Grupa zasad	Zasada	Ustawienie zabezpieczeń	Opis
Zasady blokady konta	Czas trwania blkoady konta	15	Liczba minut, przez które konto pozostaje zablokowane po zablokowaniu, zanim nie zostanie automatycznie odblokowane. Jeśli zdefiniowano próg blokady konta, czas blokady konta musi być większy lub równy czasowi resetowania.
Zasady blokady konta	Próg blokady konta	10	Liczba nieudanych prób logowania, które powodują zablokowanie konta użytkownika. Zablokowanego konta nie można używać, dopóki nie zostanie zresetowane przez administratora lub dopóki nie upłynie czas blokady konta.
Zasady blokady konta	Wyzerowanie blokady konta po	15	Liczba minut, które muszą upłynąć po nieudanej próbie zalogowania, zanim licznik nieudanych prób logowania nie zostanie zresetowany do 0.
Zasady haseł	Wymuszaj tworzenie historii hasła	24	Liczba unikatowych nowych haseł, które należy powiązać z kontem użytkownika, aby można było ponownie użyć starego hasła.
Zasady haseł	Minimalna długość hasła	14	Najmniejsza liczba znaków, które musi zawierać hasło konta użytkownika.
Zasady haseł	Hasło musi spełniać wymagania co do złożoności	Enabled	Określa, czy hasła muszą spełniać wymagania dotyczące złożoności: 1) Nie może zawierać wartości samAccountName użytkownika (nazwa konta) ani całej wartości displayName (wartość pełnej nazwy). Żadna z kontroli nie rozróżnia wielkości liter. Nazwa samAccountName jest sprawdzana w całości tylko w celu ustalenia, czy jest częścią hasła. Jeśli nazwa samAccountName ma mniej niż trzy znaki, to sprawdzenie jest pomijane. DisplayName jest analizowany dla ograniczników: przecinków, kropek, myślników lub łączników, podkreślników, spacji, znaków funta i tabulatorów. Jeśli którykolwiek z tych ograniczników zostanie znaleziony, displayName zostanie podzielony, a wszystkie przeanalizowane sekcje (tokeny) nie zostaną uwzględnione w haśle. Tokeny o długości mniejszej niż trzy znaki są ignorowane, a podciągi nie są sprawdzane. Na przykład nazwa „Erin M. Hagens" jest podzielona na trzy tokeny: „Erin", „M" i „Hagens". Ponieważ drugi żeton ma tylko jedną postać, jest ignorowany. Dlatego ten użytkownik nie może mieć hasła zawierającego „erin" lub „hagens" jako podciąg w dowolnym miejscu hasła. 2) Zawierają znaki z trzech następujących kategorii: - Wielkie litery języków europejskich (od A do D12 znaki diakrytyczne, znaki greckie i cyrylicy) - Małe litery języków europejskich (od a do z, ostre-s, ze znakami diakrytycznymi, znakami greckimi i cyrylicy) - Cyfry (od 0 do 9) - Znaki niealfanumeryczne (znaki specjalne): (~!@#$%^&*_-+=`\(){}[]:;"'<>,.?/) Symbole walut, takie jak euro lub funt brytyjski, nie nie mogą być używane. Dowolny znak Unicode, który jest sklasyfikowany jako znak alfabetyczny, ale nie jest pisany wielkimi lub małymi literami. Obejmuje to znaki Unicode z języków azjatyckich.
Zasady haseł	Zapisz hasło korzystając z szyfrowania odwracalnego	Disabled	Określa, czy system operacyjny przechowuje hasła przy użyciu szyfrowania odwracalnego.
Opcje zabezpieczeń	Konta: ogranicz używanie pustych haseł przez konta lokalne tylko do logowania do konsoli	Enabled	To ustawienie zabezpieczeń określa, czy konta lokalne, które nie są chronione hasłem, mogą być używane do logowania z lokalizacji innych niż fizyczna konsola komputera. Jeśli ta opcja jest włączona, konta lokalne, które nie są chronione hasłem, będą mogły logować się tylko na klawiaturze komputera.
Opcje zabezpieczeń	Inspekcja: Wymuś ustawienia podkategorii zasad inspekcji (Windows Vista lub nowszy), aby zastąpić ustawienia kategorii zasad inspekcji	Enabled	System Windows Vista i nowsze wersje systemu Windows umożliwiają bardziej precyzyjne zarządzanie zasadami inspekcji przy użyciu podkategorii zasad inspekcji. Ustawienie zasad kontroli na poziomie kategorii zastąpi nową funkcję zasad kontroli podkategorii. Zasady grupy pozwalają tylko na ustawienie zasad inspekcji na poziomie kategorii, a istniejące zasady grupy mogą zastąpić ustawienia podkategorii nowych komputerów, gdy są one przyłączone do domeny lub uaktualnione. Aby umożliwić zarządzanie zasadami inspekcji przy użyciu podkategorii bez konieczności zmiany zasad grupy, w systemie Windows Vista i nowszych wersjach pojawiła się nowa wartość rejestru SCENoApplyLegacyAuditPolicy, która uniemożliwia stosowanie zasad kontroli na poziomie kategorii z zasad grupy i zabezpieczeń lokalnego narzędzia administracyjnego polityki.
Opcje zabezpieczeń	Członek domeny: szyfruj lub podpisuj cyfrowo dane bezpiecznego kanału (zawsze)	Enabled	To ustawienie zabezpieczeń określa, czy cały ruch bezpiecznego kanału inicjowany przez członka domeny musi być podpisany, czy zaszyfrowany. To ustawienie określa, czy cały ruch bezpiecznego kanału inicjowany przez członka domeny spełnia minimalne wymagania bezpieczeństwa. W szczególności określa, czy cały ruch bezpiecznego kanału inicjowany przez członka domeny musi być podpisany, czy zaszyfrowany. Jeśli ta zasada jest włączona, bezpieczny kanał nie zostanie ustanowiony, chyba że zostanie wynegocjowane podpisanie lub szyfrowanie całego ruchu bezpiecznego kanału. Jeśli ta zasada jest wyłączona, szyfrowanie i podpisywanie całego bezpiecznego kanału jest negocjowane z kontrolerem domeny, w którym to przypadku poziom podpisywania i szyfrowania zależy od wersji kontrolera domeny i ustawień następujących dwóch zasad: - Członek domeny: szyfruj cyfrowo dane bezpiecznego kanału (jeśli to możliwe) - Członek domeny: podpisuj cyfrowo dane bezpiecznego kanału (jeśli to możliwe)
Opcje zabezpieczeń	Członek domeny: szyfruj cyfrowo dane bezpiecznego kanału (gdy to możliwe)	Enabled	To ustawienie zabezpieczeń określa, czy członek domeny próbuje negocjować szyfrowanie dla całego ruchu bezpiecznego kanału, który inicjuje. Jeśli ta opcja jest włączona, członek domeny zażąda szyfrowania całego ruchu bezpiecznego kanału. Jeśli kontroler domeny obsługuje szyfrowanie całego ruchu w bezpiecznym kanale, cały ruch w bezpiecznym kanale zostanie zaszyfrowany. W przeciwnym razie szyfrowane będą tylko informacje logowania przesyłane bezpiecznym kanałem. Jeśli to ustawienie jest wyłączone, członek domeny nie będzie próbował negocjować bezpiecznego szyfrowania kanału.
Opcje zabezpieczeń	Członek domeny: podpisuj cyfrowo dane bezpiecznego kanału (gdy to możliwe)	Enabled	To ustawienie zabezpieczeń określa, czy członek domeny próbuje negocjować podpisanie całego ruchu bezpiecznego kanału, który inicjuje. Jeśli ta opcja jest włączona, członek domeny zażąda podpisania całego ruchu bezpiecznego kanału. Jeśli kontroler domeny obsługuje podpisywanie całego ruchu w bezpiecznym kanale, wówczas cały ruch w bezpiecznym kanale zostanie podpisany, co gwarantuje, że nie będzie można go modyfikować podczas przesyłania.
Opcje zabezpieczeń	Członek domeny: wyłącz zmiany hasła konta komputera	Disabled	Określa, czy członek domeny okresowo zmienia hasło do konta komputera.

Opcje zabezpieczeń	Członek domeny: maksymalny wiek hasła konta komputera	30	Określa, jak często członek domeny będzie musiał zmienić hasło do konta komputera
Opcje zabezpieczeń	Członek domeny: wymaga silnego klucza sesji (Windows 2000 lub nowszy)	Enabled	Określa, czy do szyfrowania danych bezpiecznego kanału wymagana jest siła klucza 128-bitowego
Opcje zabezpieczeń	Logowanie interakcyjne: limit nieaktywności komputera	900	Liczba sekund braku aktywności po której sesja jest zablokowana
Opcje zabezpieczeń	Interactive logon: Smart card removal behavior	Lock Workstation	To ustawienie zabezpieczeń określa, co dzieje się, gdy karta inteligentna dla zalogowanego użytkownika jest usuwana z czytnika kart inteligentnych. Jeśli klikniesz Zablokuj stację roboczą we właściwościach dla tej zasady, stacja robocza zostanie zablokowana po usunięciu karty inteligentnej, umożliwiając użytkownikom opuszczenie obszaru, zabranie ze sobą kart inteligentnych i utrzymanie chronionych sesji. Aby to ustawienie działało od systemu Windows Vista, należy uruchomić usługę Zasady usuwania kart inteligentnych.
Opcje zabezpieczeń	Klient sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)	Enabled	To ustawienie zabezpieczeń określa, czy podpisywanie pakietów jest wymagane przez składnik klienta SMB.
Opcje zabezpieczeń	Klient sieci Microsoft: Wyślij niezaszyfrowane hasło w celu nawiązania połączenia z innymi serwerami SMB	Disabled	Jeśli to ustawienie zabezpieczeń jest włączone, readresator bloku komunikatów serwera (SMB) może wysyłać hasła w postaci zwykłego tekstu do serwerów SMB innych niż Microsoft, które nie obsługują szyfrowania hasła podczas uwierzytelniania. Wysyłanie niezaszyfrowanych haseł stanowi zagrożenie bezpieczeństwa.
Opcje zabezpieczeń	Serwer sieci Microsoft: podpisuj cyfrowo komunikację (zawsze)	Enabled	To ustawienie zabezpieczeń określa, czy podpisywanie pakietów jest wymagane przez składnik serwera SMB.
Opcje zabezpieczeń	Dostęp sieciowy: Zezwalaj na anonimową translację identyfikatorów SID / nazw	Disabled	To ustawienie zabezpieczeń określa, czy anonimowy użytkownik może zażądać atrybutów identyfikatora bezpieczeństwa (SID) dla innego użytkownika. Jeśli ta zasada jest włączona, użytkownik ze znajomością identyfikatora SID administratora może skontaktować się z komputerem, na którym włączono tę zasadę, i użyć identyfikatora SID, aby uzyskać nazwę administratora.
Opcje zabezpieczeń	Dostęp sieciowy: nie zezwalaj na anonimowe wyliczanie kont SAM	Enabled	To ustawienie zabezpieczeń określa, jakie dodatkowe uprawnienia zostaną przyznane dla anonimowych połączeń z komputerem. System Windows umożliwia anonimowym użytkownikom wykonywanie określonych czynności, takich jak wyliczanie nazw kont domeny i udziałów sieciowych. Jest to wygodne, na przykład, gdy administrator chce przyznać dostęp użytkownikom w zaufanej domenie, która nie utrzymuje wzajemnego zaufania. Ta opcja zabezpieczeń umożliwia nałożenie dodatkowych ograniczeń na anonimowe połączenia w następujący sposób: Włączone: Nie zezwalaj na wyliczanie kont SAM. Ta opcja zastępuje Wszyscy Uprawnieni Użytkownicy w uprawnieniach zabezpieczeń zasobów.
Opcje zabezpieczeń	Dostęp sieciowy: nie zezwalaj na anonimowe wyliczanie kont SAM i udziałów	Enabled	To ustawienie zabezpieczeń określa, czy dozwolone jest anonimowe wyliczanie kont SAM i udziałów. System Windows umożliwia anonimowym użytkownikom wykonywanie określonych czynności, takich jak wyliczanie nazw kont domeny i udziałów sieciowych. Jest to wygodne, na przykład, gdy administrator chce przyznać dostęp użytkownikom w zaufanej domenie, która nie utrzymuje wzajemnego zaufania. Jeśli nie chcesz zezwalać na anonimowe wyliczanie kont i udziałów SAM, włącz tę zasadę.
Opcje zabezpieczeń	Dostęp sieciowy: Ogranicz anonimowy dostęp do nazwanych potoków i udziałów	Enabled	Po włączeniu to ustawienie zabezpieczeń ogranicza anonimowy dostęp do udziałów i potoków do ustawień dla: - Dostęp do sieci: Nazwane potoki, do których można uzyskać dostęp anonimowo - Dostęp do sieci: udziały, do których można uzyskać dostęp anonimowo
Opcje zabezpieczeń			
Opcje zabezpieczeń			
Opcje zabezpieczeń	Dostęp sieciowy: Ogranicz klientów, którzy mogą wykonywać wywołania zdalne menadżera SAM	O:BAG:BAD:(A;;RC;;;BA)	To ustawienie zasad pozwala ograniczyć zdalne połączenia RPC do SAM. Jeśli ta opcja nie zostanie wybrana, zostanie użyty domyślny deskryptor zabezpieczeń.
Opcje zabezpieczeń	Zabezpieczenia sieciowe: Zezwalaj kontu systemowi lokalnemu na używanie pustych sesji	Disabled	Zezwól NTLM na powrót do sesji NULL, gdy jest używany z LocalSystem
Opcje zabezpieczeń	Zabezpieczenia sieciowe: Nie przechowuj wartości skrótu LAN Managera przy następnej zmianie hasła	Enabled	To ustawienie zabezpieczeń określa, czy przy następnej zmianie hasła przechowywana jest wartość skrótu LAN Manager (LM) dla nowego hasła. Skrót LM jest stosunkowo słaby i podatny na atak, w porównaniu z kryptograficznie silniejszym skrótem Windows NT. Ponieważ skrót LM jest przechowywany na komputerze lokalnym w bazie danych bezpieczeństwa, hasła mogą zostać naruszone, jeśli baza danych zostanie zaatakowana.
Opcje zabezpieczeń	Zabezpieczenia sieci: poziom uwierzytelnienia LAN Managera	Send NTLMv2 response only. Refuse LM & NTLM	To ustawienie zabezpieczeń określa, który protokół uwierzytelnienia wyzwanie / odpowiedź jest używany do logowania do sieci. Ten wybór wpływa na poziom protokołu uwierzytelniania używanego przez klientów, wynegocjowany poziom bezpieczeństwa sesji oraz poziom uwierzytelnienia akceptowany przez serwery w następujący sposób: Wyślij tylko odpowiedź NTLMv2 \ odmów LM i NTLM: Klienci używają tylko uwierzytelniania NTLMv2 i używają zabezpieczeń sesji NTLMv2 jeśli serwer to obsługuje; kontrolery domeny odrzucają LM i NTLM (akceptują tylko uwierzytelnianie NTLMv2).
Opcje zabezpieczeń	Zabezpieczenia sieci: Wymagania podpisywania klienta LDAP	Negotiate signing	To ustawienie zabezpieczeń określa poziom podpisywania danych, który jest wymagany w imieniu klientów wysyłających żądania LDAP BIND, w następujący sposób: Podpisywanie negocjacji: Jeśli Transport Layer Security / Secure Sockets Layer (TLS \ SSL) nie został uruchomiony, żądanie LDAP BIND są inicjowane z ustawioną opcją podpisywania danych LDAP oprócz opcji określonych przez osobę wywołującą. Jeśli TLS \ SSL zostało uruchomione, żądanie LDAP BIND jest inicjowane z opcjami określonymi przez osobę wywołującą.
Opcje zabezpieczeń	Zabezpieczenia sieci: minimalne zabezpieczenia sesji dla klientów opartych na NTLM SSP (włączając secure RPC)	Require NTLMv2 session security and Require 128-bit encryption	To ustawienie zabezpieczeń pozwala klientowi wymagać negocjacji 128-bitowego szyfrowania i / lub bezpieczeństwa sesji NTLMv2. Wartości te są zależne od wartości ustawienia zabezpieczeń Poziom uwierzytelnienia LAN Managera.

Opcje zabezpieczeń	Zabezpieczenia sieci: minimalne zabezpieczenia sesji dla serwerów opartych na NTLM SSP (włączając secure RPC)	Require NTLMv2 session security and Require 128-bit encryption	To ustawienie zabezpieczeń pozwala serwerowi wymagać negocjacji 128-bitowego szyfrowania i / lub bezpieczeństwa sesji NTLMv2. Wartości te są zależne od wartości ustawienia zabezpieczeń Poziom uwierzytelnienia LAN Managera.
Opcje zabezpieczeń	Obiekty systemowe: wzmocnij uprawnienia domyślne wewnętrznych obiektów systemu (np. linków symbolicznych)	Enabled	To ustawienie zabezpieczeń określa siłę domyślnej uznaniowej listy kontroli dostępu (DACL) dla obiektów. Usługa Active Directory utrzymuje globalną listę współużytkowanych zasobów systemowych, takich jak nazwy urządzeń DOS, muteksy i semafory. W ten sposób obiekty mogą być lokalizowane i współdzielone między procesami. Każdy typ obiektu jest tworzony z domyślną listą DACL, która określa, kto może uzyskać dostęp do obiektów i jakie uprawnienia są przyznawane. Jeśli ta zasada jest włączona, domyślna lista DACL jest silniejsza, umożliwiając użytkownikom niebędącym administratorami odczytywanie obiektów udostępnionych, ale nie zezwalając tym użytkownikom na modyfikowanie obiektów udostępnionych, których nie utworzyli.
Opcje zabezpieczeń	Kontrola konta użytkownika: tryb zatwierdzania przez administratora dla wbudowanego konta administratora	Enabled	Wbudowane konto administratora korzysta z trybu zatwierdzania przez administratora - każda operacja wymagająca podniesienia uprawnień spowoduje wyświetlenie monitu o zatwierdzenie tej operacji
Opcje zabezpieczeń	Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla administratorów w trybie zatwierdzania przez administratora	Prompt for consent on the secure desktop	Gdy operacja wymaga podniesienia uprawnień, użytkownik jest monitowany na bezpiecznym pulpicie o podanie nazwy i hasła uprzywilejowanego użytkownika. Jeśli użytkownik wprowadzi prawidłowe poświadczenia, operacja będzie kontynuowana z najwyższymi dostępnymi uprawnieniami użytkownika.
Opcje zabezpieczeń	Kontrola konta użytkownika: wykrywanie instalacji aplikacji i monitowanie o podniesienie uprawnień	Enabled	Po wykryciu pakietu instalacyjnego aplikacji wymagającego podniesienia uprawnień użytkownik jest monitowany o podanie nazwy użytkownika administracyjnego i hasła. Jeśli użytkownik wprowadzi prawidłowe poświadczenia, operacja będzie kontynuowana z odpowiednim uprawnieniem.
Opcje zabezpieczeń	Kontrola konta użytkownika: zezwalaj aplikacjom zpoziomem UIAccess na monitowanie o podniesienie uprawnień bez używania bezpiecznego pulpitu	Enabled	To ustawienie zasad kontroluje, czy aplikacje żądające uruchomienia z poziomem integralności interfejsu użytkownika (UIAccess) muszą znajdować się w bezpiecznej lokalizacji w systemie plików. Bezpieczne lokalizacje są ograniczone do: -... \ Program Files \, w tym podfolderów -... \ Windows \ system32 \ -... \ Program Files (x86) \, w tym podfolderów dla 64-bitowych wersji systemu Windows
Opcje zabezpieczeń	Kontrola konta użytkownika: Uruchom wszystkich administratorów w trybie zatwierdzania przez administratora	Enabled	Ta zasada musi być włączona, a powiązane ustawienia zasad UAC również muszą być odpowiednio ustawione, aby umożliwić wbudowanemu kontowi administratora i wszystkim innym użytkownikom, którzy są członkami grupy administratorów, działanie w trybie zatwierdzania przez administratora (Admin Approval Mode).
Opcje zabezpieczeń	Kontrola konta użytkownika: wirtualizuj błędy zapisu plików i rejestru w lokalizacjach poszczególnych użytkowników	Enabled	To ustawienie zasad kontroluje, czy błędy zapisu aplikacji są przekierowywane do zdefiniowanych lokalizacji rejestru i systemu plików. To ustawienie zasad ogranicza aplikacje działające jako administrator i zapisujące dane aplikacji w czasie wykonywania do % ProgramFiles%,% Windir%,% Windir% \ system32 lub HKLM \ Software.
Przypisywanie praw użytkownika	Uzyskaj dostęp do Menadżera poświadczeńjako zaufany obiekt wywołujący	No One (blank)	To ustawienie jest używane przez menedżera poświadczeń podczas tworzenia kopii zapasowej / przywracania. Żadne konta nie powinny mieć tego uprawnienia, ponieważ są przypisane tylko do Winlogon. Zapisane poświadczenia użytkowników mogą zostać naruszone, jeśli uprawnienie to zostanie przyznane innym podmiotom.
Przypisywanie praw użytkownika	Uzyskanie dostęp do tego komputera z sieci	Administrators; Remote Desktop Users	To prawo użytkownika określa, którzy użytkownicy i grupy mogą łączyć się z komputerem przez sieć. Prawo użytkownika nie ma wpływu na Usługi pulpitu zdalnego.
Przypisywanie praw użytkownika	Działanie jako część systemu operacyjnego	No One (blank)	To prawo użytkownika pozwala na podszywanie się pod dowolnego użytkownika bez uwierzytelnienia. Proces może zatem uzyskać dostęp do tych samych zasobów lokalnych, co ten użytkownik.
Przypisywanie praw użytkownika	Zezwalaj na logowanie lokalne	Administrators; Users	Określa, którzy użytkownicy mogą zalogować się do komputera
Przypisywanie praw użytkownika	Wykonuj kopie zapasowe plików i katalogów	Administrators	Określa, którzy użytkownicy mogą ominąć uprawnienia do plików i katalogów, rejestru i innych uprawnień do obiektów trwałych w celu wykonania kopii zapasowej systemu
Przypisywanie praw użytkownika	Utwórz plik stronicowania	Administrators	Określa, którzy użytkownicy i grupy mogą wywoływać wewnętrzny interfejs programowania aplikacji (API) w celu utworzenia i zmiany rozmiaru pliku strony
Przypisywanie praw użytkownika	Utwórz obiekt tokenu	No One (blank)	Określa, które konta mogą być używane przez procesy w celu utworzenia tokena, który może być następnie użyty w celu uzyskania dostępu do dowolnych zasobów lokalnych, gdy proces używa wewnętrznego interfejsu programowania aplikacji (API) do utworzenia tokena dostępu.

Przypisywanie praw użytkownika	Utwórz obiekty globalne	Administrators; LOCAL SERVICE; NETWORK SERVICE; SERVICE	To ustawienie zabezpieczeń określa, czy użytkownicy mogą tworzyć obiekty globalne dostępne dla wszystkich sesji.
Przypisywanie praw użytkownika	Utwótrz trwałe obiekty udostępnione	No One (blank)	Określa, które konta mogą być używane przez procesy do utworzenia obiektu katalogu za pomocą menedżera obiektów
Przypisywanie praw użytkownika	Debuguj programy	Administrators	Określa, którzy użytkownicy mogą dołączyć debugger do dowolnego procesu lub jądra. Programiści debugujący własne aplikacje nie muszą mieć przypisanego tego prawa użytkownika. Programiści, którzy debugują nowe składniki systemu, będą potrzebować tego prawa użytkownika, aby móc to zrobić. To prawo użytkownika zapewnia pełny dostęp do wrażliwych i krytycznych komponentów systemu operacyjnego.
Przypisywanie praw użytkownika	Określ konta komputerów i użytkowników jako zaufane w kwestii delegowania	No One (blank)	To ustawienie zabezpieczeń określa, którzy użytkownicy mogą ustawić ustawienie zaufane dla delegowania (Trusted for Delegation) dla obiektu użytkownika lub komputera.
Przypisywanie praw użytkownika	Wymuszaj zamknięcie z systemu zadalnego	Administrators	Określa, którzy użytkownicy mogą wyłączyć komputer ze zdalnej lokalizacji w sieci. Niewłaściwe korzystanie z tego prawa użytkownika może spowodować odmowę usługi.
Przypisywanie praw użytkownika	Personifikuj klienta po uwierzytelnieniu	Administrators, SERVICE, Local Service, Network Service	Przypisanie tego uprawnienia użytkownikowi pozwala programom działającym w jego imieniu na podszywanie się pod klienta. Wymaganie tego prawa użytkownika do tego rodzaju personifikacji uniemożliwia nieautoryzowanemu użytkownikowi przekonanie klienta do połączenia (na przykład przez zdalne wywołanie procedury (RPC) lub nazwane potoki) z utworzoną przez niego usługą, a następnie podszywanie się pod tego klienta, co może podnieść uprawnienia nieautoryzowanego użytkownika do poziomów administracyjnych lub systemowych.
Przypisywanie praw użytkownika	Ładuj i zwalniaj sterowniki urządzeń	Administrators	Określa, którzy użytkownicy mogą dynamicznie ładować i zwalniać sterowniki urządzeń lub inny kod w trybie jądra. To prawo użytkownika nie dotyczy sterowników urządzeń Plug and Play.
Przypisywanie praw użytkownika	Blokuj strony w pamięci	No One (blank)	Określa, które konta mogą wykorzystywać proces do przechowywania danych w pamięci fizycznej, co uniemożliwia systemowi stronicowanie danych do pamięci wirtualnej na dysku. Korzystanie z tego przywileju może znacząco wpłynąć na wydajność systemu, zmniejszając ilość dostępnej pamięci RAM.
Przypisywanie praw użytkownika	Zarządzaj dziennikami inspekcji i zabezpieczeń	Administrators	Określa, którzy użytkownicy mogą określić opcje kontroli dostępu do obiektów dla poszczególnych zasobów, takich jak pliki, obiekty Active Directory i klucze rejestru.
Przypisywanie praw użytkownika	Modyfikuj wartości środowiska oprogramowania układowego	Administrators	Określa, kto może modyfikować wartości środowiskowe oprogramowania układowego. Zmienne środowiskowe oprogramowania układowego to ustawienia przechowywane w nieulotnej pamięci RAM komputerów innych niż x86. Efekt ustawienia zależy od procesora.
Przypisywanie praw użytkownika	Wykonaj zadania konserwacji woluminów	Administrators	To ustawienie zabezpieczeń określa, którzy użytkownicy i grupy mogą uruchamiać zadania konserwacyjne na woluminie, takie jak zdalna defragmentacja.
Przypisywanie praw użytkownika	Profiluj pojedynczy proces	Administrators	To ustawienie zabezpieczeń określa, którzy użytkownicy mogą korzystać z narzędzi monitorowania wydajności do monitorowania wydajności procesów niesystemowych.
Przypisywanie praw użytkownika	Przywracaj pliki i katalogi	Administrators	Określa, którzy użytkownicy mogą ominąć uprawnienia do plików, katalogów, rejestru i innych obiektów trwałych podczas przywracania kopii zapasowych plików i katalogów, oraz określa, którzy użytkownicy mogą ustawić dowolną ważną zasadę zabezpieczeń jako właściciela obiektu.
Przypisywanie praw użytkownika	Przejmij na własność pliki lub inne obiekty	Administrators	Określa, którzy użytkownicy mogą przejąć na własność dowolny zabezpieczany obiekt w systemie, w tym obiekty Active Directory, pliki i foldery, drukarki, klucze rejestru, procesy i wątki