Struktura OU Zielonej i delegowanie uprawnień

Poziom: podstawy **Dotyczy: Active Directory, moduł ActiveDirectory (RSAT)**

Czas: ~35 min

Świeżo założona domena ma jeden folder na wszystko: `Users` i `Computers`, bez podziału na działy ani lokalizacje. Jednostki organizacyjne (OU) porządkują ten bałagan i dają miejsce, do którego linkujemy polityki GPO oraz komu nadajemy tylko wybrane uprawnienia, zamiast pełnych praw administratora domeny.

Skróty użyte na tej stronie (7)

Skrót	Co znaczy
ACL	Access Control List: lista, kto ma jakie prawa do pliku lub zasobu
AD DS	Active Directory Domain Services: rola Windows Server uruchamiająca właściwą usługę katalogową Active Directory na kontrolerze domeny
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
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
SID	w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta

Fiszka

ZMIENIA SYSTEM

Utworzenie jednostki organizacyjnej: New-ADOrganizationalUnit

```
New-ADOrganizationalUnit -Name "NazwaOU" -Path "SciezkaRodzica"
```

Zakłada nową jednostkę organizacyjną pod wskazanym rodzicem. Domyślnie, bez żadnego dodatkowego parametru, nowa jednostka od razu dostaje ochronę przed przypadkowym usunięciem.

Przykład:

```
New-ADOrganizationalUnit -Name "Komputery" -Path "DC=ad,DC=zielona,DC=example"
New-ADOrganizationalUnit -Name "Biuro" -Path "OU=Komputery,DC=ad,DC=zielona,DC=example"
```

◫◫ ZMIENIA SYSTEM

Utworzenie grupy zabezpieczeń: New-ADGroup

```
New-ADGroup -Name "NazwaGrupy" -GroupScope Global -GroupCategory Security -Path
"SciezkaOU"
```

`-GroupScope` decyduje, gdzie grupa może być używana (`Global` w naszym modelu nazewnictwa opisanym niżej), a `-GroupCategory Security` odróżnia grupę zabezpieczeń, która nosi uprawnienia, od grupy dystrybucyjnej, która służy tylko do wysyłki poczty.

Przykład:

```
New-ADGroup -Name "GG_Ksiegowosc" -GroupScope Global -GroupCategory Security -Path
"OU=Grupy,DC=ad,DC=zielona,DC=example"
```

◫◫ ZMIENIA SYSTEM

Utworzenie konta użytkownika: New-ADUser

```
$Haslo = Read-Host -AsSecureString -Prompt "Haslo poczatkowe"

New-ADUser -Name "ImieNazwisko" `
    -SamAccountName "nazwa_usera" `
    -UserPrincipalName "nazwa_usera@NazwaDomeny" `
    -Path "SciezkaOU" `
    -AccountPassword $Haslo `
    -Enabled $true
```

Konto bez podanego hasła powstaje, ale zostaje wyłączone: `-Enabled $true` wymaga, żeby hasło już wcześniej trafiło do polecenia przez `-AccountPassword`, inaczej włączenie się nie

powiedzie mimo utworzenia konta.

Przykład:

```
New-ADUser -Name "Jan Nowak" -SamAccountName "jan.nowak" -UserPrincipalName
"jan.nowak@ad.zielona.example" -Path
"OU=Biuro,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example" -AccountPassword $Haslo -Enabled
$true
```

□□ ZMIENIA SYSTEM

Przeniesienie obiektu do innej jednostki: Move-ADObject

```
Move-ADObject -Identity "DistinguishedNameObiektu" -TargetPath "SciezkaDocelowejOU"
```

Przenosi dowolny obiekt katalogu, komputer, użytkownika albo grupę, do innej jednostki organizacyjnej. Sam obiekt zostaje tym samym obiektem (te same uprawnienia specjalne, ten sam SID), zmienia się tylko jego miejsce w drzewie i w efekcie `DistinguishedName`.

Przykład:

```
Move-ADObject -Identity "CN=RDS01,CN=Computers,DC=ad,DC=zielona,DC=example" -TargetPath
"OU=Serwery,DC=ad,DC=zielona,DC=example"
```

□□ **SID** = w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta

□□ TYLKO ODCZYT

Podgląd istniejących jednostek organizacyjnych: Get-ADOrganizationalUnit

```
Get-ADOrganizationalUnit -Filter * | Format-Table Name, DistinguishedName -AutoSize
```

Przydatne przed dołożeniem kolejnej jednostki albo przed migracją komputerów, żeby zobaczyć całe istniejące drzewo naraz, zamiast klikać po konsoli poziom po poziomie.

Przykład:

```
Name              DistinguishedName
----              -----------------
```

```
Uzytkownicy       OU=Uzytkownicy,DC=ad,DC=zielona,DC=example
Komputery         OU=Komputery,DC=ad,DC=zielona,DC=example
Biuro             OU=Biuro,OU=Komputery,DC=ad,DC=zielona,DC=example
Magazyn           OU=Magazyn,OU=Komputery,DC=ad,DC=zielona,DC=example
```

TYLKO ODCZYT

Delegowanie uprawnień przez kreator: Delegation of Control Wizard

```
Active Directory Users and Computers
→ prawy przycisk na jednostce organizacyjnej (np. OU=Uzytkownicy)
→ Delegate Control...
→ Next
→ Add: wskazujemy grupę, której nadajemy uprawnienia (np. ZIELONA\GG_Kadry)
→ Next
→ Delegate the following common tasks:
   zaznaczone „Reset user passwords and force password change at next logon"
→ Next → Finish
```

Kreator jest bezpieczniejszym wyborem niż ręczne grzebanie w ACL, bo od razu pokazuje gotową listę typowych zadań do zaznaczenia, zamiast żądać znajomości konkretnych uprawnień rozszerzonych z nazwy. Ten sam efekt z poziomu wiersza poleceń, wygodny do powtórzenia skryptem na kilku jednostkach naraz, daje `dsacls`:

```
dsacls "OU=Uzytkownicy,DC=ad,DC=zielona,DC=example" /I:S /G "ZIELONA\GG_Kadry:CA;Reset Password;user"
```

`/I:S` ogranicza nadanie do obiektów potomnych (`Subobjects`), a `CA;Reset Password;user` to konkretne prawo kontrolne (`Control Access`) do resetu hasła, zawężone do obiektów typu `user`. Efekt jest identyczny z tym, co robi kreator, tylko bez klikania.

ACL = Access Control List: lista, kto ma jakie prawa do pliku lub zasobu · **CA** = Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty

Z życia wzięte

Z ŻYCIA WZIĘTE

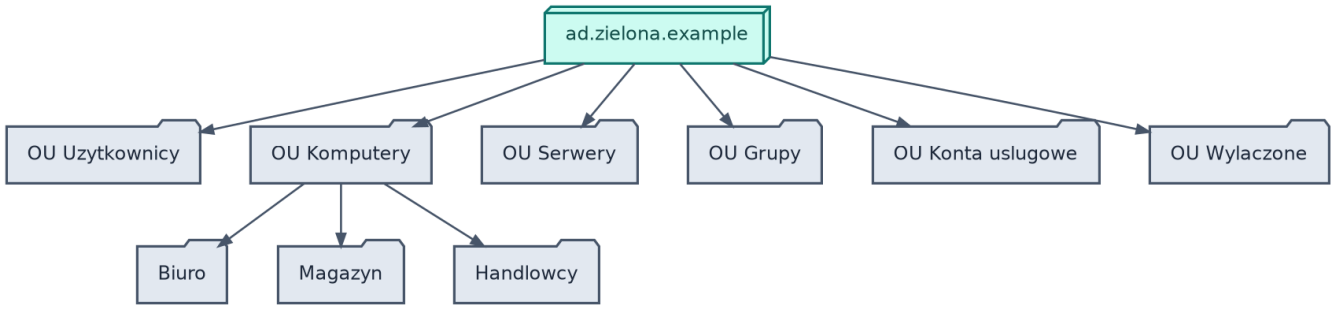
> Pani Halina z kadr od miesięcy dzwoni do Tomka za każdym razem, gdy ktoś z magazynu zapomni hasła, bo hasła może resetować tylko dział IT. Starszy administrator zakłada w końcu grupę `GG_Kadry` i deleguje jej prawo resetu haseł na jednostce `Uzytkownicy`. Od tego dnia pani Halina resetuje hasła sama, z poziomu Active Directory Users and Computers, a Tomek dostaje telefon tylko wtedy, gdy naprawdę coś się zepsuło.

Jak to działa

Rozwiń: jak to działa pod spodem

> **Pojęcie: jednostka organizacyjna (Organizational Unit, OU).** Coś w rodzaju folderu wewnątrz Active Directory, w którym grupujemy konta, komputery i inne obiekty. W odróżnieniu od zwykłego folderu w systemie plików, jednostka organizacyjna może mieć podpięte własne polityki GPO i własne, niezależne od reszty katalogu uprawnienia delegowane konkretnym osobom albo grupom.

Proponowane drzewo OU Zielonej dzieli katalog według tego, czym faktycznie administrujemy osobno: kontami, komputerami (z podziałem na lokalizacje, bo inne polityki dotyczą biura, inne magazynu), serwerami, grupami, kontami usługowymi i osobno wyłączonymi obiektami, które nie są jeszcze usunięte, ale nie powinny już nikomu przeszkadzać w codziennej pracy.



Proponowane drzewo jednostek organizacyjnych Zielonej: Uzytkownicy, Komputery z podzialem na Biuro, Magazyn i Handlowcy, Serwery, Grupy, Konta uslugowe, Wylaczone (kliknięcie otwiera pełny rozmiar)

Zasada: GPO linkujemy do jednostki organizacyjnej, nie do całej domeny. Polityka podpięta wprost do domeny działa na każdy komputer i każde konto w całej firmie naraz, łącznie z serwerami i kontami usługowymi, dla których zwykle nie ma to sensu. Osobne

jednostki `Komputery` i `Serwery` istnieją właśnie po to, żeby polityka dla stacji roboczych (na przykład wymuszenie BitLockera) nigdy przypadkiem nie trafiła na `sql01`.

> **Pojęcie: model AGDLP.** Skrócona nazwa kolejności zagnieżdżania w typowym modelu uprawnień Active Directory: konta (`Account`) trafiają do grup globalnych (`Global`), grupy globalne trafiają do grup lokalnych w domenie (`Domain Local`), a to dopiero grupa lokalna w domenie dostaje faktyczne uprawnienie (`Permission`), na przykład do udziału sieciowego. W Zielonej nazewnictwo grup wprost pokazuje, czym dana grupa jest: `GG_` na początku nazwy dla grupy globalnej (`Global Group`), zbierającej konta jednego typu (`GG_Ksiegowosc`, `GG_Kadry`), i `DL_` dla grupy lokalnej w domenie (`Domain Local`), która faktycznie niesie uprawnienie do zasobu (`DL_Ksiegowosc_RW`). Pełne zastosowanie tego modelu przy nadawaniu uprawnień do udziałów sieciowych opisaliśmy na stronie Udziały i uprawnienia NTFS na serwerze plików.

Delegowanie resetu haseł dla kadr. Pani Halina i jej zespół nie potrzebują pełnych uprawnień administratora domeny, żeby pomagać kolegom z zapomnianym hasłem. Delegujemy im tylko jedno konkretne prawo, `Reset Password`, na jednostce `Uzytkownicy`, zamiast dodawać ich do grupy `Domain Admins` z pełnią władzy nad całym katalogiem. To ten sam duch co konta usługowe zarządzane: nadajemy dokładnie tyle uprawnień, ile potrzeba do konkretnego zadania, nie więcej.

Ochrona przed przypadkowym usunięciem. Każda jednostka organizacyjna utworzona `New-ADOrganizationalUnit` dostaje domyślnie atrybut chroniący ją przed przypadkowym usunięciem z poziomu Active Directory Users and Computers czy skryptu. Usunięcie całej jednostki `Komputery` przez pomyłkę oznaczałoby usunięcie wszystkich kont komputerów w niej razem z jej podjednostkami, więc ochrona zostaje włączona, dopóki świadomie jej nie wyłączymy (`Set-ADOrganizationalUnit -Identity "..." -ProtectedFromAccidentalDeletion $false`), zwykle tuż przed faktycznym, zamierzonym usunięciem.

> ⚠ W nazwach jednostek organizacyjnych nigdy nie używamy ukośnika (`/`). Znak ten rozjeżdża ścieżkę `ADsPath`, którą część narzędzi, w tym `manage-bde`, buduje z `DistinguishedName` obiektu, i kończy się to trudnym do skojarzenia błędem dopiero przy zupełnie innej operacji, na przykład przy kopii klucza BitLockera do katalogu. Opisaliśmy ten dokładny przypadek, łącznie z naprawą istniejącej już jednostki z ukośnikiem w nazwie, na stronie BitLocker z kluczem odzyskiwania w Active Directory.

Częste błędy

Objaw	Przyczyna	Co robimy
`New-ADOrganizationalUnit` na jednostce zagnieżdżonej kończy się błędem, że rodzic nie istnieje	jednostki tworzymy w złej kolejności, `Komputery` przed jej rodzicem albo `Biuro` przed `Komputery`	tworzymy drzewo od korzenia w dół, najpierw jednostki najwyższego poziomu, dopiero potem ich podjednostki
`Remove-ADOrganizationalUnit` albo usunięcie przez konsolę zwraca odmowę dostępu	jednostka ma domyślnie włączoną ochronę przed przypadkowym usunięciem	wyłączamy ją świadomie `Set-ADOrganizationalUnit -ProtectedFromAccidentalDeletion $false`, dopiero potem usuwamy
GPO podpięte do domeny zmienia ustawienia na serwerach, mimo że miało dotyczyć tylko stacji roboczych	polityka linkowana do całej domeny zamiast do jednostki `Komputery`	odlinkowujemy GPO od domeny i linkujemy je do właściwej jednostki organizacyjnej
Grupa z prawem resetu haseł nadanym przez kreator nie działa dla użytkowników w podjednostce	delegowanie z kreatora domyślnie obejmuje też obiekty potomne, ale trzeba to świadomie zaznaczyć albo sprawdzić zasięg	sprawdzamy zasięg nadania `dsacls` na jednostce nadrzędnej, w razie potrzeby powtarzamy delegowanie bezpośrednio na podjednostce
`manage-bde -adbackup` albo skrypt audytowy nie znajduje jednostki po nazwie	nazwa jednostki organizacyjnej zawiera ukośnik albo się powtarza w innym miejscu drzewa	zmieniamy nazwę jednostki bez ukośnika, w skryptach i uprawnieniach używamy pełnego `DistinguishedName`, nie samej nazwy

□□ Ćwiczenia

1. Dlaczego w Zielonej jednostka `Komputery` dzieli się na `Biuro`, `Magazyn` i `Handlowcy`, zamiast trzymać wszystkie komputery firmy w jednej wspólnej jednostce?

Odpowiedź

Różne lokalizacje mają różne wymagania polityk: komputery w magazynie w Swarzędzu korzystają z innych ustawień niż laptopy handlowców w terenie czy stacje robocze w biurze w Pamiątkowie. Osobne podjednostki pozwalają linkować różne GPO do każdej grupy komputerów bez filtrowania po nazwie czy lokalizacji wewnątrz jednej wspólnej polityki, i bez ryzyka, że polityka dla jednej lokalizacji przypadkiem trafi na drugą.

1. Dlaczego delegujemy pani Halinie konkretne prawo `Reset Password` na jednostce `Uzytkownicy`, zamiast po prostu dodać jej konto do grupy `Domain Admins`, skoro efekt końcowy (może resetować hasła) wygląda z zewnątrz podobnie?

Odpowiedź

Grupa `Domain Admins` daje pełną kontrolę nad całym katalogiem: możliwość zmiany dowolnego obiektu, dowolnej polityki i dowolnych uprawnień w całej domenie, nie tylko resetu hasła. Delegowanie jednego konkretnego prawa na jednej konkretnej jednostce ogranicza to, co pani Halina faktycznie może zrobić, do dokładnie tego zadania, do którego jej to uprawnienie jest potrzebne, więc pomyłka albo przejęte konto nie daje od razu pełnej władzy nad domeną.

Powiązane: Active Directory od zera: pierwszy i drugi kontroler domeny · Projekt lasu i domeny Zielonej: lokacje, podsieci, FSMO, poziomy funkcjonalne i nazewnictwo · DNS w domenie: strefy, rekordy, przekazywanie · Udziały i uprawnienia NTFS na serwerze plików · BitLocker z kluczem odzyskiwania w Active Directory · Konta usługowe MSA i gMSA

Źródła: Microsoft Learn, „New-ADOrganizationalUnit (ActiveDirectory)" · Microsoft Learn, „New-ADGroup (ActiveDirectory)" · Microsoft Learn, „New-ADUser (ActiveDirectory)" · Microsoft Learn, „Move-ADObject (ActiveDirectory)" · Microsoft Learn, „Get-ADOrganizationalUnit (ActiveDirectory)" · Microsoft Learn, „Delegation of Control in AD DS on Windows Server" · Microsoft Learn, „Dsacls" · `Get-Help dsacls`

Revision #30
Created 2026-09-28 09:24:27 UTC by Tomasz Konieczny
Updated 2026-10-26 14:26:27 UTC by Tomasz Konieczny