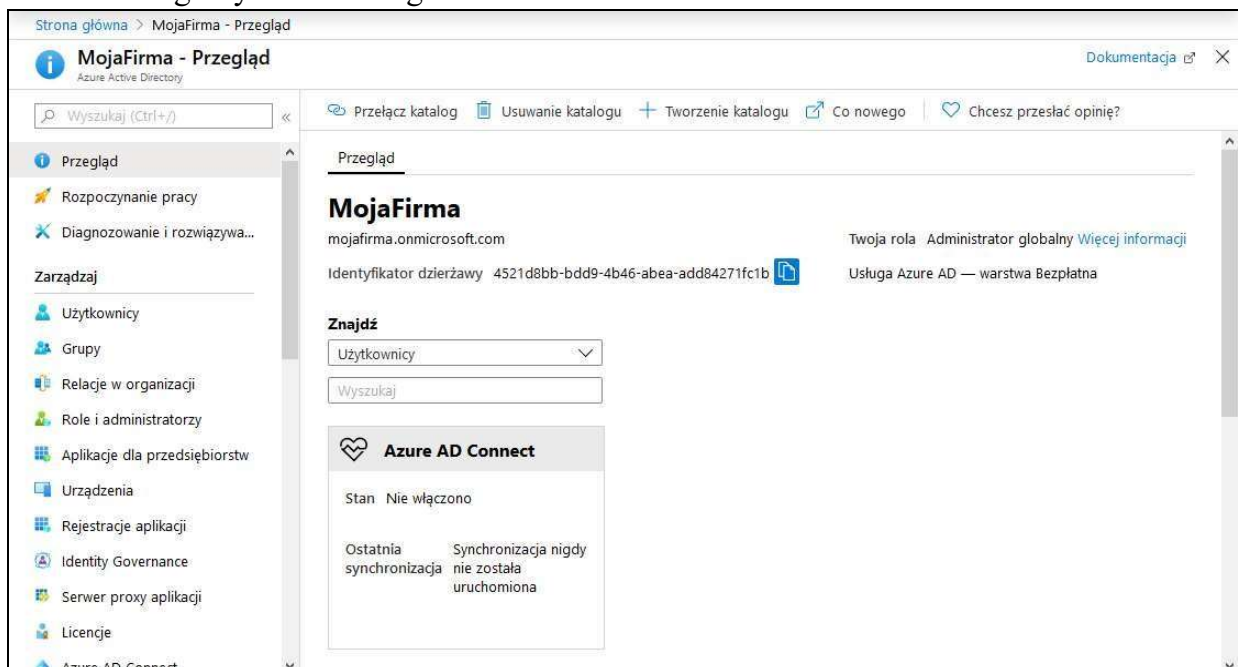
 Utworzenie katalogu zajmie około jednej minuty.

Utwórz

Tworzenie nowego katalogu trwa około 1 minuty. Aby nim zarządzać, trzeba się na niego przełączyć. Należy zwrócić uwagę, że nazwa katalogu jest widoczna pod nazwą profilu. Aby zmienić katalog, kliknij ikonę Katalog i subskrypcja znajdującą się obok nazwy profilu. Pojawi się taka oto lista:



Po przełączeniu katalogu pojawi się nowy podmiot bez przypisanych subskrypcji. Aby móc korzystać z zasobów Azure, trzeba utworzyć nową subskrypcję. Jedynym zasobem, którym można zarządzać w pustym podmiocie zdefiniowanym w bezpłatnej warstwie, jest usługa AAD. Oto ogólny widok usługi:



Pierwszą rzeczą, którą należy zrobić po utworzeniu nowego katalogu, jest dostosowanie nazwy domeny. W tym celu w widoku usługi AAD kliknij w sekcji Zarządzaj opcję Nazwy domen niestandardowych, a następnie ikonę Dodaj domenę niestandardową. Pojawi się widok, w którym możesz wpisać nazwę swojej publicznej domeny. Oto przykładowa niestandardowa domena azure.mojachmura.pl:

Niestandardowa nazwa dome... ×

MojaFirma

Niestandardowa nazwa domeny * ⓘ

azure.mojachmura.pl ✓

Dodaj domenę

Po utworzeniu niestandardowej domeny trzeba ją zweryfikować, a dokładniej — zweryfikować prawa własności do niej. W tym celu należy u rejestratora domeny utworzyć nowy rekord typu TXT lub MX. Oto przykładowe ustawienia:

azure.mojachmura.pl ×

Niestandardowa nazwa domeny

Usuń Chcesz przesłać opinię?

i Aby używać domeny azure.mojachmura.pl w usłudze Azure AD, utwórz nowy rekord TXT u rejestratora swojej nazwy domeny, posługując się informacjami poniżej.

Typ rekordu

TXT

MX

Alias lub nazwa hosta

@

Lokalizacja docelowa lub wyznaczony adres

MS=ms46890338

Czas wygaśnięcia

3600

Udostępnij te ustawienia za pośrednictwem poczty e-mail

Weryfikacja nie zakończy się pomyślnie do momentu skonfigurowania domeny przy użyciu rejestratora w sposób opisany powyżej.

Weryfikuj

Po kliknięciu przycisku Weryfikuj pojawi się komunikat o błędzie, jak na poniższym rysunku. Serwer DNS potrzebuje do 72 godzin na rozgłoszenie zmian, jednak zazwyczaj czas ten nie przekracza 30 minut. Czas zależy od wykorzystywanego serwera.

i Zweryfikuj nazwę domeny 12:48 ×

Nie można zweryfikować nazwy domeny
azure.mojachmura.pl

Gdy zmiany zostaną rozgłoszone i weryfikacja przebiegnie pomyślnie, pojawi się strona z odpowiednim komunikatem i dwiema dodatkowymi opcjami: oznaczenia domeny jako podstawowej i pobrania programu Azure AD Connect. Na razie nie będziemy zajmować się tym programem, natomiast zalecane jest oznaczenie domeny jako podstawowej. Nazwa ta będzie stanowiła sufiks nazw, to znaczy zamiast domyślnej nazwy użytkownika `nazwa_użytkownika@nazwa_domeny.onmicrosoft.com` będzie stosowana nazwa `nazwa_użytkownika@nazwa_domeny.pl`. W tym konkretnym przykładzie zamiast `nazwa_użytkownika@mojafirma.onmicrosoft.com` będzie używana domyślna nazwa `nazwa_użytkownika@azure.mojachmura.pl`. Oto strona z pomyślnie zweryfikowaną domeną:

azure.mojachmura.pl
Niestandardowa nazwa domeny

Oznacz jako podstawową Usuń

Weryfikacja zakończyła się pomyślnie.

Typ	Niestandardowa
Stan	Zweryfikowano
Federacyjne	Nie
Aby skonfigurować domenę <code>azure.mojachmura.pl</code> do federacyjnego logowania do usługi Azure Active Directory, uruchom program Azure AD Connect w sieci lokalnej.	
Pobierz program Azure AD Connect	
Główna domena	Nie
W użyciu	Nie

Utworzyłeś nowy katalog, więc możesz zacząć tworzyć konta użytkowników i przydzielać im uprawnienia dostępu do zasobów. Jednak niemal w każdym lokalnym środowisku jest już stosowane rozwiązanie do zarządzania tożsamością użytkowników. Jeżeli konta zdefiniuje się dodatkowo w chmurze, mogą się pojawić niespójności w danych. Użytkownicy będą mieli problemy z zapamiętaniem, którego konta mają używać w poszczególnych sytuacjach. Dodatkowo, jeżeli konta w obu środowiskach będą miały takie same nazwy, użytkownicy często będą logować się do niewłaściwych kont.

Na szczęście jest program Azure AD Connect, który synchronizuje usługi AAD z lokalnym kontrolerem domeny, dzięki czemu użytkownicy mogą wszędzie korzystać z jednego konta. W efekcie wszyscy są zadowoleni: użytkownicy nie muszą się zastanawiać, którego konta mają użyć (ponieważ jest tylko jedno), a administratorzy mają mniej problemów do rozwiązywania (jest mniej kont do zarządzania i przypadków blokowania kont z powodu wielokrotnego wpisania błędnego hasła).

Ponadto za pomocą programu Azure AD Connect można zaimplementować mechanizm SSO (ang. Single Sign-On — jednokrotne logowanie), dzięki któremu dostęp do zasobów

w chmurze Azure i w lokalnym środowisku jest możliwy po jednokrotnym zalogowaniu się do domeny.

Aby zsynchronizować usługę AAD z lokalnym kontrolerem domeny, należy z widoku usługi kliknąć opcję Azure AD Connect. Pojawi się informacja o aktualnym stanie synchronizacji, jak na poniższym rysunku. Jeżeli synchronizacja nie została jeszcze włączona, z tego widoku można pobrać program Azure AD Connect.

APROWIZUJ Z USŁUGI ACTIVE DIRECTORY

**Aprobowizowanie w chmurze programu Azure AD Connect**

Ta funkcja umożliwia zarządzanie aprobowizowaniem z chmury.

[Zarządzaj aprobowizacją \(wersja zapoznawcza\)](#)

Synchronizacja programu Azure AD Connect

Nie zainstalowano	Pobierz program Azure AD Connect
Ostatnia synchronizacja	Synchronizacja nigdy nie została uruchomiona
Synchronizacja skrótu hasła	Wyłączono

LOGOWANIE UŻYTKOWNIKA



Federacja	Wyłączono	Odomeny
Bezproblemowe logowanie jednokrotne	Wyłączono	Odomeny
Uwierzytelnianie przekazywane	Wyłączono	Oagenci

WPROWADZANIE ETAPOWE UWIERZYTELNIANIA W CHMURZE



Ta funkcja umożliwia testowanie uwierzytelniania w chmurze i stopniowe migrowanie z uwierzytelniania federacyjnego.

[Włącz wprowadzanie etapowe dla logowania użytkowników zarządzanych \(wersja zapoznawcza\)](#)

APLIKACJE LOKALNE



Chcesz skonfigurować dostęp zdalny do aplikacji lokalnych? [Przejdź do serwera proxy aplikacji](#)

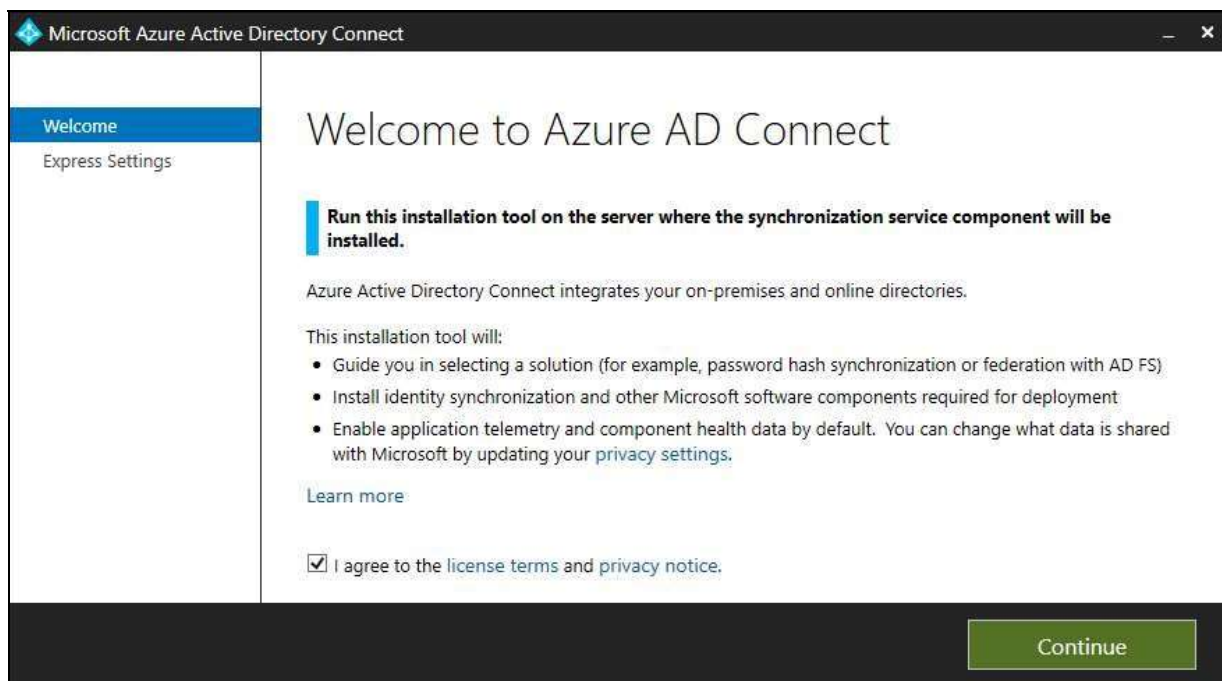
KONDYCJA I ANALIZA



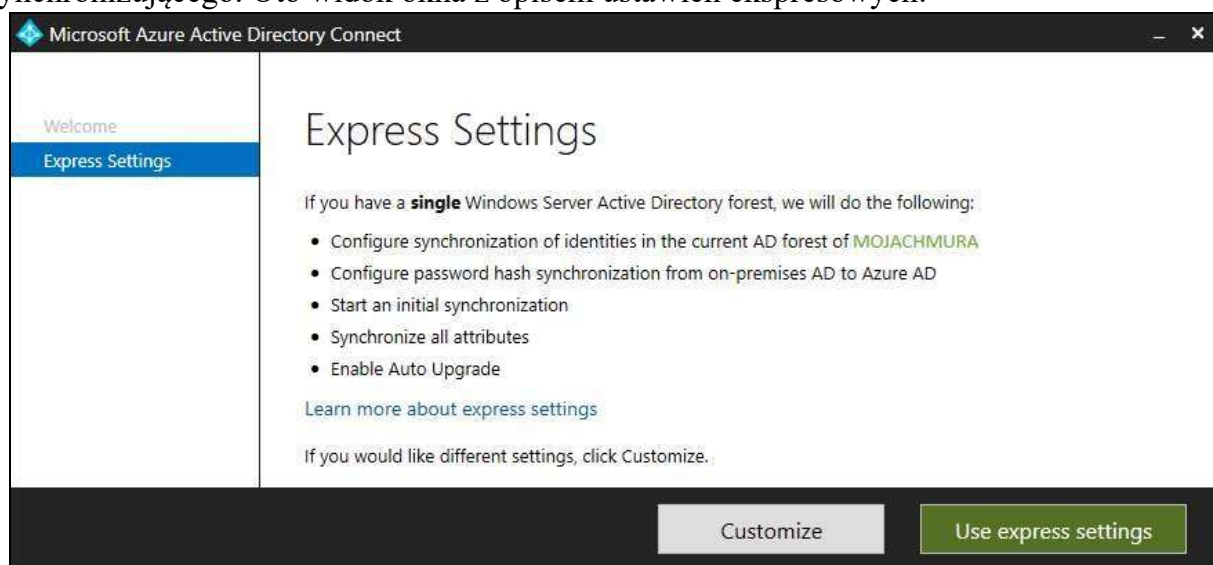
Monitoruj lokalną infrastrukturę tożsamości i usługi synchronizacji w chmurze. [Azure AD Connect Health](#)

Program Azure AD Connect instaluje się na serwerze w lokalnym środowisku. Zalecane jest wybranie serwera, który nie jest kontrolerem domeny, ale odwołuje się do niego. Wybrany serwer musi mieć połączenie z Internetem, ponieważ będzie synchronizował dane pomiędzy lokalnym kontrolerem domeny a usługą AAD. Program szyfruje wszystkie odbierane i wysyłane dane.

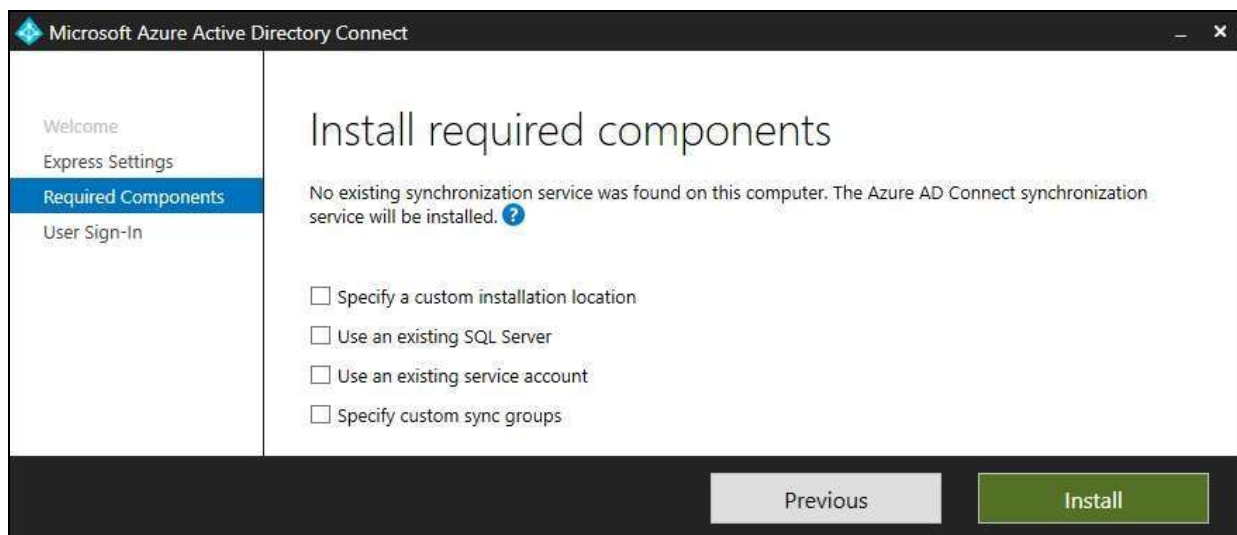
Kreator instalacji jest bardzo intuicyjny. Każdy krok jest opisany, więc nie trzeba korzystać z instrukcji (ani znać struktury lokalnego kontrolera domeny). Oto pierwsze okno programu instalacyjnego, w którym opisane są jego funkcje:



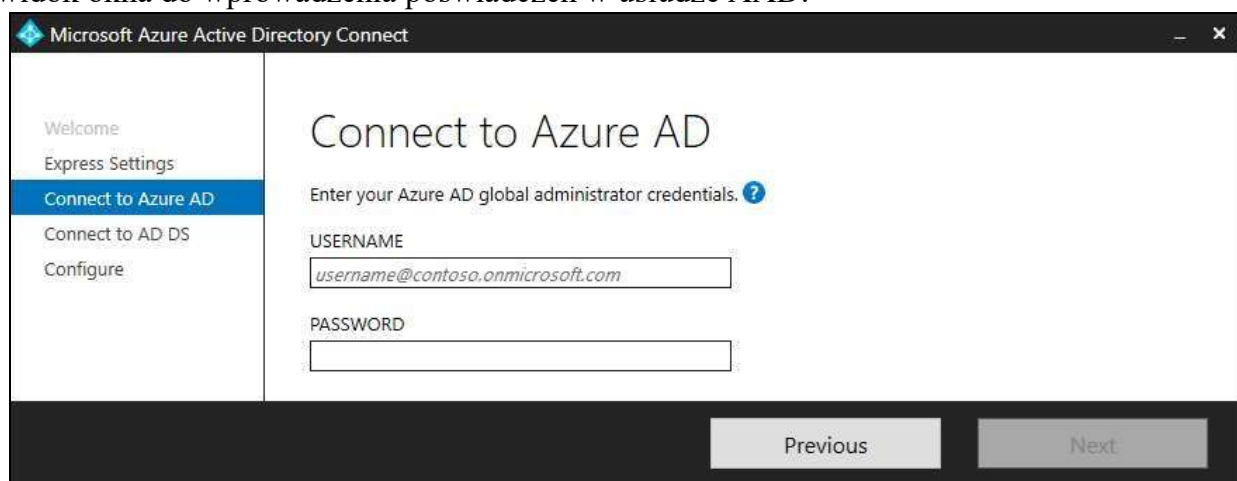
W następnym oknie należy zdecydować, czy mają być użyte ustawienia ekspresowe (przycisk Use express settings) czy niestandardowe (Customize). W pierwszym przypadku zostaną od razu określone wszystkie ustawienia, takie jak domyślna ścieżka instalacji, parametry synchronizacji, hasła, atrybuty i tożsamości, jak również zostanie zainstalowany serwer SQL Express. Program utworzy również nowe konto serwisowe dla procesu synchronizującego. Oto widok okna z opisem ustawień ekspresowych:



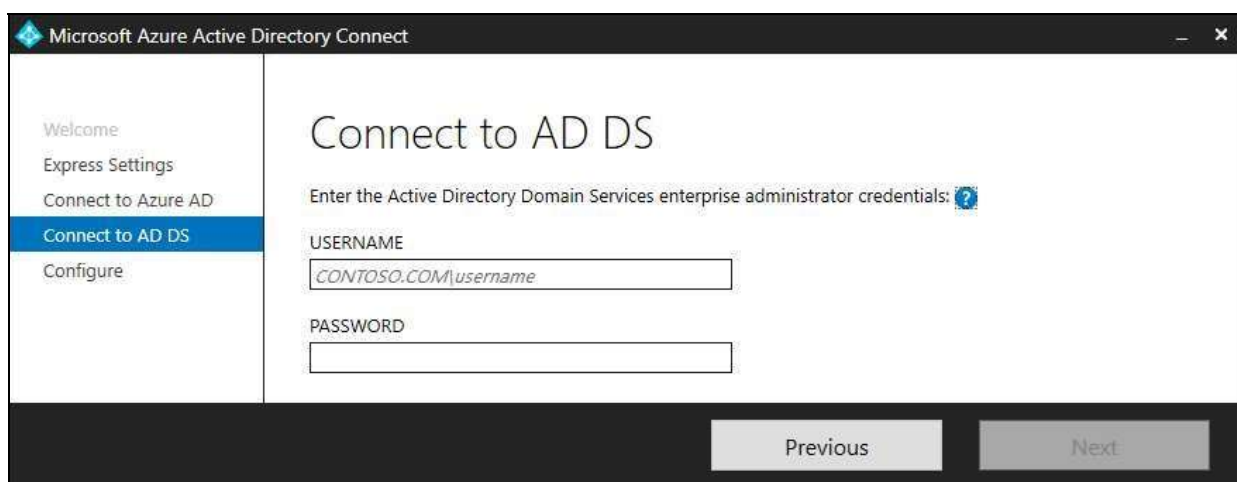
Jeżeli klikniesz przycisk Customize, będziesz mógł określić takie ustawienia jak ścieżka instalacyjna, instancja serwera SQL Server i grupy synchronizacji. Dodatkowo możesz wskazać istniejącą instancję serwera SQL Server, wybrać do synchronizowania tylko określone grupy użytkowników oraz wskazać konto dla procesu synchronizującego. Oto okno z ustawieniami niestandardowymi:



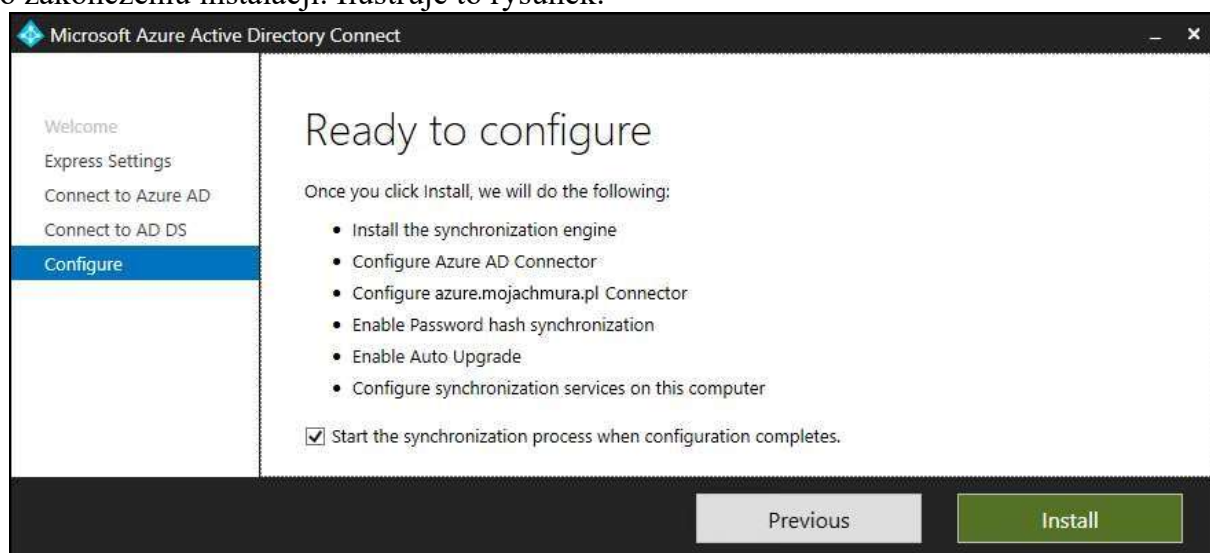
Po skonfigurowaniu ustawień musisz podać poświadczenia dla dwóch kont, które będą wykorzystywane podczas synchronizacji. Najpierw podaj login i hasło do konta w usłudze AAD z globalnymi uprawnieniami administracyjnymi. Zalecane jest w tym celu utworzenie osobnego konta. Jeżeli zostanie wybrane personalne konto administratora, to gdy zmieni on za jakiś czas pracę, jego konto zostanie usunięte, a synchronizacja zostanie wyłączona. Oto widok okna do wprowadzenia poświadczeń w usłudze AAD:



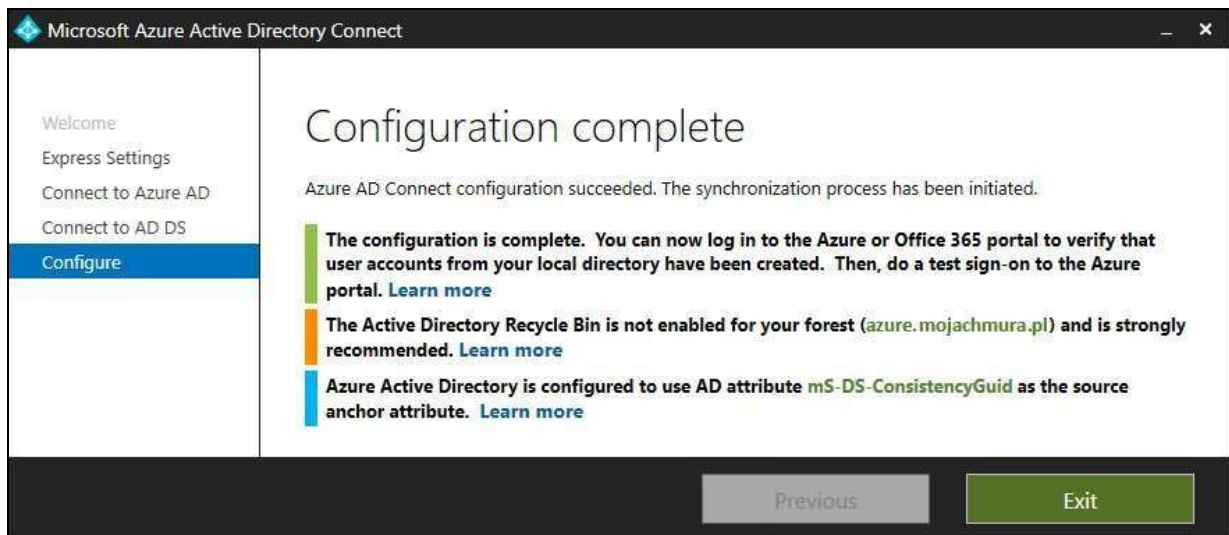
W kolejnym kroku podaj poświadczenia konta administratora usług Active Directory Domain Services. Jak poprzednio, nie powinno to być konto personalne, lecz serwisowe. Oto okno do wprowadzania opisanych poświadczeń:



Na zakończenie pojawi się okno, w którym musisz potwierdzić ustawienia instalacyjne. Widoczne są w nim operacje do wykonania oraz opcja rozpoczęcia synchronizacji zaraz po zakończeniu instalacji. Ilustruje to rysunek:



Po zakończonej instalacji pojawi się okno z informacjami o stanie programu i zalecanymi dodatkowymi operacjami do wykonania. W trakcie instalacji zostały sprawdzone aktualne ustawienia usługi AD i w tym przykładzie zalecane jest włączenie usługi Active Directory Recycle Bin. Oto wygląd ostatniego okna programu (zobacz pierwszy rysunek na następnej stronie). W widoku usługi AAD po kliknięciu opcji Azure AD Connect zmieni się informacja o stanie usługi. Nie będzie już odnośnika do pobrania programu Azure AD Connect. Zamiast tego pojawi się informacja, że synchronizacja jest włączona i ostatnio miała miejsce przed niecałą godziną. W zależności od ustawień lokalnego środowiska mogą się pojawić informacje o federacji, mechanizmie SSO i innych funkcjonalnościach. Oto przykładowy widok ze stanem usługi.



APROWIZUJ Z USŁUGI ACTIVE DIRECTORY



Aprobowizowanie w chmurze programu Azure AD Connect

Ta funkcja umożliwia zarządzanie aprobowizowaniem z chmury.

[Zarządzaj aprobowizacją \(wersja zapoznawcza\)](#)

Synchronizacja programu Azure AD Connect

Stan synchronizacji	Włączono
Ostatnia synchronizacja	Mniej niż 1 godzinę temu
Synchronizacja skrótu hasła	Włączono

LOGOWANIE UŻYTKOWNIKA



Federacja	Wyłączono	0 domen
Bezproblemowe logowanie jednokrotne	Wyłączono	0 domen
Uwierzytelnianie przekazywane	Wyłączono	0 agencji

WPROWADZANIE ETAPOWE UWIERZYTELNIANIA W CHMURZE



Ta funkcja umożliwia testowanie uwierzytelniania w chmurze i stopniowe migrowanie z uwierzytelniania federacyjnego.

[Włącz wprowadzanie etapowe dla logowania użytkowników zarządzanych \(wersja zapoznawcza\)](#)

APLIKACJE LOKALNE



Chcesz skonfigurować dostęp zdalny do aplikacji lokalnych? [Przejdź do serwera proxy aplikacji](#)














KONDYCJA I ANALIZA



Monitoruj lokalną infrastrukturę tożsamości i usługi synchronizacji w chmurze. [Azure AD Connect Health](#)

Po pomyślnej synchronizacji w usłudze AAD będą dostępne konta wszystkich użytkowników. W tej usłudze konto może mieć jedno z dwóch źródeł: Usługa AD systemu Windows Server lub Azure Active Directory. Pierwsze oznacza, że konto danego użytkownika pojawiło się w wyniku synchronizacji danych z lokalnym kontrolerem domeny. Natomiast z drugiego źródła pochodzą konta utworzone bezpośrednio w usłudze AAD. Jest jeszcze trzecie źródło, Konto Microsoft, dotyczące kont Microsoft Live.

W kolumnie Typ użytkownika widoczny jest typ Member (członek) lub Guest (gość). Pierwszego typu są konta utworzone w Twojej domenie. Konta drugiego typu należą do usługi Microsoft Live lub innej usługi AAD. Ta sama zasada dotyczy kont zewnętrznych (należących do innych podmiotów). Konta tworzone w nowym podmiocie są wyłącznie typu Member. Oto przykładowa lista członków domeny:

+ Nowy użytkownik + Nowy użytkownik-gość ↑ Tworzenie zbiorcze ↑ Zaproś zbiorczo ↑ Usuwanie zbiorcze ...				
Wyszukaj		Wyszukaj atrybuty		Pokaż
<input type="text" value="Nazwisko lub adres e-mail"/>		<input type="text" value="Nazwisko, adres e-mail (z...)"/> ▼		<input type="text" value="Wszyscy użytkownicy"/> ▼
Nazwa	Nazwa użytkownika	Typ użytkownika	Źródło	
<input type="checkbox"/>  Antoni Nowak	antoni.nowak@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Franciszek Woźniak	franciszek.wozniak@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Jakub Wiśniewski	jakub.wisniewski@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Jan Kowalczyk	jan.kowalczyk@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Julia Kowalska	julia.kowalska@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Lena Zielińska	len.zielinska@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Maja Szymańska	maja.szymanska@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  On-Premises Directory Syn	Sync_KONTROLERDOMENY_b1d87adb...	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Szymon Lewandowski	szymon.lewandowski@azure.mojachmu...	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Zofia Kamińska	zofia.kaminska@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Zuzanna Wójcik	zuzanna.wojcik@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Zofia Kamińska	zofia.kaminska@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	
<input type="checkbox"/>  Zuzanna Wójcik	zuzanna.wojcik@azure.mojachmura.pl	Member	Usługa AD systemu Windows Server	

Tworzenie nowego konta użytkownika

Źródło Azure Active Directory oznacza, że dane konto zostało utworzone w usłudze AAD. Jak już wspomniałem, do synchronizowania danych należy używać konta serwisowego. Pamiętaj, że do tego konta musi być przypisana rola globalnego administratora. Aby utworzyć nowe konto użytkownika, kliknij w widoku usługi opcję Użytkownicy, a następnie ikonę Nowy użytkownik. Oto przykład tworzenia nowego konta:

Nowy użytkownik

MojaFirma

Chcesz przesłać opinię?

Nazwa użytkownika *

AAD ✓

@

azure.mojachmura.pl ▼

Nazwa domeny, której potrzebuję, nie jest tutaj wyświetlana

Nazwa *

Administrator domeny ✓

Imię

Nazwisko

Hasło

☒ Automatycznie generuj hasło

☐ Chcę samodzielnie utworzyć hasło

Hasło początkowe

••••••••

☐ Pokaż hasło

Grupy i role

Grupy

Wybrane grupy: 0

Role

Administrator globalny

Ustawienia

Blokuj logowanie

Tak

Nie

Lokalizacja użycia

Filtruj lokalizacje użycia ▼

Informacje o stanowisku

Stanowisko

Dział

Utwórz


Domyślnie nowemu użytkownikowi tworzonemu w usłudze AAD jest przypisywana rola Użytkownik, którą można zmienić, zarówno na etapie tworzenia konta, jak i później.

Po utworzeniu konta użytkownika można monitorować jego aktywność. W tym celu w widoku konta kliknij opcję Profil. Oto przykładowy widok profilu użytkownika:

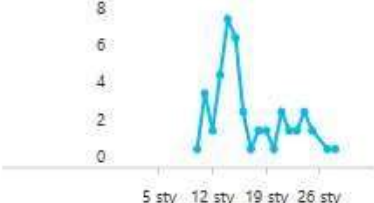
[Edytuj](#)
[Resetuj hasło](#)
[Usuń](#)
[Chcesz przesłać opinię?](#)

Administrator domeny

AAD@azure.mojachmura.pl



Logowania użytkownika



5 sty 12 sty 19 sty 26 sty

Członkostwa w grupach

1

Tożsamość [edytuj](#)

Nazwa	Imię	Nazwisko
Administrator domeny	-- --	-- --
Nazwa użytkownika	Typ użytkownika	
AAD@azure.mojachmura.pl	Member	
Identyfikator obiektu	Źródło	
e0053edf-9fa5-4ee3...	Azure Active Directory	

Informacje o stanowisku [edytuj](#)

Stanowisko	Dział	Menedżer
-- --	-- --	

Jedną z najważniejszych operacji administracyjnych jest przypisywanie ról użytkownikom. Po kliknięciu w widoku użytkownika opcji Przypisane role, a następnie ikony Dodaj przypisania pojawi się lista ról, które można przypisywać użytkownikom, wraz z opisami (zobacz pierwszy rysunek na następnej stronie).

Aby ułatwić sobie administrowanie kontami użytkowników, można je umieszczać w grupach. Role przypisywane danej grupie są automatycznie dziedziczone przez użytkowników należących do tej grupy. Ustawienia grup można synchronizować, podobnie jak ustawienia kont użytkowników. Oto przykładowe grupy, do których należy jeden z użytkowników (zobacz drugi rysunek na następnej stronie).

Role katalogu

Wybierz role administratora, które chcesz przypisać temu użytkownikowi. [Dowiedz się więcej](#)

Wyszukaj



Wyszukaj według nazwy lub o...

Typ

Wszystkie

	Rola	Opis
<input type="checkbox"/>	Administrator aplikacji	Może tworzyć wszystkie aspekty rejestracji aplikacji i aplikacji przedsiębiorstw...
<input type="checkbox"/>	Administrator aplikacji pakietu ...	Może zarządzać usługami w chmurze aplikacji pakietu Office, w tym zasadami...
<input type="checkbox"/>	Administrator aplikacji w chmu...	Może tworzyć wszystkie aspekty rejestracji aplikacji i aplikacji przedsiębiorstw...
<input type="checkbox"/>	Administrator atrybutów przep...	Może tworzyć schematy atrybutów dostępne dla wszystkich przepływów użyt...
<input type="checkbox"/>	Administrator danych zgodności	Może tworzyć zawartość zgodności i zarządzać nią.
<input type="checkbox"/>	Administrator dostępu warunk...	Może zarządzać możliwościami dostępu warunkowego.
<input type="checkbox"/>	Administrator grup	Może zarządzać wszystkimi aspektami grup i ustawieniami grup, takimi jak za...
<input type="checkbox"/>	Administrator haseł	Może resetować hasła dla użytkowników niebędących administratorami i adm...
<input type="checkbox"/>	Administrator komunikacji w us...	Może zarządzać funkcjami rozmów telefonicznych i spotkań w ramach usługi ...
<input type="checkbox"/>	Administrator licencji	Możliwość przypisywania, usuwania i aktualizacji przypisań licencji.
<input type="checkbox"/>	Administrator platformy Power	Może tworzyć wszystkie aspekty usług Microsoft Dynamics 365, PowerApps i ...

+ Dodaj członkostwa
Usuwanie członkostw
Odśwież
Kolumny
Chcesz przesłać opinię?

	Nazwa	Identyfikator obiektu	Typ grupy	Typ członkostwa
<input type="checkbox"/>	 AAD DC Administrators	5dde71dc-7eb0-4157-9292-c...	Zabezpieczenia	Przypisano
<input type="checkbox"/>	 Departament Informatyki	2128d152-daca-4808-9d42-a...	Zabezpieczenia	Zsynchronizowano

Aby aplikacja mogła uwierzytelniać użytkowników za pomocą usługi AAD, należy ją w tej usłudze zarejestrować. W wyniku rejestracji w usłudze tworzone są dwa elementy: obiekt aplikacji i nazwa główna.

Aby zarejestrować aplikację, kliknij w widoku usługi AAD opcję Rejestracje aplikacji, a potem ikonę Rejestrowanie nowej aplikacji. Następnie w widoku, który się pojawi, podaj nazwę aplikacji, jej typ (Interfejs API/aplikacja internetowa lub Natywne) oraz adres URL strony logowania (w tym przykładzie jest to <https://localhost>) (zobacz pierwszy rysunek na następnej stronie).

Po zdefiniowaniu aplikacji należy ją skonfigurować. Pierwszy widok, który się pojawi po zarejestrowaniu, zawiera dwie bardzo ważne informacje: identyfikatory aplikacji i obiektu. Dane te wykorzystuje aplikacja do uwierzytelniania użytkowników za pomocą usługi AAD. Najpierw za pomocą identyfikatora łączy się z usługą, a następnie sprawdza, czy dany użytkownik jest uprawniony do korzystania z tej aplikacji. W tym procesie, w zależności od wybranej metody uwierzytelniania, wykorzystywany jest identyfikator aplikacji lub obiektu. Oto przykładowy widok zarejestrowanej aplikacji (zobacz drugi rysunek na następnej stronie)

Tworzenie

Nazwa * ⓘ

MojaAplikacja

Typ aplikacji ⓘ

Interfejs API/aplikacja internetowa

Adres URL logowania * ⓘ

https://localhost/

Utwórz

MojaAplikacja

Zarejestrowana aplikacja

Ustawienia

Manifest

Usuń

Nazwa wyświetlana
MojaAplikacja

Identyfikator aplikacji
07b3f104-4b9d-40d1-bf89-59c2e0924192

Typ aplikacji
Interfejs API/aplikacja internetowa

Identyfikator obiektu
f0b32a5f-6097-46f4-a30f-b900a410cbe6

Strona główna
https://localhost/

Aplikacja zarządzana w katalogu lokalnym
MojaAplikacja

Aby udostępnić aplikację użytkownikom, należy zdefiniować uprawnienia i klucze. W tym celu w widoku aplikacji kliknij ikonę Ustawienia, a następnie opcję Wymagane uprawnienia. Uprawnienia należy definiować uważnie, aby nie były zbyt szerokie.

Spotkałem wielu administratorów, którzy przydzielali wszelkie możliwe uprawnienia aplikacjom wymagającym jedynie podstawowego uwierzytelniania użytkowników. Jeżeli uprawnienia są zbyt szerokie, aplikacja jest podatna na ataki hakerskie. Oto przykładowy widok uprawnień:

Ustawienia

Ustawienia filtra

Ogólne

Właściwości

Adresy URL odpowiedzi

Właściciele

Dostęp do interfejsu API

Wymagane uprawnienia

Klucze

Rozwiązywanie problemów i pomoc tech...

Rozwiązywanie problemów

Nowy wniosek o pomoc technic...

Wymagane uprawnienia

Dodaj
Udziel uprawnień

API

Uprawnienia apl...

Delegowane up...

Windows Azure Active Directory (Microsoft.Azur...

0

1

Ostatnią czynnością jest utworzenie klucza, którego aplikacja razem z identyfikatorem będzie używać do uwierzytelniania użytkowników za pomocą usługi AAD. Aby utworzyć nowy klucz, kliknij opcję Klucze, a następnie podaj opis klucza, jego czas trwania (nieobowiązkowy) i wartość. W ustawieniu Czas trwania można wybrać 1 rok, 2 lata lub Nigdy nie wygasa. Zdecydowanie odradzam stosowanie ostatniej opcji, ponieważ stanowi ona potencjalną lukę w bezpieczeństwie aplikacji. Pole Wartość nie zawiera właściwego klucza, lecz ciąg, który po zaszyfrowaniu jest używany jako klucz.

Opis	Wygasa	Wartość
NowyKlucz	Czas trwania	HasłoDoKlucza
Opis klucza	Czas trwania	Wartość zostanie wyświetlona podczas zapisywania

Klucze prywatne

Odcisk palca

Data początkowa

Wygasa

Brak wyników.

Po kliknięciu ikony Zapisz pojawi się właściwy klucz. Skopiuj go i zapisz w bezpiecznym miejscu, ponieważ po zamknięciu widoku nie będziesz już mógł pobrać jego wartości. Oto utworzony przykładowy klucz (zwróć uwagę na wyświetlany komunikat):

Opis	Wygasa	Wartość
NowyKlucz	31.01.2021	Q5npPyS6JtMvVPWne77lvYeC9XfmNILMjith2V3vvY=
Opis klucza	Czas trwania	Wartość zostanie wyświetlona podczas zapisywania

Klucze prywatne

Odcisk palca

Data początkowa

Wygasa

Brak wyników.

Aplikacja do komunikowania się z usługą AAD wykorzystuje identyfikatory i klucz. Aplikacja nie musi być wdrożona w chmurze Azure. Równie dobrze może działać w lokalnej infrastrukturze lub chmurze innego operatora.

Należy pamiętać, że w przypadku aplikacji internetowych wdrożonych w chmurze Azure można podobną funkcjonalność uzyskać za pomocą opcji Uwierzytelnianie/autoryzacja dostępnej w widoku aplikacji. Opcja ta automatycznie tworzy wszystkie niezbędne obiekty, identyfikator i klucz. Ponadto przydziela aplikacji minimalne uprawnienia, co jest dobrym rozwiązaniem. Jeżeli potrzebne są szersze uprawnienia, można je nadać ręcznie.

Jak już wspominałem, podczas rejestrowania aplikacji tworzone są obiekt aplikacji i nazwa główna usługi. Teraz jest dobry moment, aby przedstawić ideę wielopodmiotowości. Aplikacje wielopodmiotowe umożliwiają użytkownikom z różnych podmiotów korzystanie ze wspólnych usług i zasobów. Na przykład można aplikację wdrożyć w ramach własnej subskrypcji (i własnego podmiotu), a następnie udostępnić ją innym podmiotom, w których użytkownicy mogą być uwierzytelniani za pomocą osobnych usług AAD. W ten sposób użytkownicy z różnych podmiotów mogą korzystać z tej samej aplikacji i tych samych zasobów. Wielopodmiotowa aplikacja ma jeden obiekt w podmiocie macierzystym i kilka nazw głównych — po jednej dla każdego katalogu. Między aplikacją a obiektem istnieje relacja „jeden do jednego”, natomiast między aplikacją a nazwami głównymi relacja „jeden do wielu”.

Wspominałem wcześniej o mechanizmie RBAC i jego zastosowaniach do zarządzania zasobami chmurowymi i ich utrzymywania. Mechanizm ten można wykorzystywać w usłudze AAD do definiowania różnych ról i poziomów uprawnień w ramach podmiotu. W widoku usługi AAD można określić uprawnienia administratora danego podmiotu, które nie są nigdzie przenoszone. W ramach jednego podmiotu można zarządzać wieloma subskrypcjami, a każda subskrypcja może obejmować wiele zasobów.

Przypisanie użytkownikowi roli na poziomie subskrypcji powoduje automatyczne nadanie mu odpowiednich uprawnień do wszystkich grup zasobów objętych daną subskrypcją. Przypisanie roli na poziomie grupy zasobów powoduje nadanie uprawnień do wszystkich zasobów w danej grupie. Ponadto można przypisywać uprawnienia do pojedynczych zasobów.

Do przypisywania uprawnień na wszystkich powyższych poziomach (subskrypcji, grupy zasobów i zasobu) służy ta sama opcja: Kontrola dostępu (IAM). Po jej kliknięciu można wybrać rolę, typ przypisania roli oraz użytkownika, grupę użytkowników lub nazwę główną usługi. Oto przykład przypisania roli Współautor grupie użytkowników Departament Informatyki (zobacz pierwszy rysunek na następnej stronie).

Można wybierać predefiniowane role i tworzyć własne. Każdemu użytkownikowi można przypisać kilka ról. W przypadku konfliktu stosowana jest rola, której uprawnienia są najszersze. Na przykład rola Czytelnik umożliwia jedynie odczytywanie informacji o zasobach. Jeżeli zostanie przypisana użytkownikowi wraz z rolą Współautor umożliwiającą modyfikowanie zasobów, ta ostatnia będzie rolą obowiązującą. Oto lista dostępnych ról.

Jak już wspomniałem, grupom użytkowników można przypisywać role na różnych poziomach. Wszyscy użytkownicy należący do danej grupy automatycznie dziedziczą jej rolę.

Nazwy główne usług są często wykorzystywane do udzielania użytkownikom dostępu do aplikacji, które coś tworzą lub zmieniają. Na przykład zespołom programistów często udziela się dostępu do subskrypcji w celu wdrożenia aplikacji oraz tworzenia i zmieniania niezbędnych zasobów.

Usługa Azure Active Directory pozwala identyfikować i uwierzytelniać użytkowników. Użyta wraz z mechanizmem RBAC, umożliwia kontrolowanie, co kto robi, gdzie i kiedy. Są to podstawowe narzędzia do zarządzania zasobami chmurowymi i ich zabezpieczania.

W następnym rozdziale dowiesz się, co jeszcze jest potrzebne, aby czuć się bezpiecznie w chmurze Azure, oraz jak chronić dane i zasoby. Ochrona infrastruktury w chmurze wygląda inaczej niż w środowisku lokalnym i wymaga innego podejścia.