pasja-informatyki.pl

Sieci komputerowe – Windows Server #3

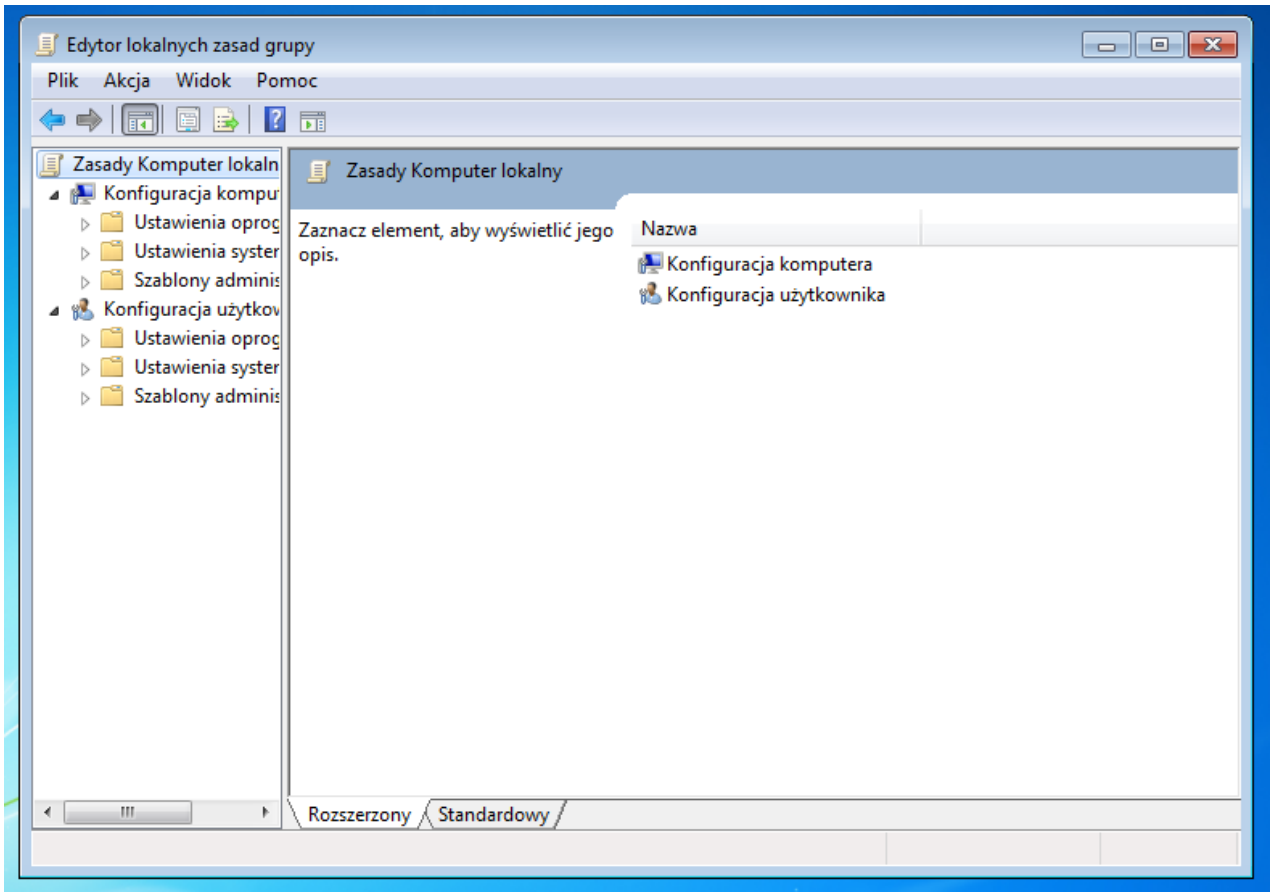
Zasady Grupy (ang. Group Policy)

Damian Stelmach

Spis treści

Zasady Grupy (ang. **Group Policy**) to **zbiór reguł i ustawień** określających zakres działania komputera oraz użytkowników danego komputera. Są to ustawienia definiujące do jakich elementów systemu, takich jak na przykład **panel sterowania**, użytkownik komputera ma dostęp, a do jakich nie. **Z jakich aplikacji** może korzystać, a z jakich nie może, a także czy może instalować i usuwać **urządzenia peryferyjnie** i korzystać z **dysków przenośnych**. Zbiór reguł, które możemy zdefiniować jest ogromny, do dyspozycji mamy grubo ponad **2000** różnego rodzaju ustawień i konfiguracji. Zasady grupy są nieodłącznym elementem **usługi Active Directory** i wraz z nią dają największe możliwości. Korzystając z Zasad Grupy za pośrednictwem Active Directory konfigurujemy je na serwerze i decydujemy dla jakich komputerów oraz użytkowników mają zostać wdrożone. Wszystkie ustawienia przechowywane są w tak zwanych **Obiektach Zasad Grupy** (ang. **Group Policy Object**).

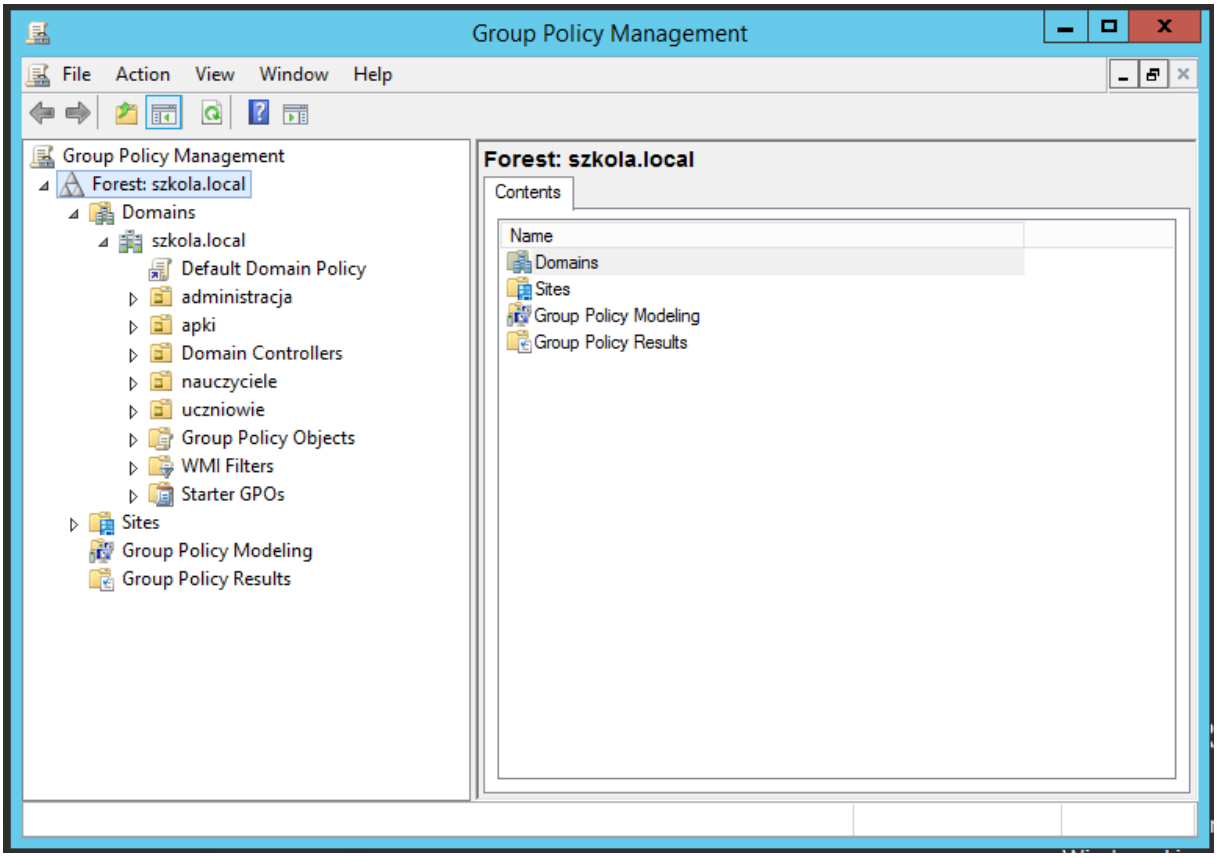
Istnieją również **zasady lokalne**, które można skonfigurować na **każdym komputerze z systemem Windows**, nawet jeśli nie należy do domeny, wówczas jednak nie mamy możliwości ich wdrażania zdalnego, a co więcej ilość opcji konfiguracyjnych jest znacznie mniejsza. Lokalny edytor zasad grupy uruchomić można wybierając ***START*** i wprowadzając polecenie ***gpedit.msc***



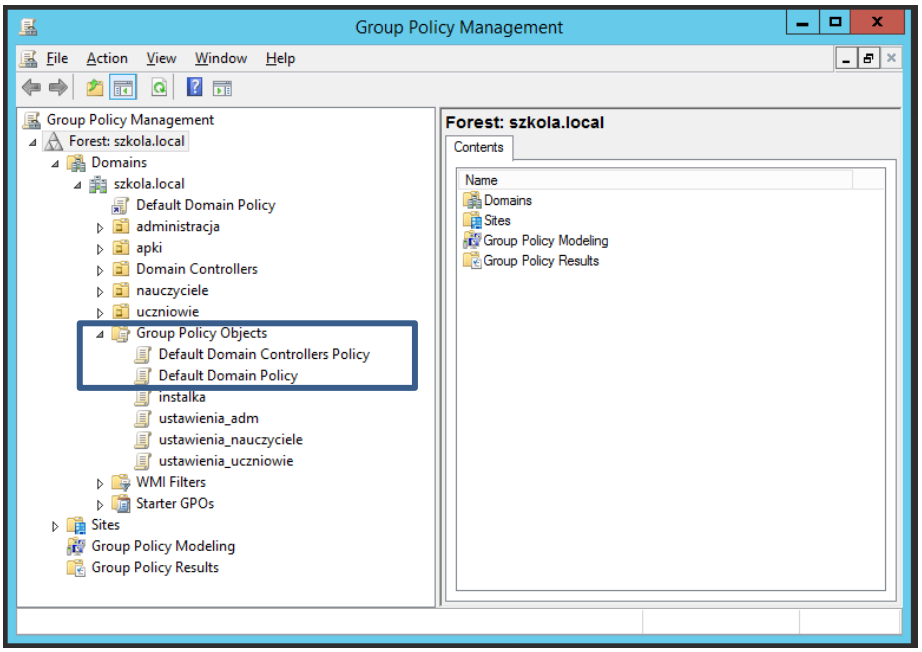
Edytor zasad na serwerze, dostępny będzie po wpisaniu polecenia ***gpmc.msc*** w oknie uruchamiania programu (***klawisz Windows + R***). Można go również uruchomić wybierając:

- dla **Windows Server 2012 R2:**
  Menadżer Serwera -> Narzędzia (Tools) -> Edytor Obiektów Zasad Grupy (Group Policy Managment)
- dla **Windows Server 2008 R2:**
  START -> Narzędzia Administracyjne (Administrative Tools) -> Edytor Obiektów Zasad Grupy

Okno zarządzania Zasadami Grupy podzielone jest na **dwa główne obszary**: obszar po lewej, zwiera domeny oraz jednostki organizacyjne w nich zawarte, obszar po prawej natomiast pozwala na modyfikację zasad oraz ich opcji:

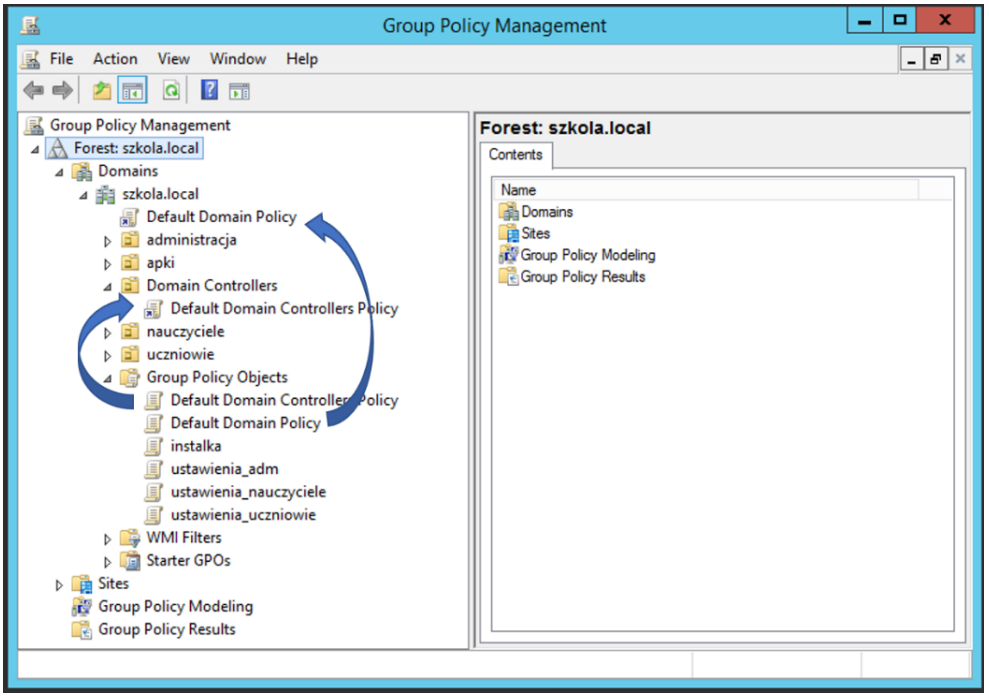


Wszystkie obiekty przygotowane dla naszej domeny, przechowywane są w **zbiorczym kontenerze** o nazwie **Obiekty Zasad Grupy** (ang. **Group Policy Objects**). Zawiera on oprócz zasad przygotowany przez administratora również **dwie zasady**, które zostały utworzone przez system podczas promowania serwera do roli kontrolera domeny. Te obiekty to: **Domyśle Zasady Kontrolerów Domeny** (ang. **Default Domain Controllers Policy**) oraz **Domyślne Zasady Domeny** (ang. **Default Domain Policy**):

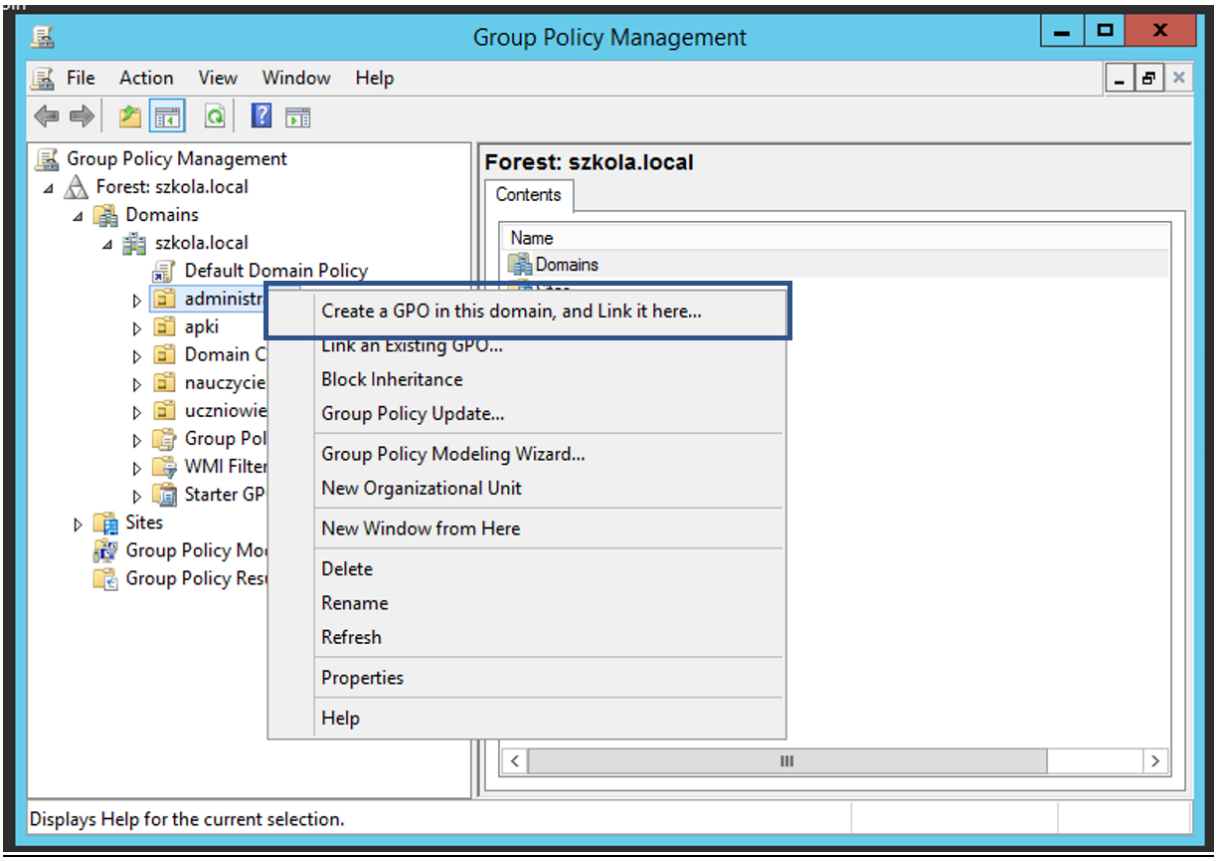


Zawierają one **wstępnie skonfigurowane zasady** (m.in. zasady haseł dla kont użytkowników) obowiązujące **wszystkie obiekty** w domenie. Można oczywiście je zmodyfikować, tak jak zrobiliśmy to poprzednio.

Aby zasady mogły oddziaływać na daną **jednostkę organizacyjną** czy **też domenę** wymagany jest do niej **odnośnik (link)**. Działa to tak, że sama zasada przechowywana jest w **zbiorczym kontenerze**, a w danej domenie czy jednostce znajduje się tylko **link do tej zasady**:



Aby uniknąć takiej sytuacji, w której utworzymy zasadę, skonfigurujemy ją odpowiednio i zapomnimy podlinkować w odpowiednim miejscu, możemy skorzystać z **opcji automatycznego linkowania**. Dostępna jest ona z poziomu menu kontekstowego. Wystarczy kliknąć PPM w jednostkę organizacyjną lub domenę, dla której chcemy utworzyć zasadę i wybrać opcję ***Utwórz Obiekt Zasady w Domenie i Podłącz Link Tutaj (ang. Create a GPO in this domain nad Link it here…)***



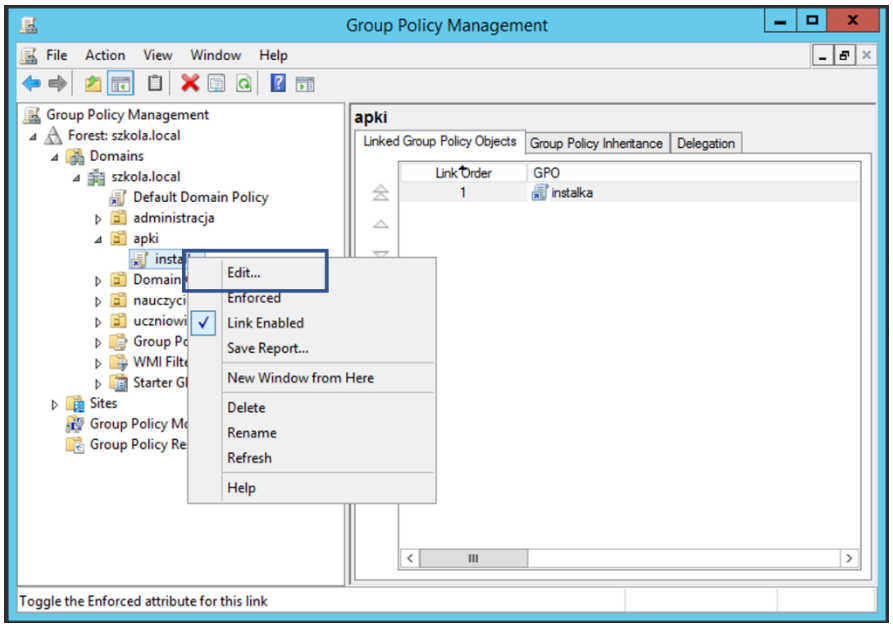
Wówczas zostanie utworzony obiekt zasady w **zbiorczym kontenerze**, a danym miejscu pojawi się **link** do niego.

Obiekty Zasad Grupy można tworzyć **lokalnie**, jak również **z poziomu serwera** dla **lokacji**, poszczególnych **domen**, jak również **jednostek organizacyjnych**. Pojawia się zatem pytanie, **w jaki sposób oraz w jakiej kolejności przetwarzane są zasady?**

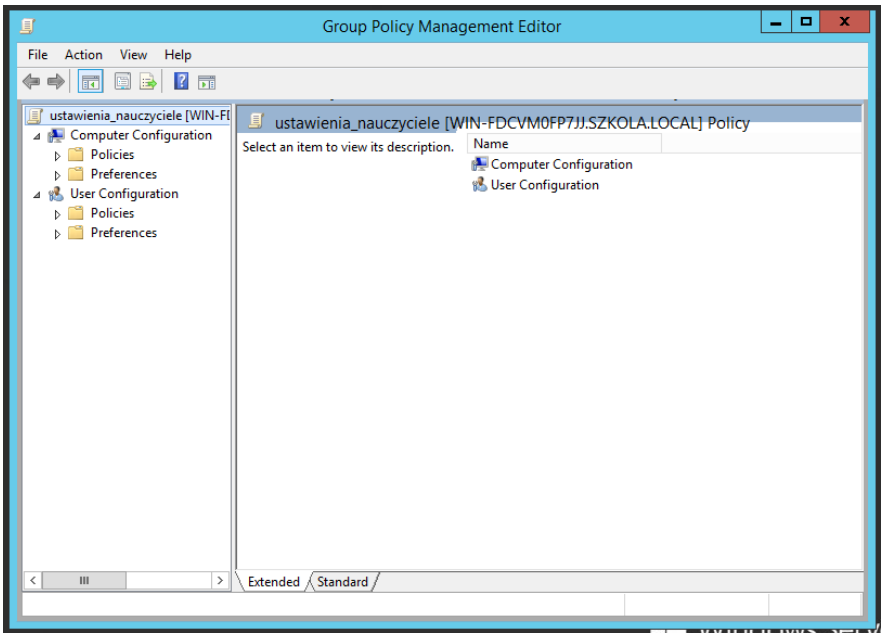
Wyobraźmy sobie sytuacje, że **dla całej domeny** (a właściwie użytkowników tej domeny) **zabroniliśmy dostępu do panelu sterowania**. **Konkretnej jednostce organizacyjnej** z kolei, **zezwoliliśmy na obsługę panelu**. Jak zatem będzie przedstawiała się kwestia dostępu dla użytkowników należących do tej jednostki organizacyjnej? **Otóż będą oni mogli korzystać z panelu** – dlaczego? Dlatego, że w p**ierwszej kolejności przetwarzane są zasady przypisywane dla jednostek organizacyjnych** i to one mają pierwszeństwo. Nawet jeśli zabronimy czegoś dla całej domeny, a zezwolimy dla jednostki to te ustawienia będą miały **priorytet**. Kolejność przetwarzania zad przedstawia poniższy diagram.

Kolejna ważna kwestia to **wdrażanie zasad**. Po tym jak dokonamy modyfikacji w obiektach zasad powinna nastąpić ich **aktualizacja**, zarówno na **serwerze**, jak również na **kliencie**. Zasady aktualizowane są **automatycznie**, co pewien czas, jednak po każdej modyfikacji obiektów warto wykonać taką **aktualizację ręcznie**. Służy do tego polecenie ***gpupdate /force*** wprowadzane w konsoli systemowej. Polecenie wykonać można na serwerze oraz na kliencie. Wówczas mamy pewność, że wszystkie zamiany, których dokonaliśmy zostaną wprowadzone od razu. Jeśli chodzi o samych klientów to aktualizacja zasad odbywa się **również podczas ponownego logowania** do systemu oraz po upływie określonego czasu. Czas ten wynosi między **90**, a **120 minut**.

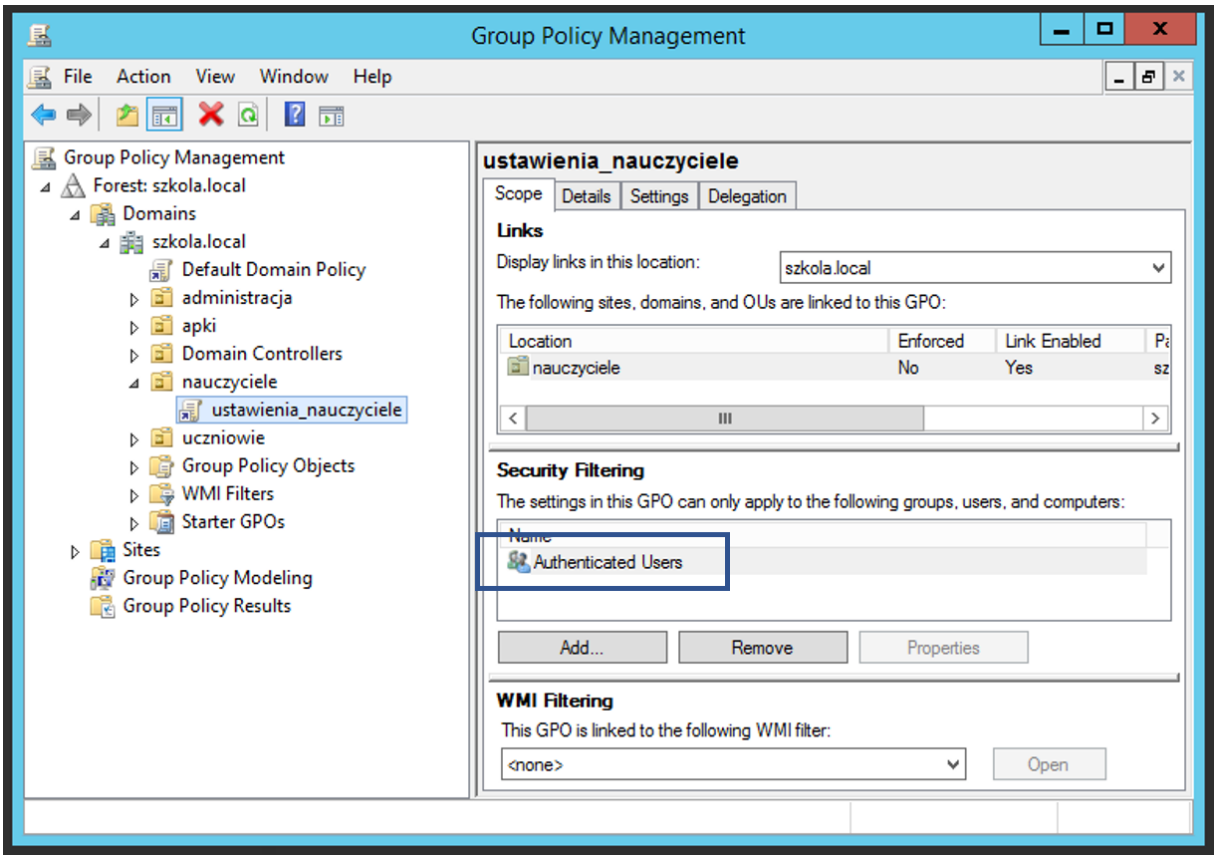
Utworzona zasada z linkiem to dopiero początek. Zasadę trzeba teraz „uzbroić" w odpowiednie ustawienia. Aby uruchomić okno edycji zasady klikamy PPM, albo w zasadę, albo w link i wybieramy ***Edytuj (ang. Edit)***



Uruchomione zostanie **okno edycji zasad**, zawierające ustawienia konfiguracyjne użytkowników i komputerów. **Ustawienia dla komputerów** dotyczą **urządzeń** bez względu na to jaki użytkownik się zaloguje, natomiast **ustawienia użytkownika** dotyczą **użytkowników** bez względu na to do jakiego komputera się zalogują. Dotyczy to oczywiście **tylko jednostek organizacyjnych**, dla których przygotowywane są zasady.



Skonfigurowane zasady domyślnie działać będą dla **wszystkich użytkowników** (lub komputerów – w zależności od wybranej konfiguracji) w danej **jednostce organizacyjnej**. Można to oczywiście zmienić, usuwając z listy ***Użytkowników Uwierzytelnionych (ang. Authenticated Users)***. Wówczas dodając do tej listy określonych **użytkowników** czy też **grupy** (oczywiście muszą być oni przypisanie do jednostki, na którą nałożyliśmy zasadę), możemy samodzielnie decydować, dla których z nich obowiązywały będą zasady.



Poniżej znajdziecie **kilkanaście przykładowych ustawień**, które ograniczają użytkownikom dostęp do poszczególnych elementów systemu operacyjnego oraz zmieniają konkretne ustawienia (opis tylko w języku angielskim):

1. Blokada całego Panelu Sterowania:

   User Configuration -> Administrative Templates -> Control Panel -> Prohibit access to Control Panel and PC settings -> ENABLED

2. Ukrycie poszczególnych elementów w Panelu Sterowania:

   User Configuration -> Administrative Templates -> Control Panel -> Hide specified Control Panel items -> ENABLED *(po włączeniu opcji wprowadzamy nazwy elementów, które chcemy zablokować)*

3. Blokada ustawień ekranu:

   User Configuration -> Administrative Templates -> Control Panel -> Display -> Disable the Display Control Panel -> ENABLED

4. Blokada zmiany tapety:

   User Configuration -> Administrative Templates -> Control Panel -> Personalization -> Prohibit changing desktop background -> ENABLED

5. Blokada usuwania drukarek:

   User Configuration -> Administrative Templates -> Control Panel -> Printers -> Prevent deletion of printers -> ENABLED

6. Wyłączenie ikon Komputer, Sieć, Kosz z pulpitu:

   User Configuration -> Administrative Templates -> Desktop-> Hide and disable all items on the desktop -> ENABLED

7. Ustawienie konkretnej tapety pulpitu:

   User Configuration -> Administrative Templates -> Desktop-> Desktop -> Desktop Wallpaper -> ENABLED *(po włączeniu tej opcji podajemy ścieżkę do konkretnej tapety)*

8. Usunięcie elementu *Uruchom* z Menu Start:

   User Configuration -> Administrative Templates -> Start Menu and Taskbar -> Remove Run menu form Start Menu -> ENABLED

9. Usunięcie elementu *Zablokuj komputer* po wciśnięciu CTRL + ALT + DEL:

   User Configuration -> Administrative Templates -> System -> Ctrl+Alt+Del Options -> Remove Lock Computer -> ENABLED

10. Usunięcie elementu *Wyloguj* po wciśnięciu CTRL + ALT + DEL:

    User Configuration -> Administrative Templates -> System -> Ctrl+Alt+Del Options -> Remove Logoff -> ENABLED

11. Blokada odczytu danych z dysków zewnętrznych:

    User Configuration -> Administrative Templates -> System -> Removable Storage Access -> Removable Disks: Deny read access -> ENABLED

12. Limit wielkości profilu użytkownika:

    User Configuration -> Administrative Templates -> System -> User Profiles -> Limit profile size -> ENABLED *(po włączeniu tej opcji określamy wielkość maksymalną profilu)*

13. Blokada dostępu do edycji rejestru:

    User Configuration -> Administrative Templates -> System -> Prevent access to registry edition tools -> ENABLED

14. Blokada dostępu do wiersza poleceń:

    User Configuration -> Administrative Templates -> System -> Prevent access to command prompt -> ENABLED

15. Uruchamianie tylko wybranych aplikacji:

    User Configuration -> Administrative Templates -> System -> Run only specified Windows applications -> ENABLED *(po włączeniu tej opcji podajemy nazwy plików uruchomieniowych aplikacji)*

16. Blokada wyświetlania wybranych partycji w Eksploratorze Windows:

    User Configuration -> Administrative Templates -> Windows Components -> File Explorer -> Hide these specified drivers in My Computer *(po włączeniu tej opcji wybieramy właściwe ustawienia)*

To oczywiście niewielki wycinek wielkich możliwości konfiguracyjnych jakie dają **Zasady Grupy**. Ustawień w samych **Szablonach Administracyjnych** (ang. **Administrative Templates**) jest ponad **150**0. Do tego dochodzą jeszcze **Preferencje Zasad** (ang. **Preferences**), **Ustawienia Oprogramowania** (ang. **Software Settings**) oraz **Ustawienia Windows** (ang. **Windows Settings**). Za ich pomocą można, np. **zdalnie instalować oprogramowanie**, **mapować drukarki** i **foldery**, czy **automatycznie kopiować na serwer zawartość katalogów z profili użytkowników**. Zachęcam do samodzielnej „zabawy" z Zasadami Grupy i testowanie poszczególnych ustawień.