OKIEM EKSPERTA

Windows Server 2022 dla profesjonalistów

Profesjonalna administracja środowiskiem Windows Server

Wydanie IV

Jordan Krause

Helion

packt

Tytuł oryginału: Mastering Windows Server 2022: Comprehensive administration of your Windows Server environment, 4th Edition

Tłumaczenie: Łukasz Piwko z wykorzystaniem fragmentów poprzedniego wydania w przekładzie Jacka Janusza

ISBN: 978-83-289-0834-5

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/ws22p4
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Rozdział 5

Zasady grupy

Jeśli czytasz tę książkę od początku do końca, co wcale nie jest żadnym dziwactwem, to masz już pewne pojęcie o zasadach grupy (ponieważ poświęciłem im parę zdań w rozdziale 3., „Active Directory"). Jednak jestem w branży IT wystarczająco długo, aby wiedzieć, że mało komu zdarza się przeczytać książkę od deski do deski. Dlatego chcę uspokoić wszystkie osoby, które trafiły na ten rozdział przypadkiem, bo przyciągnęły je słowa „zasady grupy" lub szukają odpowiedzi na konkretne pytanie. Na początku podsumujemy piękno i siłę tego, co nazywa się zasadami grupy.

Każdy bez trudu rozumie słowo „zasada", czyli pewien zbiór reguł lub standard, których należy przestrzegać. W naszym przypadku jest mowa o komputerach (i serwerach) z systemem Microsoft Windows. Zastosowanie zasad do komputerów, na przykład zasad bezpieczeństwa, zasad aplikacji albo zasad drukarek, wydaje się doskonałym pomysłem. A skoro tak, to odniesienie ich do całych grup komputerów powinno być jeszcze lepsze. Stąd właśnie wzięła się nazwa *Zasady grupy* (ang. *Group Policy*). W skrócie: **zasady grupy** to scentralizowana metoda definiowania reguł obowiązujących komputery w sieci naszej domeny. Poniżej znajduje się lista tematów, które omawiam w tym rozdziale:

- Obiekty zasad grup.
- Tworzenie obiektu zasad grupy.
- Określanie zakresu obiektu zasad grupy.
- Ustawienia komputera i użytkownika.
- Zasady a preferencje.
- Domyślne zasady grupy.
- Szablony administracyjne.
- Magazyn centralny.

Obiekty zasad grupy

To jest bardzo proste. Ogólna technologia, którą teraz omawiamy, nazywa się zasadami grupy, a indywidualny egzemplarz takich zasad to **obiekt zasad grupy** (ang. *Group Policy Object*, GPO).

GPO to pojedynczy pakiet zawierający jedno lub więcej ustawień, który odnosi się do komputera domeny, użytkownika domeny lub czasami do wielu komputerów i użytkowników na raz.

Obiekty GPO są przechowywane w Active Directory i replikowane między serwerami kontrolerów domen. Za każdym razem, gdy użytkownik domeny loguje się do należącego do domeny komputera, który jest połączony z naszą siecią, komputer ten pyta usługę Active Directory, czy ma dla niego jakieś ustawienia GPO. Następnie rusza cała lawina zdarzeń. Kontroler domeny przekazuje wszystkie ustawienia GPO, które odnoszą się do danego komputera i użytkownika. To jest kluczowa informacja. Podczas tworzenia obiekty GPO mają określany zakres, co pozwala nam na wskazanie, do kogo odnosi się każda zasada. To bardzo przydatne. Następnie ustawienia zasad zostają przesłane na nasz komputer i wymuszają pewne zdarzenia (lub ich niewystąpienie) zgodnie z wolą naszego działu informatycznego. Możemy zablokować ustawienia, wymusić ich wprowadzenie albo skonfigurować domyślne ustawienia, które użytkownicy będą mogli w razie potrzeby zmienić. Na niektórych komputerach można zastosować jeden zbiór ustawień, a na innych można zastosować całkiem przeciwne ustawienia. Można nawet zastosować wykluczające się GPO do jednego komputera, a potem patrzeć na wojnę między nimi, aby dowiedzieć się, kto wygra. Jeśli ktoś nie wie, jak działają Zasady grupy, to bardzo łatwo może narobić poważnych problemów w sieci, ponieważ za ich pomocą można zastosować ustawienia do wszystkich komputerów w domenie. Wystarczy jeden niepoprawnie użyty obiekt GPO, aby powalić całą sieć na kolana.

To brzmi bardzo uspokajająco, prawda? Wierz mi — choć podczas korzystania z zasad grupy należy pamiętać, że z wielką władzą wiąże się wielka odpowiedzialność i takie tam, to kiedy już poznasz ich możliwości, będziesz z nich bardzo często korzystać.

Przypomnienie wiadomości o zasadach grup

Wspomniałem, że zasady grupy są przetwarzane na komputerze należącym do domeny przy każdym logowaniu użytkownika. Ponadto wszystkie zasady grupy są powtórnie przetwarzane w pewnych odstępach czasu w ciągu dnia, nawet wtedy, kiedy użytkownik jest zalogowany. Domyślnie takie automatyczne odświeżenie w tle odbywa się co 90 minut i prawie nikt tego nie zmienia. To oznacza, że implementacja obiektów GPO w ciągu dnia także zazwyczaj jest w porządku, ustawienia zostaną bowiem wprowadzone nawet bez potrzeby przelogowywania użytkowników lub ponownego uruchamiania komputerów. Są jednak od tej reguły wyjątki, ponieważ niektórych ustawień GPO nie da się wprowadzić w ramach cykli odbywających się w tle i mogą one zostać włączone tylko podczas logowania. Do przykładów takich GPO należą skrypt logowania (który działa tylko w trakcie logowania lub wylogowywania komputera) czy mapowanie dysku sieciowego. Niektóre GPO są wysyłane do komputerów tylko podczas procesu logowania.

Często zdarza mi się testować ustawienia GPO, w których wprowadzam zmiany, i czekanie na koniec 90-minutowego cyklu albo ponowne uruchamianie komputera za każdym razem byłoby bardzo nieefektywne. Na szczęście istnieje proste i szybkie narzędzie wiersza poleceń, które pozwala od razu wprowadzić każdą zasadę grupy.

```
gpupdate /force
```

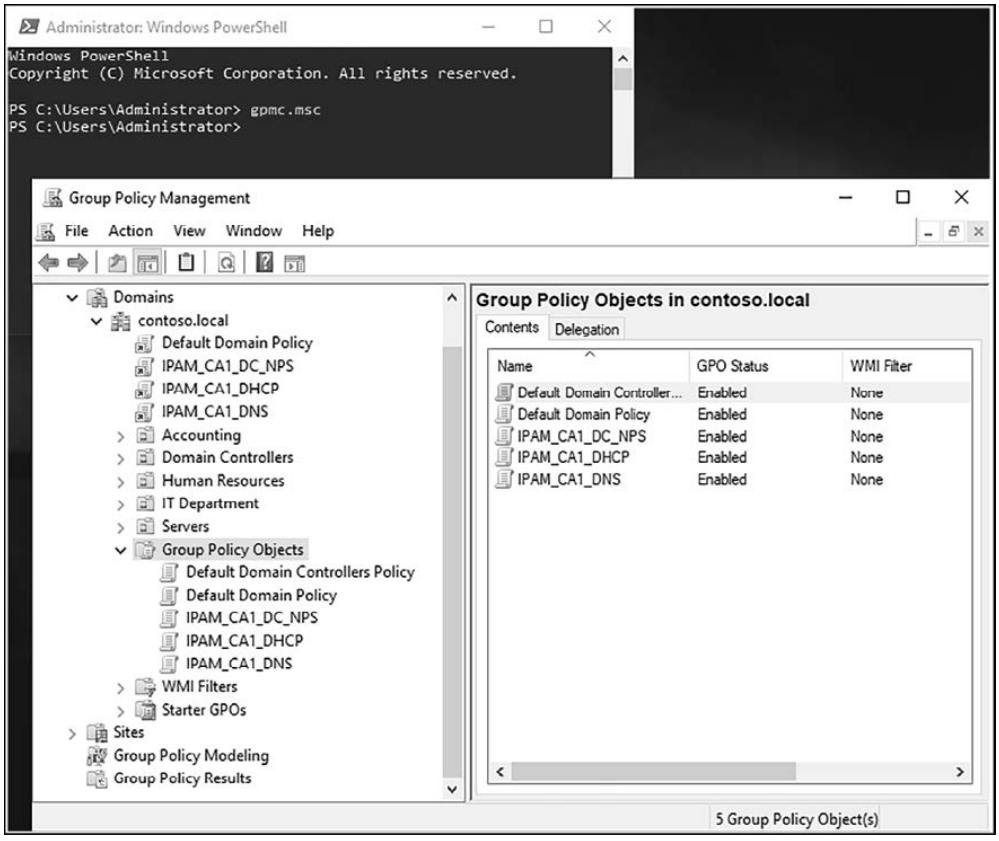
Wykonanie tego polecenia w wierszu poleceń lub narzędziu PowerShell komputera należącego do domeny spowoduje natychmiastowe wprowadzenie na nim nowych ustawień GPO. Pamiętaj tylko, że dany komputer musi mieć kontakt z kontrolerem domeny,

więc ta metoda nie zadziała, jeśli będziesz pracować w domu na laptopie niepodłączonym do sieci VPN.

Natomiast sprawdzi się ona na wszystkich komputerach w biurze lub połączonych z siecią firmową w jakikolwiek inny sposób. Polecenia `gpupdate` możesz używać do woli przez cały dzień, aby stopniowo wprowadzać nowe zasady i zmiany.

Tworzenie obiektu GPO

Najlepszą metodą nauki jest praktyka, dlatego teraz przejdziemy do rzeczy i utworzymy nowy obiekt GPO. Nie przejmuj się, na razie nigdzie go nie zastosujemy — tę przyjemność zostawimy sobie na później. Tak jak w przypadku większości innych technologii Microsoftu, do pracy z zasadami grup jest przeznaczona specjalna konsola zarządzania zasadami grupy (*Group Policy Management Console* — GPMC). Po zalogowaniu na dowolnym ze swoich kontrolerów domeny możesz uruchomić tę konsolę w *Administrative Tools* (*Narzędzia administracyjne*), w menu *Tools* (*Narzędzia*) programu *Server Manager* (*Menedżer serwera*) lub przez wywołanie programu *gpmc.msc* w menu *Start/Run* (*Start/Uruchom*), wierszu poleceń lub PowerShell (rysunek 5.1).



Rysunek 5.1. Konsola zarządzania zasadami grupy

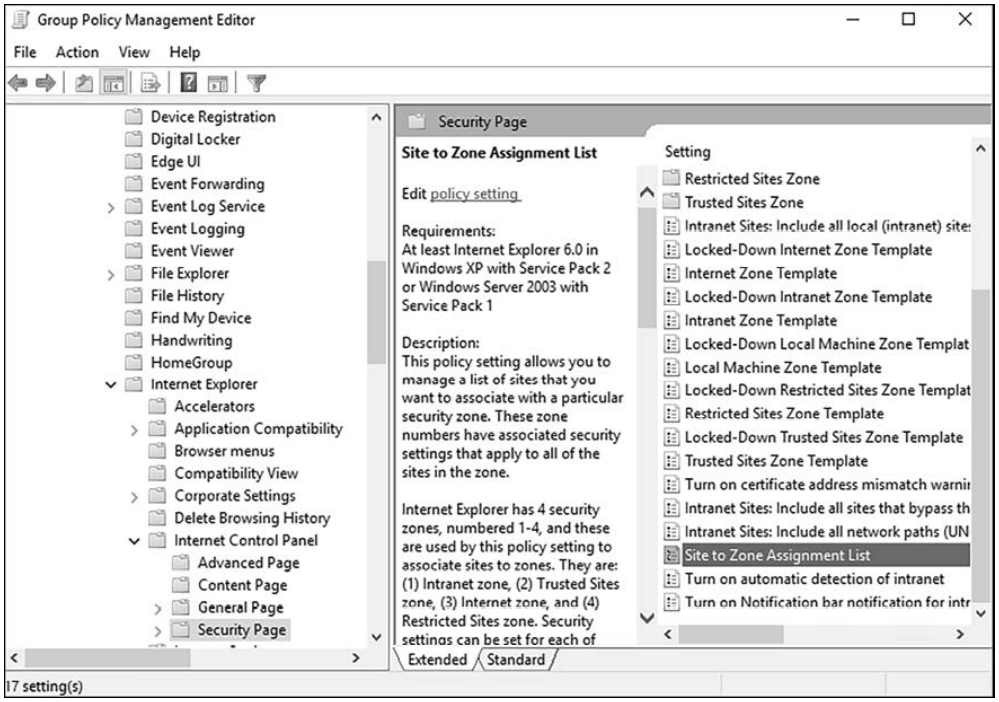
Na rysunku 5.1 zwróć uwagę, że już istnieje kilka obiektów GPO. Są to domyślne obiekty, które zawsze są dodawane podczas instalacji usługi Active Directory (więcej na temat domyślnych zasad domen piszę w dalszej części rozdziału), oraz obiekty GPO funkcji IPAM, które zostały utworzone w procesie jej konfiguracji, opisanym w rozdziale 4., „DNS i DHCP". Aby utworzyć nowy obiekt GPO w taki sposób, aby nie został zastosowany do żadnej stacji roboczej ani do żadnych użytkowników, kliknij prawym przyciskiem myszy folder *Group Policy Objects* (*Obiekty zasad grupy*) i wybierz pozycję *New* (*Nowe*). Nadaj nazwę swojemu nowemu obiektowi i kliknij przycisk *OK*. W ten sposób utworzyłeś swój pierwszy obiekt GPO! Na razie nie zawiera on żadnych ustawień ani konfiguracji oraz do niczego ani do nikogo się nie odnosi, więc jest bezużyteczny. Jednak wkrótce to zmienimy.

Dodawanie zaufanych lokalizacji

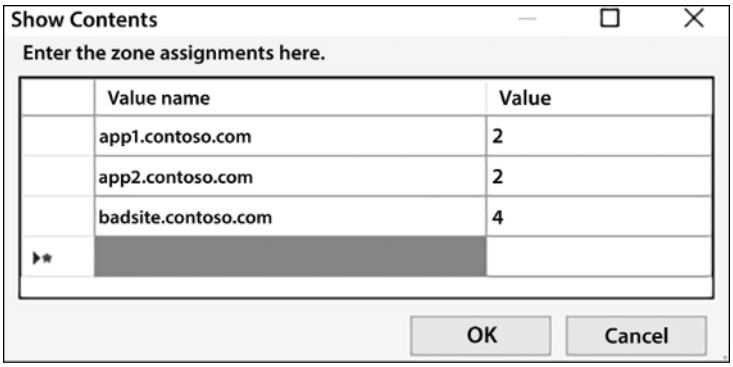
Mojemu pierwszemu GPO nadałem nazwę *Adding Trusted Sites* (*Dodawanie zaufanych lokalizacji*), ponieważ będę go używał w celu określania pewnych adresów URL jako zaufanych witryn w przeglądarce Internet Explorer na komputerze z systemem Windows 10. Jeśli w swojej sieci uruchamiasz aplikację sieciową wykorzystującą JavaScript lub kontrolki ActiveX albo coś podobnego, to być może będziesz musiał dodać tę witrynę do listy zaufanych lokalizacji w przeglądarce Internet Explorer, aby działała prawidłowo. Możesz wydrukować instrukcję dla pracowników pomocy technicznej, jak to zrobić na każdym komputerze, i poprosić ich o wykonanie tych czynności za każdego użytkownika, który zadzwoni ze skargą, że nie ma dostępu do aplikacji. Innym rozwiązaniem jest utworzenie obiektu GPO, który będzie wprowadzał zmiany automatycznie na każdej stacji roboczej, co uratuje Cię przed tymi wszystkimi telefonami. To tylko jeden mały przykład możliwości zasad grup, ale jest dobry, ponieważ jest praktyczny, a poza tym ta opcja jest głęboko zakopana w ustawieniach GPO, więc będziesz mieć okazję przyjrzeć się, jak głęboko one sięgają. Tak, zdaję sobie sprawę, że Internet Explorer już oficjalnie nie żyje i obecnie nową przeglądarką Microsoftu jest Edge. Niestety łatwiej powiedzieć, niż zrobić. Wciąż istnieje wiele aplikacji biznesowych i niestandardowych, które będą zmuszać nas do korzystania z Internet Explorera jeszcze przez wiele lat. Przechodzimy dalej.

Kliknij prawym przyciskiem myszy nowy GPO i wybierz pozycję *Edit* (*Edytuj*). Następnie wybierz kolejno *Computer Configuration/Policies/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel/Security Page* (*Konfiguracja komputera/Zasady/Szablony administracyjne/Składniki systemu Windows/Internet Explorer/Internetowy panel sterowania/Strona zabezpieczeń*). Widzisz? Mówiłem, że to głęboka struktura (rysunek 5.2).

Teraz kliknij dwa razy pozycję *Site to Zone Assignment List* (*Lista przypisywania witryn do stref*) i ustaw ją na *Enabled* (*Włączone*). To spowoduje aktywowanie przycisku *Show* (*Pokaż*), po którego kliknięciu będziesz mógł wprowadzić adresy witryn i nadać im przypisania stref. Każdemu ustawieniu GPO towarzyszy opis, z którego można się dowiedzieć, do czego dokładnie ono służy. Jak widać w przypadku wybranego przez nas ustawienia, aby ustawić wybrane witryny jako zaufane, muszę nadać im przypisanie strefy o wartości 2. Dla zabawy dodałem też jedną witrynę, której nie chcę udostępniać swoim użytkownikom, do zakazanych przez przypisanie jej wartości 4. W efekcie witryna *badsite.contoso.com* trafiła na listę witryn zabronionych na wszystkich moich komputerach (rysunek 5.3).



Rysunek 5.2. Tworzenie obiektu GPO do zarządzania zaufanymi witrynami



Rysunek 5.3. Przypisywanie witryn do różnych stref

Czy to wszystko? Prawie. Kiedy kliknę przycisk *OK*, ustawienia zostaną zapisane w GPO i będą gotowe do wdrożenia. Jak jednak wiesz, nasz obiekt GPO nie jest jeszcze do nikogo przypisany, więc na razie ma tylko ustawienia, ale nadal nic nie robi. Zanim zajmiemy się wdrażaniem, w ramach przykładu utworzymy jeszcze parę innych często używanych obiektów GPO.

Mapowanie dysków sieciowych

Serwery plików to jeden z najczęściej używanych rodzajów serwerów, ponieważ wszystkie firmy w każdej branży muszą tworzyć i prowadzić dokumentację. To nie jest rozdział o tym, jak zbudować serwer plików, określić udziały, ograniczyć uprawnienia lub korzystać z *rozproszonego systemu plików* (DFS) w celu poprawienia ogólnej elastyczności i odporności infrastruktury serwerowej, choć wszystkich tych rzeczy warto się nauczyć. Tym razem jednak zakładam, że już masz serwery plików i że znajdują się już na nich współdzielone zasoby. W swoim laboratorium testowym mam foldery udostępnione z kilku różnych serwerów:

- `\\DC1\HR`,
- `\\DC2\Accounting`,
- `\\WEB3\Installers`.

Problemem, który chcemy tu rozwiązać, jest sprawienie, aby wszystkie te współdzielone lokalizacje były automatycznie udostępniane na wszystkich stacjach roboczych mojego użytkownika. Mógłbym napisać instrukcję ręcznego dodawania tych lokalizacji przez wpisywanie ścieżek UNC w pasku adresu eksploratora plików. Mógłbym nawet pokazać kolegom i koleżankom, jak mapować dyski sieciowe w Eksploratorze plików, aby otrzymały litery dysków w ich komputerach i były w nich dostępne. Obie metody są wykonalne, ale w ten sposób przerzuciłbym część obowiązków administracyjnych na swoich użytkowników oraz dopuściłbym możliwość, że u każdego z nich udziały miałyby inną literę. U Grażyny udział *Accounting* mógłby mieć literę *R*, a u Jacka *T*.

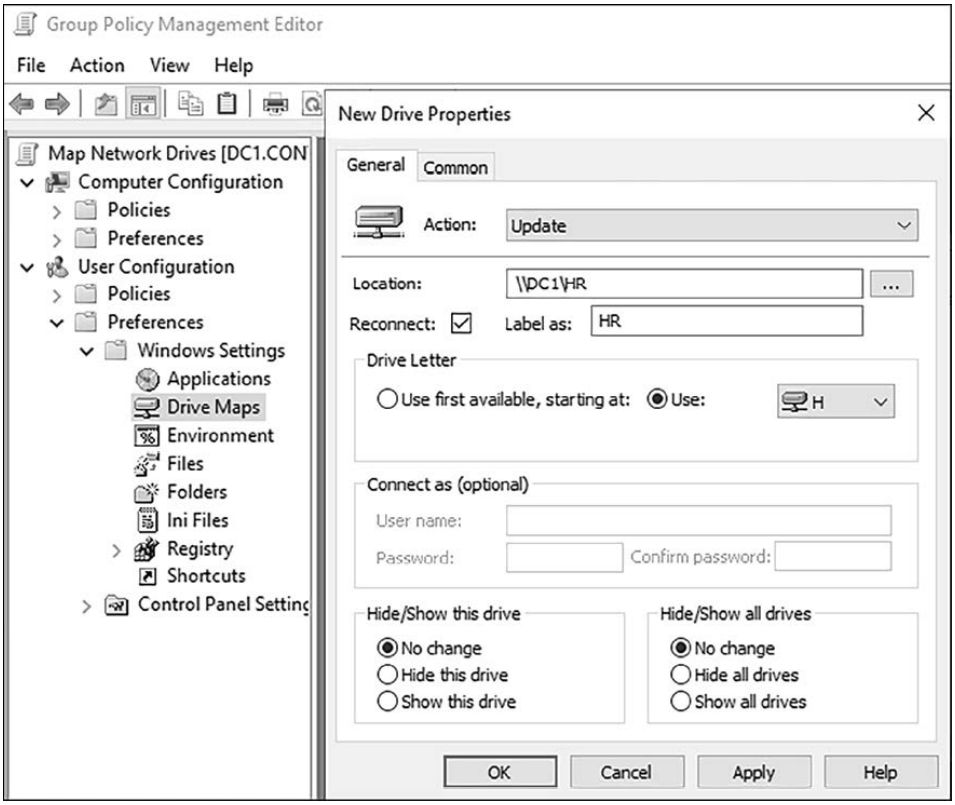
Oczywiście istnieje lepsze rozwiązanie w takiej sytuacji. Jednym z najczęstszych zastosowań obiektów GPO jest tworzenie standardowych zmapowanych dysków sieciowych na komputerach klientów. W nowym obiekcie możemy określić ścieżki UNC udziałów i przypisać im wybrane litery. Następnie przypisujemy taki obiekt do użytkowników i komputerów, a litery dysków magicznie się pojawiają, gdy użytkownicy logują się na swoich komputerach.

Utwórz nowy obiekt GPO i edytuj go w sposób opisany wcześniej. Tym razem jednak wybierz następującą pozycję: *User Configuration/Preferences/Windows Settings/Drive Maps* (*Ustawienia użytkownika/Preferencje/Ustawienia systemu Windows/Mapowanie dysków*).

Kliknięcie prawym przyciskiem myszy pozycji *Drive Maps* i wybranie pozycji *New/Mapped Drive* (*Nowy/Dysk zmapowany*) powoduje otwarcie okna konfiguracji pojedynczego zmapowanego dysku z literą. Na rysunku 5.4 widać, że mapuję dysk na ścieżkę `\\DC1\HR` oraz przypisuję mu literę `H`.

Menu rozwijane *Action* (*Akcja*) zawiera cztery pozycje: *Create* (*Utwórz*), *Replace* (*Zamień*), *Update* (*Aktualizuj*) i *Delete* (*Usuń*).

Należy dobrze zrozumieć znaczenie tych opcji, ponieważ są one obecne w konfiguracjach wielu preferencji GPO. Poniżej znajduje się zwięzły opis każdej z nich w odniesieniu do naszej nowej zasady.

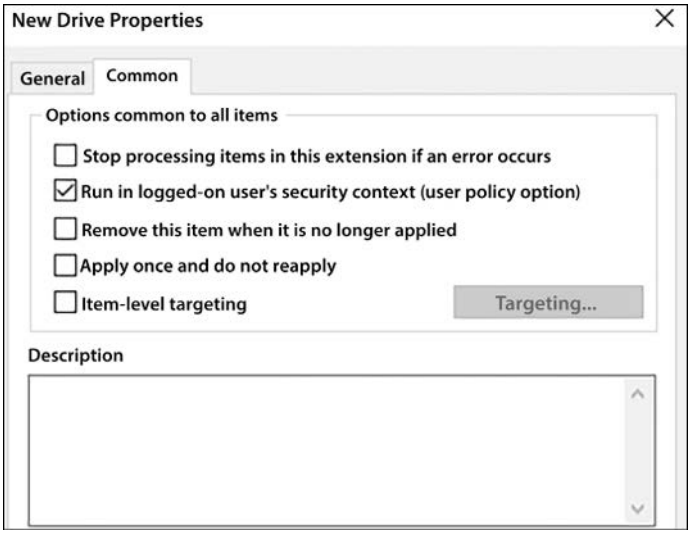


Rysunek 5.4. Mapowanie dysków przez zasady grupy

- *Create* (*Utwórz*) — ta akcja tworzy nowy zmapowany dysk, ale używaj jej tylko wtedy, gdy dysk jeszcze nie istnieje. Jeżeli litera dysku *H:* jest już używana na stacji roboczej, to nowe mapowanie zostanie zignorowane. Gdybym w naszym przykładzie użył akcji *Create*, to zostałaby ona wykonana pod warunkiem. że na danym komputerze dostępna byłaby litera dysku *H:*.
- *Replace* (*Zamień*) — ta akcja usuwa istniejące ustawienie i zastępuje je nowym. W naszym przypadku zaktualizuje mapowanie dysku *H:*, jakiekolwiek jest, przez ustawienie go na ścieżkę `\\DC1\HR`. Ta opcja jest zbędna i rzadko używana, ponieważ istnieje akcja *Update* (*Aktualizuj*).
- *Update* (*Aktualizuj*) — to jest domyślna akcja w większości ustawień preferencji i jest ona zazwyczaj najbardziej przydatna. Jeśli konfigurowane przez nas ustawienie nie istnieje, to zostanie utworzone. A jeśli już istnieje (zmapowany dysk) na danej stacji roboczej, to zostanie zaktualizowane i od tej pory będzie odzwierciedlać nową definicję GPO. Zasady mapowania dysków prawie zawsze do dodawania nowych liter dysków używają akcji *Update* (*Aktualizuj*).
- *Delete* (*Usuń*) — ta akcja usuwa wybrane ustawienie z komputera klienta. Jeśli usuwamy udział sieciowy i chcemy mieć pewność, że zostanie usunięty z wszystkich komputerów w domenie, to dzięki tej akcji możemy tego dopilnować.

Zanim w swojej definicji nowego mapowania klikniesz *OK*, przejdź jeszcze na kartę *Common* (*Wspólne*). Ta karta z pięcioma opcjami także jest dostępna w wielu ustawieniach preferencji GPO. Większość z nich nie wymaga objaśnień, chociaż określaniem wartości docelowej na poziomie elementu zajmiemy się bardziej szczegółowo w dalszej części tego rozdziału. W przypadku naszego GPO mapowania dysku chciałbym zwrócić uwagę na pole wyboru *Run in logged-on user's security context* (*Uruchom w kontekście zabezpieczeń zalogowanego użytkownika*). Nakazuje ono zasadom grupy wprowadzenie ustawień lub preferencji określonych w GPO na koncie zalogowanego użytkownika. W przypadku mapowanych dysków jest to szczególnie przydatne, ponieważ zazwyczaj chcemy, aby użytkownicy mogli korzystać ze zmapowanych dysków w swoim zwykłym środowisku.

Mimo że w większości GPO ta opcja nie jest wybierana, to akurat w przypadku GPO mapowania dysków zawsze ją włączam (rysunek 5.5).

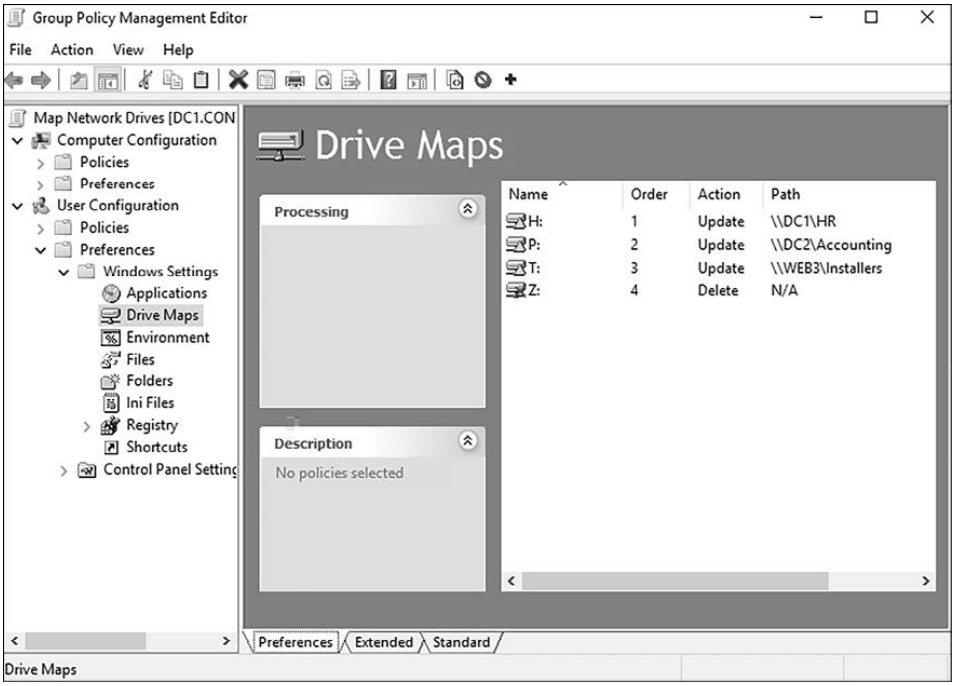


Rysunek 5.5. Mapowanie dysków w kontekście zabezpieczeń użytkownika

Wykonaj powyższe czynności dla wszystkich pozostałych liter dysków, które chcesz dodać do swojego nowego GPO, i wkrótce będziesz mógł wykonywać automatyczne mapowanie dysków w całej swojej sieci. Zdefiniowałem mapowanie dysku dla każdego z moich współdzielonych folderów oraz dodałem GPO usuwający dysk *Z:*, jeśli taki istnieje.

W moim laboratorium go nie ma, ale chodziło mi tylko o pokazanie, jak to wygląda w zasadach (rysunek 5.6).

Ten obiekt GPO także nie odnosi się jeszcze do żadnych użytkowników, ale nie martw się — kiedy utworzymy jeszcze parę przykładowych obiektów, przejdziemy do ustawień zakresów, dzięki którym zastosujemy je w akcji, oraz sprawdzimy, czy ustawienia i zmapowane dyski rzeczywiście automatycznie będą pojawiać się na komputerach klientów.



Rysunek 5.6. Dyski zmapowane przez GPO

Instalacja kluczy rejestru

Za pomocą obiektów GPO na komputerach klientów możemy tworzyć nie tylko zmapowane dyski, ale także możemy implementować klucze i wartości rejestru. Ta opcja daje szczególnie duże możliwości, ponieważ w środowisku Windows prawie wszystko można zmienić za pomocą kluczy rejestru. Utwórz więc kolejny obiekt GPO i tym razem przejdź do następującej lokalizacji: *User Configuration/Preferences/Windows Settings/Registry* (*Ustawienia użytkownika/Preferencje/Ustawienia systemu Windows/Rejestr*).

Tworzenie, zastępowanie, aktualizowanie i usuwanie kluczy rejestru przebiega mniej więcej tak samo jak w przypadku mapowania dysków sieciowych. Należy tylko uważnie wybierać opcje, aby ustawienia zadziałały. W szczególności dotyczy to pól *Key Path* (*Ścieżka klucza*) i *Value* (*Wartość*). W ramach przykładu utworzę wartość rejestru uniemożliwiającą użytkownikom zmianę obrazu tła pulpitu oraz określającą wybrany przeze mnie obraz.

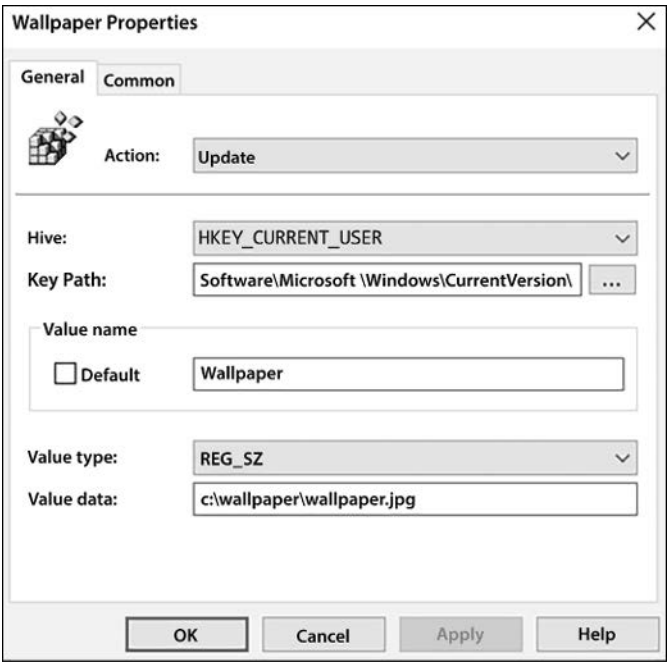
Z doświadczenia wiem, że najprostszym sposobem na zapewnienie poprawnego wypełnienia konfiguracji GPO w oknie konfiguracyjnym jest umieszczenie nowego klucza i nowej wartości rejestru na serwerze lub komputerze, na którym jest uruchomiona konsola GPMC. Dzięki temu można kliknąć przycisk z wielokropkiem i poszukać dokładnego ustawienia rejestru, zamiast próbować sobie przypomnieć jego postać w celu wpisania jej w polu *Key Path* (*Ścieżka klucza*).

W tym przykładzie wstawiam do obiektu GPO następującą informację rejestru:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
```

W kluczu rejestru systemowego nazwa wartości to *Wallpaper* (*Tapeta*).

Na rysunku 5.7 widać wypełnione przeze mnie pola w zasadach grupy.



Rysunek 5.7. Dodawanie kluczy rejestru przez zasady grupy

Ponieważ jako metodę wdrożenia tej wartości rejestru wybrałem akcję *Update* (*Aktualizuj*), za każdym razem, kiedy zasady grupy będą przetwarzane na tym komputerze, mój obiekt będzie sprawdzał, czy dany klucz rejestru istnieje, co uniemożliwi użytkownikom zmianę tapety na ich własnym pulpicie.

Zdecydowałem się na taki przykład, ponieważ jest prosty i ponieważ w zasadach grupy często zdarzają się sytuacje, że dany cel można osiągnąć na różne sposoby. Zamiast używać wartości rejestru w celu zablokowania ustawień tapety, mogłem utworzyć obiekt GPO wykorzystujący następujące ustawienie, dzięki czemu osiągnąłbym to samo bez dotykania ustawień rejestru: *User Configuration/Policies/Administrative Templates/Desktop/Active Desktop/Desktop Wallpaper* (*Ustawienia użytkownika/Zasady/Szablony administracyjne/Pulpit/Active Desktop/Tapeta pulpitu*).

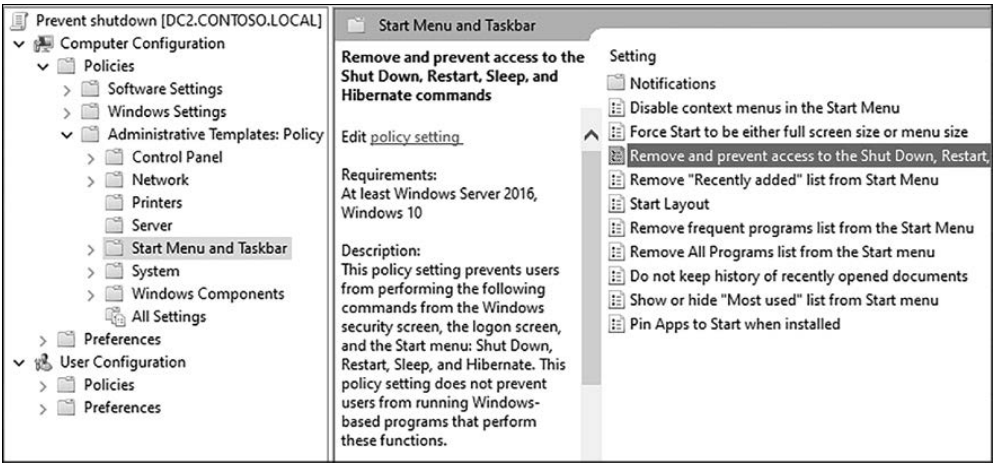
Uniemożliwianie zamknięcia systemu

Obiekty GPO bardzo często wykorzystuje się w celu tworzenia blokad bezpieczeństwa na komputerach lub serwerach. Wiele firm korzysta z usług pulpitu zdalnego, aby umożliwić użytkownikom logowanie się do wirtualnych pulpitów. Kiedy użytkownicy pracują na pulpicie zdalnym, to siedzą przy swoim komputerze, ale wszystkie czynności wykonują w obejmującym wielu użytkowników środowisku serwerowym. Gdyby któryś z nich przez

przypadek zamknął serwer, to narobiłby sporych kłopotów wszystkim pozostałym użytkownikom tego serwera. To samo dotyczy współdzielonych stacji roboczych czy komputerów, do których dostęp ma duża liczba pracowników. W tego rodzaju środowiskach jest stosowanych wiele ograniczeń, a jednym z tych, które często spotykam, jest uniemożliwienie użytkownikom zamknięcia komputera, na którym są zalogowani.

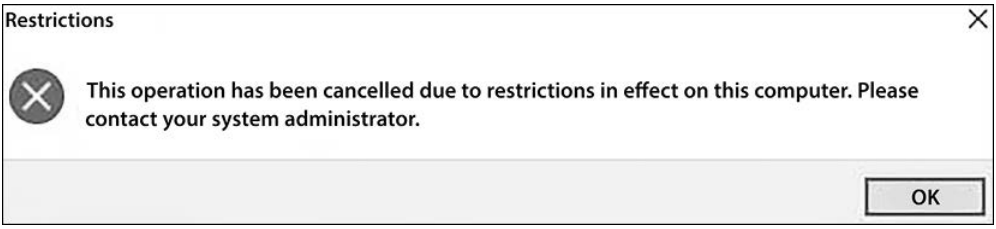
Aby zaimplementować omawiane ograniczenie do swoich maszyn, utwórz nowy obiekt GPO lub edytuj jeden z istniejących i przejdź do następującej lokalizacji ustawień: *Computer Configuration* (lub *User Configuration*)*/Policies/Administrative Templates/Start Menu and Taskbar* (*Ustawienia komputera* lub *Ustawienia użytkownika/Zasady/Szablony administracyjne/Menu start i pasek zadań*).

Teraz poszukaj pozycji o nazwie *Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands* (*Usuń polecenia Zamknij, Uruchom ponownie, Uśpienie i Hibernacja oraz wyłącz dostęp do nich*) — rysunek 5.8.



Rysunek 5.8. Obiekt GPO uniemożliwiający ponowne uruchomienie i zamknięcie systemu

Po włączeniu ta prosta zasada uniemożliwi wybranym użytkownikom zamykanie komputerów lub serwerów w Twoim środowisku domeny. Gdyby użytkownik chciał zamknąć komputer, to nie znajdzie służącej do tego opcji, ale ta zasada nie tylko usuwa przycisk zamykania. Nawet gdyby jakiś sprytny użytkownik spróbował posłużyć się czymś w rodzaju skrótu klawiszowego *Alt+F4*, który normalnie pozwala wyłączyć system, zobaczyłby tylko informację widoczną na rysunku 5.9.



Rysunek 5.9. Użytkownik nie może zamknąć systemu

Wyłączanie napędów USB

Słyszałeś kiedyś o **eksperymencie ze zgubionym pendrive'em**? Został zaprojektowany przez testerów penetracyjnych i był niezwykle pomysłowym sposobem na sprawdzenie znajomości zasad bezpieczeństwa przez pracowników firmy. Nie wiem, czy wiesz, ale podłączenie pamięci nieznanego pochodzenia do komputera to spore ryzyko. Jest wiele wirusów i ataków, których powodzenie zależy właśnie od tego, czy uda się skłonić użytkownika do włożenia zainfekowanej pamięci USB do gniazda w komputerze. We wspomnianym na początku tego akapitu eksperymencie na pendrive'ach umieszczono wirusy i rozrzucono je po parkingu firmowym, aby zobaczyć, co się stanie. Chciano sprawdzić, czy ktoś je znajdzie i podłączy do swojego komputera, aby zobaczyć, co zawierają. Gdy ktoś to zrobi, to po nim, haker przejmuje kontrolę nad jego systemem i jego informacjami.

Jeśli więc kiedykolwiek znajdziesz pamięć USB na ziemi albo jakiś sprzedawca wręczy Ci pendrive'a z rzekomymi materiałami marketingowymi podczas targów handlowych, to jedynym właściwym zachowaniem jest wyrzucenie tej rzeczy do śmieci.

Czy możesz wysłać do wszystkich pracowników e-maila z informacją o takim ryzyku? Jasne. Czy możesz ich poprosić, aby nigdy nie podłączali pamięci USB do swoich komputerów? Pewnie. Czy Cię *posłuchają*? Jestem prawie pewny, że nie. Ochrona przed takimi zdarzeniami będzie naszym ostatnim przykładem obiektu GPO. Wystarczy zmienić jedno ustawienie w GPO odnoszącym się do wszystkich komputerów w domenie, aby błyskawicznie zapewnić ochronę swojej firmy przed takim niebezpieczeństwem: *Computer Configuration/Policies/Administrative Templates/System/Removable Storage Access/All removable storage classes: Deny all accesses* (*Ustawienia komputera/Zasady/Szablony administracyjne/System/Dostęp do magazynu wymiennego/Wszystkie klasy magazynów wymiennych: odmowa dostępu*).

Włącz tę opcję, i gotowe.

Określanie zakresu obiektów GPO

Wcześniej napisałem, że zakres obowiązywania obiektów GPO można ograniczać do wybranych urządzeń lub użytkowników. Jest to chyba najważniejszy składnik całej technologii zasad grupy, który koniecznie trzeba dobrze rozumieć. Poznałeś już kilka przykładów definiowania ustawień w obiektach GPO, a w internecie można znaleźć mnóstwo informacji i dokładnych instrukcji, jak zdefiniować różne przydatne ustawienia. Jeśli chcesz wykonać jakieś zadanie na dużą skalę, poszukaj go w internecie i dodaj słowo GPO, a na pewno szybko znajdziesz informacje, jak utworzyć odpowiedni do danego celu obiekt GPO.

Jednak z tych artykułów, dokumentów Microsoftu i wpisów na blogach *nie* dowiesz się, w jakim zakresie swojej sieci zastosować dane ustawienie oraz jak dopilnować, aby nie był on zbyt szeroki. Ta decyzja należy wyłącznie do Ciebie. W tym podrozdziale opisuję dostępne w każdym obiekcie GPO opcje umożliwiające bardzo szczegółowe określenie, kto powinien otrzymać dane ustawienia lub kto nie powinien go otrzymać.

Linki

Link GPO to prawdopodobnie najważniejsze narzędzie w zestawie zasad grupy. Wiąże on obiekt GPO z lokacją w usłudze Active Directory. Połączony w ten sposób obiekt będzie stosował swoje ustawienia do użytkowników i urządzeń znajdujących się w danej lokacji.

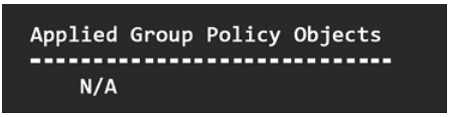
W zasadach grupy utworzyliśmy kilka obiektów GPO, ale jeszcze żadnego z nich nie zastosowaliśmy do czegokolwiek. To znaczy, że nasze obiekty nie są z niczym połączone, a kiedy to zmienimy, zaczną wykonywać swoją pracę. Zanim jednak połączymy z czymś nasze nowe obiekty, sprawdzimy, jakie obiekty GPO obecnie odnoszą się do mojego komputera z systemem Windows 10. Dzięki temu po utworzeniu połączenia będziemy mogli zweryfikować, czy nowy GPO rzeczywiście coś robi.

Narzędzie Gpresult

Do tej pory jeszcze nie było mowy o tym, jak sprawdzić, jakie zasady odnoszą się do wybranego komputera. Dlatego teraz zrobimy sobie krótką przerwę od konfiguracji i zajmiemy się tym tematem. Po zalogowaniu się do swojego komputera klienta z systemem Windows 10 mogę uruchomić wiersz poleceń lub PowerShell i wykonać następujące polecenie:

```
Gpresult /r
```

Zwraca ono sporo ciekawych informacji, ale w tej chwili najbardziej interesuje nas sekcja o nazwie *Applied Group Policy Objects* (*Zastosowane obiekty zasad grupy*). Zwróć tylko uwagę, że wyniki tego polecenia są podzielone na dwie części. Jedna jest zatytułowana *Computer Settings* (*Ustawienia komputera*), a druga — *User Settings* (*Ustawienia użytkownika*). Wkrótce dowiesz się, jaka jest różnica między ustawieniami komputera i użytkownika w GPO, a na razie chcę tylko podkreślić, że obecnie na moim testowym kliencie nie są zastosowane żadne obiekty GPO na poziomie użytkownika, co widać na rysunku 5.10.



Rysunek 5.10. Brak obiektów GPO zastosowanych do użytkownika

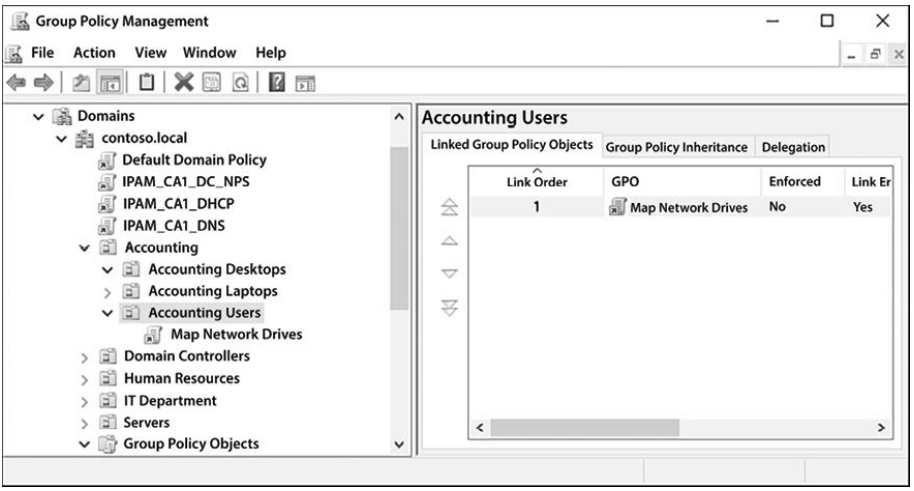
Kiedy już bardziej oswoisz się z zasadami grupy, być może często będziesz używać narzędzia `Gpresult` i wtedy przyda Ci się umiejętność ograniczania wyników tylko do ustawień użytkownika lub komputera. Jest to bardzo łatwe i polega na użyciu specjalnego przełącznika do tego polecenia:

```
Gpresult /r /scope computer
Gpresult /r /scope user
```

Ciąg dalszy z linkiem

Wracając do konsoli GPMC, znajdź w niej lokalizację, z którą chcesz *połączyć* swój nowy obiekt GPO. Ja połączę swój GPO o nazwie *Map Network Drives* i udowodnię, że wszystkie moje zmapowane dyski sieciowe zostaną automatycznie zmapowane podczas następnego logowania do stacji roboczej. Konto użytkownika, za pomocą którego się loguję, należy

do użytkowników z księgowości (*Accounting Users*). Dlatego klikam prawym przyciskiem myszy *Accounting Users* i wybieram pozycję *Link an Existing GPO* (*Połącz z istniejącym obiektem zasad grupy*). Na następnym ekranie znajdź swój nowo utworzony obiekt GPO i go wybierz. W ten sposób połączyłeś ten obiekt z wybraną jednostką organizacyjną i zmiana ta zostaje od razu wdrożona w Twojej sieci. Na rysunku 5.11 widać moje połączenie GPO pod jednostką organizacyjną *Accounting Users*.



Rysunek 5.11. Łączenie obiektu zasad grupy z jednostką organizacyjną Accounting Users

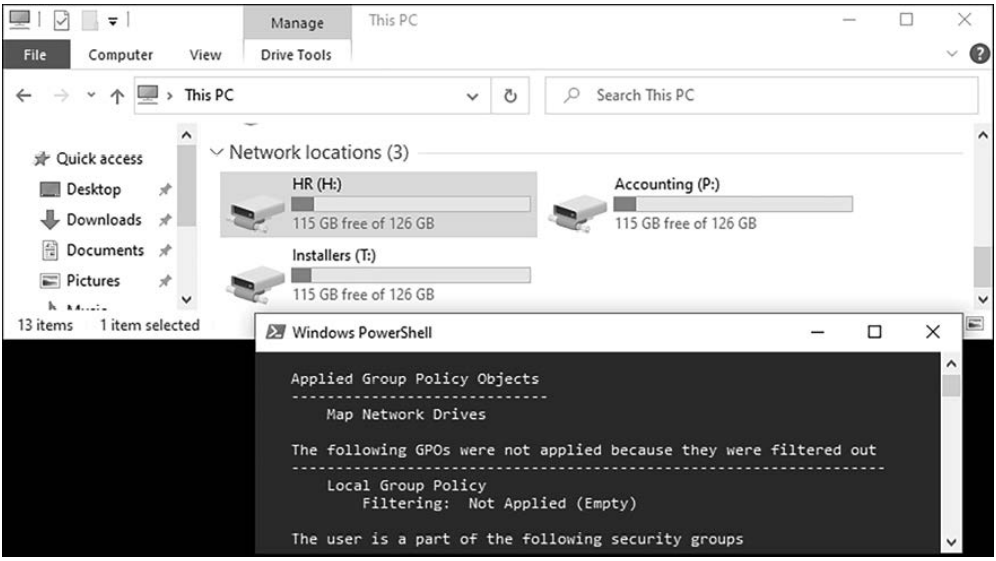
Kiedy następnym razem użytkownicy z tej jednostki zalogują się na komputerze należącym do domeny, to podczas procesu logowania powinny automatycznie zostać zmapowane dyski sieciowe.

Po zalogowaniu się do mojego komputera z systemem Windows 10 stwierdzam, że rzeczywiście te dyski się pojawiły, a ponowne wykonanie polecenia `Gpresult` pozwala dodatkowo potwierdzić, że obiekt GPO został zastosowany (rysunek 5.12).

Obiekt GPO można połączyć z większą liczbą jednostek organizacyjnych. Wystarczy wykonać te same czynności co poprzednio, wybrawszy odpowiednie jednostki. Obiekt będzie stosowany do wszystkich jednostek, które będą miały aktywne połączenia. Aby usunąć połączenie, można kliknąć je prawym przyciskiem myszy i wybrać odpowiednią opcję lub można otworzyć ustawienia obiektu zasad grupy i tam zmodyfikować jego właściwości połączeń.

Kolejność przetwarzania zasad grupy

W opisanym powyżej przykładzie połączyliśmy obiekt GPO z wybraną jednostką organizacyjną. Na niektórych rysunkach można było zauważyć, że GPO mogą być łączone także na różnych poziomach, na przykład bezpośrednio na poziomie domeny głównej *contoso.local*. Czemu to służy? Należy wiedzieć, że podczas logowania do komputera przetwarzane są zasady grup na czterech różnych poziomach. Lokalizacja połączeń ma duże znaczenie dla tego, jaki wpływ na komputery i użytkowników będą miały nasze GPO. Przyjrzymy się tym czterem poziomom przetwarzania GPO.



Rysunek 5.12. Obiekt zasad grupy został pomyślnie zaimplementowany

Zasady lokalne

Jeśli pracujesz w branży IT dostatecznie długo, to istnieje duża szansa, że obserwujesz jakiś blog lub udzielasz się na jakimś forum, gdzie ktoś opisał narzędzie *gpedit.msc*. Jego wywołanie w dowolnym systemie Windows powoduje uruchomienie programu *Local Group Policy Editor* (*Edytor lokalnych zasad grupy*). Jest to zbiór obiektów i ustawień zasad obecnych w danym systemie. Można je modyfikować ręcznie właśnie przez *gpedit.msc* lub za pośrednictwem obiektów GPO.

Pisząc to, chcę zwrócić uwagę, że podczas uruchamiania systemu Windows i logowania się użytkownika pierwszą wykonywaną czynnością jest przetworzenie ustawień obecnych w edytorze lokalnych zasad grupy. Skoro zasady lokalne są przetwarzane jako pierwsze, to znaczy, że wszelkie poziomy zasad grupy usługi Active Directory, o których zaraz będzie mowa, mogą je zastąpić. Innymi słowy, w komputerze mogą zostać zastosowane ustawienia zasad lokalnych, ale parę milisekund później w trakcie procesu uruchamiania systemu mogą one zostać zmienione przez ustawienia zasad AD.

Zasady poziomu lokacji

Pamiętasz opis lokacji i usług Active Directory z rozdziału 3.? Tutaj mają one znaczenie. Jeśli Twoje środowisko obejmuje kilka lokacji, to połączenia obiektów GPO można definiować na poziomie indywidualnych lokacji, co pozwala zasadom grupy na wysyłanie ustawień do komputerów lub użytkowników w zależności od tego, gdzie się znajdują.

Z mojego doświadczenia wynika, że połączenia GPO oparte na lokacjach są rzadkością, ale warto o tej możliwości pamiętać podczas rozwiązywania problemów z działaniem tych obiektów. Komputery i użytkownicy otrzymują zasady na poziomie lokacji tylko wtedy, gdy fizycznie się w nich znajdują, co jest określane na podstawie adresowania IP i podsieci zdefiniowanych w usługach i lokacjach Active Directory. Jeśli komputer otrzyma

ustawienia GPO dzięki połączeniu na poziomie lokacji i są one sprzeczne z lokalnymi zasadami grupy, to ostatecznie przeważą zasady lokacji, które zostaną zastosowane na dalszych etapach procesu logowania.

Zasady poziomu domeny

Niektóre zasady i ustawienia chcemy zastosować do wszystkich komputerów lub użytkowników w całej domenie. Odpowiednim miejscem dla takich ustawień są obiekty GPO na poziomie domeny. Należy podkreślić, że same te obiekty się nie zmieniają. Stosujemy je na różnych poziomach zasad, ale GPO to GPO. Mówimy tylko o hierarchii poziomów, z którymi można je *łączyć*.

Połączenia utworzone na najwyższym poziomie domeny w zarządzaniu zasadami grup domyślnie są stosowane do wszystkich komputerów lub użytkowników należących do tej domeny. Istnieje wiele innych czynników, które mogą je przefiltrować, ale w większości przypadków, jeśli połączymy GPO na poziomie domeny, to musimy się liczyć z tym, że jego ustawienia mogą zostać zastosowane do wszystkich stacji roboczych, serwerów i użytkowników. Jeśli cofniesz się parę stron do rysunków przedstawiających zrzuty ekranu z narzędzia GPMC, to zauważysz, że wszystkie GPO IPAM są połączone bezpośrednio z domeną *contoso.local*. Są to tak zwane *połączenia na poziomie domeny*.

Przyjmując, że kontynuujemy proces logowania na komputerze, zasady poziomu domeny są stosowane po zasadach poziomu lokacji. W związku z tym wszystkie ustawienia pochodzące z zasad na poziomie lokacji są już zastosowane i potencjalnie mogły zostać zmienione (jeśli wystąpił konflikt) przez zasady poziomu domeny.

Zasady poziomu jednostki organizacyjnej

Proces logowania rozpoczęliśmy od zastosowania ustawień lokalnych zasad grupy, które następnie zostały połączone z GPO poziomu lokacji i ewentualnie przez nie zmienione. Te z kolei zostały połączone z GPO poziomu domeny (i w razie konfliktów przez nie zmodyfikowane). Na pewno się domyślasz, co chcę przez to powiedzieć. Zasady poziomu jednostki organizacyjnej zostaną zastosowane na GPO poziomu domeny.

Jednostki organizacyjne, jak może wiesz, zawierają foldery odpowiadające komputerom i kontom użytkowników należącym do domeny. Większość firm wykorzystuje jednostki organizacyjne w Active Directory do rozróżniania poszczególnych typów komputerów i użytkowników. Serwery są oddzielane od stacji roboczych, użytkownicy z działu księgowości i użytkownicy z działu HR tworzą osobne grupy itd. Zagnieżdżanie jednostek organizacyjnych też nie należy do rzadkości. Podobnie jak w Eksploratorze plików można tworzyć foldery w innych folderach, w usługach AD można tworzyć jednostki organizacyjne w innych jednostkach organizacyjnych. Jest to ważne dla organizacji naszych obiektów domeny, a także dla zasad grupy.

Łączenie obiektów GPO z konkretnymi jednostkami organizacyjnymi pozwala nam stosować różne ustawienia do różnych grup ludzi lub komputerów. Kiedy obiekt GPO jest połączony z jedną jednostką organizacyjną, to zawarte w nim ustawienia obejmują tylko ją i wszystkie jej jednostki podrzędne. Ponadto z każdą jednostką organizacyjną można połączyć wiele obiektów GPO.

Zagnieżdżone jednostki organizacyjne stanowią kolejną warstwę w tej strukturze. Pamiętaj ogólną zasadę, według której zasady grup są przetwarzane od góry, a więc GPO połączone z zagnieżdżoną jednostką organizacyjną najprawdopodobniej przeważą nad GPO połączonymi na wyższym poziomie.

Filtrowanie zabezpieczeń

Po utworzeniu obiektu GPO i połączeniu go z wybraną jednostką organizacyjną mamy wystarczająco dużo informacji, aby zacząć korzystać w naszym środowisku z zasad grupy. Dystrybucja zasad między komputerami a użytkownikami za pomocą połączeń to najczęściej wybierana przez administratorów metoda, ale w wielu sytuacjach potrzebne jest jeszcze dokładniejsze filtrowanie. Co, jeśli mamy nowy obiekt GPO, który połączyliśmy z jednostką organizacyjną obejmującą wszystkie nasze komputery, ale w pewnym momencie uznaliśmy, że na niektórych komputerach chcemy zastosować te zasady, a na innych nie? Dzielenie tych komputerów na dwie grupy tylko z tego powodu byłoby bardzo słabym rozwiązaniem. W takich sytuacjach można skorzystać z techniki **filtrowania zabezpieczeń GPO**.

Filtrowanie zabezpieczeń to czynność polegająca na ograniczaniu zasięgu obiektów GPO do wybranych obiektów Active Directory. Na każdym obiekcie GPO w katalogu można ustawić filtry, które będą ograniczać jego zakres zastosowania do wybranych użytkowników, komputerów, a nawet grup użytkowników lub komputerów. Sam uważam, że szczególnie przydatna jest możliwość odnoszenia się do grup.

Utworzony wcześniej obiekt GPO *Map Network Drives* jest obecnie połączony z jednostką organizacyjną *Accounting Users*. A co, jeśli chciałbym odrobinę zmodyfikować jego zasięg? Zamiast odnosić go do jednostki organizacyjnej, może wolałbym, aby obejmował całą domenę *contoso.local*. Czy to nie oznacza, że wtedy będzie odnosił się do wszystkiego? Tak, chyba że skorzystamy z sekcji *Security Filtering* (*Filtrowanie zabezpieczeń*), aby określić konta użytkowników lub grupy kont użytkowników, do których ma on mieć zastosowanie.

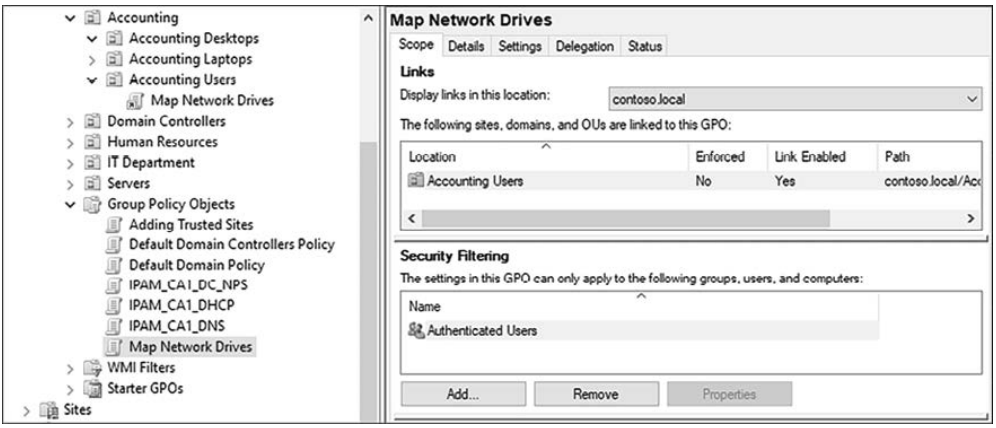
Wskazówka

Decyzje dotyczące filtrowania zabezpieczeń zawsze podejmuję przed utworzeniem połączenia. Linki stają się aktywne od razu po utworzeniu, więc uprzednia budowa odpowiednich filtrów zabezpieczeń daje pewność właściwej dystrybucji od samego początku.

Kliknięcie obiektu GPO w konsoli GPMC powoduje wyświetlenie informacji na jego temat. Na karcie *Scope* (*Zakres*) znajdują się wykaz wszystkich linków danego GPO oraz informacje dotyczące filtrowania zabezpieczeń, które zasadniczo oznaczają „wszyscy użytkownicy *i* wszystkie komputery domeny".

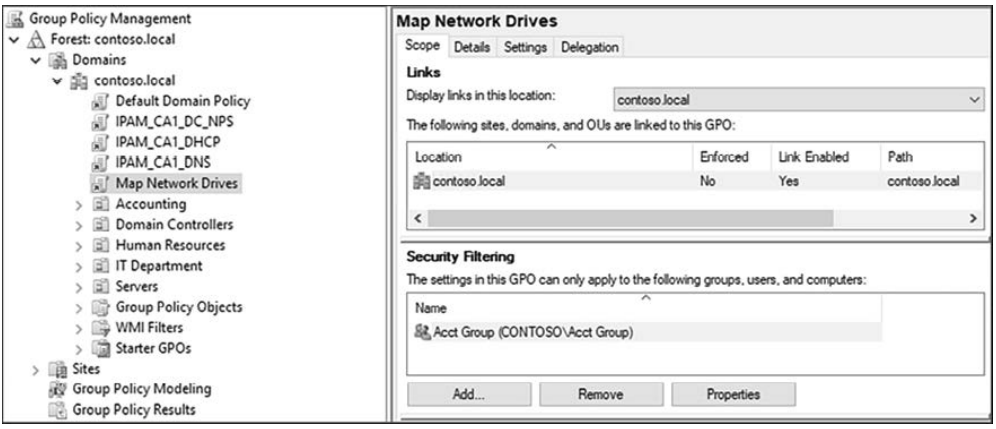
Pamiętaj, że to oznacza zarówno tych pierwszych, jak i te drugie! Na rysunku 5.13 widać dane mojego obiektu GPO *Map Network Drives*, który jest połączony z jednostką organizacyjną *Accounting Users*. Ta pozycja znajduje się w jego sekcji *Security Filtering* (*Filtrowanie zabezpieczeń*). Gdybym po prostu usunął istniejący link i utworzył nowy, na poziomie

domeny, to ten obiekt od razu zacząłby obowiązywać wszystkie konta użytkowników w całej domenie.



Rysunek 5.13. Ustawienia filtrowania zabezpieczeń obiektu GPO

Dlatego najpierw zmienię ustawienia filtrowania zabezpieczeń. Wszyscy użytkownicy z działu księgowości należą do grupy zabezpieczeń o nazwie *Acct Group* (jestem niezwykle kreatywny!). Dodanie tej grupy do sekcji *Security Filtering* (*Filtrowanie zabezpieczeń*) i **usunięcie** *użytkowników uwierzytelnionych* spowoduje, że gdziekolwiek połączę ten obiekt GPO, jego ustawienia zostaną zastosowane tylko do grupy *Acct Group*. Po wykonaniu tej czynności mogę spokojnie połączyć mój obiekt GPO z domeną najwyższego poziomu, mając pewność, że jego ustawienia będą obejmowały tylko członków grupy *Acct Group* (rysunek 5.14).



Rysunek 5.14. Ograniczanie zasięgu obiektu GPO do grupy Acct Group

Na sąsiedniej karcie, o nazwie *Settings* (*Ustawienia*), znajduje się jeszcze jedna bardzo przydatna funkcja. Kliknij tę kartę, aby wyświetlić wszystkie konfiguracje, które są obecnie ustawione w GPO. W ten sposób można łatwo sprawdzić obiekty GPO utworzone przez kogoś innego.

Filtrowanie WMI

Za pomocą dobrze zaplanowanych linków i filtrowania zabezpieczeń zakres obiektów GPO można ograniczyć na tyle precyzyjnie, że te dwie techniki wystarczą w 90% wszystkich możliwych przypadków. W tym podrozdziale opisuję metody pozwalające poradzić sobie w pozostałych 10% sytuacji. Te zaawansowane techniki filtrowania pozwalają filtrować obiekty GPO jeszcze dokładniej.

Filtrowanie WMI to genialne, choć niekoniecznie najprostsze, narzędzie, pozwalające jeszcze dokładniej określić zakres obowiązywania obiektu GPO. Filtry WMI odnoszą się do informacji WMI, które są obecne w każdym komputerze z systemem Windows, i na ich podstawie filtrują ustawienia GPO. Za pomocą filtrów WMI można sprawdzać numer wersji systemu operacyjnego, typ procesora, ilość pamięci RAM, ilość dostępnego miejsca na dysku, a czasami nawet wersję oprogramowania BIOS. Po zdefiniowaniu filtra WMI można go wybrać dla dowolnego obiektu GPO — w sekcji *WMI Filtering* (*Filtrowanie WMI*), która znajduje się bezpośrednio pod sekcją *Security Filtering* (*Filtrowanie zabezpieczeń*) w GMPC.

Filtry WMI umożliwiają wykonywanie czynności typu „zainstaluj ten ogromny program, tylko jeśli na dysku jest przynajmniej 5 GB wolnego miejsca" albo „zaimplementuj te ustawienia zapory na komputerach z systemem operacyjnym Windows Server". Innym typowym przykładem zastosowania tych filtrów jest sprawdzenie, czy dany komputer działa na sprzęcie mobilnym, co pozwala obiektom GPO odnosić się tylko do laptopów i tabletów.

Filtrowanie WMI pobiera informacje z innych składników systemu operacyjnego, a więc sprawia, że zasady grupy potrzebują trochę więcej czasu i mocy procesora. To może powodować wzrost zużycia zasobów systemowych na komputerach końcowych i spowalnia logowanie, ponieważ wszystkie czynności odbywają się w tle.

Tworzenie filtrów WMI jest ściśle powiązane z zasadami grupy, więc po dalsze instrukcje odsyłam do sekcji podsumowującej na końcu tego rozdziału, w której zamieściłem odwołanie do innej publikacji, w całości poświęconej zasadom grup.

Kierowanie indywidualne

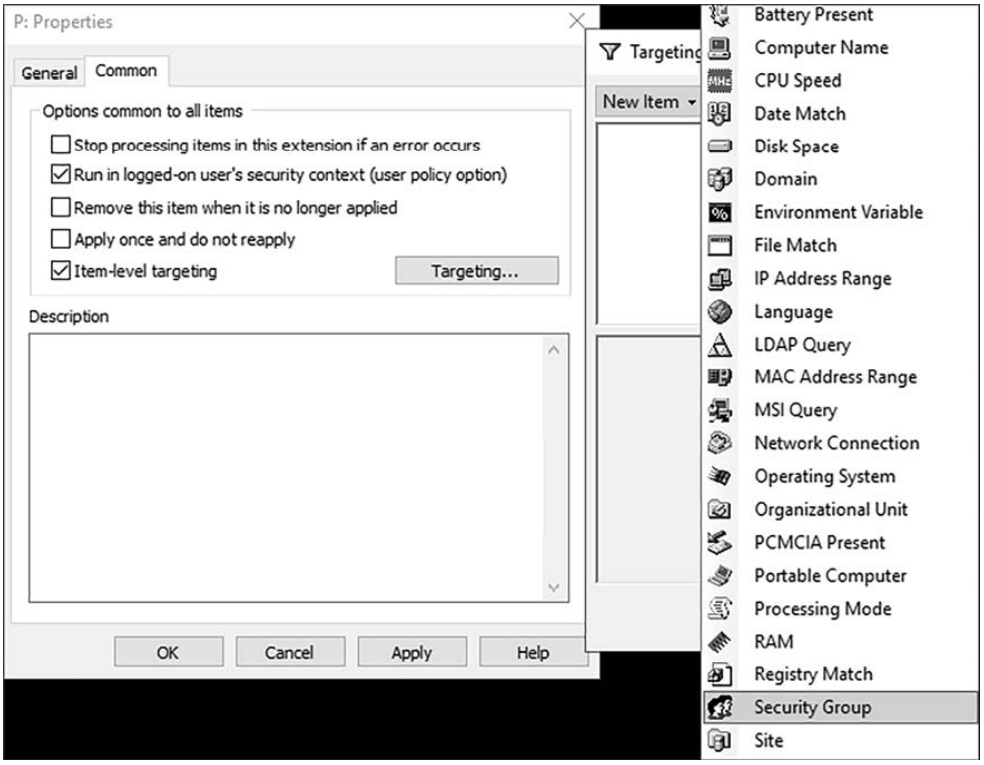
Linki, filtrowanie zabezpieczeń i filtrowanie WMI to fantastyczne narzędzia do określania zakresu zastosowania obiektów GPO do komputerów i użytkowników. A co, jeśli potrzebujemy czegoś jeszcze precyzyjniejszego? Powiedzmy, że mamy jeden obiekt GPO z wieloma ustawieniami i część z nich chcemy zastosować tylko do wybranych użytkowników lub komputerów, a resztę do innych użytkowników i komputerów.

Doskonałą ilustracją takiej sytuacji jest przykład obiektu GPO *Map Network Drives*. Zwyczajowo wszystkie dyski sieciowe umieszcza się w jednym obiekcie GPO w domenie, któremu nadaje się nazwę *Mapped Drives* lub podobną. Ponadto często jest też tak, że nie wszyscy użytkownicy powinni otrzymać wszystkie zmapowane dyski. Jakie jest najlepsze rozwiązanie w takiej sytuacji? W tym przypadku obiekt GPO można podzielić na wiele mniejszych obiektów GPO, tworząc po jednym dla każdej litery dysku, a następnie za pomocą linków i filtrów odpowiednio je rozdystrybuować między użytkownikami a komputerami. Tyle że wtedy mamy całą masę obiektów GPO, nad którymi trzeba zapanować.

W takiej sytuacji można skorzystać z opcji *Item-level targeting* (*Określanie wartości docelowej na poziomie elementu* — ILT). Nie wiem, czy pamiętasz, że wcześniej zaglądaliśmy na kartę *Common* (*Wspólne*) w ustawieniach różnych obiektów GPO. Jednym z pięciu ustawień na tej karcie jest opcja *Item-level targeting* (*Określanie wartości docelowej na poziomie elementu*), która jest dokładnie tym, czego nam potrzeba, aby spełnić marzenie o utworzeniu takiego obiektu GPO *Map Network Drives*, o jaki nam chodzi.

Jeśli przypomnisz sobie obiekt GPO *Map Network Drives* utworzony wcześniej, to będziesz wiedział, że zawiera on mapowania kilku liter dysków. Obecnie użytkownicy z mojej grupy *Acct Group* otrzymują wszystkie te dyski. Wyobraźmy sobie więc, że chcę to zmienić tak, aby mieli oni dostęp tylko do jednego z nich. W oknie edycji obiektu GPO klikam dwukrotnie mapowanie dysku *P:* i przechodzę na kartę *Common* (*Wspólne*). Zaznaczam opcję *Item-level targeting* (*Określanie wartości docelowej na poziomie elementu*) i klikam przycisk *Targeting* (*Określanie wartości docelowej*).

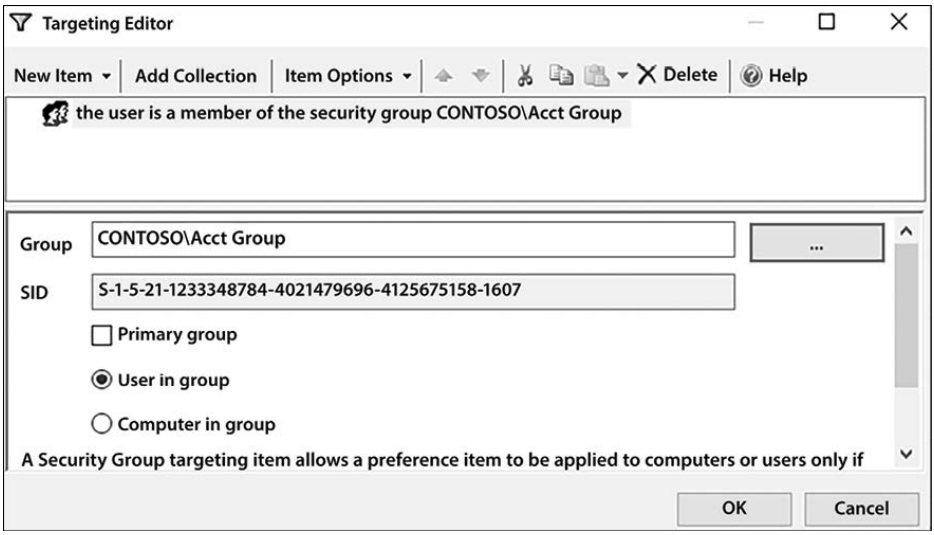
W oknie *Targeting Editor* (*Edytor elementów określania wartości docelowej*) wybierz pozycję *New Item* (*Nowy element*), co spowoduje pojawienie się długiej listy kryteriów do użycia (rysunek 5.15).



Rysunek 5.15. Dodawanie nowej grupy zabezpieczeń w edytorze elementów określania wartości docelowej

Chcę poinstruować ten obiekt GPO, że dysk *P:* powinien być mapowany tylko dla tych użytkowników, którzy należą do grupy zabezpieczeń *Acct Group*.

Wybierając dodanie nowej grupy zabezpieczeń do mojego ILT, mogę zdefiniować grupę *Acct Group*. Na rysunku 5.16 widać, że mój dysk *P:* w ustawieniach ILT został zmieniony w ten sposób, że będzie mapowany tylko podczas logowania użytkowników należących do grupy *CONTOSO\Acct Group*.



Rysunek 5.16. Stosowanie mapowania dysku P: do CONTOSO\Acct Group

Powtórz ten proces dla pozostałych dysków w swoim GPO, a otrzymasz jeden obiekt GPO zawierający wszystkie mapowania dysków dla całej organizacji. Możesz go połączyć z domeną i za pomocą filtrów ograniczyć do wszystkich uwierzytelnionych użytkowników, tak jak jest w domyślnej konfiguracji, ale dzięki ILT każdy użytkownik otrzyma mapowania tych dysków, które są przeznaczone dla jego grupy. ILT to fantastyczne narzędzie!

Delegowanie

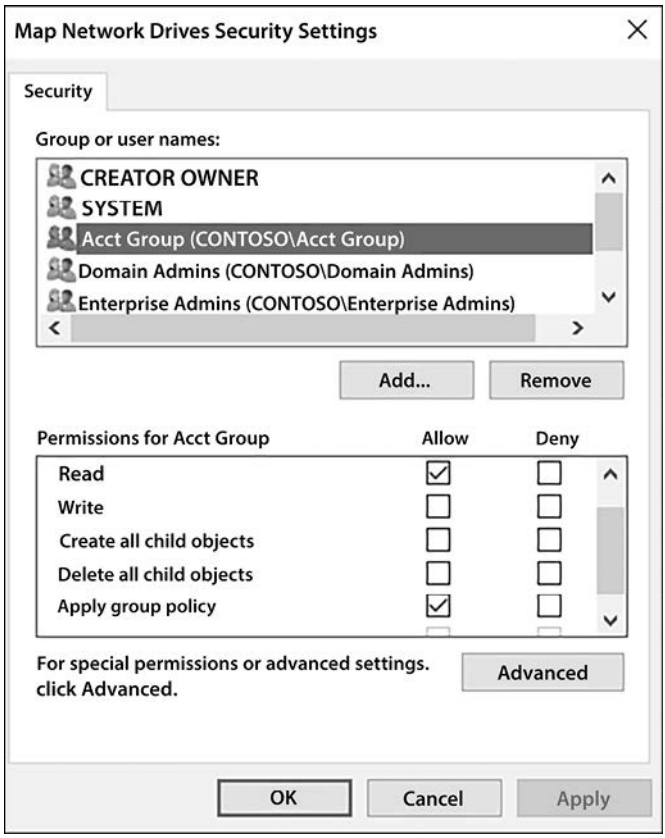
Wyobraź sobie taką sytuację: zarząd firmy prosi Cię o nałożenie ograniczeń bezpieczeństwa na wszystkich komputerach w domenie. To wygląda na idealny przypadek do użycia zasad grupy. Tylko że zarząd zarazem chce, aby jego członkowie zachowali możliwość przeglądania Instagrama i ustawiania zdjęć uśmiechniętych kociaków w tle pulpitu swoich komputerów. Dlatego poprosili, aby ograniczenia dotyczyły wszystkich *z wyjątkiem* członków grupy *Leadership* w Active Directory.

Znamy wiele sposobów na ograniczanie zasięgu obiektów GPO do wybranych użytkowników lub grup, ale jak objąć wszystko *z wyjątkiem* wybranego użytkownika lub określonej grupy? W tym celu musimy przejść do GPMC, kliknąć interesujący nas obiekt GPO i przejść na kartę o nazwie *Delegation* (*Delegowanie*).

Jeśli obiekt GPO ma zdefiniowane filtrowanie zabezpieczeń, to na karcie *Delegation* (*Delegowanie*) ujrzysz nazwy tych użytkowników lub grup.

Podczas konfiguracji filtrowania zabezpieczeń GPMC tak naprawdę w tle konfiguruje uprawnienia delegowania. Otworzyłem kartę *Delegation* (*Delegowanie*) mojego obiektu GPO *Map Network Drives*, który obecnie ma nadal zdefiniowane filtrowanie zabezpieczeń dla grupy *Acct Group*. Na karcie tej kliknąłem przycisk *Advanced* (*Zaawansowane*), który znajduje się na dole, aby otworzyć okno ze szczegółami dotyczącymi ustawień delegowania i uprawnień tego obiektu.

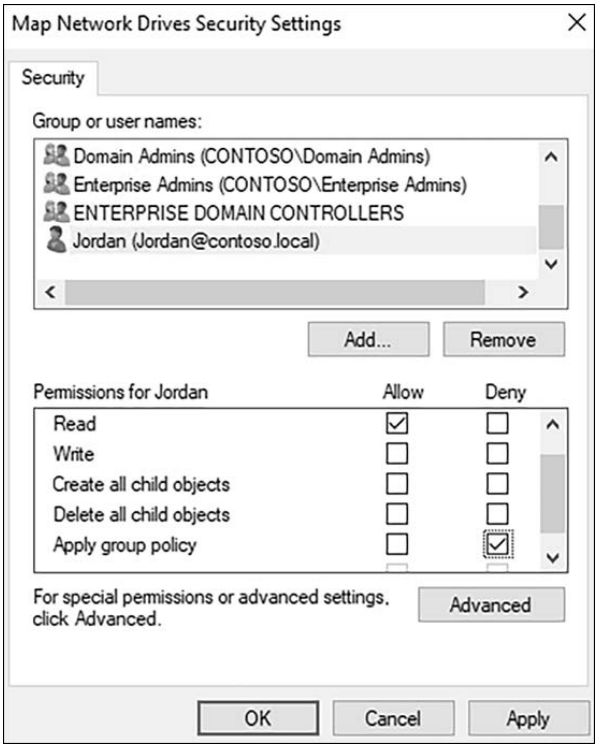
Na rysunku 5.17 widać, że moja grupa *Acct Group* ma uprawnienia *Read* (*Odczyt*) i *Apply group policy* (*Stosowanie zasad grup*) ustawione na *Allow* (*Zezwalaj*). To się stało, kiedy dodałem *Acct Group* do *Security Filtering* (*Filtrowanie zabezpieczeń*). To jest zestaw uprawnień odpowiedzialny za magię, dzięki której, kiedy ktoś loguje się na komputerze w mojej domenie, może on zarówno odczytywać ustawienia tego GPO, jak i je stosować.



Rysunek 5.17. Acct Group ma uprawnienia odczytu i stosowania

Wracając do naszego podstawowego tematu, w świecie Microsoftu odmowa uprawnień zawsze przeważa nad ich udzieleniem. Jeśli chcesz uniemożliwić użytkownikowi, komputerowi lub grupie uzyskanie ustawień wybranego obiektu GPO, to wystarczy dodać daną jednostkę do uprawnień delegowania i zaznaczyć pole wyboru *Deny* (*Odmów*) w pozycji *Apply group policy* (*Stosowanie zasad grup*). Nawet jeśli inny wpis uprawnień zezwala na stosowanie zasad grupy, to ustawienie uniemożliwi zastosowanie ustawień z tego GPO.

Aby wszystko było absolutnie jasne, na rysunku 5.18 przedstawiam jeszcze jeden zrzut ekranu. Widać na nim, że moje konto użytkownika Jordan nie może stosować obiektu *Map Network Drives*.



Rysunek 5.18. Uniemożliwienie użytkownikowi odbierania ustawień z tego obiektu GPO

To znaczy, że kiedy Jordan się zaloguje, NIE otrzyma mapowań dysków z tego GPO.

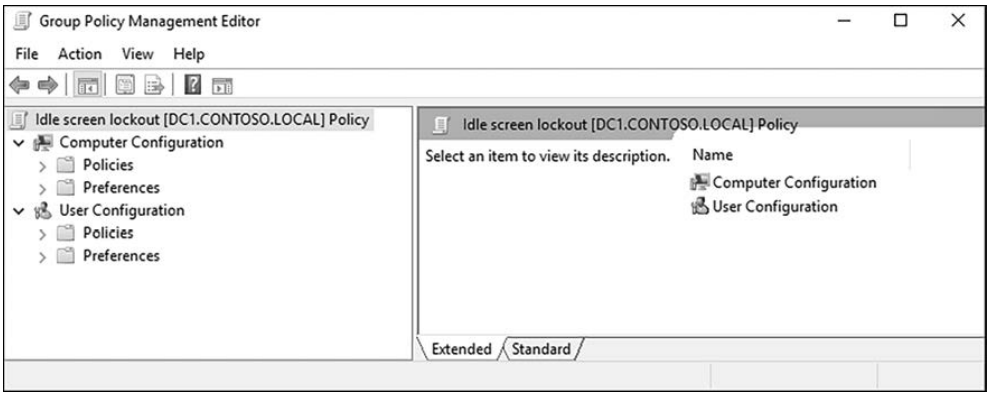
Posługuj się tym ostrożnie! Blokady GPO definiowane na karcie *Delegation* (*Delegowanie*) działają doskonale, ale łatwo zapomnieć o tych ustawieniach lub je przeoczyć w przyszłości. Wielokrotnie pomagałem różnym administratorom w rozwiązywaniu problemów z obiektami GPO, które nie były poprawnie stosowane, i okazywało się, że przyczyną była odmowa uprawnień na karcie *Delegation* (*Delegowanie*).

Konfiguracja komputera i konfiguracja użytkownika

Po paru minutach spędzonych w świecie obiektów GPO na pewno zauważyłeś, że edytor zarządzania zasadami grupy jest podzielony na dwie sekcje. Pierwszym wyborem, jakiego należy dokonać podczas poszukiwania wybranego ustawienia przy definiowaniu obiektu GPO, jest wybór między sekcjami *Computer Configuration* (*Konfiguracja komputera*) i *User Configuration* (*Konfiguracja użytkownika*). Należy wiedzieć i zawsze pamiętać, jaka jest

między nimi różnica, ponieważ nie tylko ułatwia to znalezienie odpowiednich ustawień, ale też pozwala na połączenie nowego obiektu z odpowiednim miejscem i zastosowanie go do odpowiedniego typu obiektów.

Na rysunku 5.19 widać dwie omawiane sekcje edytora.



Rysunek 5.19. Konfiguracja komputera i konfiguracja użytkownika

Konfiguracja komputera

Wszystkie ustawienia GPO znajdujące się w sekcji *Computer Configuration* (*Konfiguracja komputera*) to oczywiście opcje, które można zastosować do komputerów należących do domeny. Ale czy nie wszystkie ustawienia GPO są stosowane do komputerów? Nie, nie są. Wiele ustawień GPO nie ma zastosowania do obiektu komputera w Active Directory i wszystkie te typy ustawień GPO znajdują się właśnie w sekcji *Computer Configuration* (*Konfiguracja komputera*). Niektóre ustawienia GPO można nawet konfigurować zarówno na poziomie komputera, jak i użytkownika. Inne z kolei mogą mieć podobne opcje w obu sekcjach, ale mogą wykonywać zadanie odrobinę inaczej.

Dobrym przykładem jest zasada blokady nieużywanego ekranu. Firmy często żądają, aby ekrany komputerów same się blokowały po określonej liczbie minut braku aktywności. Dzięki temu, jeśli użytkownik odejdzie od komputera i zapomni ręcznie zablokować ekran, ten zablokuje się automatycznie, na przykład po 15 minutach.

Jeśli ktoś zleci Ci utworzenie takiej zasady, to musisz zdecydować, czy Twój obiekt GPO będzie stosowany na poziomie komputera czy na poziomie użytkownika. Ta decyzja zależy wyłącznie od Ciebie i normalnej aktywności Twoich użytkowników.

Jeśli uznasz, że najlepszym rozwiązaniem będzie blokowanie ekranu na poziomie komputera, czyli ekran zostanie zablokowany po 15 minutach bezczynności niezależnie od tego, kto jest zalogowany, to w swoim GPO powinieneś użyć następującej konfiguracji: *Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security Options/Interactive logon: Machine inactivity limit* (*Konfiguracja komputera/Zasady/Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zasady lokalne/Opcje zabezpieczeń/Logowanie interakcyjne: limit nieaktywności komputera*)

Włącz tę zasadę i ustaw jej wartość na 900 sekund, czyli 15 minut.

Konfiguracja użytkownika

Z drugiej strony wiele innych ustawień GPO w ogóle nie ma zastosowania do komputera, tylko do użytkownika domeny, który jest zalogowany na komputerze. Ustawienia sekcji *User Configuration* (*Konfiguracja użytkownika*) są powiązane z kontem użytkownika i mają zastosowanie wszędzie tam, gdzie jest on zalogowany. Przypomnij sobie obiekt GPO *Map Network Drives*, w którym wszystkie konfiguracje dysków sieciowych zostały zdefiniowane właśnie w sekcji *User Configuration* (*Konfiguracja użytkownika*). To znaczy, że mapowania te będą się pojawiały na każdym komputerze, na którym zaloguje się użytkownik. Nie da się utworzyć zmapowanych dysków sieciowych jako ustawienia GPO z sekcji *Computer Configuration* (*Konfiguracja komputera*).

Wracając do przykładu dotyczącego blokady ekranu, powiedzmy, że chcemy, aby blokada ekranu włączała się dla wybranego typu użytkowników albo nawet wszystkich użytkowników oraz aby włączała się dla nich niezależnie od tego, na którym komputerze są zalogowani. W takim przypadku nie znajdziemy specjalnego ustawienia zasady blokady ekranu do skonfigurowania w sekcji *User Configuration* (*Konfiguracja użytkownika*). Zamiast tego generalnie zaleca się kombinowanie z ustawieniami wygaszacza ekranu, które znajdują się w sekcji *User Configuration* (*Konfiguracja użytkownika*). Jeśli skonfigurujesz poniższe ustawienia GPO, to uzyskasz taki sam efekt jak w definicji blokady po wybranym okresie bezczynności w sekcji *Computer Configuration* (*Konfiguracja komputera*), ale będą one stosowane na podstawie kont użytkowników, a nie kont komputerów.

Wybierz kolejno *User Configuration/Policies/Administrative Templates/Control Panel/Personalization* (*Konfiguracja użytkownika/Zasady/Szablony administracyjne/Panel sterowania/Personalizacja*).

Włącz zasadę *Enable screen saver* (*Włącz wygaszacz ekranu*) przez wybranie pozycji *Enabled* (*Włączone*) w jej ustawieniach.

Za pomocą zasady *Force specific screen saver* (*Wymuszaj określony wygaszacz ekranu*) możesz wybrać wygaszacz ekranu, który chcesz uruchamiać.

W zasadzie *Screen saver timeout* (*Limit czasu wygaszacza ekranu*) ustaw 900 sekund.

Dodatkowo włącz zasadę *Password protect the screen saver* (*Wygaszacz ekranu chroniony hasłem*).

Odpowiednie łączenie obiektów GPO

Podczas poszukiwania konfiguracji do obiektów GPO czasami zdarza się tak, że nie mamy wyboru między konfiguracją komputera a konfiguracją użytkownika, ponieważ niektóre opcje znajdują się tylko w jednej z tych grup. Inne ustawienia z kolei można określić zarówno w jednym, jak i w drugim miejscu i wtedy wyboru musimy dokonać na podstawie tego, na jakim poziomie chcemy zastosować obiekt GPO.

Ta decyzja wiąże się bezpośrednio z lokalizacją, z którą planujemy połączyć obiekt GPO. Jeśli nasz obiekt zawiera ustawienia konfiguracji komputera, to mogą one być łączone tylko z obiektami komputerów, a więc taki GPO musielibyśmy połączyć z jednostką organizacyjną zawierającą obiekty komputerowe. Ewentualnie można wykonać połączenie z domeną, która obejmuje wszystkie jednostki organizacyjne.

To samo dotyczy sytuacji przeciwnej, to znaczy jeśli nasz nowy GPO zawiera tylko ustawienia użytkownika, to może odnosić się wyłącznie do obiektów użytkowników i wszelkie połączenia, które dla niego utworzymy, powinny odnosić się do jednostek organizacyjnych zawierających obiekty użytkowników, do których dany GPO się odnosi.

Pewnie już się domyślasz, że ogólnie dobrym zwyczajem jest tworzenie obiektów GPO zawierających ustawienia tylko dla komputerów lub tylko dla użytkowników.

Jeden obiekt GPO może zawierać wiele różnych ustawień i jeśli ma połączenie na wystarczająco wysokim poziomie, to może stosować zarówno ustawienia komputerowe, jak i użytkowników. To jednak utrudnia zarządzanie takim obiektem i dlatego za najlepszą praktykę uważa się tworzenie obiektów GPO zawierających ustawienia tylko z sekcji konfiguracji komputera lub tylko z sekcji konfiguracji użytkownika.

Pętla zwrotna przetwarzania zasad grupy

Obiekty GPO mają specjalną funkcję, która miesza konfiguracje komputera i użytkownika i może być używana w pewnych wyjątkowych przypadkach — kiedy chcemy przesłać ustawienia konfiguracji użytkownika do konkretnych komputerów, ale chcemy, aby te komputery traktowały je tak, jakby to były ustawienia konfiguracji komputera, stosując te same ustawienia zasad do *dowolnego* użytkownika, który jest zalogowany na danym komputerze.

Być może Laura z działu HR ma określony zestaw zasad na swoim komputerze do codziennej pracy, ale od czasu do czasu loguje się na publicznej stacji roboczej w poczekalni. W tej stacji obowiązuje zestaw ograniczeń, ale ponieważ należy ona do domeny, kiedy zaloguje się na niej Laura, zasady grupy potraktują tę czynność jak logowanie na jej własnym komputerze i zastosują takie same ustawienia GPO jak tam. Jeśli utworzymy obiekt GPO konfiguracji użytkownika z włączoną pętlą zwrotną przetwarzania zasad i połączymy go z tą publiczną stacją roboczą, to wszystkie te specjalne ustawienia będą obowiązywały także Laurę, mimo że nie otrzymuje ich ona na swoim własnym komputerze. Gdyby Laura miała zamiar logować się na publicznym komputerze i uzyskiwać na nim dostęp do poufnych dokumentów na swoich standardowych zasadach, to wolelibyśmy raczej jej w tym przeszkodzić.

Jeśli potrzebujesz więcej informacji na temat pętli zwrotnej przetwarzania, to w podsumowaniu na końcu tego rozdziału umieściłem informację na temat świetnego źródła wiedzy.

Zasady i preferencje

Każdy administrator korzystający z Zasad grup powinien znać różnicę między tymi dwoma pojęciami dotyczącymi ustawień obiektów GPO. Istnieją dwa typy ustawień zasad, które znacznie różnią się między sobą sposobem działania. Znamy już różnicę między ustawieniami komputera a ustawieniami użytkownika, więc teraz możemy zwrócić uwagę na podfoldery o nazwach *Policies* (*Zasady*) i *Preferences* (*Preferencje*) w edytorze zarządzania zasadami grupy.

Zasady

Zasady zarządzane, elementy znajdujące się w kategorii *Policies* (*Zasady*) zarówno ustawień użytkownika, jak i komputera, generalnie zachowują się po dżentelmeńsku. Administrator je ustawia i oczekuje efektów. Ich zastosowanie jest wymuszane i użytkownik nie może nic z tym zrobić. Kiedy odwrócimy bieg działań i usuniemy GPO z systemu, zgłaszają problem. Co dokładnie mam na myśli? Kiedy wprowadzamy pewne ustawienia w obiekcie GPO i łączymy go z wybraną lokacją, to oczekujemy, że będą one stosowane na wybranych komputerach lub do wybranych użytkowników. I tak rzeczywiście jest w przypadku wszystkich ustawień GPO, zarówno zasad, jak i preferencji, zarówno zarządzanych, jak i niezarządzanych. A co się dzieje, gdy taki obiekt GPO przestaje odnosić się do użytkownika lub komputera? Co, jeśli usuniemy połączenie GPO lub zmienimy filtry zabezpieczeń tego obiektu tak, że przestanie się odnosić do pewnej stacji roboczej? Czy takie ustawienia nadal obowiązują, czy są aktywnie usuwane?

Odpowiedź na to pytanie zależy od tego, czy pracujesz z zasadami czy z preferencjami. Prawdziwe elementy zasad aktywnie się usuwają z komputera, kiedy obiekt GPO przestaje się do niego odnosić. Dotyczy to większości wbudowanych ustawień konfiguracyjnych w zasadach grupy. W rzeczywistości zasady grupy monitorują cztery specjalne sekcje rejestru systemu Windows i przetwarzają je w każdym cyklu odświeżania zasad grupy. Wszystkie ustawienia GPO, które mają wpływ na te obszary rejestru, mogą usuwać same siebie. Niezarządzane ustawienia zasad, nawet niektóre ze znajdujących się w folderze *Policies* (*Zasady*), mogą nie zdołać się usunąć po odłączeniu obiektu GPO. Wszystko zależy od tego, o jakie ustawienie chodzi oraz jakie działania ono wykonuje na komputerach klientów, aby wprowadzić zmianę.

Istnieją zasady zarządzane i niezarządzane. Jedne i drugie są poza zasięgiem preferencji zasad grupy, którymi zajmiemy się teraz.

Preferencje

Zasady wymuszają wprowadzenie pewnych ustawień bez względu na to, czego chce użytkownik. Natomiast preferencje są dobrym sposobem na konfigurowanie ustawień ułatwiających pracę użytkownika, ale mogą one zostać przez niego zmienione. Niektóre ustawienia GPO są dostępne zarówno w zasadach, jak i preferencjach. To Ty decydujesz, czy chcesz dać użytkownikowi możliwość modyfikacji danego ustawienia, czy wolisz wymusić jego zastosowanie bez względu na wszystko.

Ponadto preferencje są „kleiste". Podczas gdy większość ustawień zasad samodzielnie się usuwa, kiedy obiekt GPO przestaje odnosić się do komputera, z preferencjami jest inaczej. Koniecznie należy o tym pamiętać podczas usuwania obiektów GPO lub ich połączeń. Preferencje zasad grupy nie znajdują się w specjalnych obszarach rejestru, o których była mowa powyżej, w związku z czym system Windows nie skanuje ich aktywnie, aby sprawdzić, czy nadal powinny mieć zastosowanie. Kiedy obiekt GPO dodaje ustawienie preferencji, to późniejsze usunięcie tego obiektu NIE powoduje przywrócenia komputera do oryginalnego stanu, chociaż użytkownik w razie potrzeby może to zrobić samodzielnie. Preferencja taka będzie cały czas aktywna na komputerze nawet po zniknięciu obiektu GPO, który ją wprowadził. Aby przywrócić jej ustawienie domyślne, użytkownik będzie musiał zrobić to ręcznie albo będzie musiał zastosować nowy obiekt GPO.

Domyślne zasady domeny

W tym rozdziale wielokrotnie korzystaliśmy z konsoli GPMC. Wiesz też już, jak wyglądają obiekty GPO, oraz umiesz znajdować ich połączenia, więc możliwe, że zauważyłeś połączony z korzeniem domeny obiekt GPO o nazwie *Default Domain Policy* (*Domyślne zasady domeny*). Znajduje się on w każdym środowisku, chyba że administrator ręcznie go usunie, czego nie radzę robić.

Domyślne zasady domeny odnoszą się do wszystkich użytkowników i komputerów należących do danej domeny. Jako że obiekt ten jest od razu gotowy do użytku i odnosi się do wszystkich, firmy często umieszczają w nim globalne zasady dotyczące haseł lub reguły zabezpieczeń. Zresztą wiele osób, które nie znają zasad grupy i nie radzą sobie z tworzeniem, łączeniem oraz filtrowaniem własnych obiektów GPO, po prostu dodaje kolejne ustawienia do domyślnych zasad domeny.

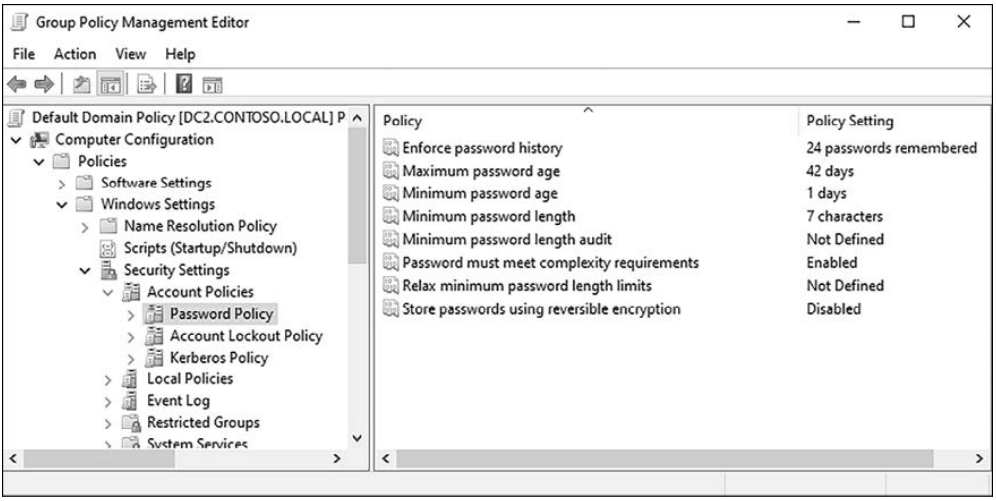
Oczywiście wszystkie one zostaną zastosowane do WSZYSTKICH użytkowników na WSZYSTKICH komputerach, włącznie z serwerami obecnymi w Twojej sieci. Wcześniej czy później taki sposób postępowania się zemści.

Ja trzymam się ogólnej zasady, aby nigdy nie ruszać domyślnych zasad domeny — z jednym wyjątkiem, kiedy chcę utworzyć globalny termin wygaśnięcia haseł i wymagania dotyczące ich poziomu złożoności. Jednak w niektórych przypadkach nawet zasady dotyczące haseł nie powinny być umieszczane w domyślnych zasadach domeny. Czasami chcemy utworzyć bardziej szczegółowe zasady z dodatkowymi ustawieniami, takimi jak możliwość ustalania różnych kryteriów dotyczących haseł dla różnych użytkowników. Szczegółowo ten temat opisuję w rozdziale 9., „Hardening i bezpieczeństwo", więc na razie poprzestaniemy na tym, że chcemy utworzyć jedną zasadę haseł obowiązującą wszystkich. To dobry przykład do przeanalizowania. Poza tym pamiętaj — jeśli kiedykolwiek w domyślnych zasadach domeny ustawisz coś innego niż reguła haseł, to prawdopodobnie robisz to źle. Utwórz własny obiekt GPO.

Kliknięcie prawym przyciskiem myszy dowolnego obiektu GPO wyświetlanego w konsoli zarządzania, a następnie wybranie opcji *Edit...* (*Edytuj...*) spowoduje otwarcie nowego okna z edytorem, który będzie zawierać wszystkie elementy wewnętrzne danej zasady. Tutaj wprowadzasz wszelkie ustawienia lub konfiguracje, które mają być częścią danego obiektu zasad grupy. Przejdź więc do edycji domyślnych zasad domeny, a następnie wybierz opcję *Computer Configuration/Policies/Windows Settings/Security Settings/Account Policies/Password Policy* (*Konfiguracja komputera/Zasady/Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zasady konta/Zasady haseł*) — rysunek 5.20.

W tym miejscu możesz zobaczyć listę różnych dostępnych opcji umożliwiających konfigurowanie zasad haseł w Twojej domenie. Dwukrotne kliknięcie dowolnego z tych ustawień pozwala je zmodyfikować, a zmiana natychmiast zaczyna obowiązywać na wszystkich komputerach przyłączonych w sieci do domeny. Na przykład widzimy, że domyślna wartość parametru *Minimum password length* (*Minimalna długość hasła*) jest ustawiona na 7 znaków. Wiele firm analizowało już zagadnienie związane ze standardową długością haseł w komputerach podłączonych do sieci. Aby pozwolić infrastrukturze katalogowej zaakceptować podjętą decyzję, wystarczy zmodyfikować to pole.

Zmiana minimalnej długości hasła na 14 znaków wymagałaby odpowiednich modyfikacji dla wszystkich kont użytkowników przy następnym resetowaniu haseł.



Rysunek 5.20. Ustawienia hasła w domyślnej zasadzie domeny

Warto to powtórzyć: chociaż domyślne zasady domeny to bardzo szybki i łatwy sposób na skonfigurowanie niektórych ustawień i przekazanie ich wszystkim, należy ostrożnie wprowadzać zmiany w taki sposób. Za każdym razem, gdy wprowadzasz tu zmianę ustawienia, pamiętaj, że wpłynie ona na wszystkie obiekty w Twojej domenie, wliczając w to Ciebie. Wiele razy będziesz jednak tworzyć zasady, które nie muszą mieć zastosowania do wszystkich. W takich przypadkach zdecydowanie zaleca się unikanie domyślnych zasad domeny, a zamiast tego skonfigurowanie zupełnie nowego obiektu zasad grupy do zadania, które zamierzasz zrealizować.

Szablony administracyjne

Edytuj jakiś obiekt GPO, dowolny, aby mieć przed oczami otwarty edytor zarządzania zasadami grupy. Rozwiń folder *Policies* (*Zasady*) w sekcji *Computer Configuration* (*Konfiguracja komputera*), *User Configuration* (*Konfiguracja użytkownika*) lub w obu. W każdym z nich znajdziesz folder o nazwie *Administrative Templates* (*Szablony administracyjne*). Większość z nas traktuje szablony administracyjne tak samo jak wszystkie inne ustawienia GPO, czyli po prostu jako zbiory elementów, za pomocą których można zarządzać użytkownikami lub komputerami. Częściowo to prawda, ale podczas gdy ustawienia oprogramowania i ustawienia systemu Windows są wbudowane w zasady grupy i są zasadniczo takie same dla każdego środowiska domenowego, szablony administracyjne są konfigurowalne.

Szablony administracyjne pokazują elastyczność zasad grupy. Każde ich ustawienie jest pobierane z plików szablonowych znajdujących się na serwerach kontrolera domeny. Są to pliki ADMX. Zawierają one wszystkie informacje potrzebne do wyświetlenia danego ustawienia w edytorze zarządzania zasadami grupy. Mogą to być na przykład opcje zawarte w ustawieniu, listy rozwijane, które mają zostać wyświetlone, oraz treść pól opisu wyświetlana, gdy administrator kliknie dwukrotnie dane ustawienie.

Każdemu plikowi ADMX towarzyszy plik ADML. Jest to plik językowy określający język ustawień zawartych w pliku ADMX.

W systemie Windows XP (i wcześniejszych) pliki tego typu nie istniały. Wówczas ustawienia w szablonach administracyjnych opierały się na plikach ADM. Dziś nikt już nie powinien korzystać z systemu Windows XP, ale wiem, że niektórzy wciąż go mają, ponieważ przynajmniej raz w miesiącu stykam się z nim u swoich klientów. Dlatego postanowiłem dodać tę informację, tak na wszelki wypadek. A na marginesie: pozbądźcie się komputerów z systemem Windows XP.

System Windows 7 i nowsze wersje rozpoznają pliki ADMX/ADML, więc zakładam, że masz aktualne środowisko, w którym nawet maszyn z już nieobsługiwanym systemem Windows 7 jest niewiele.

Implementacja plików ADMX/ADML

Z plikami ADMX możesz zetknąć się w dwóch sytuacjach. Pierwszą z nich są przenosiny na nowszą wersję systemu Windows Server. Każda wersja tego systemu operacyjnego — 2012, 2012R2, 2016, 2019, 2022 — zawiera pewną liczbę nowych i zaktualizowanych ustawień zasad grupy. Podczas instalacji pierwszego kontrolera domeny w środowisku, które jest oparte na nowszej platformie, zostaje wykonany proces o nazwie ADPrep. Polega on na przygotowaniu schematu Active Directory dla nowego systemu operacyjnego oraz wypełnieniu nowych ustawień zasad grupy. Czasami jednak wprowadzenie nowej wersji systemu operacyjnego do środowiska nie odbywa się przez instalację kontrolera domeny. W takim przypadku zasady grupy nie są aktualizowane o nowe ustawienia. A co, jeśli chcielibyśmy, aby i tak były one dostępne? Da się to załatwić przez skopiowanie plików ADMX/ADML w odpowiednie miejsce.

Drugim i najczęstszym powodem ręcznego kopiowania plików ADMX/ADML jest sytuacja, gdy dostawca oprogramowania, na przykład Microsoft, udostępnia niestandardowe pliki ADMX. Można je zainstalować w Active Directory, aby uzyskać w zasadach grupy nowe ustawienia, których normalnie w systemie Windows Server nie ma. Zobaczmy, jak się to robi.

Google Chrome (czy ja użyłem tych słów w książce o technologii Microsoftu?) to jedna z najpopularniejszych przeglądarek. Wielu administratorów ma problem z jej scentralizowanym mechanizmem konfiguracji. Nie wiem, czy wiesz, ale Google ma własny zestaw plików ADMX! Możesz je dodać do zasad grupy, aby korzystać z ustawień zdefiniowanych przez Google bezpośrednio w GPMC i rozsyłać je do komputerów swoich pracowników.

Najpierw musimy pobrać te pliki. Obecnie są one dostępne pod adresem *https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip*.

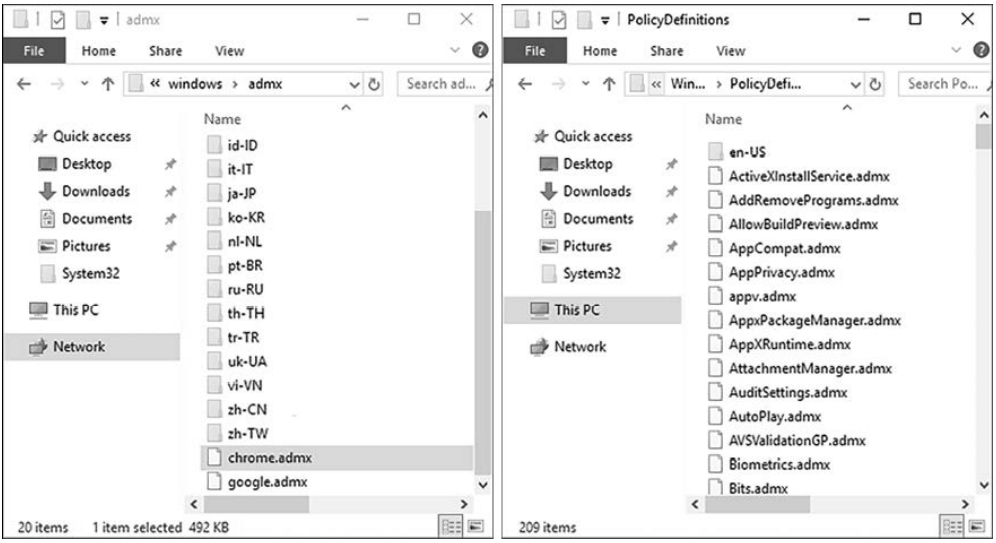
Jeśli powyższy odnośnik nie działa, poszukaj w internecie frazy `"pliki chrome admx"`. Powinieneś bez problemu znaleźć to, czego potrzebujesz.

Skopiuj te pliki do swojego kontrolera domeny i wypakuj je, aby odnaleźć pliki ADMX i ADML. Powinny znajdować się w folderze o nazwie *windows*. Pliki ADMX znajdują się bezpośrednio w nim, a pliki ADML są rozmieszczone w folderach odpowiadających poszczególnym językom. To jest zgodne z tym, co za chwilę znajdziemy w zasadach grupy. Mając przygotowane potrzebne pliki, otwórz na kontrolerze domeny następujący folder:

```
%systemroot%\PolicyDefinitions
```

(Na większości serwerów będzie to folder *C:\Windows\PolicyDefinitions*).

Na rysunku 5.21 widać pobrane przeze mnie pliki Chrome wraz z folderem *PolicyDefinitions*. Jak widać, zgodnie z oczekiwaniami zawiera on wiele plików ADMX. To właśnie dzięki nim mamy jakiekolwiek ustawienia w zasadach grupy, w folderach *Administrative Templates* (*Szablony administracyjne*).



Rysunek 5.21. Kopiowanie nowych plików ADMX do kontrolera domeny

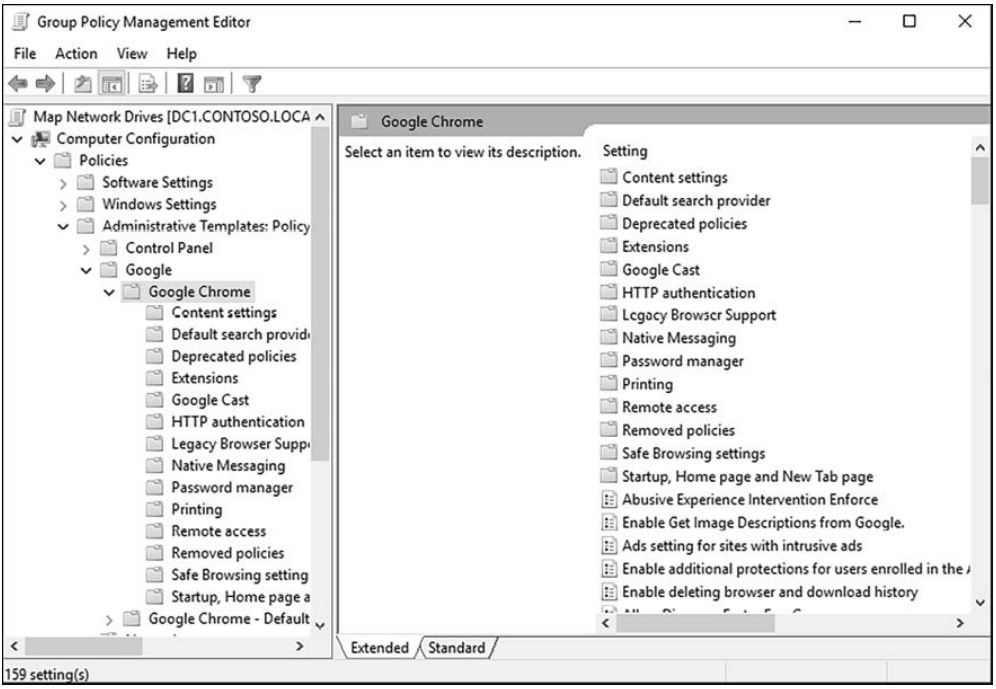
Skopiuj pliki ADMX przeglądarki Chrome do folderu *PolicyDefinitions*, a następnie skopiuj towarzyszący im plik ADML do odpowiedniego folderu w folderze *PolicyDefinitions*. To wszystko! Jeśli teraz zamkniesz i ponownie otworzysz GPMC i przejdziesz do sekcji *Administrative Templates* (*Szablony administracyjne*), to znajdziesz tam nowe ustawienia Google Chrome.

Jak widać na rysunku 5.22, dwa małe pliki ADMX zawierają ich bardzo dużo.

W tym przykładzie pracuję w swoim laboratorium testowym i przyjmuję założenie, że w środowisku znajduje się jeden kontroler domeny. Jeśli masz ich więcej, musisz skopiować pliki do folderu *%systemroot%\PolicyDefinitions* na każdym z nich lub możesz posłużyć się magazynem centralnym, którego opis znajduje się w następnym podrozdziale.

Magazyn centralny

Kiedy otwierasz konsolę zarządzania zasadami grup i tworzysz lub edytujesz obiekt GPO, to ustawienia dostępne w sesji konsoli są pobierane z plików ADMX/ADML znajdujących się na dysku twardym komputera lub serwera, na których została uruchomiona konsola. Gdyby implementacja nowych ustawień za pomocą plików ADMX wymagała ich skopiowania do odpowiedniego folderu na każdym kontrolerze domeny i na wszystkich komputerach klientów, na których są zainstalowane narzędzia RSAT, to mielibyśmy bardzo dużo pracy. Na szczęście da się to zautomatyzować.



Rysunek 5.22. Ustawienia GPO Google Chrome

W Active Directory można włączyć tak zwany *Central Store* (*Magazyn centralny*), który umożliwia replikację plików ADMX/ADML. Kiedy go włączysz, wszystkie komputery zarządzające zasadami grupy, takie jak kontrolery domen, będą z niego pobierać pliki szablonów.

Włączanie magazynu centralnego

Aby włączyć w Active Directory magazyn centralny, należy tylko utworzyć dwa foldery w specjalnym folderze o nazwie *SYSVOL*. GPMC będzie sprawdzać tę lokalizację przy uruchamianiu, aby pobrać z niej pliki ADMX/ADML. Zaloguj się na serwer kontrolera domeny i utwórz następujący folder:

```
%systemroot%\SYSVOL\sysvol\contoso.local\Policies\PolicyDefinitions
```

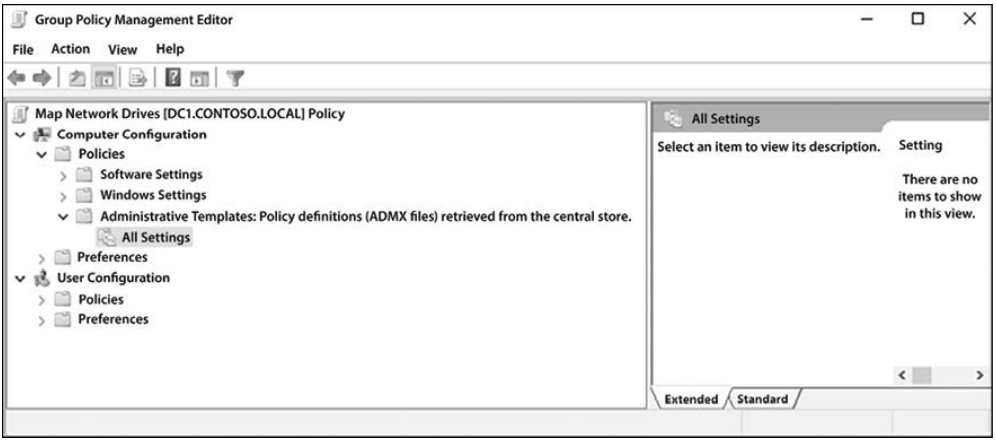
Dodatkowo w swoim nowym folderze *PolicyDefinitions* utwórz folder na językowe pliki ADML. W moim przypadku jest to folder dla języka angielskiego o nazwie *en-US*:

```
%systemroot%\SYSVOL\sysvol\contoso.local\Policies\PolicyDefinitions\en-US
```

Oczywiście *contoso.local* należy zastąpić własną domeną wewnętrzną, i na tym koniec. Kiedy utworzysz te dwa foldery, możesz ich używać do wprowadzania nowych plików ADMX i ADML. Zawarte w nich ustawienia będą dostępne wszędzie tam, gdzie uruchomisz konsolę GPMC.

Zapełnianie magazynu centralnego

Pewnie nie przyszło Ci do głowy, aby zajrzeć do któregoś z obiektów GPO i sprawdzić, jak obecnie, po włączeniu magazynu centralnego, wygląda folder *Administrative Templates* (*Szablony administracyjne*). Zrobimy to teraz. Uruchom GPMC i edytuj dowolny ze swoich obiektów GPO. Otwórz jeden z folderów w sekcji *Administrative Templates* (*Szablony administracyjne*), a okaże się, że jest pusty. Ponadto zauważysz, że pełna nazwa folderu *Administrative Templates* zmieniła się i odzwierciedla fakt, że ustawienia są pobierane z magazynu centralnego: *Administrative Templates: Policy definitions (ADMX files) retrieved from the central store* (*Szablony administracyjne: definicje zasad (pliki ADMX) pobierane z magazynu centralnego*) — rysunek 5.23.



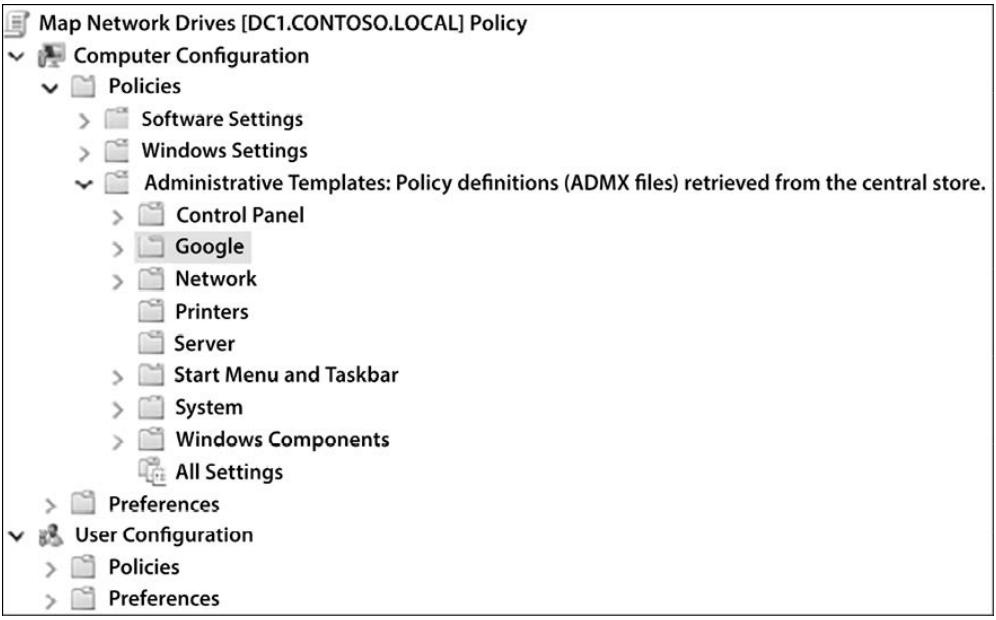
Rysunek 5.23. Folder Administrative Templates jest pusty

Chcemy nasze ustawienia z powrotem! Na szczęście one cały czas znajdują się na dysku twardym naszego kontrolera domeny, w tym samym miejscu, do którego niedawno dodawaliśmy ustawienia Google. Aby przenieść wszystkie swoje ustawienia do magazynu centralnego, wykonaj poniższe operacje kopiowania.

Skopiuj `%systemroot%\PolicyDefinitions` do `%systemroot%\SYSVOL\sysvol\contoso.local\Policies\PolicyDefinitions`.

Skopiuj `%systemroot%\PolicyDefinitions\en-US` do `%systemroot%\SYSVOL\sysvol\contoso.local\Policies\PolicyDefinitions\en-US` (wprowadź odpowiednie poprawki dla swojego języka) (rysunek 5.24).

Jak widać, teraz folder *Administrative Templates* (*Szablony administracyjne*) nadal pobiera ustawienia z magazynu centralnego, ale zawiera też skopiowane przez nas pliki ADMX używane w GPO. Magazyn centralny jest dostępny dla wszystkich kontrolerów domen w środowisku i jest replikowany przez *SYSVOL*.



Rysunek 5.24. Teraz magazyn centralny zawiera wszystkie ustawienia

Podsumowanie

Zasady grupy to niezwykle potężne narzędzie pracy w środowisku domeny. Istnieje wiele gotowych konfiguracji i ustawień, a dzięki możliwości modyfikowania rejestru na komputerach klientów nasze możliwości w zakresie zarządzania tymi komputerami przez GPO są ograniczone niemalże tylko naszą wyobraźnią.

Jak to zwykle bywa w przypadku wielu tematów dotyczących systemu Windows Server, o zasadach grupy można powiedzieć tak dużo, że powstałaby osobna książka. Na szczęście miałem okazję taką napisać. Jeśli chcesz dowiedzieć się więcej o zasadach grupy i poznać wszystkie możliwe sposoby ich użycia w celu zabezpieczenia swojej infrastruktury, przeczytaj moją książkę pt. *Mastering Windows Group Policy* (wyd. Packt).

Pytania

1. Czy ustawienia wygaszacza ekranu należą do konfiguracji komputera, czy użytkownika?
2. Co jest przetwarzane wcześniej, linki poziomu domeny czy linki poziomu jednostki organizacyjnej?
3. Jakie specjalne ustawienie GPO wymusza zastosowanie ustawień użytkownika na danym komputerze?
4. Jaki typ filtrowania obiektu GPO konfiguruje się wewnątrz samego obiektu GPO, na przykład w przypadku zasady zmapowanych dysków sieciowych?

5. Prawda czy fałsz? Użytkownik może zmienić preferencje określone w zasadach grupy.
6. Jaka jest domyślna częstotliwość odświeżania zasad grupy w tle?
7. Jakiego typu filtrowania GPO można użyć, aby przypisać ustawienia tylko do laptopów?
8. Co zrobisz, jeśli znajdziesz na parkingu pendrive z napisem „Finanse CEO”?

Windows Server 2022: nowoczesność, stabilność i bezpieczeństwo!

Windows Server stanowi podstawę całej platformy Azure. Może obsłużyć nawet najpoważniejsze zadania w środowisku chmurowym. Microsoft konsekwentnie doskonali wyjątkowe technologie pozwalające na powiązanie lokalnych centrów danych z Azure czy też na współpracę kontenerów Windows Server, Hyper-V, Dockera i Kubernetes. Ponadto praca z Serverem 2022 jest efektywna i satysfakcjonująca.

Najnowsze wydanie przewodnika, zaktualizowane pod kątem systemu Windows Server 2022, to bogate źródło wiedzy dla administratora serwerów. Przedstawia zasady instalacji i konfiguracji tego systemu, a także sposoby korzystania z centralnych narzędzi do administracji. Książka w głównej mierze jest poświęcona systemowi Windows Server 2022 LTSC, ale zawiera też najnowsze informacje dotyczące edycji SAC. Opisano tu szereg technologii dostępu zdalnego i pokazano, jak zarządzać infrastrukturą klucza publicznego i certyfikatami. Omówiono Server Core, wbudowane funkcje redundancji i metody rozwiązywania problemów. Zaprezentowane zostały również technologie infrastruktury podstawowej, w tym Active Directory, DNS, DHCP i zasady grupy.

W książce między innymi:

- zarządzanie serwerami przez Menedżera serwera, PowerShell i Windows Admin Center
- nowoczesne zabezpieczanie sieci i danych
- implementacja własnej infrastruktury klucza publicznego
- kontenery, Nano Server i integracja centrum danych z Microsoft Azure
- wirtualizacja centrum danych za pomocą Hyper-V

Jordan Krause wielokrotnie otrzymywał tytuł MVP za pracę z serwerami i technologiami sieciowymi Microsoftu. Specjalizuje się w Microsoft DirectAccess i Always On VPN, regularnie publikuje artykuły na temat tych technologii. Kieruje zespołem inżynierów rozproszonych po całym kraju.

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-0834-5
9 788328 908345
Cena: 149,00 zł
packt