Active Directory i chmura

Synchronizacja z Entra ID i przejście z GPO do Intune.

- Entra Connect i Cloud Sync: synchronizacja ad.zielona.example z Entra ID
- Intune obok domeny: audyt GPO i plan migracji

Entra Connect i Cloud Sync: synchronizacja ad.zielona.example z Entra ID

Poziom: średnio

Dotyczy: Microsoft Entra Connect Sync 2.6 na sync01, Microsoft Entra Cloud Sync, Active Directory ad.zielona.example, Microsoft Entra ID

Czas: ~30 min

Konta z Active Directory trafiają do chmury Microsoftu przez synchronizację, a od niej zależą poczta, Intune i logowanie do Microsoft 365. Plan wdrożenia, licencje i ustawienia instalatora opisuje książka Intune; ta strona wyjaśnia, jak synchronizacja działa od strony katalogu: co synchronizujemy, jak wybieramy sposób logowania, jak dbamy o `sync01` i co zmieniło się w Cloud Sync w 2026 roku. Wracamy tu przy zmianie struktury OU, przy aktualizacji `sync01` i przy pytaniu, czy Cloud Sync wystarczy.

Skróty użyte na tej stronie (10)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
ITIL	Information Technology Infrastructure Library: zbiór dobrych praktyk zarządzania usługami IT, dziś rozwijany przez PeopleCert; wersja 4 od 2019, wersja 5 od 2026
OU	Organizational Unit: folder w Active Directory grupujący konta i komputery
PHS	Password Hash Synchronization: synchronizacja skrótów haseł z Active Directory do Entra ID w postaci przetworzonej jeszcze raz, dzięki której logowanie do chmury działa bez serwerów w firmie
PRT	Primary Refresh Token: token wydawany komputerowi dołączonemu do Entra ID przy logowaniu, dzięki któremu użytkownik loguje się jednokrotnie do usług chmurowych

Skrót	Co znaczy
PTA	Pass-through Authentication: uwierzytelnianie przekazywane, w którym Entra ID oddaje sprawdzenie hasła agentowi na serwerze w firmie
SCP	Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym
SSO	Single Sign-On: jedno logowanie do wielu systemów
UPN	User Principal Name: login w formie adresu, np. jan.nowak@zielona.example

Fiszka

Komendy z modułu `ADSync` wykonujemy w PowerShellu uruchomionym jako administrator na `sync01`; moduł instaluje się razem z Entra Connect Sync. Ścieżki kreatora podajemy po angielsku, tak jak w programie. Harmonogram i wymuszenie synchronizacji różnicowej (`Get-ADSyncScheduler`, `Start-ADSyncSyncCycle -PolicyType Delta`) są na stronie Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy.

□□ ZMIENIA SYSTEM

Wstrzymanie synchronizacji przed pracami: Set-ADSyncScheduler -SyncCycleEnabled

```
Set-ADSyncScheduler -SyncCycleEnabled $false
```

Przed zmianą struktury OU, masowym importem kont albo aktualizacją `sync01` zatrzymujemy harmonogram, żeby cykl nie wysłał do chmury stanu w połowie prac. Po pracach włączamy go wartością `$true` i sprawdzamy `Get-ADSyncScheduler`.

□□ **OU** = Organizational Unit: folder w Active Directory grupujący konta i komputery

□□ TYLKO ODCZYT

Stan bieżącego przebiegu: Get-ADSyncConnectorRunStatus

```
Get-ADSyncConnectorRunStatus
```

Pusty wynik oznacza, że żaden łącznik właśnie nie pracuje i można bezpiecznie zmieniać konfigurację albo restartować serwer.

Przykład w trakcie cyklu:

```
ConnectorIdentifier                  RunState
-------------------                  --------
b891884f-051e-4a83-95af-2544101c9083 Busy
```

◫◫ TYLKO ODCZYT

Sprawdzenie automatycznej aktualizacji: Get-ADSyncAutoUpgrade

```
Get-ADSyncAutoUpgrade
```

Przykład:

```
Enabled
```

Wartość `Enabled` oznacza, że Microsoft może sam zaktualizować `sync01` do nowej wersji. `Suspended` pojawia się po zmianach, przy których automatyczna aktualizacja nie jest bezpieczna (na przykład własne reguły synchronizacji); wtedy aktualizujemy ręcznie.

◫◫ TYLKO ODCZYT

Odczyt wersji Entra Connect Sync: miiserver.exe

```
(Get-Item "C:\Program Files\Microsoft Azure AD
Sync\Bin\miiserver.exe").VersionInfo.FileVersion
```

> (ścieżka domyślnej instalacji; przy innej lokalizacji wersję czytamy w Panelu sterowania, Programy i funkcje)

Przykład:

```
2.6.92.0
```

◫◫ **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie

◫◫ TYLKO ODCZYT

Filtrowanie jednostek organizacyjnych: kreator Entra Connect

```
Microsoft Entra Connect na sync01 → Configure
→ Customize synchronization options → Next
→ logowanie kontem Hybrid Identity Administrator w Entra ID
→ Domain and OU filtering
→ Sync selected domains and OUs
→ zaznaczamy: Uzytkownicy, Komputery, Grupy
→ odznaczamy: Serwery, Konta uslugowe, Wylaczone, Administracja, Domain Controllers
→ Next → Configure
```

Po zmianie filtra kreator sam uruchamia pełny import i synchronizację. Obiekty, które wypadły z zakresu, zostaną w Entra ID usunięte (konta trafią do kosza Entra ID na 30 dni), więc przed odznaczeniem jednostki sprawdzamy, czy nikt z niej nie korzysta z poczty.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: kreator Entra Connect na `sync01`, ekran Domain and OU filtering, rozwinięte drzewo `ad.zielona.example` z zaznaczonymi jednostkami Uzytkownicy, Komputery i Grupy oraz odznaczonymi Serwery, Konta uslugowe, Wylaczone i Administracja.

OU = Organizational Unit: folder w Active Directory grupujący konta i komputery

TYLKO ODCZYT

Zmiana sposobu logowania: Change user sign-in

```
Microsoft Entra Connect na sync01 → Configure
→ Change user sign-in → Next
→ logowanie kontem Hybrid Identity Administrator
→ Password Hash Synchronization (zaznaczone)
→ Enable single sign-on: nie zaznaczamy (patrz sekcja o Seamless SSO)
→ Next → Configure
```

W tym samym oknie wybiera się uwierzytelnianie przekazywane (Pass-through authentication) i federację. Porównanie i wybór Zielonej są niżej.

TYLKO ODCZYT

Kotwica źródłowa konta: Get-ADUser mS-DS-ConsistencyGuid

```
Get-ADUser -Identity nazwa_usera -Properties mS-DS-ConsistencyGuid, objectGUID | Select-Object SamAccountName, objectGUID, mS-DS-ConsistencyGuid
```

Entra Connect zapisuje w tym atrybucie trwały identyfikator, po którym łączy konto w AD z kontem w Entra ID. Puste pole u zsynchronizowanego konta oznacza starą instalację z kotwicą `objectGUID`, co utrudni przeniesienie konta do innego lasu albo odbudowę `sync01`.

AD = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie

Z życia wzięte

Z ŻYCIA WZIĘTE

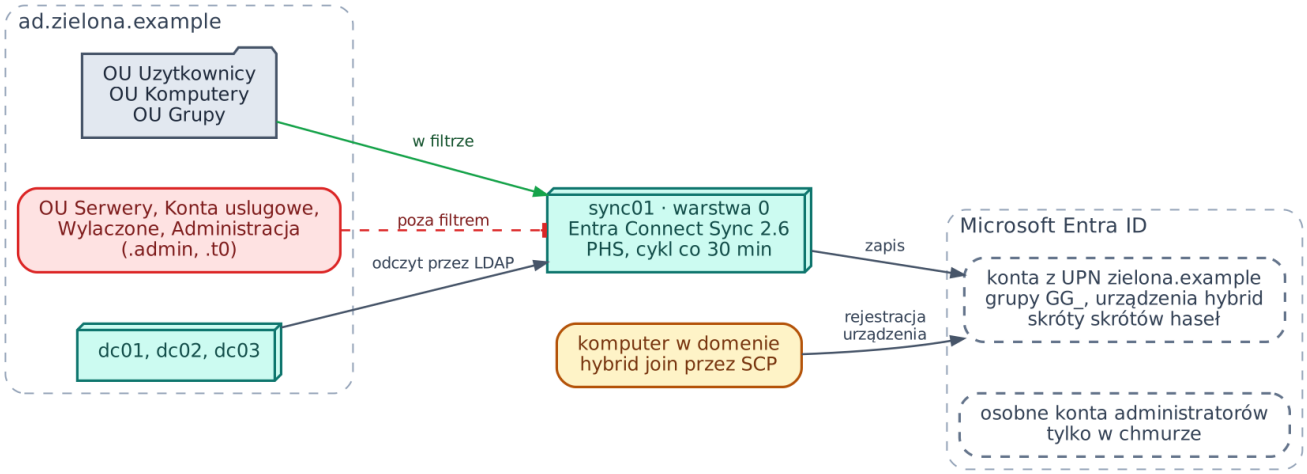
Piątek, 15:40. Tomek porządkuje jednostki organizacyjne i przenosi konta handlowców z `OU=Uzytkownicy` do nowej jednostki `OU=Handlowcy` poza drzewem użytkowników. Kwadrans później Kasia dzwoni z hotelu, że Outlook prosi o hasło i go nie przyjmuje: nowa jednostka nie była zaznaczona w filtrze Entra Connect, więc przy najbliższym cyklu pięciu handlowców zostało usuniętych z Entra ID. Konta wracają z kosza Entra ID po dopisaniu jednostki do filtra i ręcznym cyklu, ale od tego dnia zmiana struktury OU zaczyna się od `Set-ADSyncScheduler -SyncCycleEnabled $false`.

Jak to działa

Rozwiń: jak to działa pod spodem

Co i dokąd płynie

> **Pojęcie: synchronizacja tożsamości.** Program regularnie czyta wybrane obiekty z Active Directory (użytkowników, grupy, komputery) i zapisuje je w Entra ID. Źródłem prawdy zostaje AD: konto zsynchronizowane zmieniamy w AD, a zmiana trafia do chmury przy najbliższym cyklu, domyślnie co 30 minut.



Rysunek 1. Synchronizacja w Zielonej: sync01 czyta z kontrolerów jednostki Uzytkownicy, Komputery i Grupy, pomija serwery, konta usługowe i konta administracyjne, zapisuje do Entra ID konta z UPN zielona.example i skróty skrótów haseł, a komputery domenowe dołączają do Entra ID przez SCP (kliknięcie otwiera pełny rozmiar)

Co	Synchronizujemy	Dlaczego
konta pracowników w `OU=Uzytkownicy`	tak	poczta, Intune, Microsoft 365
komputery w `OU=Komputery`	tak	hybrid join, opis na stronie Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot
grupy `GG_` w `OU=Grupy`	tak	licencje i przypisania w Intune
serwery, konta usługowe, konta wyłączone	nie	nie logują się do chmury, a każdy obiekt w chmurze to dodatkowa powierzchnia ataku
konta administracyjne `.admin` i `.t0`	nie, nigdy	konto uprzywilejowane w AD nie może mieć tożsamości w chmurze, którą da się przejąć osobno; administratorzy Entra ID mają osobne konta tylko w chmurze
wbudowane konta i grupy chronione	nie	Entra Connect i tak pomija część z nich, a reszty nie zaznaczamy

Pojęcie: kotwica źródłowa (source anchor). Niezmienny identyfikator, po którym synchronizacja wie, że konto w chmurze to to samo konto co w AD. W nowych instalacjach jest nim `mS-DS-ConsistencyGuid`, wypełniany wartością `objectGUID`.

> Dopasowanie po kotwicy nazywa się twardym (hard match), a po adresie poczty albo UPN miękkim (soft match); to drugie ma znaczenie tylko przy pierwszym połączeniu istniejących kont chmurowych z kontami z AD.

Jak użytkownik loguje się do chmury: PHS, PTA, federacja

> **Pojęcie: synchronizacja skrótów haseł (PHS, Password Hash Synchronization).** Entra Connect wysyła do Entra ID nie hasło i nie sam skrót z AD, tylko skrót przetworzony jeszcze raz funkcją z solą i wieloma powtórzeniami. Logowanie do chmury sprawdza się w chmurze, bez udziału serwerów w firmie.

> **Pojęcie: uwierzytelnianie przekazywane (PTA, Pass-through Authentication).** Hasło nie opuszcza firmy jako skrót: Entra ID przekazuje próbę logowania agentowi na serwerze w firmie, a ten sprawdza hasło w AD. Gdy agenty albo kontrolery nie działają, nikt nie zaloguje się do chmury.

Cecha	PHS	PTA	Federacja (AD FS)
gdzie sprawdzane jest hasło	w Entra ID	w AD, przez agenta w firmie	na serwerach AD FS w firmie
logowanie do chmury przy awarii łącza albo serwerowni Zielonej	działa	nie działa	nie działa
dodatkowe serwery w firmie	żadne poza `sync01`	co najmniej dwa agenty, warstwa 0	farma AD FS i serwery proxy, warstwa 0
wykrywanie wycieku poświadczeń w Entra ID	tak (funkcja wymaga Entra ID P2, którego Business Premium nie ma)	nie	nie
wyłączenie konta w AD działa w chmurze	po najbliższym cyklu, do 30 minut (pilne zmiany przyspieszamy ręcznym cyklem)	od razu	od razu
dla Zielonej	wybieramy	nie	nie

Zielona wybiera PHS. Decyduje to, że Entra ID przy PHS działa także wtedy, gdy w Pamiątkowie padnie prąd albo łącze, a handlowcy w terenie dalej czytają pocztę. PHS jest też rezerwą przy

PTA i federacji, więc i tak warto go mieć. Słabą stroną PHS jest opóźnienie wyłączenia konta: przy odejściu pracownika procedura z książki ITIL kończy się ręcznym cyklem `Start-ADSyncSyncCycle -PolicyType Delta` i unieważnieniem sesji w Entra ID.

> **Pojęcie: Seamless SSO.** Dodatek, w którym komputer domenowy loguje użytkownika do chmury biletem Kerberos, bez wpisywania hasła, przez specjalne konto komputera `AZUREADSSOACC` w AD. Według dokumentacji Microsoftu komputery Windows 10 i 11 dołączone hybrydowo do Entra ID mają logowanie jednokrotne z tokenu PRT i Seamless SSO nie potrzebują. Zielona rejestruje komputery jako hybrid joined, więc Seamless SSO nie włączamy; gdyby kiedyś było potrzebne, klucz konta `AZUREADSSOACC` trzeba regularnie zmieniać według dokumentacji, a samo konto należy do warstwy 0.

sync01: serwer z kluczami do obu światów

Entra Connect Sync ma konto w AD z prawem odczytu wszystkich synchronizowanych obiektów i, przy PHS, z prawami replikacji skrótów haseł z domeny, a do tego konto w Entra ID z prawem zapisu katalogu. Kto przejmie `sync01`, może odczytać skróty haseł z AD i zmieniać konta w chmurze, dlatego serwer jest w warstwie 0 razem z kontrolerami (Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt).

Sprawa	Ustawienie w Zielonej
kto się loguje na `sync01`	tylko konta `.t0` z osobnej stacji administracyjnej
kopia	kopia całej maszyny w repozytorium `maszyny` i eksport konfiguracji do pliku (kreator: View or export current configuration); odtworzenie to zwykle nowa instalacja z importem konfiguracji
uwierzytelnianie do Entra ID	aplikacyjne (domyślne w nowych instalacjach od wersji 2.5.76.0); serwery zainstalowane wcześniej przełączamy kreatorem, bo od wersji 2.6.84.0 nie robi się to już samo
aktualizacje	automatyczne, a co kwartał sprawdzamy wersję z fiszki z historią wersji
serwer zapasowy w trybie przejściowym (staging)	do rozważenia: druga instalacja, która czyta i liczy, ale nie zapisuje do chmury, gotowa do przełączenia w kilka minut; nazwy i adresu nie nadajemy, decyzja autora

Stan wersji, który sprawdziliśmy w historii wersji Microsoftu (odczyt 19 października 2026): najnowsza wersja to 2.6.92.0 z 23 września 2026. Wersje 2.x wygasają 12 miesięcy po wydaniu nowszej, wszystkie wersje 1.x nie działają, a serwery starsze niż 2.5.79.0 przestały synchronizować 30 września 2026. Strona o planie wdrożenia Intune wspomina wymóg wersji 2.6.84.0 do 7 kwietnia 2027; w samej historii wersji takiej daty nie znaleźliśmy, ale wersja 2.6.84.0 ma tam koniec wsparcia 16 września 2027, więc praktyczny wniosek jest ten sam: na `sync01` trzymamy najnowszą wersję.

Cloud Sync: co zmieniło się w 2026 roku

> **Pojęcie: Microsoft Entra Cloud Sync.** Synchronizacja, w której w firmie działa tylko lekki agent (może stać na kontrolerze domeny), a konfiguracja i logika są w chmurze. Kilka agentów na różnych serwerach daje wysoką dostępność bez trybu przejściowego.

Gdy powstawała strona o planie wdrożenia Intune, Cloud Sync nie synchronizował obiektów komputerów, więc nie nadawał się do hybrid join. Według przewodnika decyzyjnego Microsoftu zaktualizowanego 6 października 2026 obie usługi obsługują już synchronizację urządzeń dla hybrid join, a w Cloud Sync włącza się ją osobno (agent w wersji 1.1.1107 lub nowszej, punkt połączenia usługi ustawiany skryptem z uprawnieniami Enterprise Admins). Kopia tej samej strony w serwisie docs.azure.cn wciąż oznacza funkcję jako wersję zapoznawczą, więc status sprawdzamy przed decyzją.

Cecha (według przewodnika z 6.10.2026)	Entra Connect Sync	Cloud Sync
gdzie działa logika	na `sync01`	w chmurze, w firmie agent
synchronizacja urządzeń do hybrid join	tak	tak, włączana osobno (status do potwierdzenia)
konfiguracja PTA i federacji w tym samym narzędziu	tak	nie, osobno
zaawansowane reguły synchronizacji	tak	prostsze wyrażenia
zapis zwrotny urządzeń	tak	nie, Microsoft wskazuje Cloud Kerberos Trust
limit obiektów w domenie i wielkość grup	bez limitu obiektów, grupy do 250 000 członków	150 000 obiektów, grupy do 50 000 członków
dla Zielonej	zostaje na `sync01`	ocena przy następnej dużej zmianie `sync01`

Dla 180 osób oba narzędzia są wystarczające. Zostajemy przy Entra Connect Sync, bo działa, ma skonfigurowany hybrid join i nie potrzebuje decyzji w środku wdrożenia Intune. Przejście na

Cloud Sync rozważymy przy wymianie `sync01` na Windows Server 2025, kiedy przewodnik migracji i status synchronizacji urządzeń będą pewne. Jedno narzędzie nie może synchronizować tych samych obiektów co drugie, więc ewentualne przejście robimy jednostka po jednostce, według przewodnika pilotażu Microsoftu.

Częste błędy

Objaw	Przyczyna	Co robimy
Po przeniesieniu kont do nowej jednostki znikają z Entra ID	nowa jednostka poza filtrem OU	dopisujemy jednostkę w kreatorze, cykl ręczny, konta wracają z kosza Entra ID (do 30 dni)
Konto ma w chmurze nazwę `nazwa@domena.onmicrosoft.com`	UPN w AD z sufiksem `ad.zielona.example`, który nie jest zweryfikowany w Microsoft 365	sufiks UPN `zielona.example` dla konta, opis na stronie o planie Intune
Wyłączony w AD pracownik czyta pocztę jeszcze pół godziny	PHS i cykl co 30 minut	w procedurze odejścia ręczny cykl i unieważnienie sesji w Entra ID
Zmiana w AD nie dochodzi do chmury od kilku dni	harmonogram zatrzymany po pracach i nie włączony	`Get-ADSyncScheduler`, potem `Set-ADSyncScheduler -SyncCycleEnabled $true`
`Get-ADSyncAutoUpgrade` pokazuje `Suspended`	zmiany w konfiguracji blokujące automatyczną aktualizację	aktualizacja ręczna z najnowszego instalatora, potem ponowne sprawdzenie
Konto administratora AD ma w chmurze tę samą tożsamość z prawami	konto uprzywilejowane w synchronizowanej jednostce	przenosimy konta `.admin` i `.t0` do jednostki `Administracja` poza filtrem, a role w Entra ID dajemy kontom tylko chmurowym
Po odbudowie `sync01` powstają w chmurze duplikaty kont	stara instalacja z kotwicą `objectGUID`, nowa z `mS-DS-ConsistencyGuid` bez wcześniejszego wypełnienia	przed odbudową eksport konfiguracji i ta sama kotwica w nowej instalacji

□□ Ćwiczenia

1. Dlaczego konta `.t0` nie mogą być synchronizowane do Entra ID, skoro i tak mają mocne hasła?

Odpowiedź

Bo tożsamość w chmurze to druga droga do tego samego konta: przejęcie jej w Entra ID (wyłudzenie, błąd w dostępie warunkowym) albo przejęcie AD przez zmianę w chmurze rozmywa granicę warstwy 0. Konta uprzywilejowane w AD zostają tylko w AD, a role administracyjne w Entra ID dostają osobne konta tylko chmurowe.

1. Pan Zbigniew pyta, czy przy PHS Microsoft zna nasze hasła. Co odpowiadamy?

Odpowiedź

Nie zna haseł ani skrótów w postaci z AD. Entra Connect przetwarza skrót z AD jeszcze raz jednokierunkową funkcją z solą i wieloma powtórzeniami i dopiero ten wynik wysyła. Z tego nie da się odtworzyć hasła ani zalogować się nim do AD.

1. Kiedy wybralibyśmy PTA zamiast PHS?

Odpowiedź

Gdyby firma miała zasadę, że żadna pochodna hasła nie może opuścić serwerowni, albo gdyby natychmiastowe działanie wyłączenia konta i godzin logowania z AD było ważniejsze niż logowanie do chmury przy awarii w Pamiątkowie. Zielona tak nie ma, a ceną PTA byłyby dwa agenty w warstwie 0 i zależność poczty od serwerowni.

1. Czy możemy dziś włączyć Cloud Sync obok Entra Connect, żeby go przetestować?

Odpowiedź

Tylko na obiektach, których Entra Connect nie synchronizuje, na przykład na testowej jednostce wyłączonej z filtra na `sync01`, według przewodnika pilotażu Microsoftu. Dwa narzędzia synchronizujące te same obiekty dają konflikty i duplikaty. Test robimy poza zakazem zmian i z planem wycofania w GLPI.

Powiązane: Plan wdrożenia Intune w Zielonej: licencje, Entra Connect, fazy · Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot · Intune obok domeny: audyt GPO i plan migracji · Struktura OU Zielonej i delegowanie uprawnień · Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt · Skrypty audytowe Active Directory

Źródła: (odczyt 19.10.2026) · Microsoft Learn, „Microsoft Entra Connect: Version release history” (2.6.92.0 z 23.09.2026, koniec wsparcia wersji 2.x po 12 miesiącach od nowszej, przerwanie synchronizacji dla wersji starszych niż 2.5.79.0 od 30.09.2026, uwierzytelnianie aplikacyjne domyślne od 2.5.76.0, brak automatycznego przełączania od 2.6.84.0) · Microsoft Learn, „Migrate

from Microsoft Entra Connect to Cloud Sync: Decision Guide” (aktualizacja 6.10.2026: synchronizacja urządzeń w obu narzędziach, brak PTA i federacji w Cloud Sync, limity 150 000 obiektów i 50 000 członków grupy) · Microsoft Learn, „Configure device sync with Microsoft Entra Cloud Sync” (29.09.2026, agent 1.1.1107 lub nowszy) i docs.azure.cn, ta sama strona z oznaczeniem „preview” · Microsoft Learn, „Microsoft Entra Connect Sync: Configure filtering”, „Password hash synchronization”, „Pass-through authentication”, „Seamless single sign-on: frequently asked questions”, „Design concepts: sourceAnchor (ms-DS-ConsistencyGuid)”, „Staging server and disaster recovery”, „Automatic upgrade” (`Get-ADSyncAutoUpgrade`), „Scheduler” (`Set-ADSyncScheduler`) · Microsoft Learn, „Securing privileged access: separate cloud-only administrator accounts”

Intune obok domeny: audyt GPO i plan migracji

Poziom: zaawansowany
Dotyczy: Microsoft Entra ID, Intune, Active Directory na dc01/dc02 **Czas: ~40 min**

Domena Active Directory i Intune przez jakiś czas rządzą tymi samymi komputerami naraz, zanim zdecydujemy, co zostaje po staremu, a co przechodzi do chmury. Audytujemy istniejące GPO politykę po polityce i układamy plan migracji w falach, zamiast przenosić wszystko naraz.

Skróty użyte na tej stronie (8)

Skrót	Co znaczy
BYOD	Bring Your Own Device: pracownik używa prywatnego urządzenia do pracy
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
HTML	HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce
MDM	Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi
PKI	Public Key Infrastructure: infrastruktura klucza publicznego, czyli urząd certyfikacji razem z całym mechanizmem wydawania i odwoływania certyfikatów
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
Wi-Fi	Sieć bezprzewodowa: wygodna w biurze, ale w serwerowni dokłada kolejną możliwą przyczynę awarii
XML	eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

Fiszka

KLIKAMY W INTERFEJSIE

Objęcie istniejącego komputera Intune bez reinstalacji: hybrid join i GPO

```
dc01: Group Policy Management → GPO dla jednostki z komputerami pilotażu
→ Computer Configuration → Administrative Templates → Windows Components → MDM
→ Enable automatic MDM enrollment using default Microsoft Entra credentials → Enabled
→ poświadczenia: User Credential
```

Komputer zostaje w domenie `ad.zielona.example` dokładnie tak jak wcześniej. Entra Connect przenosi jego obiekt do Microsoft Entra ID (hybrid join), a GPO każe mu samemu zapisać się do Intune. To droga bez reinstalacji z pełnym zarządzaniem. Szczegóły i warunki (licencja, zakres MDM, synchronizacja) opisuje strona Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot.

> Samo „Połącz” w Ustawienia → Konta → Uzyskaj dostęp do pracy lub szkoły na komputerze firmowym robi z niego urządzenie `Entra registered`. Ta droga jest przewidziana dla prywatnych urządzeń (BYOD) i nie daje pełnego zarządzania komputerem przez Intune, więc w Zielonej nie używamy jej dla floty.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **MDM** = Mobile Device Management: system zdalnego zarządzania telefonami i tabletami firmowymi · **BYOD** = Bring Your Own Device: pracownik używa prywatnego urządzenia do pracy

TYLKO ODCZYT

Sprawdzenie stanu rejestracji na komputerze

```
dsregcmd /status
```

Po hybrid join wiersze `AzureAdJoined` i `DomainJoined` mówią `YES`. Sam wiersz `WorkplaceJoined : YES` przy `AzureAdJoined : NO` oznacza rejestrację `Entra registered`, czyli drogę dla prywatnych urządzeń, a nie to, czego chcemy na komputerze firmowym. Sprawdzamy to polecenie zaraz po zmianie, zamiast zakładać, że przeszła poprawnie.

dsregcmd = Device Registration Command: pokaż, czy komputer jest dołączony do Entra ID, domeny albo zarejestrowany, i zdiagnozuj rejestrację

TYLKO ODCZYT

Eksport wszystkich GPO do audytu

```
Get-GPOReport -All -ReportType Html -Path C:\Audyty\wszystkie-gpo.html
```

Jeden raport HTML ze wszystkimi politykami w domenie, do przeczytania i przedyskutowania z zespołem, zanim zdecydujemy, co z każdą polityką robimy. Wariant zapisujący każde GPO do osobnego pliku XML, wygodny do dalszego przeszukiwania automatem, opisaliśmy już na stronie Skrypty audytowe Active Directory.

GPO = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **HTML** = HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce · **XML** = eXtensible Markup Language: format tekstowy do zapisu ustrukturyzowanych danych w znacznikach, tutaj używany przez PowerShell do zapisu zrzutu obiektów poleceniem Export-Clixml

Z życia wzięte

Z ŻYCIA WZIĘTE

Prezes, pan Zbigniew, wraca z urlopu z nowym laptopem kupionym w sklepie i pyta, kiedy będzie mógł na nim pracować. Wcześniej odpowiedź brzmiałaby: za dwa dni, po dojechaniu do serwerowni w Pamiątkowie i dołączeniu do domeny kablem. Teraz Tomek wysyła mu link do rejestracji konta pracy, pan Zbigniew loguje się sam z hotelu, a polityki Intune same dokładają Defendera i VPN, zanim laptop w ogóle zobaczy sieć biurową.

Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: Microsoft Entra ID. Chmurowy katalog tożsamości Microsoftu, następca nazwy Azure Active Directory. Osobny byt od domenowego Active Directory na `dc01`/`dc02`: konta, urządzenia i polityki mogą tam istnieć niezależnie od domeny, choć da się je też ze sobą zsynchronizować.

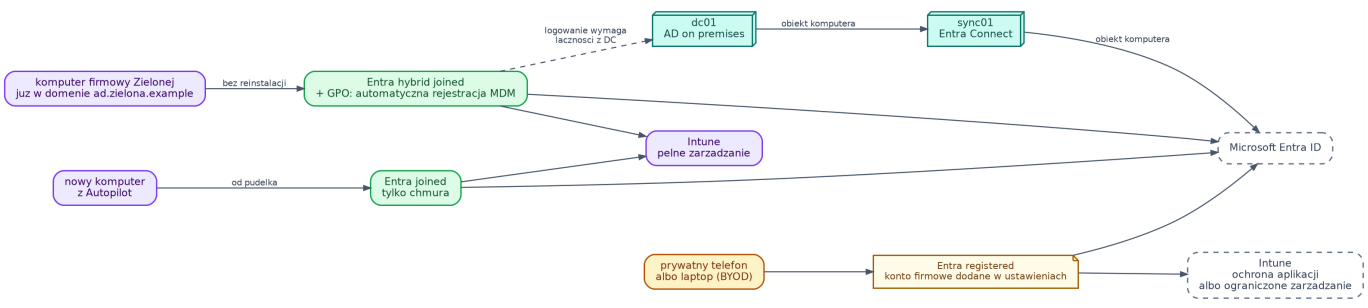
Pojęcie: Intune. Chmurowa platforma do zarządzania urządzeniami, oparta na Microsoft Entra ID zamiast na GPO: instaluje aplikacje, wymusza szyfrowanie i hasła, i

pilnuje zgodności komputera z polityką bezpieczeństwa, niezależnie od tego, czy komputer ma akurat łączność z siecią firmową, czy siedzi w hotelu na drugim końcu świata.

Pojęcie: Microsoft Defender. Wbudowany w Windows pakiet ochrony przed złośliwym oprogramowaniem, którego pełną konfigurację (skanowanie, ochronę przed manipulacją, reguły redukcji powierzchni ataku) da się scentralizować przez Intune tak samo, jak wcześniej przez GPO.

Pojęcie: Entra registered kontra Entra joined kontra hybrid joined. Trzy różne sposoby, w jaki komputer wiąże się z Microsoft Entra ID, i każdy inny stopień zależności od domeny:

Tryb	Co się dzieje	Wymaga reinstalacji istniejącego PC	Zależność od `dc01` / `dc02`
Entra registered	urządzenie (zwykle prywatne) dostaje tożsamość w Entra ID po dodaniu konta firmowego; droga dla BYOD, bez pełnego zarządzania komputerem	nie	brak
Entra hybrid joined	komputer jest jednocześnie w domenie i w pełni rozpoznany w Entra ID, zwykle przez synchronizację Entra Connect	zwykle nie, o ile już jest w domenie	tak, logowanie i część operacji wymaga łączności z kontrolerem domeny
Entra joined	komputer należy tylko do Entra ID, bez powiązania z domeną on premises	tak, istniejący komputer dołączony do domeny wymaga zresetowania Windowsa	brak

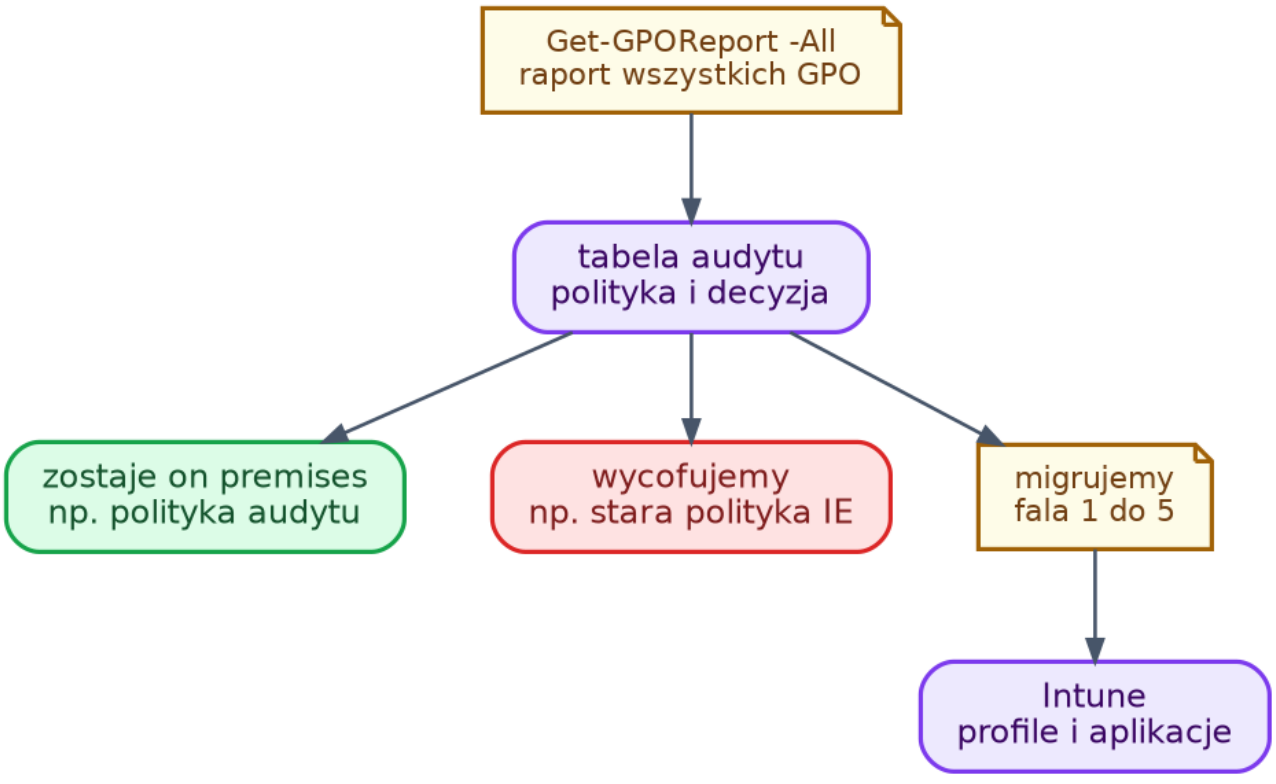


Rysunek. Trzy drogi do Entra ID: firmowy komputer w domenie przechodzi na hybrid join z automatyczną rejestracją MDM bez reinstalacji, nowy komputer dołącza do Entra ID przez Autopilot, a prywatne urządzenie jest tylko zarejestrowane i nie dostaje pełnego zarządzania (kliknięcie otwiera pełny rozmiar)

W Zielonej wybieramy `hybrid joined` z automatyczną rejestracją MDM przez GPO dla istniejącej floty: nie wymaga resetowania 180 komputerów naraz i daje pełne zarządzanie przez Intune. `Entra joined` (najlepiej przez Autopilot) zostaje wyborem dla nowych komputerów kupowanych od tej pory. `Entra registered` zostawiamy dla prywatnych telefonów i laptopów pracowników. Wcześniejsza wersja tej strony zalecała `Entra registered` dla floty; to była pomyłka, bo ta droga nie obejmuje komputera pełnym zarządzaniem.

Audyt GPO: metoda

Zamiast zgadywać, które z kilkudziesięciu GPO w domenie wciąż mają sens, przechodzimy przez pełny raport `Get-GPOReport -All` i każdą politykę przypisujemy do jednej z trzech grup, z uzasadnieniem, nie tylko z etykietą.



Raport wszystkich GPO trafia do tabeli audytu, z ktorej kazda polityka idzie do jednej z trzech decyzji (kliknięcie otwiera pełny rozmiar)

Polityka	Co robi	Decyzja	Dlaczego
Polityka haseł domeny	wymusza długość i złożoność hasła dla kont domenowych	zostaje on premises	konta domenowe i logowanie Kerberos wciąż istnieją, dopóki istnieje domena
Polityka audytu bezpieczeństwa	włącza logowanie zdarzeń logowania i zmian w AD	zostaje on premises	dotyczy samej domeny, nie stacji roboczych, Intune tego nie zastąpi
Instalacja oprogramowania (GPO Software Installation)	instaluje pakiety MSI przy starcie komputera z udziału sieciowego	migrujemy, fala 1	zależy od łączności z domeną przy każdym starcie, w Intune aplikacja instaluje się też poza siecią firmową
Stara polityka konfiguracji Internet Explorera	ustawia strony startowe i zabezpieczenia przeglądarki wycofanej z Windowsa	wycofujemy, fala 1	przeglądarka, której polityka dotyczy, już nie istnieje w obsługiwanych wersjach Windows
Autorejestracja certyfikatów użytkownika	prosi urząd certyfikacji `CA-Zielona` o certyfikat przy każdym logowaniu	migrujemy, fala 2	wymaga łączności z `dc01`, a komputery poza biurem łączą się przez zawodny VPN
Mapowanie dysków sieciowych działów	podłącza litery dysków do udziałów na `fs01`	migrujemy, fala 4	odtwarzalne skryptem logowania z Intune, ale nie jest pilne jak aplikacje i certyfikaty
Konfiguracja proxy przeglądarki	wymusza adres serwera proxy w ustawieniach systemowych	migrujemy, fala 3	prosty profil konfiguracyjny w Intune, korzyść z przeniesienia bez większego ryzyka

> Po przenosinach urzędu według strony Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona nowe certyfikaty wystawia `Zielona-CA01` na `ca01`, więc wszędzie, gdzie dziś ufamy tylko `CA-Zielona`, dokładamy zaufanie do `Zielona-Root-CA`.

Dlaczego instalacja aplikacji i autorejestracja certyfikatów schodzą z GPO najpierw

Obie polityki mają wspólną cechę: działają tylko wtedy, gdy komputer ma w danej chwili łączność z domeną, a nasz `AlwaysOn VPN` nie działa dziś niezawodnie na całej flocie. Komputer offline nie dostanie aktualizacji oprogramowania z GPO ani nie odnowi certyfikatu przy wygaśnięciu, i będzie tak działać do najbliższego podłączenia do sieci biurowej, czasem tygodniami. Intune instaluje aplikacje i odnawia certyfikaty przez internet, niezależnie od tego, czy komputer widzi akurat kontroler domeny, więc te dwie polityki idą do migracji w pierwszej kolejności, zanim zajmiemy się mniej pilnymi.

Plan migracji w pięciu falach

1. **Fala 1: aplikacje i porządki.** Migracja instalacji oprogramowania do Intune, usunięcie przestarzałej polityki Internet Explorera.
2. **Fala 2: certyfikaty.** Wybór między Certificate Connector a Cloud PKI (porównanie niżej) i migracja autorejestracji certyfikatów użytkownika.
3. **Fala 3: konfiguracja podstawowa.** Proxy, Wi-Fi, ustawienia przeglądarki i inne proste profile konfiguracyjne bez zależności od domeny.
4. **Fala 4: zasoby działowe.** Mapowanie dysków sieciowych, drukarki, skrypty logowania przeniesione na skrypty Intune uruchamiane przy logowaniu.
5. **Fala 5: zabezpieczenia i sprzątanie.** Migracja polityk Defendera i BitLockera do profili bezpieczeństwa punktu końcowego Intune, wyłączenie w pełni zmigrowanych GPO i końcowy przegląd tego, co świadomie zostaje on premises na stałe.

Certificate Connector kontra Cloud PKI

Kryterium	Certificate Connector	Cloud PKI
Gdzie działa urząd certyfikacji	on premises, dziś `AD CS` na `dc01`	w pełni w chmurze Microsoftu
Wymagana infrastruktura on premises	tak: serwer `NDES` plus zainstalowany łącznik Certificate Connector, oba z łącznością wychodzącą do Intune	żadna: bez serwera łącznika i bez własnego `AD CS`
Wykorzystuje istniejący urząd `CA-Zielona`	tak, to jego główna zaleta w Zielonej	nie, wymaga nowej hierarchii CA założonej w Intune

Kryterium	Certificate Connector	Cloud PKI
Zależność od łączności komputera z domeną przy odnawianiu	pośrednio tak: łącznik i `NDES` muszą widzieć `dc01`, choć sam klient łączy się przez SCEP z Intune	nie, cały przepływ certyfikatu idzie przez chmurę
Typowe zastosowanie	firmy z już działającym `AD CS`, które nie chcą budować nowego CA	wdrożenia od zera albo urządzenia bez żadnej łączności z siecią on premises

W Zielonej `AD CS` na `dc01` już działa i wydaje certyfikaty od lat, więc Certificate Connector pozwala odzyskać autorejestrację certyfikatów bez budowania nowego urzędu. Cloud PKI staje się bardziej naturalnym wyborem, gdyby docelowo domena on premises miała zniknąć całkiem, a nie tylko stracić część swoich dotychczasowych zadań: ta decyzja w Zielonej pozostaje otwarta do czasu zamknięcia fali 2.

Częste błędy

Objaw	Przyczyna	Co robimy
`dsregcmd /status` pokazuje `WorkplaceJoined : YES` i `AzureAdJoined : NO`, a komputer nie dostaje profili Intune	ktoś zrobił „Połącz” w ustawieniach konta, więc komputer jest tylko `Entra registered`, a hybrid join jeszcze nie przeszedł	usuwamy konto szkolne lub służbowe z ustawień, sprawdzamy synchronizację obiektu komputera w Entra Connect i GPO z automatyczną rejestracją MDM
Autorejestracja certyfikatów przestaje działać zaraz po pierwszej migracji z GPO	GPO wyłączone, zanim profil certyfikatu w Intune faktycznie doszedł do komputera	wyłączamy politykę GPO dopiero po potwierdzeniu, że nowy certyfikat z Intune faktycznie jest na komputerze
Audyt GPO trwa bardzo długo, bo trzeba ręcznie przeklikać dziesiątki polityk w konsoli	audyt liczony politykę po polityce w interfejsie graficznym zamiast masowym raportem	uruchamiamy `Get-GPOReport -All -ReportType Html` raz i czytamy jeden plik zamiast klikać po konsoli
Komputer po rejestracji w Entra ID prosi o dodatkowe logowanie przy każdym uruchomieniu aplikacji firmowej	użytkownik zalogował się do aplikacji lokalnym kontem Microsoft zamiast kontem pracy dodanym przy rejestracji	sprawdzamy w aplikacji, czy używane jest konto `imie.nazwisko@zielona.example`, nie prywatne konto Microsoft

□□ Ćwiczenia

1. Dlaczego w Zielonej wybieramy `hybrid joined` z GPO dla istniejącej floty 180 komputerów, a nie `Entra registered` ani od razu `Entra joined`?

Odpowiedź

`Entra joined` na komputerze, który już jest dołączony do domeny on premises, wymaga wyjścia z domeny i zwykle resetu Windowsa: przy 180 komputerach naraz to masowa, ryzykowna operacja. `Entra registered` jest drogą dla prywatnych urządzeń i nie daje pełnego zarządzania komputerem. `Hybrid joined` z automatyczną rejestracją MDM zostawia komputer w domenie i obejmuje go Intune bez reinstalacji, a `Entra joined` zostaje wyborem dla nowych komputerów.

1. Polityka mapowania dysków sieciowych trafia w naszym audycie do fali 4, a nie do fali 1 razem z instalacją oprogramowania. Jakim kryterium z tej strony to uzasadniamy?

Odpowiedź

Fala 1 obejmuje polityki, które zależą od stałej łączności z domeną i realnie psują się na komputerach korzystających głównie z zawodnego VPN, czyli instalację oprogramowania i autorejestrację certyfikatów. Mapowanie dysków sieciowych też korzysta z łączności domenowej, ale nie jest tak pilne: brak dostępu do udziału sieciowego jest od razu widoczny dla użytkownika i łatwy do obejścia ręcznie, więc migrujemy je później, gdy pilniejsze polityki są już bezpiecznie po drugiej stronie.

Powiązane: Windows LAPS: hasło lokalnego administratora w Active Directory · Entra Connect i Cloud Sync: synchronizacja ad.zielona.example z Entra ID · Skrypty audytowe Active Directory

Źródła: Microsoft Learn, „Join your cloud native endpoints to Microsoft Entra" · Microsoft Learn, „What is a Microsoft Entra hybrid joined device" · Microsoft Learn, „How Microsoft Entra device registration works" · Microsoft Learn, „Microsoft Cloud PKI for Microsoft Intune" · Microsoft Learn, „Types of certificate that are supported by Microsoft Intune" · `Get-Help Get-GPOReport`