

## AUTOMATYZACJA TWORZENIA UŻYTKOWNIKÓW W WINDOWS SERVER 2012

I. Wprowadzenie do ćwiczenia.

### 1. Tworzenie wielu użytkowników.

Administratorzy czasami muszą stworzyć setki kont użytkowników i korzystają wtedy z mechanizmów służących do automatyzacji procesu tworzenia dużej liczby obiektów Active Directory. Są to:

- *LDIFDE.exe* - jest narzędziem, które służy do tworzenia i modyfikacji obiektów w AD za pomocą importu z pliku **LDIF**,

- *CSVDE.exe* - jest narzędziem, które służy do tworzenia obiektów w AD za pomocą importu z pliku **CSV**,

- *Windows PowerShell* - jest narzędziem, które służy do tworzenia obiektów w AD za pomocą importu z pliku **CSV**,

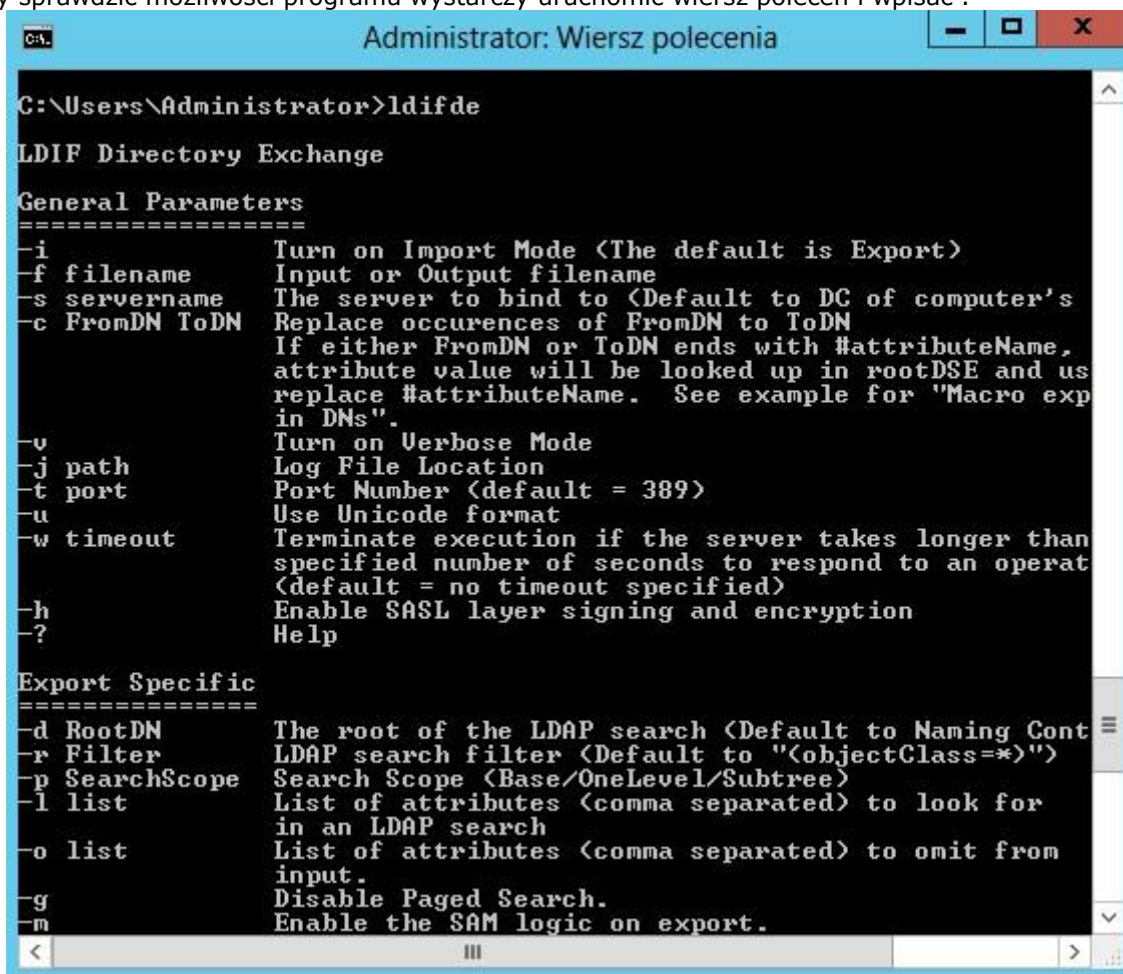
- *skrypty VBS* - tworzony jest skrypt w formacie **vbs** do tworzenia obiektów.

### 2. Korzystanie z LDIFDE.exe.

Umożliwia tworzenie, modyfikowanie i usuwanie obiektów, a także eksportowanie informacji dotyczących użytkowników czy grup do innych aplikacji lub usług.

II. Eksportowanie danych za pomocą LDIFDE.exe.

Aby sprawdzić możliwości programu wystarczy uruchomić wiersz poleceń i wpisać .



```
C:\Users\Administrator>ldifde

LDIF Directory Exchange

General Parameters
=====
-i          Turn on Import Mode (The default is Export)
-f filename Input or Output filename
-s servername The server to bind to (Default to DC of computer's
-c FromDN ToDN Replace occurrences of FromDN to ToDN
             If either FromDN or ToDN ends with #attributeName,
             attribute value will be looked up in rootDSE and us
             replace #attributeName. See example for "Macro exp
             in DNs".
-v          Turn on Uerbose Mode
-j path     Log File Location
-t port     Port Number (default = 389)
-u          Use Unicode format
-w timeout  Terminate execution if the server takes longer than
             specified number of seconds to respond to an operat
             (default = no timeout specified)
-h          Enable SASL layer signing and encryption
-?         Help

Export Specific
=====
-d RootDN   The root of the LDAP search (Default to Naming Cont
-r Filter   LDAP search filter (Default to "(objectClass=*)")
-p SearchScope Search Scope (Base/OneLevel/Subtree)
-l list     List of attributes (comma separated) to look for
             in an LDAP search
-o list     List of attributes (comma separated) to omit from
             input.
-g          Disable Paged Search.
-m          Enable the SAM logic on export.
```

Podstawowe parametry, które możemy stosować to np: i - tryb importu (eksport jest domyślnie), s - nazwa serwera, f - nazwa pliku. Spróbujemy teraz wyeksportować informacje o naszej domenie. Użyjemy polecenia:

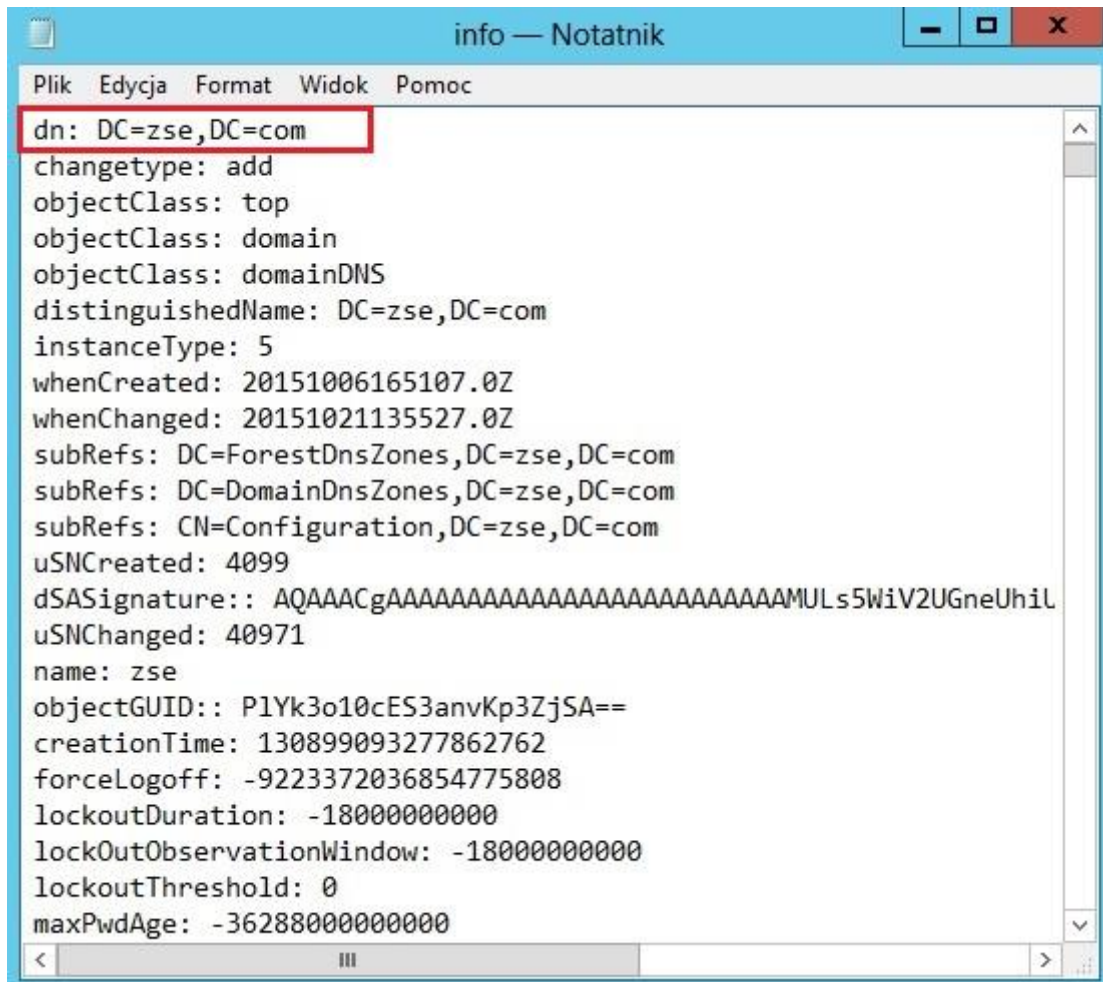
### ldifde -f info.txt



```
C:\Users\Administrator>ldifde -f info.txt
Connecting to "SERWER00.zse.com"
Logging in as current user using SSPI
Exporting directory to file info.txt
Searching for entries...
Writing out entries.....
.....
.....
233 entries exported

The command has completed successfully
C:\Users\Administrator>
```

Sprawdzamy teraz czy plik **info.txt** znajduje się w katalogu Administrator i jaką ma zawartość.



```
Plik Edycja Format Widok Pomoc
dn: DC=zse,DC=com
changetype: add
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=zse,DC=com
instanceType: 5
whenCreated: 20151006165107.0Z
whenChanged: 20151021135527.0Z
subRefs: DC=ForestDnsZones,DC=zse,DC=com
subRefs: DC=DomainDnsZones,DC=zse,DC=com
subRefs: CN=Configuration,DC=zse,DC=com
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAAMULs5WiV2UGneUhiL
uSNChanged: 40971
name: zse
objectGUID:: P1Yk3o10cES3anvKp3ZjSA==
creationTime: 130899093277862762
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
```

Jeśli chcemy uzyskać informacje o konkretnym obiekcie (np. jakimś użytkowniku) to użyjemy następującego polecenia:

```
ldifde -f info1.txt -s serwer00 -d "CN=James JB. Bond8,CN=Users,DC=zse,DC=com"
```

```
Administrator: Wiersz polecenia
C:\Users\Administrator>ldifde -f info1.txt -s serwer00 -d "CN=James JB. Bond8,CN=Users,DC=zse,DC=com"
Connecting to "serwer00"
Logging in as current user using SSPI
Exporting directory to file info1.txt
Searching for entries...
Writing out entries.
1 entries exported

The command has completed successfully

C:\Users\Administrator>
```

I ponownie sprawdzamy czy plik **info1.txt** znajduje się w katalogu Administrator i jaką ma zawartość.

```
info1 — Notatnik
Plik Edycja Format Widok Pomoc
dn: CN=James JB. Bond8,CN=Users,DC=zse,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: James JB. Bond8
sn: Bond8
givenName: James
initials: JB
distinguishedName: CN=James JB. Bond8,CN=Users,DC=zse,DC=com
instanceType: 4
whenCreated: 20151021193403.0Z
whenChanged: 20151021193524.0Z
displayName: James JB. Bond8
uSNCreated: 41027
uSNChanged: 41034
name: James JB. Bond8
objectGUID:: q4/dQC1D/k2iQSwe43KFDg==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
```

### III. Tworzenie i usuwanie kont użytkowników za pomocą LDIFDE.

To polecenie ma ograniczone możliwości (np. nie da się ustawić hasła), ale można zakładać konta dla większej grupy użytkowników. Tworzymy plik o nazwie **user.txt**, który powinien zawierać przykładowe dane:

**DN: CN=James JB. Bond2,OU=Informatycy,DC=ZSE,DC=com** - nazwa DN

**changetype: add** - dodawanie obiektu

**CN: James JB. Bond2** - pełna nazwa użytkownika

**description: "PSSO"** - opis

**objectClass: user** - typ obiektu

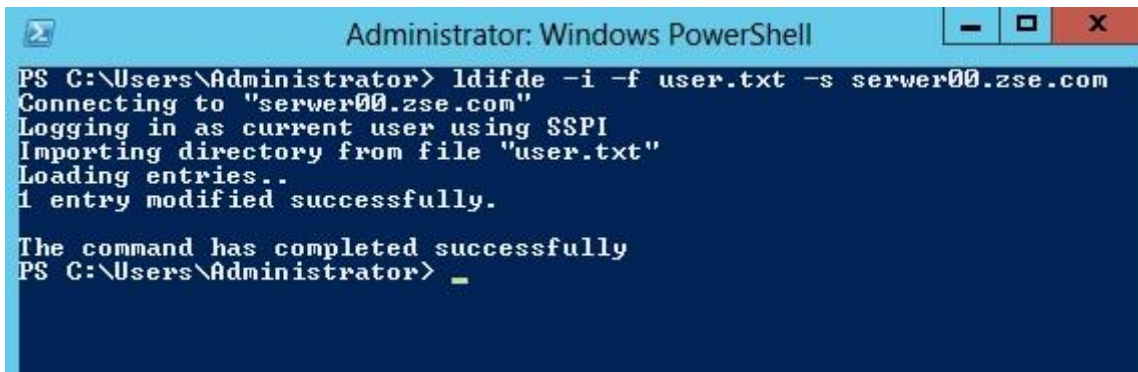
**userAccountControl: 544** - włączenie konta

**userPrincipalName: bondj2** - nazwa główna użytkownika  
**sAMAccountName: bondj2** - nazwa konta  
**givenName: James** - imię  
**sn: Bond2** - nazwisko



```
Plik Edycja Format Widok Pomoc
DN: CN=James JB. Bond2,OU=Informatycy,DC=zse,DC=com
changetype: add
CN: James JB. Bond2
description: PSSO
objectClass: user
userAccountControl: 544
userPrincipalName: bondj2
samAccountName: bondj2
givenName: James
sn: Bond2
```

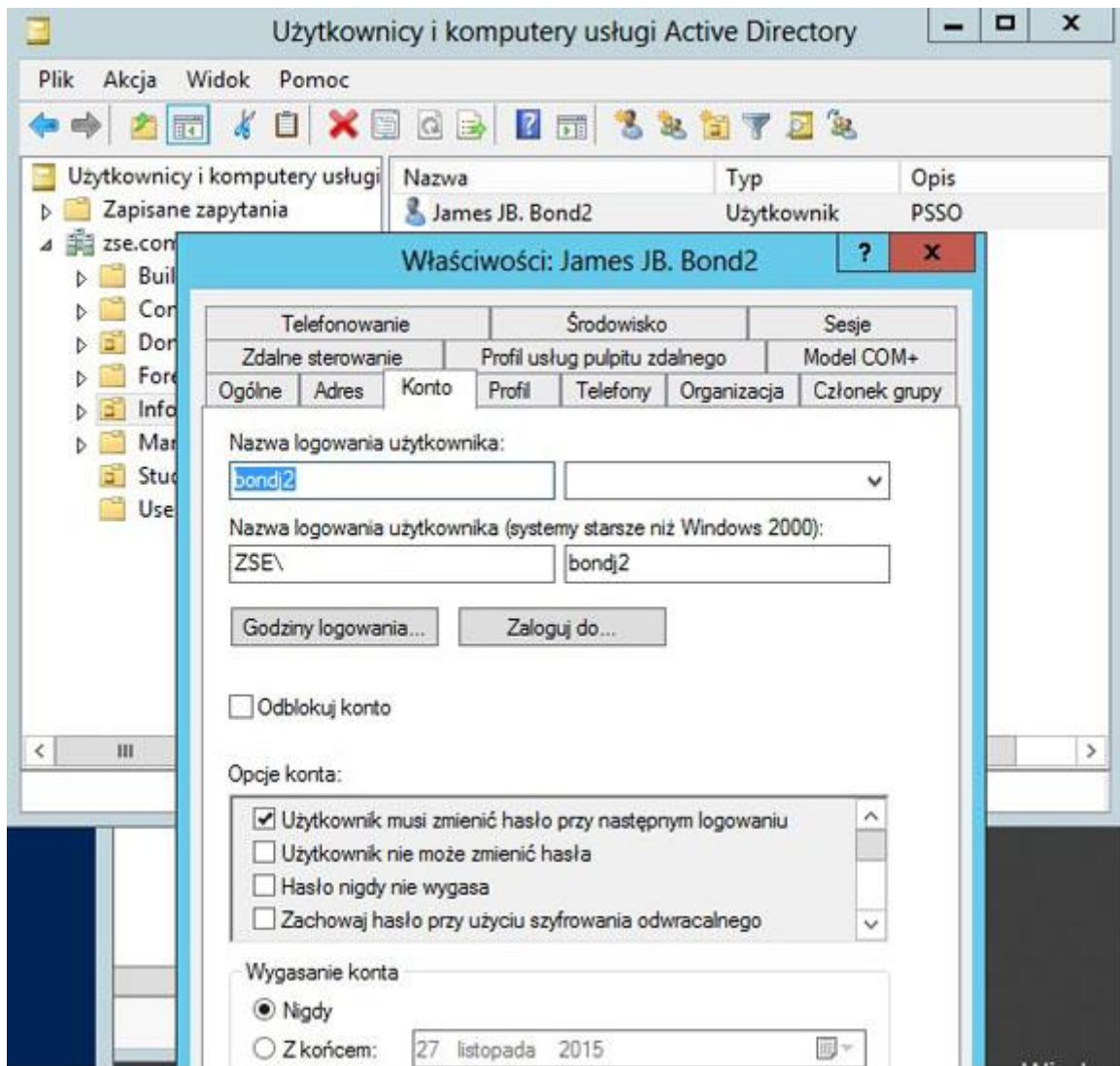
Wpisujemy teraz polecenie **ldifde -i -f user.txt -s serwer00.zse.com** i powinniśmy uzyskać poniższy efekt:



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ldifde -i -f user.txt -s serwer00.zse.com
Connecting to "serwer00.zse.com"
Logging in as current user using SSPI
Importing directory from file "user.txt"
Loading entries..
1 entry modified successfully.

The command has completed successfully
PS C:\Users\Administrator> _
```

I sprawdzamy czy nasze konto faktycznie zostało utworzone.



Teraz utworzymy więcej kont użytkowników (10). Powielamy 10-krotnie zawartość pliku **user.txt**, zmieniając w każdym bloku albo nazwy użytkowników i powiązanych z nimi wpisów, albo tylko indeksy przy nazwisku np. **Bondj2**, **Bondj3** itp. Powinno to wyglądać następująco:

```
user — Notatnik
Plik Edycja Format Widok Pomoc
DN: CN=James JB. Bond11,OU=Informatycy,DC=zse,DC=com
changetype: add
CN: James JB. Bond11
description: PSSO
objectClass: user
userAccountControl: 544
userPrincipalName: bondj11
samAccountName: bondj11
givenName: James
sn: Bond11

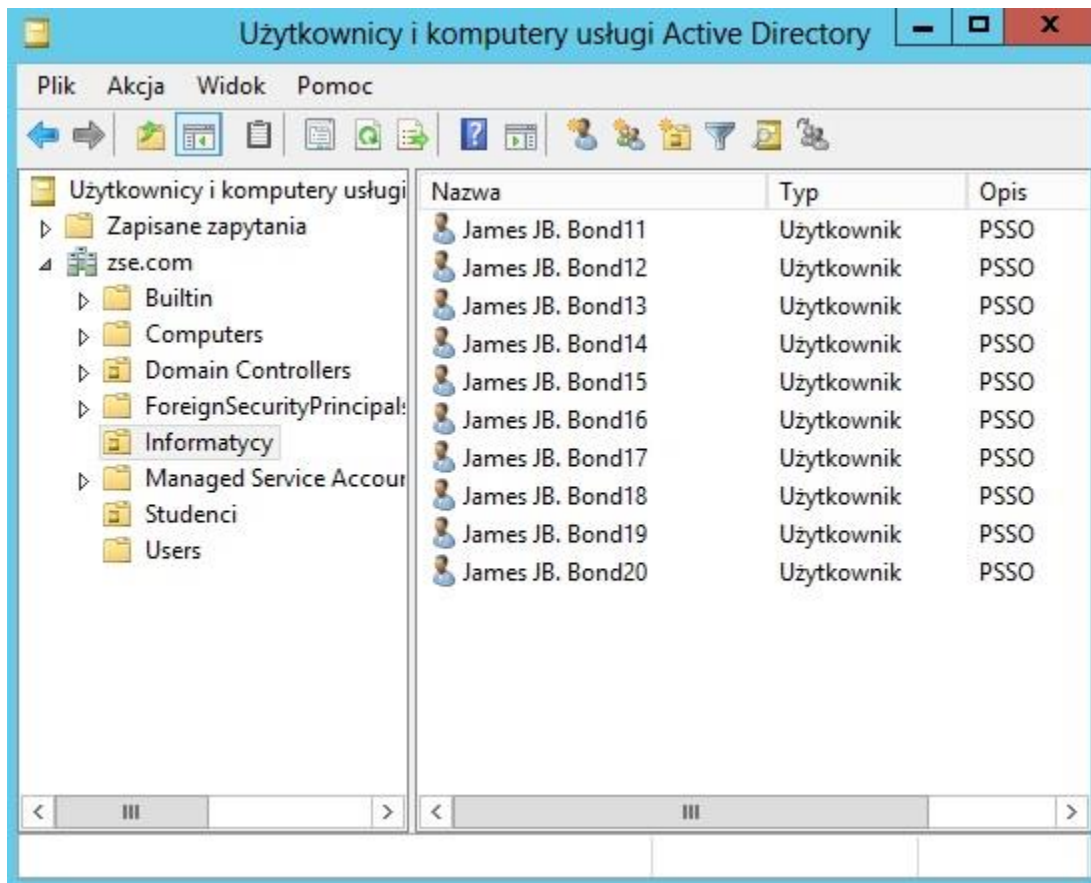
DN: CN=James JB. Bond12,OU=Informatycy,DC=zse,DC=com
changetype: add
CN: James JB. Bond12
description: PSSO
objectClass: user
userAccountControl: 544
userPrincipalName: bondj12
samAccountName: bondj12
givenName: James
sn: Bond12
```

Wpisujemy teraz polecenie **ldifde -i -f user.txt -s serwer00.zse.com** i powinniśmy uzyskać poniższy efekt z informacją, że pomyślnie zmodyfikowano 10 wpisów.

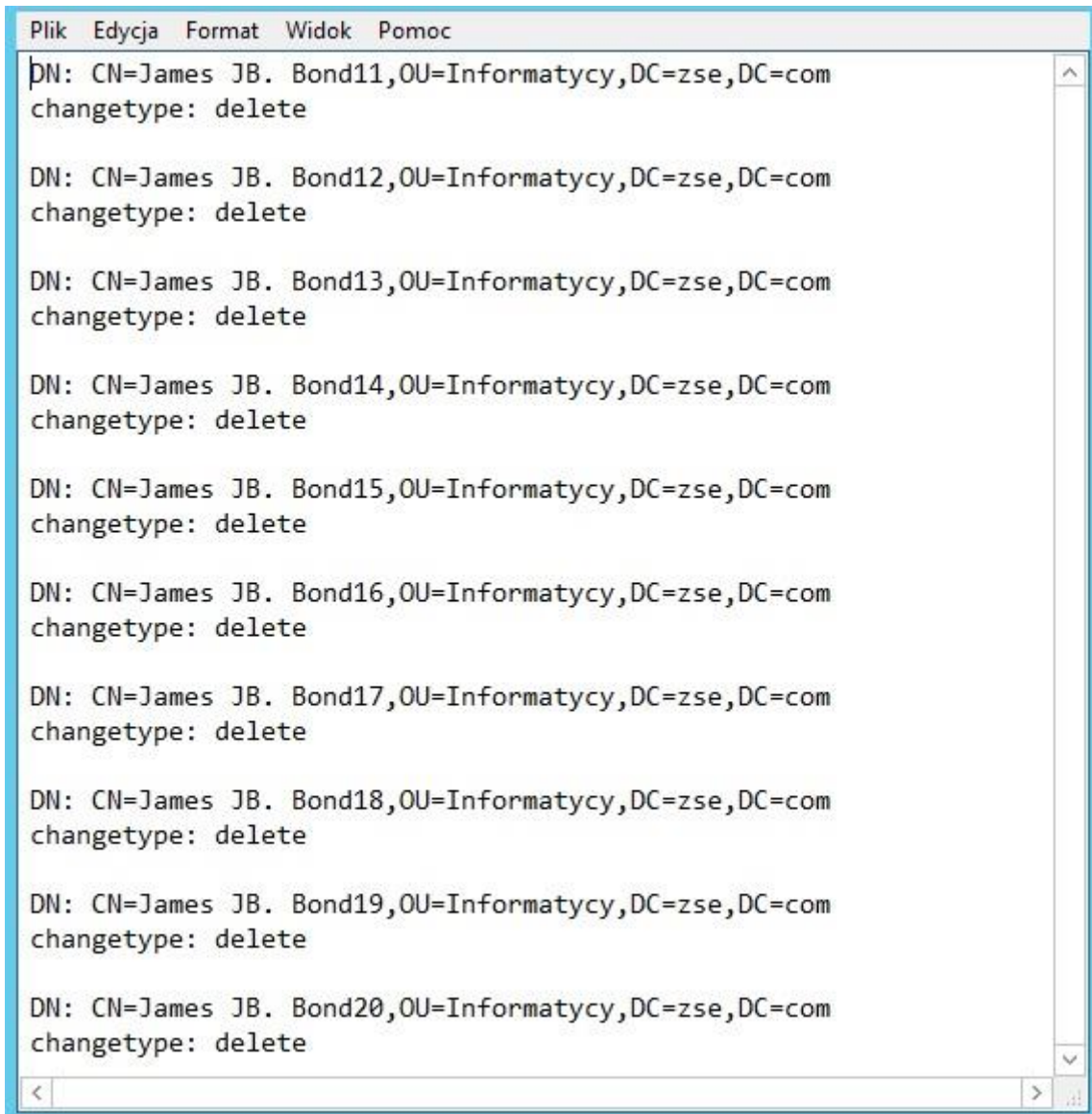
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ldifde -i -f user.txt -s serwer00.zse.com
Connecting to "serwer00.zse.com"
Logging in as current user using SSPI
Importing directory from file "user.txt"
Loading entries .....
10 entries modified successfully.

The command has completed successfully
PS C:\Users\Administrator>
```

Sprawdzamy jeszcze czy nasze konta faktycznie zostały utworzone.



Aby usunąć nasze obiekty przy użyciu **ldifde**, wystarczy zmienić w pliku (albo stworzyć nowy) parametr "add" na "delete" (pozostałe atrybuty należy wykasować).



```
Plik  Edycja  Format  Widok  Pomoc
DN: CN=James JB. Bond11,OU=Informatycy,DC=zse,DC=com
changetype: delete

DN: CN=James JB. Bond12,OU=Informatycy,DC=zse,DC=com
changetype: delete

DN: CN=James JB. Bond13,OU=Informatycy,DC=zse,DC=com
changetype: delete

DN: CN=James JB. Bond14,OU=Informatycy,DC=zse,DC=com
changetype: delete

DN: CN=James JB. Bond15,OU=Informatycy,DC=zse,DC=com
changetype: delete

DN: CN=James JB. Bond16,OU=Informatycy,DC=zse,DC=com
changetype: delete

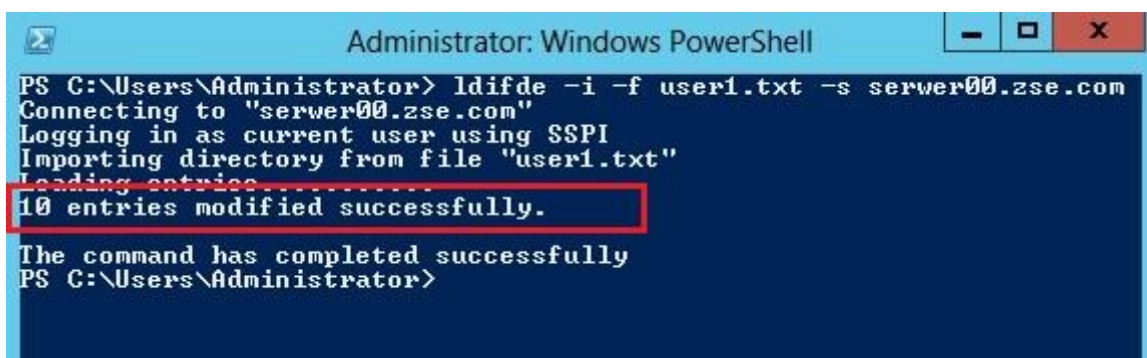
DN: CN=James JB. Bond17,OU=Informatycy,DC=zse,DC=com
changetype: delete

DN: CN=James JB. Bond18,OU=Informatycy,DC=zse,DC=com
changetype: delete

DN: CN=James JB. Bond19,OU=Informatycy,DC=zse,DC=com
changetype: delete

DN: CN=James JB. Bond20,OU=Informatycy,DC=zse,DC=com
changetype: delete
```

Wpisujemy polecenie **ldifde -i -f user1.txt -s serwer00.zse.com** i powinniśmy uzyskać poniższy efekt z informacją, że pomyślnie zmodyfikowano 10 wpisów.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ldifde -i -f user1.txt -s serwer00.zse.com
Connecting to "serwer00.zse.com"
Logging in as current user using SSPI
Importing directory from file "user1.txt"
Loading entries
10 entries modified successfully.
The command has completed successfully
PS C:\Users\Administrator>
```

IV. Tworzenie i usuwanie kont użytkowników za pomocą Windows PowerShell.

To narzędzie, które ma większe możliwości niż Ldifde (np. da się ustawić hasła) i można także zakładać konta dla większej grupy użytkowników. Najpierw utworzymy pojedynczego użytkownika za pomocą wiersza poleceń. Wpisujemy:

**new-ADUser -Name "James Bond21" -SamAccountName "bondj21" -UserPrincipalName**

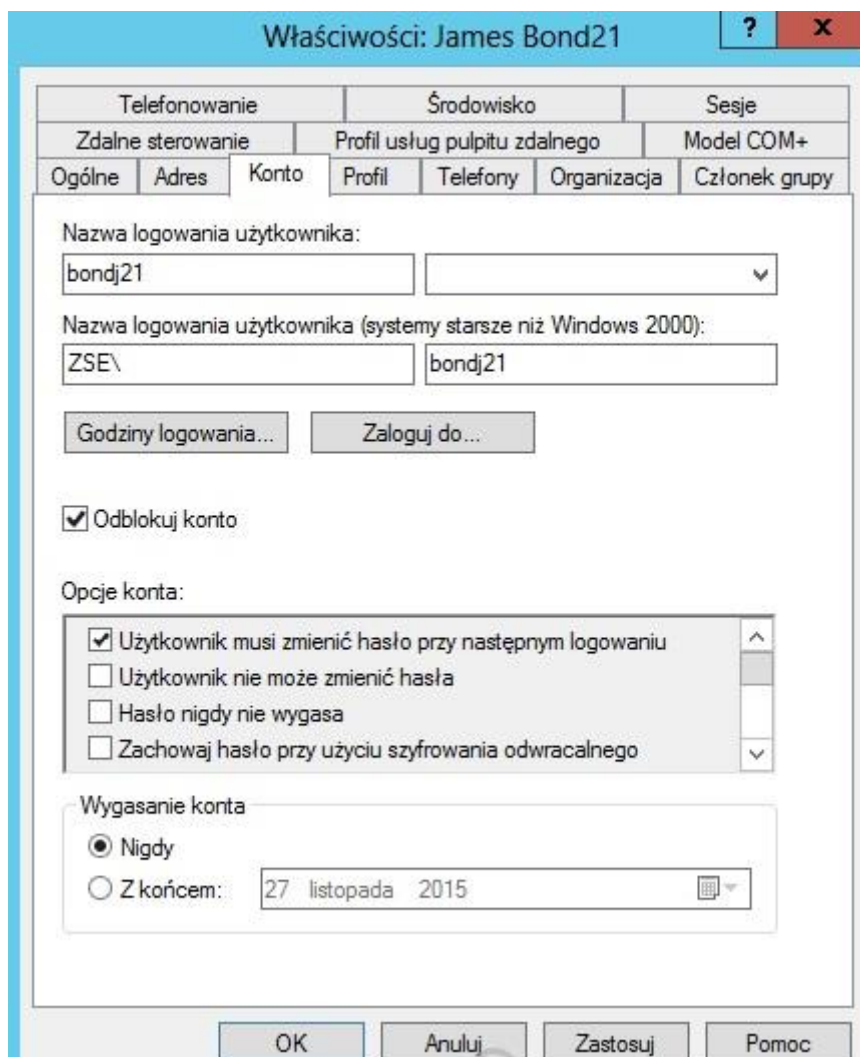


```
"bondj21" -GivenName "James" -SurName "Bond21" -path "CN=Users,DC=zse,DC=com"
-Enabled $true -AccountPassword(Read-Host -AsSecureString "Password") -
ChangePasswordAtLogon $true
```

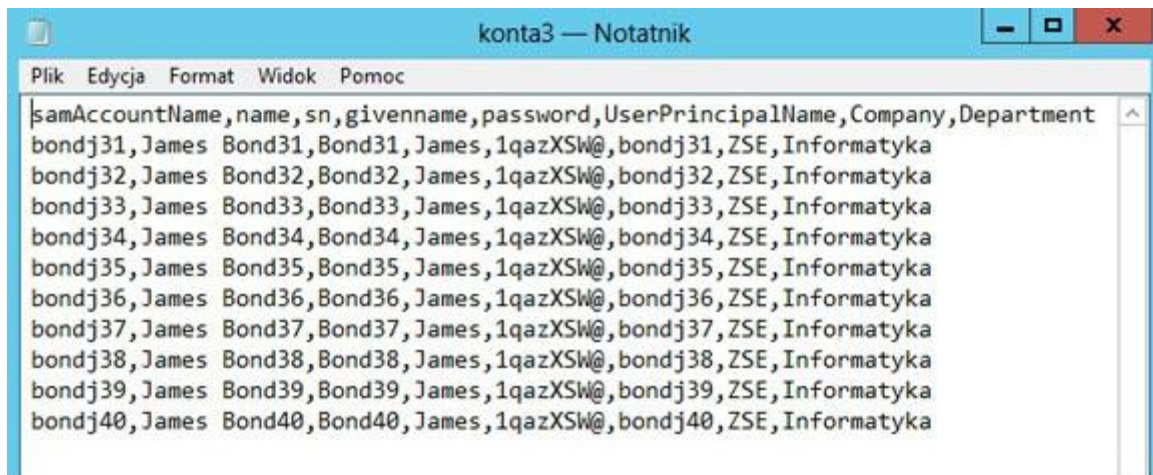


```
Administrator: Windows PowerShell
PS C:\Users\Administrator> new-ADUser -Name "James Bond21" -SamAccountName "bondj21" -UserPrincipalName "bondj21" -GivenName "James" -Surname "Bond21" -path "CN=Users,DC=zse,DC=com" -Enabled $true -AccountPassword(Read-Host -AsSecureString "Password") -ChangePasswordAtLogon $true
Password: *****
PS C:\Users\Administrator>
```

Jeśli uzyskaliśmy powyższy efekt to znaczy, że konto zostało utworzone co sprawdzamy w Active Directory.



Teraz utworzymy więcej kont użytkowników (10). Musimy utworzyć plik typu **csv**. Otwieramy albo MSeExcel albo notatnik i tworzymy plik np. **konta3.csv**, podając parametry konta oddzielone przecinkami i odpowiadające im dane.



```
konto3 — Notatnik
Plik Edycja Format Widok Pomoc
samAccountName,name,sn,givenname,password,UserPrincipalName,Company,Department
bondj31,James Bond31,Bond31,James,1qazXSW@,bondj31,ZSE,Informatyka
bondj32,James Bond32,Bond32,James,1qazXSW@,bondj32,ZSE,Informatyka
bondj33,James Bond33,Bond33,James,1qazXSW@,bondj33,ZSE,Informatyka
bondj34,James Bond34,Bond34,James,1qazXSW@,bondj34,ZSE,Informatyka
bondj35,James Bond35,Bond35,James,1qazXSW@,bondj35,ZSE,Informatyka
bondj36,James Bond36,Bond36,James,1qazXSW@,bondj36,ZSE,Informatyka
bondj37,James Bond37,Bond37,James,1qazXSW@,bondj37,ZSE,Informatyka
bondj38,James Bond38,Bond38,James,1qazXSW@,bondj38,ZSE,Informatyka
bondj39,James Bond39,Bond39,James,1qazXSW@,bondj39,ZSE,Informatyka
bondj40,James Bond40,Bond40,James,1qazXSW@,bondj40,ZSE,Informatyka
```

Wpisujemy teraz polecenie:

```
Import-CSV konto3.csv | foreach {New-ADUser -SamAccountName $_.SamAccountName  
-Name $_.Name -Surname $_.sn -GivenName $_.GivenName -Path  
"OU=Informatycy,DC=zse,DC=com" -AccountPassword (ConvertTo-SecureString -  
AsPlainText $_.password -Force) -UserPrincipalName $_.UserPrincipalName -Company  
$_.Company -Department $_.Department -Enabled $true}
```

Powinniśmy uzyskać poniższy efekt.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Import-CSV konto3.csv | foreach {New-ADUser  
-SamAccountName $_.SamAccountName -Name $_.Name -Surname $_.sn -Given  
Name $_.GivenName -Path "OU=Informatycy,DC=zse,DC=com" -AccountPasswor  
d (ConvertTo-SecureString -AsPlainText $_.password -Force) -UserPrinci  
palName $_.UserPrincipalName -Company $_.Company -Department $_.Depart  
ment -Enabled $true}  
PS C:\Users\Administrator> _
```

Sprawdzamy jeszcze czy nasze konta faktycznie zostały utworzone.

Użytkownicy i komputery usługi Active Directory

Plik Akcja Widok Pomoc

← → [New] [Refresh] [Delete] [Copy] [Paste] [Find] [Help] [Filter] [Print] [Refresh]

Użytkownicy i komputery usługi

- Zapisane zapytania
- zse.com
  - Built-in
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal:
  - Informatycy
  - Managed Service Account
  - Users

Nazwa	Typ	Opis
James Bond31	Użytkownik	
James Bond32	Użytkownik	
James Bond33	Użytkownik	
James Bond34	Użytkownik	
James Bond35	Użytkownik	
James Bond36	Użytkownik	
James Bond37	Użytkownik	
James Bond38	Użytkownik	
James Bond39	Użytkownik	
James Bond40	Użytkownik	

< ||| > < ||| >