cw16: Izolacja użytkowników FTP – tryby izolacji i globalne katalogi wirtualne (IIS FTP)

Wersja dla ucznia – praca na działającym FTPS (Explicit TLS)

Data opracowania: 2026-02-07

Cel ogólny ćwiczenia. Uczeń **analizuje, konfiguruje i porównuje tryby izolacji użytkowników FTP w IIS** oraz bada wpływ **globalnych katalogów wirtualnych** na widoczność i bezpieczeństwo zasobów, wykorzystując jednocześnie **uprawnienia NTFS** do kontroli dostępu. Uczeń wykonuje testy pozytywne i negatywne dla różnych trybów izolacji oraz formułuje wnioski dotyczące mechanizmów bezpieczeństwa i ich zastosowania.

Cele szczegółowe (uczeń potrafi):

1. Konfiguracja środowiska FTP

- **Odróżnia** cztery tryby izolacji użytkowników FTP w IIS.
- **Wyjaśnia** przeznaczenie katalogów domenowych i katalogów współdzielonych.

2. Praca z katalogami wirtualnymi

- **Tworzy** globalny katalog wirtualny (np. *shared*).
- **Tworzy** katalog wirtualny przypisany do konkretnego użytkownika (np. *tools* dla ftpuser1) oraz **opisuje różnicę** między katalogiem globalnym a per-user.

3. Zastosowanie uprawnień NTFS

- **Nadaje** właściwe uprawnienia NTFS (Modify dla użytkownika, RX dla grupy, Full Control dla Administratorzy/SYSTEM).
- **Wyjaśnia**, które elementy izolacji wynikają z NTFS, a które z konfiguracji IIS.

4. Testowanie konfiguracji

- **Testuje** logowanie oraz widoczność katalogów w różnych trybach izolacji.
- **Rozpoznaje i interpretuje** błąd **550** (brak dostępu).
- **Dokumentuje** wyniki testów.

5. Formułowanie wniosków

- **Wskazuje** najbardziej przewidywalny tryb izolacji i **uzasadnia** wybór.
- **Wyjaśnia**, jak globalne katalogi wirtualne wpływają na widoczność zasobów.
- **Określa**, kiedy użycie globalnych vdir jest przydatne w środowisku szkolnym lub firmowym.

1. Wprowadzenie (sens ćwiczenia)”

W tym ćwiczeniu poznasz praktyczne mechanizmy izolacji użytkowników FTP w usługach IIS. Sprawdzisz, jak poszczególne tryby izolacji wpływają na widoczność katalogów, dostęp użytkowników oraz bezpieczeństwo danych. Przetestujesz także działanie globalnych i per-user katalogów wirtualnych oraz porównasz izolację logiczną (IIS) z izolacją na poziomie NTFS. W ćwiczeniu wykonasz zarówno testy pozytywne, jak i negatywne, aby zrozumieć różnice między poszczególnymi konfiguracjami.

2. Stan początkowy (wymagany)

Zaliczone cw15 (konto FTP bez logowania lokalnego/RDP, reguły autoryzacji w IIS).

Uruchom skrypt PowerShell – przygotowanie środowiska. Skrypt:

- tworzy grupę GG_FTP_Users
- tworzy konta testowe domenowe: ftpuser1, ftpuser2 (opcjonalnie ftpadmin_ad)
- tworzy katalogi wg struktury domeny
- ustawia ACL NTFS: każdy użytkownik ma prawa tylko do swojego folderu
- tworzy „wspólny" katalog do testów globalnych vdir: C:\FTPSHARED

Uruchom jako Administrator na DC/serwerze FTP.

```
Import-Module ActiveDirectory
# --- Parametry ---
$GroupName = "GGFTPUsers"
$UsersOU   = "OU=FTPUsers," + (Get-ADDomain).DistinguishedName
$DomainNB  = (Get-ADDomain).NetBIOSName
$FtpRoot   = "C:\inetpub\ftproot"
$DomainRoot= Join-Path $FtpRoot $DomainNB
$SharedDir = "C:\FTPSHARED"
$Users = @(
  @{ Sam="ftpuser1"; Name="FTP User 1" },
  @{ Sam="ftpuser2"; Name="FTP User 2" }
)
# --- 1) OU ---
if (-not (Get-ADOrganizationalUnit -LDAPFilter "(ou=FTPUsers)" -ErrorAction SilentlyContinue)) {
  New-ADOrganizationalUnit -Name "FTPUsers" -Path (Get-ADDomain).DistinguishedName | Out-
Null
}
```

```
# --- 2) Grupa ---
if (-not (Get-ADGroup -Filter "Name -eq '$GroupName'" -ErrorAction SilentlyContinue)) {
  New-ADGroup -Name $GroupName -GroupScope Global -GroupCategory Security -Path $UsersOU |
Out-Null
}
# --- 3) Użytkownicy testowi ---
$Pass = ConvertTo-SecureString "zaq1@WSX" -AsPlainText -Force
foreach ($u in $Users) {
  if (-not (Get-ADUser -Filter "SamAccountName -eq '$($u.Sam)'" -ErrorAction SilentlyContinue)) {
    New-ADUser -Name $u.Name -SamAccountName $u.Sam -AccountPassword $Pass `
      -Enabled $true -PasswordNeverExpires $true -Path $UsersOU | Out-Null
  }
  Add-ADGroupMember -Identity $GroupName -Members $u.Sam -ErrorAction SilentlyContinue
}
# --- 4) Katalogi domenowe ---
New-Item -ItemType Directory -Force -Path $DomainRoot | Out-Null
foreach ($u in $Users) {
  New-Item -ItemType Directory -Force -Path (Join-Path $DomainRoot $u.Sam) | Out-Null
}
# --- 5) Katalog wspólny do testów globalnych vdir ---
New-Item -ItemType Directory -Force -Path $SharedDir | Out-Null
"Shared area for all FTP users" | Out-File -Encoding UTF8 (Join-Path $SharedDir "shared.txt")
# --- 6) ACL NTFS: izolacja ---
# Zasada: dziedziczenie wyłączone, user ma Modify, *S-1-5-32-544 Full, SYSTEM Full
foreach ($u in $Users) {
  $p    = Join-Path $DomainRoot $u.Sam
  $acct = "$DomainNB\$($u.Sam)"
  icacls $p /inheritance:r | Out-Null
  icacls $p /grant "${acct}:(OI)(CI)M" | Out-Null
  icacls $p /grant "*S-1-5-32-544:(OI)(CI)F" | Out-Null
  icacls $p /grant "SYSTEM:(OI)(CI)F" | Out-Null
```

}

 # ACL dla katalogu współdzielonego: tylko grupa GGFTPUsers

icacls $SharedDir /inheritance:r | Out-Null

icacls $SharedDir /grant "${DomainNB}\${GroupName}:(OI)(CI)RX" | Out-Null

*icacls $SharedDir /grant "*S-1-5-32-544:(OI)(CI)F" | Out-Null*

icacls $SharedDir /grant "SYSTEM:(OI)(CI)F" | Out-Null

Write-Host "OK: Przygotowano AD, katalogi i ACL pod FTP User Isolation." -ForegroundColor Green

Write-Host "Następny krok (uczeń): konfiguracja izolacji w IIS + testy." -ForegroundColor Cyan

Istnieją użytkownicy testowi w domenie: ftpuser1, ftpuser2 oraz grupa GG_FTP_Users.

Istnieje struktura katalogów: C:\inetpub\ftproot\<NETBIOS>\ftpuser1 oraz ftpuser2 (i ACL).

Klient FTPS: FileZilla i/lub WinSCP.

3. Krok 1 – przygotowanie katalogu wspólnego

Jeśli katalog C:\FTPSHARED istnieje, przejdź dalej. W przeciwnym razie utwórz go i dodaj plik shared.txt.

mkdir C:\FTPSHARED

echo Shared area> C:\FTPSHARED\shared.txt

4. Krok 2 – dodanie globalnego katalogu wirtualnego (shared)

1. IIS > Witryny > FTPS (Twoja witryna).
2. PPM na witrynie > Dodaj katalog wirtualny…
3. Alias: shared
4. Ścieżka fizyczna: C:\FTPSHARED
5. Zatwierdź OK.

5. Krok 3 – testowanie trybów izolacji (część główna)

W IIS > FTPS > „Izololowanie użytkowników FTP”. Dla każdego trybu wykonaj testy i zapisz wyniki.

Tryb A: Nie izoluj użytkowników

Ustaw: Nie izoluj użytkowników.

Zaloguj się jako ftpuser1 > sprawdź co widzi w katalogu głównym.

Sprawdź, czy widzi „shared” oraz czy widzi katalog ftpuser2.

Wniosek: jaką rolę odgrywa tu NTFS?

Tryb B: Katalog nazwa użytkownika (bez izolacji pełnej)

Ustaw: Katalog nazwa użytkownika.

Zaloguj się jako ftpuser1 (folder istnieje) > gdzie startuje sesja?

Usuń/zmień nazwę folderu ftpuser1 (tylko jeśli nauczyciel pozwoli) i sprawdź co się dzieje.

Wniosek: dlaczego to może być „pułapka" w administracji?

Tryb C: Izoluj użytkowników – wyłącz globalne katalogi wirtualne

Ustaw: Izoluj użytkowników > Katalog nazwa użytkownika (wyłącz globalne katalogi wirtualne).

Zaloguj się jako ftpuser1 > czy widzi „shared"? (oczekiwane: NIE)

Spróbuj wejść do ftpuser2 > oczekiwane: błąd 550.

Zaloguj się jako ftpuser2 i wykonaj analogiczny test.

Tryb D: Izoluj użytkowników – włącz globalne katalogi wirtualne

Ustaw: Izoluj użytkowników > Katalog nazwa użytkownika (włącz globalne katalogi wirtualne).

Zaloguj się jako ftpuser1 > czy widzi „shared"? (oczekiwane: TAK, jeśli ma prawa).

Wejdź do shared i odczytaj plik shared.txt.

Spróbuj wejść do ftpuser2 > oczekiwane: błąd 550.

6. Testy obowiązkowe (dowody)

Dowód 1: screen – ustawienie trybu C (wyłącz globalne vdir).

Dowód 2: screen – ftpuser1 nie widzi „shared" w trybie C.

Dowód 3: screen – ustawienie trybu D (włącz globalne vdir).

Dowód 4: screen – ftpuser1 widzi „shared" i plik shared.txt w trybie D.

Dowód 5: screen – błąd 550 przy próbie wejścia do ftpuser2.

7. Zadanie rozszerzone

A. Skonfiguruj „FTP katalog domowy skonfigurowany w usłudze Active Directory" dla ftpuser1 i sprawdź zachowanie.

Ta funkcja sprawia, że **IIS pobiera ścieżkę katalogu domowego bezpośrednio z atrybutu AD**, a nie z lokalnej struktury katalogów. Jest to bardziej zaawansowany tryb izolacji użytkowników.

1. Wymagania wstępne

Aby funkcja zadziałała:

1. **Użytkownik domenowy** (ftpuser1) musi istnieć w AD.
2. Musisz mieć **FTPS/FTP na IIS**, gdzie:

- działa izolacja użytkowników,
- działa uwierzytelnianie podstawowe,
- serwer jest członkiem domeny.

3. W AD musi zostać ustawiony atrybut: **msIIS-FTPRoot** (główny katalog) **msIIS-FTPDir** (podkatalog użytkownika) To one mówią IIS: gdzie jest katalog FTP danego użytkownika.

2. Przygotuj katalog domowy dla ftpuser1

Przykład katalogu: C:\FTPADHOME\ftpuser1

1. Utwórz katalog:

```
New-Item -ItemType Directory -Force -Path "C:\FTPADHOME\ftpuser1"
```

2. Ustaw uprawnienia NTFS:

```
icacls "C:\FTPADHOME\ftpuser1" /grant "DOMENA\ftpuser1:(OI)(CI)M"
icacls "C:\FTPADHOME\ftpuser1" /grant "Administratorzy:(OI)(CI)F"
icacls "C:\FTPADHOME\ftpuser1" /grant "SYSTEM:(OI)(CI)F"
```

3. Ustaw atrybuty Active Directory dla użytkownika ftpuser1

Tu decydujesz, **skąd IIS ma brać katalog domowy**.

Otwórz **Active Directory Users and Computers → ftpuser1 → Atrybuty (Attribute Editor)**

Znajdź i ustaw:

Atrybut AD	Wartość przykładowa	Znaczenie
msIIS-FTPRoot	C:\FTPADHOME	Główna ścieżka FTP
msIIS-FTPDir	ftpuser1	Podkatalog użytkownika

W efekcie IIS złoży to w: C:\FTPADHOME\ftpuser1

▶ Jeśli chcesz zrobić to PowerShellem:

```
Set-ADUser ftpuser1 -Add @{
   "msIIS-FTPRoot"="C:\FTPADHOME";
   "msIIS-FTPDir"="ftpuser1"
}
```

4. Włącz tryb „FTP katalog domowy skonfigurowany w usłudze Active Directory” w IIS

1. Otwórz **IIS Manager**
2. Przejdź do swojej witryny **FTP/FTPS**

3. Otwórz **(Izolacja użytkowników FTP)**
4. Wybierz opcję:

✓ „FTP home directory configured in Active Directory”

(*FTP katalog domowy skonfigurowany w usłudze Active Directory*)

5. Zastosuj.

Ten tryb mówi IIS: „Katalog domowy pobieraj z AD, a nie z lokalnej struktury C:\inetpub\ftproot…”

5. Restart usługi IIS

Musisz przeładować konfigurację:

iisreset

6. Test działania (bardzo ważny)

- **Test 1 - Logowanie ftpuser1**

Z klienta FTP (FileZilla / WinSCP):

- Host: IP serwera
- Protokół: FTP / FTPS
- Login: **ftpuser1**
- Hasło: domenowe

Oczekiwany rezultat:

- Użytkownik powinien startować w katalogu C:\FTPADHOME\ftpuser1
- Nie powinien widzieć żadnych katalogów domenowych typu \DOMENA\ftpuser2.
- Nie powinien wejść wyżej niż własny folder.

- **Test 2 - Dodaj plik testowy**

Do C:\FTPADHOME\ftpuser1 dodaj: test_ad.txt

Uczeń *musi widzieć ten plik* po zalogowaniu na FTP.

- **Test 3 - Test negatywny**

Zaloguj się jako:

- **ftpuser2**

Oczekiwane:

- ftpuser2 NIE zobaczy katalogu ftpuser1
- próba wejścia ręcznie → błąd **550**

7. Co tu jest ważne dydaktycznie (krótki komentarz)

Uczniowie powinni zrozumieć różnicę:

Element	Co robi
IIS User Isolation (AD Home Directory)	Decyduje, *jaką ścieżkę* widzi użytkownik
Atrybuty AD (msIIS-FTPRoot, msIIS-FTPDir)	Dostarczają *lokalizacji* katalogu domowego
NTFS	Decyduje o *realnym dostępie* do danych
Autoryzacja IIS	Decyduje, czy użytkownik może się uwierzytelnić

To jest najczystszy, najbardziej administracyjny tryb izolacji użytkowników FTP.

B. Dodaj per-user virtual directory „tools" tylko dla ftpuser1 (alias tools > C:\FTPSHARED) i potwierdź, że ftpuser2 go nie widzi.

Krok 1 - Utworzenie katalogu wirtualnego per-user (dla ftpuser1)

Otwórz **IIS Manager** > **Witryny** > wybierz swoją witrynę **FTPS**.

Rozwiń gałąź: FTPS > ftpuser1 (przykład: FTPS > ROL > ftpuser1)

Kliknij prawym przyciskiem na **ftpuser1** i wybierz:

Dodaj katalog wirtualny…

Ustaw: **Alias:** tools **Ścieżka fizyczna:** C:\FTPSHARED

Zatwierdź **OK**.

Efekt:

Tylko użytkownik *ftpuser1* otrzyma alias **/tools**, który wskazuje na wspólny katalog C:\FTPSHARED.

Krok 2 - Sprawdzenie uprawnień NTFS (ważne!)

Katalog C:\FTPSHARED ma ustawione NTFS:

Administratorzy > Pełna kontrola

SYSTEM > Pełna kontrola

GGFTPUsers > Odczyt/Wykonanie

To oznacza, że **obaj użytkownicy mogą czytać pliki**, ale **tylko ftpuser1 będzie widział alias „tools"**, bo: NTFS = kontrola danych, IIS FTP = kontrola *widoczności katalogów i aliasów*

Krok 3 - Test jako ftpuser1 (powinien widzieć „tools")

Otwórz FileZilla / WinSCP.

Połącz się: użytkownik: **ftpuser1**

Po zalogowaniu sprawdź listę katalogów.

Oczekiwane:

widzisz katalog tools

możesz wejść do: /tools/shared.txt i odczytać plik

Do oddania: screen listingu z widocznym tools.

Krok 4 - Test jako ftpuser2 (nie powinien widzieć „tools")

Połącz się jako: użytkownik: **ftpuser2**

Sprawdź listę katalogów.

Oczekiwane:

nie widzisz katalogu tools

próba wejścia ręcznego: wpisz w FileZilla: tools lub /tools

> powinna wyjść odpowiedź: **550 – The system cannot find the path specified** (lub odpowiednik w kliencie)

Do oddania: screen z błędem 550 lub brakiem aliasu.

Wniosek (który warto dopisać w ćwiczeniu)

Per-user virtual directories są **unikalne dla konkretnego użytkownika**, niezależne od: trybu izolacji (A/B/C/D), globalnych katalogów wirtualnych.

To IIS, nie NTFS, decyduje **co użytkownik „widzi"**. NTFS decyduje **do czego faktycznie ma dostęp**.

8. Pytania kontrolne (wnioski)

a. Który tryb izolacji jest najbardziej przewidywalny i dlaczego?
b. Jak globalne katalogi wirtualne wpływają na widoczność zasobów?
c. W jakim miejscu „broni" Cię NTFS, a w jakim IIS?
d. Kiedy użyłbyś trybu z globalnymi vdir w środowisku szkolnym/firmowym?