Ćwiczenie 1b. Dodawanie kontrolerów domeny do istniejącej domeny

Wstęp teoretyczny:

1. **Rozbudowa infrastruktury Active Directory**

Firma, w której pracujesz, zdecydowała się na rozbudowę swojej infrastruktury Active Directory (AD) o nowe kontrolery domeny. Aktualnie jedynym kontrolerem domeny jest system **DC1**, jednak konieczne jest dodanie nowych kontrolerów, aby zwiększyć niezawodność, wydajność oraz bezpieczeństwo całej sieci.

Kontrolery domeny – Kluczowe pojęcia:

- **Kontroler domeny (DC – Domain Controller)**: Serwer, który przechowuje i zarządza bazą danych Active Directory. Każdy kontroler może uwierzytelniać użytkowników oraz zarządzać uprawnieniami w domenie.
- **Globalny Katalog (GC – Global Catalog)**: Rola, którą pełni kontroler domeny, zawierająca podzbiór informacji z bazy AD. Globalny katalog jest niezbędny do wyszukiwania obiektów w wielu domenach oraz do logowania się do domeny.
- **DNS (Domain Name System)**: Usługa powiązana z AD, która umożliwia rozwiązywanie nazw domenowych na adresy IP.

Promowanie SERWERA na kontroler domeny (DC)

Jeśli serwer ma zostać kolejnym pełnym kontrolerem domeny w istniejącej infrastrukturze Active Directory. Oznacza to, że serwer będzie przechowywał pełną kopię bazy danych AD oraz pełnił rolę:

- **Serwera DNS**: Odpowiada za rozwiązywanie nazw dla zasobów domenowych.
- **Globalnego Katalogu (GC)**: Umożliwi użytkownikom i systemom w domenie szybkie wyszukiwanie obiektów oraz realizację zapytań o zasoby z innych domen.

Read-Only Domain Controller (RODC). RODC to specjalny typ kontrolera domeny, który przechowuje tylko kopię do odczytu bazy danych AD. Jest to szczególnie przydatne w sytuacjach, gdzie fizyczne zabezpieczenia serwerów są ograniczone, np. w zdalnych lokalizacjach. RODC ma kilka kluczowych cech:

- **Kopia do odczytu bazy AD**: Zabezpieczenie przed nieautoryzowanymi zmianami.
- **Ograniczone uwierzytelnianie**: Tylko wybrani użytkownicy mogą uwierzytelniać się na kontrolerze RODC.
- **Funkcje DNS i GC**: RODC może pełnić rolę serwera DNS i Globalnego Katalogu, jednak działa w trybie tylko do odczytu.

Role FSMO (Flexible Single Master Operation)

Każda infrastruktura Active Directory posiada pięć ról FSMO, które zapewniają, że niektóre operacje są realizowane przez jeden kontroler domeny w całej sieci lub domenie.

Role FSMO:

- **Schema Master**: Zarządza zmianami schematu AD w lesie.
- **Domain Naming Master**: Odpowiada za dodawanie/usuwanie domen w lesie.
- **RID Master**: Przydziela identyfikatory RID do tworzenia obiektów w domenie.
- **PDC Emulator**: Odpowiada za synchronizację czasu i kompatybilność z systemami pre-Windows 2000.
- **Infrastructure Master**: Zarządza aktualizacjami odnośników do obiektów między domenami.

Degradacja kontrolera domeny

Opcjonalnie, po przeniesieniu wszystkich ról FSMO można zdegradować z kontroler domeny. Oznacza to, że przestanie pełnić funkcję kontrolera domeny i zostanie przekształcony w zwykły serwer. Proces ten obejmuje:

- Usunięcie roli AD DS (Active Directory Domain Services).
- Usunięcie wpisów DNS i innych powiązanych zasobów.
- Aktualizcja ustawień sieciowych (DNS) na kontrolerach domeny i klientach

Zadanie 1

Wykonaj zadania

Firma w której jesteś zatrudniony postanowiła rozbudować infrastrukturę kontrolerów domeny. Aktualnie kontrolerem domeny jest system **DC1**.

Masz zrealizować następujące zadanie:

1. System **SVR1** powinien być kolejnym kontrolerem w domenie (DNS,GC)
2. System **SVR2** powinien być kontrolerem domeny typu RODC (DNS,GC)

Zapoznaj się z kontrolerem RODC

3. Ponieważ Kontroler domeny **DC1** mam docelowo zostać zdegradowany przenieś wszystkie role FSMO na **SVR1**, wypróbuj narzędzia GUI, wypróbuj PowerShell
4. Opcjonalnie zdegraduj **DC1**
5. Opcjonalnie dodaj **SVR4** jako kolejny Kontroler Domeny
6. Opcjonalnie zasymuluj sytuację gdy DC hostujący role FSMO uległ permanentnemu uszkodzeniu (wyłącz maszynę SVR1). Odzyskaj role (**Seize**) na SVR4 (opcja -**force** w komendzie powershell (Move-ADDirectoryServerOperationMasterRole)

Uzupełnienie

(PowerShell do przeniesienia ról):

```
Move-ADDirectoryServerOperationMasterRole -Identity “S2” -OperationMasterRole`
        DomainNamingMaster,PDCEmulator,RIDMaster,SchemaMaster,InfrastructureMaster
Move-ADDirectoryServerOperationMasterRole -Identity “S2” -OperationMasterRole  0,1,2,3,4
```

Gdzie:

DCEmulator	0
RIDMaster	1
InfrastructureMaster	2
SchemaMaster	3
DomainNamingMaster	4

repadmin /syncall DC1 /AeD - wymuszenie replikacji