Wnioski o usługę, katalog usług i onboarding: od nowego konta do odebrania dostępu

Poziom: podstawy

Dotyczy: Active Directory ad.zielona.example, GLPI, PostgreSQL na pg01, MailCow, Vaultwarden, kontrola dostępu kd01

Czas: ~40 min

Strona opisuje, co użytkownik może zamówić w IT (katalog usług Zielonej), jak przechodzi wniosek od formularza do zamknięcia, i jak przyjmujemy oraz żegnamy pracownika według listy kontrolnej. Odpowiada też na pytanie, które pan Wojtek zadaje co roku: czy osoby, które odeszły, nadal mają dostęp. Wracamy tu przy każdym nowym pracowniku, każdym odejściu i każdej prośbie o dostęp „na chwilę”.

Skróty użyte na tej stronie (15)

Skrót	Co znaczy
AGDLP	Account, Global, Domain Local, Permission: skrócona nazwa modelu zagnieżdżania grup w Active Directory, od kont przez grupy globalne i lokalne w domenie aż do faktycznego uprawnienia
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
ITIL	Information Technology Infrastructure Library: zbiór dobrych praktyk zarządzania usługami IT, dziś rozwijany przez PeopleCert; wersja 4 od 2019, wersja 5 od 2026
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)

Skrót	Co znaczy
LDAPS	LDAP szyfrowany TLS, zwykle port 636
MSSQL	Microsoft SQL Server: silnik bazy danych Microsoftu, na nim w Zielonej stoi księgowość Optima
OU	Organizational Unit: folder w Active Directory grupujący konta i komputery
RSAT	Remote Server Administration Tools: dodatkowe narzędzia administracyjne Windows do zarządzania AD, DNS i GPO ze stacji roboczej
SQL	Structured Query Language: język zapytań do relacyjnych baz danych
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
SSL	Secure Sockets Layer: dawna nazwa szyfrowania, dziś formalnie TLS
TGT	Ticket Granting Ticket: główny bilet Kerberos wydawany przez kontroler domeny po zalogowaniu, na jego podstawie komputer dostaje bilety do konkretnych usług
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Fiszka

Komendy PowerShell wykonujemy na stacji administratora z modułem ActiveDirectory (RSAT) albo na `dc01`, kontem administratora z prawami do jednostki `Uzytkownicy`. Komendy SQL wykonujemy w `psql` na `pg01` kontem właściciela bazy.

□□ KLIKAMY W INTERFEJSIE

Złożenie wniosku z katalogu: Assistance → Service catalog

```
pomoc.zielona.example → Assistance → Service catalog → kafelek usługi → formularz → Submit
```

Użytkownik wybiera usługę z kafelków, wypełnia formularz i dostaje numer wniosku. Formularz od razu pyta o to, czego potrzebujemy do realizacji, więc nie musimy dopytywać mailem.

□□ ZMIENIA SYSTEM

Utworzenie konta nowego pracownika: New-ADUser

```
$Haslo = Read-Host -AsSecureString "Hasło startowe"
New-ADUser -Name "Imię Nazwisko" -GivenName "Imię" -Surname "Nazwisko" -SamAccountName
"nazwa_usera" -UserPrincipalName "nazwa_usera@ad.zielona.example" -Path
"OU=NazwaDzialu,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example" -Department "NazwaDzialu" -
Title "Stanowisko" -Manager "nazwa_przelozonego" -AccountPassword $Haslo -
ChangePasswordAtLogon $true -Enabled $true
```

> (gdzie `OU=NazwaDzialu` to jednostka działu, np. `OU=Biuro`, a `nazwa_przelozonego` to login przełożonego, który zatwierdza dostęp)

Hasło startowe przekazujemy osobno od loginu, najlepiej osobiście pierwszego dnia. Pole przełożonego wypełniamy zawsze, bo z niego korzysta lista kontrolna offboardingu i raport dla audytora.

Przykład sprawdzenia po utworzeniu:

```
PS> Get-ADUser magda.lis -Properties Department, Manager, Enabled | Select-Object
SamAccountName, Department, Manager, Enabled


SamAccountName Department
Manager                                                              Enabled
-------------- ----------  -------
                                                                     -------
magda.lis      Ksiegowosc  CN=Halina
Kowalska,OU=Biuro,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example    True
```

OU = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

ZMIENIA SYSTEM

Dodanie do grupy działu: Add-ADGroupMember

```
Add-ADGroupMember -Identity "GG_NazwaDzialu" -Members "nazwa_usera"
```

Dostęp do udziałów nadajemy przez grupy globalne działów (`GG_Ksiegowosc`), które są członkami grup lokalnych z uprawnieniem (`DL_Ksiegowosc_RW`), zgodnie z modelem AGDLP. Użytkownika nigdy nie dopisujemy bezpośrednio do listy uprawnień folderu.

AGDLP = Account, Global, Domain Local, Permission: skrócona nazwa modelu zagnieżdżania grup w Active Directory, od kont przez grupy globalne i lokalne w domenie aż do faktycznego uprawnienia

TYLKO ODCZYT

Sprawdzenie poziomu funkcjonalnego lasu: Get-ADForest

```
(Get-ADForest).ForestMode
```

Członkostwo czasowe w grupach wymaga funkcji Privileged Access Management, a ta wymaga poziomu funkcjonalnego lasu Windows Server 2016 albo wyższego. Wynik `Windows2016Forest` (albo nowszy) oznacza, że las spełnia warunek.

Przykład:

```
PS> (Get-ADForest).ForestMode
Windows2016Forest
```

OSTROŻNIE · NIEODWRACALNE

Włączenie Privileged Access Management w lesie: Enable-ADOptionalFeature

```
Enable-ADOptionalFeature 'Privileged Access Management Feature' -Scope
ForestOrConfigurationSet -Target "NazwaLasu"
```

> (gdzie `NazwaLasu` to nazwa lasu Active Directory, w Zielonej `ad.zielona.example`)

Włączenia tej funkcji nie da się cofnąć: specyfikacja Active Directory mówi wprost, że po włączeniu nie można jej wyłączyć, a funkcja obejmuje cały las. W Zielonej jest już włączona (decyzja autora z 11 października 2026), więc tej komendy nie uruchamiamy ponownie; zostaje na stronie jako zapis tego, co zrobiono, i na wypadek odtwarzania lasu w laboratorium.

TYLKO ODCZYT

Sprawdzenie, czy funkcja jest włączona: Get-ADOptionalFeature

```
Get-ADOptionalFeature -Filter "Name -eq 'Privileged Access Management Feature'" |
Select-Object Name, EnabledScopes
```

Niepusta kolumna `EnabledScopes` oznacza, że funkcja działa i `-MemberTimeToLive` można używać. Pusta oznacza, że ktoś odtworzył las bez tej funkcji, a członkostwo czasowe zwróci błąd.

◫◫ ZMIENIA SYSTEM

Dodanie do grupy na określony czas: Add-ADGroupMember -MemberTimeToLive

```
Add-ADGroupMember -Identity "GG_NazwaGrupy" -Members "nazwa_usera" -MemberTimeToLive
(New-TimeSpan -Days 7)
```

> (gdzie `GG_NazwaGrupy` to grupa dostępu do zasobu, np. `GG_Baza_Cennik_RO` dla odczytu bazy `cennik`)

Standardowa ścieżka wniosku KU-05 „dostęp na chwilę”: członkostwo samo znika po upływie czasu, bez pamiętania o tym przez administratora. Czas ustawiamy zgodnie z wnioskiem, najwyżej 14 dni.

◫◫ TYLKO ODCZYT

Sprawdzenie pozostałego czasu członkostwa: Get-ADGroup -ShowMemberTimeToLive

```
Get-ADGroup "GG_NazwaGrupy" -Property member -ShowMemberTimeToLive | Select-Object -
ExpandProperty member
```

Pokazuje członków grupy razem z czasem życia członkostwa. Według wpisu zespołu Active Directory w Microsofcie członkowie czasowi mają przed nazwą wyróżniony dopisek z liczbą sekund do wygaśnięcia; członkowie stali są wypisani bez niego.

◫◫ ZMIENIA SYSTEM

Dostęp czasowy bez konta domenowego: CREATE ROLE z VALID UNTIL

```
CREATE ROLE nazwa_usera_tymczasowy LOGIN PASSWORD 'HasloTymczasowe' VALID UNTIL 'RRRR-MM-DD 16:00';
GRANT CONNECT ON DATABASE NazwaBazy TO nazwa_usera_tymczasowy;
GRANT USAGE ON SCHEMA public TO nazwa_usera_tymczasowy;
GRANT SELECT ON ALL TABLES IN SCHEMA public TO nazwa_usera_tymczasowy;
```

> (gdzie `NazwaBazy` to baza, np. `cennik`; `VALID UNTIL` unieważnia hasło roli w podanym momencie)

Droga zapasowa, gdy osoba nie ma konta w domenie (na przykład konsultant dostawcy) albo baza nie sprawdza grup z Active Directory. `VALID UNTIL` dotyczy tylko logowania hasłem, więc do tego zawsze przypomnienie w GLPI.

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

TYLKO ODCZYT

Zapisanie członkostwa w grupach przed odejściem: Get-ADPrincipalGroupMembership

```
Get-ADPrincipalGroupMembership -Identity "nazwa_usera" | Select-Object -ExpandProperty Name | Out-File "C:\IT\Offboarding\nazwa_usera-grupy.txt"
```

Listę grup zapisujemy i dołączamy do zgłoszenia offboardingu, zanim cokolwiek usuniemy. Bez niej nie odtworzymy dostępu, gdy okaże się, że pracownik wraca albo że jego zastępca potrzebuje tych samych praw.

IT = Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

ZMIENIA SYSTEM

Wyłączenie konta przy odejściu: Disable-ADAccount

```
Disable-ADAccount -Identity "nazwa_usera"
Set-ADUser -Identity "nazwa_usera" -Description "Wylaczone RRRR-MM-DD, zgloszenie
```

```
NumerZgloszenia"
Move-ADObject -Identity (Get-ADUser "nazwa_usera").DistinguishedName -TargetPath
"OU=Wylaczone,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example"
```

Konto wyłączamy, opisujemy numerem zgłoszenia i przenosimy do jednostki kont wyłączonych, a nie kasujemy od razu. Jednostka `OU=Wylaczone` jest częścią standardu Zielonej, a tworzy się ją tak jak inne jednostki na stronie o strukturze OU.

OU = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

OSTROŻNIE · NIEODWRACALNE

Usunięcie z grup po zapisaniu listy: Remove-ADGroupMember

```
Get-ADPrincipalGroupMembership -Identity "nazwa_usera" | Where-Object Name -ne "Domain
Users" | ForEach-Object { Remove-ADGroupMember -Identity $_ -Members "nazwa_usera" -
Confirm:$false }
```

Odbiera wszystkie członkostwa poza grupą podstawową. Wykonujemy dopiero po zapisaniu listy grup z poprzedniej karty.

TYLKO ODCZYT

Raport dla audytora: Search-ADAccount

```
Search-ADAccount -AccountDisabled -UsersOnly | Select-Object SamAccountName,
LastLogonDate, DistinguishedName
Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00 -UsersOnly | Where-Object
Enabled | Select-Object SamAccountName, LastLogonDate
```

Pierwsze polecenie pokazuje konta wyłączone, drugie konta włączone, ale nieużywane od 90 dni. Drugą listę porównujemy z listą pracowników z kadr: każde włączone konto spoza listy to sprawa do wyjaśnienia.

Przykład:

```
SamAccountName LastLogonDate
-------------- -------------
jan.nowak      2026-06-30 15:42:10
```

```
skaner.test    2026-03-02 06:01:44
```

Z życia wzięte

Z ŻYCIA WZIĘTE

Poniedziałek, 9:30, coroczny audyt. Pan Wojtek kładzie na stole listę dwunastu osób, które odeszły z Zielonej w ciągu roku, i prosi o dowód, że żadna z nich nie ma już dostępu. Tomek uruchamia `Search-ADAccount` i widzi, że jedenaście kont jest wyłączonych, a konto `jan.nowak`, handlowca, który odszedł w czerwcu, nadal jest włączone: kadry wysłały informację mailem do starszego administratora, który był wtedy na urlopie. Konto było nieużywane, ale VPN i poczta działały przez trzy miesiące. Od tego dnia odejście pracownika jest wnioskiem w katalogu, który zakładają kadry, a nie mailem do konkretnej osoby.

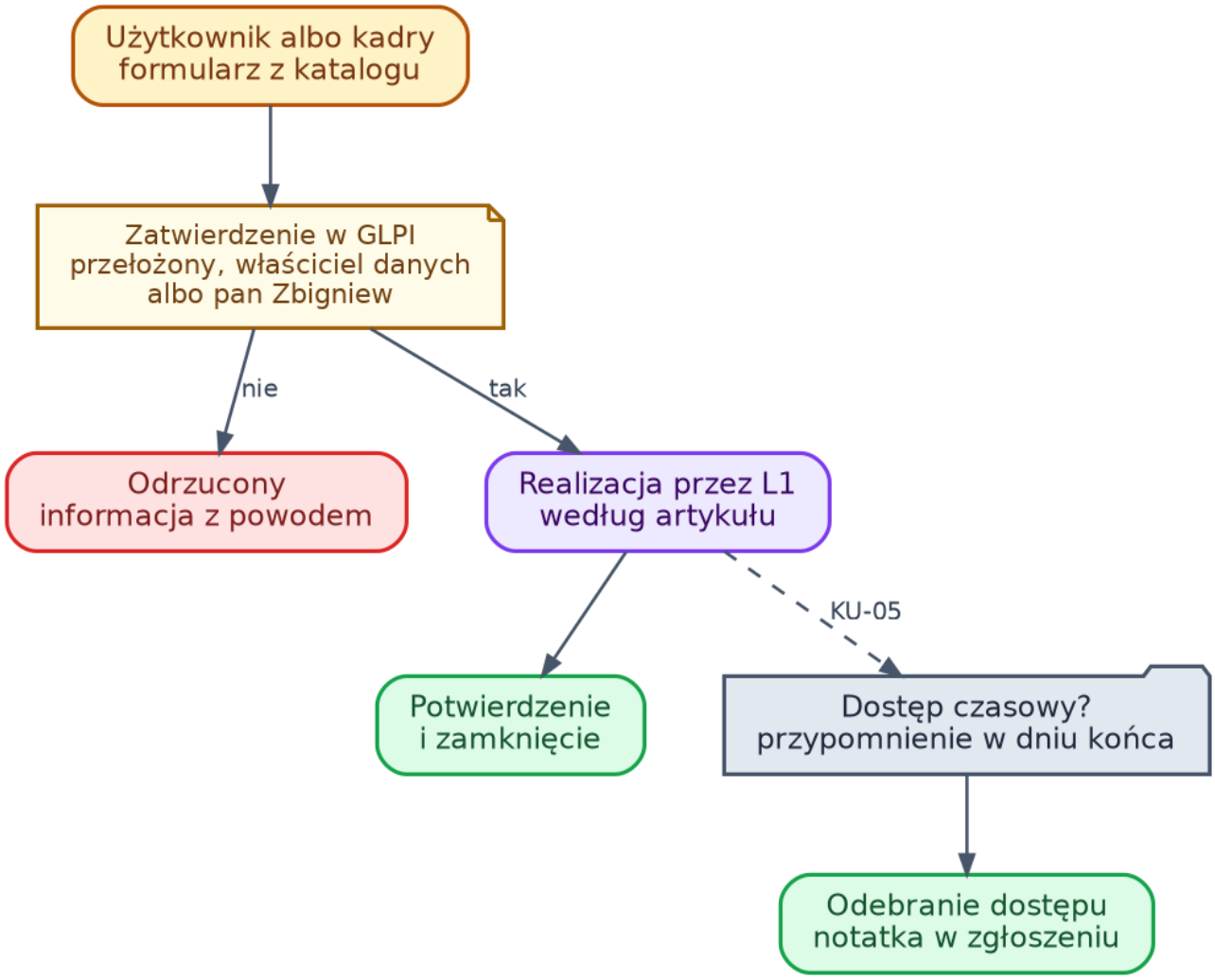
Jak to działa

Rozwiń: jak to działa pod spodem

Wniosek o usługę

> **Pojęcie: obsługa wniosków o usługę.** Praktyka, której celem jest sprawna realizacja umówionych próśb użytkowników: nowych kont, dostępów, sprzętu, informacji [1]. Wniosek różni się od incydentu tym, że nic się nie zepsuło; różni się od zmiany tym, że jego przebieg jest z góry znany i zatwierdzony.

Każdy wniosek przechodzi tę samą drogę: formularz z katalogu, zatwierdzenie przez osobę wskazaną w katalogu, realizacja przez L1, potwierdzenie i zamknięcie. Dostęp czasowy ma jeszcze jeden etap: odebranie w dniu końca.



Rysunek 1. Przebieg wniosku w Zielonej: formularz z katalogu, zatwierdzenie, realizacja przez L1, potwierdzenie i zamknięcie, a dla dostępu czasowego przypomnienie i odebranie dostępu w dniu końca (kliknięcie otwiera pełny rozmiar)

Zasady, które obowiązują każdy wniosek:

1. Wniosek zatwierdza osoba, która odpowiada za dane albo koszt (przełożony, właściciel danych, pan Zbigniew), a nie sam wnioskujący i nie administrator.
2. Zatwierdzenie jest w GLPI (przycisk zatwierdzenia albo odpowiedź na mail z GLPI), a nie w rozmowie telefonicznej.
3. Każdy dostęp ma właściciela danych i, jeśli jest czasowy, datę końca.
4. Wnioski powtarzalne realizujemy według artykułu w bazie wiedzy, żeby każdy z nas robił to tak samo.

Katalog usług Zielonej

> **Pojęcie: katalog usług.** Lista tego, co użytkownik może zamówić w IT, z opisem, kto może zamówić, kto zatwierdza i ile to trwa [1]. Katalog chroni obie strony: użytkownik wie, czego się spodziewać, a IT nie wykonuje próśb, których nikt nie zatwierdził.

Katalog usług Zielonej (standard zatwierdzony 11 października 2026):

Kod	Usługa	Kto zamawia	Kto zatwierdza	Czas realizacji	Uwagi
KU-01	Konto nowego pracownika (domena, poczta, GLPI, grupy działu)	kadry	przełożony	gotowe dzień roboczy przed pierwszym dniem pracy	wniosek najpóźniej 5 dni roboczych przed startem
KU-02	Dostęp do udziału na `fs01`	pracownik	właściciel danych (kierownik działu)	1 dzień roboczy	przez grupę `GG_`, nigdy bezpośrednio
KU-03	Laptop albo stanowisko	przełożony	pan Zbigniew (koszt)	2 dni z zapasu IT, 10 dni roboczych przy zakupie	rejestracja w Intune przez Autopilot
KU-04	Dostęp zdalny (VPN)	przełożony	przełożony i IT	1 dzień roboczy	grupa `GG_VPN_Uzytkownicy`, instrukcja z bazy wiedzy
KU-05	Dostęp czasowy do bazy danych	programista	właściciel danych i starszy administrator	1 dzień roboczy	członkostwo czasowe w grupie `GG_Baza_`, domyślnie tylko odczyt, najwyżej 14 dni
KU-06	Reset hasła albo odblokowanie konta	pracownik	bez zatwierdzenia, po potwierdzeniu tożsamości	1 godzina robocza	telefon zwrotny na numer z kadr albo osobiście
KU-07	Skrzynka współdzielona albo lista adresowa	przełożony	przełożony	2 dni robocze	MailCow, właściciel skrzynki wpisany w opisie
KU-08	Instalacja programu z listy dozwolonych	pracownik	bez zatwierdzenia (lista dozwolonych)	2 dni robocze	spoza listy: zmiana z oceną bezpieczeństwa

Kod	Usługa	Kto zamawia	Kto zatwierdza	Czas realizacji	Uwagi
KU-09	Karta dostępu do stref	przełożony	pan Zbigniew dla strefy serwerowni	2 dni robocze	grupy `GG_Dostep_`, kontroler `kd01`
KU-10	Odejście pracownika (offboarding)	kadry	przełożony	w ostatnim dniu pracy o 16:00	lista kontrolna niżej
KU-11	Pytanie albo prośba o informację	każdy	bez zatwierdzenia	2 dni robocze	odpowiedź zwykle linkiem do bazy wiedzy

> □□ Czego nie ma w katalogu, nie jest wnioskiem. Prośba spoza katalogu (nowy program spoza listy, nowa aplikacja, inny sposób działania systemu) jest zmianą i przechodzi ocenę ryzyka.

Dostęp „na chwilę”

Ola raz na kilka tygodni prosi o dostęp do bazy produkcyjnej „tylko na chwilę”, żeby sprawdzić dane po błędzie w aplikacji. To uzasadniona prośba, ale „na chwilę” bez daty końca zamienia się w dostęp na zawsze. Dlatego KU-05 realizujemy członkostwem czasowym w grupie Active Directory, a nie ręcznie nadawanymi prawami:

1. Do każdej bazy, o którą zespół Oli prosi, istnieje grupa dostępu tylko do odczytu, np. `GG_Baza_Cennik_RO`; zapis wymaga osobnej grupy i zgody właściciela danych na piśmie w GLPI.
2. Wniosek zatwierdzają właściciel danych i starszy administrator, a dyżurny dodaje osobę do grupy z `-MemberTimeToLive` na czas z wniosku, najwyżej 14 dni.
3. Członkostwo wygasa samo; usunięcie wygasłego członkostwa kontrolery domeny oceniają od razu, bez czekania na replikację.
4. W dniu końca dyżurny sprawdza `-ShowMemberTimeToLive`, że osoby już nie ma w grupie, i zapisuje to w zgłoszeniu.

Baza `cennik` na `pg01` sprawdza grupę przy każdym logowaniu: PostgreSQL uwierzytelnia hasłem domenowym przez LDAPS na kontrolerze domeny, a filtr wyszukiwania przepuszcza tylko członków grupy. Rola w PostgreSQL o nazwie konta domenowego istnieje na stałe, bez hasła, z prawami tylko do odczytu; bez członkostwa w grupie nie da się na nią zalogować. Wiersz w `pg_hba.conf` (jedna linia):

```
hostssl cennik all 10.20.20.0/24 ldap ldapserver="dc01.ad.zielona.example
dc02.ad.zielona.example" ldapscheme=ldaps ldapbasedn="DC=ad,DC=zielona,DC=example"
```

```
ldapbinddn="CN=svc_pg01_ldap,OU=KontaTechniczne,DC=ad,DC=zielona,DC=example"
ldapbindpasswd="HasloKontaTechnicznego"
ldapsearchfilter="(&(sAMAccountName=$username)(memberOf=CN=GG_Baza_Cennik_RO,OU=Grupy,DC=ad,DC=zielona,DC=example))"
```

> (gdzie `svc_pg01_ldap` to konto techniczne tylko do odczytu katalogu, a jego hasło trzymamy w Vaultwardenie; po zmianie pliku przeładowujemy konfigurację `SELECT pg_reload_conf();`)

Reguła stoi na `hostssl`, a nie `host`, bo hasło domenowe idzie od klienta do `pg01` otwartym tekstem i szyfruje je tylko SSL samego PostgreSQL (`ldapscheme=ldaps` chroni wyłącznie odcinek od `pg01` do kontrolera). W `ldapserver` podajemy oba kontrolery, `dc01` i `dc02`, żeby logowanie działało także wtedy, gdy jeden z nich nie odpowiada, tak jak na stronie Logowanie do PostgreSQL kontem z Active Directory: LDAP, LDAPS i grupy.

Opcje `ldapscheme` i `ldapsearchfilter` opisuje dokumentacja PostgreSQL 16, której wersji używa `pg01`. Tryby LDAP, certyfikat `CA-Zielona`, konto techniczne, role w bazie i filtr dla grup zagnieżdżonych opisuje strona Logowanie do PostgreSQL kontem z Active Directory: LDAP, LDAPS i grupy. Sesja otwarta przed wygaśnięciem członkostwa trwa do rozłączenia, bo PostgreSQL sprawdza grupę tylko przy logowaniu.

> □□ 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`.

Bilety Kerberos. Przy zasobach Windows, które sprawdzają grupy z biletu Kerberos (udziały na `fs01`, MSSQL z logowaniem Windows), wygaśnięcie członkostwa nie czeka na wygaśnięcie biletu. Dokumentacja Microsoftu dla wydanego Windows Server 2016 („What's new in Active Directory Domain Services in Windows Server 2016”) podaje, że kontrolery domeny skracają czas życia biletu TGT do czasu, który został w grupie z członkostwem czasowym, a przy kilku takich grupach do najkrótszego z nich. Wpis zespołu Active Directory z okresu wersji testowej dodaje, że odnowiony bilet nie zawiera już tej grupy. W dniu końca dostępu sprawdzamy czas ważności biletu `klist` na komputerze użytkownika i zapisujemy wynik w zgłoszeniu.

Gdy osoba nie ma konta w domenie, zostaje droga zapasowa z rolą `_tymczasowy` i `VALID UNTIL` z Fiszki, a po terminie usuwamy rolę:

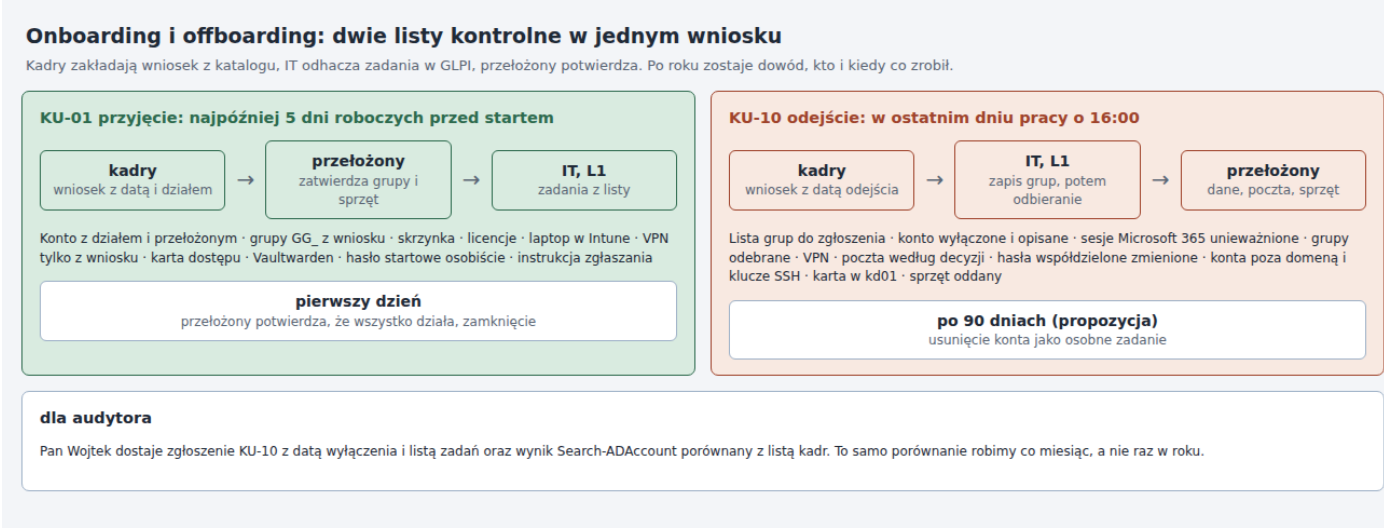
```
DROP ROLE nazwa_usera_tymczasowy;
```

> ⚠ `DROP ROLE` nie zadziała, jeśli rola jest właścicielem obiektów albo ma nadane uprawnienia. Wtedy najpierw `REASSIGN OWNED BY` i `DROP OWNED BY` w każdej bazie, w której rola coś ma, według dokumentacji PostgreSQL.

Onboarding i offboarding

> **Pojęcie: onboarding.** Przyjęcie nowego pracownika od strony IT: konto, sprzęt, dostępy, pierwsze logowanie. **Pojęcie: offboarding.** Odwrotność: odebranie wszystkich dostępów i sprzętu w dniu odejścia, z dowodem dla audytora.

Oba procesy są w Zielonej wnioskami z katalogu (KU-01 i KU-10), które zakładają kadry. Wniosek ma w GLPI zadania z listy kontrolnej, każde z osobnym odhaczeniem, więc rok później da się pokazać, kto i kiedy co zrobił.



Rysunek 2. Onboarding i offboarding jako dwie listy kontrolne w jednym wniosku: kadry zgłaszają, IT realizuje zadania, przełożony potwierdza, a po odejściu zostaje dowód dla audytora (kliknięcie otwiera pełny rozmiar)

Lista kontrolna onboardingu (KU-01):

1. Konto w domenie (`New-ADUser`) z działem, stanowiskiem i przełożonym.
2. Grupy działu `GG_` według wniosku, bez kopiowania grup „jak u koleżanki”.

3. Skrzynka w MailCow (konto z Active Directory) i dopisanie do list działu.
4. Licencje Microsoft 365, jeśli dział ich używa.
5. Laptop zarejestrowany w Intune, przypisany do użytkownika w GLPI.
6. VPN tylko, jeśli wniosek go zawiera (KU-04).
7. Karta dostępu do stref (KU-09).
8. Konto w Vaultwardenie i dopisanie do kolekcji działu, jeśli dział korzysta z haseł współdzielonych.
9. Hasło startowe przekazane osobiście, wymuszona zmiana przy pierwszym logowaniu.
10. Krótka instrukcja: jak zgłaszać sprawy do IT, adres `pomoc.zielona.example`.
11. Potwierdzenie od przełożonego po pierwszym dniu: wszystko działa.

Lista kontrolna offboardingu (KU-10), w ostatnim dniu pracy:

1. Lista grup zapisana (`Get-ADPrincipalGroupMembership`) i dołączona do zgłoszenia.
2. Konto wyłączone (`Disable-ADAccount`), opisane numerem zgłoszenia, przeniesione do `OU=Wylaczone`.
3. Sesje w Microsoft 365 unieważnione i logowanie zablokowane w Entra ID, bez czekania na synchronizację.
4. Członkostwa w grupach odebrane (po zapisaniu listy).
5. VPN: konto poza `GG_VPN_Uzytkownicy`, aktywne sesje rozłączone na `fw01`.
6. Poczta: przekierowanie albo autoodpowiedź według decyzji przełożonego, okres przechowywania skrzynki według polityki.
7. Vaultwarden: usunięcie z organizacji, zmiana haseł współdzielonych, które ta osoba znała.
8. Konta poza domeną: lokalne konta w aplikacjach, konta u dostawców, tokeny API, klucze SSH na serwerach.
9. Karta dostępu zablokowana w `kd01`, karta fizycznie oddana.
10. Sprzęt oddany: laptop, telefon, token; laptop wyczyszczony albo przekazany zgodnie z procedurą Intune.
11. Dane: przełożony wskazał, co z plikami z OneDrive i udziałów.
12. Potwierdzenie przełożonego, zamknięcie zgłoszenia.
13. Po 90 dniach usunięcie konta jako osobne zadanie.

> □□ Raz w miesiącu, w przeglądzie tygodniowym na początku miesiąca, porównujemy `Search-ADAccount -AccountInactive` z listą pracowników od kadr. To ta sama lista, o którą pyta pan Wojtek, tylko zrobiona dwanaście razy w roku, a nie raz. Więcej gotowych zapytań jest na stronie Skrypty audytowe Active Directory.

Częste błędy

Objaw	Przyczyna	Co robimy
Nowy pracownik pierwszego dnia czeka do południa na konto	kadry zgłosiły w dniu przyjścia	KU-01 najpóźniej 5 dni roboczych przed startem, w katalogu i w procedurze kadr
Nowa osoba ma dostęp do wszystkiego, co jej poprzedniczka	konto skopiowane z innego użytkownika	grupy tylko z wniosku, zatwierdzone przez przełożonego
Konto byłego pracownika włączone po pół roku	informacja o odejściu poszła mailem do jednej osoby	offboarding wyłącznie jako wniosek KU-10, comiesięczne porównanie z listą kadr
Dostęp „na chwilę” działa od roku	brak daty końca	członkostwo w grupie z `-MemberTimeToLive`, sprawdzenie w dniu końca `-ShowMemberTimeToLive`
`-MemberTimeToLive` zwraca błąd	las odtworzony bez funkcji Privileged Access Management albo poziom lasu poniżej Windows Server 2016	`Get-ADOptionalFeature` i `(Get-ADForest).ForestMode`; do czasu naprawy droga zapasowa z `VALID UNTIL`
Po odejściu nikt nie zna haseł do kont współdzielonych	hasła znała tylko ta osoba	hasła współdzielone w Vaultwardenie, zmiana po każdym odejściu
Wniosek zrealizowany bez zatwierdzenia	„przecież to tylko udział”	GLPI nie przepuszcza wniosku do realizacji bez zatwierdzenia z katalogu

□□ Ćwiczenia

1. Kadry piszą do Tomka w piątek o 15:30, że od poniedziałku przychodzi nowa księgowa. Co odpowiada Tomek i co robi w poniedziałek o 7:00?

Odpowiedź

Odpowiada uprzejmie, że przyjmuje sprawę, i sam zakłada wniosek KU-01 w imieniu kadr, prosząc panią Halinę o zatwierdzenie grup w GLPI. W poniedziałek o 7:00 tworzy konto z grupami z wniosku, a przy przeglądzie tygodniowym zgłasza kadrom, że wniosek ma przychodzić 5 dni roboczych wcześniej.

1. Ola prosi o dostęp z zapisem do bazy `cennik` na pg01 „na godzinę”, żeby poprawić dane po błędzie importu. Jak realizujemy?

Odpowiedź

Jako KU-05 z zatwierdzeniem właściciela danych i starszego administratora: dodanie Oli do grupy zapisu bazy `cennik` z `-MemberTimeToLive (New-TimeSpan -Hours 8)`, zapis tylko do tabel, których dotyczy poprawka, a w zgłoszeniu zapis, co zmieniono. Po terminie sprawdzenie `-ShowMemberTimeToLive` i notatka o odebraniu dostępu. Jeśli poprawka danych jest częsta, to sygnał do problemu w aplikacji, a nie do stałego dostępu.

1. Pan Wojtek pyta, czy konto `jan.nowak` było używane po odejściu tego pracownika. Skąd bierzemy odpowiedź?

Odpowiedź

`LastLogonDate` z `Search-ADAccount` albo `Get-ADUser` daje przybliżoną datę ostatniego logowania (atrybut replikowany z opóźnieniem do 14 dni), a dokładne logowania znajdujemy w logach kontrolerów domeny w Graylogu, w logach VPN na `fw01` i w logach MailCow. Do audytu dołączamy też zgłoszenie offboardingu z datą wyłączenia.

1. Marek zamawia przez katalog dostęp do udziału księgowości dla magazyniera. Kto zatwierdza?

Odpowiedź

Właściciel danych, czyli kierownik księgowości (pani Halina), a nie Marek ani IT. Marek może złożyć wniosek, ale nie może zatwierdzić dostępu do cudzych danych.

Powiązane: Struktura OU Zielonej i delegowanie uprawnień · Udziały i uprawnienia NTFS na serwerze plików · Skrypty audytowe Active Directory · Rejestracja urządzeń: Entra joined, hybrid, BYOD i Autopilot · GLPI w Zielonej: zgłoszenia, SLA i katalog usług na docker01

Źródła: [1] Parafraza własna na podstawie: AXELOS, „ITIL Foundation, ITIL 4 Edition” (2019), praktyki service request management i service catalogue management. · learn.microsoft.com, dokumentacja `Add-ADGroupMember` (parametr `-MemberTimeToLive`). · learn.microsoft.com, dokumentacja `Get-ADGroup` (parametr `-ShowMemberTimeToLive`). · learn.microsoft.com, archiwum blogu AskDS, „Previewing Server 2016 TP4: Temporary Group Memberships” (składnia `Enable-ADOptionalFeature`, odczyt pozostałego czasu, bilet TGT ograniczony do najkrótszego członkostwa). · learn.microsoft.com, „What's new in Active Directory Domain Services in Windows Server 2016”, sekcja Privileged access management (członkostwo z czasem życia, czas życia TGT równy czasowi pozostałemu w grupie, przy kilku grupach najkrótszemu). · learn.microsoft.com, [MS-ADTS] „Privileged Access Management Optional Feature” (poziom funkcjonalny lasu co najmniej Windows Server 2016, funkcji nie da się wyłączyć, zakres całego lasu). · learn.microsoft.com, „Privileged Access Management for Active Directory Domain Services” (wygasłe członkostwo oceniane od razu

na każdym kontrolerze). · postgresql.org/docs/16, „LDAP Authentication” (`ldapscheme`, `ldapsearchfilter`). · postgresql.org/docs, `CREATE ROLE` (klauzula `VALID UNTIL`) i `DROP ROLE`. · help.glpi-project.org, „Forms” (katalog usług w GLPI 11 i nowszych).

Revision #9
Created 2026-10-11 14:26:55 UTC by Tomasz Konieczny
Updated 2026-10-26 14:25:36 UTC by Tomasz Konieczny