

Zasady grupy - omówienie

Przystawki **Zasady grupy** można użyć do definiowania ustawień **zasad**, które są stosowane do komputerów lub użytkowników.

Zasady grupy - Infrastruktura w katalogu usługi Active Directory, która, wykorzystując katalog, umożliwia zarządzanie konfiguracją i zmianami ustawień użytkowników i komputerów, w tym informacjami o zabezpieczeniach i użytkownikach. Zasady grupy można wykorzystywać do definiowania konfiguracji dla grup użytkowników i komputerów. Poprzez Zasady grupy można określić ustawienia zasad dla zasad opartych na rejestrze, zabezpieczeń, instalacji oprogramowania, skryptów, przekierowania folderów, usług instalacji zdalnej i obsługi programu Internet Explorer. Utworzone ustawienia zasad grupy są zawarte w obiekcie zasad grupy (GPO). Przez skojarzenie obiektu GPO z wybranymi kontenerami usługi Active Directory (witrynami, domenami i jednostkami organizacyjnymi) można zastosować ustawienia zasad obiektu GPO do użytkowników i komputerów w tych kontenerach usługi Active Directory. W celu utworzenia pojedynczego obiektu GPO należy użyć Edytora obiektów zasad grupy. W celu zarządzania obiektami zasad grupy w całym zrzeczeniu można użyć konsoli zarządzania zasadami grupy.

Omówienie przystawki Zasady grupy

Ustawienia Zasady grupy określają różne składniki środowiska pulpitu użytkownika, którymi musi zarządzać administrator systemu, na przykład programy, które są dostępne dla użytkowników, programy, które pojawiają się na pulpicie użytkownika i opcje dla menu **Start**. Aby utworzyć specyficzną konfigurację pulpitu dotyczącą konkretnej grupy użytkowników, należy użyć **Edytora obiektów zasad grupy**. Ustawienia przystawki **Zasady grupy** określone przez użytkownika znajdują się w **obiekcie zasad grupy**, który jest skojarzony z wybranymi obiektami usługi **Active Directory**®—**lokacjami**, **domenami** lub **jednostkami organizacyjnymi**.

Zasady grupy mają zastosowanie nie tylko do użytkowników i komputerów klienckich, ale również do serwerów członkowskich, kontrolerów domen i do wszystkich innych komputerów z systemem Microsoft®

Windows® znajdujących się w zakresie zarządzania. Domyślnie zasady grupy, które stosuje się do domeny (co oznacza, że są stosowane na poziomie domeny, powyżej katalogu głównego przystawki **Użytkownicy i komputery usługi Active Directory**), dotyczą wszystkich komputerów i użytkowników w domenie. Przystawka Użytkownicy i komputery usługi Active Directory ma również wbudowaną jednostkę organizacyjną Kontrolery domeny. Jeśli konta kontrolerów domeny są przechowywane w tym miejscu, można wykorzystać obiekt zasad grupy Domyślne kontrolery domeny do zarządzania kontrolerami domeny niezależnie od innych komputerów.

Przystawka Zasady grupy obejmuje ustawienia **Konfiguracja użytkownika**, które dotyczą użytkowników, oraz ustawienia **Konfiguracja komputera**, które dotyczą komputerów.

Przy użyciu przystawki Zasady grupy można wykonywać następujące czynności:

- **Zarządzać zasadami opartymi na rejestrze, za pomocą Szablonów administracyjnych.** Przystawka Zasady grupy tworzy plik zawierający ustawienia rejestru, które są zapisywane w części „User” lub „Local Machine” bazy danych rejestru. Ustawienia profilu użytkownika właściwe dla użytkownika, który loguje się do danej stacji roboczej lub serwera, są zapisywane w rejestrze w kluczu **HKEY_CURRENT_USER** (HKCU), a ustawienia właściwe dla komputera są zapisywane w kluczu **HKEY_LOCAL_MACHINE** (HKLM).
- **Przypisywać skrypty.** W tym takie skrypty, jak uruchamianie komputera, zamykanie komputera oraz operacje logowania i wylogowania.

- **Przekierowywać foldery.** Można przekierowywać foldery, takie jak Dokumenty, Obrazy inne, z folderu Użytkownicy na komputerze lokalnym do lokalizacji sieciowych.
- **Zarządzać aplikacjami.** Używając rozszerzenia Instalacja oprogramowania przystawki Zasady grupy, można przypisywać, publikować, aktualizować lub naprawiać aplikacje.
- **Określać opcje zabezpieczeń.**

Obiekty zasad grupy, które istnieją domyślnie

Każdy komputer z systemem operacyjnym Windows NT ma dokładnie jeden obiekt zasad grupy, który jest przechowywany lokalnie. Ten obiekt zasad grupy zawiera podzbiór ustawień, które są dostępne w nielokalnych obiektach zasad grupy.

Domyślnie po skonfigurowaniu usługi Active Directory tworzone są dwa nielocalne obiekty zasad grupy:

- Obiekt **Domyślne zasady domeny (Default Domain Policy)** jest połączony z domeną i dotyczy wszystkich użytkowników oraz komputerów w domenie (w tym komputerów, które są kontrolerami domeny) przez **dziedzicznie zasad**.
- Obiekt **Domyślne zasady kontrolerów domeny (Default Domain Controllers Policy)** jest połączony z jednostką organizacyjną Kontrolery domeny i dotyczy zasadniczo tylko kontrolerów domeny, ponieważ konta komputerów dla kontrolerów domeny są przechowywane wyłącznie w jednostce organizacyjnej Kontrolery domeny.

Przestroga

Po przeniesieniu kontrolera domeny poza jednostkę organizacyjną Kontrolery domeny nie będzie już stosowana domyślna zasada kontrolerów domen. Jeśli konieczne jest pozostawienie kontrolera domeny w innej jednostce organizacyjnej, należy połączyć domyślną zasadę kontrolerów domeny z tą jednostką organizacyjną.

Jak i kiedy są stosowane zasady grupy

Aby wyświetlić szczegółową chronologię stosowania zasad, zobacz kolejność zdarzeń podczas uruchamiania komputera i logowania.

Następująca sekwencja zdarzeń pokazuje, w jakiej kolejności stosowane są zasady komputera i zasady użytkownika, gdy komputer jest uruchamiany i gdy użytkownik loguje się:

1. Uruchamiana jest sieć. Uruchamiane są usługi Remote Procedure Call System Service (RPCSS) oraz Multiple Universal Naming Convention Provider (MUP).
2. Dla komputera jest pobierana uporządkowana lista obiektów zasad grupy. Lista może być zależna od następujących czynników:
 - Od tego, czy komputer jest częścią domeny i dlatego podlega ustawieniom Zasady grupy za pośrednictwem usługi Active Directory.
 - Od lokalizacji komputera w usłudze Active Directory.
 - Od tego, czy lista obiektów zasad grupy uległa zmianie. Jeśli lista obiektów zasad grupy nie uległa zmianie, nie jest przeprowadzane żadne przetwarzanie. Można użyć ustawienia zasad, aby zmienić to zachowanie.
3. Stosowane są zasady komputera. Są to ustawienia znajdujące się w folderze Konfiguracja komputera, pobrane z przygotowanej listy. Domyślnie jest to proces synchroniczny, a czynności są wykonywane w następującej

- kolejności: komputer lokalny, lokacja, domena, jednostka organizacyjna, podrzędna jednostka organizacyjna itd. Podczas przetwarzania zasad komputera nie jest wyświetlany żaden interfejs użytkownika.
4. Uruchamiane są skrypty uruchamiania komputera. Domyślnie odbywa się to w sposób ukryty i synchroniczny; wykonywanie każdego skryptu musi zostać zakończone lub musi dla niego upłynąć limit czasu, aby uruchomiony został następny skrypt. Domyślny limit czasu wynosi 600 sekund. Aby zmodyfikować to zachowanie, można użyć kilku ustawień zasad.
 5. Użytkownik naciska klawisze CTRL-ALT-DEL, aby się zalogować.
 6. Po uwierzytelnieniu użytkownika ładowany jest profil użytkownika; profil jest określony przez obowiązujące ustawienia zasad.
 7. Dla użytkownika uzyskiwana jest uporządkowana lista obiektów zasad grupy. Lista ta może być zależna od następujących czynników:
 - Od tego, czy użytkownik jest częścią domeny i dlatego podlega ustawieniom Zasady grupy za pośrednictwem usługi Active Directory.
 - Od tego, czy jest włączone sprzężenie zwrotne i od stanu (Scal lub Zamień) ustawienia zasad sprzężenia zwrotnego.
 - Od lokalizacji użytkownika w usłudze Active Directory.
 - Od tego, czy lista obiektów zasad grupy uległa zmianie. Jeśli lista obiektów zasad grupy nie uległa zmianie, nie jest przeprowadzane żadne przetwarzanie. Można użyć ustawienia zasad, aby zmienić to zachowanie.
 8. Stosowane są zasady użytkownika. Są to ustawienia znajdujące się w folderze Konfiguracja użytkownika, pobrane z przygotowanej listy. Domyślnie jest to proces synchroniczny, a czynności są wykonywane w następującej kolejności: komputer lokalny, lokacja, domena, jednostka organizacyjna, podrzędna jednostka organizacyjna itd. Podczas przetwarzania zasad użytkownika nie jest wyświetlany żaden interfejs użytkownika.
 9. Uruchamiane są skrypty logowania. W odróżnieniu od skryptów systemu Windows NT 4.0, skrypty logowania oparte na zasadach grupy są domyślnie uruchamiane w sposób ukryty i asynchroniczny. Skrypt obiektu użytkownika jest uruchamiany jako ostatni w normalnym oknie.
 10. Pojawia się interfejs użytkownika systemu operacyjnego, opisany przez Zasady grupy.

Uwagi

Niektóre z tych zdarzeń można modyfikować. Można ustawić zasady, aby:

- Odwrócić domyślne ustawienia synchronicznego lub asynchronicznego uruchamiania skryptów i stosowania zasad.
- Określić limity czasu dla skryptów. Domyślnie limit czasu dla skryptów wynosi 600 sekund.
- Zmienić sposób uruchamiania skryptów, które mogą być uruchamiane jako ukryte, zminimalizowane lub w normalnym oknie.

Zasady użytkownika i komputera

Ustawienia zasad użytkownika są zlokalizowane w Zasadach grupy, w obszarze Konfiguracja użytkownika, a są one uzyskiwane, gdy użytkownik się loguje. Ustawienia zasad komputera są zlokalizowane w Zasadach grupy, w obszarze Konfiguracja komputera, a są one uzyskiwane podczas uruchamiania komputera.

Użytkownicy i Komputery to jedyne typy obiektów usługi Active Directory, których dotyczą zasady.

W szczególności zasady nie stosują się do grup zabezpieczeń. Zamiast tego, ze względu na wydajność, grupy zabezpieczeń są używane do filtrowania zasad za pomocą **wpisu kontroli dostępu**, który może zostać ustawiony na wartość **Zezwalaj** lub **Odmawiaj** albo pozostać nieskonfigurowany.

Kolejność stosowania

Zasady są stosowane w następującej kolejności:

1. Unikatowy lokalny obiekt zasad grupy.
2. Obiekty zasad grupy lokacji w kolejności określonej administracyjnie.
3. Obiekty zasad grupy domeny w kolejności określonej administracyjnie.
4. Obiekty zasad grupy jednostek organizacyjnych od największej do najmniejszej jednostki organizacyjnej (od nadrzędnej do podrzędnej jednostki organizacyjnej) i w kolejności określonej administracyjnie na poziomie każdej jednostki organizacyjnej.

Domyślnie zasady zastosowane później zastępują zasady zastosowane wcześniej, jeśli zasady te są niezgodne. Jeśli jednak zasady są zgodne, zarówno wcześniejsze, jak i późniejsze zasady składają się na zasadę efektywną.

Filtrowanie zasad na podstawie przynależności do grupy zabezpieczeń

Wpis ACE grupy zabezpieczeń w obiekcie zasad grupy może zostać ustawiony na wartość **Nieskonfigurowane** (brak uprzywilejowania), **Dopuszczalny** lub **Odmowa**. Wartość **Odmowa** ma pierwszeństwo przed wartością **Dopuszczalny**.

Blokowanie dziedziczenia zasad

Zasady, które byłyby dziedziczone od wyższych w hierarchii lokacji, domen lub jednostek organizacyjnych, mogą zostać zablokowane na poziomie lokacji, domeny lub jednostki organizacyjnej.

Wymuszanie stosowania zasad obiektów znajdujących się wyżej w hierarchii

Dla zasad, które byłyby zastępowane przez zasady w podrzędnych jednostkach organizacyjnych, można ustawić opcję **Nie zastępuj** na poziomie obiektu zasad grupy.

Uwagi

- Zasady ustawione na wartość **Nie zastępuj** nie mogą zostać zablokowane.
- Opcje **Nie zastępuj** i **Zablokuj** powinny być używane rzadko. Nierozważne użycie tych zaawansowanych opcji może utrudnić rozwiązywanie problemów.