Uprawnienia do odczytu zasobów na partycjach NTFS

System plików NTFS (New Technology File System) to obecnie najpopularniejszy system plików dla środowiska Microsoft Windows. Obecnie systemy Windows 8.x/2012 (R2) wykorzystują jego piątą wersję. Na obecne lata system zaczyna być mało wydajny dla środowisk serwerowych, w których pojemności dyskowe liczone są w eksabajtach (10^{18}).

W najnowszej, 5 wersji, system pozwala na utworzenie woluminu o wielkości 16 eksabajtów (18 446 744 073 709 551 616 bajtów). Rozmiar ten jest również niemal maksymalną wielkością pliku, jaki może zająć na woluminie (należy odjąć od jego wielkości 1 kilobajt). W przeciwieństwie do poprzednich systemów (rodzina FAT) w NTFS zaimplementowano system księgowania. Pozwala to na znacznie zwiększenie niezawodności systemu – w przypadku problemów z zapisem awarii nie ulegnie cały wolumen,a naprawa sprowadzi się do cofnięcia ostatniej operacji (podobny system ma zastosowanie np. w bazach SQL). Główna tabela plików posiada wiele kopii (w FAT tylko jedna), a sam system pozbawiony jest elementów specjalnych (jak superbloki czy obiekty specjalne). Dodatkowo wprowadzono możliwość nadawania specjalnych uprawnień do plików i katalogów, ulepszono kopiowanie danych, dodano implementację innych systemów plików (montowanych w ramach partycji NTFS) i wiele innych. Nowością jest także przybliżenie do standardu POSIX v1 – rozróżnianie wielkości znaków, sygnaturę czasową określającą czas dostępu do pliku czy łącza stałe/symboliczne.

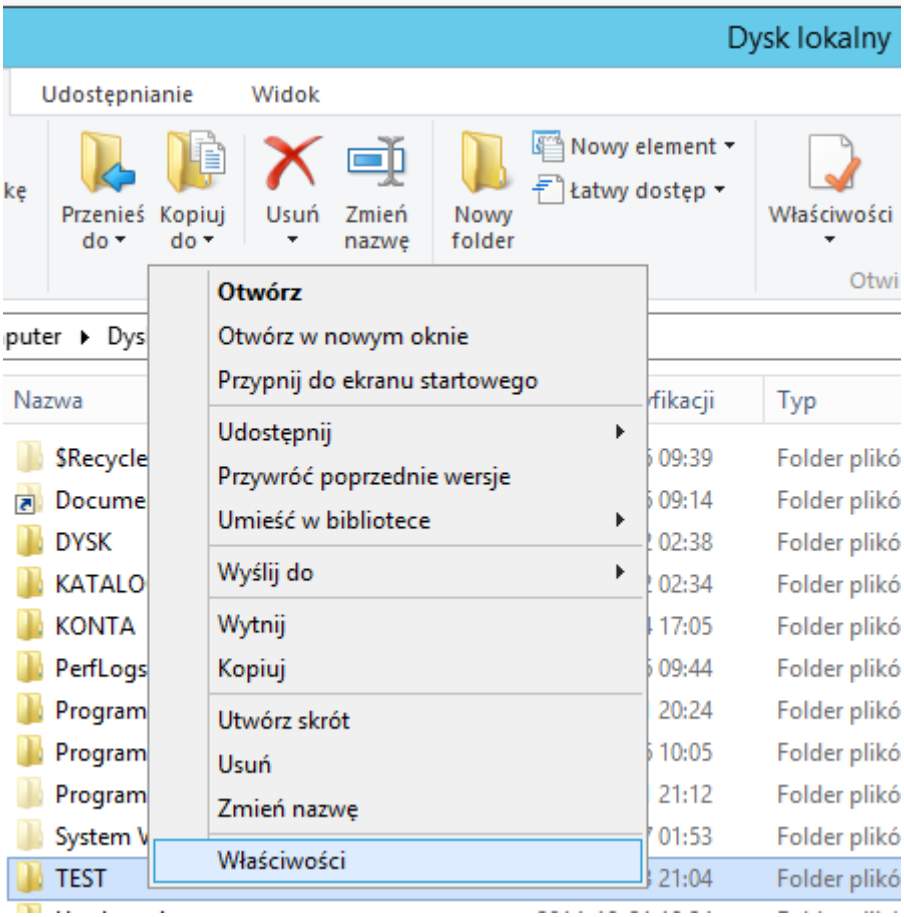
Niestety NTFSv5 nie wspiera wielu nowych rozwiązań, jak kompresja w locie, dane w nim przechowywane podlegają fragmentacji, nie posiada wbudowanego systemu kompresji danych nadmiarowych, tworzenia migawek czy też brak jest możliwości tworzenia podwoluminów (partycji w partycji – szczególnie przydane przy serwera wirtualnych). Dlatego też wraz z Windows 8.1/2012 R2 zadebiutował nowy system – ReFS. Na tę chwilę jest jednak nadal słabo wspierany zarówno przez sam Microsoft jak i firmy zewnętrzne. Ponadto system ten dalej dotykają problemy wieku dziecięcego (przepełnianie może powodować jego niedostępność, włączenie samoregeneracji może powodować znaczne spowolnienia itp.). Można się jednak spodziewać, iż w niedługim czasie to właśnie ten system plików będzie wykorzystywany w następnych wersjach systemów Windows, a jego potencjalnie niedociągnięcia zostaną wkrótce wyeliminowane.

Nie zmienia to faktu, że NTFS przez długi czas będzie jeszcze wykorzystywany przez wielu użytkowników (w tym administratorów). Najważniejsza jest bowiem kompatybilność minimum odczytu, której ReFS nie zapewni dla starszych systemów/systemów innych niż system Microsoft (ReFS ma zamkniętą implementację – jak zresztą wszystkie inne systemy plików firmy Microsoft).

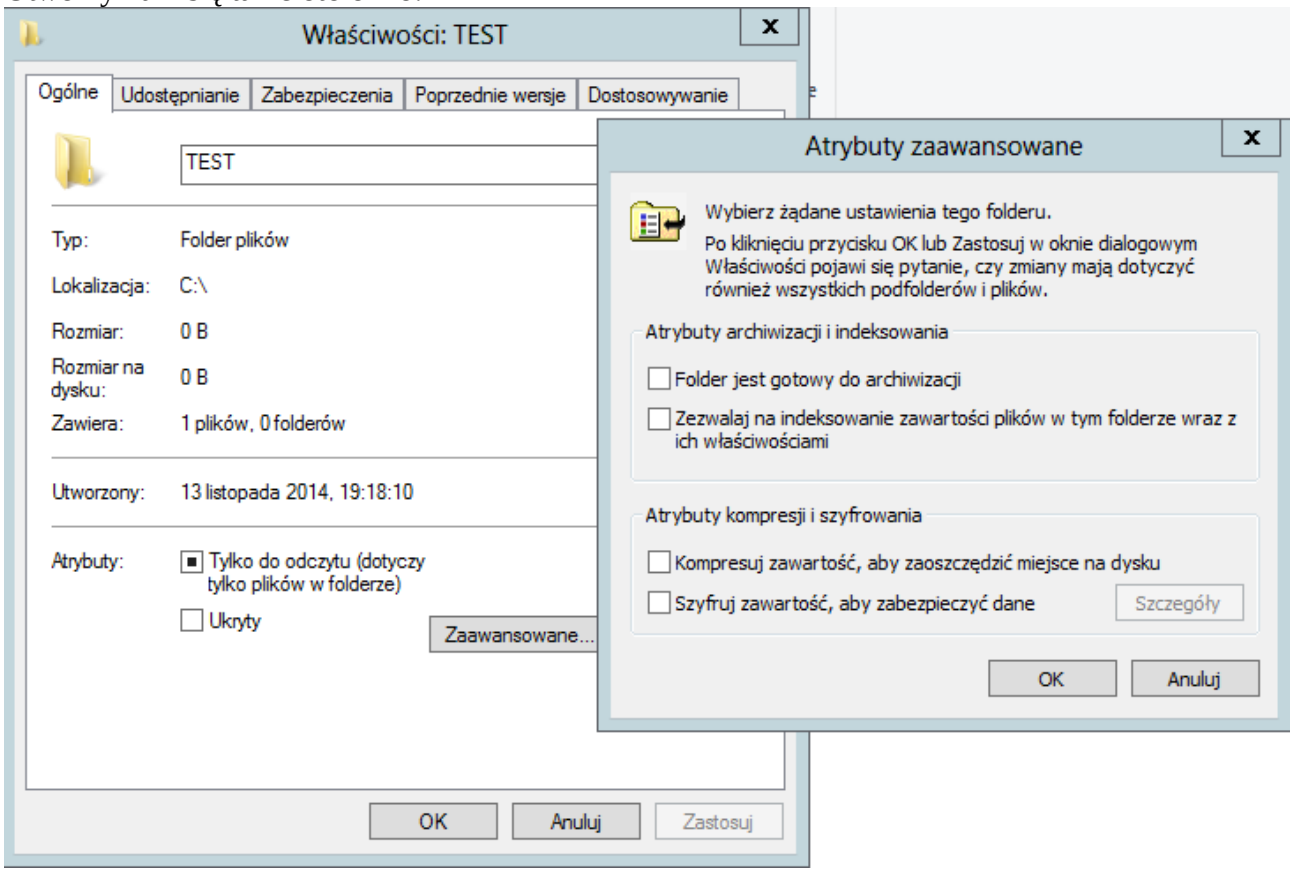
Więcej informacji o systemie NTFS można znaleźć tutaj: http://support.microsoft.com/kb/100108/pl, http://www.ntfs.com/ntfs_vs_fat.htm oraz http://en.wikipedia.org/wiki/NTFS (polska wersja zawiera w większości już nieprawdziwe informacje!).

Zarządzanie uprawnieniami odczytu folderów/plików.

Aby rozpocząć zadanie należy utworzyć gdziekolwiek (najlepiej na dysku C, lecz może być inna lokalizacja) dowolny folder (dla celów ćwiczenia utworzony został katalog TEST). By móc rozpocząć zarządzanie uprawnieniami odczytu (i nie tylko) należy wybrać właściwości tego katalogu (prawy przycisk myszy->Właściwości bądź ikona Właściwości na wstążce Narzędzia główne).



Otworzy nam się takie oto okno:



W zakładce Ogólne mamy podstawowe informacje dotyczące utworzonego folderu – lokalizację, rozmiar, rozmiar na dysku (należy pamiętać, że nie są one tożsame!) oraz ile plików/podfolderów zawiera. Część najbardziej interesująca (pod kątem uprawnień) z tej zakładki to Atrybuty:

- Tylko do odczytu – powoduje, że PLIKI zawarte w tym folderze uzyskają status tylko do odczytu. Od tego momentu nie będzie możliwa modyfikacja ich danych. Atrybut ten można więc traktować jako zabezpieczenie przed nadpisaniem pliku/ów. Proszę zauważyć, że każdy folder atrybut ten będzie miał oznaczony jako „nieznany” (w tym wypadku kwadrat) – on sam nigdy nie może być tylko do odczytu.

WAŻNE – pliki z atrybutem tylko do odczytu można przenosić/kopiować/usuwać. Atrybut ten realnie wcale nie chroni nas przed utratą ważnych danych. Sam folder/podfolder nie może być tylko do odczytu. Po ustawieniu tego parametru dla folderu pliki w nim uzyskają status Tylko do odczytu; pliki skopiowane później nie otrzymają tego statusu (chyba, że posiadały go w chwili kopiowania/przenoszenia)

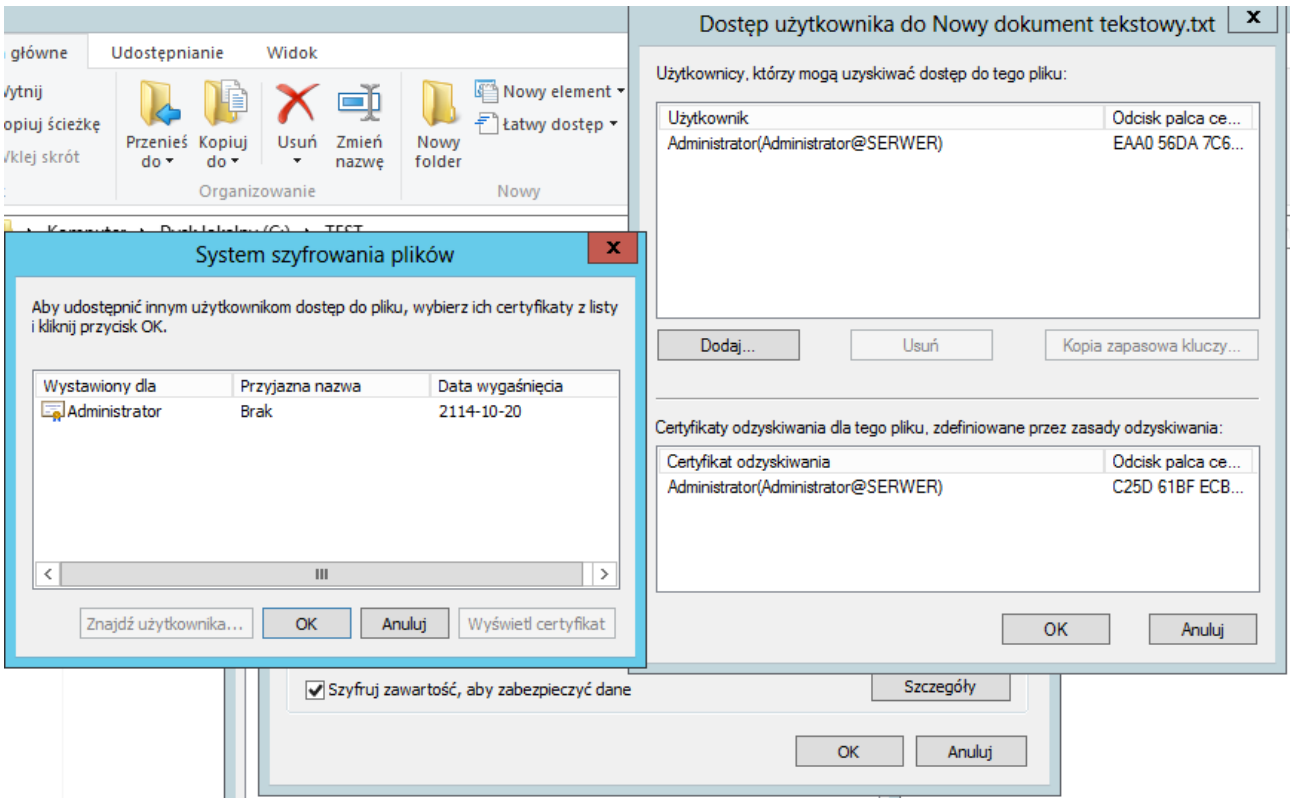
- Ukryty – folder zostaje ukryty. Oczywiście jest to bardzo proste, nad wyraz nieskuteczne zabezpieczenie – wystarczy zmienić Opcje folderów na „Pokaż ukryte pliki” by wszystkie ukryte foldery/pliki widzieć w Eksploratorze. Atrybut jest jednak użyteczny gdy chcemy uczynić bardziej „przejrzystym” poszczególne foldery ukrywając te, które nie są potrzebne zwykłemu użytkownikowi. Przykładowo aplikacja posiadająca wiele plików/folderów z danymi aplikacji nie musi ich wszystkich wyświetlać w swoim folderze lecz posiadać je ukryte – wtedy ważne pliki (np. raporty czy też pliki danych) będą lepiej widoczne/dostępne dla użytkownika.

Dodatkowo każdy folder/plik posiada Atrybuty zaawansowane:
- Folder/Plik jest gotowy do archiwizacji – atrybut wykorzystywany przez narzędzie kopii zapasowej systemu Windows. Gdy ten atrybut jest zaznaczony system wie, że ma wykonać kopię zapasową tego folderu/pliku. Po wykonaniu kopii atrybut jest zerowany. Przy ponownym wykonywaniu kopii narzędzie nie będzie już archiwizowało tego pliku/folderu chyba, że zawartość ulegnie zmianie (wtedy atrybut ustawi się samoczynnie) bądź użytkownik zmieni ustawienie tego atrybutu. Domyślnie każdy plik jest zaznaczony do archiwizacji, a folder nie.

- Zezwalaj na indeksowanie zawartości plików w tym folderze wraz z ich właściwościami – atrybut dla narzędzia indeksowania zawartości dysku twardego. Działa analogicznie jak poprzedni atrybut (gdy ustawiony plik/folder i jego zawartość jest indeksowana/po indeksacji atrybut jest ściągany i ustawiany przy zmianie).

- Kompresuj zawartość, aby zaoszczędzić miejsce na dysku – powoduje skompresowanie wskazanego folderu (i/lub plików) dzięki czemu dane w nich zawarte zajmują trochę mniej miejsca. W przypadku pojedynczych folderów działanie kompresji/dekompresji jest w miarę szybkie i nie powinno zajmować zbyt wiele czasu (niemal kompresja w locie).
INFORMACJA: O wiele lepszym rozwiązaniem jest używanie kompresji zip, wbudowanej w system od Windows XP i nowszych

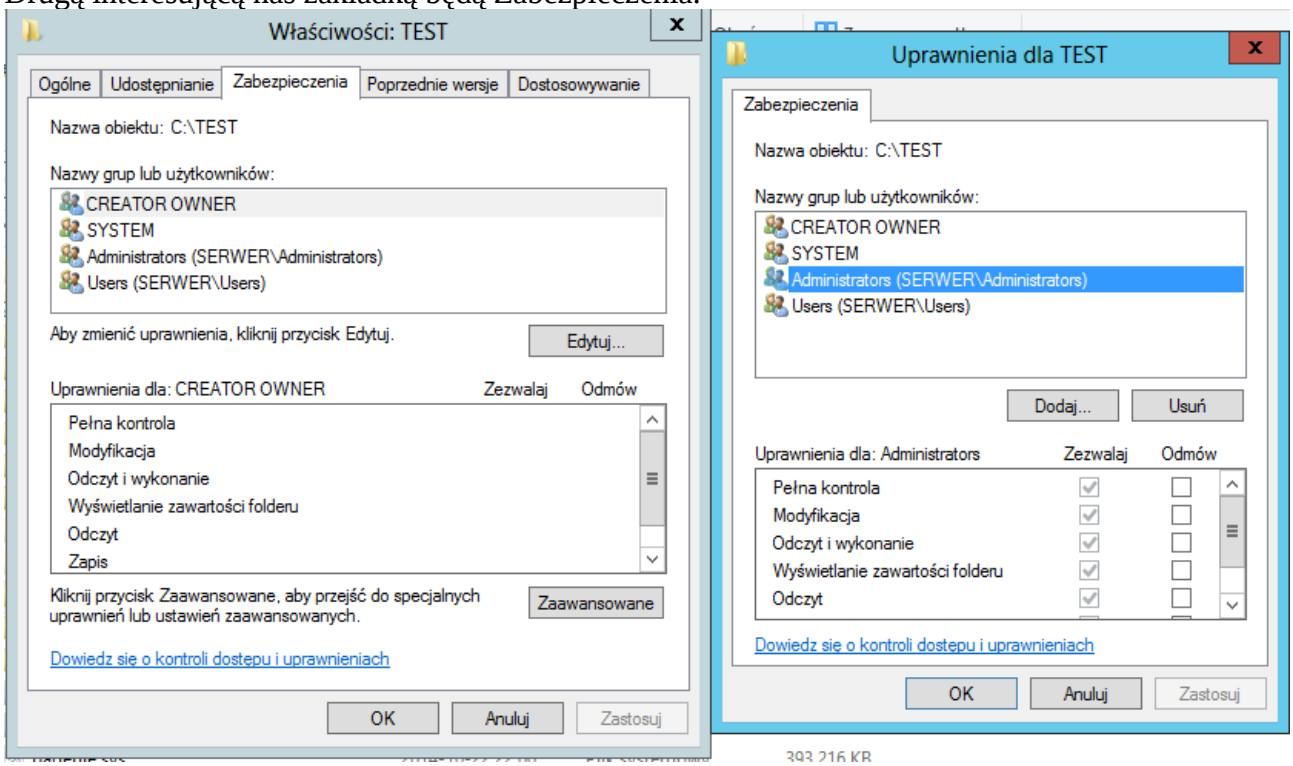
- Szyfruj zawartość, aby zabezpieczyć dane – funkcja umożliwia szyfrowanie folderów i ich zawartości w taki sposób, że tylko upoważnieni użytkownicy systemu mają do nich dostęp. Nawet jeżeli ktoś dany plik/folder skopiuje to dane pozostaną bezpieczne – chyba, że ukradnie on także nasze klucze publiczne/prywatne (szyfrowanie asymetryczne). Możemy swobodnie decydować kto ma dostęp a kto nie do poszczególnych zaszyfrowanych plików.



Więcej informacji na ten temat można znaleźć w dosyć dobrze napisanym artykule: http://www.pcworld.pl/artykuly/314619/Szyfrowanie.na.sniadanie.html .

WAŻNE: Nie jest zalecane stosowanie kompresji NTFS oraz szyfrowania NTFS (może to doprowadzić do nieodwracalnej utraty danych). Lepszym pomysłem jest np. zaszyfrować folder, a następnie dodać do niego kompresowane dane poprzez zip (od Windows Vista można również zamiast EFS używać narzędzie BitLocker).

Drugą interesującą nas zakładką będą Zabezpieczenia.



Pozwala zarządzać kontrolą dostępu i uprawnieniami (ACL – Access Control List). Mamy

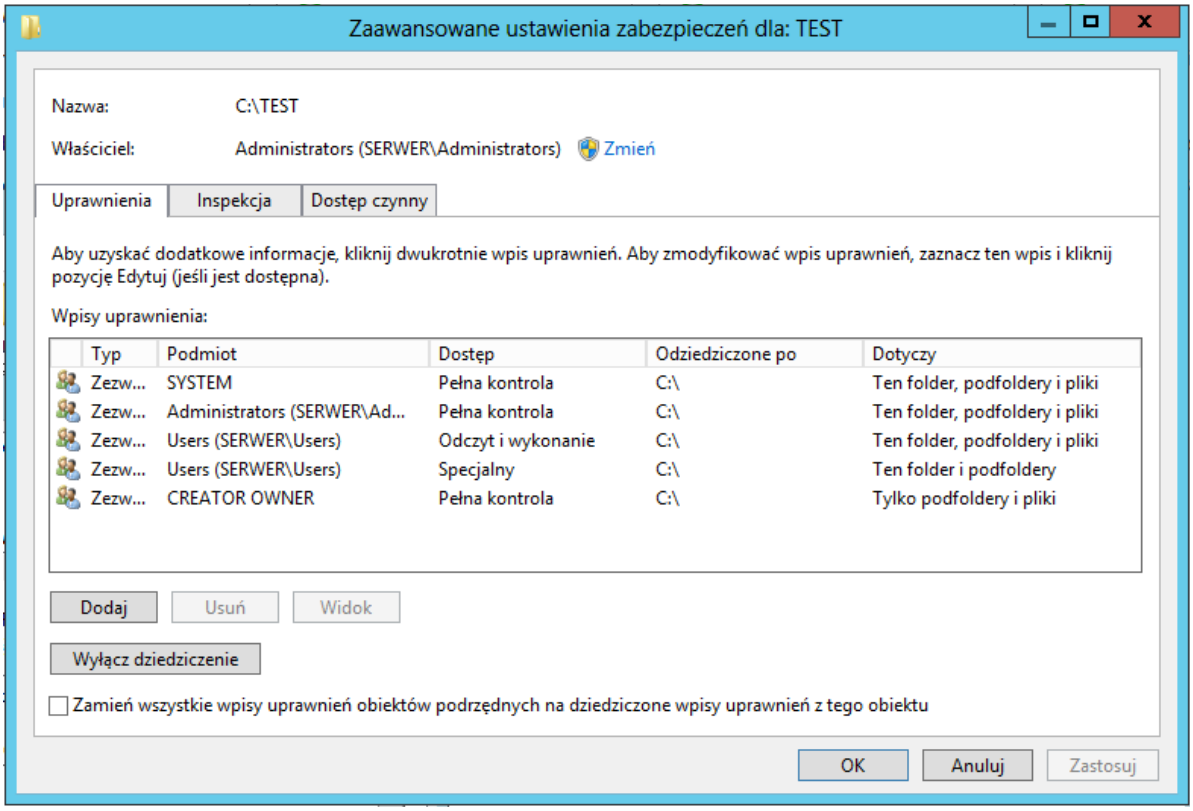
możliwość nadawania uprawnień w sposób uproszczony (przycisk Edytuj...) lub w sposób Zaawansowany (przycisk Zaawansowane).

Główny widok zakładki informuje nas o nazwie przeglądanego obiektu (może być folder bądź plik). Poniżej znajdują się upoważnione Nazwy grup lub użytkowników, którzy mają nadane/zabrane prawa do tego zasobu. Następnie (pod przyciskiem Edytuj...) wyświetlane są uprawnienia dla aktualnie wybranego użytkownika/grupy użytkowników do wybranego zasobu.

Klikając przycisk Edytuj... możemy dodawać/usuwać poszczególnych użytkowników/grupy z listy (okno po prawej). Pod przyciskami Dodaj... (dodaje użytkowników/grupy) oraz Usuń (usuwa wybranego z listy wyżej użytkownika/grupę) znajduje się lista uprawnień do zasobu z polami Zezwalaj i Odmów. Zaznaczenie w polu Zezwalaj pozwala danemu użytkownikowi/grupie na określoną czynność, a zaznaczenie w Odmów jej zabrania.
WAŻNE: Pole Odmów ma większą wagę od Zezwalaj. Nawet jeżeli ktoś ma domyślnie zaznaczone pole Zezwalaj lecz nadamy dla niego wartość Odmów to będzie ona stosowana przez zezwoleniem (innymi słowy zabronimy danej grupie/użytkownikowi określonego działania).

Opis uprawnień dla użytkownika/grupy:
- Pełna kontrola – ustawia pełne uprawnienia do obiektu, włączając w to nadpisywanie, modyfikowanie, dodawanie, przenoszenie oraz skasowanie zasobu (lub w przypadku folderów skasowanie podzasobów)
- Modyfikacja – gdy tylko ona jest ustawiona, umożliwia wskazanemu podmiotowi na wszystkie operacje względem zaosbu poza usuwaniem podfolderów/plików we wskazanym zasobie, zmianę pozwoleń oraz przejęcie zasobu na własność
- Odczyt i wykonanie – pozwala na wykonywanie plików, odczyt plików, odczytywanie atrybutów, odczytywanie rozszerzonych atrybutów, odczyt pozwoleń oraz na synchronizację (z folderami sieciowymi); pozostałe operacje na zasobach są niedozwolone
WAŻNE! To uprawnienie ma wpływ tylko na wskazany zasób (plik/folder) chyba, że włączone jest dziedziczenie
- Wyświetlanie zawartości folderu – jak poprzednio z tym, że dotyczy zasobów zawartych w folderze (uprawnienie pojawia się tylko względem folderów).
- Odczyt – pozwala na odczyt plików (dane/lista folderów), odczyt atrybutów, odczyt rozszerzonych atrybutów, odczyt uprawnień oraz synchronizację z innymi folderami
- Zapis – pozwala tworzyć pliki/zapisywać dane w plikach, tworzyć/dodawać foldery, zmieniać (zapisywać) atrybuty, zmieniać (zapisywać) rozszerzone atrybuty, odczytywać uprawnienia oraz przeprowadzać synchronizację

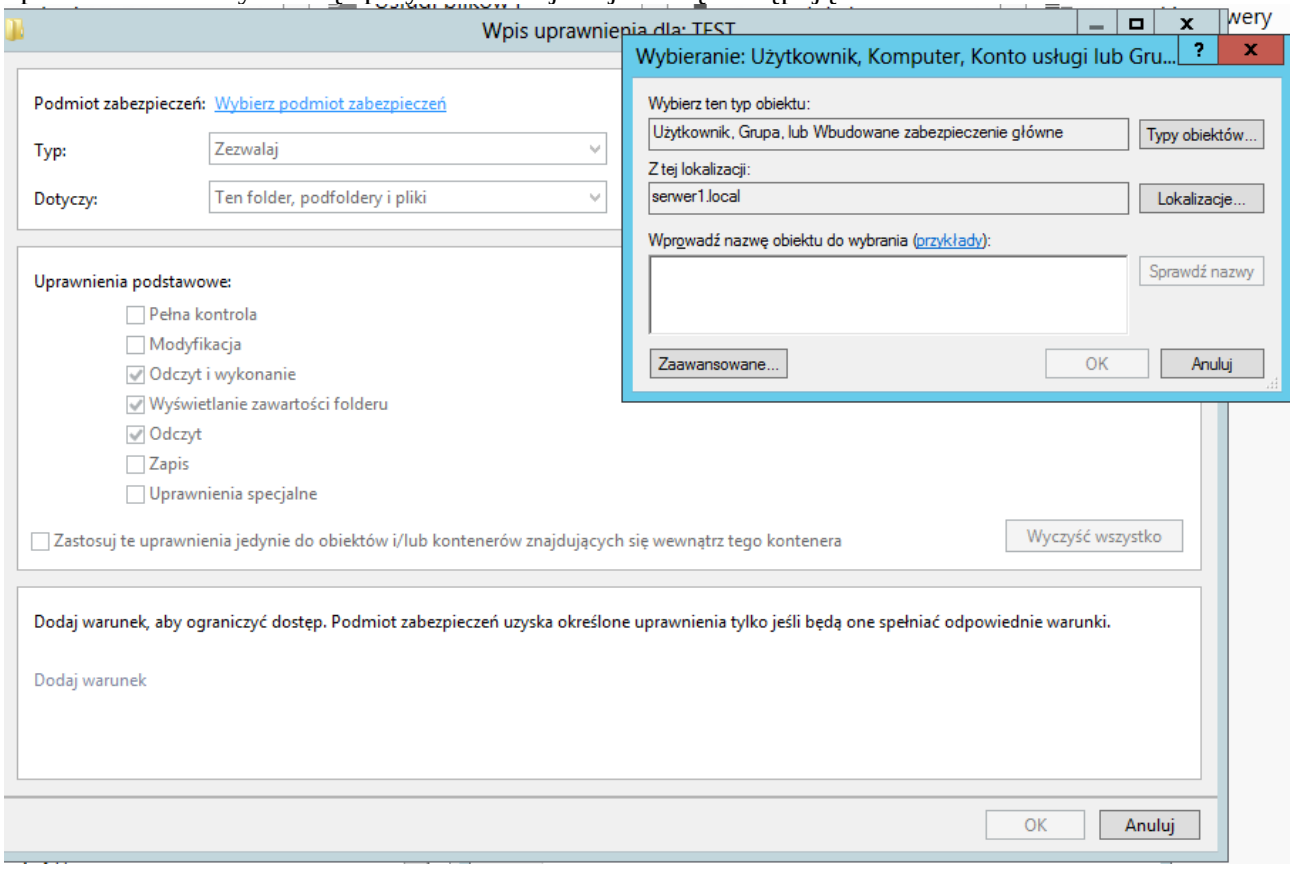
Jeżeli klikniemy przycisk Zaawansowane to pojawi się nowe okno:



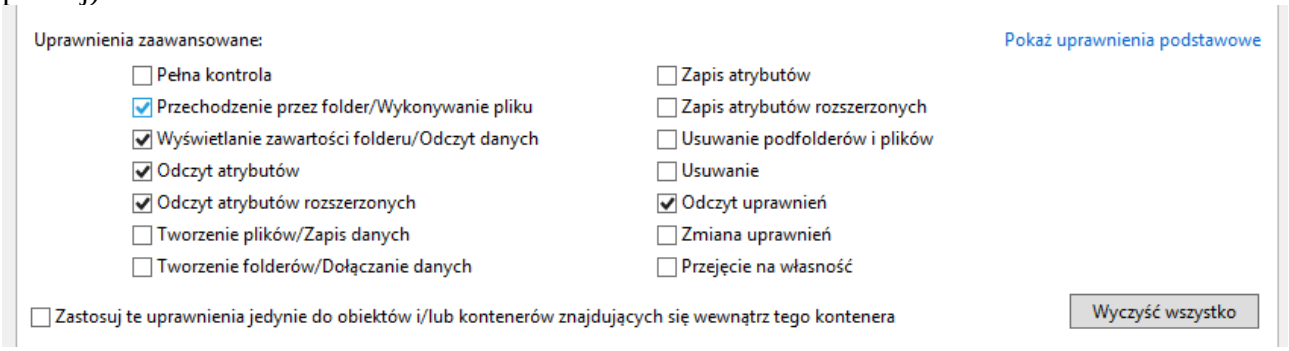
Opcja Właściciel pokazuje aktualnego właściciela zasobu. Pozwala go także zmienić (pole Zmień). Proszę zauważyć, że opcja ta chroniona jest przez UAC (User Access Control) – jest to zabezpieczenie by nikt niepowołany nie przejął pliku na własność (właściciel ma nieograniczony dostęp do katalogu/pliku).

Okno zawiera trzy zakładki – Uprawnienia, Inspekcja oraz Dostęp czynny.

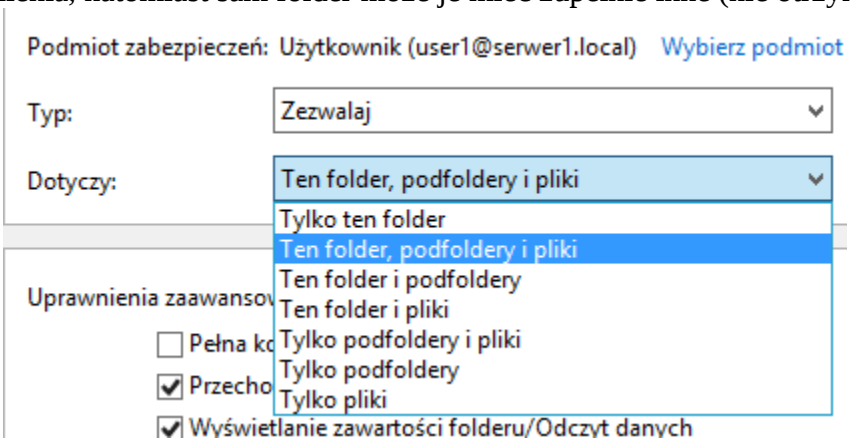
W uprawnieniach możemy dodawać kolejne uprawnienia dla grup/użytkowników. Aby dodać nowe uprawnienia należy kliknąć przycisk Dodaj. Pojawi się następujące okno:



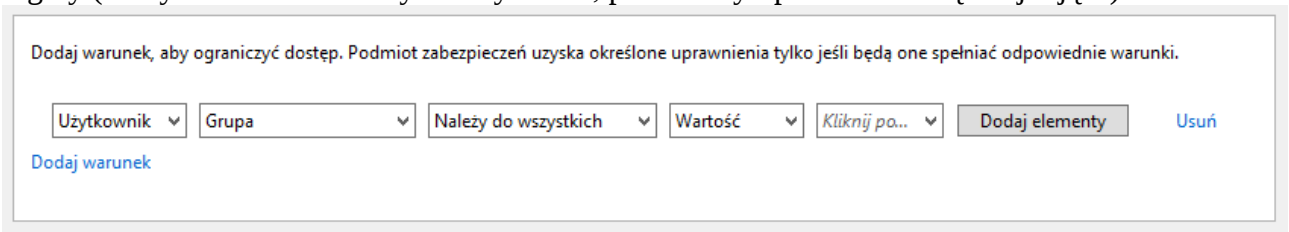
Podmiot zabezpieczeń to użytkownik lub grupa, dla której będziemy dodawać uprawnienie/uprawnienia (po kliknięciu na Wybierz podmiot zabezpieczeń pojawi się okno po prawej).



Możemy edytować uprawnienia podstawowe (opisane poprzednio) lub uprawnienia zaawansowane (pokazane na zrzucie powyżej). Możemy wybierać dowolne flagi (ustawienia). Jeżeli nie będą się pokrywać z którąkolwiek opcją przedstawioną w opisie przycisku Dodaj... (w odnośniku http://technet.microsoft.com/en-us/library/cc732880.aspx można znaleźć pełną tabelę uprawnień) to pole Dostęp na karcie Uprawnienia będzie zatytułowany „Specjalny”.
Opcja Zastosuj te uprawnienia jedynie do obiektów i/lub kontenerów znajdujących się wewnątrz tego kontenera spowoduje, że wszystkie pliki i foldery w danym folderze otrzymają ustawione przez nas uprawnienia, natomiast sam folder może je mieć zupełnie inne (nie otrzyma ich)!

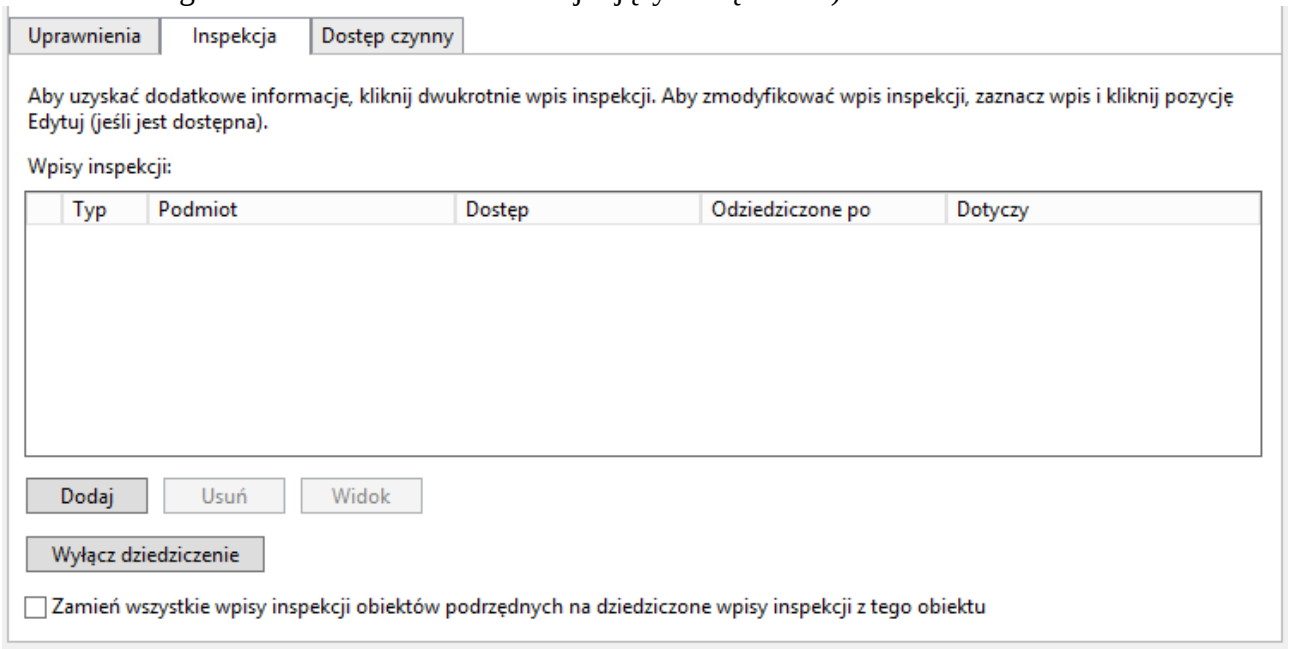


Typ może być tylko Zezwalaj lub Odmów (wtedy zaznaczone uprawnienia zostaną użytkownikowi/grupie odebrane). Pole Dotyczy pozwala określić jaki zasięg będą miały stosowane reguły (domyślnie aktualnie edytowany folder, podfoldery i pliki w nim się znajdujące).

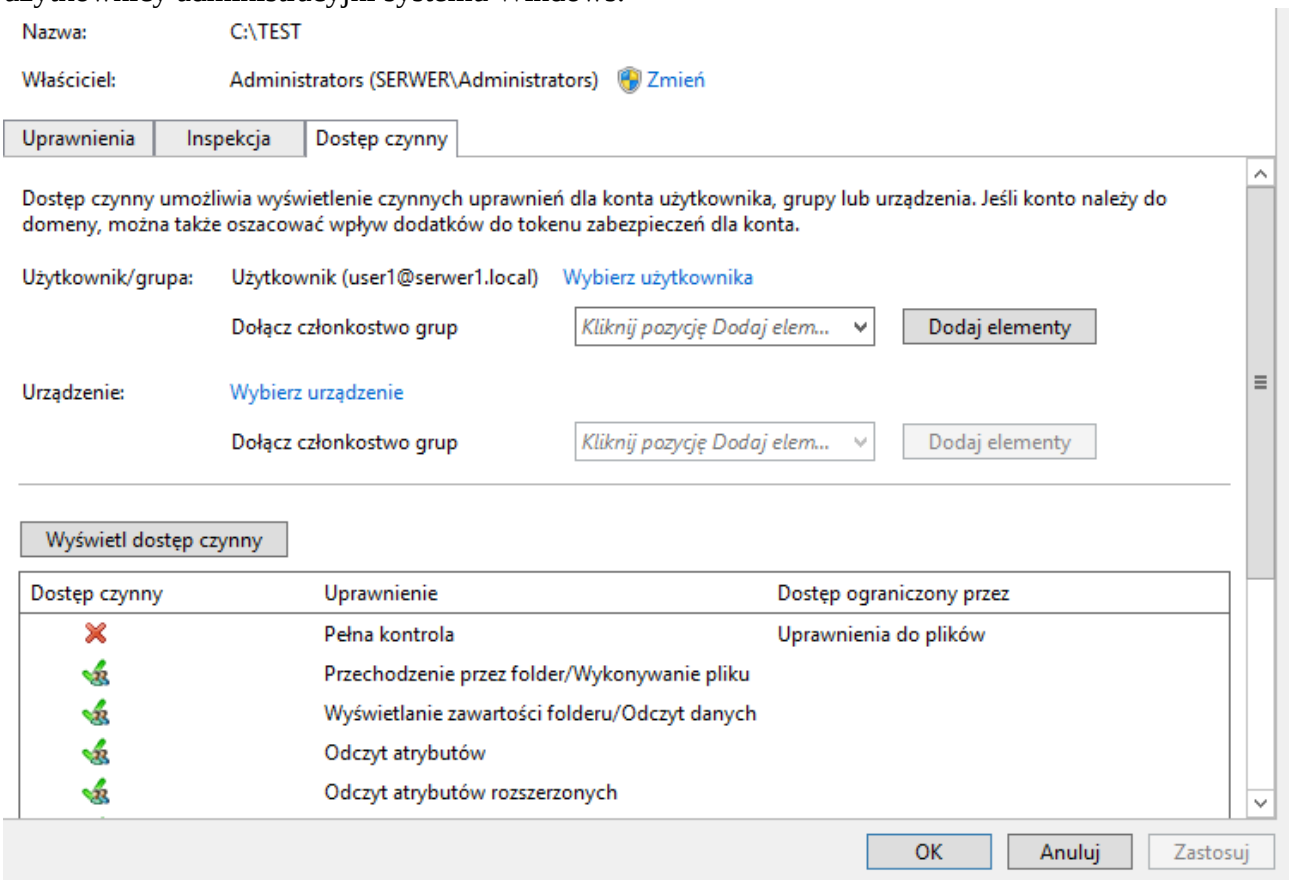


Warunek/warunki pozwalają ograniczać uprawnienia do określonych okoliczności, np. zostają one nadane jedynie w przypadku, gdy użytkownik należy do określonej grupy użytkowników (bądź korzysta z określonego urządzenia w sieci – konkretnej stacji roboczej podłączonej do domeny). Można dodawać kilka warunków, do których podłączymy kilka elementów, dla których będą one prawdziwe (tylko wtedy zostaną nadane uprawnienia). Proszę pamiętać, że nie można dodawać warunków dla typu ODMÓW.
Przycisk Wyłącz dziedziczenie jest szczególnie ważny w przypadku, gdy elementy nadrzędne posiadają dużą ilość podmiotów z szerokim zakresem uprawnień. System Windows (niestety) domyślnie przypisuje uprawnienia z kontenera nadrzędnego (w tym wypadku z dysku C:) co niekoniecznie jest pożądane/bezpieczne. Wyłączając dziedziczenie trzeba pamiętać, że można na sztywno przypisać wszystkie dotychczasowe uprawnienia (skopiować je do tego elementu) bądź

usunąć wszystkie odziedziczone (na pewno pozostanie właściciel oraz wprowadzone przez nas uprawnienia).
Zaznaczając Zamień wszystkie wpisy uprawnień obiektów podrzędnych na dziedziczone wpisy uprawnień z tego obiektu spowodujemy, że dla wszystkie pliki i katalogi w edytowanym zasobie odziedziczą uprawnienia właśnie z niego (w naszym wypadku dziedziczone byłyby uprawnienia nadane katalogowi TEST dla elementów znajdujących się w nim).



Zakładka Inspekcja wygląda podobnie do poprzedniej. Ustawienia w niej przebiegają identycznie jak w zakładce Uprawnienia. Różnica polega na tym, że ustawione wpisy inspekcji będą wywoływały zdarzenie w przypadku, gdy określony użytkownik/grupa z sukcesem uzyskają zezwolenie/odmowę do zasobów na określonych uprawnieniach. Zdarzenia te będą widzieć użytkownicy administracyjni systemu Windows.



Zakładka Dostęp czynny pozwala w trybie rzeczywistym monitorować nadane uprawnienia dla wskazanego podmiotu (można także sprawdzić uprawnienia dla wskazanego urządzenia). Czerwonym przekreśleniem zaznaczone są uprawnienia odebrane, zielonym zaznaczaniem uprawnienia nadane.

ZADANIA:

1. Należy wypróbować działanie listy uprawnień dla poszczególnych użytkowników systemu. Szczególnie ważne jest przetestowanie mechanizmu zmiany właściciela, zmiany dziedziczenia folderu nadrzędnego, nadanie dziedziczenia dla folderów podrzędnych oraz wypróbowanie uprawnień inspekcji (proszę znaleźć gdzie zapisywane/wyświetlane są ewentualne zdarzenia ustawionej inspekcji – pomocny artykuł http://technet.microsoft.com/pl-pl/library/inspekcja-i-zgodnosc-w-systemie-windows-server-2008.aspx). Zadanie należy wykonać zarówno dla katalogu nadrzędnego jak i pojedynczych plików w nim zawartych.
2. Sprawdzić, czy dla dysków lokalnych można nadawać/zdejmować uprawnienia. Jeżeli tak, to jakie, kto jest ich właścicielem itp. Jak traktowane są widoczne w kontenerze Komputer dyski twarde (jakiego typu)?

Powyższe operacje (zadania) można z powodzeniem wykonać także na systemie Windows 7/Windows 8.x (w nich także można ustawiać odpowiednie uprawnienia). Najlepszymi wersjami do tego zadania będą wersje Professional bądź wyższe.