Naprawa relacji zaufania dla komputera stacja w domenie rol00.edu.pl

Krok 1: Reset konta komputera w domenie

Na kontrolerze domeny (Windows Server 2019, np. *_dc2019):

1. Zaloguj się jako Administrator.
2. Uruchom Active Directory Users and Computers.
3. Przejdź do kontenera Computers.
4. Znajdź konto komputera stacja.
5. Kliknij prawym przyciskiem myszy i wybierz Reset Account.
6. Potwierdź operację.

Krok 2: Naprawa kanału zabezpieczeń na kliencie (Windows 11)

Na komputerze stacja:

1. Zaloguj się lokalnie jako Administrator (konto lokalne, np. .\Admin).
2. Uruchom Windows PowerShell jako Administrator.
3. Wpisz polecenie:

```
Test-ComputerSecureChannel –Repair -Credential rol00\Administrator
```

4. Podaj hasło: zaq1@WSX.

Krok 3: Restart i test logowania

1. Zrestartuj komputer stacja.
2. Spróbuj zalogować się jako użytkownik domenowy, np. IS\Administrator.

Zalety podejścia do naprawy relacji zaufania komputera stacja w domenie rol00.edu.pl według opisanych kroków:

Zalety podejścia: Reset konta + Test-ComputerSecureChannel

1. Bezpieczne i kontrolowane działanie

- Reset konta komputera w domenie nie usuwa danych ani nie wymaga reinstalacji systemu.
- Operacja jest wykonywana przez administratora domeny, co zapewnia kontrolę nad procesem.

2. Brak konieczności odłączania od domeny

- Nie trzeba przełączać komputera do grupy roboczej i ponownie go dodawać do domeny.
- Unika się restartów i potencjalnych problemów z profilami użytkowników.

3. Szybkość i prostota

- Polecenie PowerShell Test-ComputerSecureChannel –Repair jest szybkie i skuteczne.
- Wymaga tylko jednego restartu po naprawie.

4. Zachowanie istniejących ustawień

- Komputer zachowuje nazwę, SID, członkostwo w domenie i przypisane polityki GPO.
- Nie ma potrzeby ponownej konfiguracji profilu użytkownika ani aplikacji.

5. Możliwość automatyzacji

- Proces można zautomatyzować w skryptach PowerShell lub wdrożyć jako część procedury naprawczej w pracowni.

6. Zgodność z praktykami administracyjnymi

- Metoda jest zgodna z dokumentacją Microsoft i stosowana w środowiskach produkcyjnych.

Wady podejścia: Reset + Test-ComputerSecureChannel

1. Wymaga lokalnego konta administratora

- Jeśli konto .\Admin jest wyłączone lub użytkownik nie zna hasła, nie można wykonać naprawy.
- W środowiskach z ograniczonym dostępem lokalnym może to być problematyczne.

2. Brak interfejsu graficznego

- Brak wizualnego potwierdzenia może powodować niepewność co do efektu działania.

3. Nie rozwiązuje problemów z replikacją lub DNS

- Jeśli problem z relacją zaufania wynika z błędów replikacji AD, DNS lub SID, samo Test-ComputerSecureChannel może nie wystarczyć.
- W takich przypadkach konieczne są dodatkowe działania administracyjne.

4. Możliwość błędnego użycia polecenia

- Wpisanie błędnych danych uwierzytelniających (np. złej domeny lub loginu) może pogłębić problem.
- Brak komunikatu o sukcesie może wprowadzać w błąd.

5. Brak pełnej automatyzacji

- Wymaga ręcznego uruchomienia PowerShell i wpisania polecenia.
- Nie nadaje się do masowego naprawiania wielu komputerów bez dodatkowych skryptów.

6. Nie przywraca ustawień GPO ani profili użytkowników

- Jeśli relacja zaufania została zerwana na poziomie SID lub profilu, użytkownik może mieć problemy z dostępem do swojego środowiska po naprawie.

Naprawa relacji zaufania w GUI (Windows 11)

Odłączenie i ponowne podłączenie do domeny

1. Zaloguj się lokalnie jako .\Admin.
2. Otwórz:

- Panel sterowania > System > Zaawansowane ustawienia systemu > zakładka Nazwa komputera.
- Lub użyj skrótu Win + Pause/Break > kliknij Zmień ustawienia.

3. Kliknij Zmień….
4. Wybierz Grupa robocza i wpisz np. WORKGROUP.
5. Zatwierdź zmiany i zrestartuj komputer.

6. Po restarcie ponownie przejdź do tego samego okna i wybierz Domena.
7. Wpisz nazwę domeny rol00.edu.pl, podaj dane konta domenowego rol00\Administrator i hasło zaq1@WSX.
8. Zatwierdź i zrestartuj komputer.

Zalety podejścia GUI (odłączenie i ponowne podłączenie do domeny)

1. Intuicyjność dla uczniów i początkujących
- Cały proces odbywa się w środowisku graficznym, bez potrzeby użycia PowerShell.
- Łatwy do pokazania na lekcji lub w pracowni.
2. Brak potrzeby znajomości poleceń
- Nie wymaga wpisywania komend ani znajomości składni PowerShell.
3. Pełna rekonfiguracja relacji z domeną
- Odłączenie i ponowne podłączenie resetuje SID komputera w domenie.
- Może rozwiązać problemy głębsze niż tylko zerwany kanał zabezpieczeń.
4. Możliwość zmiany nazwy komputera
- W trakcie procesu można zmienić nazwę komputera, jeśli jest taka potrzeba.
5. Widoczność efektów
- Użytkownik widzi komunikaty potwierdzające sukces operacji.

Wady podejścia GUI

1. Utrata powiązań z profilem użytkownika
- Po ponownym podłączeniu do domeny może zostać utworzony nowy profil użytkownika.
- Użytkownik może stracić dostęp do swoich danych na pulpicie, w dokumentach itp.
2. Wymaga dwóch restartów
- Jeden po odłączeniu od domeny, drugi po ponownym podłączeniu.
3. Potencjalne problemy z GPO
- Po ponownym podłączeniu mogą nie działać przypisane wcześniej zasady grupy (GPO), dopóki nie zostaną ponownie zsynchronizowane.
4. Możliwość błędów przy wpisywaniu danych
- Błędna nazwa domeny lub dane logowania mogą spowodować niepowodzenie operacji.
5. Brak automatyzacji
- Proces wymaga ręcznego wykonania kroków, nie nadaje się do masowego wdrażania.