

Spis treści

Systemy plików w Windows 10	2
Systemy plików.....	2
System FAT32	2
System NTFS	3
System ReFS.....	5
Zarządzanie dyskami.....	5
Tworzenie nowej partycji	6
Usuwanie partycji.....	6
Ustawienia programu Zarządzanie dyskami	6
Zmiana litery napędu.....	7
Typowe zadania zarządzania dyskami	7
Defragmentacja	8
Usuwanie niepotrzebnych plików.....	8
Uruchamianie komputera	8
Plik boot.ini.....	9
Boot Configuration Data	9
Zadania	10
Cechy charakterystyczne systemu plików NTFS v.5.....	11
Przydziały dyskowe	11
Kompresja danych na partycjach NTFS.....	11
Kompresja, a operacje dyskowe.....	11
Szyfrowanie z użyciem EFS (Encrypting File System)	12
<i>Rys. 4 Okno szyfrowania / kompresji pliku</i>	14
Odczyt / eksport certyfikatu użytkownika.....	15
<i>Rys. 6 Okno Wybierz użytkownika</i>	16
Import certyfikatu użytkownika.....	18
Zadania	19
Usługi.....	20
Tabela: 1. Usługi dostępne w systemie Windows.....	20
Zarządzanie usługami.....	27
Sposoby uruchamiania usług	28
Wybór konta użytkownika, którego usługa będzie używała do logowania	29
Akcje odzyskiwania	30

Zależności usług.....	31
Zadania	32

Systemy plików w Windows 10

Jednym z podstawowych zadań administratora jest zarządzanie dyskami. System Windows 10 posiada szereg narzędzi, które pozwalają na efektywne wykonywanie zadań administratorskich oraz na konfigurowanie zaawansowanych ustawień obejmujących takie zagadnienia, jak np. odporność na uszkodzenia.

Systemy plików

System Windows 10 został zaprojektowany w ten sposób, by umożliwiał korzystanie z wielu systemów plików, przez co zapewnia dostęp do już istniejących danych oraz aplikacji. Windows 10 obsługuje następujące systemy plików:

- FAT32,
- exFAT,
- CDFS,
- NTFS.

System FAT32

Microsoft wprowadzając na rynek system Windows 95 OSR2 wprowadził również nowy system plików o nazwie FAT32. Oprócz nadawania plikom długich nazw, system ten umożliwia tworzenie partycji o rozmiarach do 2TB. Klastry w systemie FAT32 są znacznie mniejsze niż w systemie FAT16, gdyż do ich adresowania wykorzystane są 32 bity, a nie 16 bitów. FAT32 używa 32-bitowych wpisów w tablicy alokacji plików, jednakże system Windows rezerwuje pierwsze cztery bity, co oznacza, że system FAT32 może teoretycznie posiadać maksymalnie 228 klastrów.

System exFAT

exFAT (Extended File Allocation Table, znany również jako FAT64) – system plików stworzony przez Microsoft specjalnie na potrzeby nośników zewnętrznych (np.: pamięci flash, dyski SSD, zewnętrzne dyski magnetyczne). Został zawarty w następujących systemach operacyjnych: Windows Embedded CE 6.0, Windows Vista z dodatkiem Service Pack 1, Windows 7, Windows Server 2008, Windows 8, Windows 8.1 i Windows 10. System plików domyślnie obsługuje system Mac OS X Snow Leopard 10.6.5 lub nowszy. W systemach Linux otrzymujemy możliwość odczytu i zapisu plików po

zainstalowaniu pakietów exfat. exFAT może być używany wszędzie tam, gdzie system plików NTFS nie jest najlepszym rozwiązaniem, na przykład ze względu na dużą nadmiarowość struktury danych i zaawansowany systemem zarządzania prawami dostępu i własności.

Unowocześnienia względem systemu plików FAT32:

- skalowalność do dużych rozmiarów dysków,
- limit wielkości pliku wynosi 264 bajtów (16 eksabajtów), dla FAT32 limit wynosił 232 bajtów (4 gigabajty),
- rozmiar klastra można zwiększyć do 32 MB,
- udoskonalono wydajność przy kopiowaniu/usuwaniu plików dzięki wprowadzeniu funkcji "free space bitmap" (indeksowanie pustej przestrzeni dyskowej dla poprawy wydajności zapisu plików),
- nieograniczona liczba plików w pojedynczym katalogu,
- system zarządzania prawami własności.

System NTFS

System NTFS został opracowany przez firmę Microsoft specjalnie dla systemu Windows NT. Od systemu Windows XP NTFS występuje w wersji 5, która oprócz elementów znanych z wcześniejszej wersji takich jak uprawnienia do plików i katalogów czy kompresja, posiada również możliwość szyfrowania danych oraz obsługę przydziałów dyskowych (quota). NTFS zapewnia wysoki poziom bezpieczeństwa danych zgromadzonych na dysku. Jest również systemem bardzo wydajnych.

Podobnie jak w systemach typu Unix czy Linux zapewnia przywileje dostępu na poziomie plików. Struktura woluminu NTFS przypomina system FAT z pewnymi różnicami. Została ona zaprezentowana na rysunku 1.

Informacje rozruchowe partycji	Główna tablica plików (MFT)	System	Pliki i katalogi (foldery)
--------------------------------	-----------------------------	--------	----------------------------

Rys. 1 Struktura woluminu NTFS

Informacje standardowe	Nazwa	Informacje zabezpieczeń	Dane i indeks
------------------------	-------	-------------------------	---------------

Rys. 2 Główna tablica partycji MFT

Główna tablica partycji MFT (Master File Table) jest bardzo podobna do tablicy alokacji plików znanej z systemu FAT. Zawiera jednakże znacznie więcej informacji. Struktura typowego wpisu w MFT została zaprezentowana na rysunku 2. Najważniejszym dodatkiem do MFT jest sekcja zabezpieczeń. Znajdują się tam informacje o tym, kto jest właścicielem pliku oraz o uprawnieniach, jakie mają inni użytkownicy w dostępie do tego pliku. Oprócz MFT kolejnym ważnym elementem, który występuje w

NTFS jest plik dziennika, służący do notowania aktywności dysku. Dzięki temu, w razie awarii system może odtworzyć spójność danych. Rozmiar tego pliku jest zależny od rozmiaru woluminu i może osiągnąć rozmiar nawet 4MB dla dużych woluminów.

Tabela1. Rozmiary klastrów w systemach plików			
Rozmiar woluminu	Rozmiar klastra FAT16	Rozmiar klastra FAT32	Rozmiar klastra NTFS
7 MB–16 MB	2 KB	Nie obsługiwany	512 bajtów
17 MB–32 MB	512 bajtów	Nie obsługiwany	512 bajtów
33 MB–64 MB	1 KB	512 bajtów	512 bajtów
65 MB–128 MB	2 KB	1 KB	512 bajtów
129 MB–256 MB	4 KB	2 KB	512 bajtów
257 MB–512 MB	8 KB	4 KB	512 bajtów
513 MB–1,024 MB	16 KB	4 KB	1 KB
1,025 MB–2 GB	32 KB	4 KB	2 KB
2 GB–4 GB	64 KB	4 KB	4 KB
4 GB–8 GB	Nie obsługiwany	4 KB	4 KB
8 GB–16 GB	Nie obsługiwany	8 KB	4 KB
16 GB–32 GB	Nie obsługiwany	16 KB	4 KB
32 GB–2 TB	Nie obsługiwany	Nie obsługiwany	4 KB

- Woluminy FAT mniejsze od 16 megabajtów (MB) są formatowane jako FAT12.

- Woluminy FAT16 większe niż 2 gigabajty (GB) nie są dostępne dla komputerów używających systemu MS-DOS, Windows 95, Windows 98 i wielu innych.
- Mimo że woluminy FAT32 mogą teoretycznie osiągać rozmiar aż do 2 terabajów (TB), to w systemie Windows istnieje ograniczenie rozmiaru formatowanego woluminu FAT32 do 32 gigabajtów. System Windows może jednak odczytywać i zapisywać większe woluminy FAT32, które zostały sformatowane w innych systemach operacyjnych.
- Implementacja systemu FAT32 w systemie Windows ogranicza maksymalną liczbę klastrów woluminu FAT32, który może zostać zainstalowany, do 4.177.918. Jest to maksymalna ilość klastrów w woluminie FAT32, która może zostać sformatowana w systemie Windows 98.
- Woluminy NTFS mogą teoretycznie osiągać rozmiar aż do 16 eksabajtów (EB), ale w praktyce są ograniczone do 2 terabajtów.
- Użytkownik może określić rozmiar klastra podczas formatowania woluminu NTFS. Kompresja NTFS nie jest jednak obsługiwana w przypadku klastrów większych niż 4 kilobajty (KB).

System ReFS

Aby wyeliminować słabe strony NTFS, Microsoft w Windows od wersji 8 wprowadził ReFS (Resilient File System, ang. wytrzymały system plików). Do otwierania, zamykania, odczytywania oraz zapisywania danych nowy system operacyjny wykorzystuje to samo API co w przypadku NTFS. Producenci oprogramowania do backupu albo partycjonowania mogą niewielkim nakładem pracy dodać obsługę ReFS.

Wiele dobrze znanych funkcji, takich jak szyfrowanie za pomocą BitLockera albo dowiązania symboliczne do bibliotek, pozostanie zachowanych, podczas gdy inne, np. kompresja danych, znikną. Sporo nowych rozwiązań ReFS dotyczy tworzenia struktury plików i folderów oraz zarządzania nią.

Funkcje te są ukierunkowane na automatyczne korygowanie błędów, ekstremalną skalowalność i działanie w trybie always online. Microsoft wykorzystuje do tego celu koncepcje stosowane w przypadku baz danych, takie jak drzewa B+. Foldery mają strukturę tabel z plikami pełniącymi rolę wpisów. Te mogą otrzymywać określone atrybuty wstawiane jako subtabele, w ogólnym obrazie powstaje hierarchiczna struktura drzewiasta. Nawet do zarządzania wolną przestrzenią wykorzystywane są tabele. W efekcie mamy do czynienia z wydajną architekturą, którą da się dobrze skalować. Centrum ReFS stanowi tabela obiektów będąca spisem treści wszystkich tabel w systemie plików.

Zarządzanie dyskami

Narzędzie Zarządzanie dyskami jest graficznym narzędziem, służącym do wykonywania różnych zadań związanych z zarządzaniem dyskami. Narzędzie to znajduje się w konsoli **Zarządzanie komputerem**.

Jest to więc jedna z przystawek konsoli MMC. Do podstawowych zadań, które można tym narzędziem wykonać zaliczamy:

- tworzenie, formatowanie i usuwanie partycji,
- monitorowanie i wyświetlanie informacji o partycjach,
- skanowanie i naprawa błędów dyskowych,
- zmiana rozmiarów partycji.

Aby mieć dostęp do tego narzędzia należy posiadać uprawnienia administratora.

Tworzenie nowej partycji

W celu utworzenia partycji na dysku, należy wykonać następujące kroki:

1. Wybrać wolną przestrzeń przeznaczoną na partycję. Wolny obszar dysku wyświetlany jest jako zakreskowany pasek.
2. Na wybranym obszarze należy kliknąć prawym klawiszem myszy i wybrać polecenie *Utwórz partycję*. W wyświetlonym oknie dialogowym należy wybrać typ partycji (podstawowa, rozszerzona, dysk logiczny w partycji rozszerzonej).
3. Następnie należy postępować z poleceniami kreatora.

Usuwanie partycji

W celu usunięcia partycji z dysku, należy kliknąć na niej prawym klawiszem myszy i z rozwiniętego menu wybrać polecenie *Usuń partycję*. W ten sposób nie da się usunąć partycji systemowej Windows. Usunięcie partycji jest trwałe i powoduje utratę informacji na niej zawartych.

Ustawienia programu Zarządzanie dyskami

Narzędzie **Zarządzanie dyskami** pozwala użytkownikowi na wyświetlenie danych w trzech widokach. Możliwość ta dotyczy zarówno sekcji górnej, jak i dolnej. Aby zmienić widok dysków w sekcji górnej i dolnej należy wybrać odpowiednią opcję z menu **Widok**. Dzięki temu możemy dostosować wygląd tego narzędzia odpowiednio do naszych potrzeb. Bardzo wygodnym rozwiązaniem jest również możliwość sortowania wyświetlonych informacji według wybranej kolumny. Odbyna się to poprzez kliknięcie nagłówka kolumny, według której chcemy posortować. Powtórne kliknięcie spowoduje posortowanie w kolejności odwrotnej.

Możliwe jest również ustawienie własnych kolorów wyświetlanych w widoku graficznym. Aby móc zmienić kolory, należy z menu **Widok** wybrać polecenie *Ustawienia*. W wyświetlonym oknie dialogowym można ustawiać kolor takich elementów jak: obszar nieprzydzielony, partycja podstawowa, partycja rozszerzona, wolne miejsce, itp.

Podobnie można konfigurować wygląd samego programu **Zarządzanie dyskami**. W tym celu należy wybrać z menu **Widok** pozycję *Dostosuj*.

Zmiana litery napędu

Aby zmienić literę, jaka jest przyporządkowana partycji lub napędowi CD należy kliknąć na interesującym nas woluminie i wybrać z menu pozycję *Zmień literę dysku i ścieżkę*. Należy jednak uważać przy zmianie litery przypisanej woluminom, na których zainstalowano jakieś programy. Zmiana litery nie zmodyfikuje ani rejestru Windows, ani plików inicjalizujących (.ini), które są używane przez zainstalowane programy. W przypadku wystąpienia takiej zmiany, Windows może spróbować odszukać odpowiedni program na dysku i poprawić ścieżkę dostępu do niego.

Samodzielne przypisanie litery do dysku spowoduje że zostanie ona „przyczepiona” do dysku. Oznacza to, że nie zmieni się przy dodawaniu i usuwaniu woluminów, tak długo jak same litery przypisanej do tego napędu nie zmienimy.

Warto zauważyć, iż w przypadku gdy dodajemy dysk z partycjami podstawowymi, Windows przetasowuje litery w taki sposób, aby partycje podstawowe miały jak najniższe litery. Można temu zaradzić samodzielnie przypisując litery odpowiednim partycjom.

Typowe zadania zarządzania dyskami

Do typowych zadań zarządzania dyskami należą takie czynności jak sprawdzanie stanu dysku, defragmentacja dysku, wykonywanie kopii bezpieczeństwa danych, usuwanie zbędnych plików lub też udostępnianie katalogów innym użytkownikom.

System Windows posiada odpowiednie narzędzia pozwalające wykonać te czynności. Zostaną one krótko omówione w tej części. Do narzędzi tych można się dostać na kilka sposobów. Najprostszy sposób to dwukrotne kliknięcie na ikonie **Mój komputer** znajdującej się na pulpicie, a następnie kliknięcie prawym klawiszem na interesującej nas partycji i wybranie polecenia **Właściwości**. Innym sposobem jest kliknięcie w lewym dolnym rogu ekranu prawym klawiszem myszy i wybranie odpowiedniej opcji z menu kontekstowego. Okno dialogowe z właściwościami danej partycji można również wywołać poprzez kliknięcie prawym klawiszem myszy wybranej partycji w narzędziu **Zarządzanie dyskami**.

Defragmentacja

Partycje oparte na systemie NTFS nie ulegają aż tak dużej fragmentacji jak partycje FAT. NTFS jest systemem plików, który dużo lepiej radzi sobie z tym zjawiskiem. Fragmentacja jest to zjawisko, które występuje wtedy, gdy części jednego z plików rozrzucone są w różnych miejscach na dysku. Aby zlikwidować występującą fragmentację danych system Windows został wyposażony w narzędzie **Defragmentator dysków**. Jest to okrojona wersja programu **Disk Keeper**. Aby przeprowadzić defragmentację, należy wywołać okno dialogowe właściwości żądanej partycji i w zakładce **Narzędzia** wybrać element **Optymalizacja**.

Defragmentator może być również wywołany jako przystawka konsoli MMC.

Usuwanie niepotrzebnych plików

W trakcie pracy z systemem Windows może się zdarzyć sytuacja, że na dysku będą się znajdować zbędne pliki. Aby zwolnić miejsce, które zajmują te pliki, należy skorzystać z programu **Oczyszczanie dysku**. Program ten przeszukuje wybrany dysk i wyświetla następnie listę plików, które mogą zostać bezpiecznie usunięte.

Aby uruchomić ten program należy w menu **Start** wpisać **Oczyszczanie dysku** (Disk Cleanup).

Uruchamianie komputera

Proces uruchamiania przebiega według następującej procedury:

1. Uruchamiane są testy początkowe (power-on test).
2. Odszukiwany jest dysk startowy i odczytywana jest zawartość pierwszego sektora (MBR – Master Boot Record), aby ustalić nazwę programu, który należy uruchomić. Ponieważ rekord MBR ma ograniczoną pojemność następuje więc przekierowanie do programu NTLDR. Jest to program ładujący Windows.
3. NTLDR jest wprowadzany do pamięci i uruchamiany. Przełącza on model pamięci na płaski, dzięki czemu ignorowany jest limit 640kB pamięci i jest ona traktowana jako jeden blok.
4. Uruchamiany jest odpowiedni mini system plików obsługujący wolumeny systemu Windows.
5. Następuje odczyt pliku BOOT.INI i wyświetlona zostaje lista dostępnych systemów operacyjnych. Automatyczna selekcja nastąpi po upływie czasu podanego w linii konfiguracyjnej pliku BOOT.INI.

6. Po wybraniu określonej wersji systemu Windows, NTLDR uruchamia NTDETECT.COM, który przeprowadza test systemu podobny do procedury POST. W jego trakcie rozpoznaje aktualnie zainstalowany sprzęt i sporządza listę, która jest przekazywana z powrotem do NTLDR. Loader system Windows próbuje załadować wybraną wersję systemu Windows, drzewo sprzętu natomiast zostaje zapisane do rejestru do klucza HKEY_LOCAL_MACHINE\HARDWARE.
7. Następnie NTLDR odnajduje i ładuje jądro systemu NTOSKRNL.EXE i przekazuje mu informację o sprzęcie przygotowane przez NTDETECT.COM. Po załadowaniu jądra wraz z biblioteką HAL.DLL następuje przekazanie mu sterowania. W tym miejscu ładowane są właściwe sterowniki, ale nie są one inicjalizowane
8. Następuje inicjalizacja załadowanych wcześniej sterowników. Ponadto ładowane i inicjalizowane są pozostałe sterowniki.
9. Uruchamiane są wymagane podsystemy m.in. podsystem Windows WIN64 odpowiedzialny za kontrolę nad portami wejścia/wyjścia oraz ekranem.
10. Następnie uruchomiona zostaje aplikacja WINLOGON.EXE. Uruchamia ona lokalnego administratora zabezpieczeń LSASS.EXE. Na ekranie pojawia się wówczas ekran z komunikatem logowania do systemu.
11. Użytkownik może się więc już zalogować do systemu, proces startowy jest nadal kontynuowany i pozostałe usługi zostaną rozpoczęte w tle. Po prawidłowym zalogowaniu użytkownika, procedura startowa oceniana jest jako poprawna.

Plik boot.ini

We wcześniejszych wersjach systemu Windows plik boot.ini był plikiem systemowym, który zawierał informacje o systemach operacyjnych Windows zainstalowanych na komputerze. Informacje te były wyświetlane podczas procesu uruchamiania po włączeniu komputera. Było to najbardziej przydatne w konfiguracjach uruchamiania wielu systemów operacyjnych lub dla użytkowników zaawansowanych bądź administratorów, którzy potrzebowali dostosować sposób uruchamiania systemu Windows.

Boot Configuration Data

W nowszych systemach Windows plik boot.ini został zastąpiony plikiem danych konfiguracji rozruchu (BCD, Boot Configuration Data). Ten plik jest bardziej uniwersalny niż plik boot.ini i można zastosować go w przypadku platform komputerowych, które używają innych sposobów uruchamiania komputera niż system BIOS (basic input/output system, system podstawowych operacji wejścia/wyjścia).

Jeżeli wymagane są zmiany w danych konfiguracji rozruchu, takie jak usunięcie wpisów z listy wyświetlanych systemów operacyjnych, należy użyć narzędzia wiersza poleceń Bcdedit - zaawansowanego narzędzia przeznaczonego dla administratorów i specjalistów IT.

Jeżeli komputer jest skonfigurowany do uruchamiania wielu systemów operacyjnych, nadal można zmienić za pomocą apletu System w Panelu sterowania, który system operacyjny Windows ma być uruchamiany domyślnie i jak długo ma być wyświetlana lista systemów operacyjnych. Otwórz okno System z panelu sterowania. W lewym okienku kliknij łącze Zaawansowane ustawienia systemu. Wymagane uprawnienia administratora. Jeśli zostanie wyświetlony monit o hasło administratora lub potwierdzenie, wpisz hasło lub potwierdź. Kliknij kartę Zaawansowane, a następnie w obszarze Uruchamianie i odzyskiwanie kliknij przycisk Ustawienia. W obszarze Uruchamianie systemu wybierz domyślny system operacyjny i czas wyświetlania listy systemów operacyjnych, kliknij przycisk OK, a następnie kliknij przycisk OK ponownie.

Zadania

1. Jakie systemy plików obsługuje Windows 10?
2. Czy Windows 10 może być uruchamiany z partycji FAT32?
3. Opisz procedurę utworzenia partycji.
4. Czy można usunąć partycję systemową?
5. Jakie możliwości konfiguracyjne ma program Zarządzanie dyskami?
6. Czy można zmienić literę przypisaną partycji, na której zainstalowany jest system? Jaka będzie reakcja systemu?
7. Przypisz napędowi CD literę I.
8. Podmontuj napęd CD-ROM do katalogu c:\cd.
9. Utwórz nową partycję FAT32 o rozmiarze do 500MB i sformatuj ją. Przydziel jej literę D i ustaw jej etykietę na moja.
10. Zmień rozmiar utworzonej partycji na 700 MB. Czy da się to zrobić bez straty danych?
11. Skonwertuj partycję D (moja) na system plików NTFS bez utraty danych. W tym celu przed przystąpieniem do konwersji utwórz dowolny dokument na partycji D. Sprawdź dane po zakończeniu konwersji.
12. Uruchom defragmentację dysku na Twoim komputerze?
13. Przeprowadź proces analizowania. Jaki będzie jej efekt?
14. Wymień inne sposoby wywołania Defragmentator dysków, oprócz tych wymienionych w tekście.
15. Uruchom narzędzie Oczyszczanie dysku?
16. Przeanalizuj procedurę uruchamiania systemu znajdującego się na Twoim komputerze?

Cechy charakterystyczne systemu plików NTFS v.5

Przydziały dyskowe

W systemie Windows 10 funkcjonuje mechanizm przydziałów dyskowych (quota). Mechanizm ten daje administratorowi możliwość nadawania przydziałów dyskowy dla użytkowników oraz grup. Dzięki temu, możemy ograniczyć przestrzeń dyskową, z której mogą korzystać użytkownicy lub grupy.

Aby określić przydział, należy wykonać następujące kroki:

1. Kliknąć prawym klawiszem myszy na obiekcie (folder lub wolumin), na który mają być nałożone ograniczenia przydziałów i wybrać z menu kontekstowego polecenie Właściwości.
2. Następnie należy wybrać zakładkę Przydziały.
3. Następnie należy zaznaczyć pole Włącz zarządzanie przydziałami.
4. Kolejnym krokiem jest naciśnięcie przycisk Wpisy przydziałów i w wyświetlonym oknie ustalenie właściwych przydziałów. Aby dodać nowy przydział, należy wybrać pozycję Nowy wpis przydziału z menu Przydział.
5. Następnie należy dodać użytkowników lub grupy, dla których chcemy dodać przydział i nacisnąć klawisz OK.
6. W wyświetlonym oknie należy określić opcje przydziału dla wybranego użytkownika lub grupy i nacisnąć przycisk OK.

Kompresja danych na partycjach NTFS

W systemie Windows 10 kompresji mogą podlegać tylko dane niezaszyfrowane. Możliwe jest oddzielne określanie kompresji folderu i plików. Możliwe jest więc wystąpienie sytuacji, że skompresowany folder będzie zawierał nieskompresowane pliki oraz nieskompresowany folder będzie zawierał skompresowane pliki. System plików NTFS podaje zawsze rozmiar pliku po ewentualnej kompresji. Istnieje możliwość włączenia opcji wyróżniania plików skompresowanych. System kompresji jest dla aplikacji "przezroczysty", tzn. pliki skompresowane przed udostępnieniem ich pewnej aplikacji są rozpakowywane. Po zamknięciu lub zapisaniu pliku jest on kompresowany ponownie.

Kompresja, a operacje dyskowe

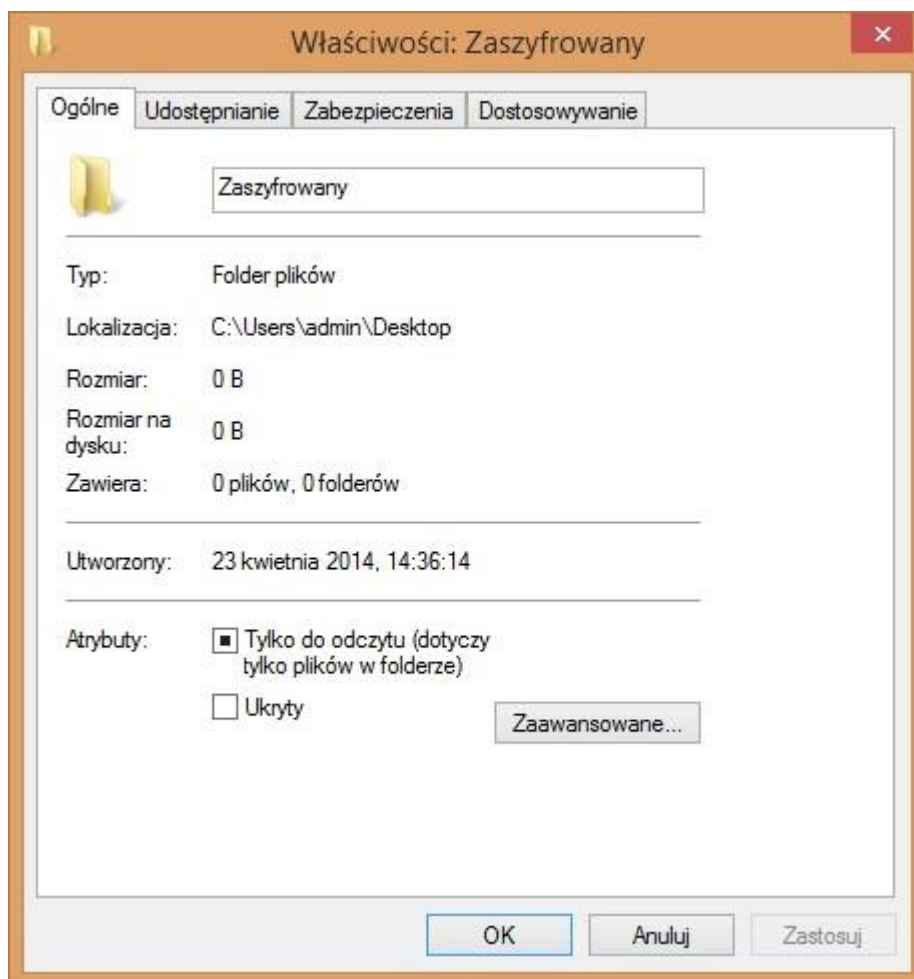
- plik przenoszony w ramach jednej partycji NTFS zachowuje atrybut kompresji,
- plik kopiowany lub przenoszony z partycji dowolnego typu, dziedziczy atrybut kompresji katalogu nadrzędnego, w którym będzie się znajdował,

- plik kopiowany lub przenoszony na partycję inną, niż NTFS nie będzie kompresowany, ▪
kopiowanie pliku skompresowanego odbywa się trójstopniowo: rozpakowanie pliku, skopiowanie rozpakowanego pliku, kompresja pliku docelowego.

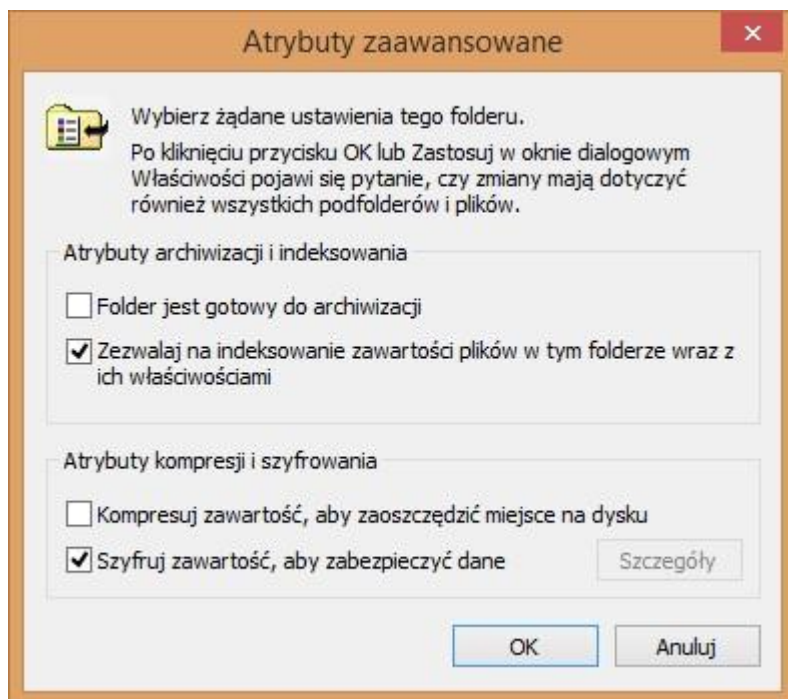
Szyfrowanie z użyciem EFS (Encrypting File System)

- Operacje szyfrowania i deszyfrowania są przeprowadzane w tle i są niewidoczne dla użytkowników aplikacji. Podczas używania pliku jest on automatycznie deszyfrowany i szyfrowany ponownie podczas zapisu na dysk.
- EFS umożliwia dostęp do zaszyfrowanego pliku tylko autoryzowanemu użytkownikowi.
- Administrator może odzyskać plik zaszyfrowany przez dowolnego użytkownika.
- EFS posiada wbudowany system odzyskiwania danych. Z szyfrowania danych można korzystać wyłącznie jeśli w systemie istnieje przynajmniej jeden klucz odzyskiwania. EFS automatycznie generuje klucze odzyskiwania i umieszcza je w rejestrze systemu, gdy nie jest możliwy dostęp do domeny.
- Wymagany jest przynajmniej jeden agent odzyskiwania EFS. Można wyznaczyć dowolną liczbę agentów do zarządzania programem odzyskiwania EFS. Każdy agent wymaga posiadania certyfikatu EFS Recovery Agent.
- Szyfrowanie danych i ich kompresja wykluczają się wzajemnie. Niemożliwa jest bowiem kompresja danych zaszyfrowanych.
- Po zaszyfrowaniu folderu, pliki w nim zapisane będą automatycznie szyfrowane. Pliki szyfrowane są blokami, przy pomocy innych kluczy do szyfrowania każdego bloku. Do szyfrowania wykorzystywany jest szybki algorytm wykorzystujący klucze symetryczne. Klucze przechowywany jest w polu DDF (Data Decryption Field) oraz DRF (Data Recovery Field), znajdujących się w nagłówku pliku.
- Podczas otwierania zaszyfrowanego pliku, system EFS automatycznie wykrywa szyfrowanie i wyszukuje certyfikat użytkownika oraz powiązany z nim klucz prywatny. EFS wykorzystuje ten klucz do deszyfrowania pola DDF i odblokowania listy kluczy szyfrujących, co pozwala na jawne wyświetlenie zawartości pliku.
- Możliwa jest zmiana nazwy pliku po zaszyfrowaniu.
- Przy przenoszeniu pliku z folderu zaszyfrowanego do niezaszyfrowanego na tej samej partycji plik pozostaje zaszyfrowany.
- Dostęp do zaszyfrowanego pliku jest zakazany wszystkim użytkownikom, poza właścicielem klucza prywatnego. Tylko właściciel klucza lub agent EFS może odszyfrować plik. Użytkownik nie posiadający klucza prywatnego nie będzie mógł odczytać zawartości pliku nawet, gdy uzyska do niego dostęp (np. mając prawo Take Ownership).

- Jeśli klucz prywatny właściciela pliku jest niedostępny, agent odzyskiwania może otworzyć zaszyfrowany plik, wykorzystując swój klucz prywatny do pola DRF i odblokowując w ten sposób listę kluczy szyfrujących pliku.

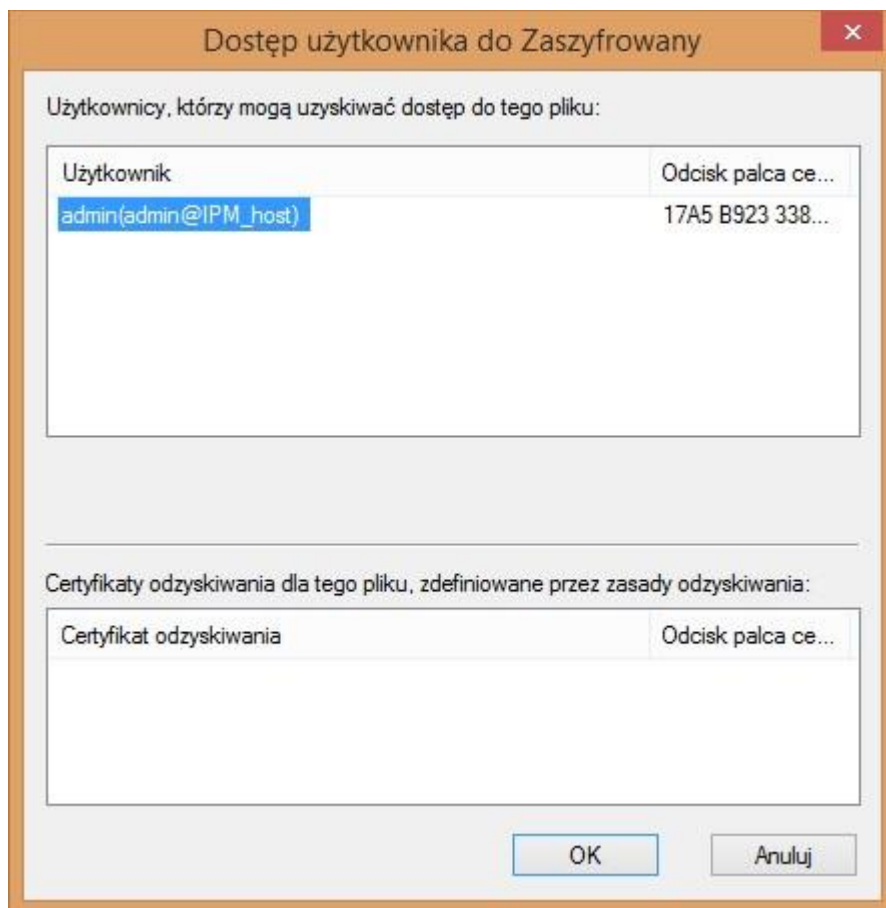


Rys. 3 Okno właściwości pliku



Rys. 4 Okno szyfrowania / kompresji pliku

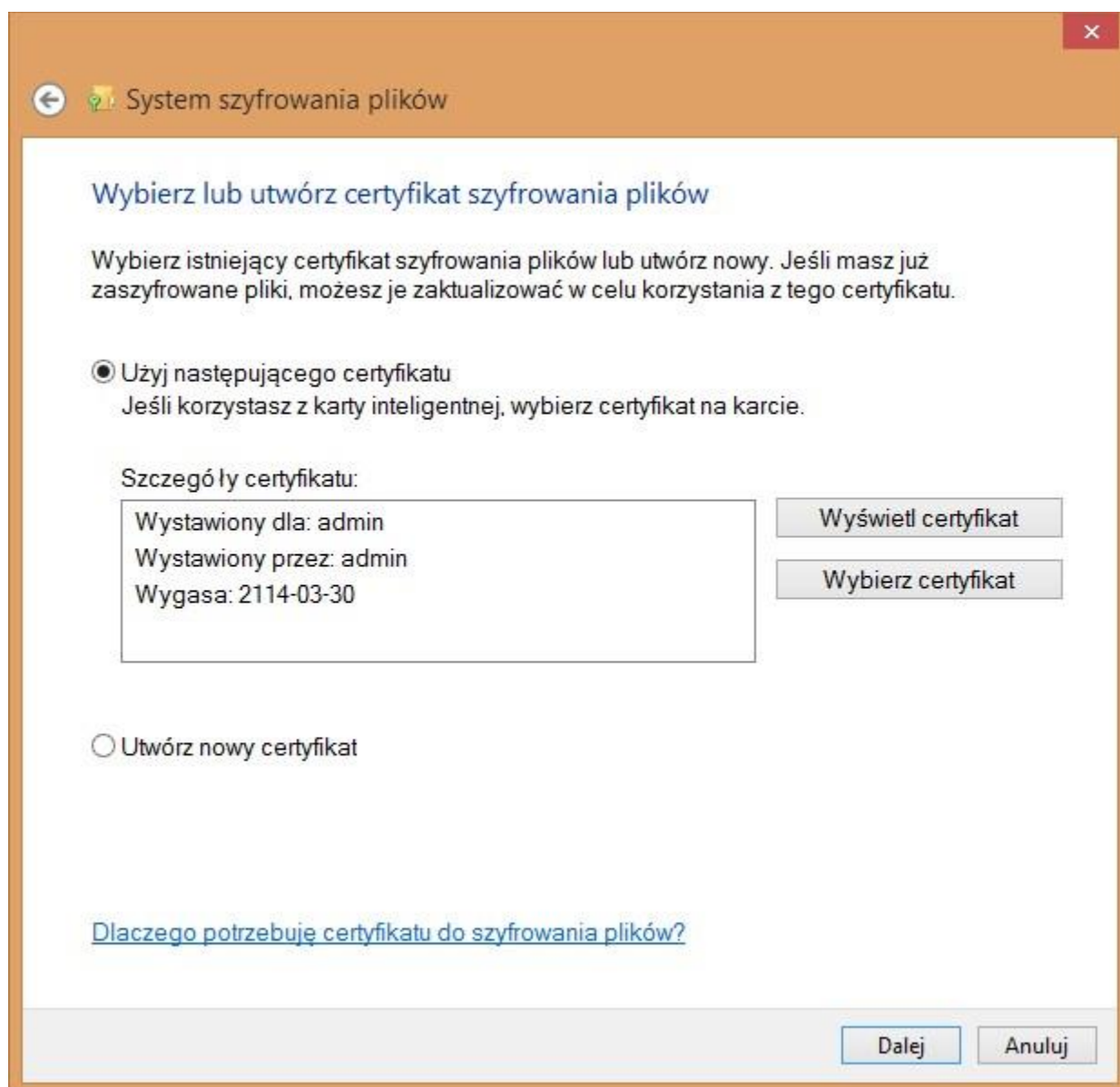
Po zaakceptowaniu i wykonaniu procesu szyfrowania, w oknie z rys. 4 można teraz wybrać polecenie **Szczegóły**, aby dowiedzieć się, jacy użytkownicy z jakimi certyfikatami mogą uzyskać dostęp do szyfrowanego pliku.



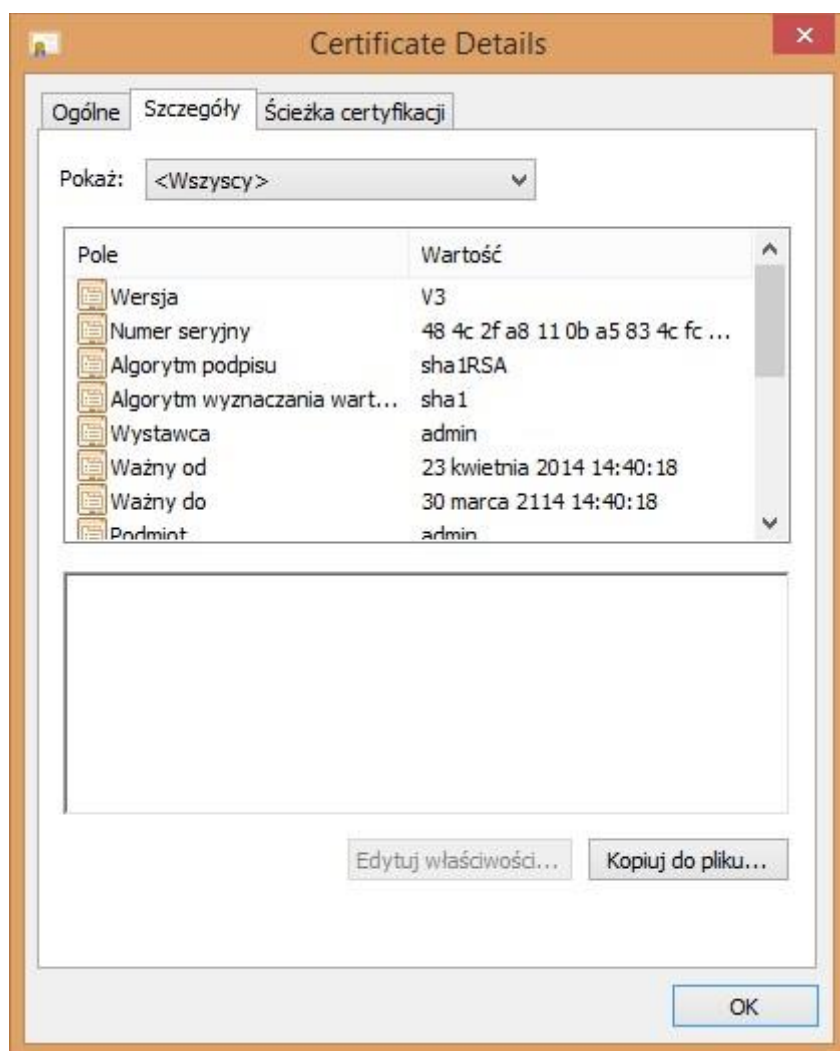
Rys. 5 Okno Szczegóły szyfrowania

Odczyt / eksport certyfikatu użytkownika

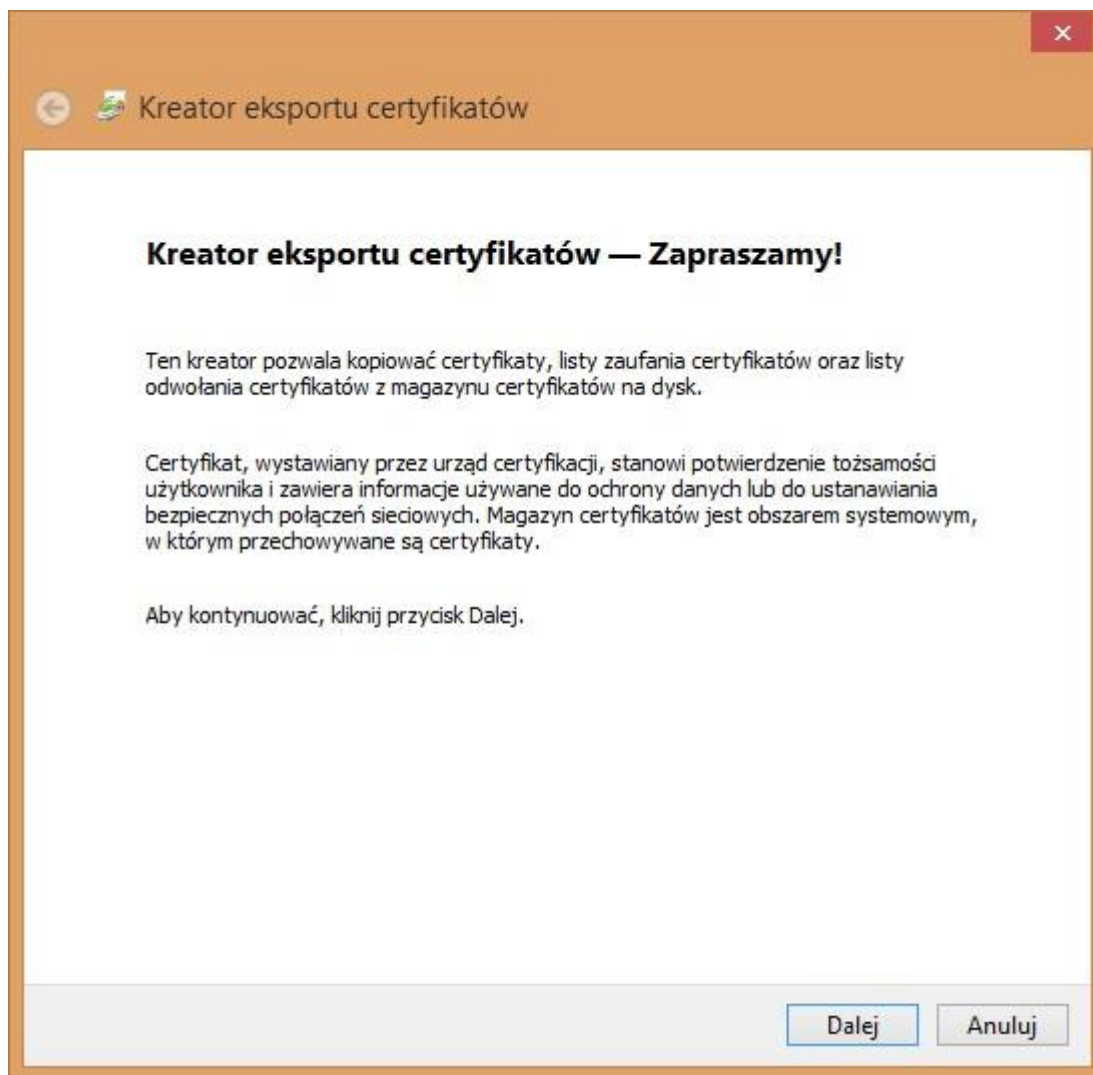
1. W menu Start należy wpisać część nazwy aplikacji **Zarządzaj certyfikatami szyfrowania plików**, uruchomić ją i kliknąć "Dalej",
2. Następnie Wybierz certyfikat (Rys 6) i zakładka Szczegóły (Rys. 7)
3. W celu wyeksportowania certyfikatu należy wcisnąć przycisk kopiuj do pliku (Rys. 8)



Rys. 6 Okno Wybierz użytkownika



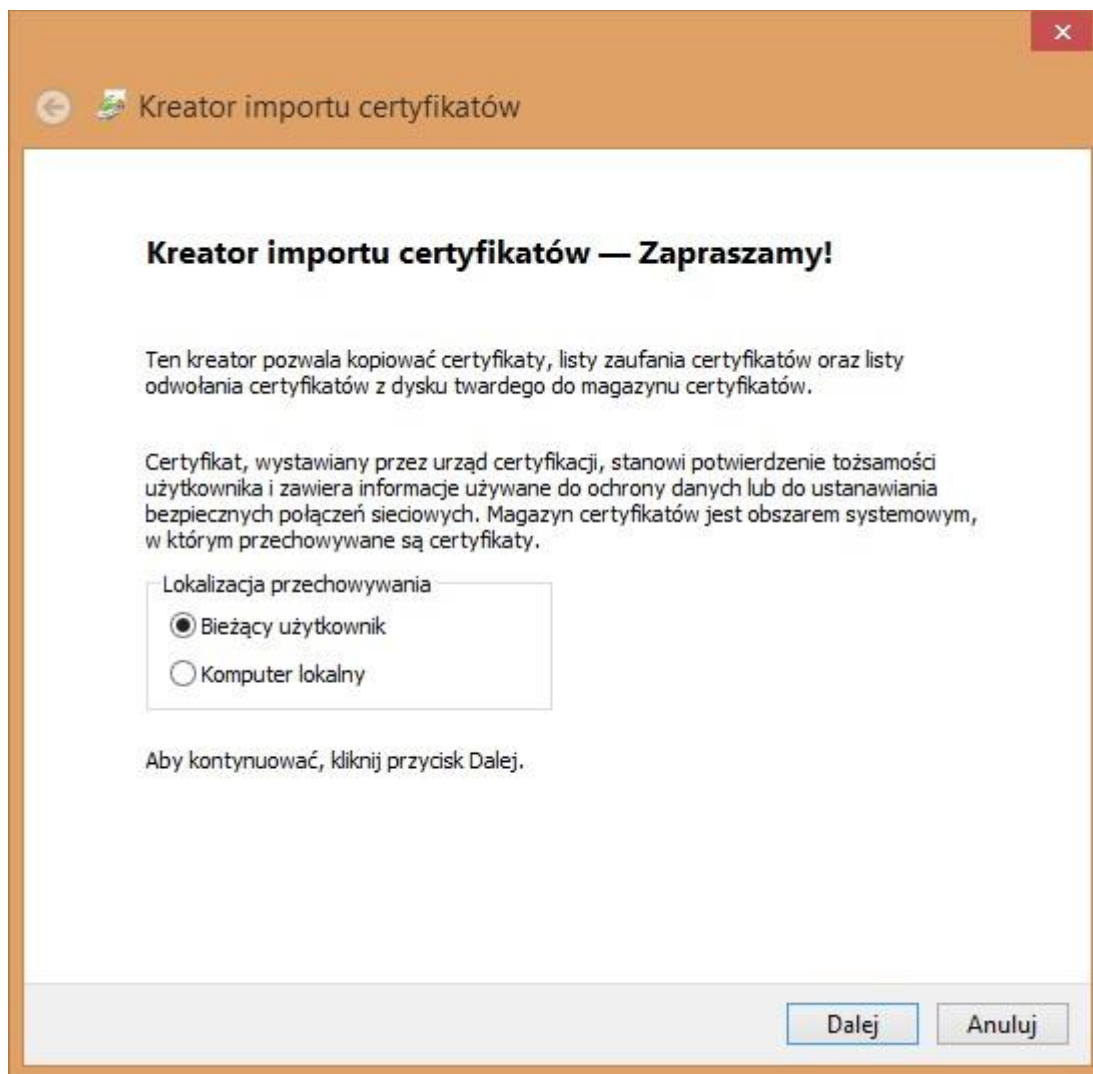
Rys. 7 Okno certyfikatu użytkownika



Rys. 8 Okno eksportu certyfikatu użytkownika

Import certyfikatu użytkownika

Wygenerowany plik z kluczem prywatnym danego użytkownika należy zaimportować. Użytkownik, który zaimportuje taki klucz będzie miał prawo do odczytywania zaszyfrowanych plików. Należy uruchomić plik z rozszerzeniem .pfx (np. dwukrotne kliknięcie myszy) w celu rozpoczęcia operacji importu. Pojawia się okno dialogowe kreatora importu (Rys. 9).



Rys. 9 Okno importu certyfikatu użytkownika

Należy podać hasło, którym zabezpieczono plik .pfx w czasie operacji eksportowania.

Zadania

1. Do czego służą przydziały dyskowe?
2. Utwórz dla konta guest ograniczenie 2 MB z poziomem ostrzeżeń na poziomie 1.5 MB.
Zaloguj się na konto guest i przetestuj działanie przydziałów w praktyce.
3. Jako jeden użytkownik np. usr1 zaszyfruj dwa nowe dowolne pliki
4. Upewnij się, że do tego pliku wszyscy użytkownicy mają prawo pełnej kontroli
5. Wyeksportuj swój klucz prywatny do pliku .pfx
6. Zaloguj się jako inny użytkownik np. usr2
7. Zobacz, czy możesz teraz odczytać zawartość zaszyfrowanych plików
8. Skasuj jeden z nich. Można?

9. Zaimportuj klucz prywatny poprzedniego użytkownika
10. Zobacz, czy teraz możesz odczytać zawartość zaszyfrowanego pliku.

Usługi

Usługa jest to proces służący do uruchamiania określonych funkcji systemowych. Nawet w momencie, gdy użytkownik loguje się do systemu w tle mogą być ciągle uruchamiane pewne usługi systemowe. Te usługi umożliwiają funkcjonowanie drugiego planu systemu Windows. Mogą one być automatycznie uruchamiane podczas startu systemu albo też uruchamiane ręcznie za pośrednictwem apletu znajdującego się w **Narzędziach administracyjnych** lub jako jedna zakładka w **Menadźerze zadań** (uruchamiany chociażby kombinacją klawiszy Ctrl+Shift+Esc). Aktualne usługi zależą do zainstalowanych programów i wykorzystywanej konfiguracji. Warto zauważyć, iż nie wszystkie usługi są wyświetlane w aplikacji **Menadźer zadań**. Dzieje się tak dlatego, że te usługi są uruchamiane przez procesy usługowe, które są współdzielonymi procesami używanymi do konserwacji zasobów systemu. W poniższej tabelce zestawiono najważniejsze z wielu usługi oraz ich funkcje dla systemów z rodziny Windows. Ponadto został tam zaprezentowany przykład optymalnej konfiguracji usług systemowych.

Tabela: 1. Usługi dostępne w systemie Windows

Nazwa usługi	Std.	Zalecane	Opis/zalecenia
Aktualizacje automatyczne	Auto	Wył.	Umożliwia automatyczną aktualizację systemu.
Aplikacja systemowa modelu COM+	Ręcznie	Ręcznie	Kontroluje obiekty COM+.
Bufor wydruku	Auto	Auto	Jeśli nie korzystasz z drukarki ustaw na Ręcznie.
ClipBook	Ręcznie	Ręcznie	Zapewnia działanie schowka i dzielenie się nim ze zdalnymi komputerami.
Creative Service for CDROM Access	Auto	Wył.	Sterownik Creative'a do obsługi napędu CDROM (dotyczy katry SB Live!)
DDE sieci	Ręcznie	Ręcznie	Zapewnia przepływ informacji DDE przez sieć.

Distributed Transaction Coordinator	Ręcznie	Ręcznie	Koordynuje transakcje pomiędzy bazami danych i systemami plików.
Dostęp do urządzeń interfejsu HID	Wył.	Wył.	Zapewnia działanie zdalnych kontrolerów (gier) i in. podobnych urządzeń bazujących na HID (Human Interface Devices).
DSDM DDE sieci	Ręcznie	Ręcznie	Zapewnia dzielenie informacji DDE przez sieć.
Dziennik zdarzeń	Auto	Auto	Serwis ten nie może zostać zatrzymany ręcznie, ponieważ zapewnia działanie logowanie komunikatów wysyłanych przez programy.

Dzienniki wydajności i alerty	Ręcznie	Ręcznie	Loguje informacje o wydajności i komunikaty alarmach.
Harmonogram zadań	Auto	Ręcznie	Umożliwia działanie harmonogramu zadań (Scheduled Tasks).
Host uniwersalnego urządzenia Plug and Play	Ręcznie	Ręcznie	Zapewnia wsparcie dla UPnP.
Instalator Windows	Ręcznie	Ręcznie	Instalator plików MSI.
Instrumentacja zarządzania Windows	Auto	Auto	W razie wyłączenia większość aplikacji windowsowych może przestać działać poprawnie. Jeśli wyłączyłeś serwis Event Log, to możesz ustawić na Ręcznie, bowiem ten jest od niego zależny.
Karta inteligentna	Auto	Ręcznie	Kontroluje dostęp od kart inteligentnych.
Karta wydajności WMI	Ręcznie	Ręcznie	Zapewnia dostęp do informacji o wydajności dla providerów WMI HiPerf.
Klient DHCP	Auto	Auto	Pozwala na konfigurację sieci przez rejestrowanie adresów IP i nazw DNS.

Klient DNS	Auto	Auto	Ustawia i cache'uje nazwy DNS.
Klient śledzenia łączy rozproszonych	Auto	Ręcznie	Zapewnia poprawne połączenia pomiędzy plikami NTFS w obrębie komputera bądź domeny sieciowej.
Kompozycje	Auto	Auto	Zapewnia obsługę tematów systemu. Jeśli nie korzystamy z interfejsu LUNA możemy ustawić na Ręcznie.
Konfiguracja zerowej sieci bezprzewodowej	Auto	Ręcznie	Umożliwia automatyczną konfigurację dla kart 802.11. Jeśli nie posiadamy takiej karty ust. na Ręcznie.
Kopiowanie woluminów w tle	Ręcznie	Ręcznie	Kontroluje kopie woluminów przy użyciu tzw. "cienia"; serwis potrzebny do poprawnego działania programów wykonujących kopie zapasowe (backup).
Logowanie do sieci	Ręcznie	Ręcznie	Jeśli jesteś podłączony do domeny Windows - ustaw na Auto.
Logowanie pomocnicze	Auto	Ręcznie	Umożliwia uruchamianie procesów jako inny użytkownik.
Lokalizator usługi zdalnego wywołania procedury (RPC)	Ręcznie	Ręcznie	Zarządza bazą RPC.

Magazyn chroniony	Auto	Auto	Zwiększa bezpieczeństwo poprzez ochronę prywatnych kluczy, ważnych danych itp.
Magazyn wymienny	Ręcznie	Ręcznie	
Menedżer autopołączenia dostępu zdalnego	Ręcznie	Ręcznie	Tworzy połączenie do zdalnej sieci.
Menedżer dysków logicznych	Auto	Auto	Wykrywa i monitoruje podłączone dyski twarde.

Menedżer kont zabezpieczeń	Auto	Auto	Składa informacje o ochronie dla lokalnych kont użytkowników.
Menedżer połączeń usługi Dostęp zdalny	Ręcznie	Ręcznie	Tworzenie połączeń sieciowych.
Menedżer przekazywania	Auto	Ręcznie	Kontroluje synchroniczne i asynchroniczne transfery plików pomiędzy klientami i serwerami w sieci.
Menedżer sesji pomocy pulpitu zdalnego	Ręcznie	Ręcznie	Umożliwia działanie Remote Desktop.
MS Software Shadow Copy Provider	Ręcznie	Ręcznie	Zapewnia możliwość kopiowania plików będących aktualnie w użyciu przy użyciu tzw. cienia (Shadow)
NetMeeting Remote Desktop Sharing	Ręcznie	Ręcznie	Umożliwia dzielenie pulpitu poprzez program NetMeeting
Norton AntiVirus Auto Protect Service	Ręcznie	Ręcznie	Obsługuje komunikaty NAV Auto-Protect. Jeśli nie korzystasz w ogóle z Norton Antivirus'a, ustaw na Wył.
Numer seryjny nośnika przenośnego	Auto	Ręcznie	Serwis uzyskujący numer seryjny. Jeśli masz podłączone do komputera jakieś przenośne urządzenie audio ustaw na Auto.
NVIDIA Driver Helper Service	Auto	Auto	Serwis pomocniczy NVIdii. Jeśli chcesz, żeby system zamykał się szybciej - ustaw na Wył. (ciut gorsze osiągi karty graficznej) w przeciwnym wypadku ustaw na Ręcznie; zaś jeśli często używasz aplikacji/gier 3D - Auto).
Plug and Play	Auto	Auto	Obsługa Plug&Play.
Połączenia sieciowe	Ręcznie	Ręcznie	Kontroluje obiekty w panelu Network Connections, zarówno dla połączeń w sieci LAN jak i zdalnych.

Pomoc i obsługa techniczna	Auto	Ręcznie	Umożliwia działanie pomocy i wsparcie technicznego. Jeśli często korzystasz z pomocy ustaw na Automatic.
Pomoc TCP/IP NetBIOS	Auto	Ręcznie	Zapewnia obsługę NetBIOS przez serwis TCP/IP (NetBT) i rozdzielczość nazw NetBIOS.
Pomocnik karty inteligentnej	Auto	Ręcznie	Kontroluje dostęp od kart inteligentnych.
Posłaniec	Auto	Auto	Transmituje wysłane przez sieć i Alerter wiadomości pomiędzy klientami i serwerami. Jeśli nie jesteś podłączony do sieci - ustaw na Ręcznie.
Przeglądarka komputera	Auto	Ręcznie	Pobiera listę komputerów w sieci LAN. W przypadku korzystania z niej należy ustawić na Auto.
QoS RSVP	Ręcznie	Ręcznie	Zapewnia obsługę standardu QoS do kontroli ruchu w sieci.
Rejestr zdalny	Auto	Ręcznie	Zdalna obsługa rejestru systemowego.
Routing i dostęp zdalny	Wył.	Wył.	Umożliwia routowanie.
Rozpoznawanie lokalizacji w sieci (NLA)	Ręcznie	Ręcznie	Zbiera i zapisuje informacje o sieci oraz powiadamia programy o zmianach w tych zapisach.
Rozszerzenia sterownika Instrumentacji zarządzania Windows	Ręcznie	Ręcznie	Zapewnia kontrolę nad wysyłaniem informacji do i ze sterowników.
ScriptBlocking Service	Auto	Ręcznie	Blokowanie skryptów firmy Norton. Można również ustawić na Wył..

Serwer	Auto	Ręcznie	Umożliwia współdzielenie zasobów komputera (pliki, drukarki) w sieci.
Stacja robocza	Auto	Auto	Kontroluje połączenia sieciowe do zdalnych serwerów.
System zdarzeń COM+	Ręcznie	Ręcznie	System zdarzeń COM+.
Telefonia	Ręcznie	Ręcznie	Obsługa telefonii API (TAPI) dla programów korzystających z połączeń głosowych, także bazujących na telefonii internetowej (przez IP).
Telnet	Ręcznie	Ręcznie	Zapewnia działanie Telnet'u.

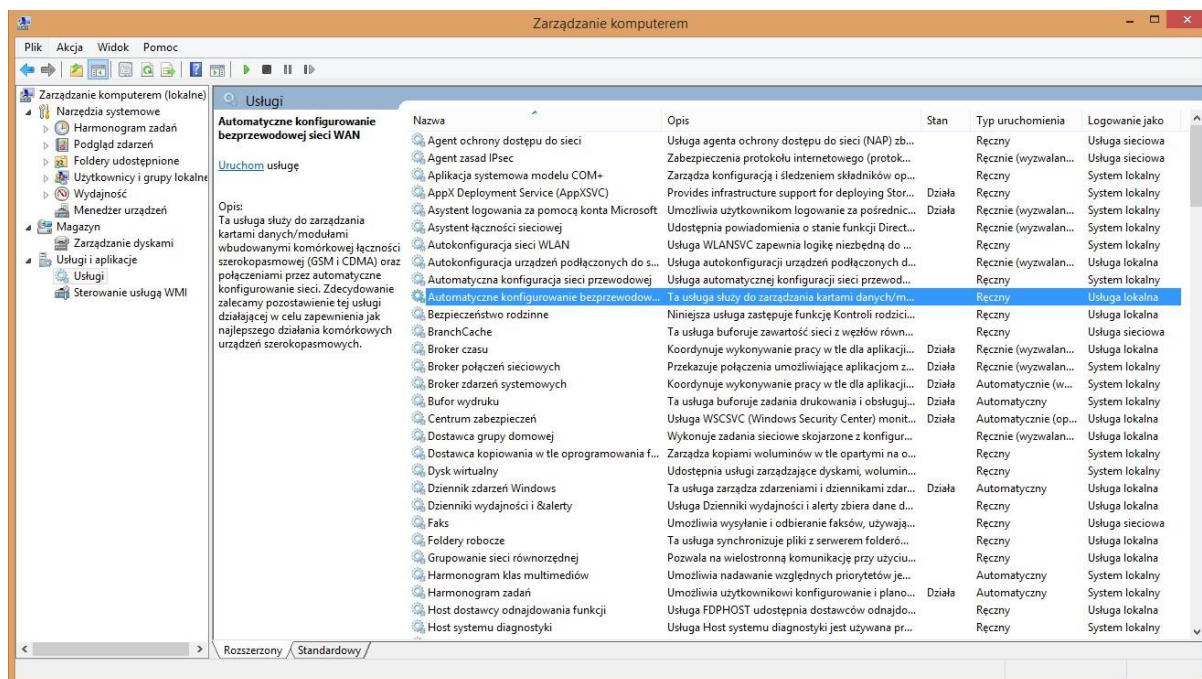
Urządzenie alarmowe	Auto	Ręcznie	Umożliwia powiadamianie wybranych użytkowników o alarmach administracyjnych.
Usługa administracyjna Menedżera dysków logicznych	Ręcznie	Ręcznie	Konfiguruje HDD i woluminy.
Usługa bramy warstwy aplikacji	Ręcznie	Ręcznie	Zapewnia działanie dzielenie połączenia internetowego oraz firewalli firm trzecich.
Usługa COM nagrywania dysków CD IMAPI	Auto	Ręcznie	Kontroluje nagrywanie płyt CD. Jeśli serwis zostanie wyłączony niemożliwe będzie nagrywanie płyt CD.
Usługa Czas systemu Windows	Auto	Auto	Umożliwia automatyczną aktualizację daty/czasu. W razie braku dostępu do Internetu ust. na Ręcznie.
Usługa indeksowania	Ręcznie	Ręcznie	Zapewnia bardzo szybkie wyszukiwanie plików na dysku.
Usługa inteligentnego transferu w tle	Ręcznie	Ręcznie	Transmituje dane podczas nieużywania sieci.

Usługa NT LM Security Support Provider	Ręcznie	Ręcznie	Zapewnia ochronę RPC.
Usługa odnajdywania SSDP	Ręcznie	Ręcznie	Umożliwia obsługę UPnP (Universal Plug&Play)
Usługa przywracania systemu	Auto	Auto	Zapewnia działanie narzędzia System Restore. Jeśli z niego nie korzystamy - można ustawić na Ręcznie.
Usługa raportowania błędów	Auto	Ręcznie	Umożliwia wysyłanie raportów o błędach.
Usługi IPSEC	Auto	Ręcznie	Kontroluje założenia ochrony IP - uruchamia sterownik ISAKMP/Oakley (IKE) oraz driver ochronny IP. W przypadku podłączenia do domeny Windows - należy ustawić na Auto.
Usługi kryptograficzne	Auto	Ręcznie	Zapewnia działanie usług: Catalog Database Service (kontroluje sygnatury plików Windows); Protected Root Service (zarządza certyfikatami Trusted Root Certification Authority) oraz Key Service (wspomaga kontrolowanie certyfikatów).
Usługi terminalowe	Ręcznie	Ręcznie	Pozwala na podłączenie wielu użytkowników do jednego komputera.
WebClient	Auto	Ręcznie	Zależne od tego są usługi Remote Desktop, Fast User Switching, Remote Assistance i Terminal Server. Pozwala programom na tworzenie, dostęp i modyfikację plików "Internet-based".
Windows Audio	Auto	Auto	Kontroluje urządzenia audio. Możemy wyłączyć tylko jeśli nie korzystamy w ogóle z dźwięku.

Windows Image Acquisition (WIA)	Ręcznie	Ręcznie	Zapewnia obsługę skanerów i kamer cyfrowych.
WMDM PMSP Service	Auto	Auto	
Wykrywanie sprzętu powłoki	Auto	Auto	
Zapora połączenia internetowego / Udostępnianie połączenia internetowego	Auto	Auto	Obsługa wbudowanego firewall'a. Jeśli nie jesteś podłączony do sieci/Internetu - ustaw na Wył..
Zarządzanie aplikacjami	Ręcznie	Ręcznie	Zapewnia działanie usług instalacyjnych.
Zasilacz awaryjny (UPS)	Ręcznie	Ręcznie	Wsparcie dla urządzeń UPS.
Zawiadomienie o zdarzeniu systemowym	Auto	Ręcznie	Rejestruje zdarzenia systemowe: logowanie, podłączenie do sieci, stan zasilania.
Zdalne wywoływanie procedur (RPC)	Auto	Auto	Zapewnia obsługę zdalnych procedur RPC.
Zgodność szybkiego przełączania użytkowników	Ręcznie	Ręcznie	Umożliwia działanie szybkiej zmiany użytkownika.

Zarządzanie usługami

Do zarządzania usługami systemowymi służy narzędzie **Usługi** znajdujące się w **Narzędziach administracyjnych** (Rysunek 10).



Rys. 10. Narzędzie Zarządzanie komputerem z wybranym elementem Usługi

Umożliwia ono uruchamianie, zatrzymywanie, wstrzymywanie lub wznawianie usług. Ponadto pozwala na konfigurowanie opcji uruchamiania i odzyskiwania. Przy pomocy tego narzędzia możemy również włączać lub wyłączać wybrane usługi dla określonego profilu sprzętu. Aby uruchomić, zatrzymać, wstrzymać lub wznówić usługę należy:

1. Otworzyć okno **Usługi**.
2. Następnie kliknąć prawym przyciskiem myszy żadaną usługę, a następnie wybrać polecenie **Uruchom**, **Zatrzymaj**, **Wstrzymaj**, **Wznów** lub **Uruchom ponownie**.

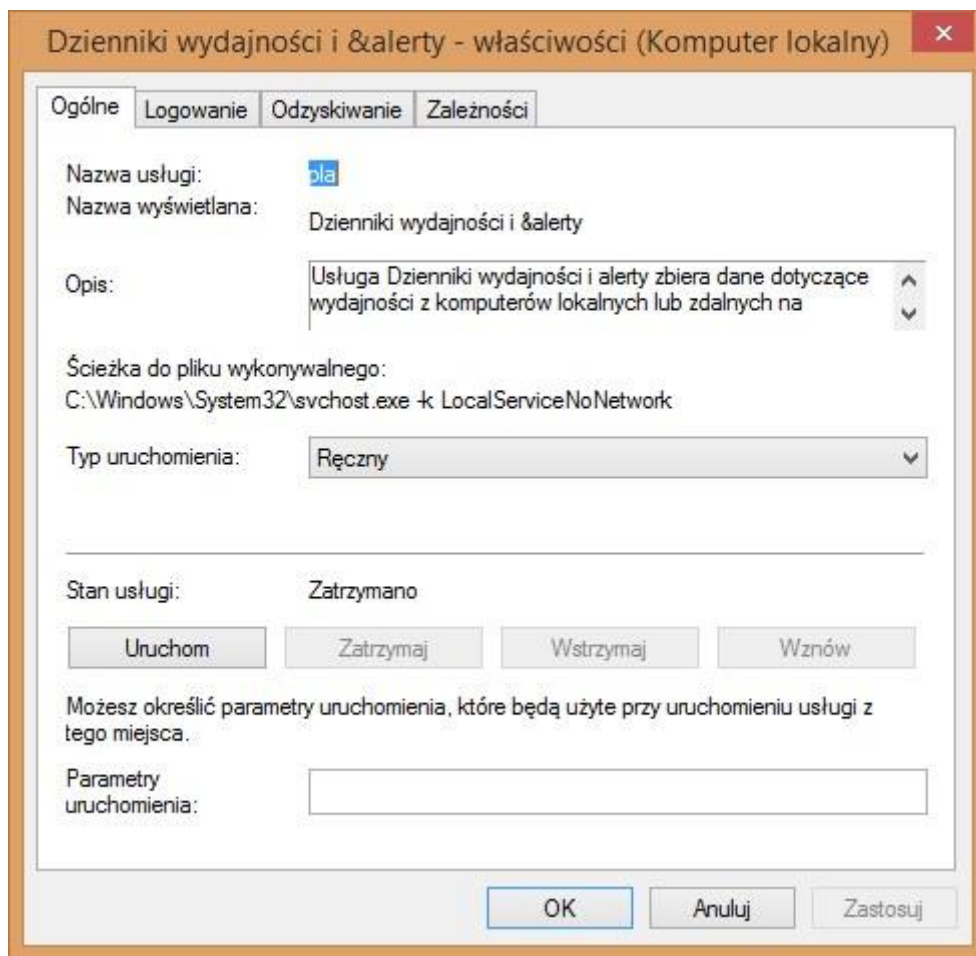
Aby przekazać do usługi parametry startowe, przed kliknięciem polecenia Uruchom należy kliknąć żadaną usługę prawym przyciskiem myszy, z menu kontekstowego wybrać polecenie **Właściwości**, a następnie wpisać wymagane parametry w polu **Parametry uruchomienia** (Rysunek 11). Przy wprowadzaniu parametrów należy pamiętać, iż znak kreski ułamekowej odwróconej (\) traktowany jest jako znak ucieczki. Aby go więc wprowadzić w parametrze należy wpisać go dwa razy (\\).

Sposoby uruchamiania usług

Aby określić sposób uruchamiania wybranej usługi należy:

1. Otworzyć okno **Usługi**.
2. Kliknąć prawym przyciskiem myszy wybraną usługę, którą chcemy skonfigurować i z menu kontekstowego wybrać polecenie **Właściwości**.
3. Na zakładce **Ogólne** w obszarze **Typ uruchamiania**, należy wybrać jedną z opcji:

Automatyczny, Ręczny lub Wyłączony (Rysunek 11).

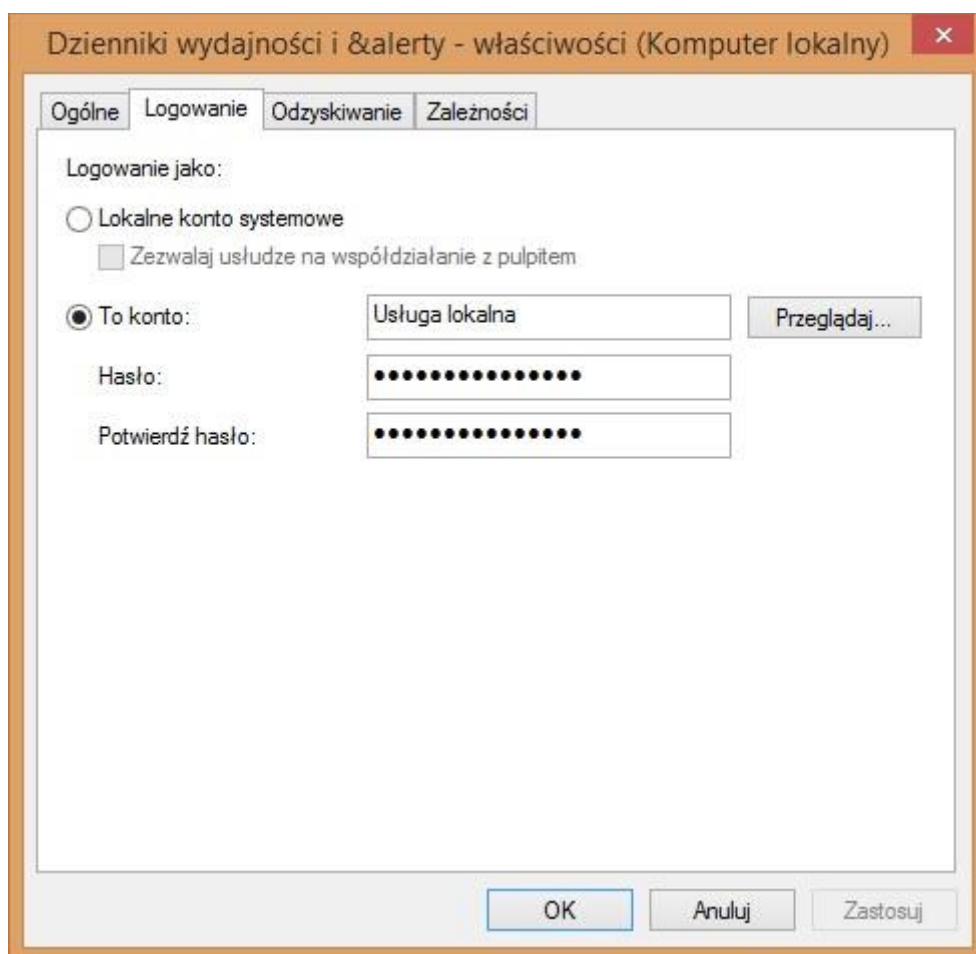


Rys. 11. Zakładka Ogólne wybranej usługi

W trybie automatycznym usług uruchamiana jest w momencie startu systemu. W trybie ręcznym usługa może być uruchomiona przez użytkownika lub usługę zależną. Trzeci typ uruchomienia uniemożliwia uruchomienie usługi zarówno przez system w sposób automatyczny, jak i ręcznych przez użytkownika, bądź usługę zależną.

Wybór konta użytkownika, którego usługa będzie używała do logowania

W celu wybrania konta użytkownika, którego usługa będzie używała do logowania należy kliknąć prawym klawiszem myszy wybraną usługę, do której chcemy przypisać konto użytkownika lub grupy, i z menu wybrać polecenie **Właściwości**. Następnie na zakładce **Logowanie** należy zaznaczyć opcję **To konto** i kliknąć przycisk **Przeglądaj**. W polu **Szukaj w**, należy wybrać domenę lub grupę roboczą żadanego użytkownika lub grupy, w polu **Nazwa** należy natomiast kliknąć konto użytkownika lub grupy i kliknąć przycisk OK. Następnie w polach **Hasło** i **Potwierdź hasło** należy wpisać hasło dla konta użytkownika.



Rys. 12. Zakładka Logowanie

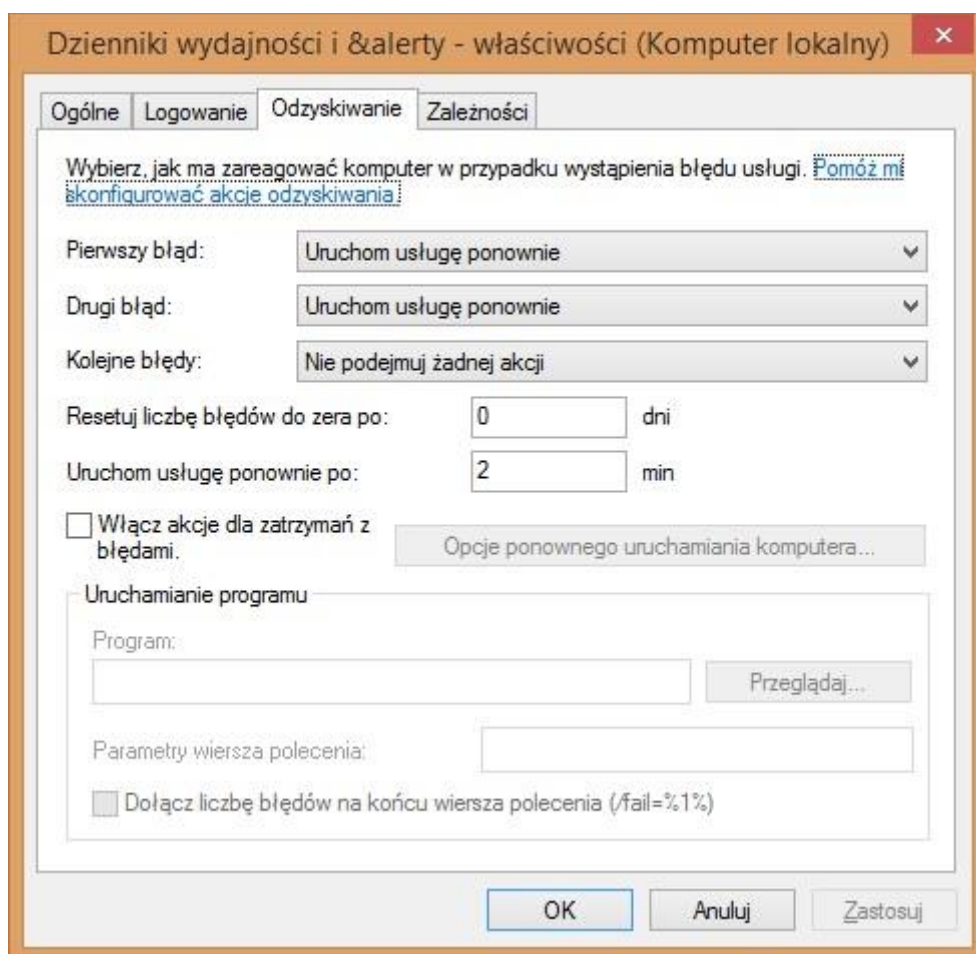
*Konto to powinno być utworzone przy użyciu narzędzia **Użytkownicy i grupy lokalne** zawartego w konsoli **Zarządzanie komputerem**. We właściwościach dla tego konta należy zaznaczyć opcję **Hasło nigdy nie wygasa** oraz upewnić się, że należy ono do odpowiednich grup. Konto to powinno być utworzone specjalnie na potrzeby logowania się do danej usługi.*

Usługa może również nie wymagać logowania. Należy wówczas wybrać opcję **Lokalne konto systemowe**.

Jeśli włączona lub wyłączona usługa spowoduje problemy z uruchomieniem komputera, należy uruchomić komputer w trybie awaryjnym. Korzystając z tego trybu możliwa będzie zmiana konfiguracji usługi lub przywrócenie domyślnej konfiguracji.

Akcje odzyskiwania

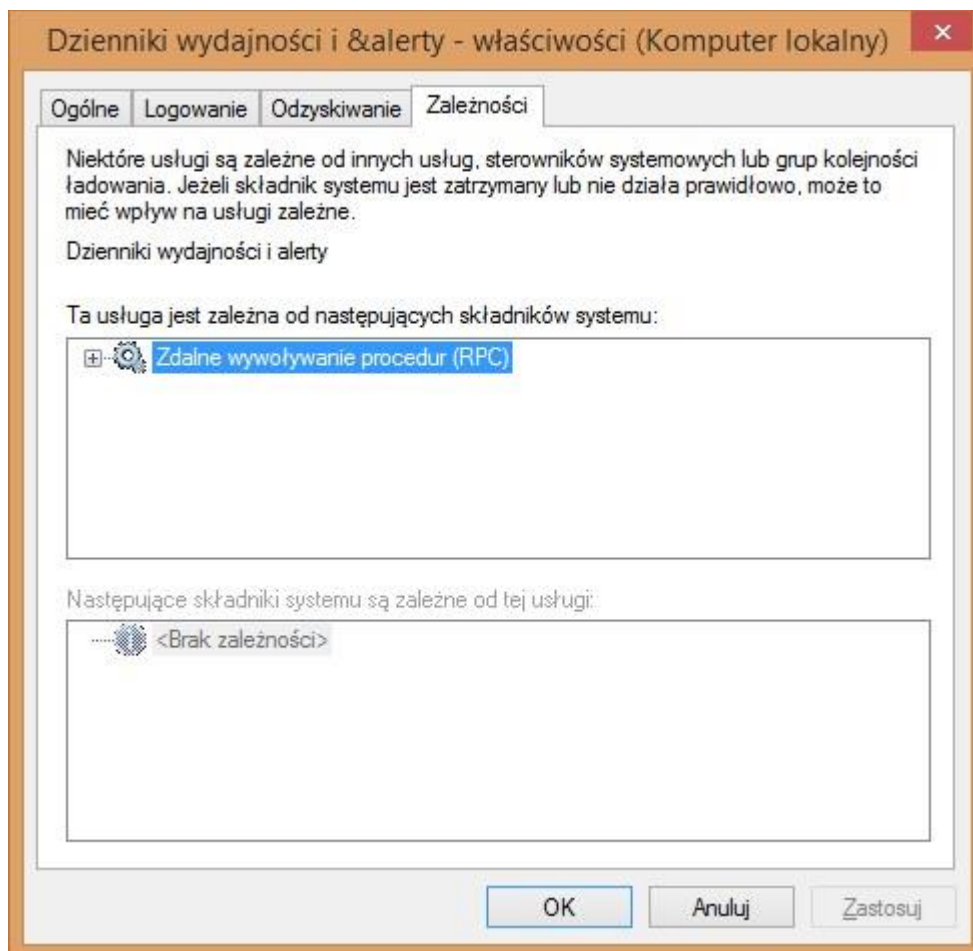
Aby skonfigurować akcje odzyskiwania podejmowane, gdy usługa ulegnie awarii należy na karcie **Odzyskiwanie** kliknąć żądane akcje w polach **Pierwszy błąd**, **Drugi błąd** i **Kolejne błędy** (Rysunek 13).



Rys. 13. Zakładka Odzyskiwanie

Zależności usług

Zakładka Zależności pozwala podejrzeć powiązania między wybraną usługą, a innymi usługami systemowymi. Górna lista pozwala zidentyfikować inne usługi, które muszą być uruchomione, aby ta usługa działała. Dolna lista natomiast identyfikuje usługi, do działania których wymagane jest uruchomienie tej usługi.



Rys. 14. Różne rodzaje zależności między usługami

Zadania

1. Do czego służy zakładka Zależności?
2. Jak zależności pomiędzy usługami wpływają na ich wyłączanie?