Polska

Microsoft Windows

ROZDZIAŁ 22

Zasady grupowe

Zasady grupowe stanowią jedną z ważniejszych technologii Zarządzania adaptacją i konfiguracją, oferowanych w systemie operacyjnym Microsoft Windows 2000. Administratorzy wykorzystują Zasady grupowe do określenia opcji związanych z zarządzanymi konfiguracjami pulpitów dla grup komputerów i użytkowników. Zasady grupowe są elastyczne i zawierają ustawienia dotyczące: zasad opartych na rejestrze, zabezpieczeń, instalacji oprogramowania, skryptów, uruchamiania i zamykania komputera, logowania i wylogowywania użytkowników oraz przeadresowania folderów. Microsoft Windows 2000 Server zawiera setki konfigurowalnych ustawień Zasad grupowych. Zasady grupowe umożliwiają organizacjom obniżenie kosztów obsługi systemów komputerowych, pozwalając administratorom na udoskonalanie i sterowanie pulpitami użytkowników.

W tym rozdziale

Dodatkowe informacje w Resource Kit

- Więcej informacji o Zarządzaniu adaptacją i konfiguracją znajduje się w tej książce w rozdziale „Wprowadzenie do zarządzania pulpitami”.
- Więcej informacji o regulowaniu dostępu znajduje się w tej książce w rozdziale „Kontrola dostępu”.
- Więcej informacji o kopiach zapasowych Zasad grupowych znajduje się w tej książce w rozdziale „Tworzenie i przywracanie kopii zapasowej Active Directory”.
- Informacje o snap-in Instalacja oprogramowania znajdują się w rozdziale „Instalacja i konserwacja oprogramowania”.

Zasady grupowe

Zasady grupowe pozwalają na jednorazowe zdefiniowanie środowisk użytkowników, po czym ustawienia będą automatycznie wymuszane przez system operacyjny.

Obiekty Zasad grupowych nie są profilami. Profil zawiera ustawienia, które użytkownik może zmienić, dotyczą one: pulpitu, ustawień rejestrowych w plikach NTUser.dat, katalogu profili, foldera Moje dokumenty, foldera Ulubione itp. Zasady grupowe zarządzane są przez administratora i stanowią narzędzie administracyjne obsługiwane przez MMC i służące do ustawienia zasad obowiązujących grupy użytkowników i komputerów.

Domyślnie, Zasady grupowe są dziedziczone z poziomu lokacji przez poziom domeny i z poziomu domeny przez poziom jednostki organizacyjnej. Ustawienia Zasad grupowych obowiązujące danego użytkownika lub komputer zależą od kolejności i poziomu zastosowania obiektów Zasad grupowych (połączenia obiektów z zakresami docelowymi). Zasady mogą być zablokowane na poziomie lokacji Active Directory, domeny lub jednostki organizacyjnej, alternatywnie zasady mogą być wymuszane na poziomie pojedynczego obiektu Zasad grupowych. Aby to wykonać, należy połączyć obiekt z zakresem docelowym oraz ustawić na łączu opcję Nie zastępuj (No override).

Domyślnie, Zasady grupowe dotyczą wszystkich użytkowników i komputerów (ale nie pozostałych obiektów) znajdujących się w danej lokacji, domenie lub jednostce organizacyjnej.

Uwaga: Zasady grupowe nie dotyczą grup zabezpieczenia.

Grupy zabezpieczenia są używane do filtrowania Zasad grupowych, czyli do ograniczenia ich zakresu. Aby to wykonać, należy odpowiednio ustawić uprawnienia Zastosowania Zasad grupowych i Odczytu na obiekcie Zasad grupowych dotyczące poszczególnych grup zabezpieczenia. Procedura ta jest omówiona dalej w niniejszym rozdziale.

Uwaga: Dla celów Zasad grupowych, położenie grupy zabezpieczenia w Active Directory jest bez znaczenia.

Porównanie systemów zasad w Windows NT 4.0 i Windows 2000

W Microsoft Windows NT 4.0 wprowadzono Edytor zasad systemowych (Poledit.exe), narzędzie służące do określania konfiguracji użytkowników i komputerów, przechowywanych w rejestrze Windows NT. Zasady ustawione w tym Edytorze dotyczą wszystkich komputerów domeny posiadających Windows NT Workstation 4.0 lub Windows NT Server 4.0. Ustawienia Zasad systemowych są ustawieniami rejestrowymi regulującymi zachowanie różnych komponentów środowiska pulpitu.

W Windows 2000 można utworzyć konfigurację pulpitu dla danej grupy użytkowników lub komputerów za pomocą snap-in Zasady grupowe. W przypadku klientów Windows 2000, Zasady grupowe prawie całkowicie zastępują Edytor zasad systemowych. Snap-in umożliwia zarządzanie konfiguracjami pulpitów dla dużych grup komputerów i użytkowników, które mogą być zagnieżdżone lub zawierać część wspólną. Nielokalne obiekty Zasad grupowych mogą być połączone z dowolną liczbą zakresów docelowych, którymi mogą być lokacje, domeny lub jednostki organizacyjne w Active Directory.

Zasady systemowe w Windows NT 4.0, Windows 95 i Windows 98

Ustawienia określone w edytorze zasad systemowych (Poledit.exe):

- Dotyczą domen.
- Mogą ulec dalszemu przystosowaniu bazującemu na przynależności do grup zabezpieczenia.
- Nie są zabezpieczone (mogą być modyfikowane przez użytkowników posługujących się edytorem rejestru Regedit.exe).
- Pozostają w profilach użytkowników, czasem nadmiernie długo. Ustawienie Zasad systemowych Windows NT 4.0 zostaje usunięte dopiero po jego modyfikacji w Edytorze zasad systemowych lub po modyfikacji rejestru przez użytkownika.
- Są ograniczone do administracyjnie wymuszanych typów zachowania pulpitu opartych na ustawieniach rejestrowych.

Uwaga: Ustawienia rejestrowe w Windows NT 4.0 czasem powodują problemy w przypadku zmian przynależności użytkownika do grup zabezpieczenia. Ustawienia mogą wówczas wymagać ręcznej

modyfikacji lub usunięcia.

Snap-in Zasady grupowe oferuje wbudowane funkcje związane z ustawieniami rejestrowymi, ustawieniami zabezpieczeń, instalacją oprogramowania, skryptami i przeadresowaniem folderów. Utworzone ustawienia Zasad grupowych zawarte są w obiekcie Zasad grupowych. Każdy komputer Windows 2000 posiada jeden lokalny obiekt Zasad grupowych, a może podlegać także dowolnej liczbie nielokalnych (opartych na Active Directory) obiektów Zasad grupowych.

Ustawienia Zasad grupowych są w Windows 2000 główną metodą scentralizowanego zarządzania adaptacją i konfiguracją.

Ustawienia Zasad grupowych:

- Mogą być powiązane z lokacjami, domenami i jednostkami organizacyjnymi.
- Dotyczą wszystkich użytkowników i komputerów należących do danej lokacji, domeny lub jednostki organizacyjnej.
- Mogą ulec dalszemu przystosowywaniu opierającemu się na przynależności użytkowników lub komputerów do grup zabezpieczenia.
- Są zabezpieczone (mogą zostać zmienione tylko przez administratora).
- Zostają usunięte i zastąpione przy każdej zmianie zasad.
- Mogą służyć do precyzyjnego sterowania pulpitami i do udoskonalenia komputerowego środowiska użytkownika.

Uwaga: W przeciwieństwie do rejestrowych ustawień Zasad systemowych w Windows NT 4.0, ustawienia Zasad grupowych w Windows 2000 zostają usunięte z rejestru w momencie, gdy dany obiekt Zasad grupowych przestaje obowiązywać. Ustawienia zapisywane są w następujących zabezpieczonych miejscach w rejestrze: \Software\Policies oraz \Software\Microsoft\Windows\CurrentVersion\Policies.

Struktura Active Directory i Zasady grupowe

Wprowadzenie Zasad grupowych jest jedną z kwestii, które należy rozważyć podczas planowania struktury Active Directory dla danej organizacji. Podstawowymi jednostkami Zasad grupowych są obiekty Zasad grupowych. Z zakresem docelowym można połączyć cały obiekt Zasad grupowych, ale nie jego podzbiór. Także przy filtrowaniu zakresu Zasad grupowych za pomocą grup zabezpieczenia można włączyć lub wyłączyć tylko cały obiekt Zasad grupowych, nie jego części. Zakres zastosowania rozszerzeń Zasad grupowych – Instalacja oprogramowania i Przeadresowanie folderów – można regulować w oparciu o przynależność do grup zabezpieczenia, wykorzystując uprawnienia.

Istnieją dwa rodzaje obiektów Zasad grupowych: lokalne i nielokalne.

Uwaga: Każdy komputer Windows 2000 posiada tylko jeden lokalny obiekt Zasad grupowych.

W tej części rozdziału zakłada się, że wszystkie obiekty Zasad grupowych są nielokalne, chyba że określono inaczej.

Obiekty Zasad grupowych przechowywane są w domenie Windows 2000 i obowiązują w lokacjach, domenach lub jednostkach organizacyjnych, z którymi obiekty są połączone.

- Obiekt Zasad grupowych połączony z lokacją (przy użyciu konsoli Lokacje i usługi Active Directory [Active Directory Sites and Services]) obowiązuje we wszystkich domenach w tej lokacji.
- Obiekt Zasad grupowych połączony z domeną obowiązuje wszystkich użytkowników i komputery należące do domeny oraz, w wyniku dziedziczenia, wszystkich użytkowników i komputery należące do jednostek (i ogólnych kontenerów Active Directory) znajdujących się pod domeną w drzewie przestrzeni nazw Użytkownicy i komputery Active Directory (Active Directory Users and Computers).
- Obiekt Zasad grupowych połączony z jednostką organizacyjną obowiązuje wszystkich użytkowników i komputery należące do danej jednostki oraz do jednostek (i ogólnych kontenerów Active Directory) znajdujących się pod nią w drzewie przestrzeni nazw

Użytkownicy i komputery Active Directory (Active Directory Users and Computers).

Obiekt Zasad grupowych nie może być połączony z ogólnym kontenerem Active Directory (w konsoli Użytkownicy i komputery Active Directory ikona kontenera ogólnego przypomina standardową ikonę foldera, podczas gdy ikona jednostki organizacyjnej zawiera także małą książkę). Użytkownicy i komputery należące do ogólnych kontenerów Active Directory dziedziczą ustawienia z obiektów Zasad grupowych zastosowanych na wyższych poziomach drzewa Active Directory.

W pierwszej kolejności zostaje zastosowany lokalny obiekt Zasad grupowych. Następnie zostają zastosowane obiekty Zasad grupowych połączone z lokacjami (w kolejności określonej przez administratora), następnie obiekty połączone z domenami, a na końcu obiekty połączone z jednostkami administracyjnymi (rozpoczynając od jednostki najwyżej usytuowanej w hierarchii Active Directory). Obiekty połączone z daną jednostką organizacyjną zostają zastosowane w kolejności określonej przez administratora.

Powyżej omówiona kolejność zastosowania obiektów Zasad grupowych (1. Lokalny, 2. Lokacja, 3. Domena, 4. Jednostka organizacyjna) ma znaczenie przy projektowaniu Active Directory. Domyślnie, zasady zastosowane później zastępują zasady zastosowane wcześniej, o ile ustawienia są Włączone (Enabled) lub Wyłączone (Disabled). Ustawienia Nie skonfigurowane (Not Configured) nie mają wpływu na wcześniej zastosowane ustawienia.

Istnieją także mechanizmy pozwalające zmienić domyślne zachowanie omówione powyżej. Najpotężniejsze są ustawienia Nie zastępuj (No Override) i Wymuszaj dziedziczenie zasad (Enforce Policy Inheritance). Zalecane jest ograniczenie stosowania tych ustawień.

Zarządzanie Zasadami grupowymi

Przy zarządzaniu Zasadami grupowymi ważne jest zrozumienie następujących kwestii:

Infrastruktura i mechanizmy Zasad grupowych

Sposób funkcjonowania Zasad grupowych, w tym łączenie obiektów Zasad grupowych i filtrowanie zakresu Zasad grupowych za pomocą grup zabezpieczenia.

Wymagania administracyjne

Uprawnienia, które musi posiadać administrator używający Zasad grupowych w środowisku Active Directory.

Model rozszerzeń snap-in MMC

Wyjaśnia zawartość ekranu konsoli MMC wyświetlanego podczas użytkowania snap-in Zasady grupowe i jego rozszerzeń.

Infrastruktura i mechanizmy Zasad grupowych

W tej części omówione są obiekty Zasad grupowych, łącza służące do ich zastosowania, snap-in używany do ich edycji i grupy zabezpieczenia używane do określenia ich zakresu.

Obiekty i snap-in Zasad grupowych

Obiekty Zasad grupowych można traktować jako dokumenty powiązane ze snap-in Zasad grupowych, podobnie jak pliki .doc są powiązane z Microsoft Word lub pliki .txt z Notatnikiem. Analogia ta nie jest jednak dokładna. Zmiany dokonane w obiekcie Zasad grupowych nie są odkładane do momentu wykonania polecenia zapisu, lecz są już realizowane podczas edycji.

Uwaga: Obiekty Zasad grupowych nie mogą być otwierane w trybie tylko do odczytu.

Łącza z lokacjami, domenami i jednostkami organizacyjnymi

Obiekty Zasad grupowych mogą być połączone z określonymi lokacjami, domenami i jednostkami organizacyjnymi, co maksymalizuje i rozszerza możliwości Active Directory.

Dane zawarte w obiektach Zasad grupowych są oceniane przez klientów, którzy w przypadku konfliktu ustalają kolejność pierwszeństwa ustawień Zasad grupowych na podstawie hierarchicznej struktury Active Directory.

Dostęp do snap-in Zasad grupowych

Nielokalny obiekt Zasad grupowych można utworzyć przy użyciu snap-in Zasad grupowych, jako rozszerzenia snap-in Active Directory lub jako autonomicznej konsoli MMC.

Dostęp do snap-in jest najczęściej uzyskiwany poprzez konsolę Użytkownicy i komputery Active Directory (Active Directory Users and Computers). W ten sposób obiekty Zasad grupowych mogą być łączone z domenami lub jednostkami organizacyjnymi. Aby połączyć te obiekty z lokacjami, należy uzyskać dostęp do Zasad grupowych poprzez Lokacje i usługi Active Directory (Active Directory Sites and Services). W obu konsolach Active Directory Zasady grupowe są dostępne z menu kontekstowego. Należy kliknąć prawym przyciskiem myszy odpowiednią lokację, domenę lub jednostkę organizacyjną, wybrać Właściwości (Properties) i kliknąć zakładkę Zasady grupowe (Group Policy). Przykłady procesu tworzenia obiektów Zasad grupowych znajdują się w Pomocy Windows 2000.

Filtrowanie na podstawie przynależności do grup zabezpieczenia

Zakres Zasad grupowych można filtrować na podstawie przynależności komputerów i użytkowników do grup zabezpieczenia, ustawiając uprawnienia DACL (dyskrecjonalne listy kontroli dostępu). Metoda ta umożliwia szybsze przetwarzanie obiektów Zasad grupowych oraz ograniczenie praw do tworzenia i modyfikacji obiektów Zasad grupowych lub ich łączy z Active Directory.

Szczegółowe informacje znajdują się dalej w tym rozdziale pod hasłem „Filtrowanie i delegowanie Zasad grupowych za pomocą grup zabezpieczenia”.

Wymagania administracyjne

Aby ustawić Zasady grupowe w stosunku do danej lokacji, domeny lub jednostki organizacyjnej Active Directory, należy mieć dostęp do kontrolera domeny Windows 2000 dla danego katalogu Active Directory oraz posiadać uprawnienia odczytu i zapisu w stosunku do woluminu systemowego kontrolerów domeny (foldera Sysvol) i prawa modyfikacji w stosunku do danej lokacji, domeny lub jednostki organizacyjnej. Folder woluminu systemowego zostaje utworzony przy instalacji kontrolera domeny Windows 2000 lub po wyznaczeniu serwera Windows 2000 jako kontrolera domeny.

Aby zastosować filtrowanie zakresu Zasad grupowych na podstawie grup zabezpieczenia Windows 2000, należy ustawić uprawnienia na zakładce Zabezpieczenia (Security) na stronach właściwości obiektu Zasad grupowych. Uprawnienia służą także do delegowania praw korzystania ze snap-in Zasady grupowe.

Model rozszerzeń snap-in MMC

Główne węzły snap-in Zasady grupowe są rozszerzeniami snap-in MMC. Do tych rozszerzeń należą: Szablony administracyjne, Skrypty, Ustawienia zabezpieczeń, Instalacja oprogramowania, Usługi instalacji zdalnej, Konserwacja Internet Explorer i Przeadresowanie folderów.

Domyślnie, po uruchomieniu snap-in Zasady grupowe załadowane zostają wszystkie dostępne rozszerzenia. Domyślne zachowanie można zmienić, wykorzystując oferowane przez MMC możliwości tworzenia niestandardowych konsol, a także sterując zachowaniem MMC za pomocą ustawień Zasad grupowych (pod Konfiguracja użytkownika\Szablony administracyjne\Komponenty Windows\Microsoft Management Console\).

Projektanci mogą utworzyć rozszerzenia snap-in Zasady grupowe w celu udostępnienia dodatkowych ustawień. Niektóre rozszerzenia snap-in, na przykład rozszerzenie Ustawienia zabezpieczeń, posiadają kilka dalszych rozszerzeń.

Więcej informacji znajduje się dalej w tym rozdziale pod hasłami „Delegowanie praw

modyfikacji Zasad grupowych" i „Rozszerzenia snap-in Zasady grupowe" oraz pod odsyłaczem do Microsoft Platform SDK na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.

Konfigurowanie Zasad grupowych

Do właściwego korzystania z Zasad grupowych potrzebne jest zrozumienie cech interfejsu użytkownika Zasad grupowych oraz ról, odgrywanych przez nie podczas konfigurowania Zasad grupowych.

Przestrzeń nazw snap-in Zasady grupowe

Węzeł główny snap-in Zasady grupowe jest wyświetlany pod nazwą określającą obiekt Zasad grupowych i jego domenę, w następującym formacie:

<nazwa obiektu Zasad grupowych> [<nazwa serwera>] Zasady

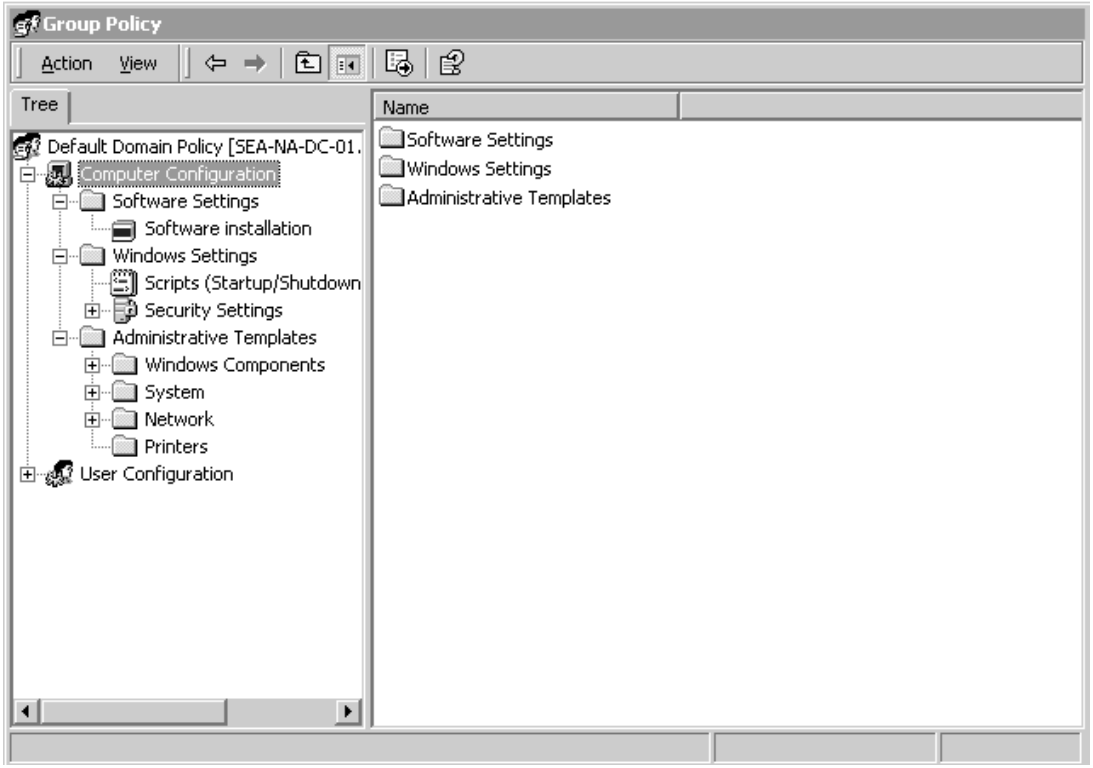
Na przykład:

Domyślne zasady domeny [MSMSRV01.Reskit.com] Zasady

Następny poziom przestrzeni nazw zawiera dwa węzły: Konfiguracja komputera (Computer Configuration) oraz Konfiguracja użytkownika (User Configuration). Są to główne foldery służące do skonfigurowania określonych środowisk pulpitowych i wymuszania Zasad grupowych dla grup komputerów i użytkowników w sieci.

Konfiguracja komputera

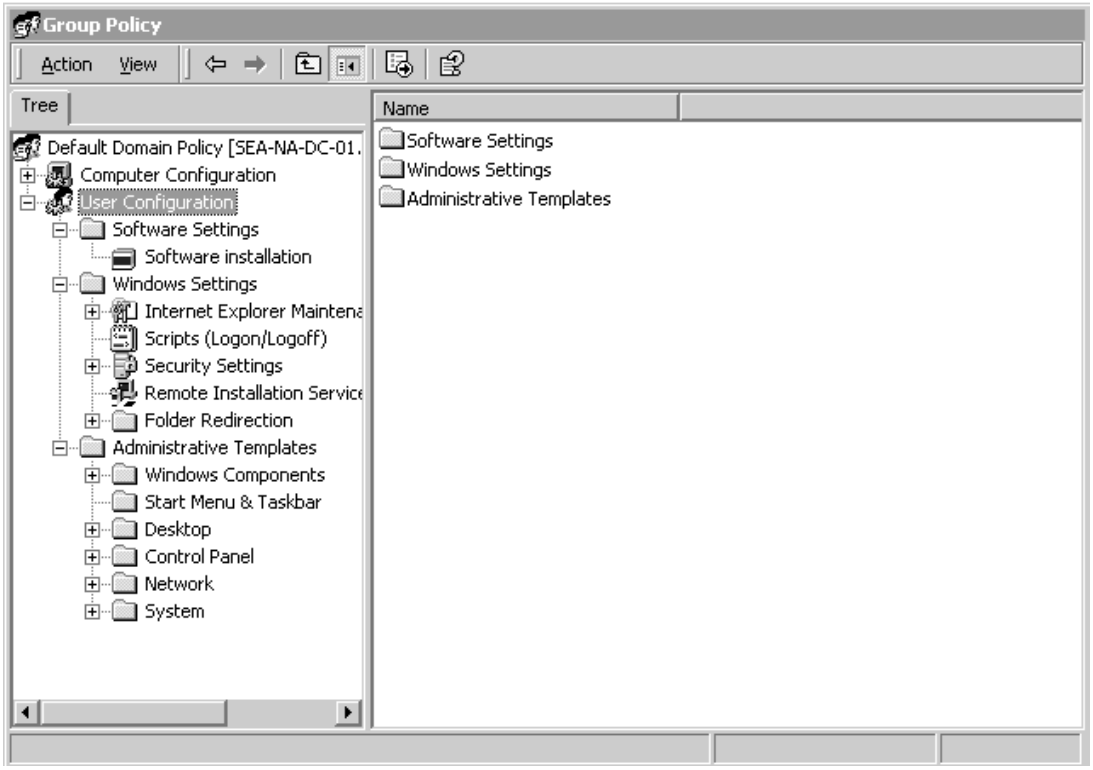
Pod węzłem Konfiguracja komputera znajdują się wszystkie ustawienia związane z komputerem, dotyczące: zachowania systemu operacyjnego, zachowania pulpitu, ustawień zabezpieczeń, skryptów uruchamiania i zamykania komputera, opcji przypisanych aplikacji i ustawień aplikacji. Zasady grupowe dotyczące komputera zostają zastosowane przy inicjacji systemu operacyjnego oraz okresowo według omówionego dalej w tym rozdziale cyklu odświeżania. Generalnie, w przypadku konfliktów, zasady związane z komputerem mają pierwszeństwo przed zasadami skonfigurowanymi dla użytkownika.



Rysunek 22.1 Konfiguracja komputera w konsoli snap-in Zasady grupowe

Konfiguracja użytkownika

Pod węzłem Konfiguracja użytkownika znajdują się wszystkie ustawienia związane z użytkownikiem, dotyczące: zachowania systemu operacyjnego, ustawień pulpitu, ustawień zabezpieczeń, opcji przypisanych i opublikowanych aplikacji, przeadresowania folderów oraz skryptów logowania i wylogowywania. Zasady grupowe dotyczące użytkowników zostają zastosowane w momencie zalogowania oraz okresowo zgodnie z cyklem odświeżania.



Rysunek 22.2 Konfiguracja użytkownika w konsoli snap-in Zasady grupowe

W niektórych ściśle zarządzanych środowiskach komputerowych (takich jak szkoły, biblioteki, pracownie, recepcja) zalecane jest wymuszanie określonej konfiguracji pulpitu niezależnie od logującego się użytkownika. Aby to wykonać, należy uzupełnić lub nawet zastąpić ustawienia Konfiguracji użytkownika konta użytkownika ustawieniami Konfiguracji użytkownika konta komputera. Proces ten nazywa się sprzężeniem zwrotnym i jest omówiony dalej w tym rozdziale pod hasłem „Wsparcie Sprzężenia zwrotnego w Zasadach grupowych”.

Pod węzłami Konfiguracja użytkownika i Konfiguracja komputera usytuowanych jest kilka węzłów podrzędnych, między innymi:

- Ustawienia oprogramowania (Software Settings), gdzie niezależni producenci oprogramowania mogą dodać dalsze rozszerzenia. Jeśli żadnych rozszerzeń nie dodano, to pod tym węzłem znajdzie się tylko rozszerzenie Instalacja oprogramowania dołączone do Windows 2000.
- Ustawienia Windows (Windows Settings), węzeł zawierający rozszerzenia dostarczone przez Microsoft.
- Szablony administracyjne, węzeł zawierający przestrzeń nazw dla ustawień zasad opartych na rejestrze. Aby rozszerzyć przestrzeń nazw Szablonów administracyjnych, należy kliknąć prawym przyciskiem myszy jeden z dwóch węzłów Szablony administracyjne i wybrać Dodaj/usuń szablony (Add/Remove Templates). Szablony są zawarte w plikach o rozszerzeniu .adm.

Rozszerzenia snap-in Zasady grupowe

Rozszerzenie snap-in Zasady grupowe może rozszerzyć przestrzeń nazw Zasad grupowych pod węzłem Konfiguracja użytkownika, pod węzłem Konfiguracja komputera lub pod jednym i drugim jednocześnie. Większość rozszerzeń rozszerza oba węzły, ale oferowane opcje

często się różnią. Rozszerzenia snap-in Zasady grupowe dołączone do Windows 2000 są omówione poniżej.

Szablony administracyjne (Administrative Templates)

Szablony administracyjne zawierają zasady grupowe oparte na rejestrze, służące do wymuszania ustawień rejestrowych dotyczących zachowania i wyglądu pulpitu, w tym komponentów systemu operacyjnego i aplikacji. Istnieje ponad 450 ustawień, więcej ustawień można dodać za pomocą plików .adm. Aby uniknąć utworzenia zbyt trwałych ustawień rejestrowych (patrz pierwsza część niniejszego rozdziału), należy umieścić ewentualne dodatkowe ustawienia rejestrowe pod \Software\Policies lub \Software\Microsoft\Windows\CurrentVersion\Policies.

Ustawienia zabezpieczeń (Security Settings)

Rozszerzenie to służy do ustawienia zabezpieczeń związanych z komputerami i użytkownikami należącymi do zakresu danego obiektu Zasad grupowych. Zdefiniować można ustawienia zabezpieczeń dotyczące komputera lokalnego, domeny i sieci.

Instalacja oprogramowania (Software Installation)

Snap-in Instalacja oprogramowania służy do centralnego zarządzania oprogramowaniem w organizacji. Programy można przypisać użytkownikom lub komputerom oraz opublikować dla użytkowników (ale nie dla komputerów). Komputer docelowy musi posiadać Windows 2000 oraz klienckie rozszerzenie Instalacji oprogramowania, Appmgmts.dll. Aby zainstalować Windows 2000 na komputerze zdalnym, należy skorzystać z Usług instalacji zdalnej (RIS).

Skrypty (Scripts)

Skrypty mogą być wykorzystane do automatyzacji sesji uruchamiania i zamykania komputerów oraz logowania i wylogowywania użytkowników. Użyć można dowolnego języka wspieranego przez WSH (Windows Script Host), na przykład Microsoft Visual Basic Scripting Edition (VBScript), JavaScript, Perl oraz plików wsadowych w stylu MS-DOS (.bat i .cmd).

Usługi instalacji zdalnej (Remote Installation Services)

Ustawienia Usług instalacji zdalnej (RIS) sterują zachowaniem funkcji zdalnej instalacji systemu operacyjnego z perspektywy komputerów klienckich. Zasady grupowe wymagają klienta Windows 2000, nie wystarczy klient Active Directory oparty na wcześniejszej wersji Windows.

Konserwacja Internet Explorer (Internet Explorer Maintenance)

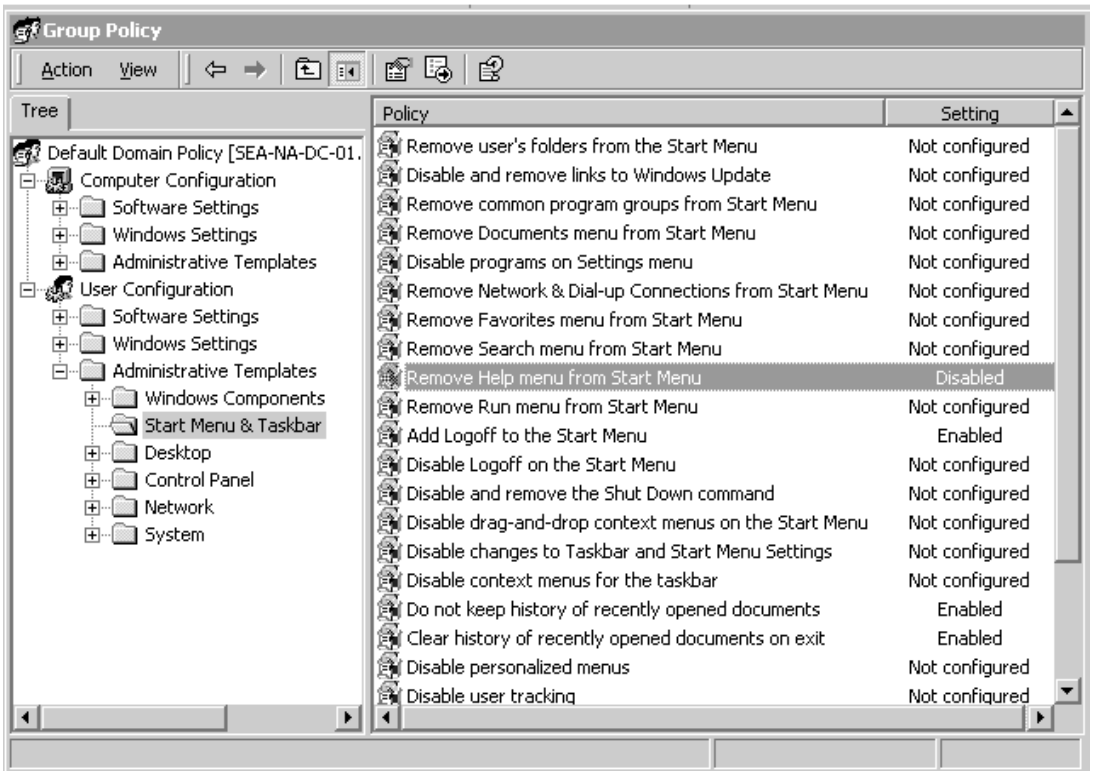
Konserwacja Internet Explorer służy do administracji i dostosowania Microsoft Internet Explorer na komputerach Windows 2000.

Przeadresowanie folderów

Przeadresowanie folderów umożliwia skierowanie specjalnych folderów Windows 2000 (Moje dokumenty, Dane aplikacji, Pulpit, Menu Start) z domyślnej lokacji w profilu użytkownika do alternatywnego adresu w sieci, gdzie mogą podlegać centralnemu zarządzaniu.

Szablony administracyjne

W Windows 2000, węzeł Szablony administracyjne (Administrative Templates) snap-in Zasady grupowe zawiera plik .adm określający ustawienia rejestrowe, które mogą być modyfikowane poprzez obiekt Zasad grupowych interfejsu użytkownika. Niektóre ustawienia Szablonu administracyjnego są przedstawione na rysunku 22.3. W panelu Zasady (Policy) pokazana jest część ustawień należących do Konfiguracji użytkownika w Domyślnych zasadach domeny w obiekcie Zasad grupowych.



Rysunek 22.3 Ustawienia Szablonu administracyjnego w Zasadach grupowych

> **Uwaga:** W Windows NT 4.0, Edytor zasad systemowych wykorzystuje pliki nazywane szablonami administracyjnymi (pliki .adm) do określenia które ustawienia rejestrowe wolno modyfikować – przestrzeń nazw zawierająca te ustawienia jest prezentowana w Edytorze. W Windows 2000 pliki .adm zawierają nowe cechy, takie jak tekst wyjaśniający. Informacje o ustawieniach szablonów administracyjnych dołączonych do Windows 2000 Server znajdują się w pliku informacyjnym GP.chm na CD-ROM Windows 2000 Resource Kit.

Szablony administracyjne sterują na różne sposoby zachowaniem systemu operacyjnego Windows 2000 oraz jego komponentów i aplikacji. Ustawienia zostają zapisane w rejestrze pod odpowiednim kluczem HKEY_CURRENT_USER lub HKEY_LOCAL_MACHINE.

Plik .adm jest plikiem tekstowym Unicode określającym hierarchię kategorii i podkategorii, które definiują sposób wyświetlania opcji w interfejsie użytkownika snap-in Zasady grupowe. Ponadto plik wskazuje miejsca w rejestrze, w których ewentualne zmiany powinny zostać dokonane, określa opcje lub ograniczenia wartości związane z danym ustawieniem, a w niektórych przypadkach określa wartości domyślne. Domyślnie, konsola Zasady grupowe zawiera trzy pliki .adm: System.adm, Inetres.adm i Conf.adm, które razem zawierają ponad 450 ustawień dla klientów Windows 2000. Plik Inetres.adm zawiera ustawienia dotyczące Internet Explorer, a plik Conf.adm (który domyślnie nie zostaje załadowany) zawiera ustawienia Microsoft NetMeeting.

> **Uwaga:** Aby wyświetlić informacje o danym ustawieniu Zasad grupowych, należy wybrać zakładkę Wyjaśnij (Explain) na stronach właściwości ustawienia.

Węzły Szablony administracyjne w snap-in Zasady grupowe można rozszerzyć, tworząc niestandardowe pliki .adm. Informacje o tworzeniu plików .adm znajdują się w Pomocy Windows 2000.

Nadmiernie trwałe ustawienia rejestrowe

W Windows NT 4.0, ustawienia rejestrowe muszą być wycofywane ręcznie. Natomiast w Windows 2000 ustawienia są usuwane i zastępowane nowymi po każdej zmianie obowiązujących zasad. Fakt ten należy wziąć pod uwagę w przypadku, gdy planowane jest zastosowanie ustawień rejestrowych typu Windows NT 4.0 na komputerach opartych na Windows 2000.

Więcej informacji znajduje się dalej w tym rozdziale pod hasłem „Użytkowanie szablonów administracyjnych Windows NT 4.0 w konsoli Zasad grupowych Windows 2000”.

Inne rozszerzenia Zasad grupowych wykorzystujące rejestr

Rejestr wykorzystywany jest przez Usługi instalacji zdalnej (RIS) i Przydziały dyskowe. RIS posiada węzeł w konsoli Zasad grupowych, ale nie posiada rozszerzenia (pliku .dll) po stronie klienta (typowy klient nie posiada systemu operacyjnego). Komponent Przydziały dyskowe posiada rozszerzenie po stronie klienta (Dskquota.dll), ale nie posiada węzła w konsoli Zasad grupowych.

Usługi instalacji zdalnej

Usługi instalacji zdalnej (RIS) są opcjonalnym komponentem systemu operacyjnego Windows 2000 Server. Rozszerzenie RIS w Zasadach grupowych określa, które opcje (instalacja automatyczna, instalacja niestandardowa, instalacja z restartem itp.) będą dostępne na ekranie w kreatorze instalacji klienta.

Gdy klient wspierający technologię rozruchu zdalnego PXE uzyskuje dostęp do serwera instalacji zdalnej w celu instalacji systemu operacyjnego, to serwer RIS sprawdza Zasady grupowe dotyczące opcji zdalnej instalacji zdefiniowanych dla użytkownika. Zadanie to zostaje wykonane przez usługę Warstwa negocjacji informacji o rozruchu (BINL). Usługa ta imituje użytkownika logującego się w przedrozruchowym klienckim interfejsie użytkownika RIS i analizuje obowiązujące obiekty Zasad grupowych. Na podstawie tej analizy usługa określa, które ekrany zostaną przesłane do procesu przedrozruchowego na kliencie RIS, do wyświetlenia użytkownikowi.

Zasady RIS są przechowywane w folderze Sysvol pod ścieżką: Policies\{<GUID GPO>} \User\Microsoft\RemoteInstall\oscfilter.ini. Szczegółowe informacje o RIS znajdują się w rozdziale „Zdalna instalacja systemu operacyjnego”.

Ustawienia zabezpieczeń

W ramach obiektu Zasad grupowych można zdefiniować konfigurację zabezpieczeń zawierającą ustawienia zastosowane do jednego lub więcej zakresów zabezpieczenia wspierane w Windows 2000 Professional lub Windows 2000 Server. Określona konfiguracja zabezpieczeń zostaje zastosowana do komputerów w ramach wymuszania Zasad grupowych.

Rozszerzenie snap-in Zasady grupowe – Ustawienia zabezpieczeń – uzupełnia istniejące systemowe narzędzia zabezpieczające, takie jak zakładka Zabezpieczenia (Security) na stronie właściwości obiektu (lub pliku, foldera itp.) oraz Użytkownicy lokalni i grupy (Local Users and Groups) w Zarządzaniu komputerami. W razie potrzeby można skorzystać z istniejących narzędzi do modyfikacji określonych ustawień.

Do zakresów zabezpieczenia, które mogą być objęte konfiguracją komputera, należą:

Zasady kont

Są to ustawienia dotyczące haseł, blokowania i Kerberos w domenach Windows 2000.

> **Uwaga:** Ustawienia te są skonfigurowane tylko na poziomie domeny. Jeśli zostaną utworzone na poziomie jednostki organizacyjnej, to będą ignorowane.

Zasady lokalne

Obejmują ustawienia dotyczące inspekcji (udanych lub nieudanych prób zalogowania), praw użytkowników (kto ma dostęp do komputera z sieci) i opcji zabezpieczeń (czy wolno połączyć się z komputerem anonimowo).

Dziennik zdarzeń

W tej części znajdują się ustawienia dotyczące dzienników zdarzeń,(dostawiłam przecinek) aplikacji, zabezpieczeń i systemu (na przykład, dotyczące wielkości dzienników i metody utrzymywania informacji). Dzienniki są dostępne w Podglądzie zdarzeń (Event Viewer).

Grupy ograniczone

Określić można, którzy użytkownicy i które grupy muszą należeć do ograniczonych grup zabezpieczenia, takich jak Administratorzy lub Płace. Jeśli w sytuacji awaryjnej do grupy dodano dodatkowego użytkownika, to zostanie on automatycznie usunięty z grupy

w momencie kolejnego odświeżenia Zasad grupowych. Mechanizm ten może być używany także do wymuszania składu grup na stacjach roboczych w domenie (czyli do zapewnienia przynależności określonych administratorów domeny do lokalnych grup Administratorów na stacjach roboczych).

Usługi systemowe

Ustawienia te dotyczą trybu uruchamiania i uprawnień dostępu do usług systemowych, na przykład, kto jest uprawniony do uruchomienia i zatrzymania usługi fax.

Rejestr

W tym miejscu znajdują się ustawienia dotyczące kluczy rejestrowych, między innymi dotyczące kontroli dostępu, inspekcji i praw własności.

System plików

W tym miejscu znajdują się ustawienia dotyczące obiektów systemu plikowego, między innymi dotyczące kontroli dostępu, inspekcji i praw własności.

Przyrostowe szablony zabezpieczeń

Windows 2000 zawiera kilka przyrostowych szablonów zabezpieczeń. Domyślnie, szablony są przechowywane pod %systemroot%\Security\Templates. Szablony można dostosować za pomocą snap-in MMC Szablony zabezpieczeń (Security Templates) i importować do rozszerzenia snap-in Zasady grupowe – Ustawienia zabezpieczeń.

Szablony te są przeznaczone dla komputerów Windows 2000 skonfigurowanych przy użyciu domyślnych ustawień zabezpieczeń Windows 2000. Szablony modyfikują domyślne ustawienia w sposób przyrostowy, nie kumulatywny.

Uwaga: Nie należy stosować szablonów przyrostowych do systemów Windows 2000 powstałych w wyniku uaktualnienia Windows NT 4.0.

Szablony przyrostowe należy stosować tylko do systemów Windows 2000, które zostały zainstalowane na czystych partycjach NTFS. W przypadku komputerów NTFS uaktualnionych z Windows NT 4.0 lub wcześniejszych wersji, można zastosować Podstawowy (Basic) szablon zabezpieczeń w celu wprowadzenia domyślnych ustawień zabezpieczeń Windows 2000 (patrz poniżej). Nie można zabezpieczać systemów Windows 2000 zainstalowanych w systemach plików typu FAT.

Konfiguracje zabezpieczeń

Zastosować można standardowe szablony ustawień zabezpieczeń. Dostępne są konfiguracje: Kompatybilna, Bezpieczna oraz Podwyższonego bezpieczeństwa.

Kompatybilna (Compatible)

Szablon Kompatybilny (Compatws.inf) może być zastosowany na stacjach roboczych i na serwerach. Jego celem jest umożliwienie uruchomienia starszych aplikacji w Windows 2000 przez użytkowników nie należących do grup Administratorzy i Użytkownicy zaawansowani. Domyślnie, aplikacje nie certyfikowane dla Windows 2000 nie mogą być uruchamiane pomyślnie przez zwykłych użytkowników, ale szablon Kompatybilny rozszerza domyślne uprawnienia tak, aby łatwiej było uruchomić starsze aplikacje, takie jak Microsoft Office 97, na komputerze Windows 2000. Środowisko, w którym zastosowano ten szablon, nie jest uważane za zabezpieczone.

Bezpieczna (Secure)

Konfiguracja Bezpieczna zapewnia dodatkowe zabezpieczenia dla części systemu operacyjnego pozostających poza zakresem domyślnych uprawnień kontroli dostępu. Odpowiednie szablony nazywają się Securews.inf i Securedc.inf i mogą być zastosowane na stacjach roboczych, serwerach i kontrolerach domen

Konfiguracja ta zawiera wzmocnione ustawienia dotyczące zasad kont, inspekcji

i niektórych często używanych kluczy rejestrowych związanych z zabezpieczeniami. Szablony Bezpieczne nie modyfikują list kontroli dostępu, ale przenoszą wszystkich członków grupy Użytkownicy zaawansowani do grupy Użytkownicy.

Podwyższonego bezpieczeństwa (High Secure)

Konfiguracja Podwyższonego bezpieczeństwa zapewnia jeszcze mocniejsze zabezpieczenia niż konfiguracja Bezpieczna. Odpowiednie szablony, Hisecws.inf i Hisecdc.inf, mogą być zastosowane na stacjach roboczych, serwerach i kontrolerach domen.

Konfiguracja Podwyższonego bezpieczeństwa wymaga, aby wszystkie komunikacje sieciowe były cyfrowo podpisane i zaszyfrowane. Może to uniemożliwić komunikację pomiędzy komputerami Windows 2000 a klientami posiadającymi wcześniejsze wersje (na przykład, Microsoft Windows 98), które nie wspierają tych samych mechanizmów ochrony komunikacji sieciowych. W tej konfiguracji Użytkownicy zaawansowani posiadają te same uprawnienia dostępu do kluczy rejestru i systemu plików co zwykli Użytkownicy. Oznacza to, że użytkownikom można nadać uprawnienia do wykonania zaawansowanych zadań, takich jak utworzenie dzierżaw i ustawienie godziny systemowej, bez nadania im uprawnień pozwalających na uruchamianie aplikacji nie certyfikowanych dla Windows 2000. Gdy szablon Podwyższonego bezpieczeństwa zastosowano do serwera, to użytkownik Terminal Server zostaje usunięty ze wszystkich list ACL dotyczących systemu plików i rejestru, co oznacza, że użytkownicy logujący się w środowiskach Terminal Server podlegają tym samym ograniczeniom co zwykli użytkownicy.

Domyślne szablony zabezpieczeń Windows 2000

Jak wcześniej wspomniano, powyższe szablony (Kompatybilny, Bezpieczny i Podwyższonego bezpieczeństwa) przyrostowo modyfikują domyślne ustawienia zabezpieczeń istniejące po czystej instalacji Windows 2000 w partycji NTFS. Aby zastosować domyślne ustawienia do uaktualnionych komputerów lub do komputerów, na których przeprowadzono czystą instalację, a później dokonano modyfikacji, należy wykorzystać następujące szablony:

- Basicwk.inf — służy do zastosowania na komputerach Windows 2000 Professional domyślnych ustawień we wszystkich zakresach oprócz Praw użytkowników i Przynależności do grup.
- Basicsv.inf — służy do zastosowania na komputerach Windows 2000 Server domyślnych ustawień we wszystkich zakresach oprócz Praw użytkowników i Przynależności do grup.
- Basicdc.inf — służy do zastosowania na kontrolerach domen Windows 2000 domyślnych ustawień we wszystkich zakresach oprócz Praw użytkowników i Przynależności do grup. Prawa użytkowników i Przynależność do grup nie są modyfikowane, ponieważ szablony te są najczęściej używane do wycofania zmian list ACL dotyczących systemu plików albo rejestru lub do zastosowania domyślnych list ACL Windows 2000 do komputerów uaktualnionych z Windows NT 4.0. W tych przypadkach wskazane jest zwykle zachowanie istniejących praw użytkowników i przynależności do grup.

Instalacja oprogramowania

Snap-in Instalacja oprogramowania służy do centralnego zarządzania dystrybucją oprogramowania w organizacjach. Programy dla grup użytkowników mogą być przypisane lub opublikowane, a programy dla grup komputerów – przypisane.

Gdy aplikacje są przypisane grupom użytkowników, to wszyscy użytkownicy automatycznie mają dostęp do nich z pulpitu. Gdy użytkownik zaloguje się w Windows 2000, to skrót do aplikacji pojawi się w menu Start, a informacje o aplikacji, w tym adresy pakietu aplikacji i źródłowych plików instalacyjnych, zostaną umieszczone w rejestrze. Aplikacja zostanie zainstalowana w momencie, gdy użytkownik po raz pierwszy uruchomi ją z menu Start. Jeśli użytkownik usunie przypisaną aplikację za pomocą foldera Dodaj/usuń programy (Add/Remove Programs) w Panelu sterowania, to po następnym uruchomieniu komputera skrót do aplikacji pojawi się ponownie.

Gdy aplikacja jest opublikowana dla grupy użytkowników, to użytkownicy mogą wybrać, czy chcą ją zainstalować. Nie pojawiają się skróty na pulpitach ani lokalne wpisy rejestrowe dotyczące aplikacji. Informacje potrzebne do instalacji opublikowanych aplikacji

przechowywane są w obiekcie Zasad grupowych.

Aby zainstalować opublikowaną aplikację, można wykorzystać listę dostępnych programów znajdującą się pod ikoną Dodaj/usuń programy (Add/Remove Programs) w Panelu sterowania. Alternatywnie, użytkownicy mogą otworzyć plik dokumentu związany z daną opublikowaną aplikacją (na przykład, otwarcie pliku .xls spowoduje instalację Microsoft Excel).

Skrypty

We wcześniejszych wersjach Windows, jedynym wspieranym rodzimym językiem skryptowania był język polecenia MS-DOS. W Windows 2000 możliwości rozszerzono o architekturę skryptowania Microsoft ActiveX. Windows 2000 zawiera WSH (Windows Script Host), niezależny od języka host skryptowania, przeznaczony dla 32-bitowych platform Windows. WSH wymaga małej pamięci i służy jako kontroler aparatów skryptowania ActiveX. WSH umożliwia bezpośrednie uruchomienie skryptów w Windows 2000 poprzez dwukrotne kliknięcie pliku skryptu lub wpisanie nazwy pliku skryptu w wierszu polecenia. Skrypty można utworzyć za pomocą dowolnego narzędzia skryptowania WSH, takiego jak system programowania VBScript lub Microsoft JScript. Niezależni producenci oprogramowania oferują wsparcie innych popularnych języków skryptowych w WSH. WSH pozwala na uruchamianie skryptów .vbs i .js bezpośrednio z pulpitu Windows lub z konsoli polecenia, bez konieczności wbudowania skryptów w dokument HTML. Windows 2000 wspiera także pliki wsadowe typu MS-DOS (o rozszerzeniach .bat i .cmd).

Węzeł Skrypty znajdujący się pod Konfiguracją komputera zawiera ustawienia pozwalające określić skrypty uruchamiania i zamykania oraz skrypty logowania i wylogowywania.

W Windows 2000 wspieranych jest pięć rodzajów skryptów:

- Odziedziczone skrypty logowania
- Skrypty logowania Zasad grupowych
- Skrypty wylogowywania Zasad grupowych
- Skrypty uruchamiania Zasad grupowych
- Skrypty zamykania Zasad grupowych

W tabeli 22.1 przedstawione są niektóre ustawienia Zasad grupowych dotyczące skryptów.

Tabela 22.1 Ustawienia Zasad grupowych dotyczące skryptów

Ścieżka	Ustawienia Zasad grupowych
Konfiguracja komputera/Szablony administracyjne/System/Logowanie/ (Computer Configuration/Administrative Templates/System/Logon/)	Uruchom skrypty logowania synchronicznie (Run Logon Scripts Synchronously) Uruchom skrypty uruchamiania asynchronicznie (Run Startup Scripts Asynchronously) Uruchom skrypty zamykania jako widoczne (Run Shutdown Scripts Visible) Uruchom skrypty uruchamiania jako widoczne (Run Startup Scripts Visible)
Konfiguracja użytkownika/Szablony administracyjne/System/Logowania/Wylogowywania (User Configuration/Administrative Templates/System/Logon/Logoff)	Uruchom skrypty logowania synchronicznie (Run Logon Scripts Synchronously) Uruchom stare skrypty logowania jako ukryte (Run Legacy Logon Scripts Hidden) Uruchom skrypty logowania jako widoczne (Run Logon Scripts Visible) Uruchom skrypty wylogowywania jako widoczne (Run Logoff Scripts Visible)

Jeśli ukryty skrypt oczekuje na wprowadzenie danych przez użytkownika, to system sprawia wrażenie zawieszonego. Domyślny czas oczekiwania wynosi 600 sekund. Wartość tę można ustawić w Zasadach grupowych: Konfiguracja komputera\Szablony administracyjne\System\Logowanie\Maksymalny czas oczekiwania na skrypty Zasad grupowych (Maximum wait time for Group Policy scripts).

Jeśli skrypty uruchomione są w zminimalizowanym oknie, to poprzez normalizację okna można zatrzymać wykonywanie skryptu.

Ustawienie Wyłącz zachętę polecenia (Disable the Command Prompt) znajdujące się pod Konfiguracja użytkownika\Szablony administracyjne\System, uniemożliwia uruchamianie

plików wsadowych (plików o rozszerzeniach .cmd i .bat). Opcja ta nie powinna być stosowana w przypadku klientów Usług terminalowych, ponieważ uniemożliwiłaby uruchamianie skryptów Kompatybilności aplikacji. Szczegółowe informacje znajdują się w tekście wyjaśnienia Windows.

Odziedziczone skrypty logowania są skryptami określonymi w obiekcie Użytkownika. Skrypty te powinny być brane pod uwagę w przypadku mieszanego środowiska zawierającego klientów Windows NT 4.0, Microsoft Windows 95, Windows 98 i Windows 2000. Na klientach Windows 2000 i Windows 98 mogą być uruchamiane skrypty .vbs .js, ale na klientach Windows NT 4.0 i Windows 95 skrypty te muszą być wbudowane w pliki wsadowe (.bat). Skrypty działają w normalnym oknie. Alternatywnie, można zainstalować Windows Script Host, który wspiera skrypty niewbudowane we wsady. Nazwy skryptów i ich wiersze polecenia są przechowywane w pliku .pol w postaci kluczy i wartości rejestrowych.

Więcej informacji o WSH znajduje się pod odsyłaczem do Windows Script Technologies na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.

Przeadresowanie folderów

Rozszerzenie Przeadresowanie folderów służy do skierowania do alternatywnego adresu (na przykład, do dzierżawy sieciowej) następujących specjalnych folderów:

- Dane aplikacji
- Pulpit
- Moje dokumenty
  - Moje obrazy
- Menu Start

Skierowanie foldera Moje dokumenty do \\<nazwa serwera>\<nazwa dzierżawy>\% username% przyniesie użytkownikowi następujące korzyści:

- Dokumenty użytkownika są dostępne na dowolnym komputerze, niezależnie od tego, czy stosowane są profile mobilne.
- Gdy stosowane są profile mobilne, a folder Moje dokumenty nie jest zawarty w profilu, to proces logowania i wylogowywania działa szybciej (folder Moje dokumenty nie musi być kopiowany pomiędzy serwerem a klientem).
- Dane przechowywane w sieci, zamiast na komputerze lokalnym, są łatwiejsze do zarządzania i zabezpieczania.
- Foldery sieciowe mogą być udostępnione użytkownikom nawet wówczas, gdy pracują odłączeni od sieci, za pomocą technologii Plików trybu offline.

Powyższe zalety dotyczą także przeadresowania innych folderów. Skierowanie do dzierżawy DFS zapewnia odporność na awarię serwera. Więcej informacji o folderach trybu offline znajduje się w rozdziale „Zdalna instalacja systemu operacyjnego”.

Rozszerzanie snap-in Zasady grupowe

Zewnętrzni projektanci mogą opracować własne rozszerzenia snap-in Zasady grupowe. Do możliwych metod należą:

- Utworzenie szablonu administracyjnego (pliku .adm). Więcej informacji znajduje się w Pomocy Windows 2000.
- Utworzenie rozszerzenia snap-in MMC Zasady grupowe i dostarczenie interfejsu użytkownika do ustawiania zasad grupowych dotyczących danej aplikacji. Do przechowywania i dystrybucji zasad zalecane są następujące mechanizmy:
  - Najłatwiej jest wykorzystać API odpowiedni dla snap-in MMC Zasady grupowe, do zapisania Zasad grupowych opartych na rejestrze w szablonie Zasad grupowych. Więcej informacji znajduje się pod odsyłaczem do Microsoft Platform SDK na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.
  - Można użyć funkcji GetFileSysPath do przechowywania informacji nie opartych na rejestrze (opartych na plikach) w podfolderze szablonu Zasad grupowych. Folder należy nazwać zgodnie z konwencją <nazwa spółki>\<nazwa aplikacji>\<wersja>, a następnie należy umieścić w podfolderze szablonu żądane pliki. Po stronie klienta Winlogon wywoła odpowiednie dla tego narzędzia rozszerzenie klienckie, które przetwarza

informacje przechowywane w katalogu w szablonie Zasad grupowych. Projektant musi skorzystać z tego mechanizmu we właściwy sposób. Przechowując dane w podfolderze szablonu Zasad grupowych, aplikacja wykorzystuje wbudowane mechanizmy Zasad grupowych (szablon Zasad grupowych oraz Winlogon) w celu zastosowania specjalnych zasad nie opartych na rejestrze. Więcej informacji o funkcji GetFile SysPath znajduje się pod odsyłaczem do SDK na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.

- Dane mogą być przechowywane w kontenerze Zasad grupowych. Zaleca się użycie kontenera Zasad grupowych lub szablonu Zasad grupowych, ale nie obu jednocześnie.

Rozszerzenia Zasad grupowych po stronie klienta

Większość rozszerzeń snap-in Zasad grupowych zawiera także rozszerzenia strony klienta – pliki DLL odpowiedzialne za realizację Zasad grupowych na komputerach klienckich. Istnieją także rozszerzenia klienckie, takie jak Przydziały dyskowe, które nie odpowiadają określonemu snap-in. Więcej informacji znajduje się dalej w tym rozdziale pod hasłem „Zasady komputera dla rozszerzeń po stronie klienta”.

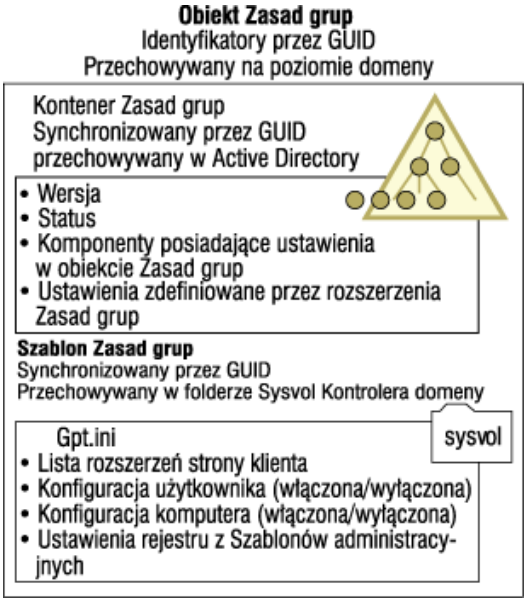
Przechowywanie Zasad grupowych

Istnieją dwa rodzaje obiektów Zasad grupowych: lokalne i nielokalne. Na każdym komputerze Windows 2000 przechowywany jest tylko jeden lokalny obiekt Zasad grupowych. Nielokalne obiekty Zasad grupowych są oparte na Active Directory.

Obiekty nielokalne (oparte na Active Directory)

Nielokalne obiekty Zasad grupowych przechowują informacje w dwóch miejscach: kontenerze Zasad grupowych i szablonie Zasad grupowych. Są one nazywane przy użyciu identyfikatora GUID, który jest używany do ich synchronizacji.

Typowe miejsca przechowywania danych zawarte w obiekcie Zasad grupowych są przedstawione na rysunku 22.4.



Rysunek 22.4 Model przechowywania Zasad grupowych

Uwaga: Administrator nie pracuje bezpośrednio z szablonem i kontenerem, lecz poprzez narzędzia Active Directory, takie jak konsola Zasad grupowych.

Kontener Zasad grupowych

Kontener Zasad grupowych jest obszarem Active Directory przeznaczonym do przechowywania właściwości obiektów Zasad grupowych. W tym miejscu znajdują się informacje o Zasadach grupowych komputera i użytkownika, mianowicie:

- Informacje o wersji, umożliwiające synchronizację z informacjami przechowywanymi w szablonie Zasad grupowych.
- Informacje o statusie obiektu Zasad grupowych (włączony lub wyłączony).
- Lista komponentów (rozszerzeń) posiadających ustawienia w obiekcie Zasad grupowych.
- Ustawienia zasad określone przez rozszerzenia snap-in.

Przykładowo, kontener Zasad grupowych zawiera informacje używane przez snap-in Instalacja oprogramowania do określenia statusu programów dostępnych do instalacji. Znajdują się tu: dane dla wszystkich aplikacji, interfejsy i API obsługujące publikację i przypisywanie aplikacji.

Szablon Zasad grupowych

Obiekty Zasad grupowych przechowują informacje również w szablonie Zasad grupowych – strukturze folderów znajdującej się w folderze wolumina systemowego (Sysvol) kontrolerów domen w podfolderze \Policies. Szablon Zasad grupowych zawiera: ustawienia zasad oparte na szablonach administracyjnych, ustawienia zabezpieczeń, aplikacje dostępne do instalacji oraz pliki skryptowe.

Gdy obiekt Zasad grupowych zostaje zmodyfikowany, to nazwa katalogu przypisywana szablonowi Zasad grupowych jest identyfikatorem GUID modyfikowanego obiektu Zasad grupowych. Na przykład, folder szablonu Zasad grupowych może otrzymać następującą nazwę:

%systemroot%\sysvol\SYSVOL\www.Reskit.com \Policies\{47636445-af79-11d0-91fe-080036644603}

Snap-in Zasady grupowe może przechowywać dane poza obiektem Zasad grupowych, ale wymaga to, co najmniej, umieszczenia łącza z obiektem Zasad grupowych w kontenerze Zasad grupowych (przechowalni danych Active Directory) lub w szablonie Zasad grupowych (danych plikowych przechowywanych w folderze Sysvol).

Uwaga: Utworzenie kopii zapasowych samych Zasad grupowych nie jest możliwe. Aby utworzyć kopię zapasową Active Directory, należy być członkiem grupy Operatorzy kopii zapasowej. Wymagane jest uprawnienie Wykonania kopii zapasowej plików i katalogów (Backup Files and Directories). Instrukcje dotyczące tworzenia kopii zapasowych Active Directory znajdują się w rozdziale „Tworzenie i przywracanie kopii zapasowej Active Directory”.

Plik Gpt.ini

W każdym głównym folderze szablonu Zasad grupowych znajduje się plik o nazwie Gpt.ini. W przypadku lokalnych obiektów Zasad grupowych informacje przechowywane w pliku Gpt.ini określają:

- Które klienckie rozszerzenia snap-in Zasady grupowe zawierają dane dotyczące komputera lub użytkownika w obiekcie Zasad grupowych.
- Czy część Konfiguracja użytkownika lub Konfiguracja komputera jest wyłączona.
- Numer wersji rozszerzenia snap-in Zasady grupowe utworzonego przez obiekt Zasad grupowych.

Lokalne obiekty Zasad grupowych

Lokalny obiekt Zasad grupowych istnieje na każdym komputerze, a domyślnie skonfigurowane są tylko węzły znajdujące się pod węzłem Ustawienia zabezpieczeń. Pozostałe ustawienia nie są ani włączone, ani wyłączone. Lokalny obiekt Zasad grupowych przechowywany jest pod %systemroot%\System32\GroupPolicy i w jego listach DACL nadawane są następujące uprawnienia:

- Administratorzy: pełna kontrola
- System operacyjny: pełna kontrola
- Użytkownik: odczyt

Jeśli grupie Administratorzy lokalni odebrano uprawnienie odczytu, to Zasady grupowe nie

będą stosowane. Jest to wygodny sposób uniemożliwienia administratorom lokalnym dostępu do obiektu Zasad grupowych, pomimo że posiadają uprawnienie zastosowania Zasad grupowych.

W przypadku lokalnego obiektu Zasad grupowych plik Gpt.ini zawiera następujące informacje:

GPCUserExtensionNames

Lista identyfikatorów GUID informująca aparat kliencki o rozszerzeniach po stronie klienta, które umieściły dane Użytkownika w obiekcie Zasad grupowych. Format wygląda następująco: [{<GUID rozszerzenia klienckiego>}{<GUID rozszerzenia MMC>}{<GUID ewentualnego drugiego rozszerzenia MMC>}][pierwsza część powtarzana odpowiednią ilość razy].

GPCMachineExtensionNames

Lista identyfikatorów GUID informująca aparat kliencki o rozszerzeniach po stronie klienta, które umieściły dane Komputera w obiekcie Zasad grupowych.

Options

Opcje dotyczące obiektu Zasad grupowych, takie jak Wyłącz konfigurację użytkownika (User portion disabled) i Wyłącz konfigurację komputera (Computer portion disabled).

GPCFunctionalityVersion

Jest to numer wersji narzędzia rozszerzenia Zasad grupowych, które utworzyło obiekt Zasad grupowych.

Podfoldery szablonu Zasad grupowych

Folder szablonu Zasad grupowych zawiera drzewo podfolderów. Liczba podfolderów jest zależna od obiektu Zasad grupowych, ale zawsze istnieją co najmniej dwa foldery (Machine i User).

Machine

Zawiera plik Registry.pol zawierający ustawienia rejestrowe dotyczące komputerów. W momencie inicjacji komputera plik Registry.pol zostaje załadowany i zastosowany do części rejestru znajdującej się pod HKEY_LOCAL_MACHINE.

User

Zawiera plik Registry.pol zawierający ustawienia rejestrowe dotyczące użytkowników. W momencie zalogowania użytkownika na komputerze plik ten zostaje załadowany i zastosowany do części rejestru znajdującej się pod HKEY_CURRENT_USER.

W folderze szablonu Zasad grupowych zawarty jest także plik Gpt.ini z informacjami o wersji. W przypadku obiektów Zasad grupowych opartych na Active Directory plik ten zawiera numer wersji obiektu Zasad grupowych w wierszu o następującym formacie:

```
Version=<numer wersji>
```

Numer wersji jest dziesiątkową reprezentacją ośmiocyfrowej liczby szesnastkowej (DWORD). Cztery najmniej znaczące cyfry reprezentują numer wersji Ustawień komputera, a cztery najbardziej znaczące cyfry – numer wersji Ustawień użytkownika. Na przykład: wpis

```
Version=65539
```

oznacza, że wersja Ustawień komputera wynosi 3, a wersja Ustawień użytkownika wynosi 1 (ponieważ liczba 65539 w systemie szesnastkowym ma postać 0X00010003).

Folder szablonu Zasad grupowych może zawierać także następujące podfoldery:

Adm

Zawiera wszystkie pliki .adm dla danego obiektu Zasad grupowych.

Machine\Scripts\Shutdown

Zawiera skrypty do wykonania przy zamykaniu komputera.

Machine\Scripts\Startup

Zawiera skrypty do wykonania przy uruchamianiu komputera.

Machine\Applications

Zawartość tego foldera zależy od aplikacji przypisanych komputerowi przez dany obiekt

Zasad grupowych.

Machine\Microsoft\Windows NT\Secedit

Zawiera GptTmpl.inf, domyślne ustawienia zabezpieczeń dla kontrolera domeny Windows 2000.

User\Applications

Zawiera pliki ogłoszenia (pliki .aas) używane przez instalator Windows.

User\Documents & Settings

Zawiera Fdeploy.ini, plik zawierający informacje o statusie przeadresowania specjalnych folderów bieżącego użytkownika.

User\Microsoft\RemoteInstall

Zawiera OSCfilter.ini, plik zawierający opcje użytkownika dotyczące instalacji systemu operacyjnego za pomocą Usług instalacji zdalnej.

User\Microsoft\IEAK

Zawiera ustawienia dla snap-in Konserwacja Internet Explorer.

User\Scripts\Logoff

Zawiera skrypty do wykonania przy wylogowywaniu użytkownika.

User\Scripts\Logon

Skrypty do wykonania przy logowaniu użytkownika.

Uwaga: Foldery User i Machine zostają utworzone podczas instalacji, a inne foldery są tworzone miarę potrzeby w momencie ustawienia zasad.

Pliki Registry.pol

W rozszerzeniu Szablony administracyjne (Administrative Templates) informacje są zapisywane w szablonie Zasad grupowych w plikach tekstowych o nazwie Registry.pol. Pliki te zawierają niestandardowe ustawienia do zastosowania w rejestrze pod Machine lub User, określone w snap-in Zasady grupowe. Plik Registry.pol w Windows 2000 jest odpowiednikiem pliku Config.pol w Windows 95, Windows 98 lub Windows NT 4.0 NT.

W szablonie Zasad grupowych zostają utworzone dwa pliki Registry.pol. Jeden (przechowywany w podkatalogu \Machine) dotyczy Konfiguracji komputera, a drugi (w podkatalogu \User) dotyczy Konfiguracji użytkownika.

Uwaga: Format plików .pol w szablonie Zasad grupowych różni się od formatu plików .pol stosowanych we wcześniejszych wersjach Windows.

Pliki .pol utworzone w Windows NT 4.0 i Windows 95 mogą być zastosowane tylko do systemu operacyjnego, w którym zostały utworzone. Pliki .pol produkowane przez Edytor zasad systemowych w Windows NT 4.0 są plikami binarnymi, podczas gdy pliki Registry.pol produkowane pod węzłem Szablony administracyjne w snap-in Zasady grupowe są plikami tekstowymi z wbudowanymi łańcuchami binarnymi.

Aby wyświetlić pliki .pol bez ich zastosowania do rejestru, należy wykorzystać narzędzie Regview.exe z CD-ROM Microsoft Windows 2000 Server Resource Kit.

Więcej informacji o plikach Registry.pol znajduje się pod odsyłaczem do Microsoft Platform SDK na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.

Łącza obiektu Zasad grupowych

Łącza służą do zastosowania obiektów Zasad grupowych do lokacji, domen lub jednostek organizacyjnych. Nielokalny obiekt Zasad grupowych nie połączony z lokacją, domeną lub jednostką organizacyjną nie ma wpływu na żadnego użytkownika ani komputer, nawet w domenie przechowywania.

Opcje Nie zastępuj i Zablokuj dziedziczenie zasad

Ustawienie opcji Nie zastępuj (No Override) na określonym łączu obiektu Zasad grupowych uniemożliwia zastępowanie danych zasad przez obiekty Zasad grupowych połączone z niższym poziomem Active Directory. Ustawienie tej opcji uniemożliwia także zastępowanie zasad przez obiekty Zasad grupowych połączonych z tym samym poziomem bez opcji Nie zastępuj. Jeśli kilka łączy na tym samym poziomie Active Directory ustawiono na Nie zastępuj, to należy określić ich priorytety. Łącza występujące na liście na wyższej pozycji mają pierwszeństwo w przypadku wszystkich skonfigurowanych ustawień (ustawień Włączonych [Enabled] lub Wyłączonych [Disabled]).

Jeśli obiekt Zasad grupowych połączono z domeną, a na łączu ustawiono opcję Nie zastępuj, to skonfigurowane ustawienia zawarte w tym obiekcie będą dotyczyć wszystkich jednostek organizacyjnych należących do tej domeny. Obiekty Zasad grupowych połączone z jednostkami organizacyjnymi nie mogą zastępować obiektu połączonego z domeną. Alternatywnie można zablokować dziedziczenie Zasad grupowych w Active Directory, przy użyciu opcji Zablokuj dziedziczenie zasad (Block Policy inheritance) na zakładce Zasady grupowe na stronie właściwości domeny lub jednostki organizacyjnej. Opcja ta nie istnieje na poziomie lokacji.

Poniżej przedstawione są niektóre istotne fakty dotyczące powyższych opcji:

- Opcja Nie zastępuj jest ustawiona na łączu, nie na lokacji, domenie, jednostce organizacyjnej czy obiekcie Zasad grupowych.
- Opcja Zablokuj dziedziczenie zasad jest ustawiona na domenie lub jednostce organizacyjnej, a więc dotyczy każdego obiektu Zasad grupowych połączonego z tym lub wyższym poziomem Active Directory, o ile może zostać zastąpiony.
- W przypadku konfliktu opcja Nie zastępuj ma pierwszeństwo przed Zablokuj dziedziczenie zasad.

Aby zobaczyć z czym obiekt Zasad grupowych jest połączony, należy otworzyć obiekt w konsoli Zasad grupowych, kliknąć prawym przyciskiem myszy węzeł główny, wybrać Właściwości (Properties) i kliknąć zakładkę Łącza (Links). Następnie należy wybrać domenę z menu rozwijanego i kliknąć Znajdź teraz (Find Now).

Wiele obiektów Zasad grupowych

Każdy nielokalny obiekt Zasad grupowych jest przechowywany w określonej domenie (domenie przechowywania). Nie należy mylić domeny przechowywania z domeną, z którą obiekt Zasad grupowych jest połączony.

Z daną lokacją, domeną lub jednostką organizacyjną może być połączonych wiele obiektów Zasad grupowych. Natomiast jeden obiekt Zasad grupowych może być połączony z wieloma lokacjami, domenami i jednostkami organizacyjnymi, bez względu na to, w której domenie obiekt jest przechowywany.

Obiekt Zasad grupowych może być połączony ze swoją domeną przechowywania. Jest to zalecane w przypadku, gdy połączenia sieciowe z innymi domenami działają wolno.

Możliwe jest także ustanowienie więcej niż jednego łącza pomiędzy danym obiektem Zasad grupowych a daną lokacją, domeną lub jednostką organizacyjną, jednakże metoda ta jest rzadko przydatna.

Dla maksymalizacji wydajności należy uniknąć łączy z obiektem Zasad grupowych przechowywanym w innej domenie.

Edycja obiektu Zasad grupowych w innych domenach

Aby móc edytować obiekt Zasad grupowych, należy spełnić następujące warunki:

- Należy posiadać uprawnienia odczytu/zapisu (lub Pełnej kontroli) w stosunku do obiektu Zasad grupowych.
- Należy być zalogowanym w domenie przechowywania obiektu Zasad grupowych lub z domenie zaufanej przez tę domenę.

Filtrowanie i delegowanie Zasad grupowych za pomocą grup zabezpieczenia

W Zasadach grupowych, grupy zabezpieczenia są używane do:

- Filtrowania zakresu obiektu Zasad grupowych
- Delegowania sterowania Zasadami grupowymi

Filtrowanie zakresu obiektu Zasad grupowych

W celu wykorzystania filtrowania zakresu zastosowania danego obiektu Zasad grupowych, należy użyć zakładki Zabezpieczenia (Security) na stronie właściwości obiektu Zasad grupowych.

Filtrowanie zawsze dotyczy całego obiektu Zasad grupowych, nie jego części. Nie jest to jednak prawdą w przypadku Przeadresowania folderów i Instalacji oprogramowania, dla których ustawione są dodatkowe listy ACL na poziomie obiektu Zasad grupowych oparte na przynależności do grup zabezpieczenia.

Ustawianie uprawnień otrzymania Zasad grupowych

Lista DACL (dyskrecjonalna lista kontroli dostępu) jest listą uprawnień (odczytu, zastosowania Zasad grupowych, pełnej kontroli itp.) dotyczących obiektu Zasad grupowych lub innego obiektu. Lista DACL ustawiona na obiekcie Zasad grupowych służy do umożliwienia lub uniemożliwienia dostępu do obiektu użytkownikom lub komputerom należącym do określonych grup zabezpieczenia.

Dostęp do zakładki Zabezpieczenia (Security) strony właściwości obiektu Zasad grupowych można uzyskać klikając prawym przyciskiem myszy węzeł główny snap-in Zasady grupowe. Alternatywnie można otworzyć stronę właściwości lokacji, domeny lub jednostki organizacyjnej połączonej z danym obiektem Zasad grupowych, wybrać zakładkę Zasady grupowe (Group Policy) i kliknąć prawym przyciskiem myszy obiekt wybrany z listy obiektów Zasad grupowych.

Grupy posiadające uprawnienia Zastosowania Zasad grupowych i Odczytu w stosunku do obiektu Zasad grupowych otrzymują skonfigurowane w nim ustawienia Zasad grupowych, o ile podlegają one obiektowi w Active Directory. Domyślnie, zidentyfikowani użytkownicy posiadają uprawnienia Zastosowania Zasad grupowych i Odczytu, ale nie Zapisu ani Pełnej kontroli. Oznacza to, że domyślnie użytkownicy nie mogą modyfikować informacji zawartych w obiekcie Zasad grupowych. Domyślnie, administratorzy domeny, administratorzy przedsiębiorstwa i system lokalny posiadają Pełną kontrolę bez uprawnienia Zastosowania Zasad grupowych. Domyślnie, administratorzy są także zidentyfikowanymi użytkownikami, czyli posiadają także atrybut Zastosowania Zasad grupowych. Więcej informacji znajduje się dalej w tym rozdziale pod hasłem „Edycja obiektów Zasad grupowych”.

Uwaga: Zaleca się odebranie uprawnień Odczytu grupom, których członkowie nie muszą otrzymywać zasad i nie są administratorami. Przetwarzanie Zasad grupowych jest szybsze w przypadku, gdy niepotrzebne uprawnienia Odczytu i Zastosowania Zasad grupowych są wyłączone. Sytuacja, w której jeden użytkownik posiada uprawnienie odczytu powyżej 1000 obiektów Zasad grupowych, spowoduje błąd Zasad grupowych (patrz rozdział „Rozwiązywanie problemów w Zarządzaniu adaptacją i konfiguracją pulpitu”).

Administratorzy sieciowi (członkowie grupy Administratorzy przedsiębiorstwa lub Administratorzy domeny) mogą wykorzystać zakładkę Zabezpieczenia (Security) w stronie właściwości obiektu Zasad grupowych do delegowania sterowania obiektami Zasad grupowych, czyli do określenia, które grupy administracyjne mogą modyfikować ustawienia obiektów Zasad grupowych. Aby to wykonać, administrator sieciowy może zdefiniować grupy administratorów (na przykład, Administratorzy marketingu) i nadać tym grupom uprawnienie Odczytu/zapisu w stosunku do wybranych obiektów Zasad grupowych.

Uprawnienie Pełnej kontroli w stosunku do obiektu Zasad grupowych nie wystarcza do umożliwienia połączenia go z lokacją, domeną lub jednostką organizacyjną. Można jednak nadać to prawo za pomocą Kreatora delegowania kontroli.

Delegowanie sterowania Zasadami grupowymi

Zasady grupowe należą do zadań administracyjnych Windows 2000, które mogą podlegać delegowaniu. Możliwe jest niezależne delegowanie trzech następujących zadań:

- Zarządzanie łączami Zasad grupowych z daną lokacją, domeną lub jednostką organizacyjną.

Tworzenie obiektów Zasad grupowych.

- Edycja obiektów Zasad grupowych.

Nielokalne Zasady grupowe, podobnie jak wszystkie narzędzia administracyjne oparte na Active Directory, wymagają kontrolera domeny Windows 2000. Podobnie jak większość narzędzi administracyjnych Windows 2000, Zasady grupowe są obsługiwane w konsolach MMC. Prawami tworzenia, konfigurowania i otwierania konsol MMC można zarządzać za pomocą ustawień Zasad grupowych znajdujących się w folderze:

<nazwa obiektu Zasad grupowych>/Konfiguracja użytkowników /Szablony administracyjne/Komponenty Windows/Microsoft Management Console/

oraz w jego podfolderach.

Ustawienia uprawnień w stosunku do obiektu Zasad grupowych są przedstawione w tabeli 22.2.

Tabela 22.2 Ustawienia uprawnień w stosunku do obiektu Zasad grupowych.

Grupy lub użytkownicy	Uprawnienie
Zidentyfikowany użytkownik	Odczyt oraz Zastosowanie Zasad grupowych
Administratorzy domeny, Administratorzy przedsiębiorstwa, Twórca, Właściciel, System lokalny	Pełna kontrola, bez Zastosowania Zasad grupowych

Uwaga: Domyślnie, administratorzy są także użytkownikami zidentyfikowanymi, a więc posiadają włączony atrybut Zastosowania Zasad grupowych (Apply Group Policy). Więcej informacji znajduje się dalej w tym rozdziale pod hasłem „Edycja obiektów Zasad grupowych”.

Aby administrować Zasadami grupowymi, należy zalogować się na lokalnym lub zdalnym kontrolerze domeny, co wymaga specjalnego uprawnienia. Uprawnienie to posiadają administratorzy domeny oraz wewnętrzny administrator kontrolera domeny.

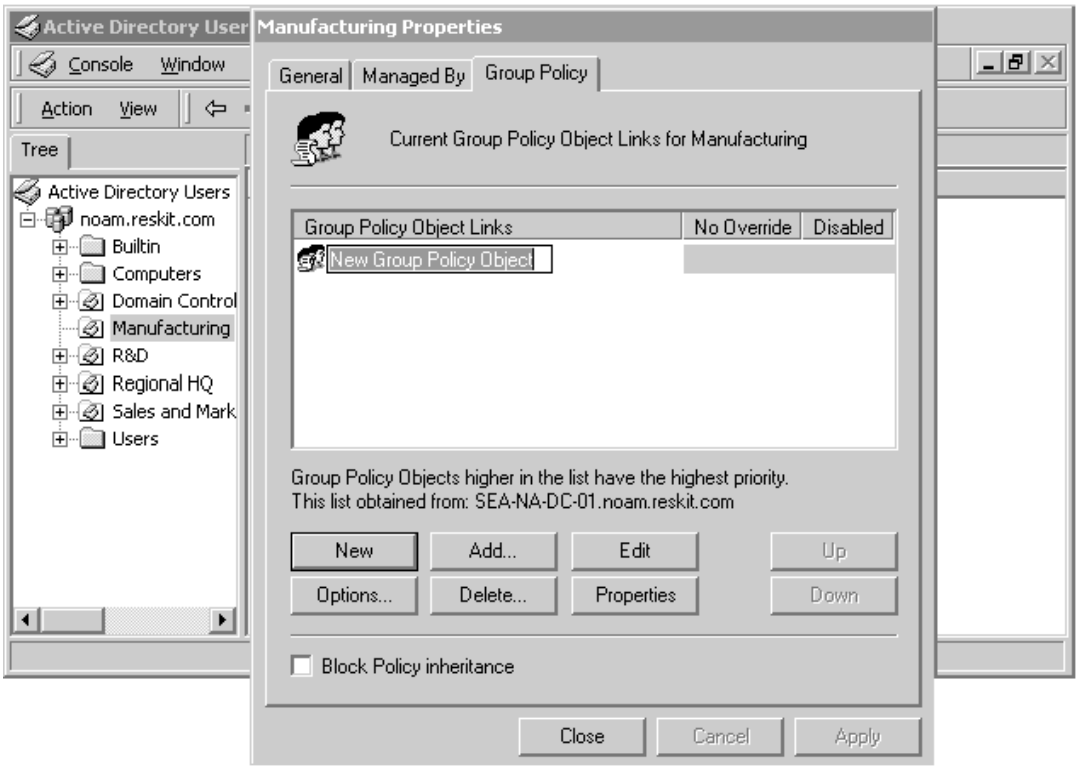
Osoby nie będące administratorami mogą zalogować się na kontrolerze domeny tylko w przypadku, gdy posiadają uprawnienia lokalnego logowania. Ustawienie to należy do obiektu Zasad grupowych Domyślne kontrolery domeny, połączonego z jednostką organizacyjną Kontrolery domeny w konsoli Użytkownicy i komputery Active Directory, pod ścieżką Konfiguracja komputera/Ustawienia Windows/Ustawienia zabezpieczeń /Zasady lokalne/Przypisywanie praw użytkowników/Lokalne logowanie.

Zalecane jest utworzenie grupy zabezpieczenia zawierającej użytkowników potrzebujących możliwości lokalnego logowania na kontrolerze domeny oraz dodanie tej grupy do listy pokazanej w formularzu Lokalne logowanie (Log On Locally). Należy pamiętać, że do czasu odświeżenia zasad na kontrolerze domeny, nowe ustawienia nie wejdą w życie.

Zarządzanie łączami Zasad grupowych z daną lokacją, domeną lub jednostką organizacyjną

Na zakładce Zasady grupowe (Group Policy) na stronie właściwości lokacji, domeny lub jednostki organizacyjnej można określić, które obiekty Zasad grupowych są połączone z daną lokacją (domeną, jednostką organizacyjną). Odpowiednie ustawienia przechowywane są w dwóch właściwościach Active Directory: gPLink i gPOptions. Właściwość gPLink zawiera listę łączy, wraz z ich priorytetami, a gPOptions zawiera ustawienia Zablokuj dziedziczenie zasad (Block Policy Inheritance) w stosunku do domen lub jednostek organizacyjnych (w przypadku lokacji ustawienie to jest niedostępne).

Na rysunku 22.5 przedstawione jest utworzenie nowego obiektu Zasad grupowych w konsoli Użytkownicy i komputery Active Directory. Domyślna nazwa obiektu brzmi Nowy obiekt Zasad grupowych (New Group Policy Object), ale można wybrać nazwę bardziej opisową. Obiekt ten będzie przechowywany w domenie noam.reskit.com i zostanie automatycznie połączony z jednostką organizacyjną Produkcja.



Rysunek 22.5 Tworzenie nowego obiektu Zasad grupowych

Active Directory wspiera ustawianie uprawnień w stosunku do określonych właściwości. Jeśli użytkownicy posiadają uprawnienie Odczytu i Zapisu w stosunku do właściwości gPLink i gPOptions, to mogą zarządzać listą obiektów Zasad grupowych połączonych z daną lokacją, domeną lub jednostką organizacyjną. Aby nadać użytkownikowi te uprawnienia, należy uruchomić zadanie Zarządzaj łączami Zasad grupowych (Manage Group Policy links) w Kreatorze delegowania kontroli.

Tworzenie obiektów Zasad grupowych

Domyślnie, nowe obiekty Zasad grupowych mogą zostać utworzone tylko przez: Administratorów domeny, Administratorów przedsiębiorstwa, Twórców/właścicieli Zasad grupowych i system operacyjny. Aby umożliwić utworzenie obiektów Zasad grupowych przez innego użytkownika lub grupę, administrator domeny może dodać tego użytkownika lub grupę do grupy zabezpieczenia Twórcy/właściciele Zasad grupowych. Gdy członek tej grupy utworzy obiekt Zasad grupowych, to zostanie on twórcą/właścicielem obiektu i będzie mógł edytować ten obiekt. Członek tej grupy otrzymuje uprawnienie pełnej kontroli tylko w stosunku do obiektów utworzonych przez niego lub jawnie do niego delegowanych. Nie otrzymuje pełnej kontroli nad pozostałymi obiektami ani prawa połączenia obiektów Zasad grupowych z lokacjami, domenami i jednostkami organizacyjnymi.

Edycja obiektów Zasad grupowych

Domyślnie, Administratorzy domeny, Administratorzy przedsiębiorstwa, system operacyjny i Twórca/właściciel obiektu Zasad grupowych otrzymują uprawnienie Pełnej kontroli w stosunku do obiektu Zasad grupowych, ale bez atrybutu Zastosowanie Zasad grupowych (Apply Group Policy). Mogą oni edytować obiekt. Natomiast, nawet jeśli posiadają oni konta w lokacjach, domenach i jednostkach organizacyjnych Active Directory połączonych z obiektem, to ustawienia zasad zawarte w tym obiekcie nie dotyczą ich, chyba że spełnione są oba następujące warunki:

- Posiadają oni, jako członkowie drugiej grupy zabezpieczenia, uprawnienie Zastosowania Zasad grupowych (Apply Group Policy) ustawione na Zezwalaj.
- Nie posiadają, jako członkowie jakiejkolwiek grupy zabezpieczenia, ustawienia Zastosowania Zasad grupowych – Odmów.

Domyślnie, zidentyfikowani użytkownicy posiadają uprawnienie Odczytu w stosunku do obiektu Zasad grupowych z włączonym atrybutem Zastosowanie Zasad grupowych (Apply Group Policy).

Uwaga: Domyślnie, administratorzy są także zidentyfikowanymi użytkownikami, a więc posiadają włączony atrybut Zastosowanie Zasad grupowych (Apply Group Policy). Istnieją dwie metody zmiany tej sytuacji:

- Usunięcie z listy zidentyfikowanych użytkowników i dodanie nowej grupy zabezpieczenia z atrybutem Zastosowanie Zasad grupowych (Apply Group Policy) ustawionym na Zezwalaj (Allow). Nowa grupa powinna zawierać wszystkich użytkowników, których mają dotyczyć nowe Zasady grupowe.
- Ustawienie atrybutu Zastosowanie Zasad grupowych (Apply Group Policy) na Odmów (Deny) w stosunku do grup: Administratorzy domeny/przedsiębiorstwa oraz ewentualnie Twórcy/właściciele. Zapobiega to zastosowaniu obiektu Zasad grupowych do członków tych grup. Należy pamiętać, że ustawienie Odmów (Deny) zawsze ma pierwszeństwo przed ustawieniem Zezwalaj (Allow) ewentualnie zastosowanym dla innej grupy, której dany użytkownik jest członkiem.

Gdy użytkownik nie będący administratorem utworzy obiekt Zasad grupowych, to zostanie on Twórcą/właścicielem obiektu Zasad grupowych. Twórcą/właścicielem obiektu utworzonego przez administratora jest grupa Administratorzy domeny.

Aby zmodyfikować obiekt Zasad grupowych, użytkownik musi posiadać w stosunku do niego uprawnienia Odczytu i Zapisu. Obiekt Zasad grupowych nie może być otwarty w trybie tylko do odczytu. Zmiany dokonywane podczas edycji są wprowadzane natychmiast, bez etapu zapisu lub „aktywizacji”. Aby uniknąć błędów, podczas edycji można odłączyć obiekt Zasad grupowych od lokacji, domen i jednostek organizacyjnych lub wyłączyć węzły Konfiguracja użytkownika i Konfiguracja komputera.

Użytkownik edytujący obiekt Zasad grupowych musi być administratorem albo twórcą/właścicielem lub mieć delegowany dostęp do obiektu. Aby nadać użytkownikowi delegowany dostęp, administrator lub twórca/właściciel dodaje go do listy Twórców/właścicieli obiektu na zakładce Zabezpieczenia (Security) na stronie właściwości obiektu Zasad grupowych.

Przykłady delegowania Zasad grupowych

Poniżej przedstawione są trzy przykłady delegowania Zasad grupowych.

Przykład 1

W tym przykładzie użytkownik otrzymuje uprawnienia sterowania jednostką organizacyjną pozwalające mu na połączenie istniejących obiektów Zasad grupowych z jednostką organizacyjną, ale nie na tworzenie nowych obiektów.

Rola odgrywana w tym przykładzie przez pojedynczego użytkownika może być odgrywana także przez grupę zabezpieczenia.

1. W snap-in Użytkownicy i komputery Active Directory (Active Directory Users and Computers) należy kliknąć prawym przyciskiem myszy odpowiednią jednostkę i wybrać Deleguj kontrolę (Delegate Control).
2. W Kreatorze delegowania kontroli należy kliknąć Dalej (Next) na stronie wprowadzającej, wybrać nazwę odpowiedniego użytkownika do delegowania i kliknąć Dalej (Next).
3. Na liście zadań należy wybrać Zarządzanie łączami Zasad grupowych (Manage Group Policy links), kliknąć Dalej (Next) oraz Koniec (Finish).

Wybrany użytkownik może dodawać i usuwać łącza pomiędzy określoną jednostką organizacyjną a dowolnymi obiektami Zasad grupowych, w stosunku do których posiada on uprawnienie Odczytu.

Jeśli obiekt Zasad grupowych jest przechowywany w innej domenie, to domena

użytkownika musi być domeną zaufaną względem domeny przechowywania.

Przykład 2

W tym przykładzie użytkownik otrzymuje uprawnienie do utworzenia nowych obiektów Zasad grupowych.

Uprawnienie to jest przydatne w wielu przypadkach w kombinacji z uprawnieniem utworzenia łączy opisanym powyżej. Aby nadać użytkownikowi uprawnienie utworzenia nowych obiektów Zasad grupowych, należy:

1. W konsoli Użytkownicy i komputery Active Directory (Active Directory Users and Computers) odnaleźć kontener Użytkownicy (Users) w głównym folderze domeny.
2. Kliknąć dwukrotnie Twórcy/właściciele Zasad grupowych (Group Policy Creator Owners).
3. Na stronie właściwości wybrać zakładkę Członkowie (Members).
4. Kliknąć Dodaj (Add) i dodać wybranego użytkownika do grupy Tworców/właścicieli.

Użytkownik może teraz utworzyć nowe obiekty Zasad grupowych. Użytkownik tworzący obiekt zostaje jego Twórcą/właścicielem.

Aby utworzyć obiekty Zasad grupowych w konsoli Użytkownicy i komputery Active Directory, należy kliknąć prawym przyciskiem myszy odpowiednią domenę lub jednostkę organizacyjną, kliknąć Właściwości (Properties), wybrać zakładkę Zasady grupowe (Group Policy) i kliknąć Nowe (New). Domyślnie, nowe obiekty zostają połączone z domeną lub jednostką organizacyjną, przy której zostały utworzone. Jeśli użytkownik lub administrator tworzący w ten sposób obiekt nie posiada uprawnienia połączenia obiektu z daną domeną albo jednostką, to przycisk Nowe na stronie właściwości pojawi się przyciemniony.

Przykład 3

W tym przykładzie nieadministracyjny użytkownik lub grupa użytkowników otrzymuje prawo kontroli w stosunku do obiektu Zasad grupowych. Aby nadać takie uprawnienie, należy:

1. Otworzyć obiekt Zasad grupowych w snap-in Zasady grupowe.
2. Kliknąć prawym przyciskiem myszy węzeł główny, wybrać Właściwości (Properties) i kliknąć Zabezpieczenia (Security).
3. Kliknąć Dodaj (Add) w celu dodania użytkownika lub grupy, a następnie kliknąć Pełna kontrola (Full control).
4. Ustawić odpowiednio opcję Zastosowanie Zasad grupowych (Apply Group Policy).

   Jeśli pole wyboru Zastosowanie Zasad grupowych jest wyczyszczone, to pole wyboru Pełna kontrola również zostanie wyczyszczone, ale użytkownik wciąż ma dostęp odczytu/zapisu do obiektu Zasad grupowych.
5. Kliknąć OK w celu zapisania zmian.

   Teraz wybrany użytkownik lub grupa może edytować obiekt Zasad grupowych.

Tworzenie konsol MMC do delegowania Zasad grupowych

Utworzyć można konsole MMC Zasad grupowych określające, którzy użytkownicy i które grupy mają uprawnienia dostępu do danych obiektów Zasad grupowych, lokacji, domen lub jednostek organizacyjnych. Uprawnienia dotyczące obiektu Zasad grupowych są definiowane na zakładce Zabezpieczenia (Security) na stronie właściwości obiektu.

Tego typu delegowanie jest rozszerzane przez ustawienia Zasad grupowych dotyczące MMC (pod węzłem Szablony administracyjne\Komponenty Windows\Microsoft Management Console). Ustawienia te pomagają określić, które snap-in MMC dany użytkownik może uruchomić (lub którego snap-in użytkownik nie może uruchamiać). Więcej informacji znajduje się w tekście na zakładce Wyjaśnij (Explain) dla poszczególnych ustawień.

Niestandardowe konsole (pliki .msc) można utworzyć dla Zasad grupowych tak samo, jak dla innych snap-in.

Utworzyć można konsole Zasad grupowych obejmujące tylko część rozszerzeń snap-in Zasad grupowych. Na przykład, utworzyć można niestandardową konsolę Zasad grupowych zawierającą tylko rozszerzenie Ustawienia zabezpieczenia. W ten sposób można zdefiniować ustawienia Zasad grupowych metodą modularną.

Utworzyć można także niestandardowe konsole zawierające egzemplarze Zasad

grupowych, które są powiązane z różnymi obiektami Zasad grupowych lub zawierają snap-in nie związane z Zasadami grupowymi.

Wykorzystywane przez snap-in pliki DLL muszą być obecne na komputerze, na którym działa konsola. Jeśli komputer jest kontrolerem domeny, to pliki DLL są prawdopodobnie już obecne. Aby zainstalować je ma serwerze członkowskim Windows 2000 lub na komputerze Windows 2000 Professional, należy przypisać lub opublikować Narzędzia administracyjne Windows 2000. Pakiet ten nazywa się Adminpak.msi i znajduje się na CD-ROM Windows 2000 Server.

Istnieje kilka sposobów uruchomienia snap-in Zasady grupowe, zależnie od celu. Więcej informacji znajduje się w Pomocy Windows 2000. Zaleca się, aby Zasady grupowe były delegowane za pomocą Konsol niestandardowych. Aby to wykonać, należy uruchomić Zasady grupowe jako autonomiczny snap-in:

Aby uruchomić Zasady grupowe jako autonomiczny snap-in. należy:

1. Kliknąć Start, kliknąć Uruchom (Run) w wpisać MMC.
2. W oknie MMC, w menu Konsola (Console), kliknąć Dodaj/Usuń przystawkę (Add/Remove Snap-in).
3. Na zakładce Autonomiczna kliknąć Dodaj.
4. W oknie dialogowym kliknąć Zasady grupowe (Group Policy), a następnie kliknąć Dodaj (Add).
5. W oknie dialogowym wyboru obiektu Zasad grupowych, kliknąć Przeglądaj (Browse) i odnaleźć żądany obiekt.
6. Kliknąć Rozszerzenia (Extensions) i wybrać odpowiednie rozszerzenia.
7. Kliknąć Koniec (Finish).
8. Kliknąć OK. Snap-in Zasady grupowe zostanie otwarty wraz z wybranym obiektem Zasad grupowych.
9. Po określeniu żądanych ustawień zasad kliknąć Zapisz jako (Save As) w menu Konsola (Console) w celu zapisania ustawień w pliku .msc.

Aby ustawić uprawnienia dostępu, należy użyć zakładki Zabezpieczenia (Security) na stronie Właściwości (Properties) wybranego obiektu Zasad grupowych. Uprawnienia te umożliwiają lub uniemożliwiają dostęp do obiektu określonym grupom.

Istnieją dziesiątki ustawień Zasad grupowych dających lub zabraniających dostępu do różnych snap-in i rozszerzeń. Przydatne mogą być ustawienia znajdujące się w następujących folderach:

- Konfiguracja użytkownika/Szablony administracyjne/Microsoft Management Console
- Konfiguracja użytkownika/Szablony administracyjne/Microsoft Management Console/Ograniczone/Dozwolone snap-in
- Konfiguracja użytkownika/Szablony administracyjne/Microsoft Management Console/Ograniczone/Dozwolone snap-in/Rozszerzenia snap-in
- Konfiguracja użytkownika/Szablony administracyjne/Microsoft Management Console/Ograniczone/Dozwolone snap-in/Zasady grupowe

Przetwarzanie Zasad grupowych

Zasady grupowe są przetwarzane w następującej kolejności:

Lokalny obiekt Zasad grupowych. Jest to jedyne źródło Zasad grupowych w przypadku komputerów autonomicznych lub należących do grup roboczych. Lokalny obiekt Zasad grupowych zawsze zostaje przetworzony.

Obiekty połączone z Active Directory. W pierwszej kolejności obiekty połączone z lokacją, następnie obiekty połączone z domeną, a na końcu obiekty połączone z jednostką organizacyjną (W przypadku zagnieżdżonych jednostek organizacyjnych nadrzędne jednostki są przetwarzane przed podrzędnymi). Na każdym poziomie może być połączonych kilka obiektów Zasad grupowych, jeden lub żaden. Jeśli istnieje więcej niż jedno łącze, to ustawić można ich priorytety.

Uwaga: Opcje Zablokuj dziedziczenie zasad lub Nie zastępuj mogą wpłynąć na obecność lub nieobecność obiektów Zasad grupowych na liście obiektów do przetwarzania, ale nie na ich kolejność. Blokowanie odbywa się na poziomie domeny lub jednostki organizacyjnej, powodując usunięcie wszystkich nielokalnych obiektów Zasad grupowych, które byłyby przetwarzane wcześniej, oprócz tych ustawionych na Nie zastępuj (No Override). Lokalny obiekt Zasad grupowych nie może zostać zablokowany. Ustawienie Nie zastępuj jest atrybutem łącza, czyli dotyczy tylko danego obiektu Zasad grupowych i tylko danej, połączonej z nim lokacji, domeny lub jednostki organizacyjnej.

Zasady dotyczące komputera są przetwarzane w momencie uruchomienia komputera, a zasady dotyczące użytkownika w momencie jego zalogowania. Generalnie, w przypadku konfliktu zasady dotyczące komputera mają pierwszeństwo przed zasadami dotyczącymi użytkownika. Nie jest to właściwość infrastruktury Zasad grupowych, lecz konwencja przestrzegana przez system operacyjny i aplikacje wykorzystujące Zasady grupowe, chyba że w stosunku do danego ustawienia takie zachowanie jest nieodpowiednie.

Uwaga: Kwestie dotyczące przetwarzania zasad mogą wystąpić podczas migracji z Windows NT 4.0 do Windows 2000. Więcej informacji znajduje się dalej w tym rozdziale pod hasłem „Kwestie dotyczące Zasad grupowych i migracji”.

Większość ustawień Zasad grupowych jest realizowana na komputerze klienckim przez pliki DLL nazywane rozszerzeniami strony klienta. Wyjątek stanowią Usługi instalacji zdalnej, ponieważ plik DLL nie może być używany przed instalacją systemu operacyjnego.

Dla każdego rozszerzenia strony klienta kolejność przetwarzania obiektów Zasad grupowych jest zwrócona przez funkcję Microsoft Win32 GetGPOList.

W większości przypadków ustawienia znajdujące się pod węzłem Konfiguracja komputera mają pierwszeństwo przed odpowiednimi ustawieniami pod węzłem Konfiguracja użytkownika. Istnieje parę wyjątków (opisanych w tekście wyjaśniającym poszczególne ustawienia). Przykładem jest ustawienie Szablony administracyjne\Komponenty Windows\Instalator Windows\Zawsze instaluj z podwyższonymi uprawnieniami (Always install with elevated privileges), które jest aktywne tylko w przypadku, gdy jest włączone w obu miejscach.

Zasady grupowe mają wpływ tylko na użytkowników i komputery zawarte w lokacjach, domenach i jednostkach organizacyjnych. Obiekty Zasad grupowych nie mogą być zastosowane do grup zabezpieczenia.

Przetwarzanie synchroniczne i asynchroniczne

Asynchroniczne procesy funkcjonują niezależnie i mogą działać równocześnie na różnych wątkach. W przypadku procesów synchronicznych kolejny proces nie może się rozpocząć, dopóki poprzedni proces się nie zakończy. W przypadku ustawień Zasad grupowych dotyczących tych typów procesów, należy wybrać szybsze procesy asynchroniczne lub bezpieczniejsze, bardziej przewidywalne przetwarzanie synchroniczne.

Domyślnie, Zasady grupowe są przetwarzane synchronicznie. Przetwarzanie zasad dotyczących komputera zostaje zakończone przed pojawieniem się okna dialogowego CTRL+ALT+DEL, a przetwarzanie zasad dotyczących użytkownika zostaje zakończone przed aktywizacją powłoki i jej udostępnieniem użytkownikowi.

Uwaga: Można wybrać ustawienia zmieniające zachowanie domyślne i wprowadzające przetwarzanie asynchroniczne. Nie jest to zalecane, chyba że istnieją bardzo przekonujące przyczyny związane z wydajnością. Bezpieczniejsze jest pozostawienie synchronicznego przetwarzania.

Zasady grupowe dotyczące komputerów zostają zastosowane w momencie uruchomienia komputera. Wobec użytkowników, Zasady grupowe zostają zastosowane przy logowaniu.

Okresowe odświeżanie

Można ustanowić okresowe przetwarzanie Zasad grupowych. Domyślnie, jest to wykonywane co 90 minut z losowym przesunięciem wynoszącym do 30 minut. Domyślne wartości można zmienić za pomocą ustawienia Zasad grupowych pod węzłem Szablony administracyjne. Określenie wartości zerowej spowoduje ustawienie interwału odświeżania na siedem sekund.

Aby zmienić to ustawienie, należy zmodyfikować obiekt Zasad grupowych Domyślne kontrolery domeny, połączony z jednostką organizacyjną Kontrolery domeny. Ustawienie znajduje się pod ścieżką Konfiguracja komputera/Szablony administracyjne/System/Zasady grupowe/Interwał odświeżania Zasad grupowych dla komputerów (Group Policy Refresh Interval for Computers).

Ostrzeżenie: Ustawienie zbyt krótkiego interwału odświeżania spowoduje częste odświeżanie powłoki Windows, co wiąże się z zamykaniem menu kontekstowych, miganiem ekranu itp. Krótkie interwały należy stosować tylko podczas testów lub demonstracji.

W przypadku kontrolerów domen domyślny interwał wynosi pięć minut. Odpowiednie ustawienie znajduje się pod ścieżką Konfiguracja komputera /Szablony administracyjne/System/Zasady grupowe/Interwał odświeżania Zasad grupowych dla kontrolerów domen (Group Policy Refresh Interval for Domain Controllers).

Instalacja oprogramowania i Przeadresowanie folderów są przetwarzane tylko przy uruchamianiu komputera lub logowaniu użytkownika, nie podczas okresowego odświeżania. Przetwarzanie okresowe tych rozszerzeń jest nieodpowiednie. Na przykład, w przypadku Instalacji oprogramowania, można włączyć ustawienia Zasad grupowych powodujące automatyczne usunięcie aplikacji, które już nie są przypisane. Jeśli Zasady grupowe spróbują usunąć aplikację lub uaktualnić przypisaną aplikację automatycznie, podczas gdy użytkownik jej używa, to nastąpi błąd.

Opcjonalne przetwarzanie niezmienionych Zasad grupowych

Aby zapewnić najwyższy poziom zabezpieczenia ustawień Zasad grupowych, należy zastosować ustawienie Przetwarzaj nawet gdy obiekty Zasad grupowych nie zostały zmienione (Process Even If The Group Policy Objects Have Not Changed) w stosunku do każdego rozszerzenia Zasad grupowych po stronie klienta, które takiego ustawienia wymaga. Ustawienia te znajdują się pod ścieżką Konfiguracja komputera\Szablony administracyjne\System\Zasady grupowe. Domyślnie, każde rozszerzenie strony klienta aktualizuje swoje ustawienia tylko po ich zmianie. Wybór powyższej opcji spowoduje zastosowanie ustawień podczas każdej sesji logowania w Active Directory. Oznacza to jednak zmniejszenie wydajności.

Zasady grupowe i sieciowa szerokość pasma

Gdy Zasady grupowe wykrywają wolne połączenie, to ustawiają flagę informującą o tym fakcie rozszerzenia strony klienta.

Poniżej przedstawione są domyślne ustawienia dotyczące stosowania zasad poprzez wolne połączenie. „Włączone” oznacza, że przetwarzanie odbywa się nawet w przypadku połączenia uważanego za wolne.

- Ustawienia zabezpieczeń — Włączone (i może zostać wyłączone)
- Szablony administracyjne — Włączone (i nie może zostać wyłączone)
- Instalacja oprogramowania — Wyłączone
- Skrypty — Wyłączone
- Przeadresowanie folderów — Wyłączone
- Konserwacja Internet Explorer — Wyłączone

Z wyjątkiem snap-in Szablony administracyjne i Ustawienia zabezpieczeń, istnieją ustawienia służące do włączania lub wyłączanie tego przetwarzania.

Zasady dotyczące definicji połączenia wolnego

Stosując Zasady grupowe można ustawić definicję połączenia wolnego dla komputerów, użytkowników i profili użytkowników.

Uwaga: Windows 2000 dodaje algorytm IP kontaktujący się z serwerem metodą ping, podczas gdy Windows NT 4.0 po prostu mierzy wydajność systemu plików.

Aby ustalić, czy połączenie będzie traktowane jako wolne, stosuje się następujący algorytm:

Wysłać serwerowi ping zawierający 0 bajtów danych. Odmierzyć liczbę milisekund (czas#1). Jeśli wartość #1 jest mniejsza od 10 ms, to zakończyć procedurę (połączenie będzie traktowane jako szybkie).

Wysłać serwerowi ping zawierający 2 KB niekompresowalnych danych i odmierzyć liczbę milisekund (czas#2). Algorytm wykorzystuje wcześniej skompresowany plik .jpg – gdyby użyto pliku kompresowalnego, to modem by go skompresował i pozorna szybkość sieci byłaby podwyższona.

DELTA = czas#2 - czas#1. W ten sposób odejmuje się czas inicjacji sesji. DELTA równa się ilości czasu (w milisekundach) wymaganego do przesłania 2 KB.

DELTĘ mierzy się trzykrotnie, a oblicza się średnią wartość DELTY, nazwaną AVG.

Szybkość połączenia (Z) w kilobitach na sekundę (Kbps) wynosi:

Z ="32000/AVG."

Ponieważ:

(Z Kbps) = 2 * (2 KB) * (8 bitów/bajt) * (1000 milisekund/sekundę) / (AVG milisekund).

Mnożymy przez czynnik 2, ponieważ 2 KB danych przeszły przez każdy modem, kartę Ethernet lub inne urządzenie w pętli w obie strony.

Uwaga: Otrzymana szybkość Z jest średnią szybkością ładowania w obie strony. W większości przypadków szybkości w obie strony są równe, ale jeśli się różnią, to należy wziąć ten fakt pod uwagę. Na przykład, w przypadku ADSL (Asymmetric Digital Subscriber Line) szybkość ładowania może wynosić w stronę serwera 128 Kbps, a w stronę klienta 768 Kbps.

Jeśli wartość Z jest mniejsza od określonego progu (domyślnie 500 Kbps) to połączenie jest uważane za wolne. W przeciwnym przypadku połączenie będzie traktowane jako szybkie.

Wartość progu można ustawić pod ścieżką <nazwa obiektu Zasad grupowych>/Konfiguracja komputera/Szablony administracyjne /System/Zasady grupowe/Wykrywanie wolnych połączeń w Zasadach grupowych (Group Policy slow link detection).

Aby określić ustawienia dotyczące wykrywania wolnych połączeń dla komputerów, należy otworzyć węzeł Konfiguracja komputera \Szablony administracyjne\System\Zasady grupowe. Ustawienia dla użytkowników znajdują się pod węzłem Konfiguracja użytkownika\Szablony administracyjne\System\Zasady grupowe.

Limit czasu wolnych połączeń dla zasad profili użytkowników znajduje się pod węzłem Konfiguracja komputera\Szablony administracyjne \System\Logowanie. W pierwszej kolejności kod profili próbuje skontaktować się z serwerem metodą ping. Jeśli serwer nie wspiera IP, to kod stosuje wcześniejszą metodę polegającą na mierzeniu wydajności systemu plików. Przy konfigurowaniu tego ustawienia należy określić limity dotyczące szybkości połączenia (w Kbps) oraz czasu tranzytu (w ms).

Odczyty rejestru

Za pomocą API, rozszerzenia snap-in Zasady grupowe mogą tymczasowo założyć blokady typu mutex (wzajemne wyłączne) w celu odczytania wartości ustawień. Jeśli blokada nie

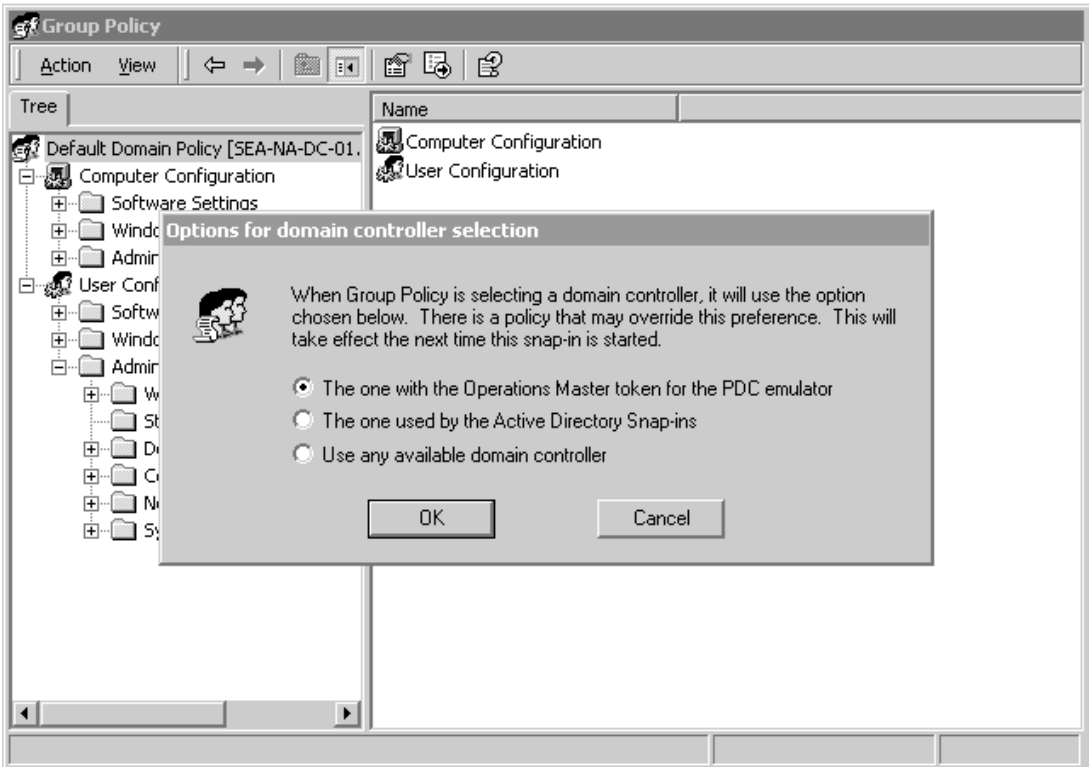
zostanie zwolniona w ciągu 10 minut, to rozszerzenie zostanie zmuszone do jej zwolnienia. W ten sposób unika się automatycznego odświeżenia Zasad grupowych podczas procesu odczytywania.

Więcej informacji o interfejsach API Zasad grupowych w Windows 2000 znajduje się pod odsyłaczem do Microsoft Platform SDK na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.

Określanie kontrolera domeny do ustawiania Zasad grupowych

Istnieją dwa sposoby ustawienia opcji Zasad grupowych dotyczących kontrolera domeny. W interfejsie użytkownika snap-in Zasady grupowe użytkownik może ustawić te opcje w oknie dialogowym Opcje kontrolera domeny (DC Options). Druga metoda, opisana później, polega na ustawianiu opcji przez głównych administratorów domeny pod węzłem Szablony administracyjne.

Menu Widok (View) w snap-in Zasady grupowe zawiera pozycję Opcje kontrolera domeny (DC Options), która pozwala otworzyć okno dialogowe zawierające opcje dotyczące kontrolera domeny używanego do edycji Zasad grupowych (rysunek 22.6).



Rysunek 22.6 Opcje wyboru kontrolera domeny

W powyższym oknie dialogowym można wybrać następujące opcje:

Posiadający główny token operacji dla emulatora kontrolera PDC (The one with the Operations Master token for the PDC emulator)

Jest to domyślna i zalecana opcja, zapobiegająca utracie danych. W tym przypadku snap-in Zasady grupowe musi wykorzystać tylko jeden kontroler domeny. Jeśli dwóch administratorów dokonuje zmian tego samego obiektu Zasad grupowych na różnych kontrolerach domeny w tym samym cyklu replikacji, to może nastąpić utrata danych spowodowana przez replikację. Zalecane jest ograniczenie liczby administratorów upoważnionych do administrowania Zasadami grupowymi oraz zastosowanie omówionej opcji wyboru kontrolera domeny. Zaleca się także, aby administratorzy wiedzieli, którzy inni administratorzy mogą edytować ten sam obiekt Zasad grupowych.

Używany przez przystawki usługi Active Directory (The one used by Active Directory Snap-ins)

W tym przypadku snap-in Zasady grupowe wykorzystuje ten sam kontroler domeny, co

snap-in Active Directory.

Użyj dowolnego dostępnego kontrolera domeny (Use any available domain controller)

W większości przypadków jest to najmniej korzystna opcja. Najprawdopodobniej zostanie wybrany kontroler domeny w lokacji lokalnej.

Wszystkie powyższe opcje można zastąpić przy użyciu ustawień zasad, tak jak opisano poniżej.

Zasady dotyczące opcji kontrolera domeny

Domyślnie, gdy obiekt Zasad grupowych jest edytowany w snap-in Zasady grupowe, to wykorzystany jest token operacji głównego kontrolera domeny. Oznacza to, że snap-in jest zawsze powiązany z tym samym kontrolerem domeny.

Główny administrator domeny może zastosować zasady dotyczące wyboru kontrolera domeny przez Zasady grupowe. Jeśli wybrana opcja jest niedostępna, to użytkownik otrzyma komunikat błędu. W tym przypadku pozycja menu Opcja kontrolera domeny (DC Options) będzie przyciemniona (niedostępna), dlatego że istnieje ustawienie zasad mające pierwszeństwo przed którąkolwiek opcją wybraną przez użytkownika. Administrator domeny może określić, na przykład, że wszyscy administratorzy muszą korzystać z głównego kontrolera domeny. Opcje dotyczące kontrolera domeny znajdują się w snap-in Zasady grupowe pod węzłem Konfiguracja użytkownika\Szablony administracyjne\System\Zasady grupowe. Dostępne są takie same opcje jakie znajdują się w oknie dialogowym opisanym w poprzedniej części.

Na przykład, administrator znajdujący się na innym kontynencie niż główny kontroler domeny może wybrać lokalną edycję zasad, ze względu na wydajność. Należy pamiętać, że w przypadku, gdy ktoś inny edytuje ten sam obiekt Zasad grupowych w tym samym czasie, to wyniki mogą być trudne do przewidzenia.

Domyślnie, jeśli snap-in Zasady grupowe nie może uzyskać dostępu do wybranego kontrolera domeny, to pojawi się następujący komunikat błędu: „Obsługa błędu nieudanego kontaktu z kontrolerem domeny (Error Handling on Failure to Reach a Domain Controller)”. Można anulować operację lub spróbować ponownie skontaktować się z kontrolerem domeny przy użyciu którejś z trzech opcji:

- Posiadający główny token operacji dla emulatora kontrolera PDC (The one with the Operations Master token for the primary domain controller emulator).
- Używany przez przystawki usługi Active Directory (The one used by Active Directory Snap-ins).
- Użyj dowolnego dostępnego kontrolera domeny (Use any available domain controller).

Natomiast w przypadku błędu: „Nie można odnaleźć kontrolera domeny. Mogą istnieć zasady uniemożliwiające wybór innego kontrolera domeny (Failed to find a domain controller. There may be a policy that prevents you from selecting another domain controller)”, należy sprawdzić, czy włączono następujące ustawienie Zasad grupowych:

<nazwa obiektu Zasad grupowych>/Konfiguracja użytkownika /Szablony administracyjne/System/Zasady grupowe/Wybór kontrolera domeny Zasad grupowych.

Wyniki wyboru kontrolera domeny

W tabeli 22.3 przedstawione są wyniki zastosowania różnych kombinacji warunków dotyczących kontrolera domeny. Użyto następujących określeń:

- Główny kontroler domeny: jest to kontroler domeny posiadający token operacji dla głównego emulatora kontrolera domeny.
- Odziedziczony: oznacza kontroler domeny używany przez snap-in Active Directory.
- 1) i 2) : oznacza, że próbuje się w pierwszej kolejności opcję 1), a następnie 2).

Tabela 22.3 Wyniki wyboru kontrolera domeny

Preferencja użytkownika	Ustawienie zasad	Odziedziczony kontrolera domeny	Wyniki
Nieokreślona	Nieokreślone	nie dotyczy	1) Główny kontroler domeny 2) Zachęta

Główny kontroler domeny	Nieokreślone	nie dotyczy	1) Główny kontroler domeny 2) Zachęta
Odziedziczony	Nieokreślone	Tak	Odziedziczony
Odziedziczony	Nieokreślone	Nie	Dowolny kontroler domeny
Dowolny	Nieokreślone	nie dotyczy	Dowolny kontroler domeny
nie dotyczy	Główny kontroler domeny	nie dotyczy	Tylko główny kontroler domeny
nie dotyczy	Odziedziczony	Tak	Odziedziczony
nie dotyczy	Odziedziczony	Nie	Dowolny kontroler domeny
nie dotyczy	Dowolny	nie dotyczy	Dowolny kontroler domeny

Przetwarzanie Zasad grupowych po stronie klienta

Niektóre komponenty Zasad grupowych zawierają rozszerzenia po stronie klienta (pliki .dll). Rozszerzenia te są ładowane w miarę potrzeby podczas przetwarzania zasad na komputerze klienckim. Komputer kliencki otrzymuje listę obiektów Zasad grupowych i ustala, które rozszerzenia strony klienta posiadają dane umieszczone w tych obiektach. Rozszerzenia te zostają wywołane z podaniem listy obiektów Zasad grupowych do przetwarzania. Pozostałe rozszerzenia strony klienta nie są wywoływane.

Rozszerzenia strony klienta przedstawione są w tabeli 22.4.

Tabela 22.4 Rozszerzenia po stronie klienta

Rozszerzenie	Nazwa pliku DLL
Rejestr (pod Szablonami administracyjnymi)	Userenv.dll
Przydziały dyskowe (pod Szablonami administracyjnymi)	Dskquota.dll
Przeadresowanie folderów	Fdeploy.dll
Skrypty	Gptext.dll
Instalacja oprogramowania	Appmgmts.dll
Zabezpieczenia	Scecli.dll
Zabezpieczenia IP	Gptext.dll
Odtwarzanie EFS (Encrypting File System)	Scecli.dll
Konserwacja Internet Explorer	iedkcs32.dll
Usługi instalacji zdalnej	brak

Preferencje dotyczące rozszerzeń po stronie klienta

Wartości umieszczone w rejestrze przez rozszerzenia strony klienta są preferencjami, nie ustawieniami Zasad grupowych. Można jednak zastosować zasady określające, że rozszerzenie ma zostać uruchomione nawet przy użyciu wolnego połączenia i niezależnie od ilości danych.

Wszystkie snap-in MMC rejestrują się w rejestrze pod kluczem:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\SnapIns\{GUID snap-in}

REG_SZ może przyjąć którąś z poniższych wartości:

- About
- NameString
- NodeType
- Provider
- Version

Rozszerzenia Zasad grupowych po stronie klienta rejestrują się w powyższym miejscu oraz pod:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Winlogon\GPExtensions\{CSE-GUID}

REG_DWORD może przyjąć którąś z następujących wartości:

Ważne: Wartości REG_DWORD są podane tylko dla informacji. Zmiana tej wartości nie jest zalecana.

- EnableAsynchronousProcessing
- LastPolicyTime
- MaxNoGPOListChangesInterval
- NoBackgroundPolicy
- NoGPOListChanges
- NoMachinePolicy
- NoSlowLink
- NoUserPolicy
- NotifyLinkTransition
- PerUserLocalSettings
- PrevSlowLink
- RequiresSucessfulRegistry
- Status
- This possible REG_SZ valuename
- ProcessGroupPolicy
- This REG_EXPAND_SZ valuename
- DllName

Uwaga: LastPolicyTime i Status są ustawiane automatycznie przez aparat Zasad grupowych, nie przez rozszerzenia strony klienta.

Zasady komputera dla rozszerzeń po stronie klienta

Dla każdego rozszerzenia strony klienta istnieją zasady komputera obejmujące maksymalnie trzy opcje (w przypadku niektórych rozszerzeń jedna z opcji jest niedostępna). Są to następujące opcje:

Zezwalaj na przetwarzanie poprzez wolne połączenie sieciowe (Allow processing across a slow network connection)

Gdy rozszerzenie strony klienta rejestruje się w rejestrze, to ustawia w nim wartości określające, czy ma zostać wywołane w przypadku stosowania wolnego połączenia. Niektóre rozszerzenia przesyłają duże ilości danych, co w przypadku wolnego połączenia może znacznie zmniejszyć wydajność. Instalacja dużej aplikacji poprzez 28,8 Kbps linię modemową jest niepraktyczna.

Nie stosuj podczas okresowego przetwarzania w tle (Do not apply during periodic background processing)

Zasady dotyczące komputera zostają zastosowane przy uruchamianiu oraz okresowo, w tle, mniej więcej co 90 minut. Zasady dotyczące użytkownika są zastosowane przy logowaniu użytkownika, a później co 90 minut. Niektóre rozszerzenia nie wykonują okresowego przetwarzania zasad, ponieważ mogłoby to zakłócić pracę użytkownika. Na przykład, rozszerzenie Instalacja oprogramowanie mogłoby spróbować usunąć aplikację, która jest aktualnie używana przez użytkownika lub przez inną aplikację. Stosując opcję Nie stosuj podczas okresowego przetwarzania w tle można jawnie określić, czy rozszerzenie będzie działać w tle.

Przetwarzaj nawet wtedy, gdy obiekty Zasad grupowych nie zostały zmienione (Process Even If The Group Policy Objects Have Not Changed)

Domyślnie, jeśli obiekty Zasad grupowych przechowywane na serwerze nie zostały zmienione, to ich zastosowanie na kliencie nie jest konieczne, ponieważ klient powinien już posiadać wszystkie obowiązujące ustawienia. Jednakże użytkownik będący administratorem swojego komputera może zmienić niektóre ustawienia. Użytkownik może, na przykład, zmienić opcje zabezpieczenia pliku lub usunąć aplikację albo jej ikonę. W takim przypadku warto ponownie zastosować żądane ustawienia podczas logowania użytkownika lub okresowego odświeżania.

W tabeli 22.5 przedstawione są rozszerzenia, w stosunku do których istnieją tylko dwie opcje zasad komputera.

Tabela 22.5 Opcje zasad dotyczące rozszerzeń strony klienta

Rozszerzenie	Niedostępna opcja	Przyczyna
Szablony administracyjne	Zezwalaj na przetwarzanie poprzez wolne połączenie sieciowe	Zasady rejestrowe zostają zawsze zastosowane, ponieważ sterują pozostałymi rozszerzeniami.
Ustawienia zabezpieczenia	Zezwalaj na przetwarzanie poprzez wolne połączenie sieciowe	Ustawienia zabezpieczeń zawsze muszą być realizowane, nawet w przypadku wolnego połączenia
Przeadresowanie folderów	Nie stosuj podczas okresowego przetwarzania w tle	Użytkownik może używać folderów lub ich zawartości
Instalacja oprogramowania	Nie stosuj podczas okresowego przetwarzania w tle	Mogłaby zostać usunięta otwarta aplikacja

Na przetwarzanie zasad mają wpływ także kwestie nie związane z określonymi ustawieniami zasad i niewidoczne w interfejsie użytkownika. Do nich należą:

Komunikaty i zdarzenia

W momencie zastosowania Zasad grupowych zostaje wysłany komunikat WM_SETTINGCHANGE oraz sygnał zdarzenia. Aplikacje, których okna mogą otrzymać komunikaty, mogą zareagować na zmianę Zasad grupowych na podstawie otrzymanego komunikatu. Pozostałe aplikacje (w tym większość usług) mogą wykryć odpowiednie zdarzenie.

Przetwarzanie na żądanie

Aplikacje mogą zażądać zastosowania Zasad grupowych za pomocą funkcji RefreshPolicy. Aby odświeżyć zasady ręcznie, należy:

1. Kliknąć Uruchom (Run) w menu Start.
2. W celu odświeżenia zasad pod węzłem Konfiguracja komputera, wpisać:

   secedit /refreshpolicy MACHINE_POLICY [/enforce]

   W celu odświeżenia zasad pod węzłem Konfiguracja użytkownika, wpisać:

   secedit /refreshpolicy USER_POLICY [/enforce]
3. Kliknąć OK.

Opcjonalny parametr „/enforce” powoduje odświeżenie zasad zawartych w rozszerzeniach Ustawienia zabezpieczeń i EFS niezależnie od tego, czy nastąpiła zmiana zasad. Parametr ten nie wywiera żadnego wpływu na pozostałe rozszerzenia.

Limit czasu przetwarzania Zasad grupowych

Istnieje limit czasu (60 minut), przed upływem którego wszystkie rozszerzenia strony klienta powinny zakończyć przetwarzanie zasad. W przeciwnym przypadku rozszerzenie zostanie zatrzymane i jego ustawienia nie będą przetwarzane. Nie ma ustawienia Zasad grupowych zmieniającego domyślny limit czasu.

Zasady grupowe na komputerach autonomicznych

Aby ustawić Zasady grupowe lokalnie na komputerach nie należących do domeny, należy ustawić komputer lokalny jako fokus snap-in Zasady grupowe. Aby otworzyć snap-in, należy wysłać polecenie „MMC” i dodać snap-in Zasady grupowe do konsoli MMC.

Lokalny obiekt Zasad grupowych

Lokalne obiekty Zasad grupowych istniejące na komputerach autonomicznych obejmują tylko szablony Zasad grupowych. Lokalny obiekt Zasad grupowych znajduje się w folderze %SystemRoot%\System32\GroupPolicy. Każde rozszerzenie snap-in Zasady grupowe wysyła zapytanie do Zasad grupowych w celu ustalenia typu obiektu Zasad grupowych (lokalny czy oparty na Active Directory), a następnie ustala, czy powinno być wyświetlone w konsoli. Informacje o tym, które rozszerzenia snap-in Zasady grupowe zostają otwarte, są przedstawione w tabeli 22.6.

Tabela 22.6 Które rozszerzenia snap-in Zasady grupowe zostają załadowane

Rozszerzenie	Załadowane po wyborze lokalnego obiektu Zasad grupowych
Ustawienia zabezpieczeń	Tak
Szablony administracyjne	Tak
Instalacja oprogramowania	Nie
Skrypty	Tak
Konserwacja Internet Explorer	Tak
Usługi instalacji zdalnej	Nie
Przeadresowanie folderów	Nie

Uruchamianie Zasad grupowych w Windows 2000 Professional

Windows 2000 Professional nie zawiera wstępnie skonfigurowanej konsoli MMC dającej bezpośredni dostęp do nielokalnych Zasad grupowych (oprócz Ustawień zabezpieczeń, dostępnych w Panelu sterowania). Można jednak utworzyć niestandardową konsolę Zasad grupowych, stosując następującą procedurę:

Aby uruchomić snap-in Zasad grupowych w Windows 2000 Professional, należy:

1. Kliknąć Uruchom (Run), wpisać MMC i kliknąć OK.
2. W oknie MMC, w menu Konsola (Console), kliknąć Dodaj/usuń przystawkę (Add/Remove Snap-in).
3. Na zakładce Autonomiczny (Standalone) kliknąć Dodaj (Add).
4. W oknie dialogowym dodawania snap-in kliknąć Zasady grupowe (Group Policy) i kliknąć Dodaj (Add). Pojawi się okno dialogowe Wybieranie obiektu zasad grupowych (Select Group Policy object).
5. Kliknąć Komputer lokalny (Local Computer) w celu edycji lokalnego obiektu Zasad grupowych lub Przeglądaj (Browse) w celu odnalezienia innego obiektu Zasad grupowych.
6. Kliknąć Koniec (Finish).
7. Kliknąć OK. Snap-in zostanie otwarty wraz z określonym obiektem Zasad grupowych.

Uwaga: Aby zastosować snap-in Zasady grupowe do komputera zdalnego, należy posiadać uprawnienia umożliwiające użycie snap-in oraz prawa administracyjne na komputerze docelowym.

Stosowanie snap-in Zasad grupowych do komputera zdalnego

Obiekt Zasad grupowych wyświetlony jako węzeł główny konsoli Zasad grupowych jest nazywany „fokusem”. Fokusem konsoli może być lokalny obiekt Zasad grupowych dowolnego komputera lub dowolny obiekt Zasad grupowych oparty na Active Directory.

Uwaga: Fokus należy ustawić przy dodawaniu rozszerzenia do pliku konsoli MMC lub poprzez wysłanie odpowiedniego polecenia. Fokus nie może zostać zmieniony w czasie, gdy konsola Zasad grupowych jest otwarta.

Aby dodać Zasady grupowe do konsoli MMC, której fokusem jest określony komputer zdalny, należy:

1. Kliknąć Uruchom (Run) i wpisać MMC. Alternatywnie można otworzyć istniejącą zapisaną konsolę, taką jak Console1.mmc.
2. W oknie MMC, w menu Konsola (Console), kliknąć Dodaj/usuń przystawkę (Add/Remove Snap-in).
3. Na zakładce Autonomiczny (Standalone) kliknąć Dodaj (Add).
4. W oknie dialogowym kliknąć Zasady grupowe (Group Policy) i kliknąć Dodaj (Add). Domyślnie fokus jest ustawiony jako komputer lokalny.
5. Kliknąć Przeglądaj (Browse).
6. Wybrać zakładkę Komputer (Computer).
7. Wybrać Inny komputer (Another Computer).

8. Wpisać lub odnaleźć nazwę żądanego komputera.
9. Wybrać dostępne domeny z listy rozwijanej Szukaj w (Look in).

Wspierane są następujące formaty nazw komputerów:

- Nazwy NetBIOS, na przykład:

```
ThisComputer
```

- Nazwy w stylu DNS, na przykład:

```
ThisComputer.Reskit.com
```

Przy uruchamianiu snap-in Zasady grupowe z wiersza polecenia można zastosować następujące parametry:

- Aby określić komputer:

```
/gpcomputer:<nazwa_komputera>
```

Gdzie <nazwa_komputera> może być nazwą w stylu NetBIOS lub DNS.

Na przykład:

```
gpedit.msc /gpcomputer:" ThisComputer"
```

lub

```
gpedit.msc /gpcomputer:" ThisComputer.Reskit.com"
```

Należy zwrócić uwagę na brak spacji po:

```
/gpcomputer:
```

oraz na konieczność użycia cudzysłowu.

- Aby określić ścieżkę ADSI:

```
/gpobject:" <ścieżka ADSI>"
```

Na przykład:

```
/gpobject:" LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=Reskit,DC=com"
```

Aby umożliwić wykorzystanie tych parametrów w stosunku do zapisanego pliku konsoli, należy zaznaczyć opcję „Zezwalaj na zmianę fokusa przystawki zasad grup przy uruchamianiu z wiersza polecenia. Dotyczy tylko sytuacji, w których konsola została już zapisana. (Allow the focus of the Group Policy snap-in to be changed when launching from the command line. This only applies if you save the console)". W pliku Gpedit.msc dostarczonym wraz z Windows 2000 opcja ta jest włączona.

Uwaga: Rozszerzenie Ustawienia zabezpieczeń nie wspiera zdalnego zarządzania zasadami lokalnymi w Windows 2000.

Przetwarzanie lokalnego obiektu Zasad grupowych

Lokalny obiekt Zasad grupowych jest przetwarzany nawet w przypadku, gdy w domenie lub jednostce organizacyjnej włączono opcję Zablokuj dziedziczenie zasad.

Lokalne obiekty są przetwarzane przed nielokalnymi (opartymi na Active Directory). W przypadku konfliktu pierwszeństwo mają zasady nielokalne. Jeśli komputer zostanie wycofany z domeny, to lokalne ustawienia zasad wciąż obowiązują i nie mogą już zostać zastąpione.

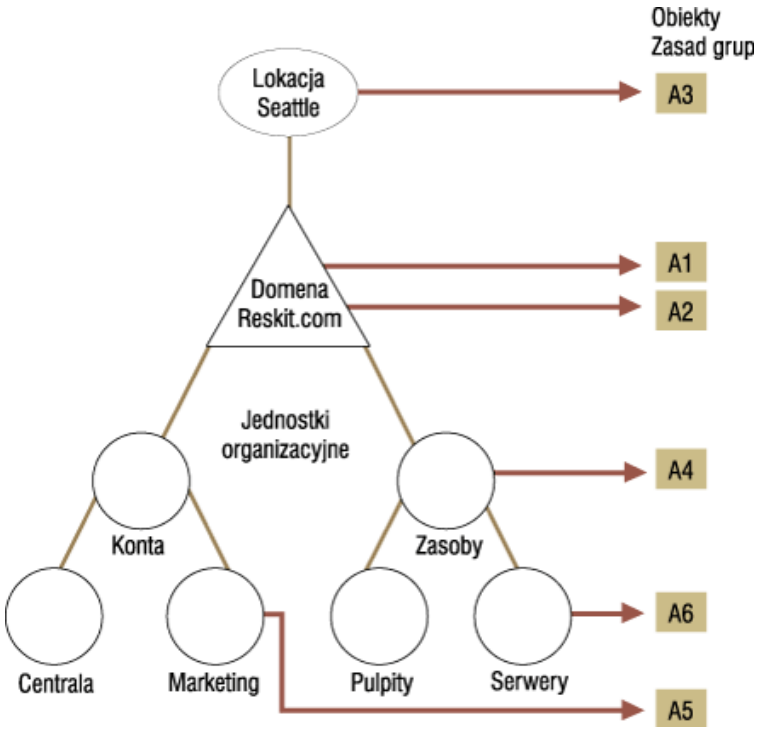
Jeśli obiekty Konta komputera i Konta użytkownika są zarządzane przez kontrolery domeny Windows NT 4.0, a więc nie są zawarte w Active Directory, to żaden lokalny obiekt Zasad grupowych nie zostanie przetworzony. Inne kwestie związane z migracją są omówione dalej w tym rozdziale pod hasłem „Kwestie dotyczące migracji i Zasad grupowych".

Wsparcie sprzężenia zwrotnego w Zasadach grupowych

Sposób, w jaki Zasady grupowe są zastosowane wobec użytkownika lub komputera zależy od położenia obiektu użytkownika lub komputera w Active Directory. Jednak w niektórych przypadkach żądane jest zastosowanie zasad wobec użytkownika w sposób zależny wyłącznie od położenia obiektu komputera. Jest to możliwe dzięki funkcji Zasad grupowych zwanej sprzężeniem zwrotnym.

Uwaga: Sprzężenie zwrotne jest wspierane tylko w środowisku opartym wyłącznie na Windows 2000. Konta komputera i konto użytkownika muszą należeć do Active Directory, nie do kontrolera domeny Windows NT 4.0. Komputer kliencki musi być oparty na Windows 2000.

Sprzężenie zwrotne jest opisane w poniższym przykładzie. W tym scenariuszu zakłada się, że administrator posiada uprawnienia administratora domeny dające pełną kontrolę nad komputerami i użytkownikami należącymi do danej domeny (Reskit). Domena Reskit przedstawiona jest na rysunku 22.7.



Rysunek 22.7 Domena Reskit

Użytkownicy pracujący na własnych stacjach roboczych powinni podlegać Zasadom grupowym ustawionym w oparciu o położenie obiektu użytkownika. Natomiast użytkownicy logujący się na komputerze, którego obiekt komputera należy do jednostki organizacyjnej Serwery, powinni podlegać zasadom użytkownika opartym na położeniu obiektu komputera, nie na położeniu obiektu użytkownika.

Na rysunku 22.8, zgodnie z normalnym przetwarzaniem Zasad grupowych, do komputerów należących do jednostki organizacyjnej Serwery zostają zastosowane obiekty Zasad grupowych A3, A1, A2, A4 i A6, w tej kolejności, podczas uruchamiania komputera. Wobec użytkowników należących do jednostki organizacyjnej Marketing zastosowane są obiekty A3, A1, A2 i A5, w tej kolejności, niezależnie od użytkowanego komputera.

W niektórych przypadkach powyższa metoda przetwarzania może być nieodpowiednia, na przykład, gdy aplikacje przypisane lub opublikowane dla użytkowników w jednostce Marketing nie powinny zostać zainstalowane na komputerach należących do jednostki organizacyjnej Serwery. Sprzężenie zwrotne umożliwia określenie dwóch kolejnych sposobów pobrania listy obiektów Zasad grupowych dla użytkownika pracującego na komputerach jednostki Serwery. Zastosować można tryb scalania lub tryb zastępowania.

Tryb scalania

W tym trybie, po zalogowaniu użytkownika lista jego obiektów Zasad grupowych zostaje pobrana normalnie za pomocą funkcji GetGPOList, anastępnie GetGPOList zostaje wywołana ponownie przy użyciu położenia komputera w Active Directory. Lista obiektów odpowiadających położeniu komputera zostaje dołączona do końca listy obiektów użytkownika. Oznacza to, że obiekty komputera mają wyższy priorytet niż obiekty użytkownika. W tym przykładzie powstanie lista: A3, A1, A2, A5, A3, A1, A2, A4, A6 (obiekty występujące na końcu listy posiadają najwyższy priorytet).

Tryb zastępowania

W tym trybie lista obiektów użytkownika nie zostaje pobrana. Stosuje się tylko listę obiektów Zasad grupowych opartą na obiekcie komputera. Na rysunku 22.7 powstaje lista: A3, A1, A2, A4, A6.

Funkcja sprzężenia zwrotnego jest realizowana w aparacie Zasad grupowych, nie w funkcji GetGPOList. Przed zastosowaniem zasad użytkownika aparat przeszukuje rejestr w celu ustalenia, czy istnieje ustawienie zasad komputera określające tryb zastosowania zasad użytkownika. Następnie, na podstawie tego ustawienia, aparat wywołuje w odpowiedni sposób funkcję GetGPOList.

Wsparcie klientów Windows NT 4.0, Windows 95 i Windows 98

Zasady grupowe Windows 2000 nie wspierają klientów opartych na Windows NT 4.0, Windows 95 i Windows 98, pomimo że te wersje Windows są wspierane przez Active Directory.

W przypadku klientów Windows NT 4.0 należy zastosować szablony administracyjne w stylu Windows NT 4.0 (pliki .adm) i pliki Edytora zasad systemowych Windows NT 4.0 (Poledit.exe).

Do zarządzania klientami Windows 95 i Windows 98, należy użyć Edytora zasad systemowych.

W przypadku komputerów klienckich posiadających Windows NT 4.0, Windows 95 lub Windows 98 plik .pol (Config.pol w Windows 95/98, Ntconfig.pol w Windows NT 4.0) utworzony w systemie operacyjnym klienta musi zostać skopiowany do dzierżawy Netlogon domeny (%systemroot%\SYSVOL\sysvol\<nazwa domeny>\SCRIPTS w Windows 2000, %systemroot%\winnt\system32\Repl\Import\Scripts w Windows NT 4.0).

Informacje o instalacji Edytora zasad systemowych znajdują się w Pomocy Windows 2000 Server. Edytor jest zawarty w Windows 2000 Server, nie w Windows 2000 Professional. Edytor zasad systemowych jest zawarty w opcjonalnym pakiecie narzędzi administracyjnych Windows 2000 (Adminpak.msi), który znajduje się na CD-ROM Windows 2000 Server i może zostać zainstalowany na komputerach Windows 2000 Professional.

Użytkowanie szablonów administracyjnych Windows NT 4.0 w konsoli Zasad grupowych Windows 2000

Ustawienie Pokaż tylko zasady (Show Policies Only), w menu Widok (View) w konsoli Zasad grupowych, jest domyślnie włączone. Uniemożliwia ono dostarczenie przestrzeni nazw przez szablony administracyjne Windows NT 4.0. Jest to bezpieczne, ponieważ z punktu widzenia administratora Windows 2000 zasady Windows NT 4.0, oparte na rejestrze, są nadmiernie trwałe. Jeśli opcja Pokaż tylko zasady zostanie wyłączona, to prawdziwe ustawienia Zasad grupowych będą wyświetlane w kolorze niebieskim, a ustawienia Zasad systemowych w czerwonym. Po kolejnym uruchomieniu snap-in ustawienia „obce” zostaną ponownie ukryte.

Zalecane jest zastosowanie ustawienia wymuszającego włączenie opcji Pokaż tylko zasady (pod: Konfiguracja użytkownika/Szablony administracyjne/System/Zasady grupowe) w przypadkach, gdy zadania administracyjne Zasad grupowych są delegowane za pomocą niestandardowych konsol. W ten sposób użytkownicy konsol nie mogą wyłączyć opcji Pokaż tylko zasady.

Kwestie dotyczące Zasad grupowych i migracji

W organizacjach posiadających wiele sieciowych komputerów Windows NT 4.0, w tym: główne i zapasowe kontrolery domen, autonomiczne serwery klienckie oraz klienckie stacje robocze, jednoczesne uaktualnienie wszystkich komputerów do Windows 2000 może być niepraktyczne. Przy uaktualnianiu sieci opartej na Windows NT 4.0 do Windows 2000 należy wiedzieć czego się spodziewać podczas procesu migracji i po jego ukończeniu.

Podczas migracji konieczne może być zarządzanie domeną zawierającą wszystkie następujące rodzaje komputerów:

- Kontrolery domen Windows 2000 Server
- Kontrolery domen Windows NT 4.0 Server
- Klienci Windows 2000 Professional
- Klienci Windows 2000 Server
- Klienci Windows NT 4.0 Workstation
- Klienci Windows NT 4.0 Server
- Komputery posiadające wcześniejsze wersje Windows, takie jak Windows 98

Istnieje wiele typów interakcji do rozważenia, ale warunki po stronie klienta nie są zbyt skomplikowane.

Strona klienta

Zasady grupowe są wspierane tylko na komputerach Windows 2000. Klienci Windows NT 4.0 otrzymują Zasady systemowe administrowane poprzez Edytor zasad systemowych (Poledit.exe). Komputerami Windows 95/98 zarządza się przy użyciu kompatybilnych z tymi systemami wersji Zasad systemowych. Plik .pol utworzony w programie Poledit.exe może być zastosowany tylko na komputerach, których system operacyjny odpowiada systemowi, w którym plik .pol utworzono. Komputery Windows NT nie mogą wykorzystać pliku Config.pol (pochodzącego z Zasad systemowych Windows 95/98), a komputery Windows 98 lub Windows 95 nie mogą wykorzystać pliku NTConfig.pol (pochodzącego z Zasad systemowych Windows NT).

Strona kontrolera domeny

W tej części opisana jest interakcja Zasad systemowych Windows NT 4.0 z Zasadami grupowymi Windows 2000, podczas migracji. Zakłada się, że wszystkie komputery klienckie (komputery inne niż kontrolery domen) posiadają Windows 2000 Professional lub Windows 2000 Server, chyba że określono inaczej.

Aby użytkownik mógł zalogować się w domenie, użytkownik oraz komputer muszą być znani w domenie. Należy zrozumieć zachowanie obserwowane w przypadku, gdy jedno lub oba konta nie zostały jeszcze uaktualnione z Windows NT 4.0 do Windows 2000.

Konta komputera i użytkownika na kontrolerach domeny Windows NT 4.0

Konta mogą znajdować się na tym samym kontrolerze domeny lub na różnych kontrolerach. W sieci mogą także istnieć kontrolery domen Windows 2000, ale nie obsługujące danych kont. Użytkownik i komputer nie należą do Active Directory.

Uruchamianie systemu

Przy uruchamianiu komputera zostają zastosowane lokalne Zasady grupowe dotyczące komputera.

Logowanie użytkownika

Przy logowaniu użytkownika zostają zastosowane Zasady systemowe Windows NT 4.0 (w pierwszej kolejności zasady dotyczące komputera, a następnie dotyczące użytkownika). Następnie, jeśli lokalne Zasady grupowe zmieniły się od momentu ich ostatniego zastosowania, to zostaną zastosowane lokalne Zasady grupowe dotyczące użytkownika, a następnie Zasady systemowe Windows NT 4.0 dotyczące użytkownika.

Konta komputera i użytkownika na kontrolerach domeny

Windows 2000

W tym przypadku oba konta należą do Active Directory. Sieć może zawierać także kontrolery domeny Windows NT 4.0, ale nie biorą one udziału w negocjacjach przy uruchamianiu/logowaniu, ponieważ klienci Windows 2000 preferują kontrolery domeny Windows 2000.

Uruchamianie systemu

W momencie rozruchu zostają zastosowane Zasady grupowe Windows 2000 dotyczące komputera.

Logowanie użytkownika

Przy logowaniu zostają zastosowane Zasady grupowe Windows 2000 dotyczące użytkownika.

Windows NT 4.0 zarządza kontem komputera, a Windows 2000 zarządza kontem użytkownika

W tym przypadku konto użytkownika należy do Active Directory, natomiast konto komputera nie należy do Active Directory i jest zarządzane przez kontroler domeny Windows NT 4.0. Jest to często spotykany scenariusz.

Uruchamianie systemu

Przy uruchamianiu zostają zastosowane lokalne Zasady grupowe dotyczące komputera.

Logowanie użytkownika

Przy logowaniu użytkownika komputer otrzymuje Zasady systemowe, a następnie użytkownik otrzymuje wszystkie odpowiednie Zasady grupowe. Użytkownik nie otrzymuje Zasad systemowych.

Uaktualnianie kont komputerów

Podczas uaktualniania kont komputerów z Windows NT 4.0 do Windows 2000 mogą powstać kwestie związane z trwałością ustawień. Istniejące ustawienia Zasad systemowych nie są usuwane z rejestru klienta przy uaktualnianiu kontrolera domeny. Należy poszukać niepożądanych wpisów pozostających po Zasadach systemowych i podjąć kroki naprawcze, takie jak usunięcie starych ustawień za pomocą programu Regini.exe (znajdującego się w folderze %systemroot%/System32/).

Przykładowo, zasady dotyczące nagłówka logowania są traktowane w inny sposób w Windows 2000 niż w Windows NT 4.0 (pod węzłem Ustawienia zabezpieczeń zamiast w szablonie administracyjnym). Jeśli po uaktualnieniu konta komputera okaże się, że zasady nagłówka logowania Windows NT 4.0 są wciąż stosowane, to należy jednorazowo zmienić odpowiednie ustawienie.

Zaleca się unikać tego typu problemów przeprowadzając czystą instalację systemu operacyjnego Windows 2000, zamiast uaktualnienia Windows NT 4.0.

Windows NT 4.0 zarządza kontem użytkownika, a Windows 2000 zarządza kontem komputera

W tym przypadku konto komputera, a nie konto użytkownika, należy do Active Directory. Kontem użytkownika zarządza kontroler domeny Windows NT 4.0.

Podczas migracji do Windows 2000, domeny zasobów Windows NT 4.0 (które często zawierają konta komputerów, drukarki, foldery udostępnione itp.) są często przekształcane w jednostki organizacyjne Active Directory. W ten sposób kilka domen zasobów Windows NT 4.0 może być połączonych w jedną domenę Windows 2000. Zazwyczaj, uaktualnienie domen zasobów w ten sposób wymaga mniejszej ilości komputerów niż uaktualnienie wszystkich kont użytkowników, dlatego omawiany scenariusz jest rzadziej spotykany niż poprzedni.

Uruchamianie systemu

Wszystkie Zasady grupowe dotyczące komputera są zastosowane do komputera przy jego uruchamianiu.

Logowanie użytkownika

Przy logowaniu użytkownika zastosowane zostają Zasady systemowe dotyczące użytkownika. Jeśli lokalny obiekt Zasad grupowych został zmieniony od momentu jego ostatniego zastosowania, to zastosowane zostają lokalne Zasady grupowe dotyczące użytkownika, a następnie Zasady systemowe Windows NT 4.0 dotyczące użytkownika. Zasady systemowe dotyczące komputera nie są zastosowane.

Uaktualnianie kont użytkowników

Gdy kontami użytkowników zarządzał kontroler domeny Windows NT 4.0, to rejestry komputerów klienckich mogły być zmieniane w częściach znajdujących się poza aprobowanymi drzewami Zasad grupowych. Po uaktualnieniu kontrolera domeny zawierającego konta użytkowników do Windows 2000, ustawienia pozostaną na klientach, chyba że administrator wycofa je za pomocą Zasad systemowych. Łatwiejsze jest przeprowadzenie czystych instalacji Windows 2000.

Relacje zaufania z wcześniejszymi wersjami Windows

Istnieje subtelna kwestia związana ze sposobem traktowania zaufania w Windows NT 4.0, którą należy wziąć pod uwagę podczas uaktualniania do Windows 2000.

Załóżmy, że istnieje relacja zaufania pomiędzy kontrolerem domeny Windows 2000 (kontroler A) a kontrolerem domeny Windows NT 4.0 (B). Komputer B zostaje uaktualniony do Windows 2000, a następnie jednostka organizacyjna zarządzana przez a zostaje połączona z obiektem Zasad grupowych przechowywanym w domenie B. Użytkownik należący do tej jednostki organizacyjnej loguje się na a oczekując otrzymania ustawień od obiektu Zasad grupowych przechowywanego w domenie B — ale oczekiwany efekt nie następuje. Przyczyną jest fakt, iż podczas uaktualniania kontrolera domeny relacja zaufania nie podlega automatycznemu uaktualnieniu, a użytkownik nie będzie mieć dostępu do dzierżawy Sysvol na komputerze B.

Aby rozwiązać ten problem, należy usunąć relację zaufania po uaktualnieniu komputera B do Windows 2000, a następnie utworzyć nową relację zaufania w stylu Windows 2000.

Zalecane metody

Użycie Zasad grupowych zamiast Zasad systemowych Windows NT 4.0

Zasady systemowe są nadmiernie trwałe z perspektywy Windows 2000. Zasady grupowe są odświeżane po każdej zmianie zasad.

Wyłączenie nieużywanych części obiektu Zasad grupowych

Jeśli wszystkie ustawienia pod węzłem Konfiguracja użytkownika lub pod węzłem Konfiguracja komputera są Nie skonfigurowane (Not Configured), to należy ten węzeł wyłączyć, w celu przyspieszenia procesu uruchamiania komputera lub logowania użytkownika.

Jeśli wyłączone są obie części obiektu Zasad grupowych, to będzie on funkcjonować tak, jak gdyby nie był połączony z żadną lokacją, domeną ani jednostką organizacyjną, pomimo że łącza wciąż istnieją.

Ograniczenie stosowania opcji Zablokuj dziedziczenie zasad (Block Policy Inheritance) i Nie zastępuj (No Override)

Regularne stosowanie tych funkcji utrudnia rozwiązywanie problemów związanych z zasadami.

Minimalizacja liczby obiektów Zasad grupowych powiązanych z użytkownikami w domenach lub jednostkach organizacyjnych

Im więcej obiektów Zasad grupowych powiązanych z użytkownikiem, tym dłużej będzie trwać proces logowania.

Filtrowanie zasad w oparciu o przynależność do grup zabezpieczenia

Należy pamiętać, że obiekt Zasad grupowych nie będzie dotyczyć użytkownika, jeśli wpisy

kontroli dostępu (ACE) nie są ustawione na Zezwalaj (Allow) w stosunku do grup zabezpieczenia, do których użytkownik należy. Mechanizm ten ma na celu uniknięcie zastosowania zasad wobec użytkowników (lub komputerów), którzy normalnie podlegaliby im z powodu łączy lub dziedziczenia. Jest to skuteczny mechanizm, który powinien być maksymalnie wykorzystany w celu przyspieszenia logowania użytkowników i uruchamiania komputerów.

Ograniczenie zastępowania zasad dotyczących użytkownika zasadami dotyczącymi komputera

Zasady należy zastąpić tylko w przypadku, gdy konfiguracja pulpitu musi być stała niezależnie od logującego się użytkownika.

Uniknięcie stosowania obiektów Zasad grupowych przechowywanych w innej domenie

Przetwarzanie obiektów Zasad grupowych z innych domen zwiększa czas logowania lub uruchamiania.

Zasoby dodatkowe

- Najnowsze informacje o Zasadach grupowych w Windows 2000 Server znajdują się pod odsyłaczami do Microsoft Windows 2000 Server i do ResourceLink na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.
- Więcej informacji o ustawieniach szablonów administracyjnych dołączonych do Windows 2000 Server znajduje się w pliku informacyjnym GP.chm na CD-ROM Windows 2000 Server Resource Kit.
- Więcej informacji o API Zasad grupowych znajduje się w Microsoft Windows 2000 Platform Software Development Kit oraz pod odsyłaczem do Microsoft Platform SDK na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.
- Informacje o MMC znajdują się w Microsoft Windows 2000 Platform Software Development Kit.
- Praktyczne przykłady Zasad grupowych znajdują się pod odsyłaczem do Windows 2000 Management Services na stronie http://www.microsoft.com/windows2000/techinfo/reskit/default.asp.