Zarządzanie zasadami grupy

Dołączanie stacji roboczych do domeny ma jeszcze jedną niewątpliwą zaletę – możliwość zarządzania zasadami grupy dla poszczególnych użytkowników bądź grup użytkowników czy komputerów (w zasadzie każdemu obiektowi w domenie można przypisać odpowiednie zasady grupy).

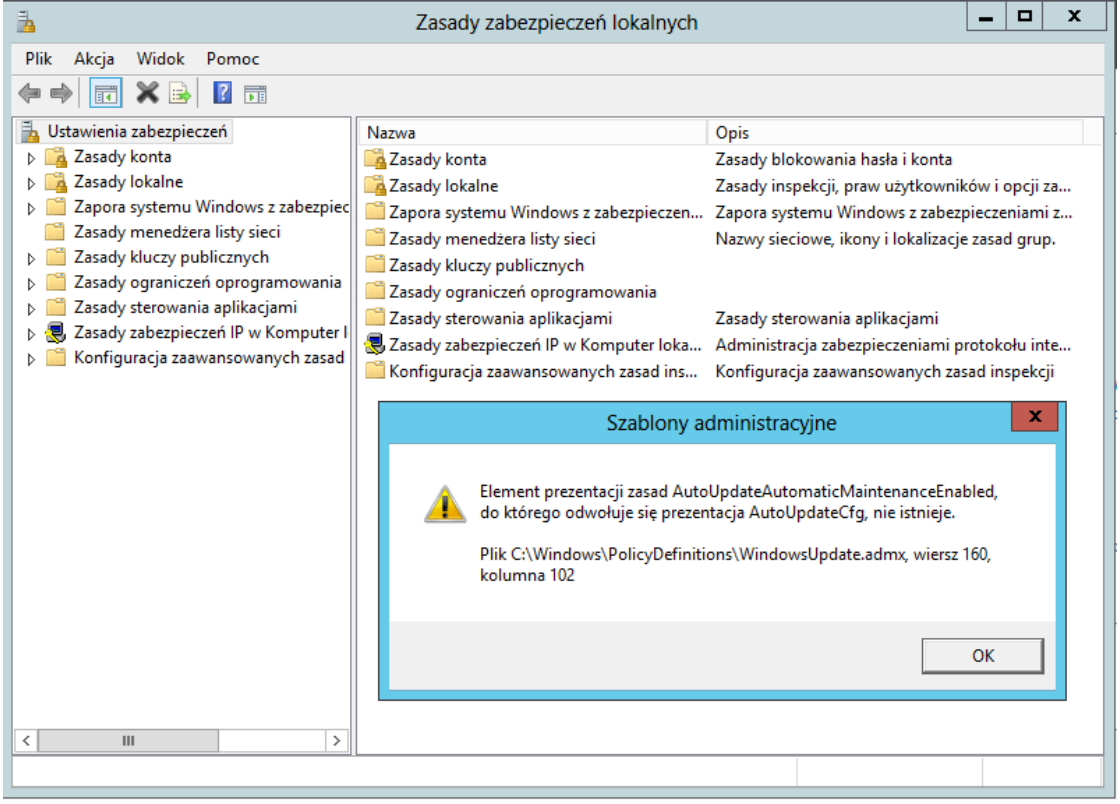
Czym są zasady grupy? Ogólnie rzecz biorąc jest to zbiór uprawnień i zakazów dla poszczególnych użytkowników naszej domeny. Dzięki nim np. uczniowie w szkole nie mają prawa do zmiany jakichkolwiek opcji systemowych, nie mogą instalować oprogramowania ani logować się bezpośrednio na serwerze, nauczyciele mogą instalować oprogramowanie lecz nie mogą nic zmieniać w systemie (np. odinstalować jakichkolwiek składników systemu czy też dodawać nowych użytkowników) podczas gdy administrator może zmieniać każdy szczegół systemu w stacji roboczej (lecz nie może np. logować się i zmieniać jakichkolwiek ustawień na serwerze poprzez pulpit zdalny – tego może dokonać jedynie siedząc fizycznie przy serwerze). Dodatkowo to poprzez zasady grupy mamy możliwość zabronić/pozwolić poszczególnym użytkownikom uruchamiać dane aplikacje, włączać/wyłączać system, zmieniać hasła, wymuszać odpowiednie długości haseł czy też liczbę prób, po których konto użytkownika zostanie zablokowane. Także w grupach istnieje możliwość ustanowienia okresu, co który użytkownik musi zmienić hasło na nowe (tego typu operacja jest bardzo ważna ze względu na np. ochronę danych osobowych).

INFORMACJA: Systemy z linii co najmniej Professional (Windows Vista, Windows 7, Windows 8/8.1) bądź Bussiness/Ultimate także dają możliwość zarządzania zasadami grupy. W ich przypadku jest to zarządzanie zasadami zabezpieczeń lokalnych. Określone poprzez nie uprawnienia/zakazy dotyczą jedynie komputera, na którym zainstalowany jest dany system i tylko użytkowników nie będących administratorami (ewentualnie wszelkie obostrzenia dla administratora należy dodawać ręcznie).

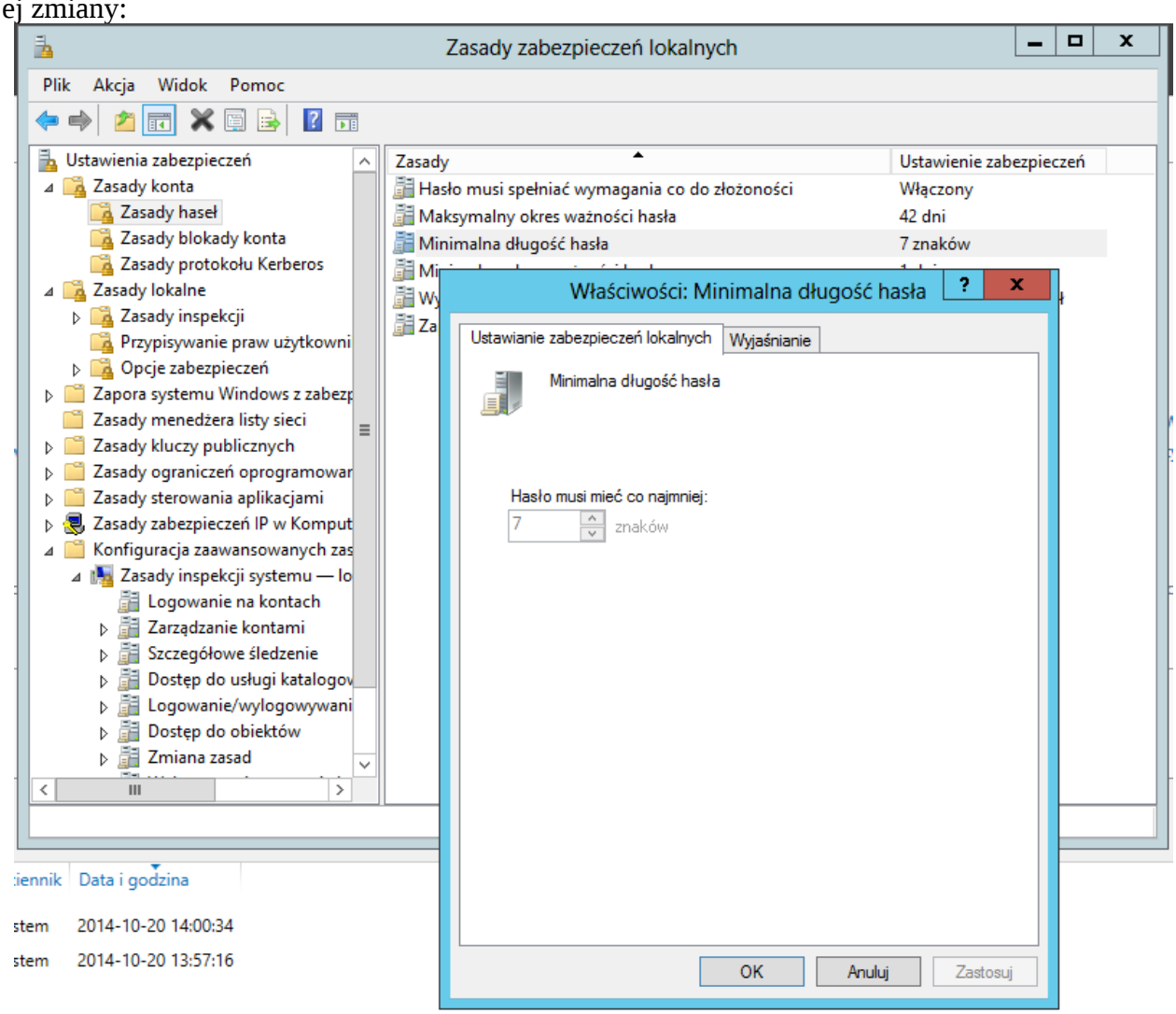
INFORMACJA: Tak naprawdę firma Microsoft tylko nie daje odpowiednich narzędzi do zarządzania polityką zabezpieczeń dla systemów z niższych linii (Standard/Starter). Wszelkich ustawień można dokonywać bezpośrednio poprzez rejestr systemowy. Ustawienia zabezpieczeń wraz z opisem można znaleźć np. na stronie http://gpsearch.azurewebsites.net/ .

System Windows Server 2012 posiada dwa narzędzia do zarządzania polityką zabezpieczeń – Zasady zabezpieczeń lokalnych oraz, po zainstalowaniu roli Active Directory, Zarządzanie zasadami grupy. Domyślnie wraz z instalacją i konfiguracją domeny pierwsze z narzędzi powinno przestać być aktywne (tak samo jak ma to miejsce w przypadku zarządzania kontami lokalnych użytkowników, które przejmuje odpowiednie narzędzie z zestawu dla Active Directory). Jednak w niektórych przypadkach oba z tych narzędzi mogą być aktywne i mieć wpływ na zabezpieczenie serwera (pierwsze z nich ma zasięg działania jedynie na serwerze).

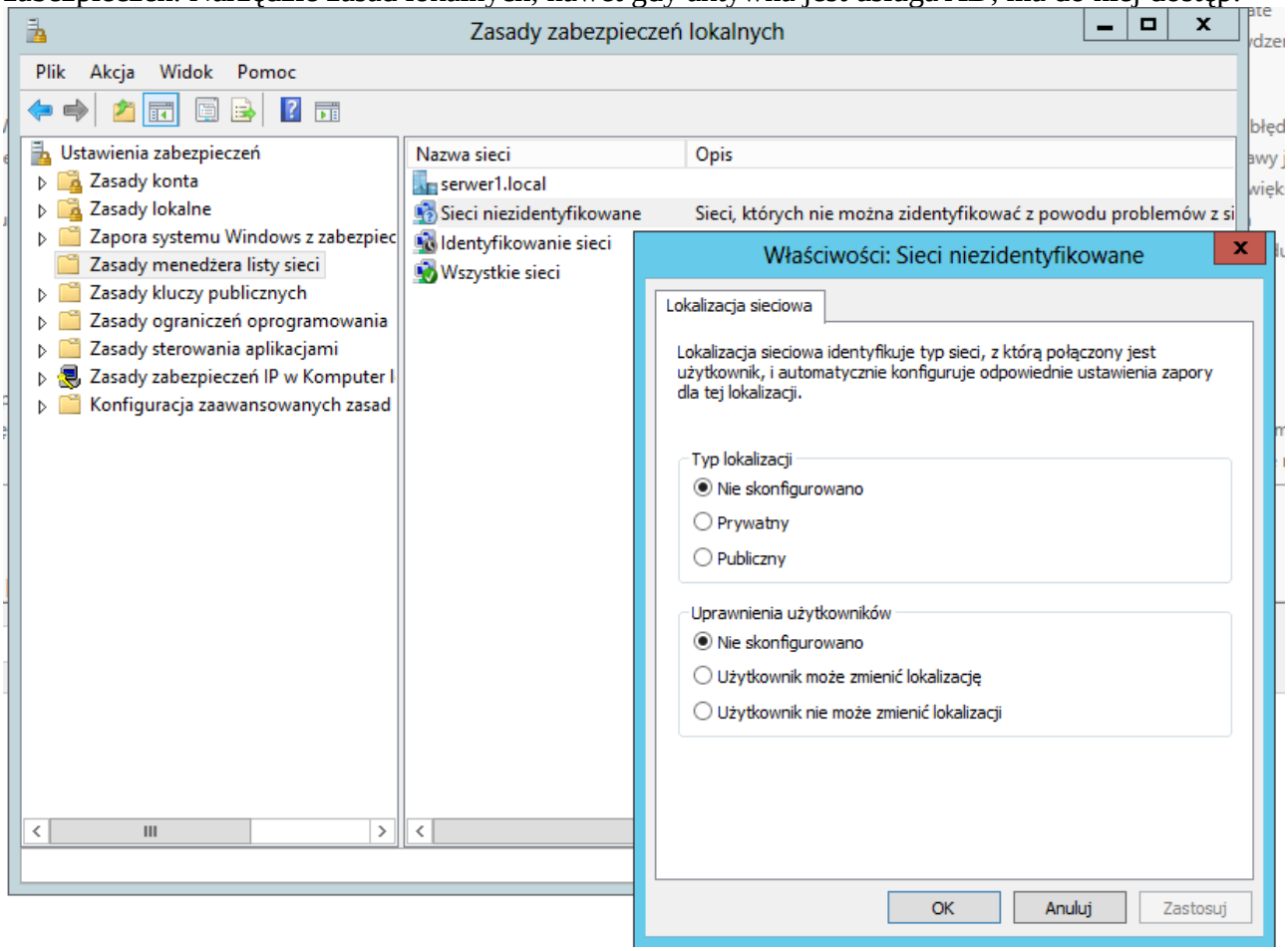
W przypadku próby uruchomienia Zasady zabezpieczeń loklanych może nas przywitać taki oto komunikat:



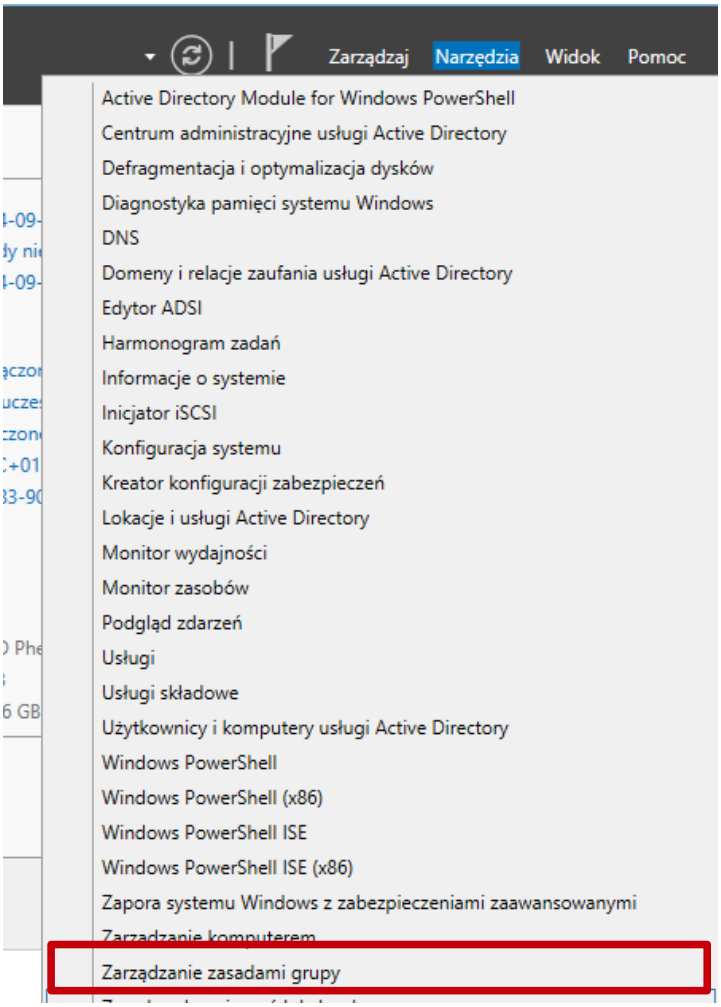
Można go oczywiście zignorować ten komunikat (potwierdzenie) jednak zmiana większości ewentualnych zasad zakończy się niepowodzeniem. Przykładowo niedostępne będą ustawienia zabezpieczeń konta, jak długość hasła, dopuszczalna ilość błędów w haśle przy logowaniu czy okres ważności hasła. Po wybraniu takowej właściwości nie będziemy mieli po prostu możliwości jej zmiany:



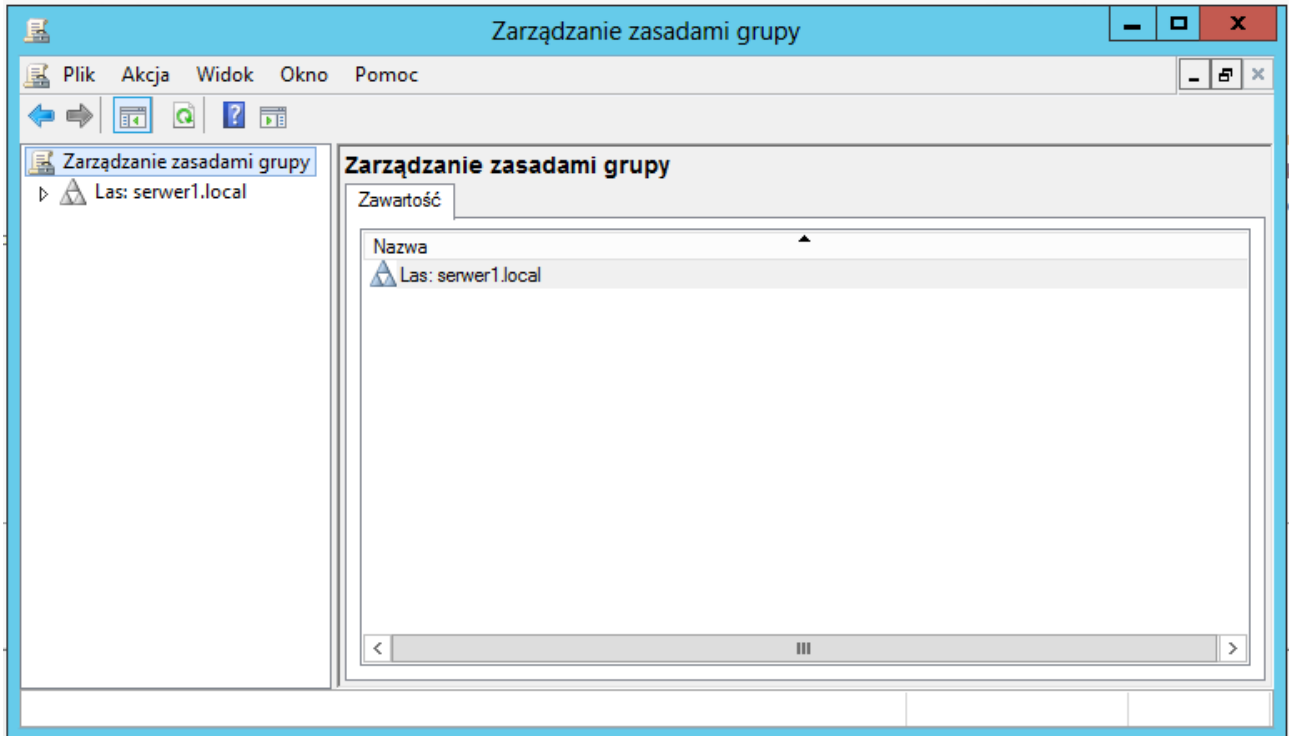
Inne ustawienia są tutaj jednak jak najbardziej dostępne, jak chociażby Zasady menedżera listy sieci. To tutaj konfigurowane są wstępne ustawienia sieci, do których miał dostęp nasz serwer. Proszę pamiętać, że wraz z systemem Windows Vista firma Microsoft wprowadziła w systemie zapamiętywanie ustawień sieci dla każdego nowego połączenia; system identyfikuje taką sieć na podstawie adresu IP, MAC urządzenia docelowego (WLAN) a także za pomocą SSID (WLAN). Dla każdej z tych sieci tworzy profil jej użytkowania – czyli listę działań dozwolonych i niedozwolonych (przykładowo brak rozsyłania zawartości w danej sieci, udostępnianie jedynie urządzeń drukujących czy też tworzy tzw. sieć zaufaną – wszystkie znajdujące się w niej urządzenia widzą się nawzajem i pozwalają na przeglądanie udostępnionej zawartości).
Tak jak zostało wspomniane, wstępna segregacja nowych połączeń to także zadanie zasady zabezpieczeń. Narzędzie zasad lokalnych, nawet gdy aktywna jest usługa AD, ma do niej dostęp:



Tak czy inaczej jako administratorzy usługi katalogowej nie będziemy raczej korzystać z wyżej opisywanego narzędzia. Do naszej dyspozycji Microsoft oddaje znacznie potężniejsze narzędzie – Zarządzanie zasadami grupy (dostępne np. poprzez menu Narzędzia)

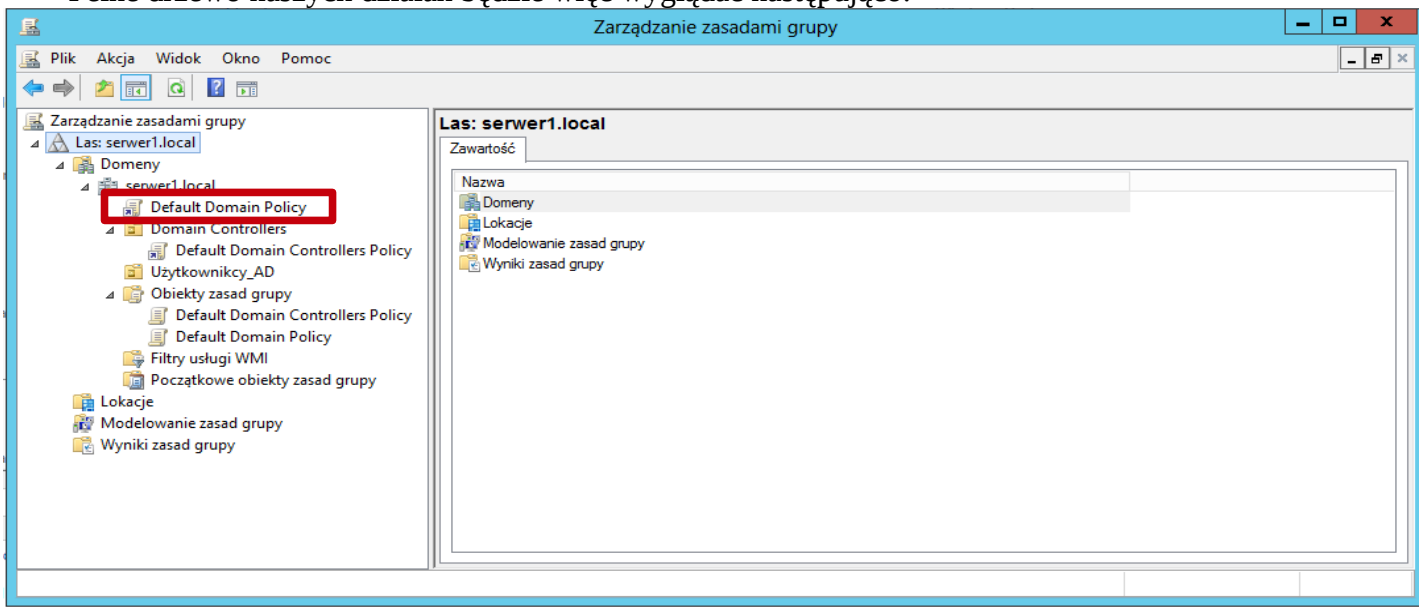


Po pierwszym uruchomieniu okno narzędzia będzie wyglądać w ten sposób:

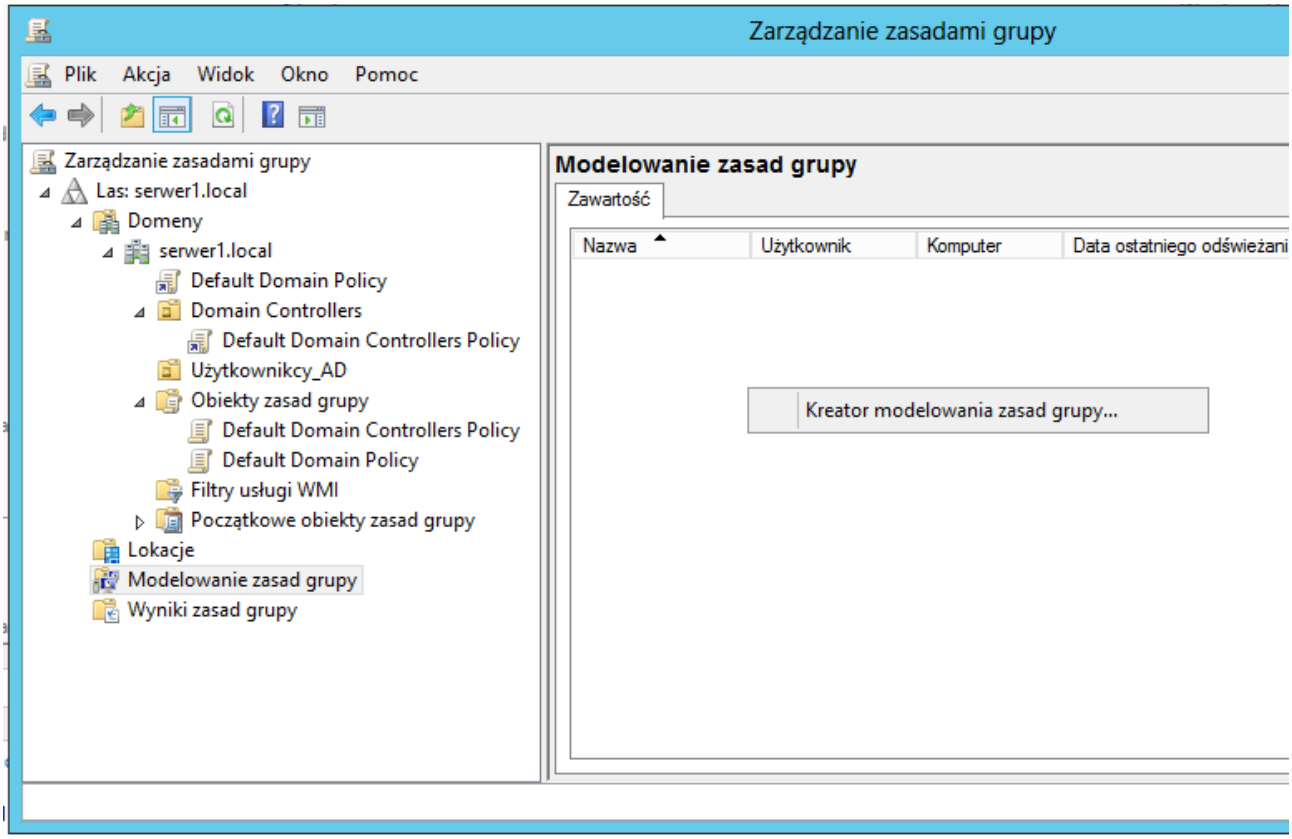


Jak można się domyślać, możemy mieć za jego pomocą dostęp do zabezpieczeń wszystkich administrowanych przez nas domen i/lub lasów (wszystkich powiązanych z aktualnie użytkowanym serwerem!). Przystawka ma swoje opcje (menu Widok->Opcje). Można tutaj ustawić/zmienić ilość

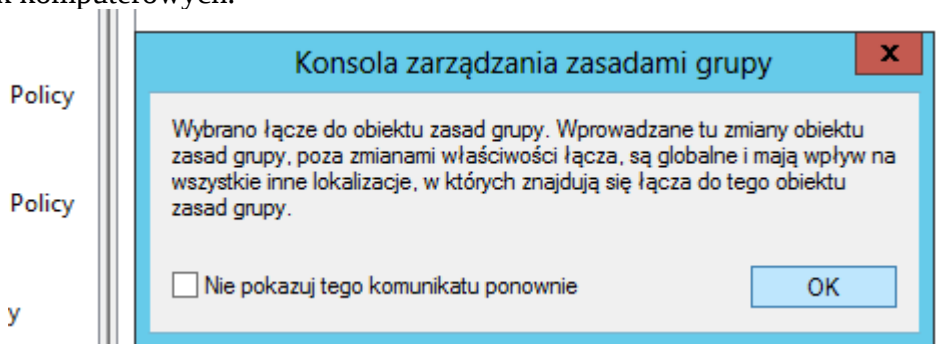
wyświetlanych kolumn, sposób zapisu raportów działania zasad grup (domyślnie zapisuje je systemie Windows oraz katalogu SYSVOL), a także zmienić sposób prezentacji danych (zakładka Ogólne).
Nas jednak będzie bardziej interesować samo zarządzanie polityką zabezpieczeń AD. W naszym wypadku mamy do czynienie tylko z jednym lasem domen, w której znajduje się tylko nasz serwer. Pełne drzewo naszych działań będzie więc wyglądać następująco:



Każdy las może posiadać kilka domen. W naszym wypadku jest to utworzona przez nas domena (na zrzucie ma nazwę serwer1.local). Każda taka domena posiada swoją politykę zabezpieczeń najczęściej nazywającą się Default Domain Policy. Proszę jednak zauważyć, że w głównej gałęzi jest ona jednak jedynie skrótem (czerwona ramka), a jej prawdziwa lokalizacja jest w innym miejscu.
Następny w drzewie naszego serwera jest kontener o nazwie Domain Controllers (kontrolery domeny), w których mamy skrót do działających na ten obiekt zabezpieczeń Default Domain Controllers Policy. Ustawienia tych zabezpieczeń będą oddziaływać jedynie na kontrolery domeny (nie zaś na wszystkie pozostałe stacje robocze).
W dalszej częście mamy dostęp do tworzonego przez nas kontenera Użytkownicy_AD, dla którego możemy nadać indywidualną politykę zabezpieczeń.
W Obiekty zasad grupy są właściwe definicje zabezpieczeń – tutaj znajdują się definicje, do których skróty znajdują się w głównej gałęzi serwera oraz kontrolerów domeny.
Filtry usługi WMI (Windows Management Instrumentation) można nadawać w przypadku gdy chcemy, by pewne ustawienia zabezpieczeń nie oddziaływały na tę usługę.
Ostatni folder/kontener, Początkowe obiekty zasad grupy, nie posiada swojej zawartości. Można jednak kliknąć na przycisk tworzenia domyślnych zasad zabezpieczeń, a narzędzie wygeneruje zabezpieczenia np. dla systemów Windows XP czy Windows Vista.
Kolejne 3 foldery widoczne na zrzucie, Lokacje, Modelowanie zasad grupy oraz Wyniki zasad grupy należą do całego lasu (nie ograniczają się do utworzonej przez nas domeny). Pierwszy z folderów pozwala na zarządzanie dostępem do stron wewnętrznych AD (o ile są ustawione – na razie takowej nie posiadamy). Modelowanie zasad grupy służy do „przetestowania” ustawień grupy dla wskazanych grup użytkowników (bądź konkretnego użytkownika) i/lub wskazanych komputerów w domenie. Ponadto można sprawdzić jak dane zabezpieczenia wpłyną na maszynę docelową w przypadku słabego połączenia sieciowego czy przy zastosowanych konkretnych filtrach WMI. Podobne zadanie spełnia folder Wyniki zasad grupy – pozwala nam zebrać pełne informacje jakie zasady grupy są zastosowane dla wskazanego komputera, jak działają w różnych warunkach itp. Domyślnie oba foldery są puste. W celu rozpoczęcia generowania raportu wystarczy wybrać dany folder i po prawej stronie okna kliknąć prawym przyciskiem myszy. Pojawi się menu podręczne z jedną opcją: Kreator modelowania zasad grupy/Kreator wyników zasad grupy.

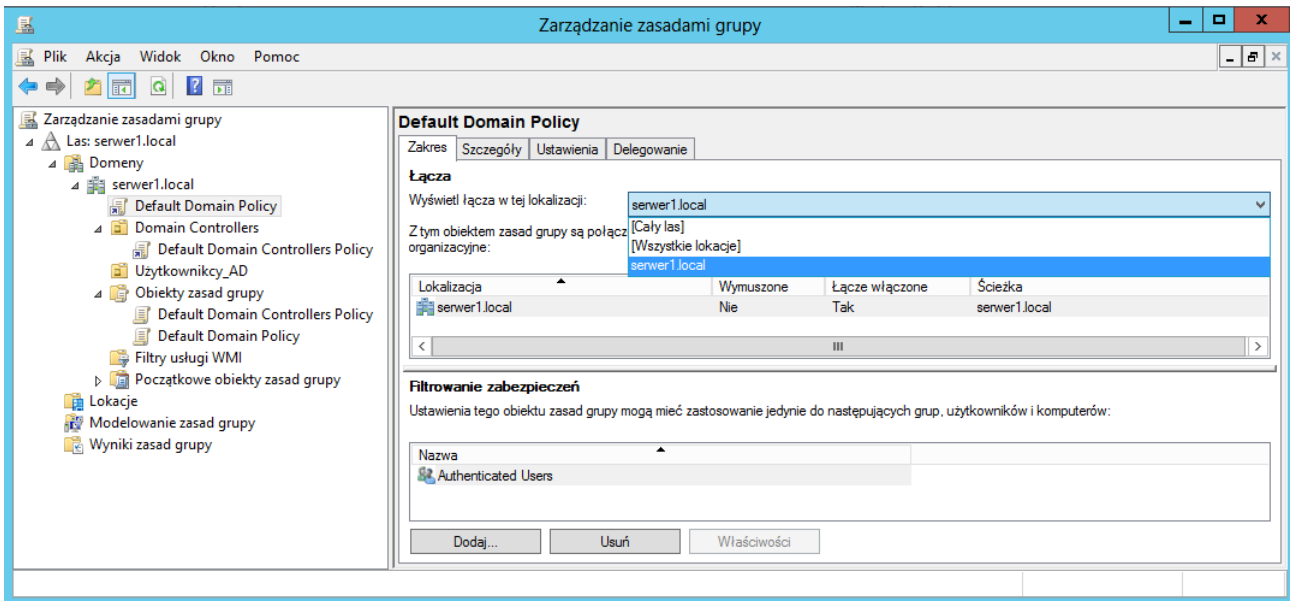


Kliknijmy na Default Domain Policy. Jeżeli klikniemy na skrót narzędzie poinformuje nas, że zmiany dokonane w skrócie będą miały bezpośrednie przełożenie na ustawienia w elemencie docelowym, czyli zmodyfikujemy tym samym ustawienia innych obiektów, które również mogą korzystać z tejże zasady. Komunikat można również wyłączyć (poprzez zaznaczenie opcji by się więcej nie pojawiał) chociaż nie jest to mądre posunięcie – trzeba pamiętać, że któregoś razu możemy nie zauważyć, iż działamy na kopii i przez nieuwagę zmienić pilotkę dla wielu folderów czy jednostek komputerowych.



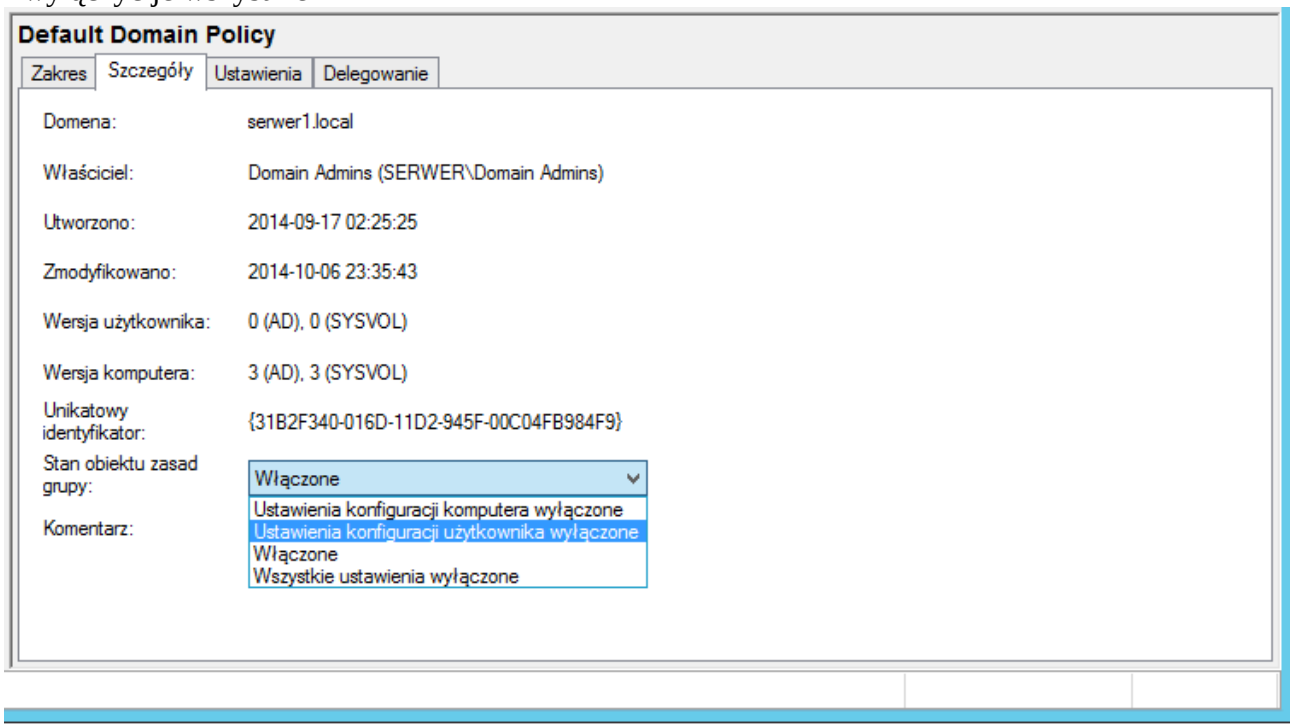
W prawej części okna pojawią się 4 zakładki.

Pierwsza z nich, Zakres, pokazuje do których lokalizacji oraz grup użytkowników dana polityka zabezpieczeń jest stosowana. W tym wypadku tylko dla naszej domeny (serwer1.local) oraz dla użytkowników autoryzowanych (mających swoje konta na serwerze). Proszę zauważyć iż żadna grupa administracyjna nie jest podpięta pod te zabezpieczenia (w przeciwnym wypadku administrator nie mógłby zrobić pewnych rzeczy z systemem co byłoby rażącym błędem!). W przypadku lokalizacji kolumna wymuszenie mówi nam czy polityka zabezpieczeń jest wymuszona (nie oznacza, że jej zasady mogą zostać zastąpione innymi zasadami, dostępnymi dla pewnej grupy/kontenera) a kolumna Łącze włączone informuje czy skrót do ustawień zabezpieczeń jest włączony (w naszym wypadku jest włączony). Gdyby był wyłączony to nasza grupa zabezpieczeń nie miała by odniesienia do aktualnie używanej domeny.

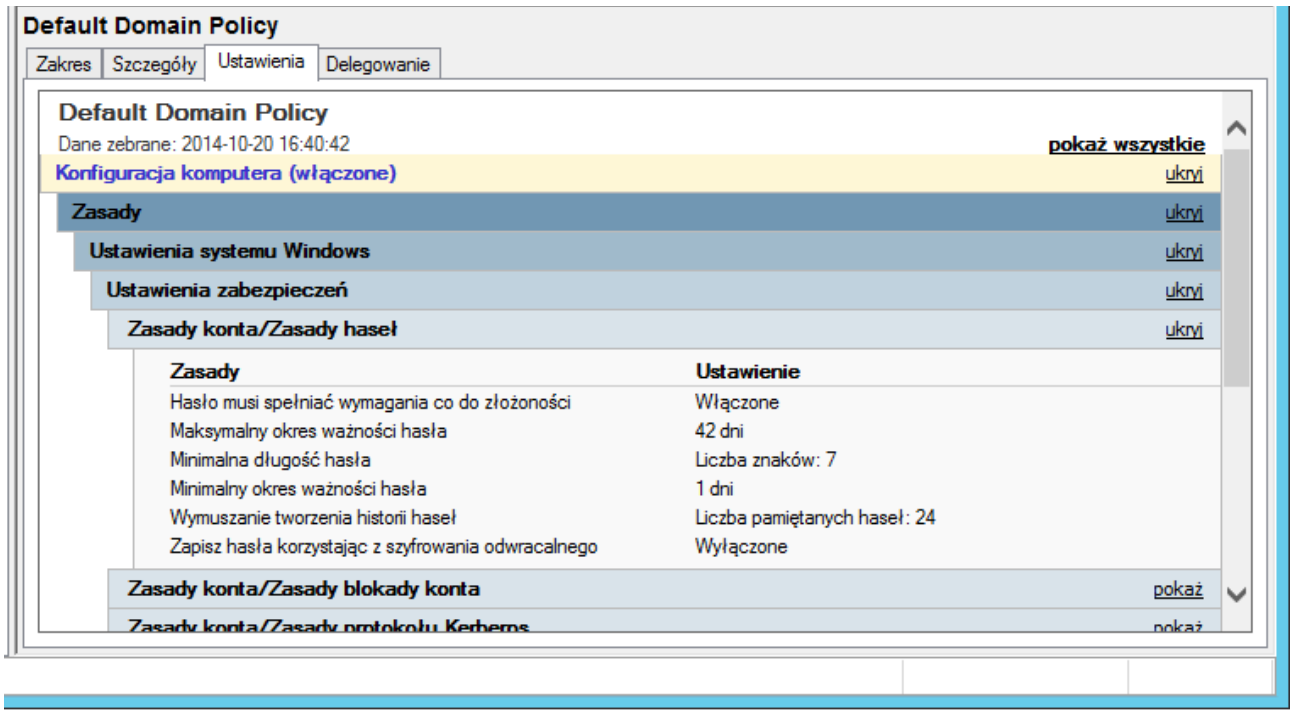


Zakładka Szczegóły pozwala ustalić kiedy zabezpieczenie zostało utworzone, kiedy zmodyfikowane, do kogo się odnosi oraz umożliwia włączenie/wyłączenie danego zabezpieczenia; możliwe jest:

- włączenie ustawienia dla użytkowników poprzez wybranie opcji Ustawienia konfiguracji komputera wyłączone
- włączenie konfiguracji dla komputerów poprzez Ustawienia konfiguracji użytkownika wyłączone
- włączyć oba wyżej wymienione typy zabezpieczeń
- wyłączyć je wszystkie

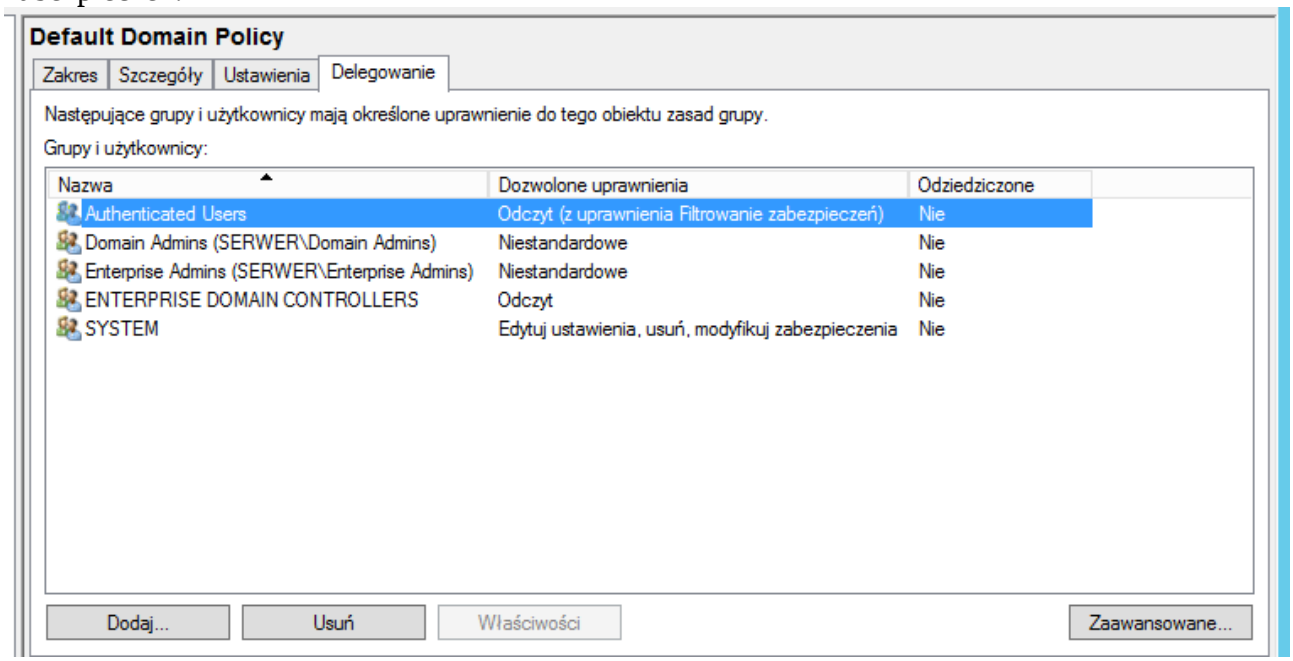


W zakładce Ustawienia możemy zapoznać się z pełnym raportem dotyczącym zabezpieczeń, na które wpływa dana polityka. Raport generowany jest w postaci pliku XML i wyświetlany jest w postaci „przyjaznej” - każda gałąź może być ukryta/pokazana, a kolejna zawartość wyświetlana jest „wewnątrz” warstwy nadrzędnej. Przykładowo by wyświetlić aktualne zasady konta/zasady haseł należy uaktywnić kolejne warstwy w ten sposób

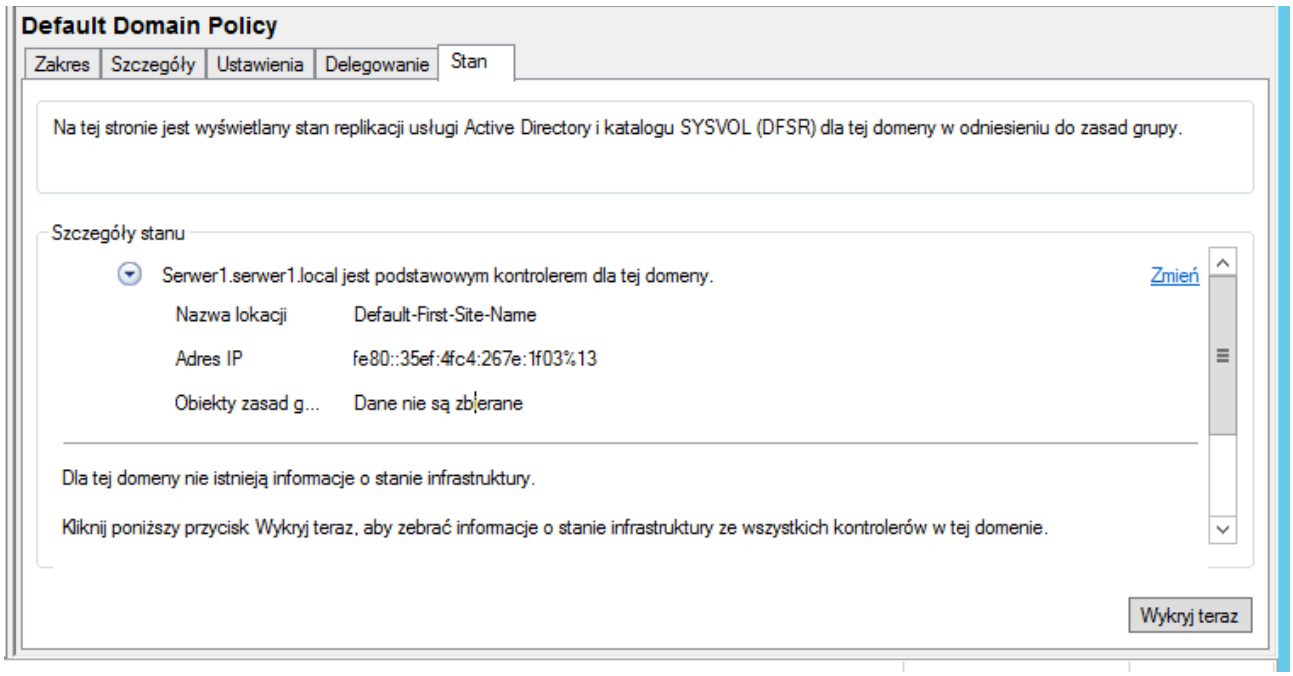


Dobrym zwyczajem jest dogłębne zapoznanie się z tym raportem zanim rozpocznie się ewentualne zmiany polityki zabezpieczeń.

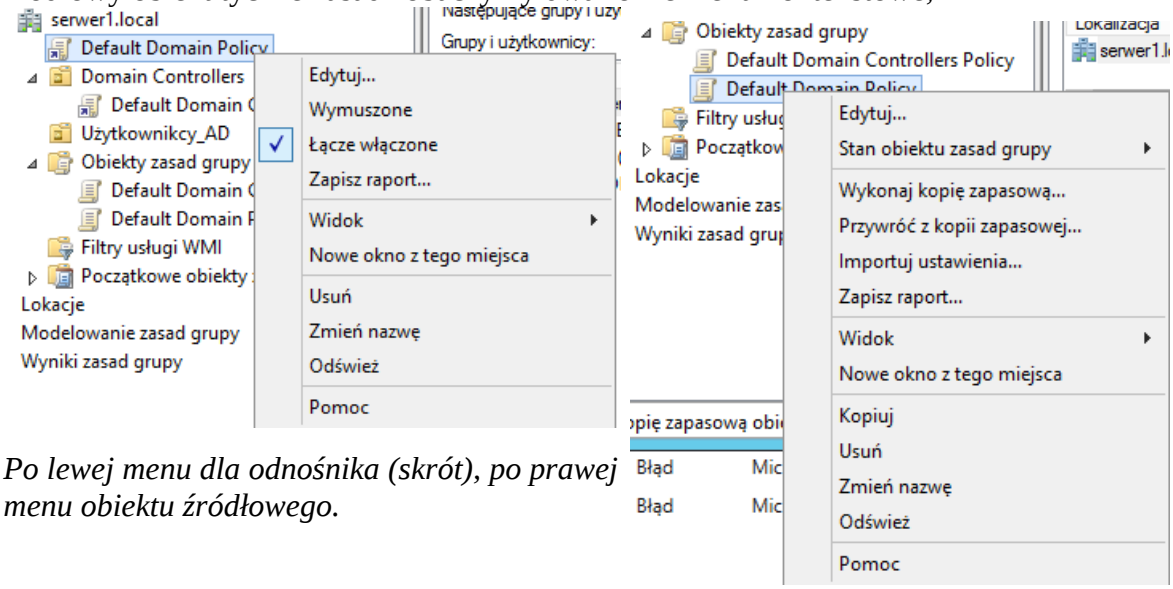
Zakładka Delegowanie pozwala na ustawienie uprawnień kto może, a kto nie korzystać z wybranej polityki zabezpieczeń. Ponadto pokazuje kto ma prawa edycyjne danej grupy (nawet administrator systemu może nie mieć odpowiednich uprawnień do edycji!). Zawsze uprawnionymi do tego typu działań są użytkownicy Administratorzy grup zabezpieczeń (po angielsku grupa nazywa się Group Policy Creator Owner). Nasze aktualnie użytkowane konto ma odpowiednie uprawnienia do edycji zabezpieczeń.



Jeżeli wybralibyśmy grupę zabezpieczeń (dostępna w Obiekty zasad grupy) to pojawia się jeszcze jedna zakładka o nazwie Stan. Jej zawartość mówi o replikacji (kopiowaniu) tejże polityki zabezpieczeń na kolejnych członków domeny (kontrolery podrzędne). Ponieważ nie posiadamy innych kontrolerów domeny to wskazana grupa nie będzie replikowana.



Klikając prawym przyciskiem myszy na odniesienie (skrót) do zasad grupy zabezpieczeń oraz na źródłowy obiekt tychże zasad zobaczymy dwa różne menu kontekstowe;



Po lewej menu dla odnośnika (skrót), po prawej menu obiektu źródłowego.

- opcja Edytuj pozwala na przejście do edycji zasad wchodzących w skład danej polityki zabezpieczeń (dostępne w obu przypadkach).
- opcja Zapisz raport... powoduje zapisanie informacji dostępnych w zakładce Ustawienia do pliku HTML w celu późniejszego przejrzenia ich.

Zajmijmy się różnicami.

W menu dla odnośnika mamy następujące opcje:

- Wymuszone – w przypadku wybrania tej opcji pojawia się przy niej symbol odznaczenia. Powoduje ona wymuszenie zastosowania wszystkich zasad dla całej domeny (wszelkie inne zostaną pominięte)
- Łącze włączone – włącza/wyłącza połączenie odnośnika do obiektu źródłowego grupy zabezpieczeń. Przy wyłączonym łączu element nie ma wpływu na element, do którego został przypisany

W menu obiektu mamy opcje:

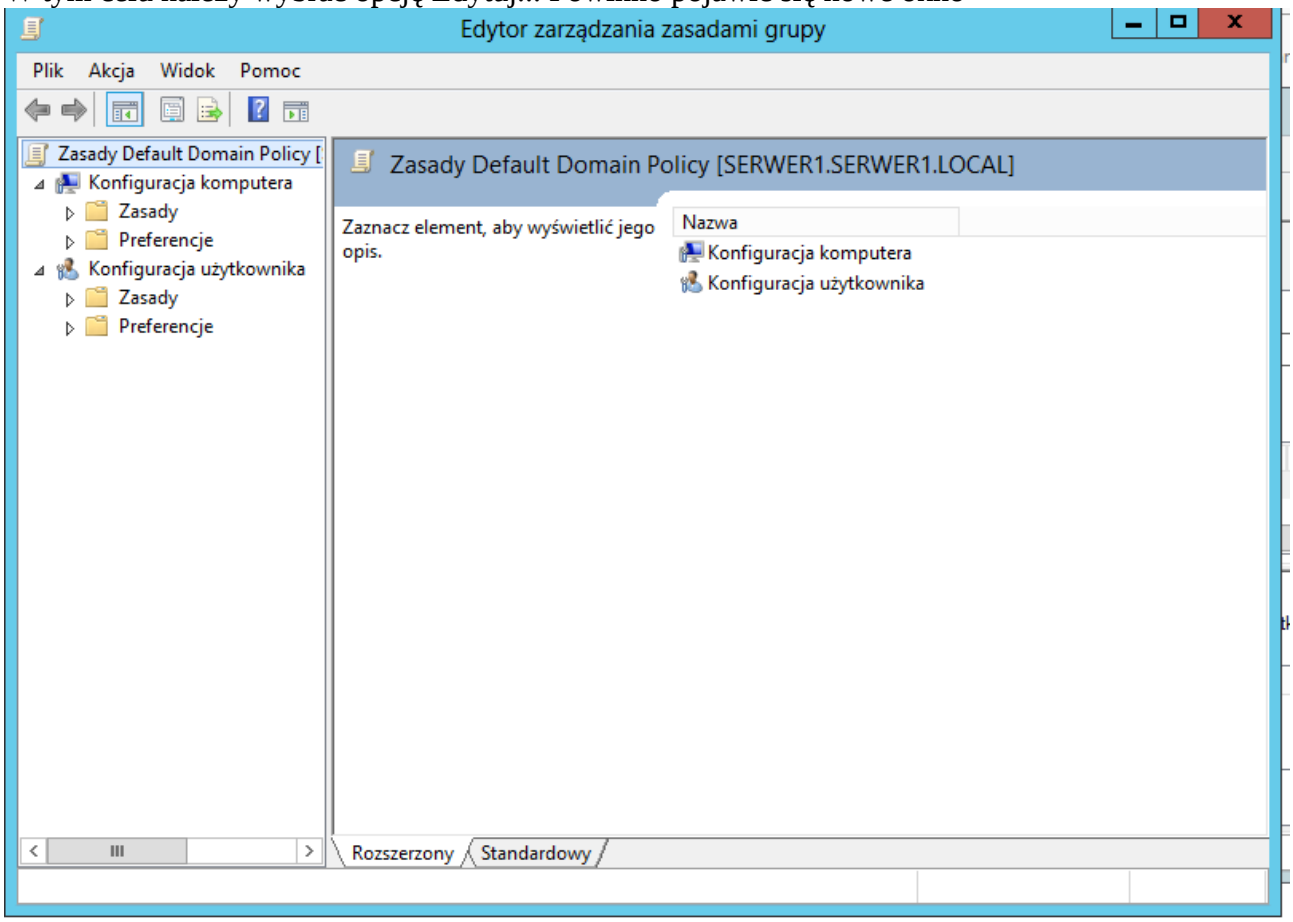
- Stan obiektu zasad grupy – otwiera podmenu w którym widnieją identycznie opcje jak na zakładce Szczegóły. Pozwala wybrać stan działania obiektu (wyłączenie go tutaj powinien mieć bezpośredni

wpływ na wszystkie odniesienia!)
- Wykonaj kopię zapasową... - jedna z nowości od Windows 2008 Server. Pozwala na stworzenie pełnej kopii wszystkich ustawień danej polityki zabezpieczeń by móc ją później przywrócić/dodać na nowy serwer
- Przywróć z kopii zapasowej... - jeżeli posiadamy kopię zapasową grupy zabezpieczeń to możemy ją przywrócić przy pomocy tej opcji
- Importuj ustawienia... - można wskazać kopię zapasową innej grupy zabezpieczeń by zaimportować do aktualnie edytowanej jej wszystkie ustawienia

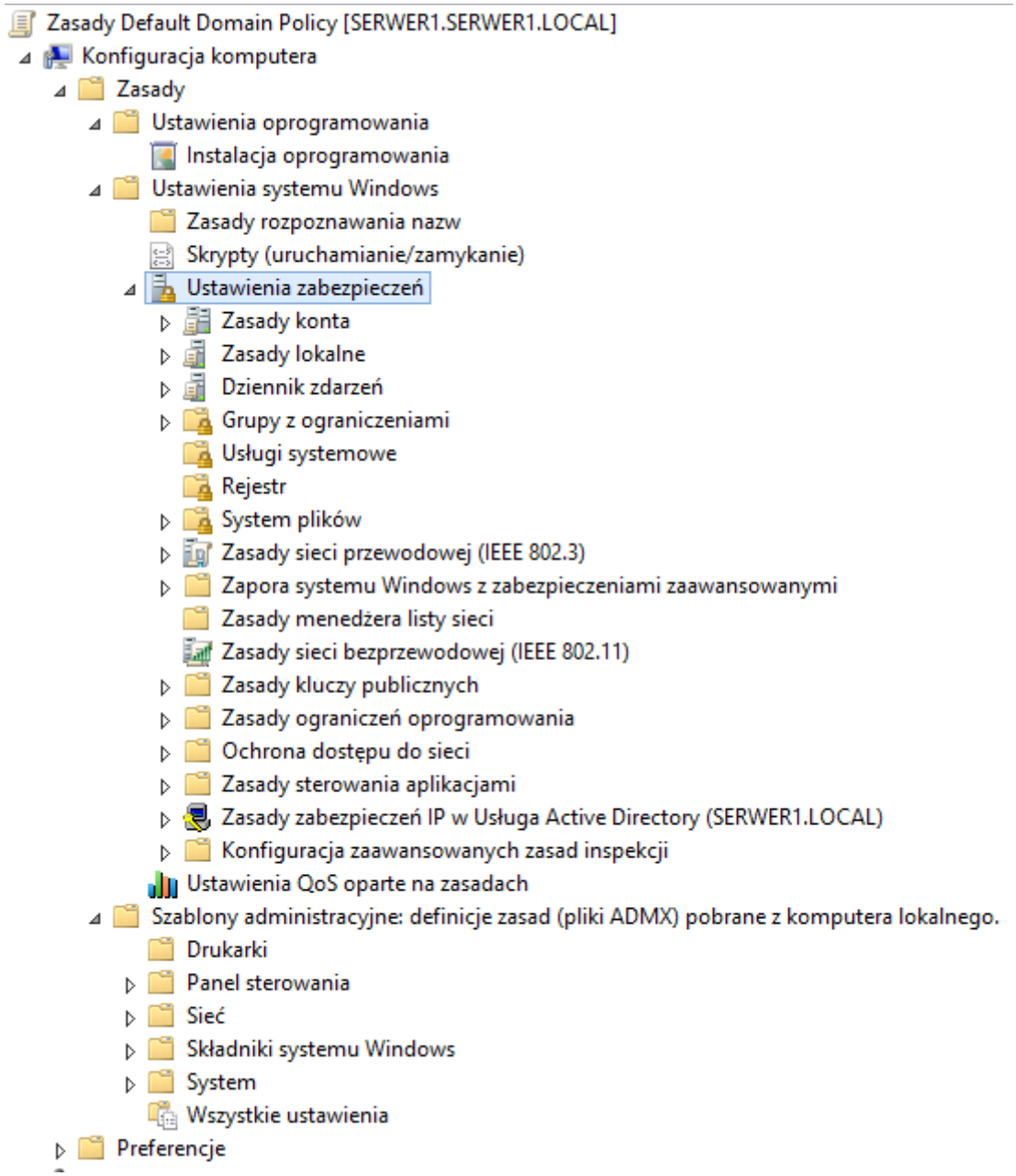
Pozostałe opcje niewiele różnią się od pozostałych menu kontekstowych i nie będą omawiane.

W poniższym materiale skupimy się na głównym „zadaniu” zasad zabezpieczeń, jakim jest odpowiednia konfiguracja systemu, ustawień dla haseł, a także co może/nie może użytkownik domeny na komputerze, z którego w danej chwili będzie korzystał.

Spróbujmy edytować domyślne zabezpieczenia domeny.
BARDZO WAŻNE! Proszę zrobić migawkę (Snapshot) przed dalszą pracą. Niektóre ustawienia mogą być w razie awarii trudne do odwrócenia (bądź niemożliwe).
W tym celu należy wybrać opcję Edytuj... Powinno pojawić się nowe okno



Będziemy w nim dokonywać wszystkich zmian polityki zabezpieczeń. Z pozoru opcji ustawień jest niewiele (dwa elementy – Konfiguracja komputera oraz Konfiguracja użytkownika) jednak drzewko opcji jest bardzo rozbudowane. Przyjrzyjmy mu się bliżej:



Na szczycie listy w Zasadach mamy następujące kategorie:
- Ustawienia oprogramowania – opcja pozwala na zautomatyzowanie dystrybucji (instalacji) oprogramowania w komputerach należących do domeny. Jeżeli danego pakietu oprogramowania w stacji roboczej nie będzie to serwer wykona taką instalację zanim użytkownik zostanie zalogowany na swoje konto.

- Ustawienia systemu Windows – to w zasadzie kategoria skupiająca wszystkie ustawienia zabezpieczeń komputerów należących do danej grupy zabezpieczeń.
1) Zasady rozpoznawania nazw – pozwala na bezpośrednią edycję rozpoznawania nazw w usłudze DNS przez stacje robocze dzięki czemu administrator może mieć pełną kontrolę nad stronami, które będzie przeglądał użytkownik systemu (przy przekierowaniu/wymuszeniu serwera DNS możliwe jest zablokowanie określonych adresów domenowych)
- Skrypty – pozwala administratorowi na uruchamianie skryptów CDM/Powershell przy logowaniu się użytkownika jak i przy zamknięciu systemu. Dzięki temu można uruchamiać lokalne oprogramowanie, zdarzenia czy też usługi blokując np. większość usług systemu (zostawiając tylko te, których użytkownik potrzebuje do pracy w ramach swoich obowiązków). Na zakończenie mogą uruchamiać się skrypty czyszczące pulpit, wskazany katalog czy też przywracające funkcjonalność systemu.

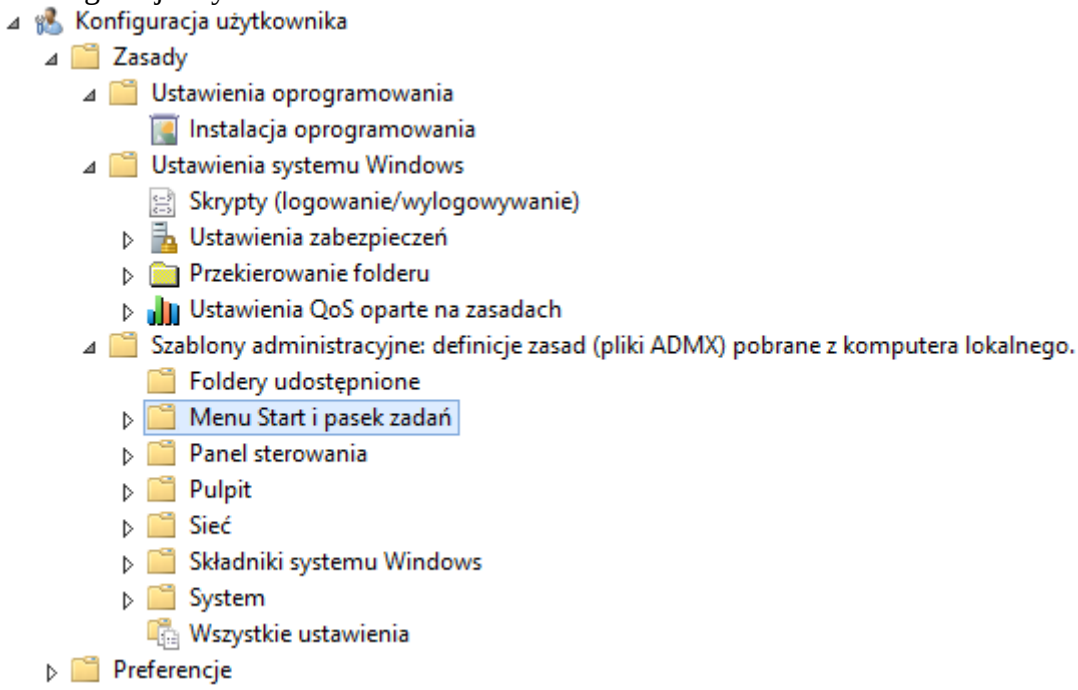
- Ustawienia zabezpieczeń – w tej części znajdują się wszystkie opcje związane z ogólnym bezpieczeństwem komputera/komputerów działających w ramach wskazanej domeny. Można decydować o zabezpieczeniu kont użytkowników (hasła, blokowanie), o przypisywaniu praw dla poszczególnych użytkowników czy też o metodach zapisu/przechowywania dziennika zdarzeń poszczególnych systemów stacji roboczych/serwera.
Innymi opcjami, którymi można zarządzać poprzez Ustawienia zabezpieczeń:
1) Grupy z ograniczeniami – można dodawać konkretne grupy użytkowników, które będą posiadać pewne (ustalone) ograniczenia w korzystaniu z systemu operacyjnego
2) Usługi systemowe – pozwala zarządzać usługami systemowymi na komputerach dostępnych w ramach domeny (decydować o ich uruchamianiu, wyłączaniu czy dodatkowych opcjach)
3) Rejestr – pozwala dodawać/usuwać poszczególne klucze w rejestrze w komputerach domeny
4) System plików – pozwala na centralne zarządzanie dostępem do wskazanych przez administratora plików i katalogów.
5) Zasady sieci przewodowej – pozwala na tworzenie szablonów grup sieci przewodowych (prywatna/praca/publiczna) dla systemów Windows Vista bądź nowszych (wcześniejsze wersje systemu nie miały szablonów sieciowych)
6) Zapora systemu Windows z zabezpieczeniami zaawansowanymi – pozwala na pełną kontrolę nad zaporą ogniową wbudowaną w system Windows (od Windows XP SP2).
7) Zasady menedżera listy sieci – pozwala ustawiać domyślne akcje dla sieci zaufanych, niezaufanych, nowo wykrytych. Pozwala także zmieniać ustawienia już dodanych sieci
8) Zasady sieci bezprzewodowej – to samo jak dla punktu 5)
9) Zasady kluczy publicznych – pozwala kompleksowo zarządzać wszystkimi kluczami i certyfikatami zapisanymi w systemie. Klucze te mogą być dodawane z chwilą odwiedzania strony WWW, na której klucz jest potrzebny. Klucze mogą zostać również dodane w chwili korzystania z aplikacji, która ich wymaga, przez użytkownika itp.
10) Zasady ograniczeń oprogramowania – pozwala np. na decydowanie które typy plików może wykorzystywać użytkownik (dopuszczone rozszerzenia plików), jak ma się zachowywać system w przypadku nieautoryzowanego (niezaufanego) wydawcy itp. Domyślnie zasady ograniczenia nie są tutaj ustawione lecz można je dodać poprzez menu Akcja lub poprzez kliknięcie prawym przyciskiem myszy i wybranie opcji Nowe zasady ograniczeń oprogramowania
11) Ochrona dostępu do sieci – pozwala na zarządzanie protokołami dostępowymi do sieci LAN/WAN. Dodatkowo administrator ma tutaj możliwość dodawania zaufanych adresów URL – tylko z tych adresów użytkownik docelowy będzie mógł korzystać.
12) Zasady sterowania aplikacjami (AppLocker) – pozwala na decydowanie jakie aplikacje może uruchamiać użytkownik. Dotyczy to zarówno plików wykonywalnych jak i np. plików projektów
13) Zasady zabezpieczeń IP w Usługa Active Directory – pozwala na zarządzanie dostępnymi protokołami IP w serwerze oraz stacjach roboczych (np. z którego protokołu klienci mają korzystać w sieci LAN, z którego w sieci WAN itd.)
14) Konfiguracja zaawansowanych zasad inspekcji – pozwala na ustawienie szczegółowej inspekcji dla każdej wyżej opisanej zasady zabezpieczeń. Pozwala m.in. na szczegółowe sprawdzanie poświadczeń logującego się użytkownika, uruchamianej usługi/aplikacji itp.
Ustawienia QoS oparte na zasadach – pozwala administratorowi zarządzać usługami w sieci oraz przydziałem dla nich odpowiedniego transferu (przynajmniej dla sieci LAN). Jeżeli administrator chciałby dodatkowo przydziałami łącza dla aplikacji internetowych to serwer AD musi posiadać rolę rozdzielania łącza internetowego (patrz wcześniejsze materiały).

- Szablony administracyjne – pozwala na szczegółowe zarządzanie usługami systemu Windows stacji roboczej. To tutaj znajdują się możliwości wyłączenia Panelu Sterowania (niewidoczny dla użytkowników objętych polisą zabezpieczeń), wyłączenie grupy sieciowej, zablokowanie menu kontekstowego w systemie i wiele wiele innych.

-Preferencje – pozwala administratorowi na pełne zarządzanie zaawansowanymi ustawieniami

poszczególnych stacji roboczych – dostępem do kluczy w rejestrze, zmiennych środowiskowych, menedżera urządzeń czy też przystawek w Panelu sterowania (wraz z włączaniem/wyłączaniem poszczególnych opcji).

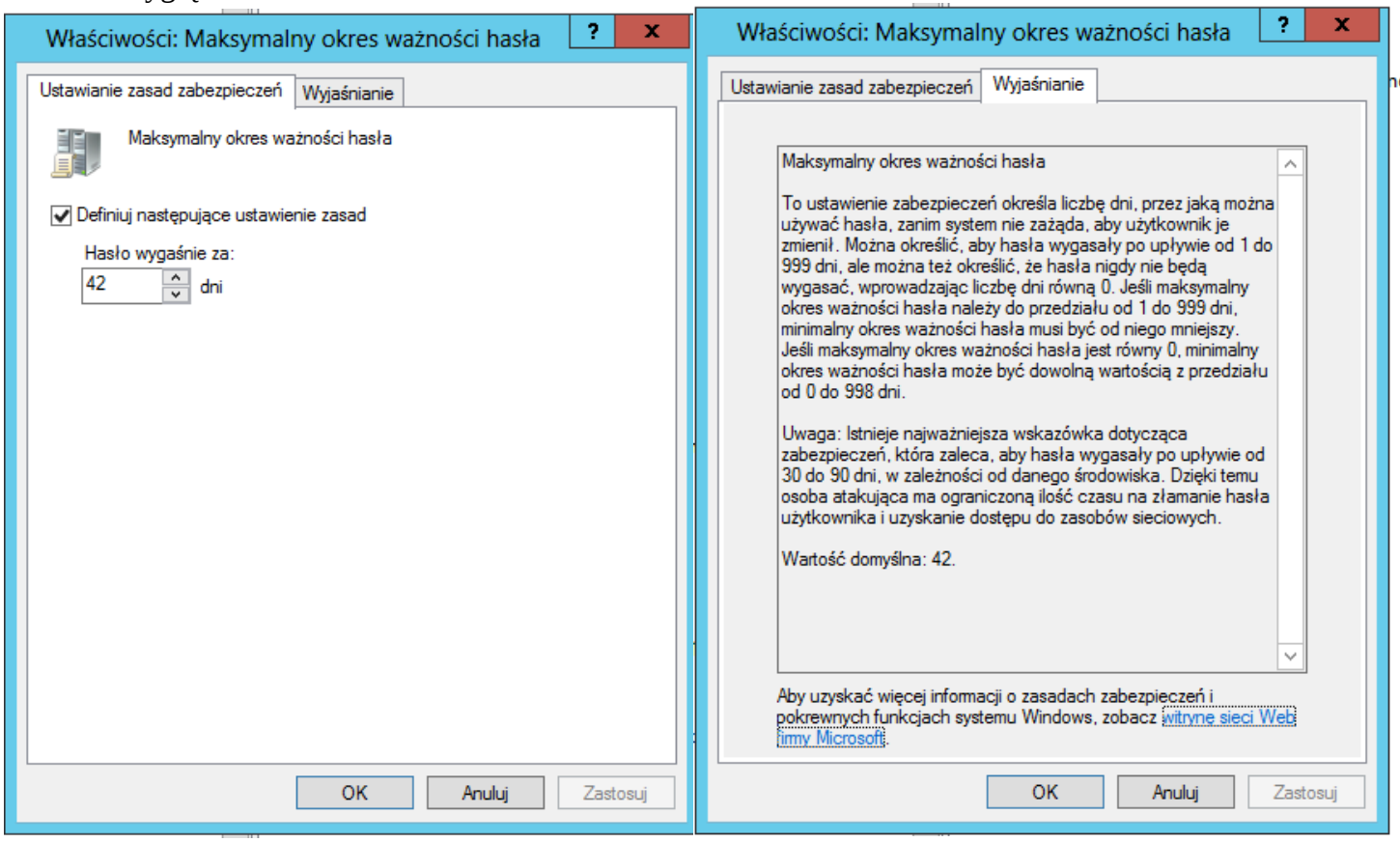
Drzewo konfiguracji użytkownika:



Ustawień jest mniej lecz są one nastawione typowo dla poszczególnych użytkowników logujących się za pomocą kont domenowych.
- Zasady:
1) Ustawienia oprogramowania – jak poprzednio lecz dotyczą tylko użytkowników domenowych (nie całego systemu, który może mieć inną politykę zabezpieczeń!)
2) Skrypty – odnoszą się tylko do użytkownika (nie systemu Windows). Mogą to byś skrypty tylko dla wybranych kont i zawierać dodatkowe skrypty/skrypty niwelujące działania skryptów systemowych
3) Ustawienia zabezpieczeń – w tym wypadku są to ustawienia kluczy publicznych dla konkretnych użytkowników oraz ograniczeń oprogramowania z nimi związanych\
4) Przekierowanie folderu – tutaj można przekierowywać domyślne lokalizacje folderów dla każdego użytkownika (Menu Start, Pulpit, Pobrane, Gry). Można dzięki tym ustawieniom zmieniać ich lokalizację (inny dysk) bądź łączyć w jeden, wspólny folder
5) Ustawienia QoS oparte na zasadach – tak jak poprzednio z tym, że tylko dla wskazanego użytkownika
- Szablony administracyjne
1) Foldery udostępnione – pozwala na decydowanie, czy użytkownik może cokolwiek udostępniać w sieci
2) Menu start i pasek zadań – szczegółowe opcje dotyczące tych dwóch elementów systemu (w Windows 8/8.1 zamiast Menu Start definiujemy niektóre opcje Ekranu Startowego)
3) Panel sterowania – ustawienia dla panelu sterowania (wyłączanie poszczególnych opcji lub wszystkiego)
4) Pulpit – pozwala decydować co wolno robić a czego nie użytkownikowi z pulpitem systemowym (np. można wzbronić zmiany tapety, motywów itp.)
5) Sieć – pozwala odciąć bądź ograniczyć dostęp do ustawień sieciowych w systemie klienckim
6) Składniki systemu Windows – pozwala ograniczać dostęp użytkownikowi domeny do systemowych usług
7) System – pozwala zmieniać ustawienia systemowe (np. zachowanie na kliknięcie kombinacji ALT+CTRL+DEL)

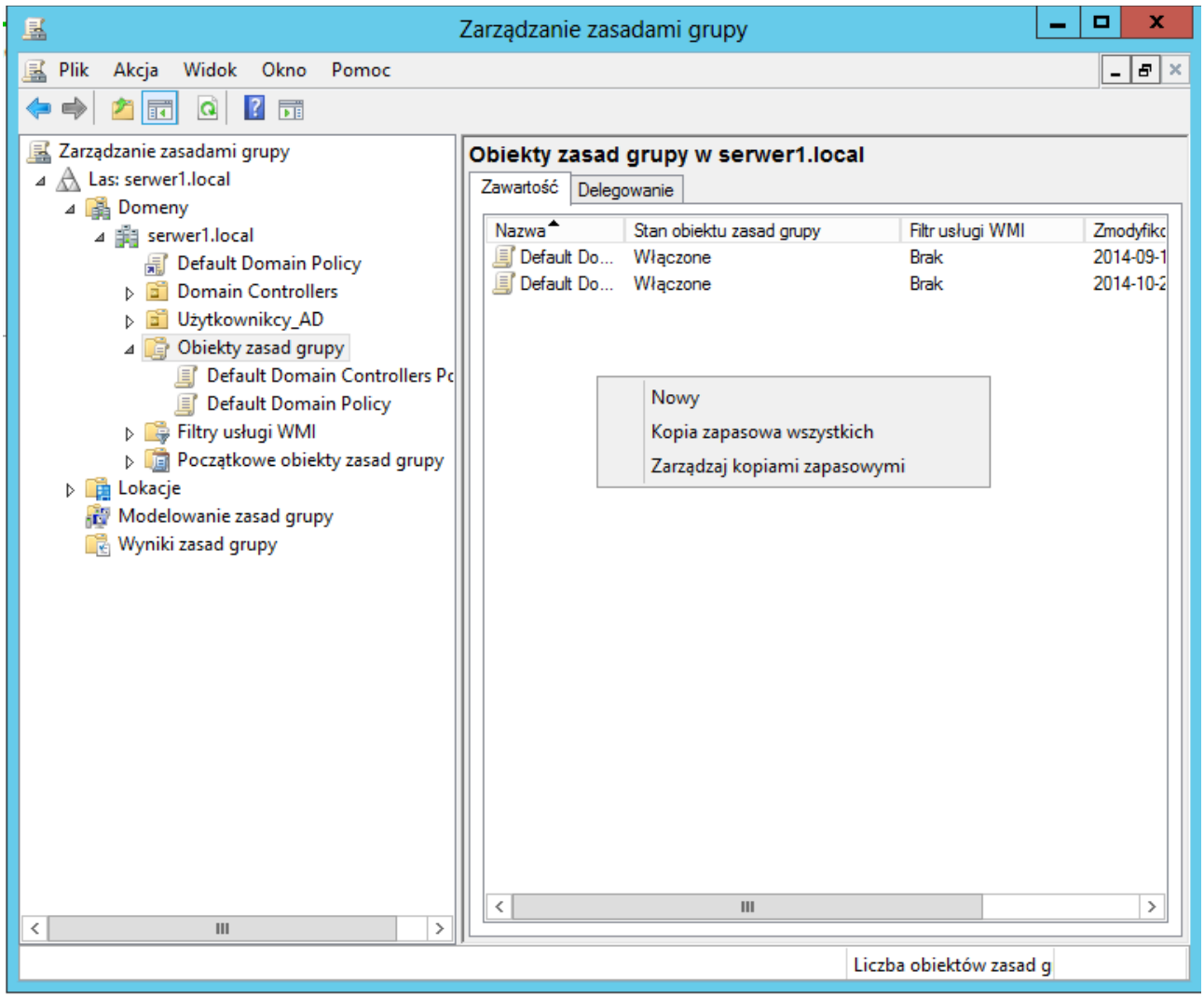
8) Wszystkie ustawienia – element-odnośnik do wszystkich wyżej opisanych ustawień i opcji (nieuporządkowane po folderach)
- Preferencje – tak jak w przypadku Konfiguracji komputera pozwala zarządzać niemal wszystkimi zaawansowanymi aspektami konta użytkownika. Przykładowo istnieje możliwość odgórnego dodawania określonych aplikacji do systemu, ustawiać dostęp do zmapowanych dysków, podmieniać klucze rejestru itp.

Oczywiście powyższy opis to jedynie bardzo ogólne wyjaśnienia drzewa zabezpieczeń domeny. Na szczęście firma Microsoft udostępniła odpowiednie opisy poszczególnych opcji z poziomu tegoż narzędzia oraz, w przypadku bardziej złożonych operacji, także odnośniki do odpowiednich podstron internetowych/podstron pomocy systemu (offline). Nam jednak będzie potrzebny dostęp jedynie do najbardziej podstawowych opcji. Przykładowa pomoc dla opcji ustawienia ważności hasła wygląda tak:

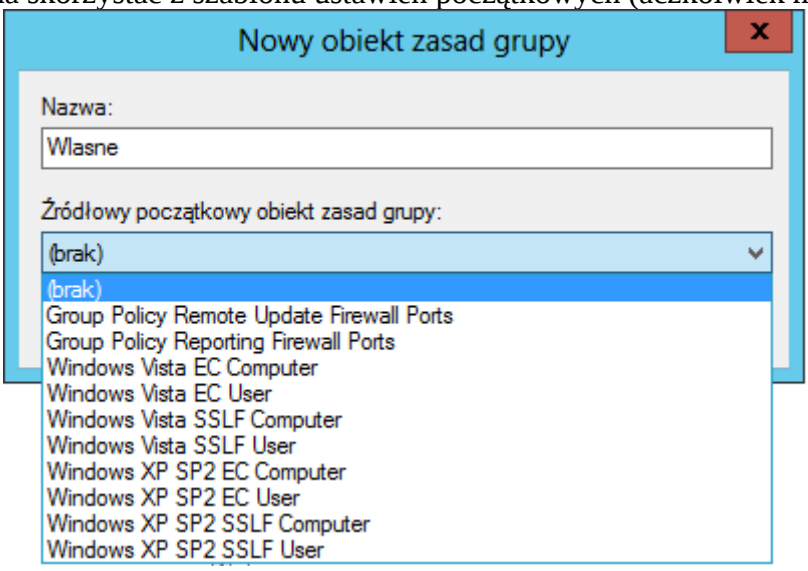


Tym samym wiemy, że okres ważności hasła system przechowuje jako liczbę dni, po których system ma poprosić użytkownika o zmianę hasła. Maksymalna ilość dnia dla ważności hasła to niemal 1000 dni (dokładnie 999). Jeżeli natomiast nie chcemy ustawiać ważności hasła to możemy wpisać wartość 0 – system będzie wiedział, że hasło jest ważne bezterminowo. Proszę zwrócić uwagę, że poszczególne zabezpieczenia (jak wyżej omawiane) można zdezaktywować poprzez odznaczenie opcji Definiuj następujące ustawienie zasad. Wtedy wartość takiego zabezpieczenia będzie ustawiona na Nie zdefiniowano, a system domyślnie przyjmie, że hasła są bezterminowe.

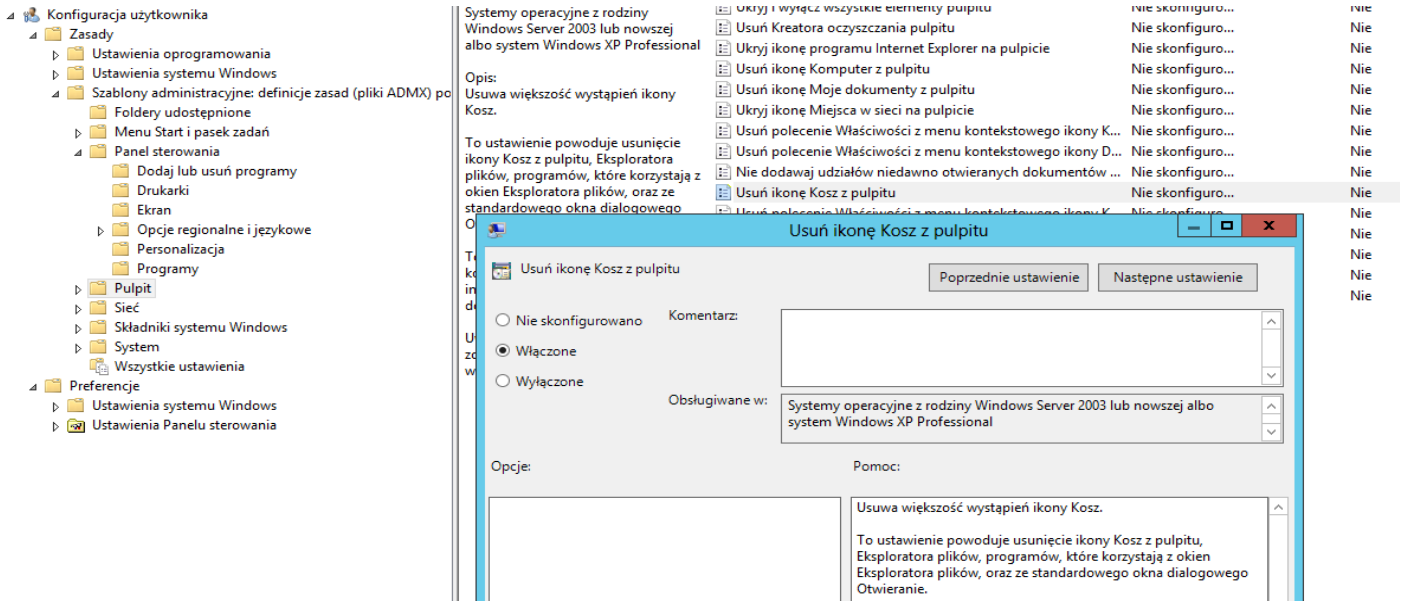
Tworzenie nowych zasad grupy zabezpieczeń jest stosunkowo proste. Należy wejść w kontener Obiekty zasad grupy, kliknąć prawym przyciskiem myszy na prawej przestrzeni (są w niej 2 grupy zabezpieczeń) i z menu wybrać Nowy (można też kliknąć prawym przyciskiem myszy na kontener)



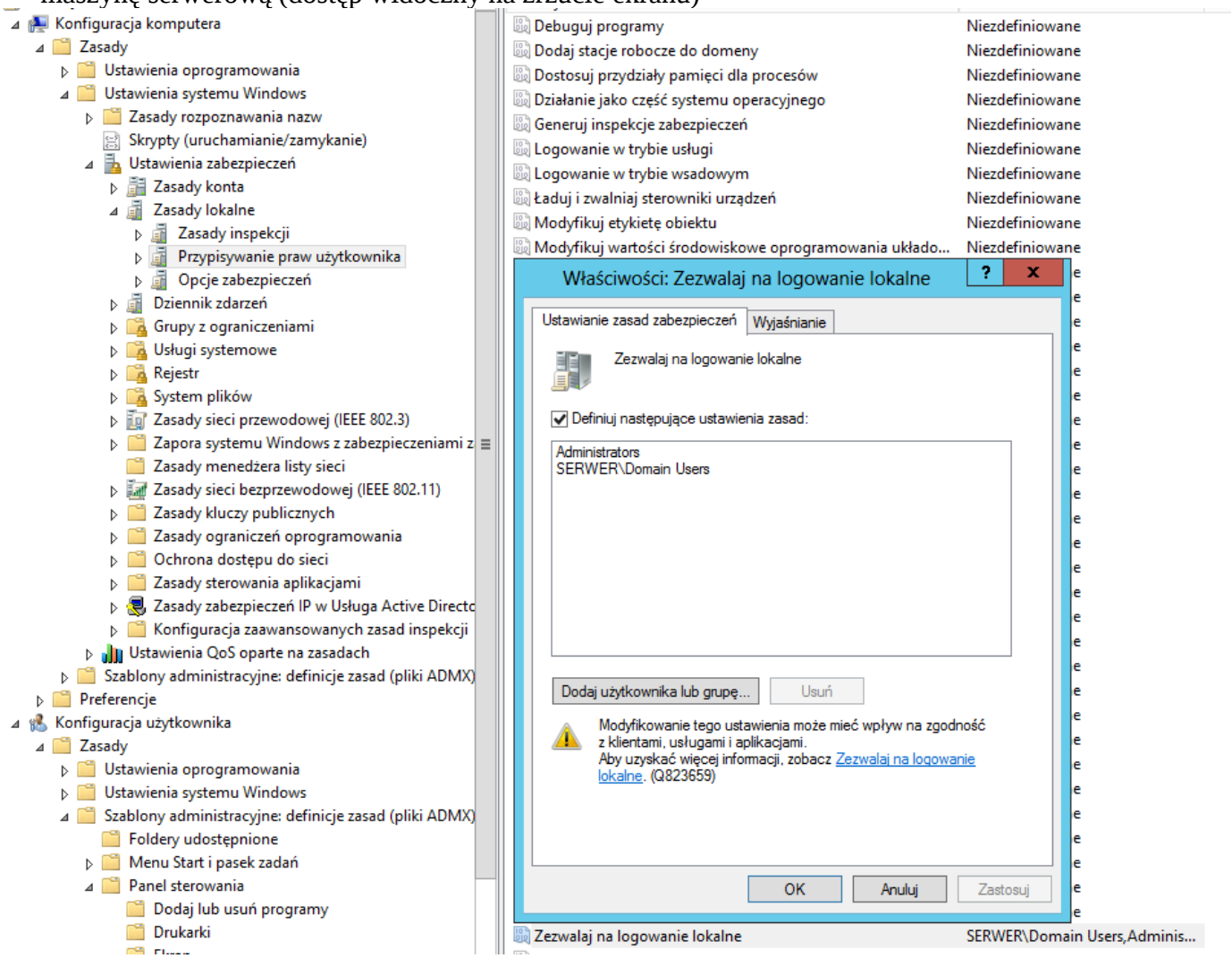
Pojawi się nowe okno, w którym należy wpisać nazwę nowego obiektu zasad grupy (dowolna). Opcjonalnie można skorzystać z szablonu ustawień początkowych (aczkolwiek nie trzeba).



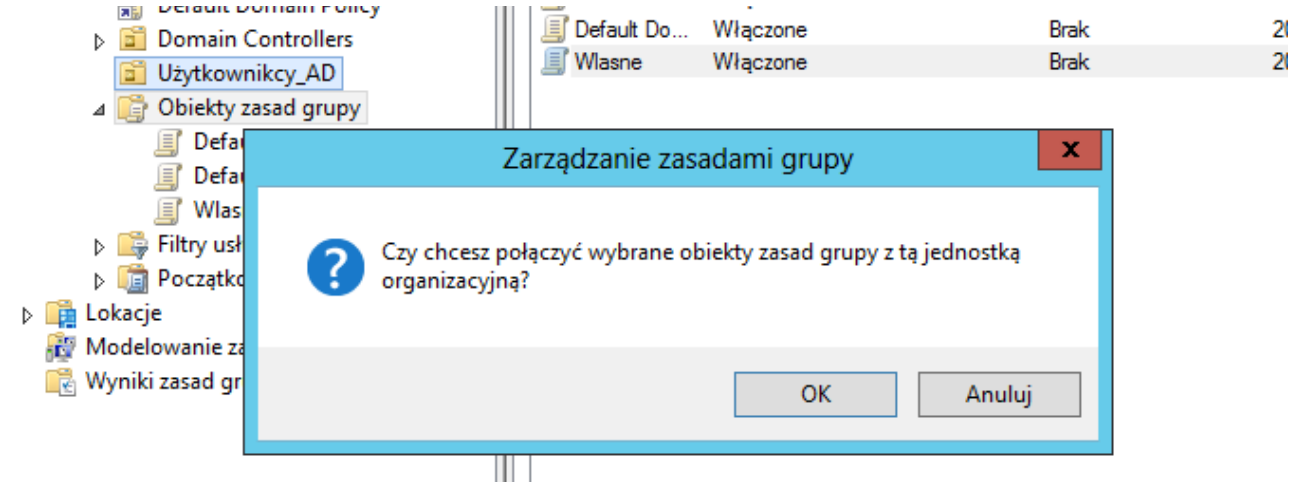
Po akceptacji nowa grupa zabezpieczeń pojawi się w otwartym kontenerze.
Teraz spróbujmy zmienić jakąś opcję systemową, którą zauważymy zaraz po zalogowaniu do systemu klienckiego. W tym celu wymuśmy usunięcie ikony kosza z pulpitu (poniższy zrzut ekranu przedstawia lokalizację zasady):



Stan „Włączone” (widoczny na zrzucie) aktywuje usunięcie ikony (nie robi tego natomiast opcja Wyłączone – ona oznacza, że kosz będzie widoczny!; tyczy się to większości ustawień).
Drugą opcją niech będzie zezwolenie logowania się naszego zwykłego użytkownika lokalnie na maszynę serwerową (dostęp widoczny na zrzucie ekranu)

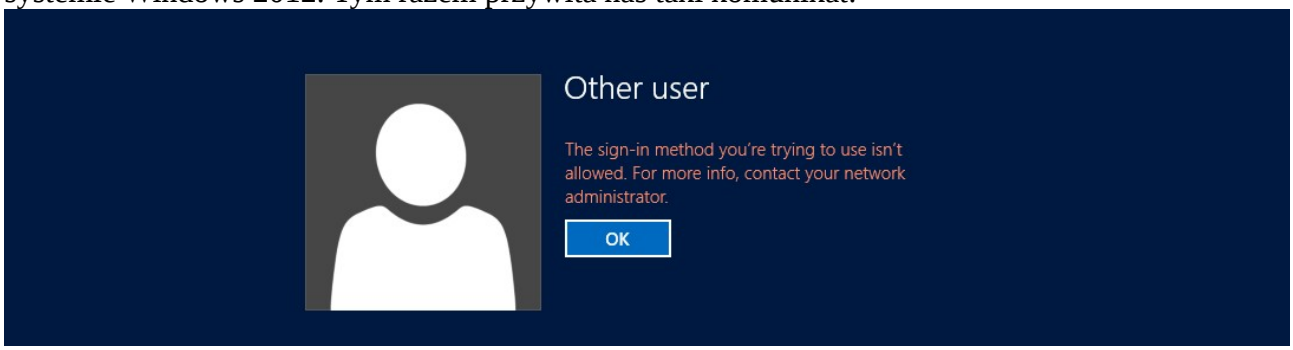


Ustawiamy jak na zrzucie.
Teraz dodajmy naszą politykę zabezpieczeń dla naszych użytkowników (w tym wypadku kontener Użytkownicy_AD) Wystarczy przeciągnąć go i upuścić nad kontener, o resztę zadba narzędzie.

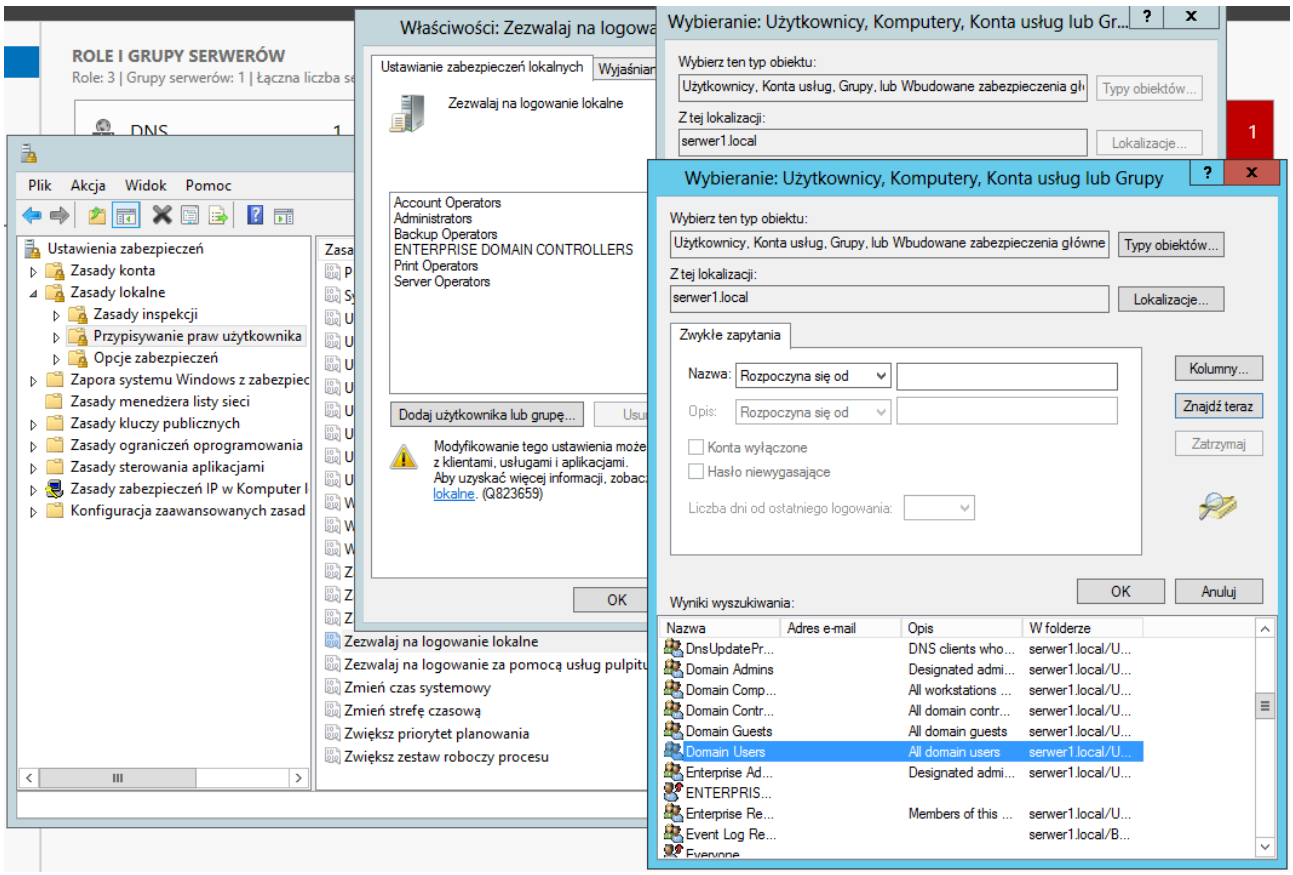


Na powyższe pytanie odpowiadamy twierdząco.
Teraz zalogujmy się na system Windows 8.1. Pulpit zaraz po zalogowaniu powinien wyglądać w ten sposób:

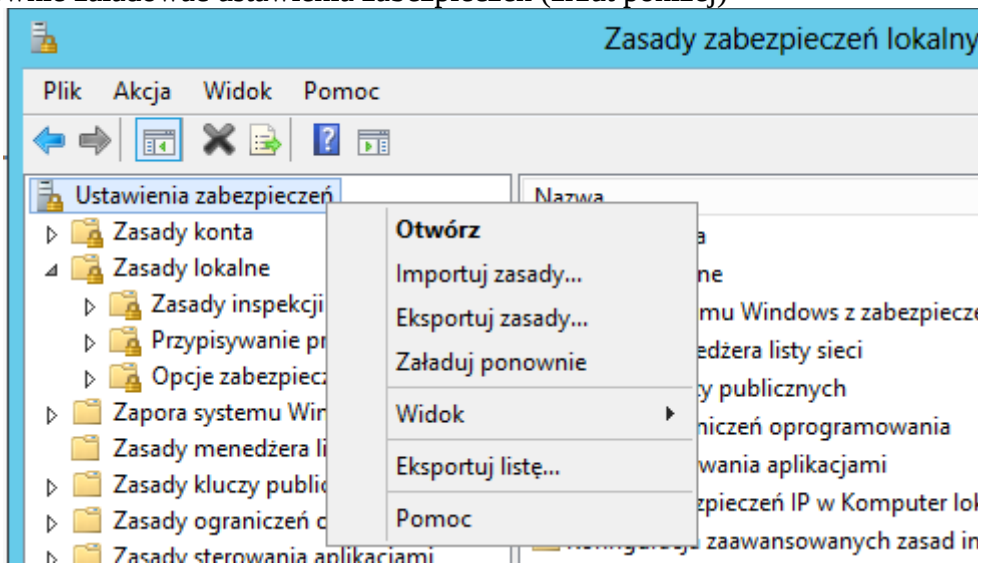
Ikona kosza zniknęła. Spróbujmy w takim układzie zalogować się jako zwykły użytkownik na systemie Windows 2012. Tym razem przywita nas taki komunikat:



oznaczający mniej więcej tyle, że nasz użytkownik nie ma praw do logowania się systemu poprzez konto lokalne. Dlaczego tak się stało?
Otóż na serwer nie działa polityka zabezpieczeń domeny. Tak naprawdę na system wpływa tylko i wyłączenie polityka zabezpieczeń lokalnych.
Wróćmy na konto Administratora i wybierzmy Zasady zabezpieczeń lokalnych. W otwartym oknie wybieramy Zasady lokalne->Przypisywanie praw użytkownika. Odnajdujemy frazę Zezwalaj na logowanie lokalne. W nowo otwartym oknie klikamy Dodaj użytkownika lub grupę... Wyskoczy okno Wybieranie: Użytkownicy, Komputery, Konta usług lub Grupy , w którym wybieramy przycisk Zaawansowane... . W nowym oknie klikamy Znajdź teraz. W wynikach wyszukiwania odnajdujemy grupę Domain Users (Użytkownicy domeny w polskiej wersji) bądź nazwę konta naszego użytkownika i klikamy go dwukrotnie. Poniższą akcję ilustruje poniższy zrzut:



INFORMACJA: W przypadku gdyby przycisk Dodaj użytkownika lub grupę... nie był aktywny należy ponownie załadować ustawienia zabezpieczeń (zrzut poniżej)



Po tej operacji zasady zabezpieczeń lokalnych powinny być dostępne. Można ponownie spróbować zalogować się jako zwykły użytkownik do serwera. Tym razem bez problemu powinniśmy zalogować się na nasze konto.

ZADANIA:

1. Proszę zmodyfikować zasady zabezpieczeń haseł – minimalna długość hasła na 10 znaków, hasło powinno być zmieniane co 30 dni, czas blokady hasła na 3 minuty (przy 3 nieudanych próbach zalogowania) oraz czas wyzerowania licznika po 10 minutach. Dodatkowo użytkownicy domenowi (nie administratorzy!) nie powinni mieć możliwości logowania się do systemu przez pulpit zdalny.
2. Każdy użytkownik domeny powinien mieć ustawiony jeden, domyślny awatar (np. z logo

szkoły). Ponadto proszę wyłączyć gadżety pulpitu (mało bezpieczne). Użytkownicy nie powinni mieć możliwości uruchamia Windows Media Center. Proszę również zezwolić by użytkownicy domeny mogli instalować sterowniki do urządzeń.
PODPOWIEDŹ: opcje znajdują się szablonach administracyjnych konfiguracji komputera.
3. Proszę foldery Pulpit oraz pobieranie przekierować do jednego, wspólnego dla wszystkich użytkowników katalogu.
4. Użytkownicy powinni mieć zabroniony dostęp do panelu sterowania.
5. Użytkownicy nie powinni mieć możliwości dopasowywania pasków narzędzi pulpitu.
6. Użytkownicy domeny nie powinni mieć dostępu do łącza Gry.
7. Ikony folderów Muzyka oraz Sieć powinny być ukryte.
8. Dostęp do wiersza poleceń powinien zostać zabroniony.
9. Użytkownicy nie powinni mieć możliwości uruchamiania aplikacji Notatnika oraz Internet Explorera (odpowiednio notepad.exe oraz iexplore.exe)
10. Użytkownicy nie powinni mieć możliwości udostępniania plików w otoczeniu sieciowym.
11. Należy zabronić możliwości wyświetlenia stanu aktywnego połączenia.

Po wykonaniu zmian należy zalogować się na konto użytkownika i sprawdzić efekt działań. Następnie należy zalogować się na stacji roboczej jako administrator domeny (konto Administrator) i zobaczyć czy jego również tyczą się ustawione przez nas zabezpieczenia. Jaki będzie efekt? Proszę także przetestować inne ustawienia (dodawanie innych polityk zabezpieczeń, włączanie/wyłączanie ogólnych zabezpieczeń itp.).