**Ćwiczenie 9: Konfigurowanie polisy – Ustawienia preferencji**

**Zadanie 12: Ustaw dla polisy jednostki organizacyjnej Gdansk, jako preferencje użytkownika:**

* **Ustawienie zabezpieczeń strefy internetowej jako maksymalnych**
* **Dodanie nowej drukarki sieciowej wskazującej na drukarkę zainstalowaną na kontrolerze domeny**
* **Włączenie na komputerach funkcjonalności hibernacji, gdzie zamknięcie klapy laptopa powoduje jej wykonanie**
* **Utworzenie na stacjach roboczych konta lokalnego o nazwie menadzerFinanse**

**Zaloguj się na komputerze klienta jako administrator i sprawdź czy pojawiła się drukarka, konto lokalne menedzerFinanse oraz w przeglądarce internetowej zostały wdrożone ustawienia?**

**Zaloguj się na komputerze klienta jako analitykMK i sprawdź czy pojawiła się drukarka, konto lokalne menedzerFinanse oraz w przeglądarce internetowej zostały wdrożone ustawienia? Zdefiniuj analogiczne ustawienia jako preferencje komputera. *Jaki jest teraz efekt?***

**Sposób wykonania:**

* Konsola Group Policy Management / Operacja na polisie **Edit**
* *Lokalizacje*:
	+ Preferencje dla konta komputera – Computer Configuration / Policies / **Preferences**
	+ Preferencje dla konta użytkownika - User Configuration /Policies / **Preferences**

**Szczegółowy tutorial:**

1. Uruchom obie maszyny wirtualne jeśli nie są one uruchomione.
2. W maszynie wirtualnej serwera przejdź do konsoli **Server Manager** -> menu **Tools** -> konsola **Group Policy Management (GPM).**
3. W konsoli **GPM** przejdź do domeny **zsl.pl** -> jednostka organizacyjna **Polska/Gdansk.**
4. Zaznacz link do polisy o nazwie**OddzialGdansk** i wybierz operację **Edit.**
5. Pojawi się konsola **Group Policy Management Editor**.
6. Przejdź do sekcji **User Configuration / Preferences / Control Panel Settings**
7. Wybierz na sekcji Internet Settings operację New / Internet Explorer 5 and 6
8. Na zakładce **Security** dla **Internet** ustaw zabezpieczenia jako **Hight**. 
9. Wybierz na sekcji **Printer** operację **New / Shared Printer**.
10. Wskaż jako drukarkę drukarkę udostępnioną w domenie **drukarkaLokalna1**… oraz akcję **Create**. 
11. W sekcji **Power Options** wybierz operację **New / Power Options (XP**) i zaznacz zgodnie z obrazkiem poniżej. 
12. W sekcji Local Users and Accounts wybierz operację **New / User Account**.
13. Zdefiniuj konto zgodnie z rysunkiem poniżej. 
14. Na komputerach serwera i klienta wymuś odświeżenie polisy wchodząc do konsoli **Command Prompt** (Wiersz Polecenia) i wprowadzając polecenie **gpupdate / force**.
15. Zrestartuj maszynę klienta.
16. Zaloguj się na komputerze klienta jako **administrator** i sprawdź czy pojawiła się drukarka, konto lokalne menedzerFinanse (W systemie klienta kliknij na przycisk **Start** -> **Mój komputer** -> prawy przycisk myszki i operacja **Zarządzaj**. Rozwiń folder **Użytkownicy i grupy lokalne** -> **Konta…**) oraz w przeglądarce internetowej (Panel sterowania / **Opcje internetowe** / **zakładka Zabezpieczenia**) ***zostały wdrożone ustawienia***?
17. Zaloguj się na komputerze klienta jako ***analitykTwojeInicjały*** i ***sprawdź czy pojawiła się drukarka, konto lokalne menedzerFinanse oraz w przeglądarce internetowej zostały wdrożone ustawienia?***
18. Zdefiniuj analogiczne ustawienia jako preferencje komputera. ***Jaki jest teraz efekt?***

**Zadanie 13**: **Włącz zasady inspekcji dla domeny zsl.pl dla audytu logowania. Kilkakrotnie podaj błędne hasło jako menedzerTwojeInicjały. Sprawdź czy zarejestrowane zostały stosowne zdarzenia.**

**Sposób wykonania:**

* *Zarządzanie polisami* - konsola Group Policy Management / Operacja na polisie **Edit**
* *Lokalizacja* - Computer Configuration \ (Policies od 2008 Windows Server) \ Windows Settings \ Security Settings \ Audit Policies – polisa **Audit account logon events**
* *Odblokowanie konta* - zależy od ustawień polisy: automatyczne lub ręcznie (właściwości konta, zakładka Account)
* Sprawdzenie logów audytu - konsola **Event Viewer**

**Szczegółowy tutorial:**

1. Uruchom obie maszyny wirtualne jeśli nie są one uruchomione.
2. W maszynie wirtualnej serwera przejdź do konsoli **Server Manager** -> menu **Tools** -> konsola **Group Policy Management (GPM).**
3. W konsoli GPM przejdź do domeny zsl.pl.
4. Zaznacz link do polisy o nazwie **Default Domain Policy** i wybierz operację **Edit**. ***Czym różni się zasięg implementacji polis Default Domain Controlers Policy oraz Default Domain Policy?***
5. Pojawi się konsola **Group Policy Management Editor**.
6. Przejdź do sekcji **Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Local Policies \ Audit Policy**
7. Zdefiniuj ustawienia zgodnie z rysunkiem poniżej. 
8. Na komputerach serwera i klienta wymuś odświeżenie polisy wchodząc do konsoli **Command Prompt** (Wiersz Polecenia) i wprowadzając polecenie **gpupdate / force**
9. Zrestartuj maszynę klienta.
10. Na komputerze klienta 2-krotnie podaj błędne hasło jako menedzerTwojeInicjały.
11. W maszynie wirtualnej serwera przejdź do konsoli **Server Manager** -> menu **Tools** -> konsola **Event Viewer**.
12. Przejdź do sekcji **Security** i znajdź ostatni wpis dla **Audit failure**. Zapoznaj się z jego treścią. ***Czy informacje o błędnym logowaniu zostały zawarte*?**

**Zadanie 14**: **Włącz zasady inspekcji dla domeny dla audytu dostępu do katalogów i plików. Ustaw dla katalogu c:\zasoby\Polska monitorowanie dostępu w zakresie jego usuwania. Jako menedzerTwojeInicjaly spróbuj skasować ten katalog. Sprawdź zarejestrowane zdarzenia.**

**Sposób wykonania**:

* *Zarządzanie polisami* - konsola Group Policy Management / Operacja na polisie **Edit**
* *Włączenie audytu* - Computer Configuration \ (Policies w 2008 Server) \ Windows Settings \ Security Settings \ Audit Policies – polisa **Audit object access**
* *Ustawienie audytu dla folderu* - po włączeniu audytu każdy monitorowany obiekt musi mieć indywidualnie zdefiniowane śledzone zdarzania. Sposób ustawienia:
	+ Właściwości folderu \ zakładka **Security** \ Ustawienia zaawansowane (przycisk **Advanced**) \ zakładka **Auditing**
	+ Dodanie wpisu – przycisk **Add**, wskazanie:
		- kont użytkowników i grup, które śledzenie ma obejmować
		- zdarzeń, które mają być śledzone
		- typu śledzenia: sukces, porażka
* *Sprawdzenie logów audytu* - konsola **Event Viewer**

**Szczegółowy tutorial:**

1. Uruchom obie maszyny wirtualne jeśli nie są one uruchomione.
2. W maszynie wirtualnej serwera przejdź do konsoli **Server Manager** -> menu **Tools** -> konsola **Group Policy Management (GPM).**
3. W konsoli **GPM** przejdź do domeny **zsl.pl**.
4. Zaznacz link do polisy o nazwie **Default Domain Policy** i wybierz operację **Edit**.
5. Pojawi się konsola **Group Policy Management Editor.**
6. Przejdź do sekcji **Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Local Policies \ Audit Policy**
7. Dla **Audit object access** włącz audyt dla **Success** (na wypadek gdyby komuś udało się skasować zasób pomimo, że nie powinien mieć do tego prawa) i **Failure**.
8. Wejdź we właściwości folderu **c:\zasoby\Polska**.
9. Na zakładce **Security** kliknij na przycisk **Advanced.**
10. Przejdź na zakładkę **Auditing**.
11. Kliknij na przycisk **Add**.
12. W oknie **Auditing Audit for Polska** kliknij na odnośnik **Select a principal**.
13. Wskaż grupę **Everyone**.
14. Ustaw audyt dla sukcesu i porażek dla folderu i „pod elementów”. W ten sposób będzie miało miejsce logowanie informacji również o działaniach w podfolderach.
15. Kliknij na odnośnik **Show Advanced Permissions** i zaznacz monitorowanie usunięć. 
16. Zatwierdź ustawienia. W przypadku problemów z wdrożeniem audytu dla wszystkich podfolderów kliknij na **Continue**. ***Jaka jest tego przyczyna?***
17. Na komputerze serwera wymuś odświeżenie polisy wchodząc do konsoli **Command Prompt** (Wiersz Polecenia) i wprowadzając polecenie **gpupdate / force.**
18. Na komputerze klienta zaloguj się jako **menedzerTwojeInicjały**.
19. W polu **Start / Uruchom** podaj adres folderu udostępnionego
 **\\kontroler.zsl.pl\materialy$.**
20. Spróbuj skasować katalog **Polska**, jak i któryś z jego podkatalogów.
21. W maszynie wirtualnej serwera (zdarzenia są zawsze zawarte w logach komputera, na którym znajduje się monitorowany zasób) przejdź do konsoli **Server Manager** -> menu Tools -> konsola **Event Viewer**.
22. Przejdź do sekcji **Security**.
23. W związku z tym, że liczba wpisów może być na sekcji **Security** wybierz operację **Filter ….** 
24. Wypełnij dane filtrowania zgodnie z ze zrzutem poniżej. 
25. Posortuj dane po kolumnie **Keywords**, tak aby na początku były wpisy **Audit Failure**.
26. Wejdź we właściwości pierwszego z wpisów i dokładnie się z nim zapoznaj. ***Czy informacje o próbie usunięcia katalogu Polska lub jego podkatalogu są w nim zawarte?***

**Zadanie 15:** **Sprawdź jakie są ustawienia dla polis: Default Domain Policy i Default Domain Controlers Policy. Gdzie mają one zastosowanie? Wyeksportuj dane polisy domenowej jako stronę HTML.**

**Sprawdź jakie będzie mieć ustawienia polis użytkownik analitykTwojeInicjały jeśli zaloguje się na komputerze Klient.**

**Sposób wykonania:**

* *Zarządzanie polisami* - konsola Group Policy Management / Operacja na polisie **Edit**
* *Sprawdzenie ustawień polisy* - Właściwości polisy w sekcji **Group Policy Objects** \ zakładka **Settings**
* *Sprawdzenie ustawień polisy w kontkretnym konkteście* - konsola Group Policy Management / sekcja **Group Policy Modeling** lub **Group Policy Result**. ***Czym one się od siebie różnią?***

**Szczegółowy tutorial:**

1. W maszynie wirtualnej serwera przejdź do konsoli **Server Manager** -> menu **Tools** -> konsola **Group Policy Management (GPM).**
2. W konsoli **GPM** przejdź do domeny zsl.pl.
3. Zaznacz link do polisy o nazwie **Default Domain Policy** i przejdź na zakładkę **Settings**.
4. Kliknij na odnośnik **Show all** i zapoznaj się z informacjami, które zawiera raport. ***Jakie z ustawień uznałbyś za kluczowe (czyt. znacząco wpływające na korzystanie z domeny)?***
5. Analogicznie zaznacz link do polisy o nazwie **Default Domain Controlers Policy** i przejdź na zakładkę **Settings**. Kliknij na odnośnik **Show all** i zapoznaj się z informacjami, które zawiera raport.
6. Powróć do sprawdzenia ustawień polisy **Default Domain Policy**.
7. Na obszarze raportu kliknij prawym przyciskiem myszy i wybierz operację **Save report …**
8. Zapisz raport jako stronę **html**.
9. Otwórz raport z lokalizacji zapisania.