

## Laboratorium 05A

**Temat:** Group Policy Object (GPO) - Podstawy

### Przywrót maszyny wirtualne po poprzednich ćwiczeniach

#### Scenariusz

Kontynuujesz pracę jako administrator w firmie „KEJA Corp”. Kierownik działu IT zlecił

wykonanie pewnych czynności związanych z GPO

### Zadania do wykonania

#### Zadanie 1

Zapoznaj się z funkcjonowaniem Group Policy. Zapoznaj się z tworzeniem i edytowaniem Obiektów GPO, z Blokowaniem dziedziczenia, z wymuszaniem Polis itp.

#### Zadanie 2

- Polityki w firmie dotyczące kont komputerów powinny zaczynać się od **C**\_
  - Polityki w firmie dotyczące kont użytkowników powinny zaczynać się od **U**\_
  - Polityka **Default Domain Policy** nie powinna być zmieniana - wyjątek stanowi polityka haseł i polityka blokowania kont po nieudanych próbach logowania.
  - Polityki w firmie dotyczące zarówno kont komputerów jak i użytkowników powinny zaczynać się od **A**\_ (polityki niepolecane)
  - **Nazwa polityki** powinna określać na co dana polityka ma wpływ
  - Zaleca się tworzenie osobnych polityk do niezależnych funkcjonalności.
1. Polityka haseł dla użytkowników domeny jest następująca:
    - Historia haseł 15
    - Maksymalny okres ważności hasła 30
    - Minimalny okres ważności hasła 2
    - Minimalna długość hasła 10
    - Hasła muszą spełniać wymogi co do złożoności
  2. Polityka blokowania konta: Po 3 nieudanych próbach konto powinno zostać trwale zablokowane. Licznik nieudanych prób ma się zresetować po 120 minutach.
  3. Poniższe ustawienia mają być **zawsze wdrażane** dla wszystkich komputerów w firmie
    - a. Always wait for the network at computer startup and logon
    - b. Default Logon domain: keja.msft
    - c. Logowania lokalne nie powinny być cache'owane na serwerach – innymi słowy każdorazowe logowanie wymaga uwierzytelnienia przez kontroler domeny.
    - d. Grupa Administratorów powinna dodawana do profilu przechodnich użytkowników (Add the Administrators security group to roaming user profiles)
    - e. Właściciel profili przechodnich nie powinien być sprawdzany (Do not check for user ownership of Roaming Profile Folders)

- f. Automatyczne wylogowywanie użytkowników po czasie 120 s. bezczynności(Interactive logon: Machine inactivity limit).
  - g. Wyłączanie dostępu do portów USB (All Removable Storage classes: Deny all access).
  - h. Ograniczenie dostępu do rejestru (Prevent access to the registry editing tools).
4. Poniższe ustawienia mają być **zawsze wdrażane** dla wszystkich użytkowników w firmie. Zakładamy że konta użytkowników znajdują się w OU=Users która znajduje się w OU KejaMain.
- i. Wyłączenie dostępu do Panelu sterowania i ustawień (Prohibit access to Control Panel and PC settings).
  - j. Ograniczenie dostępu do określonych dysków (np. dysku C: )( Hide these specified drives in My Computer)
  - k. Blokada dostępu do Menedżera zadań (Remove Task Manager).
  - l. Wyłączenie możliwości uruchamiania wybranych aplikacji ( np. cmd.exe, powershell.exe) (Don't run specified Windows applications).
  - m. Zablokowanie możliwości zmiany tapety (prevent changing desktop background).

### Testowanie ustawień

- Dla następujących użytkowników ma być włączony system starzenia się haseł: **ewa, ala, grzegorz** – włącz go używając np. AD Users and Computers lub PowerShell
- Przetestuj powyższe ustawienie. m.in. Spróbuj zalogować się na **SVR1** jako **ala**. Po zalogowaniu zmień hasło. – Udało się ?
- Zaloguj się jako Grzegorz po czym wyloguj się i spróbuj się kilkukrotnie zalogować z błędny hasłem.
- Przeprowadź inne testy.
- Sprawdź czy polityki zostały wdrożone zarówno na komputer

### Zadanie 3

2. Server **SVR1** został przeniesiony do **Katowic**, skoryguj jego lokalizację w **AD** (jeśli nie ma odpowiedniego OU to je utwórz)
3. Dla wszystkich serwerów w firmie należy wprowadzić następujące ustawienie (przygotuj odpowiednie polityki i je udokumentuj)
  - a. Zarządzać serwerami powinni jedynie:
    - administrator lokalny
    - administratorzy domenowi
    - członkowie grupy IT

**ustawienie to powinno nadpisać ewentualne inne polityki.**
  - b. Prawo do **wyłączania komputera** oraz **logowania lokalnego**, oraz możliwość łączenia się przed **RDP** mają tylko wskazani w poprzednim punkcie użytkownicy
  - c. Użytkownicy powinni być powiadomiani 7 dni przed wygaśnięciem hasła.
  - d. Na wszystkich serwerach ma zostać wyłączone serwis „windows audio”.

## Testowanie ustawień: Przetestuj powyższe ustawienia na serwerze SVR1

### Zadanie 4

Komputer **SVR2** w ramach tego laboratorium pełni rolę komputera klienckiego

1. Komputer **SVR2** został przeniesiony do **Opola**, skoryguj jego lokalizację w **AD**.
2. Dla wszystkich komputerów klienckich mają zostać wdrożone następujące ustawienia
  - a. Zarządzać komputerami klienckimi powinni jedynie:
    - administrator lokalny
    - administratorzy domenowi
    - członkowie grupy IT
  - b. Serwisy
    - Windows Remote Management WinRm powinien być włączony automatycznie
    - Microsoft iSCSI Initiator powinien być włączony automatycznie
3. Dla komputerów klienckich w **Opolu** lokalnie logować mogą się członkowie lokalnej grupy administratorów i działu **HR**.
4. Dla wszystkich pracowników działu **HR** powinny być wdrożone następujące ustawienia
  - a. Zabronienie dostępu do Control Panel i PC Settings
  - b. ScreenSaver: Włącza się po 2 minutach bezczynności, wymaga podania hasła aby odblokować komputer
  - c. Pracownicy nie powinni mówić zmieniać wyglądu swojego Windowsa (desktop,Theme itp.)
  - d. Na dysku C: powinien być zawsze dostępny folder TEMPFILE

### Zadanie 5

Przygotowujesz się do wdrożenia serwera **SVR3**. Server fizycznie będzie znajdować się w Opolu. Utwórz jego konto w odpowiedniej OU, a następnie dodaj serwer do domeny ( pamiętaj o zmianie nazwy na **SVR3** , konfiguracji IP , jego adres to 172.16.0.13/16)

Po wdrożeniu upewnij się że odpowiednie GPO zostały wdrożone.

**Cele dydaktyczne.** Po zakończeniu ćwiczenia powinieneś umieć:

- Tworzyć i edytować Obiekty GPO
- Wyszukiwać niezbędne ustawienia w obiektach GPO
- Decydować o kolejności wdrażania GPO