

*Krzysztof Wołk*

# **Biblia**

## **Windows Server 2012**

**Podręcznik Administratora**



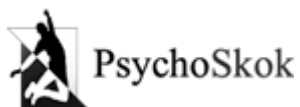
---

# Biblia Windows Server 2012

## Podręcznik Administratora

---

Krzysztof Wołk



**2012**

Copyright © by Krzysztof Wołk, 2012

Copyright © by Wydawnictwo Psychoskok, 2012

Wszelkie prawa zastrzeżone. Żaden fragment nie może być publikowany ani reprodukowany bez pisemnej zgody wydawcy.

Opracowanie graficzne i projekt okładki:

Krzysztof Wołk & Wydawnictwo Psychoskok

ISBN: 978-83-63548-08-7

Wydawnictwo Psychoskok

ul. Chopina 9 pok. 23, 62-507 Konin

Tel. (63) 242 02 02, kom. 665-955-131

<http://wydawnictwo.psychoskok.pl>

e-mail: [wydawnictwo@psychoskok.pl](mailto:wydawnictwo@psychoskok.pl)

# Spis treści

<b>O KSIĄŻCE .....</b>	<b>7</b>
<b>O AUTORZE .....</b>	<b>8</b>
<b>1. INSTALACJA .....</b>	<b>9</b>
1.1. WYMAGANIA SPRZĘTOWE I OPIS ŚRODOWISKA .....	10
1.2. PROCES INSTALACJI .....	11
<b>2. POST INSTALACJA .....</b>	<b>17</b>
2.1. NOWY INTERFEJS UŻYTKOWNIKA .....	17
2.2. CZYNNOŚCI POST-INSTALACYJNE .....	22
2.2.1. <i>Aktualizacje</i> .....	23
2.2.2. <i>Zmiana nazwy komputera</i> .....	25
2.3. KONFIGURACJA SIECI .....	27
2.4. ZARZĄDZANIE PROCESORAMI I PAMIĘCIĄ OPERACYJNĄ .....	29
<b>3. ACTIVE DIRECTORY DOMAIN SERVICES .....</b>	<b>31</b>
3.1. CZYM JEST DOMENA? .....	31
3.2. INSTALACJA ACTIVE DIRECTORY DOMAIN SERVICES .....	34
3.3. WSTĘPNA KONFIGURACJA AD DS .....	41
3.4. ACTIVE DIRECTORY USERS AND COMPUTERS .....	45
3.5. ACTIVE DIRECTORY ADMINISTRATIVE CENTER .....	70
<b>4. SERWER DNS .....</b>	<b>76</b>
4.1. ZAPOZNANIE Z KONSOLĄ DNS MANAGER .....	76
4.2. RĘCZNA KONFIGURACJA STREFY DNS .....	79
4.3. ZARZĄDZANIE SERWEREM DNS .....	84
4.4. ZAPASOWY SERWER DNS .....	90
<b>5. SERWER DHCP .....</b>	<b>99</b>
5.1. INSTALACJA PIERWSZEGO SERWERA DHCP .....	99
5.2. KONFIGURACJA SERWERA DHCP .....	103



5.3.	ZARZĄDZANIE SERWEREM DHCP .....	109
5.3.1.	<i>DHCP Policies</i> .....	113
5.4.	WYSOKA DOSTĘPNOŚĆ DHCP .....	118
5.4.1.	<i>Konfiguracja klastra DHCP</i> .....	118
5.4.2.	<i>Split-Scope</i> .....	122
<b>6.</b>	<b>IIS Z FTP ORAZ URZĄD CERTYFIKACJI</b> .....	<b>125</b>
6.1.	INSTALACJA ROLI WEB SERVER (IIS) .....	125
6.2.	INSTALACJA ACTIVE DIRECTORY CERTIFICATE SERVICES .....	128
6.3.	AKTUALIZACJA PLATFORMY .NET .....	139
6.4.	TWORZENIE NOWYCH CERTYFIKATÓW .....	141
6.5.	ZARZĄDZANIE SERWEREM IIS .....	144
6.6.	URUCHAMIANIE SERWERA FTP .....	152
6.7.	IIS I PHP .....	158
<b>7.</b>	<b>NETWORK ACCESS PROTECTION</b> .....	<b>164</b>
7.1.	NETWORK POLICY AND ACCESS SERVICES .....	164
7.2.	ZARZĄDZANIE NETWORK POLICY SERVER .....	168
<b>8.</b>	<b>VPN, DIRECT ACCESS I NAT</b> .....	<b>177</b>
8.1.	INSTALACJA ROLI REMOTE ACCESS .....	177
8.2.	KONFIGURACJA VPN I NAT .....	181
8.3.	KONFIGURACJA DIRECTACCESS .....	190
<b>9.</b>	<b>POLISY (ZARZĄDZANIE ZASADAMI GRUPY)</b> .....	<b>195</b>
9.1.	WYBRANE NOWOŚCI W GPO .....	202
<b>10.</b>	<b>UPRAWNIENIA SIECIOWE I NA SYSTEMIE PLIKÓW</b> .....	<b>205</b>
10.1.	UPRAWNIENIA SIECIOWE .....	205
10.1.1.	<i>Dodatkowe ustawienia udostępnianych plików</i> .....	208
10.2.	UPRAWNIENIA NTFS .....	209
10.3.	AUTORYZACJA METODĄ CLAIM .....	215
10.3.1.	<i>Nakładanie uprawnień Claim</i> .....	216

10.3.2.	Definiowanie Claim Types .....	222
10.4.	UPRAWNIENIA NA SYSTEMIE PLIKÓW REFS .....	227
10.5.	ZARZĄDZANIE DRUKARKAMI .....	230
10.5.1.	Instalowanie drukarek .....	230
10.5.2.	Zarządzanie dostępem do drukarek sieciowych.....	233
<b>11.</b>	<b>SERWER PLIKÓW .....</b>	<b>236</b>
11.1.	INSTALACJA ROLI SERWERA PLIKÓW .....	236
11.2.	ZAPOZNANIE Z NOWYM PODEJŚCIEM DO USŁUG PLIKÓW .....	237
11.3.	STORAGE POOLS.....	246
11.4.	ZARZĄDZANIE PRZEZ MENADŻERA SERWERA PLIKÓW.....	249
11.4.1.	Zarządzanie Ostonami Plików .....	249
11.4.2.	Zarządzanie Przydziałami.....	253
<b>12.</b>	<b>PRACA ZDALNA.....</b>	<b>256</b>
12.1.	WSTĘPNA KONFIGURACJA SERWERA .....	256
12.2.	KORZYSTANIE Z POMOCY ZDALNEJ .....	259
12.3.	NAWIĄZYWANIE POŁĄCZENIA PULPITU ZDALNEGO .....	265
<b>13.</b>	<b>ZARZĄDZANIE DYSKAMI .....</b>	<b>268</b>
12.4.	WIRTUALNE DYSKI .....	276
12.5.	INSTALACJA SYSTEMU NA WIRTUALNYM DYSKU .....	279
<b>14.</b>	<b>WDS – ZDALNA INSTALACJA .....</b>	<b>286</b>
<b>15.</b>	<b>HYPER – V .....</b>	<b>294</b>
A.	INSTALACJA.....	294
B.	ZARZĄDZANIE HYPER-V.....	299
<b>16.</b>	<b>WINDOWS SERVER UPDATE SERVICES .....</b>	<b>321</b>
<b>17.</b>	<b>BEZPIECZEŃSTWO DANYCH I KOMPUTERA .....</b>	<b>333</b>
A.	WINDOWS BACKUP .....	333
B.	SHADOW COPIES .....	344

C.	BITLOCKER .....	350
D.	KILKA UWAG OGÓLNYCH.....	358
i.	<i>Polityka haseł.....</i>	358
ii.	<i>Podmiana logon.scr .....</i>	360
iii.	<i>Niezabezpieczone serwery wydruku .....</i>	361
iv.	<i>Best Practices Analyzer.....</i>	363
<b>18.</b>	<b>REMOTE DESKTOP SERVICES.....</b>	<b>364</b>
<b>19.</b>	<b>SERWER WYDRUKU .....</b>	<b>381</b>
<b>20.</b>	<b>SERWER FAKSÓW .....</b>	<b>385</b>
<b>21.</b>	<b>VOLUME ACTIVATION SERVICES .....</b>	<b>393</b>
A.	INSTALACJA.....	393
B.	WSTĘPNA KONFIGURACJA VA SERVICES .....	394
<b>22.</b>	<b>TRIKI .....</b>	<b>399</b>
A.	WĘDRUJĄCY I WYMUSZONY PROFIL UŻYTKOWNIKA .....	399
B.	DANE W CHMURZE - MAPOWANIE SKYDRIVE .....	403
C.	GODMODE .....	408
<b>23.</b>	<b>WINDOWS 2012 CORE .....</b>	<b>410</b>
A.	INSTALACJA WSTĘPNA KONFIGURACJA .....	410
B.	ZARZĄDZANIE SYSTEMEM W WERSJI CORE.....	415
i.	<i>Interfejsy użytkownika.....</i>	415
ii.	<i>Podstawowe role serwera .....</i>	418

## O Książce

Niniejsza książka stanowi praktyczny przewodnik po Windows Serwer 2012. Stanowi ona propozycję nie tylko dla początkujących administratorów, lecz także dla tych doświadczonych, pragnących szybko i w przyjazny sposób poznać nowości nowego systemu serwerowego firmy Microsoft. Prezentuje ona w sposób praktyczny najważniejsze funkcje i możliwości nowego systemu serwerowego. Poza niezbędną teorią zawiera także szczegółowe instrukcje i ćwiczenia, w których każdy, nawet najdrobniejszy element jest zawarty na rzucie ekranowym objaśnionym tak, aby nawet osoba, która pierwszy raz pracuje z Windows Serwer spokojnie poradziła sobie z konfiguracją i administracją tymże systemem. Książka została tak napisana, aby przechodząc przez nią od początku do końca, użytkownikowi udało się w pełni skonfigurować własny serwer, a następnie nadzorować jego działanie i nim administrować. Została ona oparta na wersji RC systemu Windows Server 2012 w wersji angielskiej, dlatego też finalne nazwy funkcji w języku polskim mogą nieznacznie odbiegać od tych, które ukażą się wraz polską edycją systemu. Nie mniej jednak książka jest kompatybilna zarówno z anglojęzyczną jak i polskojęzyczną wersją systemu, która dopiero będzie miała swoją premierę. Wszelkie ewentualne poprawki zostaną opublikowane na blogu autora <http://www.wolk.pl>. Z tej lektury czytelnik nauczy się także współpracować z maszynami i sieciami opartymi o systemy z rodziny Mac OS X oraz Linux. Współdzielenie się zasobami oraz wspólna praca w domenie czy grupie roboczej nie będzie stanowić dla czytelnika żadnego problemu. Czytelnik także zapozna się z innymi zaawansowanymi możliwościami nowego serwera. Jest to idealna pozycja dla czytelników mających już dość encyklopedycznych pozycji i pragnących lektury ukierunkowanej na praktykę i ćwiczenia.

## O Autorze



Jest magistrem inżynierem informatyki, absolwentem Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych. Obecnie doktorant i ćwiczeniowca na powyższej uczelni, a zawodowo trener IT. Jego specjalnością są produkty serwerowe firm Apple oraz Microsoft, a także aplikacje graficzne firmy Adobe. Od 2009 roku redaktor portalu informatycznego in4.pl oraz własnego bloga [www.wolk.pl](http://www.wolk.pl), na łamach których opublikował kilkadziesiąt artykułów oraz poradników w dziedzinie informatyki. Tworzy także autorskie materiały szkoleniowe, udziela się na portalu e-biotechnologia.pl, a także autor niektórych artykułów dla magazynu iCoder Magazine. Posiada także liczne certyfikaty firm Apple i Microsoft, między innymi Apple Certified System Administrator (ACSA), Microsoft Certified System Administrator (MCSA) oraz Microsoft Certified IT Professional (MCITP).

# 1. Instalacja

Niniejszy rozdział opisuje proces instalacji systemu Windows Server 2012. Instalację można wykonać na własną rękę na dowolnym komputerze, lecz w celach ćwiczeniowych zalecana jest instalacja według książki w środowisku wirtualnym przy użyciu wersji testowej Microsoft Windows Server 2012 oraz systemu maszyn wirtualnych VirtualBox. Zaleca się także wykonywać częste migawki maszyny wirtualnej, np. przed instalacją kolejnych ról serwera. Pozwoli to w razie błędu w konfiguracji szybko przywrócić maszynę do stanu poprzedniego.

Windows Server 2012 występuje w czterech edycjach:

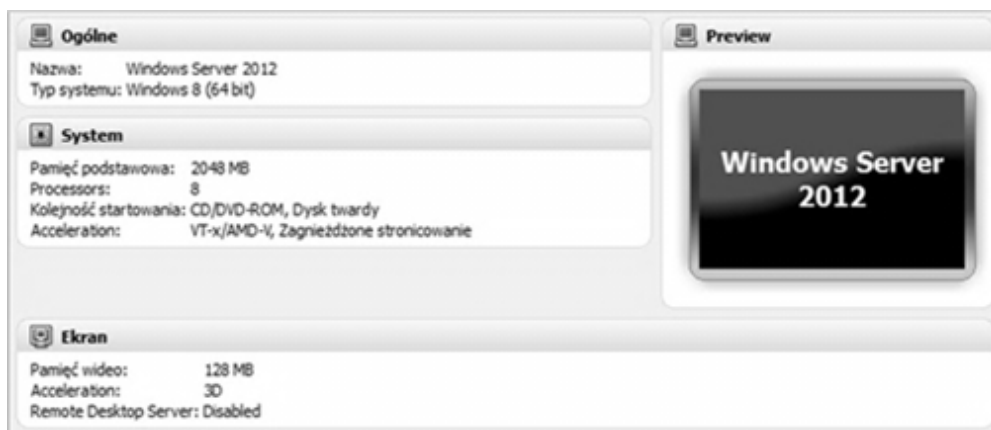
- **Foundation** - ograniczona jest do serwerów jednoprocessorowych, może obsłużyć maksymalnie 15 użytkowników, a także nie wszystkie funkcje są dostępne.
- **Essentials** - ograniczona jest do serwerów jednoprocessorowych, ilość użytkowników ograniczona jest do 25, a także nie wszystkie funkcje są dostępne.
- **Standard** - posiada wszystkie funkcje oraz nie ma limitów na ilość procesorów, natomiast wymaga wykupienia licencji dostępowych CAL, dla każdego użytkownika lub urządzenia. Ta edycja pozwala także na zainstalowanie systemu Windows Server 2012 jeden raz fizycznie na maszynie, a następnie w ramach tego samego serwera fizycznego na uruchomienie dwóch wirtualnych instancji tego systemu.
- **Datacenter** - posiada wszystkie funkcje oraz nie ma limitów na ilość procesorów, natomiast wymaga wykupienia licencji dostępowych CAL, dla każdego użytkownika lub urządzenia. Ta edycja pozwala także na zainstalowanie systemu Windows Server 2012 jeden raz fizycznie na maszynie, a następnie w ramach tego samego serwera fizycznego na uruchomienie nielimitowanej ilości wirtualnych instancji tego systemu.

Właśnie na tej wersji systemu została oparta ta książka.

Więcej informacji na temat różnic między edycjami systemu Windows Server 2012 można znaleźć na stronie Microsoft.com. Na tej samej stronie można pobrać kilkudziesięciodniową wersję testową tego systemu operacyjnego.

## 1.1. Wymagania sprzętowe i opis środowiska

W tym dziale zajęto się dość prostym zagadnieniem, jakim jest instalacja systemu. Do tego celu będzie potrzebny komputer lub wirtualna maszyna z procesorem wspierającym architekturę x64 taktowany zegarem minimum 1,4 GHz, z 512MB pamięci RAM oraz minimum 32 GB wolnego miejsca na dysku. W praktyce zaleca się użycie minimum dwurdzeniowego procesora, 4 GB pamięci RAM oraz dużego i szybkiego dysku. W komputerze potrzebne też będą dwie karty sieciowe. Jedna podłączona do sieci lokalnej, a druga do globalnej. Tworząc wirtualne środowisko zadbano o to.



Stworzono też trzy wirtualne dyski twarde. Nie są one wymogiem. Zdecydowano się na nie w celu dalszego zaprezentowania pracy na macierzach dyskowych.



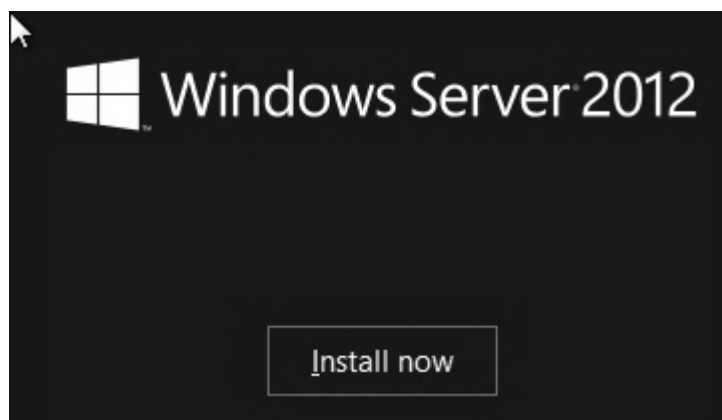
## 1.2. Proces instalacji

Instalator systemu wygląda bardzo podobnie do tego znanego z Windows 7 i Windows Vista. Do zaprezentowania kolejnych kroków została użyta testowa wersja systemu Windows Server 2012 RC dostępna do pobrania na stronach Microsoft. Po uruchomieniu komputera z płyty CD po chwili pojawi się ekran powitalny. Należy ustawić preferencje systemowe i nacisnąć przycisk **Dalej (Next)**.

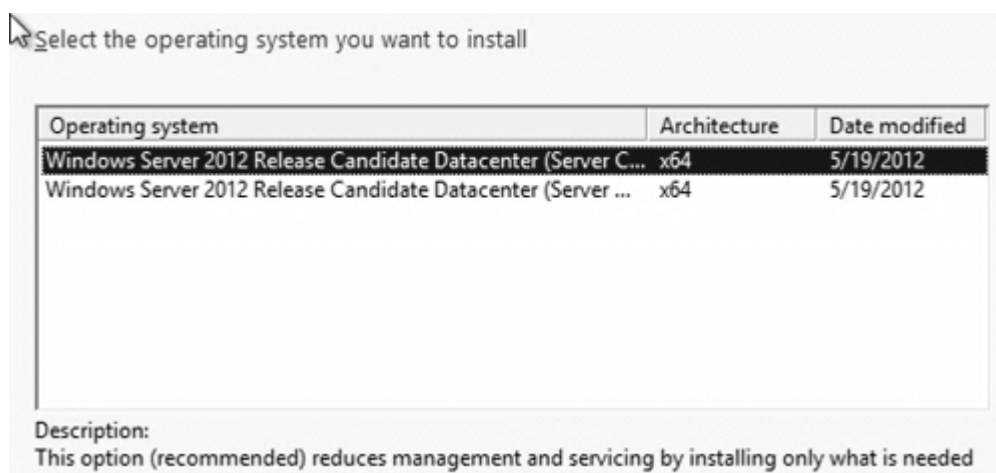




Na kolejnej planszy należy kliknąć przycisk **Zainstaluj Teraz** (*Install Now*).



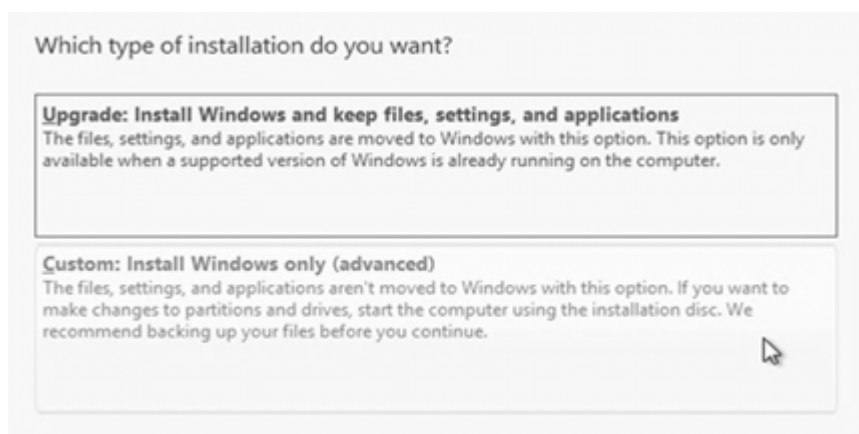
W kolejnym oknie instalatora należy wybrać wersję systemu Windows, na którą została zakupiona licencja.



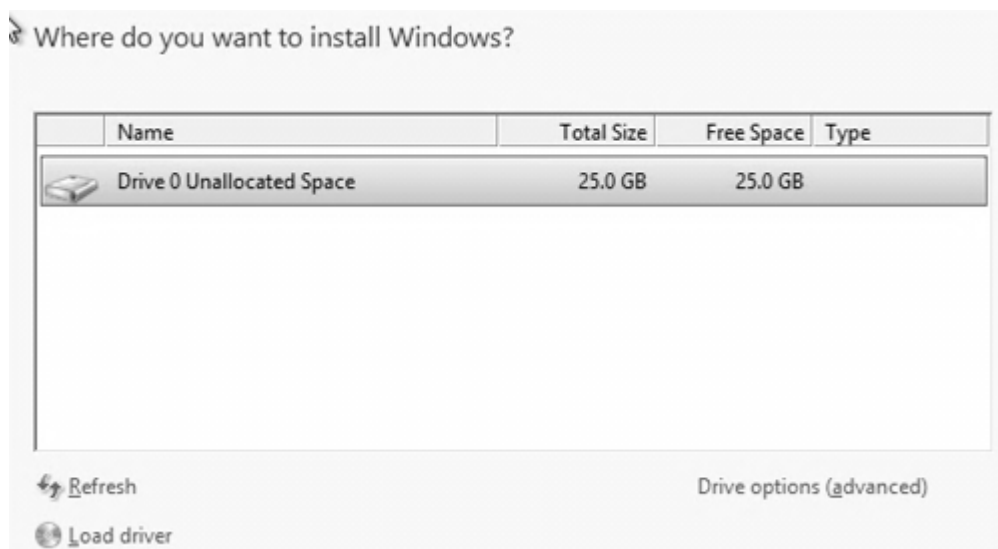
W następnym kroku należy zaakceptować umowę licencyjną i kliknąć przycisk **Dalej** (*Next*).



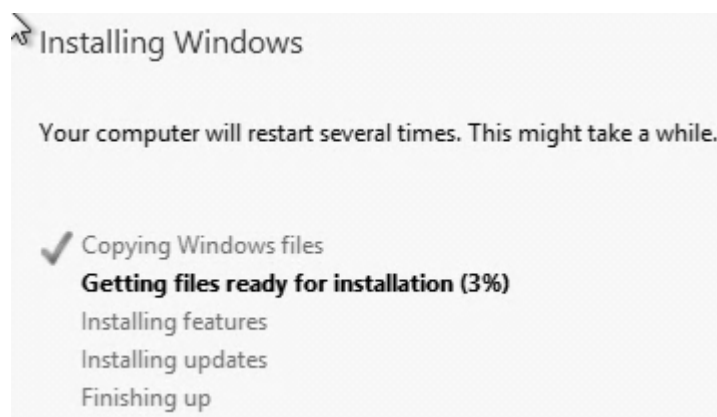
Jako, że przygotowywana jest nowa instalacja należy wybrać opcję niestandardową, czyli zaawansowaną (***Install Windows only (advanced)***).



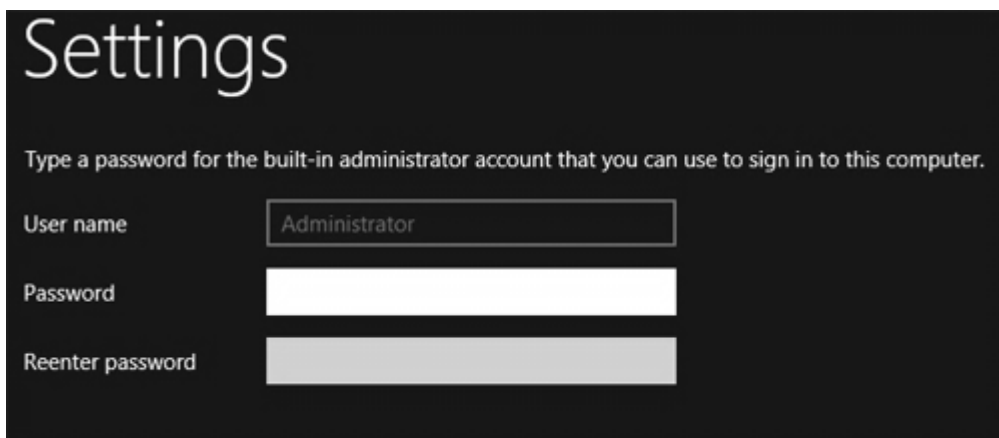
Pojawi się ekran wyboru dysku, na którym ma zostać zainstalowany system operacyjny. W tym przypadku zostanie zaznaczony ***Dysk0***, a następnie należy kliknąć przycisk ***Dalej (Next)***. Drzewo partycji utworzy się automatycznie.



Rozpocznie się proces instalacji, którego czas trwania będzie zależny od wydajności komputera, na którym się on odbywa.




Po wgraniu wszystkich plików podczas pierwszego uruchomienia komputer poprosi o zmianę hasła dla konta administratora. Należy dwukrotnie wprowadzić hasło, a następnie kliknąć przycisk **Zakończ (Finish)**. Hasło musi spełniać odpowiednie normy bezpieczeństwa, tj. musi mieć minimum 7 znaków, w tym jedną dużą literę, jedną cyfrę i jeden znak specjalny jak np. @ lub !.

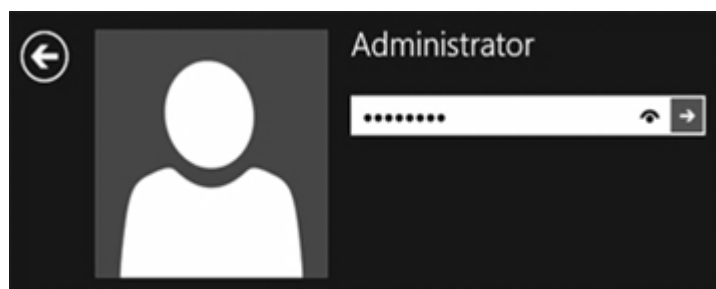


Pojawi się ekran logowania. Aby się zalogować należy na klawiaturze wcisnąć kombinację klawiszy **CTRL+ALT+DEL**.

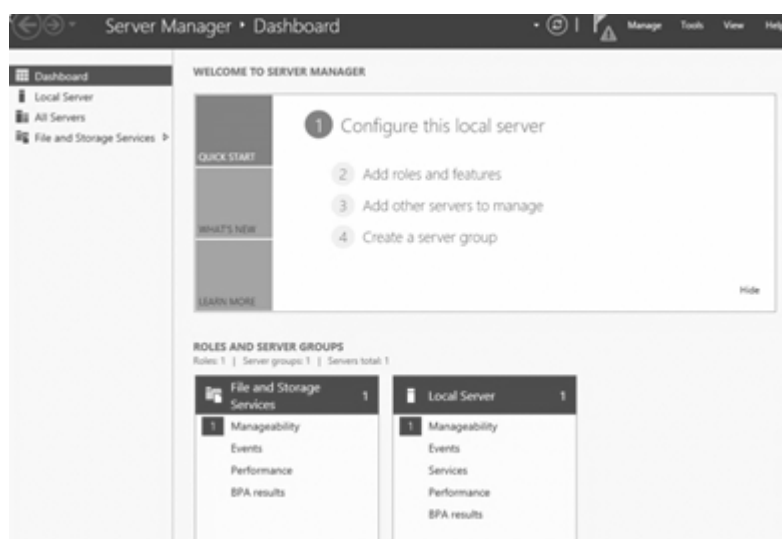


W oknie, które się zostanie wyświetlone należy podać hasło dla pożądanego

użytkownika, a następnie kliknąć ikonę  tuż obok pola wpisywania hasła.



Po zalogowaniu się zostanie załadowany nowy interfejs użytkownika, znany z systemu Windows 8. Na pierwszy rzut oka nie ma w nim przycisku **Start**, ani zwyczajnych okienek, lecz interfejs Metro oraz Menadżer Serwera, gdzie znajduje się większość ról, funkcji i opcji, którymi można zarządzać. Osoby znające system Windows Server 2008 nie powinny być zdziwione, ponieważ właśnie ten system był czymś pośrednim pomiędzy Windows 2003, a unifikacją okienek do nowego standardu. Mowa tu choćby o centrum Administracyjnym Active Directory, które miało zastąpić wcześniejszą wersję konsoli do zarządzanie kontami użytkowników i urządzeń. System Windows jest już zainstalowany!



## 2. Post instalacja

Po pomyślnym uruchomieniu serwera zanim przejdzie się do jego dalszej konfiguracji należy wykonać kilka ważnych czynności. Przede wszystkim zapoznać się z zupełnie nowym interfejsem użytkownika i odmienioną konsolą Menadżera Serwera względem wcześniejszych wersji. Następnie zaktualizować serwer, skonfigurować interfejsy sieciowe i przygotować maszynę do awansu na kontroler domeny.

### 2.1. Nowy interfejs użytkownika

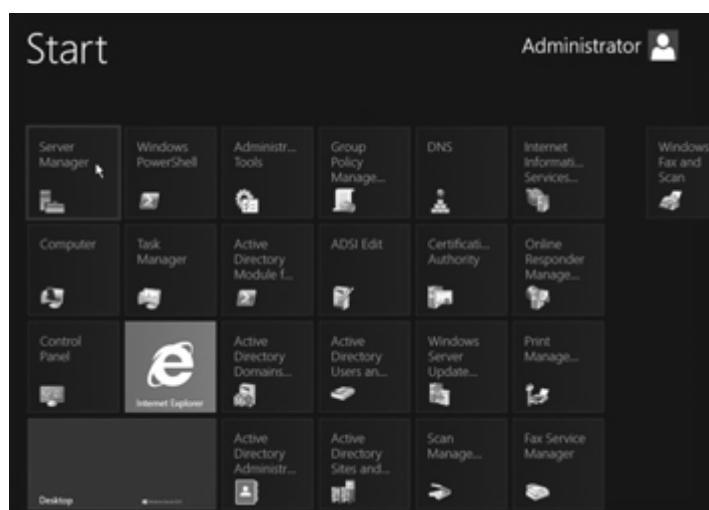
Nowy system serwerowy firmy Microsoft to także nowy interfejs. Osoby widzące go po raz pierwszy zainteresuje na pewno brak rzucającego się w oczy przycisku Start.



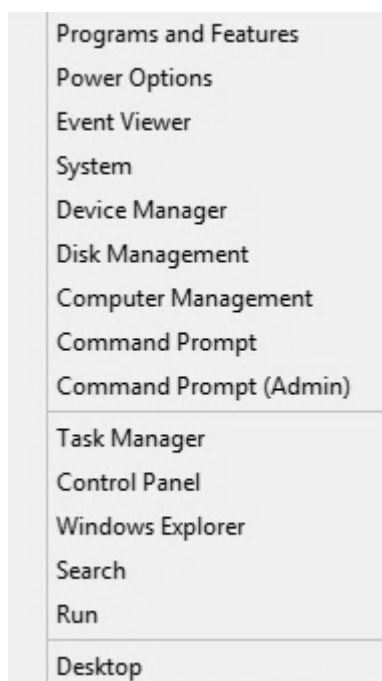
Aby dostać się do menu Start należy myszką zjechać do lewego dolnego rogu ekranu, pojawi się wtedy przycisk przenoszący do niego.



Po jego kliknięciu pojawi się „kafelkowe” menu **Start** znane już z systemu Windows 8.



Kliknięcie przycisku **Start** prawym przyciskiem myszy otworzy menu kontekstowe, a w nim wyświetli zawartość menu Start w formie uproszczonej.



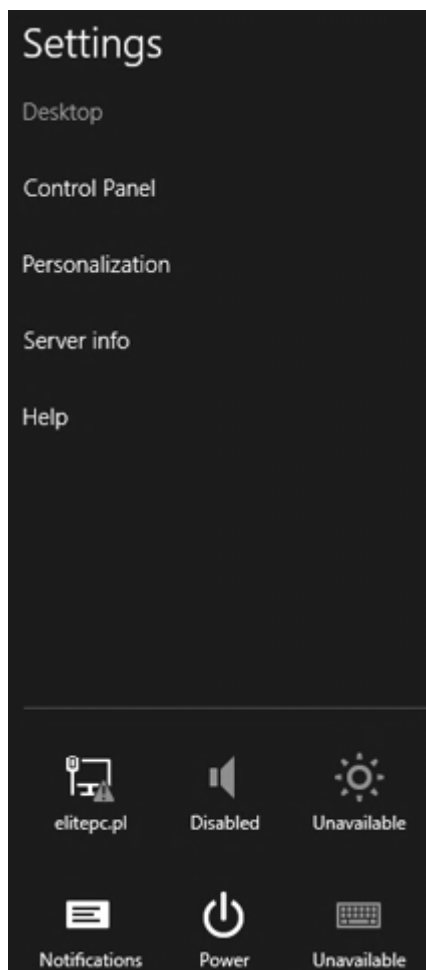
Z kolei ustawienie myszki w prawym dolnym rogu ekranu spowoduje pojawienie się bocznego menu oraz okienka informacyjnego. Zainstalowanie komponentu **Desktop**

**Experience** da możliwość zmiany wyglądu standardowych pasków. Domyślnie w bocznym menu znajdują się tylko trzy przyciski. **Wyszukaj (Search)** odpowiedzialny za wyszukiwanie, **Start** uruchamiający nowy ekran menu Start oraz **Ustawienia (Settings)**.

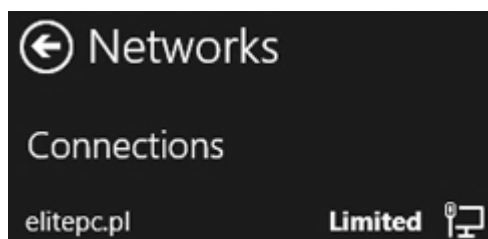


Przycisk **Ustawienia (Settings)** przenosi nas do innego menu bocznego związanego z ustawieniami. Znajdują się tam odnośniki do **Ustawień Pulpitu (Desktop)**, **Panelu Sterowania (Control Panel)**, **Opcji Personalizacji (Personalization)**, **Informacji (Server info)** oraz **Pomocy (Help)**. W jego dolnej części znajduje się także sześć ikon. Odpowiadają one kolejno za połączenia sieciowe, dźwięk, podświetlenie ekranu, notyfikacje, opcje związane z zasilaniem komputera oraz klawiaturami.



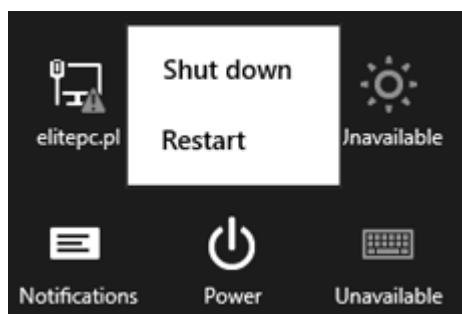


Po kliknięciu w **Networks** pojawią się informacje dotyczące aktualnego stanu połączeń sieciowych.

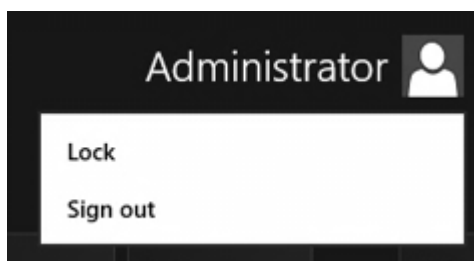


W kolejnym wybraniu przycisku **Power** pozwoli na wyłączenie bądź ponowne

uruchomienie komputera.



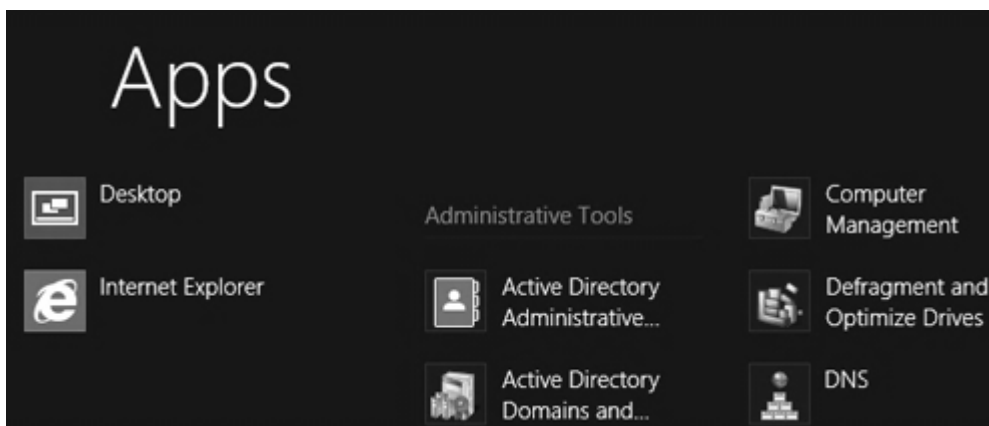
Wróciwszy do ekranu **Start**. W jego prawym górnym rogu znajduje się nazwa obecnie zalogowanego użytkownika. Po kliknięciu na niej pojawią się dwie opcje. Jedną z nich będzie zablokowanie komputera, a drugą wylogowanie się użytkownika. Gdy zostanie zainstalowany dodatek **Desktop Experience** dodatkowo pojawi się możliwość zmiany obrazka użytkownika.



Po kliknięciu w menu **Start** prawym przyciskiem myszy w dowolnym jego miejscu, w dolnej części ekranu się pasek, a na nim przycisk **All Apps**.



Jego użycie spowoduje przeniesienie do widoku, w którym zaprezentowane zostaną wszystkie konsole i aplikacje uporządkowane w odpowiednich sekcjach.



Na pasku menu znajduje się ikona **Menadżera Serwera (Server Manager)**. Stanowi on niejako centrum zarządzania serwerem. Głównie przy jego użyciu będzie odbywało się zarządzanie komputerem i instalowanie dodatkowych funkcji i ról. Zostanie on szczegółowo omówiony przy okazji instalacji ról serwera, a także podczas zarządzania nimi w najbliższych działach.



## 2.2. Czynności Post-instalacyjne

Kiedy na komputerze zainstalowane są już wszystkie urządzenia można spokojnie przystąpić do podstawowej jego konfiguracji. Z pomocą przychodzi **Konsola Zarządzania Serwerem (Server Manager)**, która w swoim głównym oknie prezentuje 4 podstawowe kroki. Pierwszym z nich jest konfiguracja serwera

lokalnego.



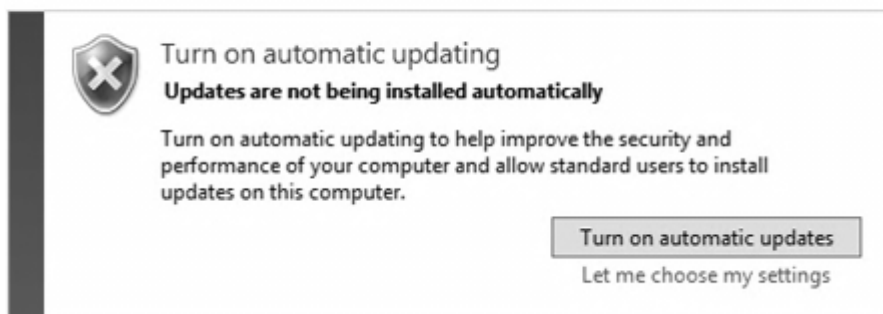
Po wybraniu opcji **Konfiguruj Serwer Lokalny (Configure this local server)** włączona zostanie konsola, w której można zmienić nazwę komputera, przyłączyć go do grupy roboczej, a także zarządzać aktualizacjami, firewallem, raportowaniem błędów, ustawieniami sieci, zwiększonymi zabezpieczeniami IE, itp.

Computer name	WIN-1GUSDGA931N	Last installed updates
Workgroup	WORKGROUP	Windows Update
		Last checked for updates
Windows Firewall	Public: On	Windows Error Reporting
Remote management	Enabled	Customer Experience Improvement Prog
Remote Desktop	Disabled	IE Enhanced Security Configuration
NIC Teaming	Disabled	Time zone
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID
Ethernet 2	IPv4 address assigned by DHCP, IPv6 enabled	
Operating system version	Microsoft Windows NT 6.2.8400.0	Processors
Hardware information	innotek GmbH VirtualBox	Installed memory (RAM)

### 2.2.1. Aktualizacje

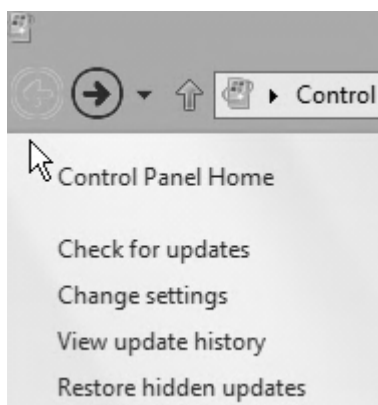
W pierwszej kolejności warto uruchomić aktualizacje automatyczne i zainstalować wszystkie dostępne aktualizacje, używając przycisku **Włącz automatyczne aktualizacje (Turn on automatic updates)**.

## Windows Update



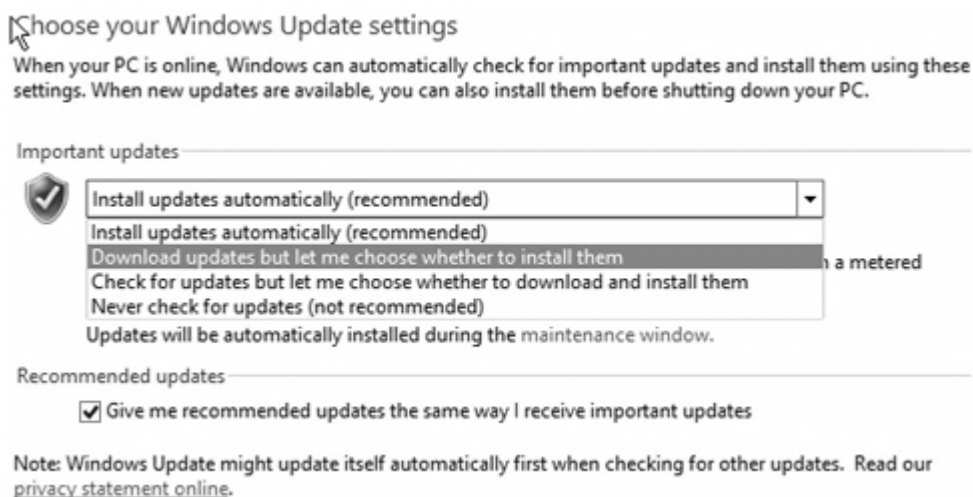
Kiedy system zostanie przeanalizowany można rozpocząć aktualizację klikając przycisk **Zainstaluj Aktualizacje (Install Updates)**.

W menu po lewej stronie należy wybrać opcję **Zmień Ustawienia (Change Settings)**.



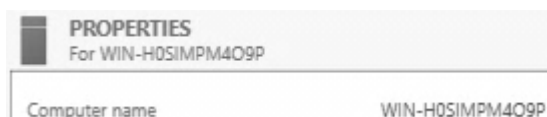
W oknie, które się pojawi najwygodniej będzie wybrać opcję pierwszą – **Zainstaluj aktualizacje automatycznie (Install updates automatically)**. Jeśli jednak na celu jest uniknięcie samoistnych instalacji aktualizacji, a co za tym idzie ponownych uruchomień komputera należy wybrać opcję drugą – **Pobierz aktualizacje, ale daj mi wybrać kiedy zostaną zainstalowane (Download updates but let me choose whether to Install them)**, która jest w przypadku serwera znacznie bezpieczniejsza

dla zachowania ciągłości pracy. Następnie należy kliknąć **OK**.

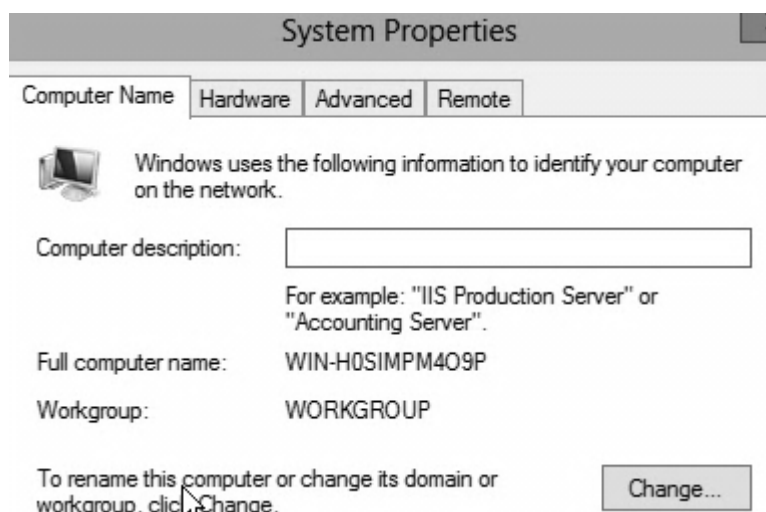


## 2.2.2. Zmiana nazwy komputera

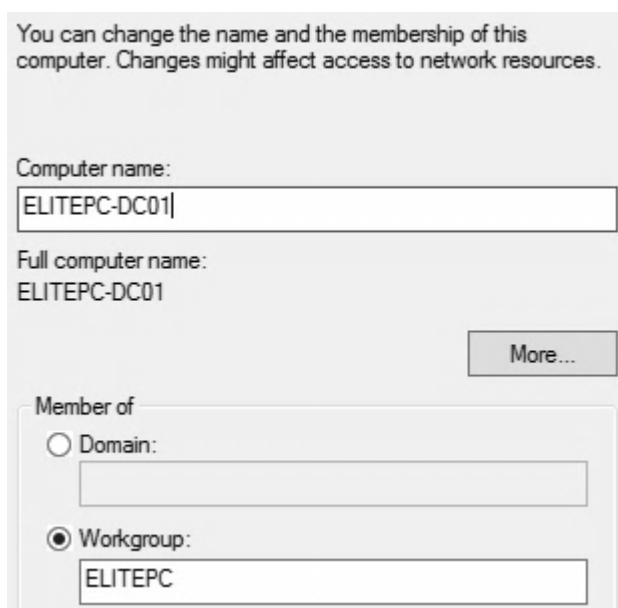
Na ekranie podsumowującym *Menadżera Serwera (Server Manager)*, w sekcji *Właściwości (Properties)* znajduje się parametr *Nazwa Komputera (Computer Name)*, gdzie należy kliknąć w nazwę komputera.



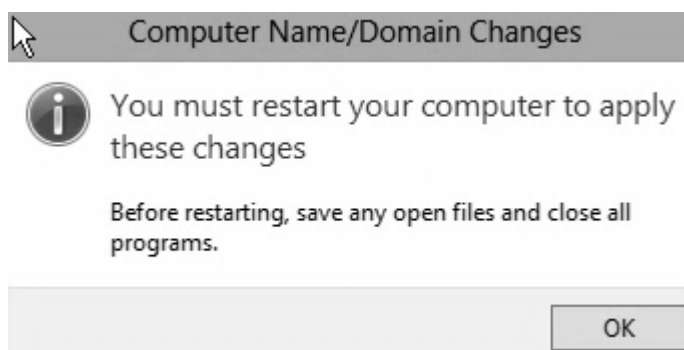
W karcie *Nazwa Komputera (Computer Name)* należy kliknąć przycisk **Zmień (Change)**.



Lepiej na początku ustalić sobie sposób nazewnictwa komputerów, aby utrzymać porządek w sieci np. ElitePC-DC01, gdzie ElitePC to nazwa firmy, DC – Kontroler Domeny (Domain Controller), a 01 to numer komputera. Zamiennie do DC w nazewnictwie można użyć skrótów SR dla oznaczenia serwera oraz WS (Work Station) dla stacji roboczych.

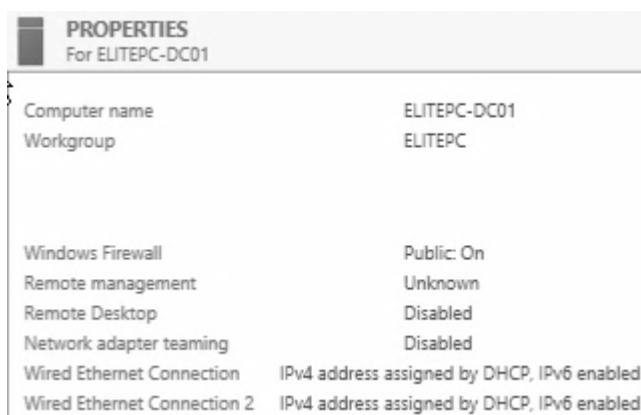


W komunikacie, który się pojawi należy kliknąć przycisk **OK** i uruchomić ponownie komputer.



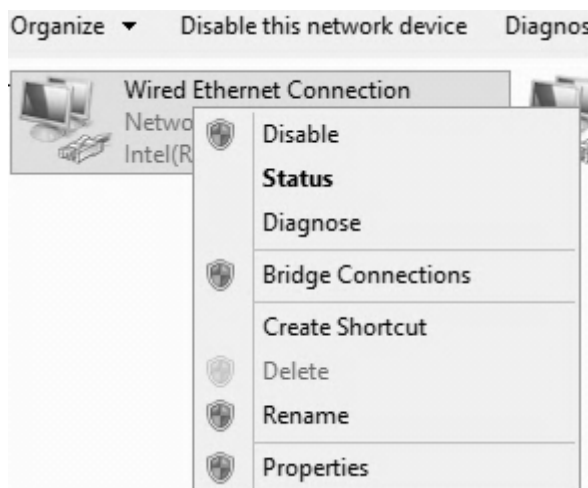
## 2.3. Konfiguracja sieci

Kolejnym krokiem będzie zmiana nazw interfejsów sieciowych tak, aby w każdej chwili wiedzieć czy operuje się na łączu internetowym czy też lokalnym. Połączenie z Internetem warto nazwać WAN, a z sieć lokalną LAN. Wystarczy kliknąć na wybranym połączeniu w konsoli zarządzania serwerem.

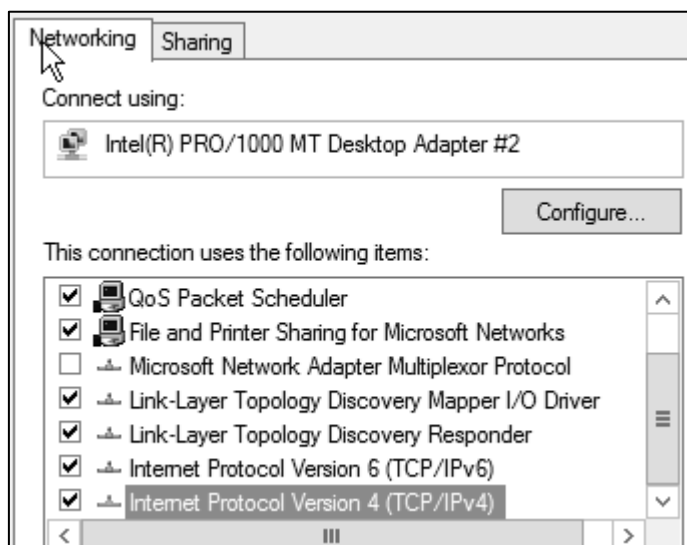


Na karcie sieciowej podpiętej do Internetu należy kliknąć prawym guzikiem i wybrać opcję **Zmień nazwę (Rename)**. Tą samą czynność należy powtórzyć dla drugiej karty sieciowej.





Przy interfejsie łączącym z siecią lokalną należy wejść we **Właściwości (Properties)** i ustalić stały adres IP, ponieważ chodzi tu o serwer. Należy wejść we Właściwości protokołu IPv4.




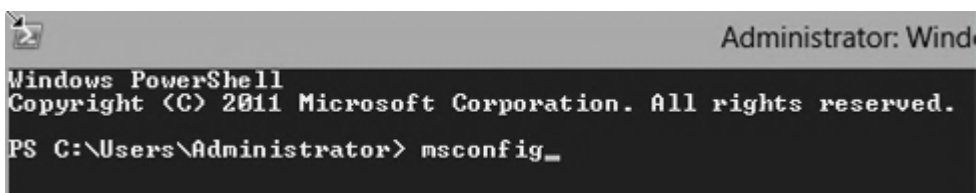
Należy wprowadzić adresy IP z dowolnego zakresu, na przykład standardowa adresacja 192.168.1.1 przy masce 255.255.255.0.

☐ Obtain an IP address automatically  
☒ Use the following IP address:

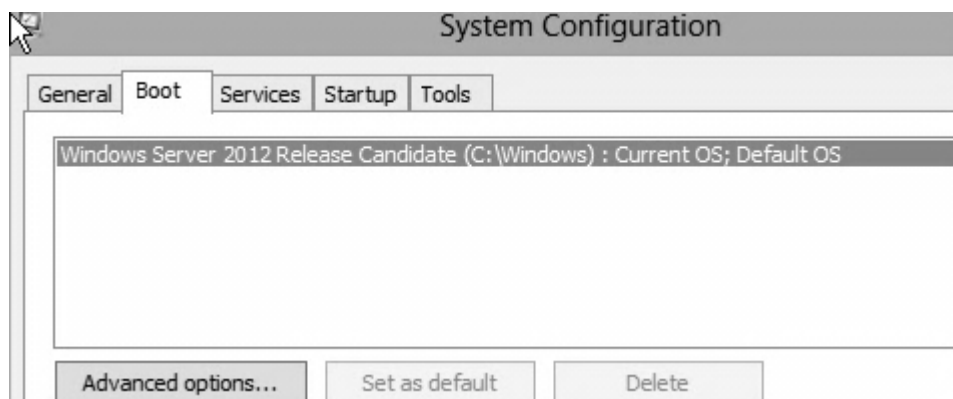
IP address:	192 . 168 . 0 . 1
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

## 2.4. Zarządzanie procesorami i pamięcią operacyjną

Ostatnim krokiem post instalacyjnym będzie uruchomienie większej liczby rdzeni procesora podczas startu systemu. W tym celu należy kliknąć na ikonę  paska Start związaną z konsolą *Power Shell* i wydać polecenie *msconfig*.



W zakładce *Rozruch (Boot)* konieczne jest kliknięcie *Opcji Zaawansowanych (Advanced options)*.



W następnej kolejności należy zaznaczyć opcję *Liczba procesorów (Number of*

*processors*), a w rozwijanej liście wybrać ich tak dużo jak to jest tylko możliwe.

**BOOT Advanced Options**

☒ Number of processors: 4

☐ Maximum memory: 0

☐ PCI Lock

☐ Debug

**Global debug settings**

☒ Debug port: COM1

☒ Baud rate: 115200

☐ Channel: 0

USB target name:

OK Cancel

### 3. Active Directory Domain Services

*Usługi Domenowe Active Directory (Active Directory Domain Services)* są niezbędne do awansu serwera na główny kontroler domeny. Serwer stanie się w ten sposób centralną bazą danych użytkowników odpowiedzialnych za autentykację i autoryzację użytkowników. Zostaną wyjaśnione takie pojęcia jak grupa robocza oraz domena. Czytelnik zrozumie, w jakim celu wdraża się domenę oraz na czym polega struktura drzewa oraz lasu. W następnej kolejności prześledzi proces instalacji pierwszego kontrolera domeny oraz nauczy się zarządzać obiektami przechowywanymi w Active Directory za pomocą konsoli *Active Directory Users and Computers* oraz *Active Directory Administrative Center*.

#### 3.1. Czym jest domena?

Na początek warto wyjaśnić kilka pojęć. Przede wszystkim, czym jest domena oraz dlaczego się ją stosuje zamiast grup roboczych. Dla przykładu w grupie roboczej lista kont użytkowników, uprawnienia użytkowników i zabezpieczenia systemu przechowywane są lokalnie, tzn. osobno na każdym komputerze wchodzącym w skład grupy roboczej. Każdy komputer jest jednostką autonomiczną. Aby móc pracować na komputerze należącym do grupy roboczej, trzeba mieć konto na tym komputerze. Wiąże się to z tym, że w przypadku, gdy osób pracujących na jednym komputerze może być więcej, co oznacza konieczność powielania kont na różnych komputerach. To samo się tyczy ustawień i oprogramowania. Co więcej, jeśli ktoś zachowa jakiś plik na jednym komputerze, to nie otworzy go już na innym chyba, że ręcznie go przekopiuje. Dla przykładu można wyobrazić sobie sytuację, w której zarządza się kilkunastoma komputerami i należy aktualizować programy, wprowadzać konta nowym pracownikom itp. Byłaby to strasznie żmudna praca. W domenie natomiast zarządzanie informacją o kontach użytkowników, komputerach domeny oraz zasadach obowiązujących w domenie jest scentralizowane. Komputery współdzielą bazę danych kont, zasad, zabezpieczeń, która znajduje się na kontrolerach domeny. W trakcie logowania się na konto w domenie Windows, dane

użytkownika porównywane są z danymi zapisanymi w kontrolerze domeny. Przestaje mieć znaczenie, z którego konkretnie komputera loguje się dany użytkownik, i tak zachowa swoje pliki i ustawienia. W przypadku instalacji nowego oprogramowania wystarczy, że administrator wyda taką „dyspozycję” na serwerze, a komputery podłączone do domeny same sobie poradzą z instalacją. Naturalnie logowanie na lokalne konta użytkowników tak jak to miało miejsce w przypadku grupy roboczej dalej jest możliwe. To oczywiście tylko czubek góry lodowej, więcej możliwości zostanie przedstawione w kolejnych rozdziałach.

Obecnie rozróżnia się dwa typy domen: NT4 oraz domena Active Directory, której będzie poświęcone najwięcej uwagi. Active Directory to usługa katalogowa będąca implementacją protokołu LDAP. Jest następcą NT4 i usuwa największe wady poprzednika. Wprowadzono do niej hierarchiczność przechowywania informacji, dużo wyższe limity przechowywania informacji (powyżej 1 miliona obiektów w domenie Active Directory) oraz rozszerzalność schematu zawierającego definicje obiektów.

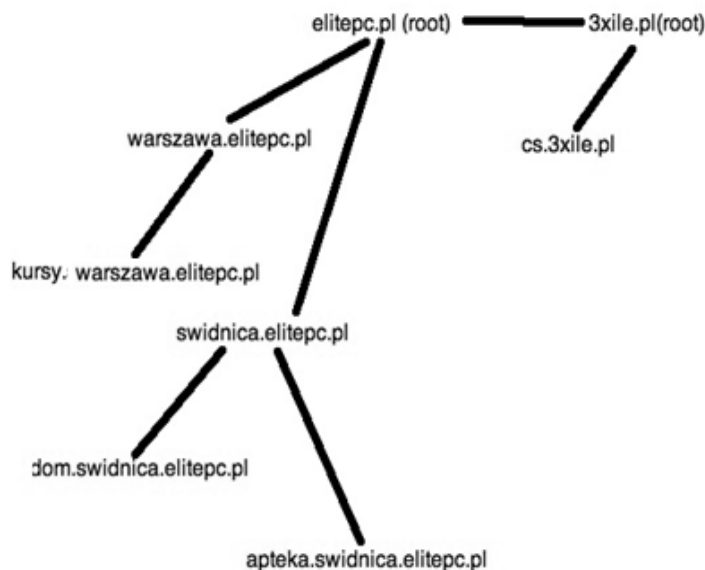
Domeny zorganizowane są hierarchicznie tworząc strukturę drzewa. Drzewo posiada zawsze przynajmniej jedną domenę – domenę najwyższego poziomu (ang. root) – korzeń drzewa. Pozostałe domeny (o ile istnieją) mogą być umieszczone poniżej domeny najwyższego poziomu, tworząc drzewo. Takie rozwiązanie często stosuje się w przypadku kilku siedzib firmy lub na przykład do wygodnego zarządzania komputerami w dwóch odległych od siebie miejscach. Jako przykład poniżej pokazano fragment drzewa dla firmy ElitePC:



Każde drzewo należy do jakiegoś lasu, każdy las składa się z przynajmniej jednego drzewa. Nie ma możliwości utrzymywania drzewa bez utrzymywania lasu.

### **Uwaga!**

To odnosi się również do domeny Active Directory – domena nie może istnieć samodzielnie, musi istnieć w jakimś drzewie i jakimś lesie. Jeżeli jest to pierwsza domena, to tworzy pierwsze drzewo, (którego korzeniem się staje) oraz pierwszy las. Poniżej przykład lasu z dwoma drzewami:

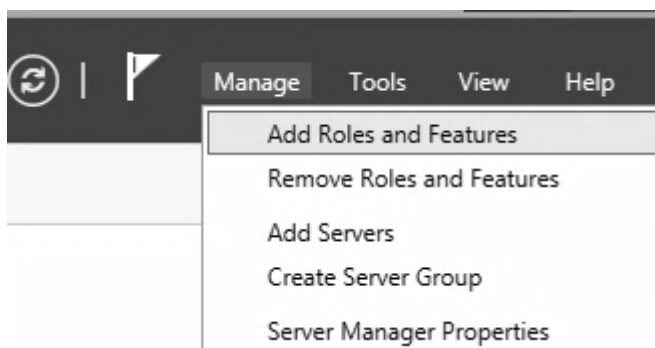


### 3.2. Instalacja Active Directory Domain Services

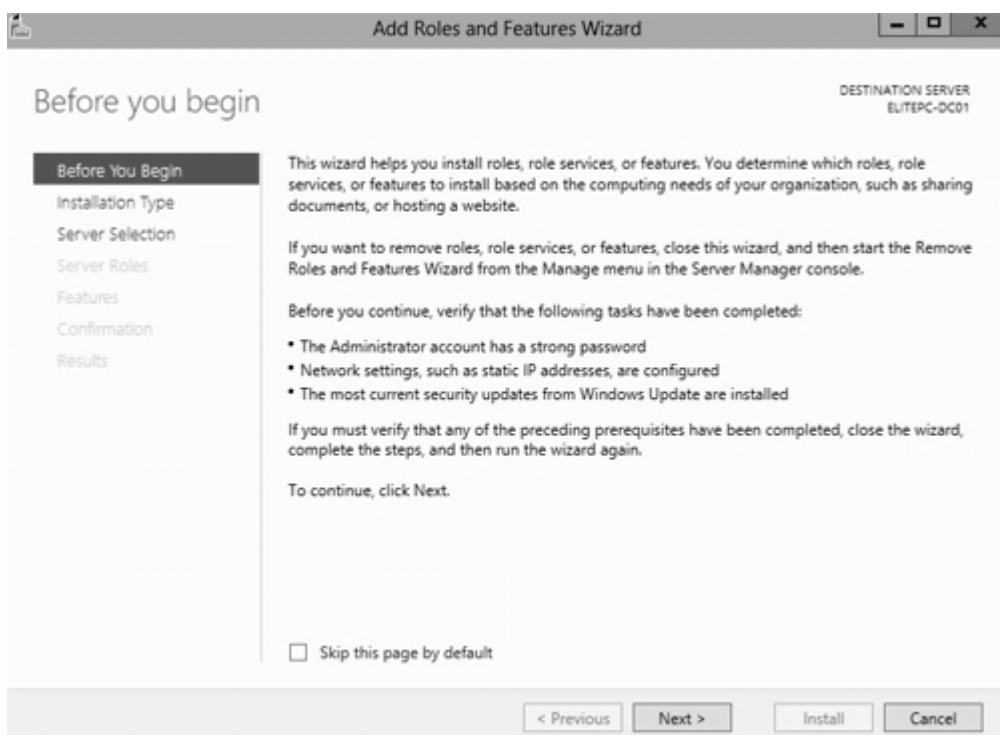
W przypadku, gdy serwer jest kierowany ku zastosowaniom domowym, czy małej firmy wystarczy jedna domena. Aby rozpocząć instalację należy kliknąć ikonkę **Menadżer Serwera (Server Manager)** znajdującą się obok guzika **Start**. Warto zapamiętać ten krok, gdyż będzie on często wykonywany.



W **Menadżerze Serwera (Server Manager)** będą instalowane praktycznie wszystkie role dostępne w tym produkcie.



W górnym menu po prawej stronie należy kliknąć przycisk *Zarządzaj (Manage)*, a następnie opcję *Dodaj Role i Funkcje (Add Roles and Features)*. Pojawi się plansza powitalna, gdzie konieczne jest kliknięcie przycisku *Dalej (Next)*.



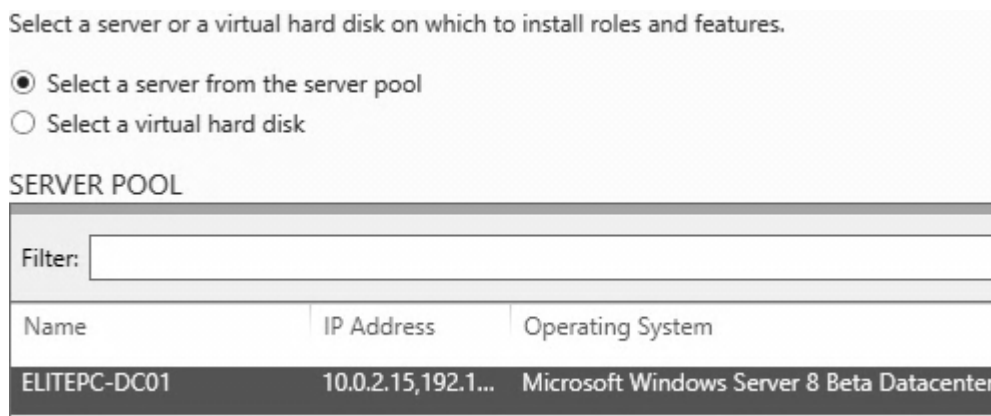
Jedną z nowości Windows Server 2012 jest możliwość instalowania ról serwera na zdalnych komputerach, obrazach dysków VHD czy na maszynach wirtualnych. Na potrzeby tej publikacji i dla ułatwienia zrozumienia omawianych zagadnień na razie



będą instalowane wszelkie nowe role i funkcje na tej samej maszynie. Należy wybrać więc opcję pierwszą Role-based i kliknąć **Dalej (Next)**. Instalacja oparta na scenariuszu jest nowością w systemie Windows Server 2012. Dzięki niej można jednocześnie instalować komponenty związane z **Usługami Pulpitu Zdalnego (Remote Desktop Services)**. AD jest instalowane, jako klasyczna rola.

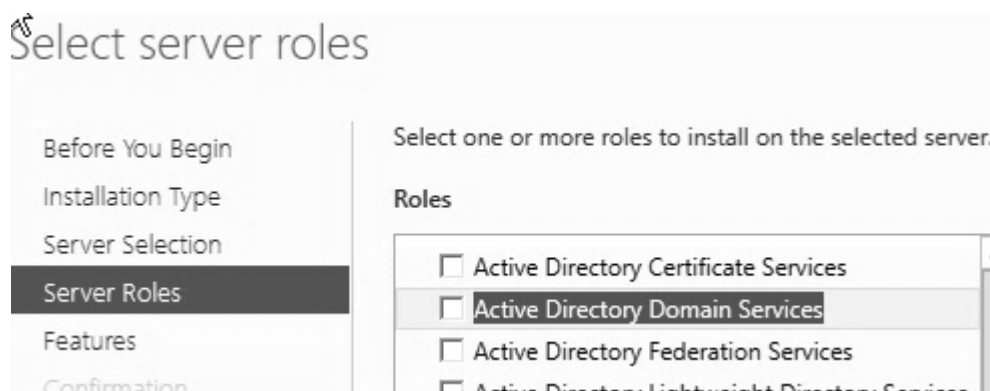


W kolejnym kroku należy wybrać serwer, na jakim dana rola ma zostać skonfigurowana. W środowisku przykładowym naturalnie do wyboru jest tylko jedna maszyna. Należy ją zaznaczyć i wybrać przycisk **Dalej (Next)**. Jest to kolejna z nowości w systemie Windows Server 2012. Pozwala ona zdalnie instalować role na innych serwerach, a także je wgrywać na wirtualne dyski VHD, które można potem podmontować pod konkretny serwer.

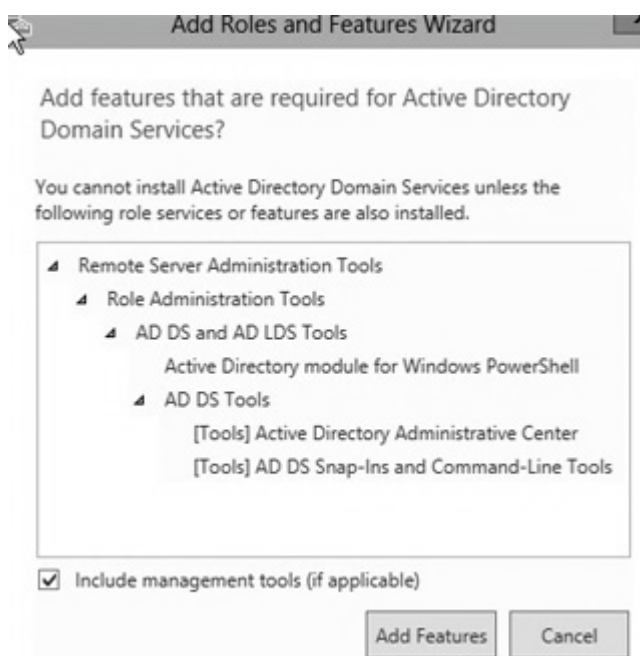


Następnie należy wybrać **Usługi Domenowe w Usłudze Active Directory (Active Directory Domain Services)**. Znaczący temat zauważają, że Role są niemalże

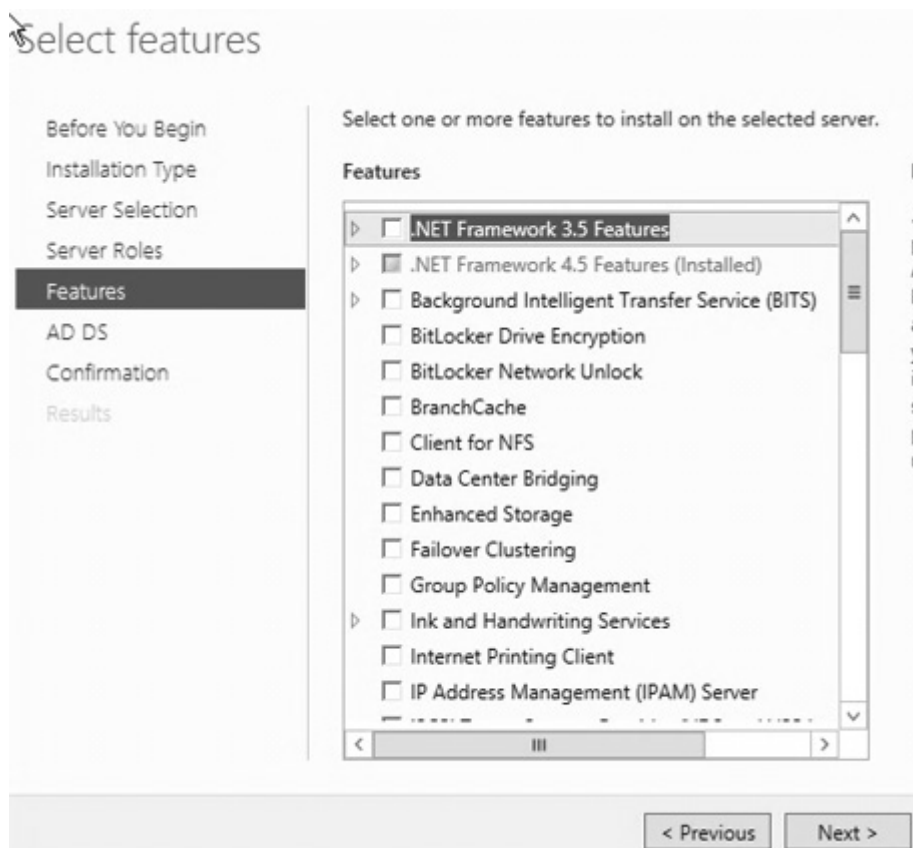
identyczne z tymi z Windows Server 2008 R2. Nowością jest **Zdalny Dostęp (Remote Access)**, który w rzeczywistości jest nową nazwą dla **Direct Access** oraz **Usługi Aktywacji Woluminowej (Volume Activation Services)** związane z aktywacją licencji woluminowych.



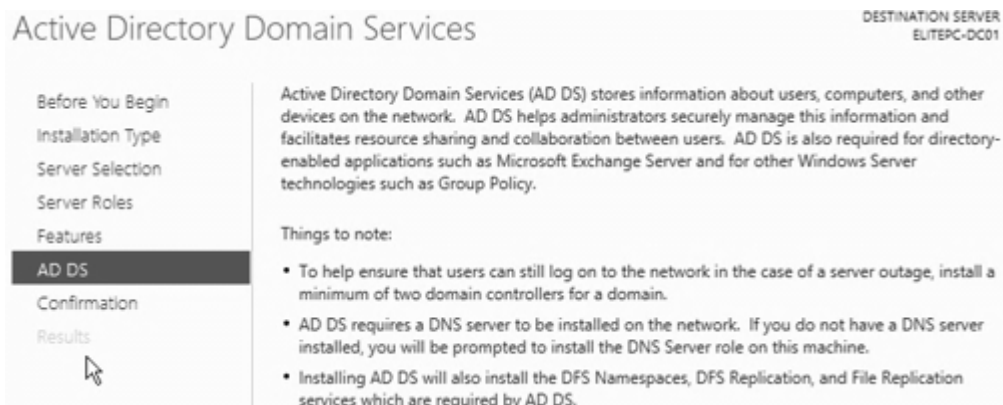
Pojawi się komunikat, na którym należy kliknąć **Dodaj Wymagane Funkcje (Add Features)**, a następnie **Dalej (Next)**.



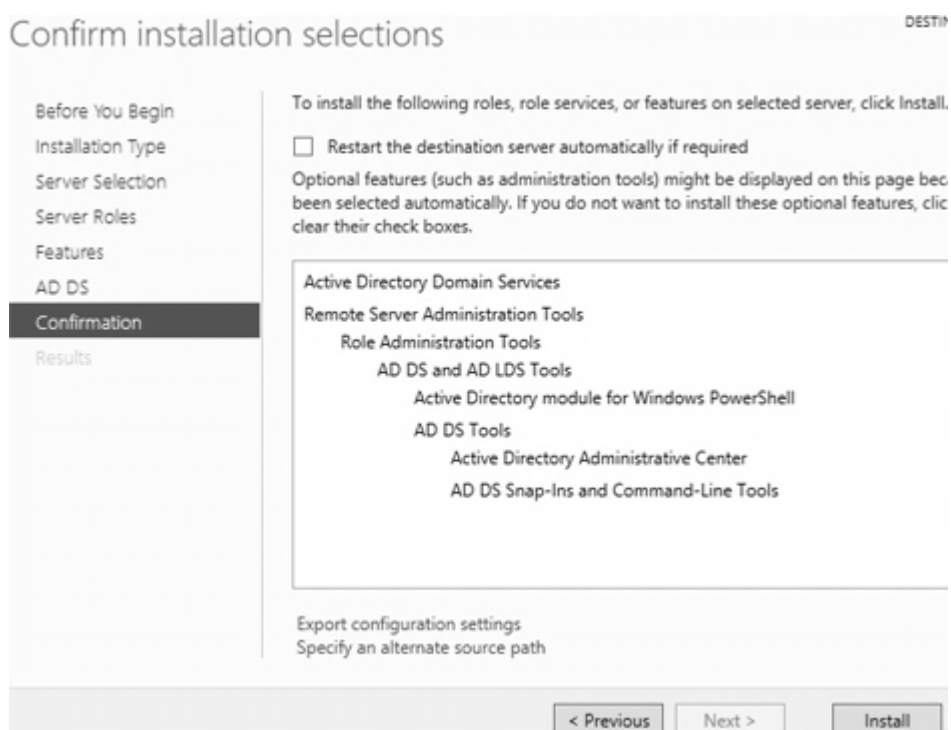
Następnie ponownie należy kliknąć przycisk **Dalej (Next)**.



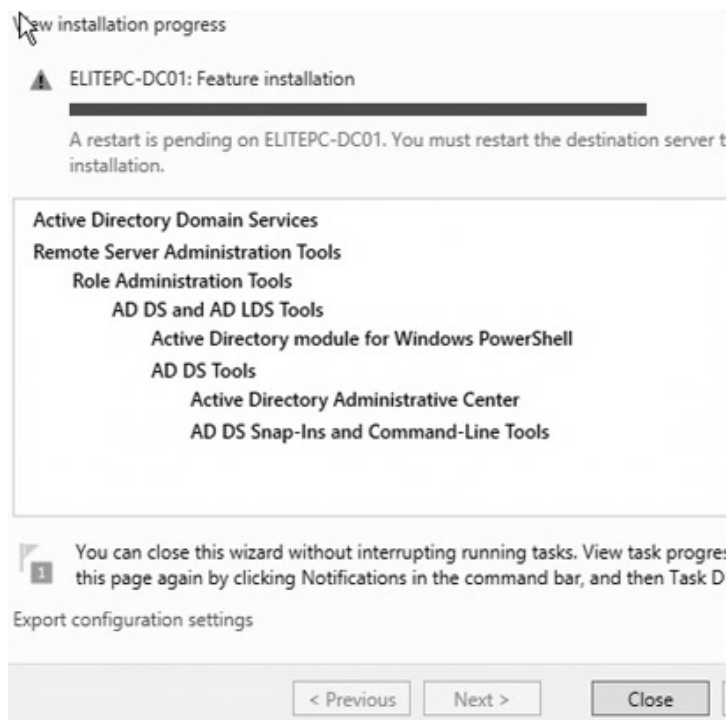
Poniższe okno prezentuje informacje podsumowujące oraz dotyczące dalszych kroków instalacyjnych. Między innymi powiadamia ono o konieczności zainstalowania serwera DNS, ponieważ ta rola jest wymagana do prawidłowego działania AD. Wgrany zostanie także komponent odpowiadający za replikację serwera DFS, który został wprowadzony już w Windows 2003 R2 do replikacji wolumenu SYSVOL. Po raz kolejny należy kliknąć **Dalej (Next)**.



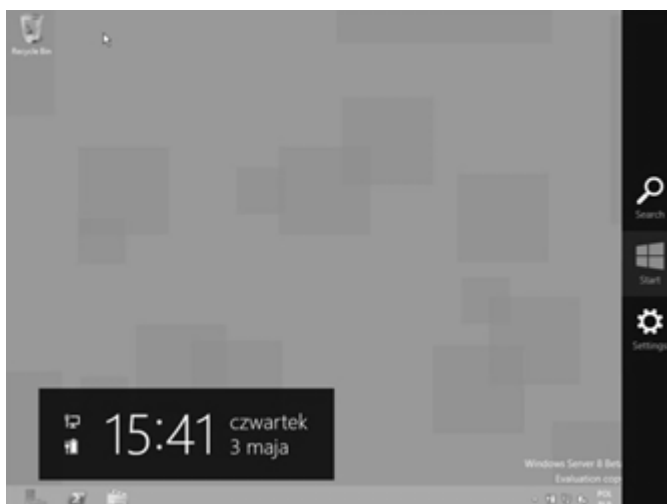
Na ostatniej już planszy należy wybrać przycisk **Zainstaluj (Install)**.



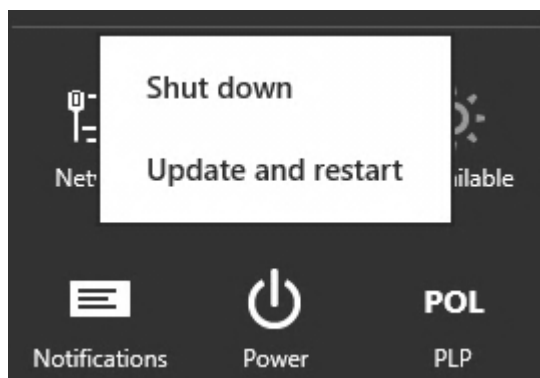
Proces instalacji chwilę potrwa, gdy dobiegnie końca należy kliknąć **Zakończ (Close)**.



Komputer należy uruchomić ponownie, aby instalacja dobiegła końca. Będąc na pulpicie należy wcisnąć kombinację klawiszy **Windows** + **C**, a następnie wybrać **Ustawienia (Settings)**.

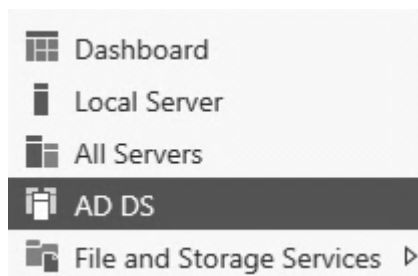


Następnie należy wybrać **Zasilanie (Power)** i **Uruchom Ponownie (Restart)**.



### 3.3. Wstępna konfiguracja AD DS

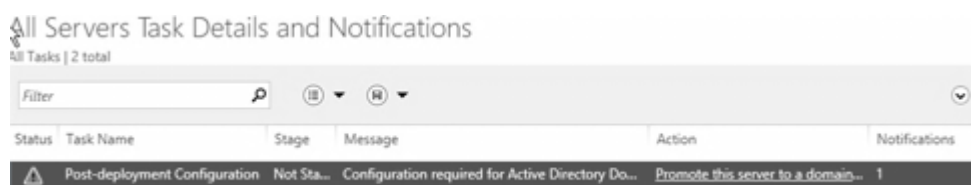
W **Menadżerze Serwera (Server Manager)** w menu po lewej stronie należy kliknąć w **Usługi Domenowe w Usłudze Active Directory (AD DS)**.



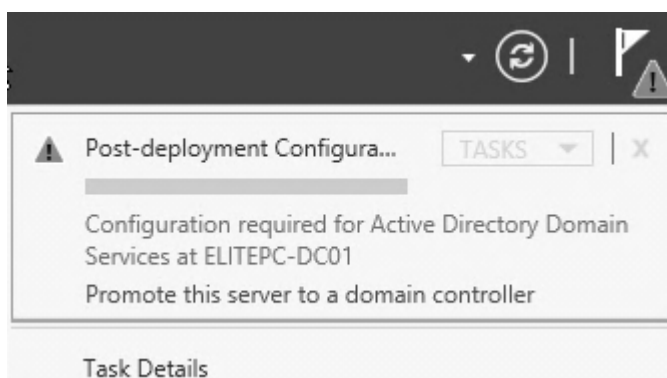
Kiedy plansza się załaduje, po prawej stronie znajduje się wyróżniony napis **Więcej (More)**, który należy wybrać.



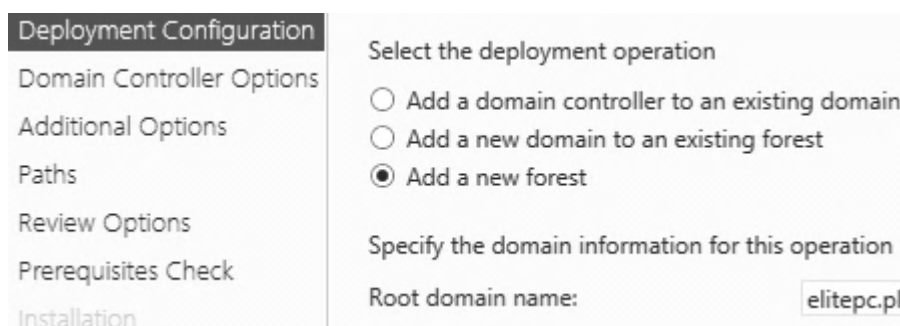
A następnie **Promuje ten serwer na kontroler domeny (Promote this server to a domain Controller)** poprzez wybranie odpowiedniej akcji.



To samo można uzyskać korzystając bezpośrednio z menu akcji, które oznaczone jest w górnym menu chorągiewką.

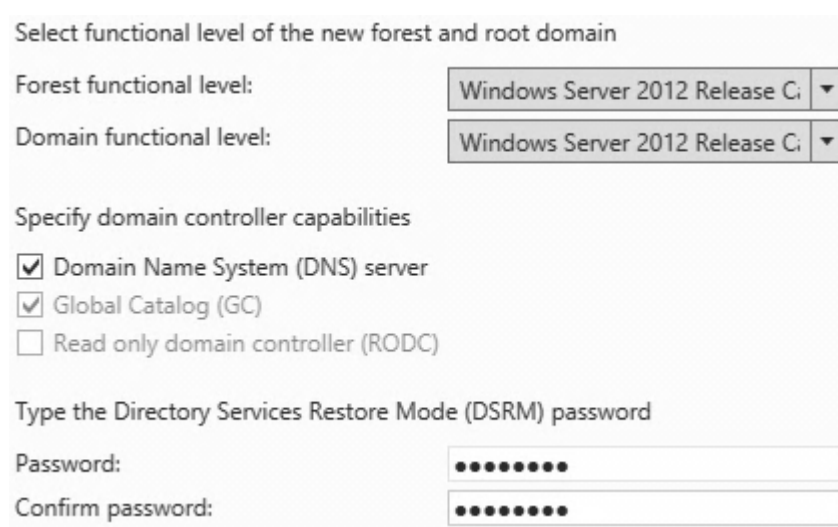


Ponieważ tworzony jest pierwszy serwer, który jednocześnie będzie głównym kontrolerem domeny w sieci, należy wybrać opcję trzecią. W przeciwnym wypadku, kiedy serwer miałby zostać wpięty do istniejącej już struktury, konieczne byłoby wybranie opcji drugiej lub pierwszej. Niezbędne jest także podanie nazwy domeny, która ma zostać stworzona.

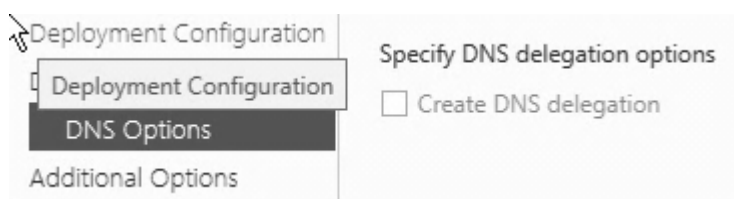


Należy ustawić poziom funkcjonalności lasu tak, aby był kompatybilny z resztą

sieci. Jeżeli istniałby już jakiś kontroler domeny, pracujący pod kontrolą Windows Server 2003, musiałby zostać wybrany taki sam poziom. Wiązałoby się to niestety z utratą nowych funkcjonalności wprowadzonych w Windows Server 2012. W przypadku przedstawionym w książce należy wybrać poziom najwyższy, czyli Windows Server 2012. Przy okazji zostanie zainstalowany serwer DNS, ponieważ takowego w domenie jeszcze nie ma, a jest niezbędny do jej prawidłowego funkcjonowania. Konieczne jest także podanie w kreatorze hasła niezbędnego w razie potrzeby przywracania usługi katalogowej.



W następnej kolejności należy **Dalej (Next)**.



Na kolejnej planszy nie są konieczne żadne zmiany, dlatego też należy przejść do kolejnej karty klikając **Dalej (Next)**, chyba, że nazwa kontrolera dla komputerów korzystających z NetBIOS ma być inna niż domyślna.



Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

Podobnie jest w przypadku ścieżek, chyba, że dane mają być przechowywane na osobnym nośniku.

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:	<input type="text" value="C:\Windows\NTDS"/>
Log files folder:	<input type="text" value="C:\Windows\NTDS"/>
SYSVOL folder:	<input type="text" value="C:\Windows\SYSVOL"/>

Na planszy podsumowującej należy kliknąć **Dalej (Next)**.

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "elitepc.pl". This is also the name of the new forest.

The NetBIOS name of the domain: ELITEPC

Forest Functional Level: Windows Server 2012 Release Candidate

Domain Functional Level: Windows Server 2012 Release Candidate

Additional Options:

Global catalog: Yes

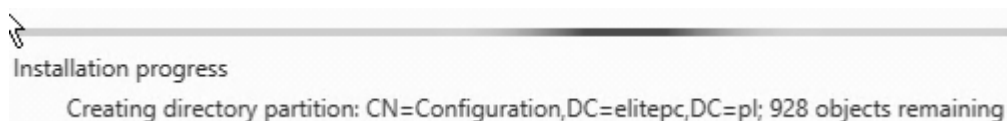
DNS Server: Yes

Create DNS Delegation: No

System zostanie poddany analizie. Jeżeli wszystko przebiegnie pomyślnie można kliknąć przycisk **Zainstaluj (Install)**.

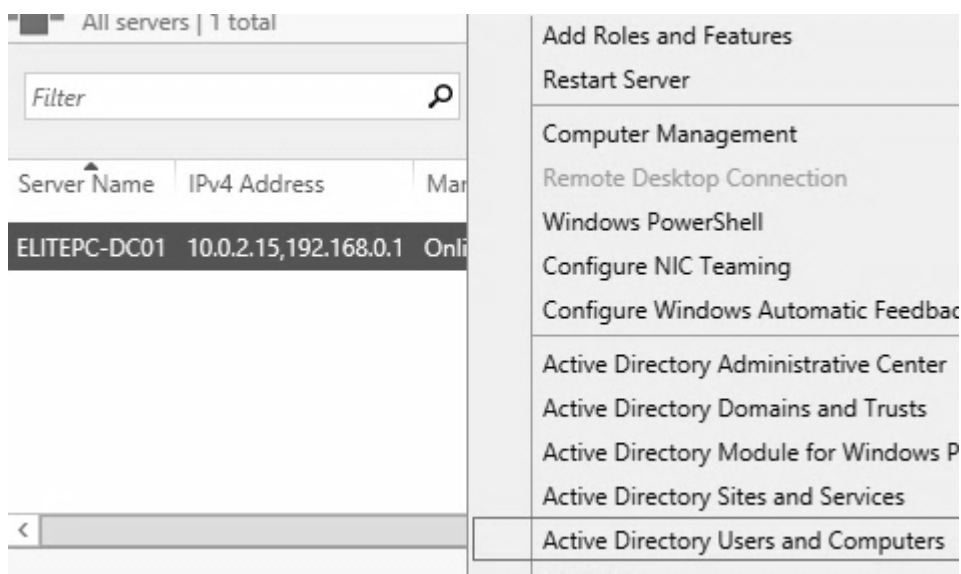
✓ All prerequisite checks passed successfully. Click 'Install' to begin installation.

Proces instalacji zajmie dłuższą chwilę. Należy zatem uzbroić się w cierpliwość.



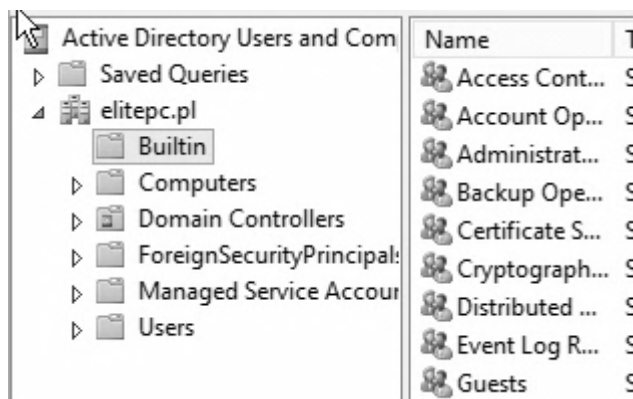
### 3.4. Active Directory Users and Computers

Po ponownym uruchomieniu komputera w *Menadźerze Serwera (Server Manager)* konieczne jest wybranie *AD DS (Active Directory Domain Services)*, następnie na serwerze należy kliknąć prawym klawiszem myszy i wybrać *Komputery i Użytkownicy Usługi Active Directory (Active Directory Users and Computers)*.

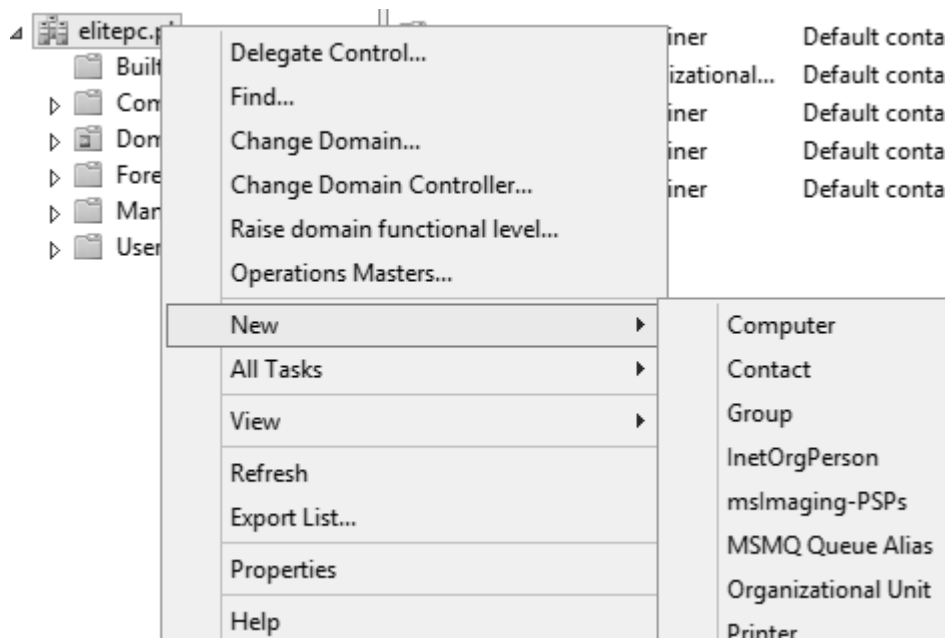


Jest to miejsce szalenie ważne, ponieważ będą w nim tworzone grupy i konta dla użytkowników oraz komputerów, będą im przypisywane odpowiednie role i uprawnienia. W system Windows jest już wbudowana całkiem pokaźna liczba grup bezpieczeństwa. W przypadku przykładowym nie będzie jednak potrzeby tworzenia nowych grup, mimo, że daje to ogromne możliwości w przydzielaniu i odbieraniu uprawnień użytkownikom. Opis ról dostępny jest pod adresem:

<http://technet.microsoft.com/pl-pl/library/cc756898%28WS.10%29.aspx> .



Przechodząc do praktyki, warto od samego początku utrzymywać ład i porządek, a także intuicyjne nazwy. Dlatego też na początek zostanie stworzona nowa Jednostka Organizacyjna. Dla zobrazowania czym ona jest, można ją traktować, jako byt podobny do katalogu. W celu jej utworzenia konieczne jest kliknięcie prawym klawiszem myszy na nazwie domeny, następnie w przycisk **Nowy (New)** i wybranie opcji **Jednostka Organizacyjna (Organizational Unit)**.

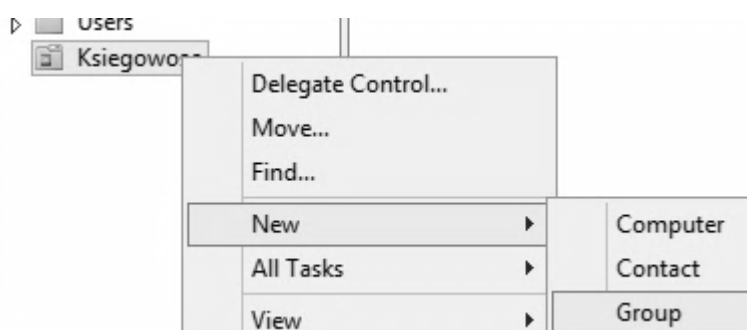


W celu ćwiczeniowym zostanie stworzona jednostka organizacyjna o nazwie

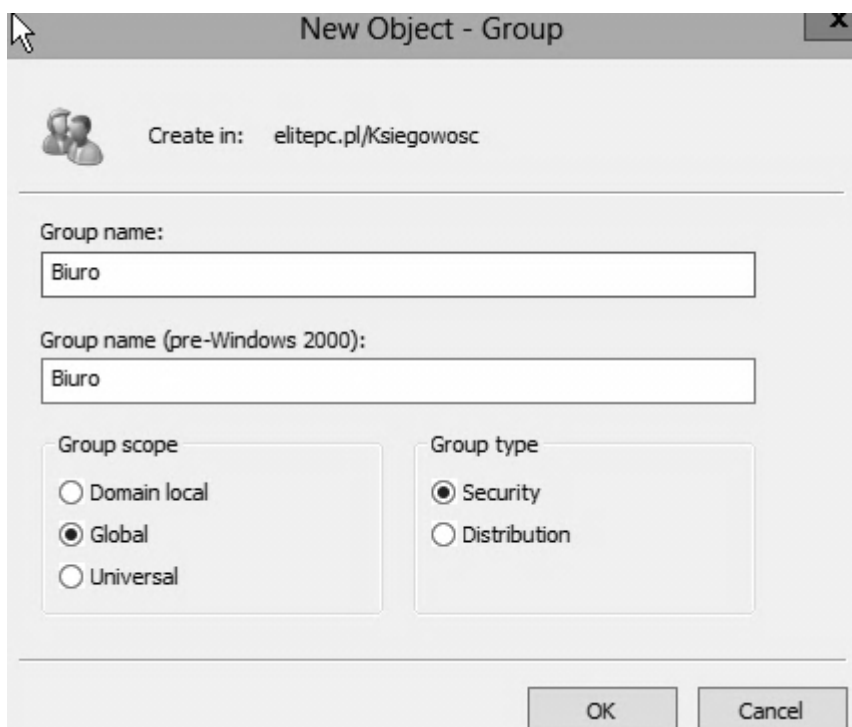
Księgowość (oczywiście starając się nie używać przy tym polskich znaków), gdzie będą przechowywani zatrudnieni księgowi. Wybór, a także akceptacja jej utworzenia zostaną zatwierdzone przyciskiem **OK**.



Następnie powstanie nowa grupa. W tym celu należy kliknąć prawym przyciskiem myszy na nowo powstałym elemencie, a następnie w *Nowy (New)* i *Grupa (Group)*.



Dokonany zostanie podział na pracowników, którzy pracują na kasach oraz na tych, którzy pracują w biurze. Odpowiednio niech będą to grupy Kasa i Biuro. Czynność trzeba powtórzyć dla każdej z grup. Na planszy, która się pojawi należy podać nazwę dla grupy oraz zaznaczyć opcje w taki sam sposób jak jest to zrobione na poniższej ilustracji i kliknąć przycisk **OK**.



New Object - Group

Create in: elitepc.pl/Ksiegowosc

Group name:  
Biuro

Group name (pre-Windows 2000):  
Biuro

Group scope

- ☐ Domain local
- ☒ Global
- ☐ Universal

Group type

- ☒ Security
- ☐ Distribution

OK Cancel

Grupy dystrybucyjne mogą być używane tylko z aplikacjami poczty e-mail (np. Exchange) do wysyłania poczty e-mail do grup użytkowników. Grupy dystrybucyjne nie obsługują zabezpieczeń, co oznacza, że nie są wyświetlane na listach arbitralnej kontroli dostępu (DACL, Discretionary Access Control List). Jeśli jest potrzebna grupa służąca do kontroli dostępu do zasobów udostępnionych, należy utworzyć grupę zabezpieczeń.

Grupy zabezpieczeń, jeśli są używane z rozważą, stanowią wydajny sposób udzielania dostępu do zasobów w sieci.

Za pomocą grup zabezpieczeń można wykonywać następujące operacje:

- Przypisywanie praw użytkownika grupom zabezpieczeń w usłudze Active Directory. Prawa użytkownika są przypisywane grupie zabezpieczeń w celu ustalenia czynności, jakie członkowie danej grupy mogą wykonać w zakresie domeny (lub lasu). Prawa użytkownika są automatycznie

przypisywane niektórym grupom zabezpieczeń podczas instalowania usługi Active Directory, aby ułatwić administratorom określenie roli administracyjnej poszczególnych osób w domenie. Na przykład użytkownik dodany do grupy „Operatorzy kopii zapasowych” w usłudze Active Directory może wykonywać kopie zapasowe plików i katalogów znajdujących się na każdym kontrolerze domeny, a także przywracać te pliki i katalogi z kopii zapasowych. Jest to możliwe, ponieważ domyślnie grupie „Operatorzy kopii zapasowych” są automatycznie przypisywane prawa użytkownika, wykonywanie kopii zapasowych plików i katalogów oraz przywracanie plików i katalogów, a członkowie grupy dziedziczą prawa użytkownika przypisane grupie.

- Za pomocą przystawki **Zasady grupy (Group Policies)** można przypisać grupom zabezpieczeń prawa użytkownika, aby ułatwić delegowanie określonych zadań. Przypisując delegowane zadania, należy zachować dużą ostrożność, ponieważ niedoświadczony użytkownik mający zbyt wiele praw w grupie zabezpieczeń stanowi zagrożenie dla bezpieczeństwa sieci.
- Przypisywanie uprawnień do zasobów grupom zabezpieczeń. Uprawnień nie wolno mylić z prawami użytkownika. Uprawnienia przypisuje się grupom zabezpieczeń dla danego zasobu udostępnionego. Decydują one o tym, kto ma mieć możliwość dostępu do zasobu i na jakim poziomie np. pełna kontrola (Full Control). Niektóre uprawnienia są przypisywane automatycznie np. dla obiektów domeny, po to aby określić różne poziomy dostępu domyślnych grup, jak np. Administratorzy domeny czy Operatorzy kont.

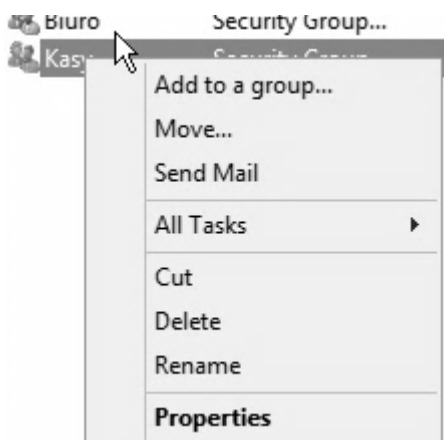
Grupy zabezpieczeń wymieniane są na listach DACL. Listy te określają uprawnienia do obiektów i zasobów. Administratorzy powinni przypisywać uprawnienia do zasobów (drukarek, udziałów plików itp.) nie pojedynczym użytkownikom, lecz całym grupom zabezpieczeń. Przypisywanie uprawnień grupie jest o tyle wygodne, że nie trzeba powtarzać wielokrotnie tej samej procedury. Każde konto, które zostało przydzielone do grupy otrzymuje prawa narzucone tej grupie w usłudze

Active Directory, tak samo jak i uprawnienia tej grupy do określonych zasobów.

Grupy zabezpieczeń, podobnie jak grupy dystrybucyjne mogą zostać użyte jako adresaci poczty e-mail. Gdy zostanie wysłana wiadomość e-mail do danej grupy, otrzymają ją wszyscy jej członkowie.

Grupy będą bardzo pomocne jeśli większej liczbie użytkowników będą miały zostać przypisane dane uprawnienia, a innej już nie, np. w ćwiczeniowym przypadku kasjerzy nie powinni mieć tak wysokich uprawnień jak pracownicy biurowi.

Naturalnie tak utworzonej grupie należałoby nadać odpowiednie prawa. W przypadku z przykładu niech to będą prawa zwykłego Użytkownika. Zostanie więc wykorzystana wbudowana w system Windows grupa bezpieczeństwa. W tym celu należy kliknąć prawym klawiszem myszy na **Właściwości (Properties)** na przykład kasjerów.



W oknie, które się pojawi konieczne jest przejście do zakładki **Członek Grupy (Member Of)** i wybranie przycisku **Dodaj (Add)**.

General	Members	Member Of	Managed By
---------	---------	-----------	------------

Member of:

Name	Active Directory Domain Services Folder

Add... Remove

Następnie należy kliknąć **Zaawansowane (Advanced)**.

Select Groups

?

X

Select this object type:

Groups or Built-in security principals

Object Types...

From this location:

elitepc.pl

Locations...

Enter the object names to select (examples):

Check Names

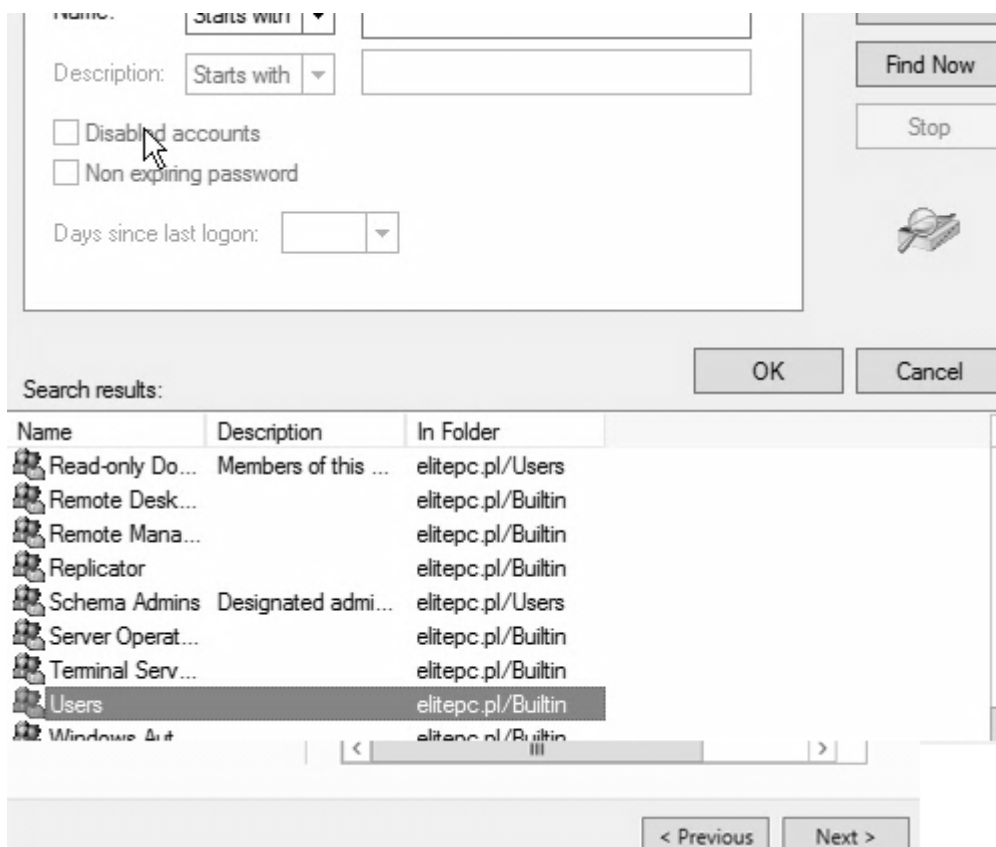
Advanced...

OK

Cancel

W dalszej kolejności należy kliknąć **Znajdź teraz (Find Now)**, a z listy, jaka się wygeneruje wybrać **Użytkownicy (Users)** i kliknąć przycisk **OK**, a następnie jeszcze raz **OK**.

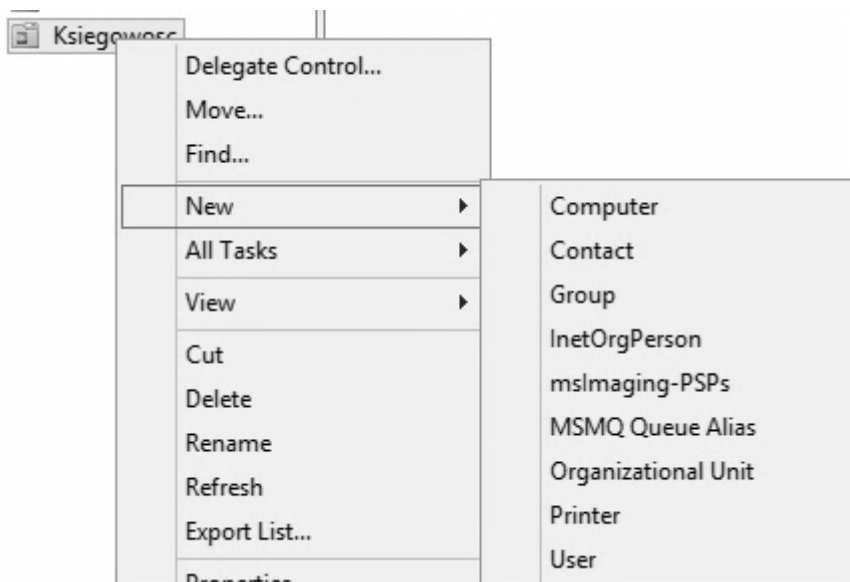




Jak widać kasjerzy są już w Użytkownikach. Należy kliknąć **OK**.



Dla testu zostanie dodany użytkownik, na którym będą przeprowadzane różne doświadczenia w dalszej części książki. W celu stworzenia użytkownika należy prawym przyciskiem myszy kliknąć na **Księgowość > Nowy (New) > Użytkownik (User)**.



Trzeba wypełnić wszystkie pola. Ważna jest nazwa logowania użytkownika, gdyż to dzięki niej będzie się on mógł zalogować na danym komputerze. W przykładzie zastosowano nazwę kasjer\_01.

New Object - User

Create in: elitepc.pl/Ksiegowosc

First name: kasjer\_01 Initials:

Last name:

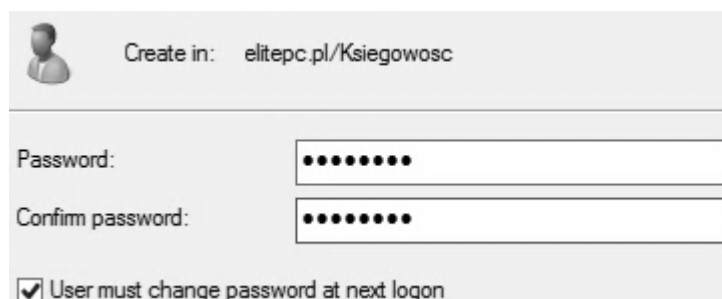
Full name: kasjer\_01

User logon name: kasjer\_01 @elitepc.pl

User logon name (pre-Windows 2000): ELITEPC\ kasjer\_01

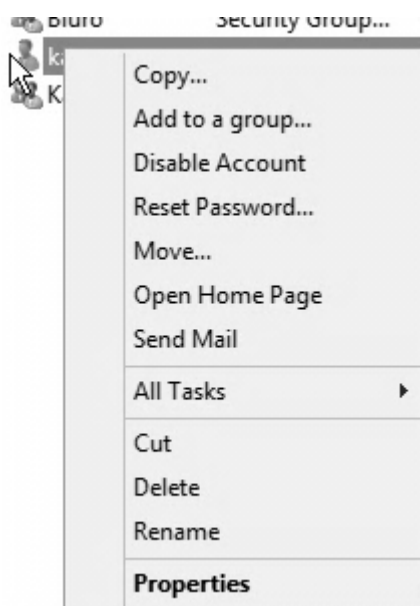
Na następnej karcie należy wybrać dla tego użytkownika odpowiednie hasło. Warto zostawić zaznaczoną opcję *Użytkownik musi zmienić hasło przy następnym*

**logowaniu** (*User must change password at next logon*), aby to on mógł sobie w trakcie pierwszego logowania je zmienić wedle własnych upodobań. Należy kliknąć dalej **Dalej** (*Next*), a następnie **Zakończ** (*Finish*).

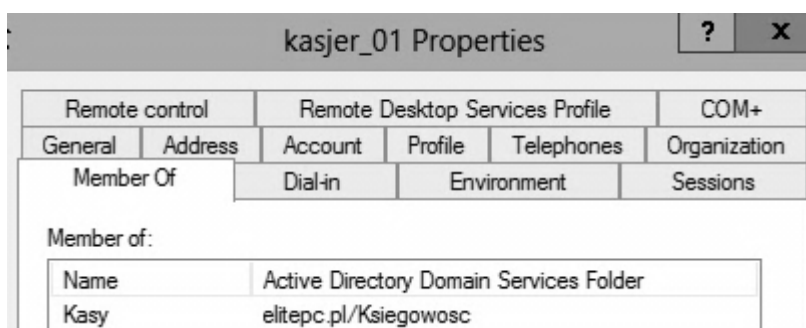


The screenshot shows a user creation window. At the top, it says 'Create in: elitepc.pl/Ksiegowosc'. Below this are two text boxes: 'Password:' and 'Confirm password:', both containing eight dots. At the bottom, there is a checkbox labeled 'User must change password at next logon' which is checked.

W następnej kolejności należy wejść w jego **Właściwości** (*Properties*) klikając prawym przyciskiem myszy, a następnie w zakładkę **Członek Grupy** (*Member of*).



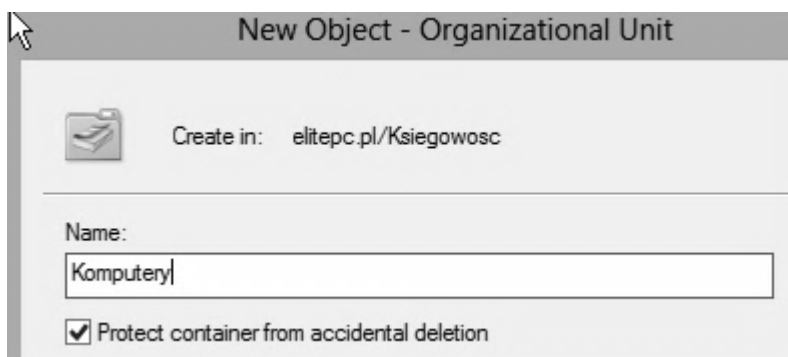
Domyślnie jest on **Użytkownikiem Domeny** (*Domain Users*). Można więc skasować tą pozycję, a potem dodać go do grupy "Kasy".



Grupę kasy można natomiast teraz przypisać do grupy ***Użytkownicy Domeny (Domain Users)***. To, co zostało uzyskane to pewnego rodzaju hierarchia (dziedziczenie). Użytkownicy należą do grupy Kasy, a grupa Kasy należy do jednej lub więcej innych grup. Dzięki temu można swobodnie zarządzać uprawnieniami wielu użytkowników naraz zamiast każdego użytkownika z osobna.

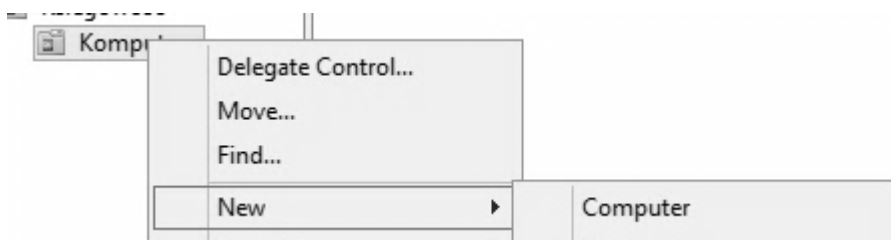
Należy sprytnie zarządzać zarówno grupami użytkowników jak i jednostkami organizacyjnymi, ponieważ nie tylko ułatwi to pracę administratorowi systemu i zwiększy bezpieczeństwo, ale także pozwoli wydajnie zarządzać np. Zasadami grupy, które można przyłączać wyłącznie do jednostek organizacyjnych.

Zostanie teraz stworzona kolejna jednostka organizacyjna, lecz tym razem wewnątrz księgowości. Zostanie nazwana "Komputery". Będą tam przechowywane konta dla komputerów w tym dziale.

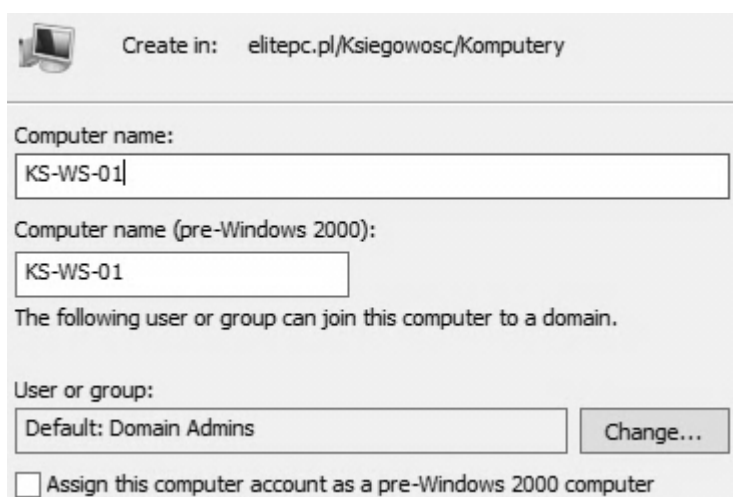


Teraz należy kliknąć prawym przyciskiem myszy na ***Komputery*** > ***Nowy*** >

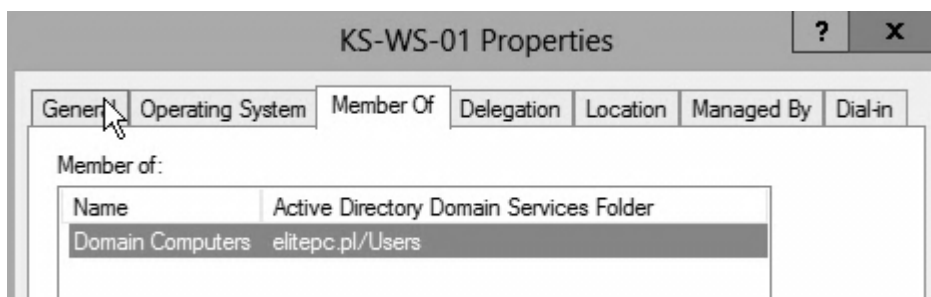
***Komputer (Komputery > New > Computer).***



A następnie stworzyć maszynę, która będzie się nazywać KS-WS-01

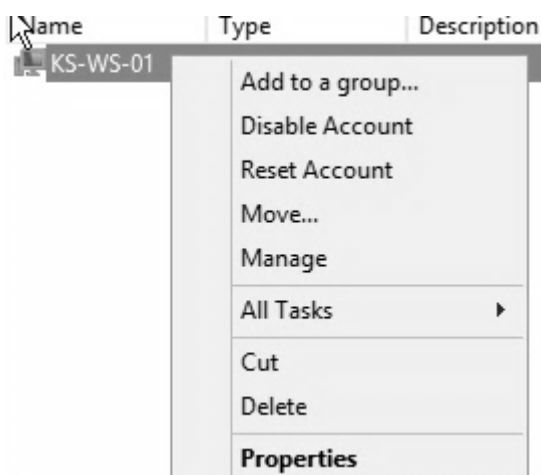


Komputer domyślnie zostanie przypisany do grupy ***Komputery Domeny (Domain Computers)***. Co można sprawdzić klikając w jego ***Właściwości (Properties)***.

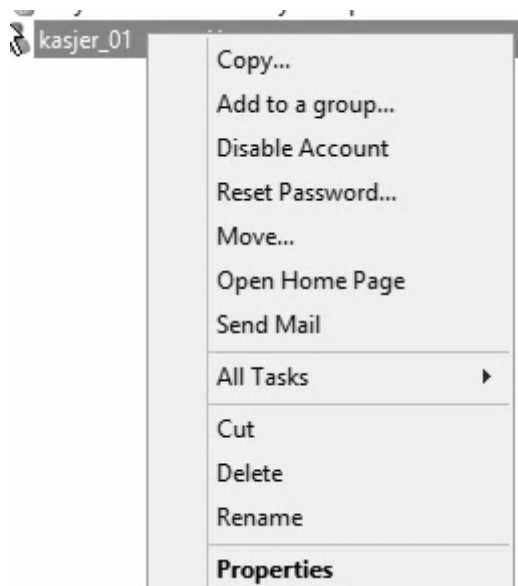


Trzeba pamiętać, że każdy komputer z systemem Windows NT, Windows 2000 lub

nowszym, który zostaje dołączony do domeny, otrzymuje własne konto komputera. Podobnie jak konta użytkowników, konta komputerów umożliwiają uwierzytelnianie oraz inspekcję dostępu komputera do sieci i zasobów domeny. Każde konto komputera musi być unikatowe. Uniemożliwi to niepowołanym osobom podłączenie się do sieci bez zgody administratora. Skoro zostali już stworzeni i pogrupowani użytkownicy oraz konta komputerów, warto jeszcze zwrócić uwagę na ich właściwości. Po kliknięciu prawym guzikiem myszy na koncie komputera są dwie ważne opcje. Jedną z nich jest **Wyłączenie Konta (Disable Account)**, a drugą **Zresetowanie Konta (Reset Account)**. Ta druga niezbędna jest wtedy, gdy maszyna o danej nazwie uległa awarii i została wymieniona na nową. Nowego komputera nie podłączy się do domeny do chwili zresetowania konta.



W przypadku konta użytkownika również można je wyłączyć, a także zresetować mu hasło opcją **Resetuj Hasło (Reset Password)**. Przydatna jest także możliwość **Wysłania Wiadomości (Send Mail)**.



Kont użytkownika z założenia nie powinno się kasować z kilku względów. Jednym z nich jest to, że na miejsce danego pracownika może przyjść jego następca – musiałoby wtedy albo zostać utworzone dla niego nowe konto, wprowadzane wszelkie ustawienia oraz uprawnienia. Prościej będzie użyć opcji **Kopiuj (Copy)**.

Create in: elitepc.pl/Ksiegowosc

First name:  Initials:

Last name:

Full name:

User logon name:

User logon name (pre-Windows 2000):

Będzie konieczne podanie nowej nazwy użytkownika oraz hasła, natomiast wszelkie inne ustawienia jak np. uprawnienia czy zamontowane dyski sieciowe pozostaną

zachowane. Z racji tego, że na ogół ustawień jest dość dużo praktykuje się właśnie stworzenie wzorcowego konta użytkownika w obrębie danej Grupy i kopiowanie zamiast tworzenia za każdym razem nowego konta. Użytkowników, którzy przestają być potrzebni najlepiej wyłączyć i przenieść do wcześniej przygotowanej jednostki organizacyjnej (np. czasowo wyłączeni). Można teraz wejść we właściwości jakiegoś konta użytkownika.

**Kasjer02 Properties** [?] [X]

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
<b>General</b>	Address	Account	Profile
	Telephones	Organization	

**Kasjer02**

First name:  Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

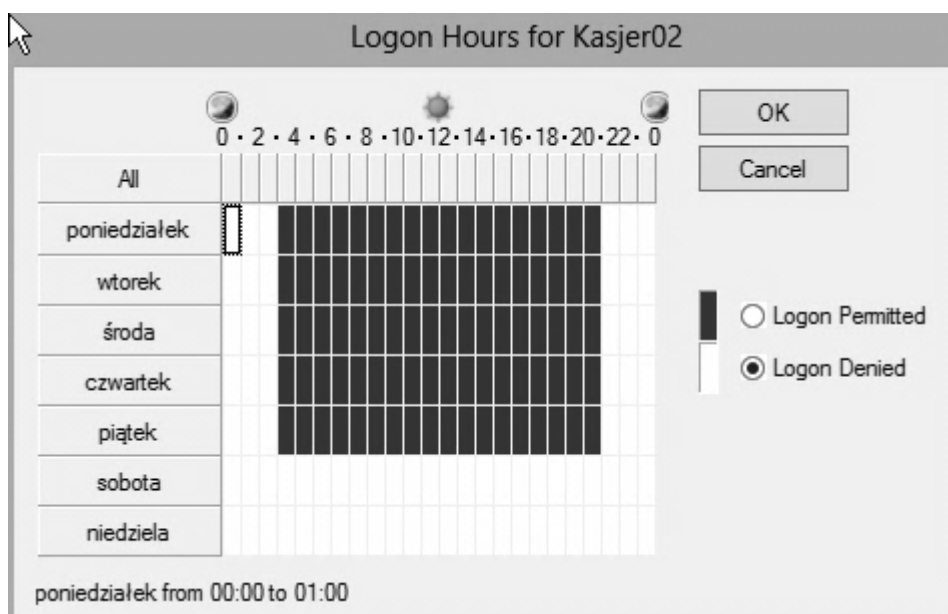
W zakładkach **Ogólne (General)**, **Adres (Address)**, **Telefony (Telephones)** oraz **Organizacja (Organization)** znajdują się jedynie pola, w które można wpisać jakieś informacje o użytkowniku.



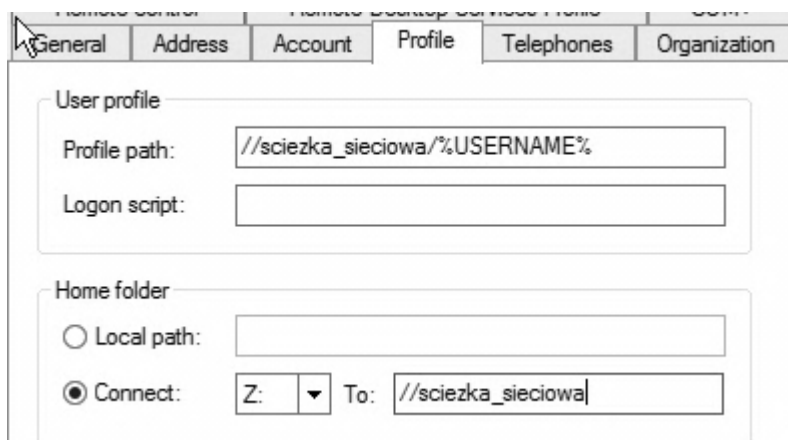
General	Address	Account	Profile	Telephones	Organization
User logon name: <input type="text" value="kasjer02"/> <input type="text" value="@elitepc.pl"/>					
User logon name (pre-Windows 2000): <input type="text" value="ELITEPC\"/> <input type="text" value="kasjer02"/>					
<input type="button" value="Logon Hours..."/>		<input type="button" value="Log On To..."/>			
<input type="checkbox"/> Unlock account					
Account options: <div> <input checked="" type="checkbox"/> User must change password at next logon  <input type="checkbox"/> User cannot change password  <input type="checkbox"/> Password never expires  <input type="checkbox"/> Store password using reversible encryption           </div>					
Account expires: <div> <input checked="" type="radio"/> Never  <input type="radio"/> End of: <input type="text" value="2 czerwca 2012"/> </div>					

W zakładce **Konto (Account)** warto zwrócić uwagę na to, iż można zmienić login użytkownika lub nadać inny dla różnych domen. Warto korzystać z funkcji **Wygasania ważności konta (Account Expires)**, która powoduje wyłączenie konta po upływie jakiejś daty (np. w dniu końca umowy o pracę). Dzięki temu administrator nie musi pamiętać o wyłączeniu konta zwolnionego pracownika.

Bezpieczeństwo sieci można dodatkowo zwiększyć za pomocą ustawień **Godzin Logowania (Logon Hours)**.

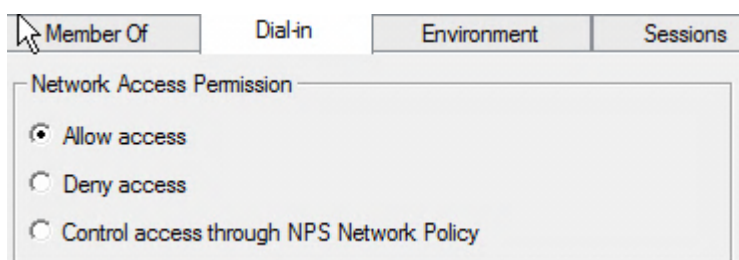


W łatwy sposób można określić to, w jakich godzinach konto może być używane, a w jakich nie. Dzięki temu potencjalny włamywacz, jeżeli nawet dostanie się na takie konto, to poza godzinami pracy, czyli wtedy, gdy nie ma nadzoru nad siecią, nie będzie w stanie niczego zrobić.

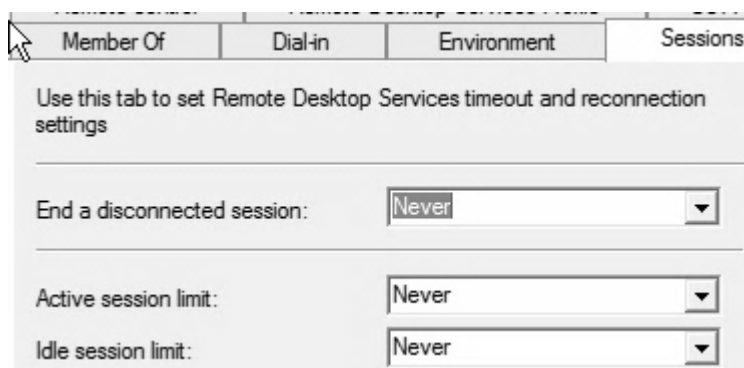


W zakładce **Profil (Profile)** można określić ścieżkę sieciową dla profilu, czyli lokalizację w sieci, gdzie dany profil ma być przechowywany. Parametr

**%USERNAME%** to zmienna środowiskowa, która zwraca nazwę użytkownika. Dzięki temu w podanej lokalizacji zostanie utworzony katalog o nazwie takiej samej jak nazwa użytkownika. Kopiując tak skonfigurowany profil pewne jest, że każdy nowy użytkownik dostanie swój własny prywatny folder w zasobie sieciowym. Istnieje także możliwość zamontowania dysku sieciowego. Niestety ograniczona do jednego dysku. Więcej można zamontować za pomocą Zasad Grupy.



W zakładce **Telefonowanie (Dial –in)** warto zwrócić uwagę na to, czy użytkownik ma zgodę na dostęp do sieci z zewnątrz. Jeżeli takiej nie ma to np. nie będzie mógł się podłączyć do wewnętrznej sieci za pomocą VPN’a itp. Na taki dostęp można mu pozwolić lub wybrać opcję trzecią, która mówi o tym, że **NPS** zajmie się jego weryfikacją (o czym już w dalszych działach).

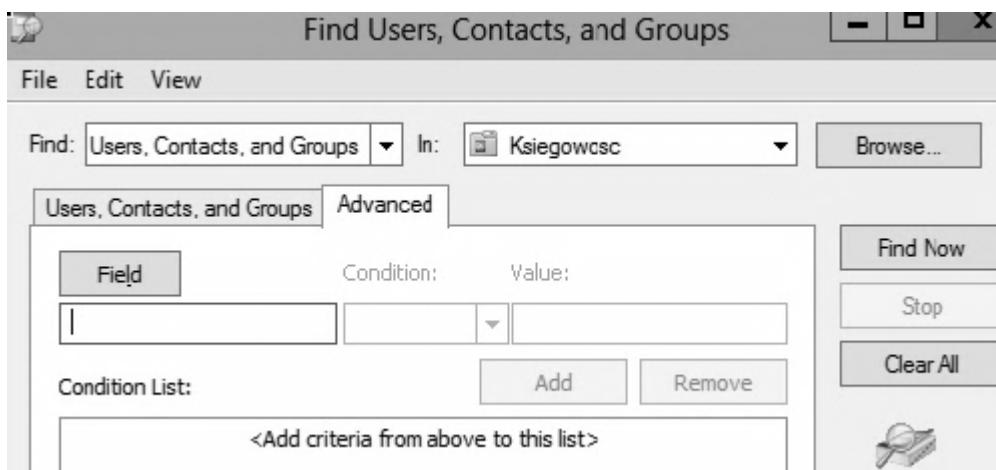


Ze względów licencyjnych i nie tylko w zakładce **Sesje (Sessions)** warto ustawić limity czasu trwania sesji tak, aby użytkownicy nieaktywni lub tacy, którzy zostawili

włączone komputery przed wyjściem do pracy byli automatycznie wylogowywani.



Za pomocą ikonki można dostać się do wyszukiwarki Active Directory, w której można tworzyć kwerendy, które przefiltrują dokładnie całą usługę katalogową i pomogą wyłuskać pożądane informacje.



Zamykając dział dotyczący Active Directory warto nadmienić, iż w obrębie jednostki organizacyjnej nie powinno znajdować się więcej niż 5000 użytkowników ze względów wydajnościowych.

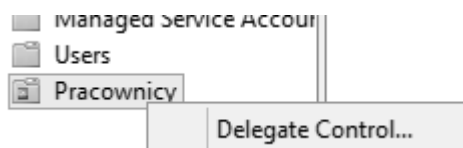
Active Directory Users and Com			
Saved Queries			
elitepc.pl			
Built-in			
Computers			
Domain Controllers			
ForeignSecurityPrincipal			
Managed Service Account			
Users			
Name	Type	Description	
Administrator	User	Built-in account	
Allowed RODC Password Replication Group	Security Group	Members in	
Cert Publishers	Security Group	Members of	
Cloneable Domain Controllers	Security Group	Members of	
Denied RODC Password Replication Group	Security Group	Members in	
DnsAdmins	Security Group	DNS Admins	
DnsUpdateProxy	Security Group	DNS clients	
Domain Admins	Security Group	Domain Admins	

Warto także pamiętać, że w jednostce organizacyjnej *Użytkownicy (Users)* znajduje

się bardzo newralgiczne konto Administrator.

Każdy użytkownik Windows posiada **Identyfikator Bezpieczeństwa (Security Identifier)**, który wygląda mniej więcej tak: S-1-5-21-3627861015-3361044348-30300820-1013. Konto Administrator posiada na samym końcu zawsze liczbę 500, czyli wygląda mniej więcej tak: S-1-5-21-3623811015-3361897348-30300820-500. Dzięki temu potencjalny włamywacz posiada wiedzę na temat tego, które konto to Administrator. Dlatego też jednym z pierwszych kroków w pracy z Active Directory powinno być powielenie konta administratora. Można to osiągnąć wyłącznie poprzez opcję **Kopiuj (Copy)**, a następnie wyłączenie pierwotnego konta z wcześniejszym nadaniem mu bardzo złożonego hasła.

Naturalnie administrator nie jest osobą odpowiedzialną za całe działanie serwera. Na ogół różne osoby zarządzają różnymi rolami a nawet częściami ról. Tak samo jest w przypadku Active Directory. W celu przeprowadzenia demonstracji należy stworzyć jednostkę organizacyjną Pracownicy oraz użytkownika Szef. Następnie na jednostce organizacyjnej pracownicy należy przycisnąć prawy guzik myszki i wybrać **Deleguj kontrolę (Delegate Control)**.



Ukaże się kreator, który pozwala na przedelęgowanie kontroli nad pojedynczą jednostką organizacyjną i jej zawartością wybranemu użytkownikowi. Użytkownik ten będzie mógł zarządzać innymi użytkownikami, nadawać im uprawnienia, tworzyć grupy, komputery, jednostki organizacyjne oraz inne obiekty Active Directory, lecz tylko wewnątrz jednostki organizacyjnej Pracownicy. Należy kliknąć **Dalej (Next)**.

## Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.


Kolejne okno kreatora służy do określenia tego, komu kontrola zostanie przedelegowana. Tych użytkowników lub ich grupy dodaje się przyciskiem **Dodaj (Add)**.

### Users or Groups

Select one or more users or groups to whom you want to delegate control.



Selected users and groups:

 Szef (szef@elitepc.pl)

Add...

Remove

Następnie należy określić jakie zadania dany użytkownik będzie mógł realizować. Do wyboru jest kilka predefiniowanych szablonów. Istnieje także możliwość stworzenia nieszablonowego zadania.

## Tasks to Delegate

You can select common tasks or customize your own.

☒ Delegate the following common tasks:

- ☒ Create, delete, and manage user accounts
- ☐ Reset user passwords and force password change at next logon
- ☐ Read all user information
- ☐ Create, delete and manage groups
- ☐ Modify the membership of a group
- ☐ Manage Group Policy links
- ☐ Generate Resultant Set of Policy (Planning)

☐ Create a custom task to delegate

Na karcie podsumowującej należy kliknąć **Zakończ (Finish)**.

## Completing the Delegation of Control Wizard

You have successfully completed the Delegation of Control wizard.

You chose to delegate control of objects in the following Active Directory folder:

elitepc.pl/Pracownicy

The groups, users, or computers to which you have given control are:

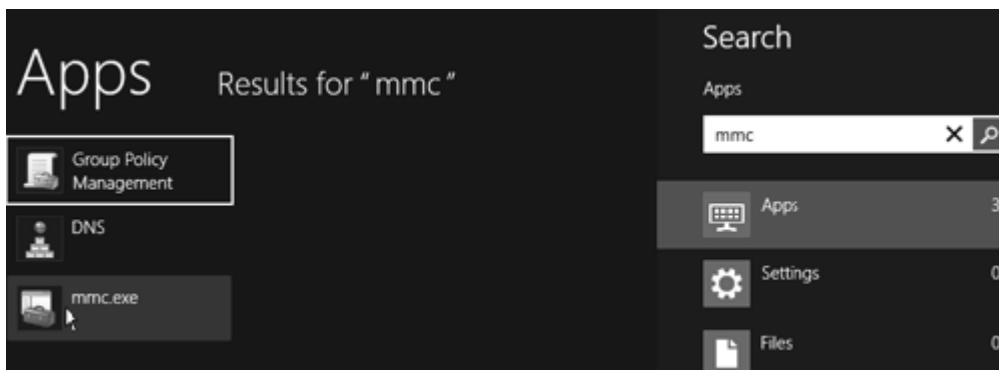
Szef (szef@elitepc.pl)

You chose to delegate the following tasks:

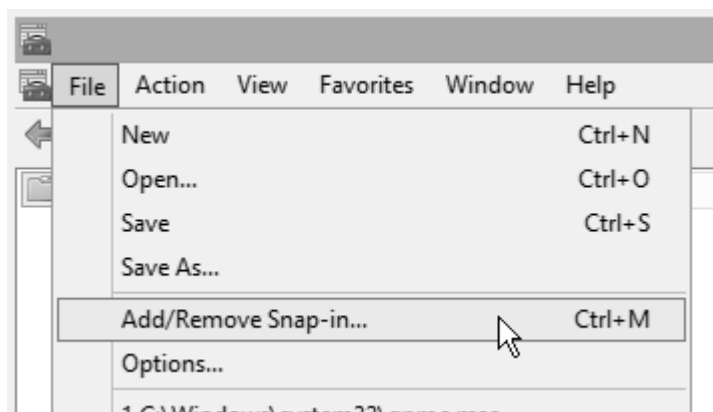
To close this wizard, click Finish.

Fizyczny dostęp do serwera jest niewskazany nawet dla administratora, a tym bardziej dla zwykłego użytkownika. Dlatego też należy dać użytkownikom możliwość zarządzania rolami, do których mają dostęp. Można to uczynić tworząc własną konsolę MMC. Aby ją stworzyć w menu Start należy wyszukać aplikacji

MMC i ją uruchomić.

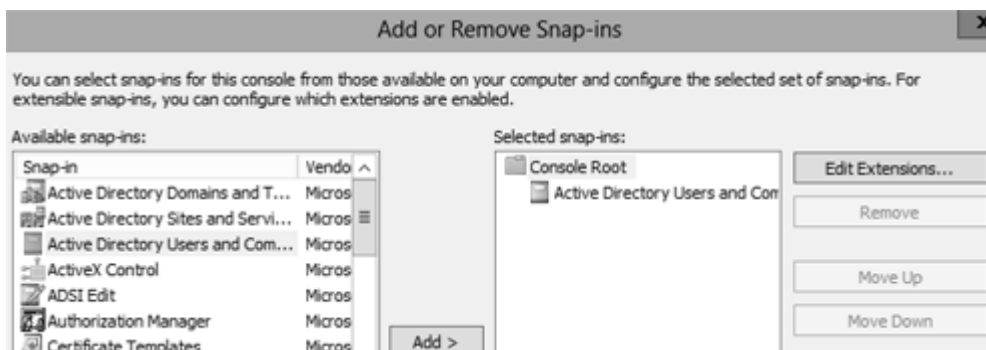


W programie, który się uruchomi należy wybrać **Plik (File)** i opcję **Dodaj/Usuń Przystawkę (Add or Remove Snap-ins)**.

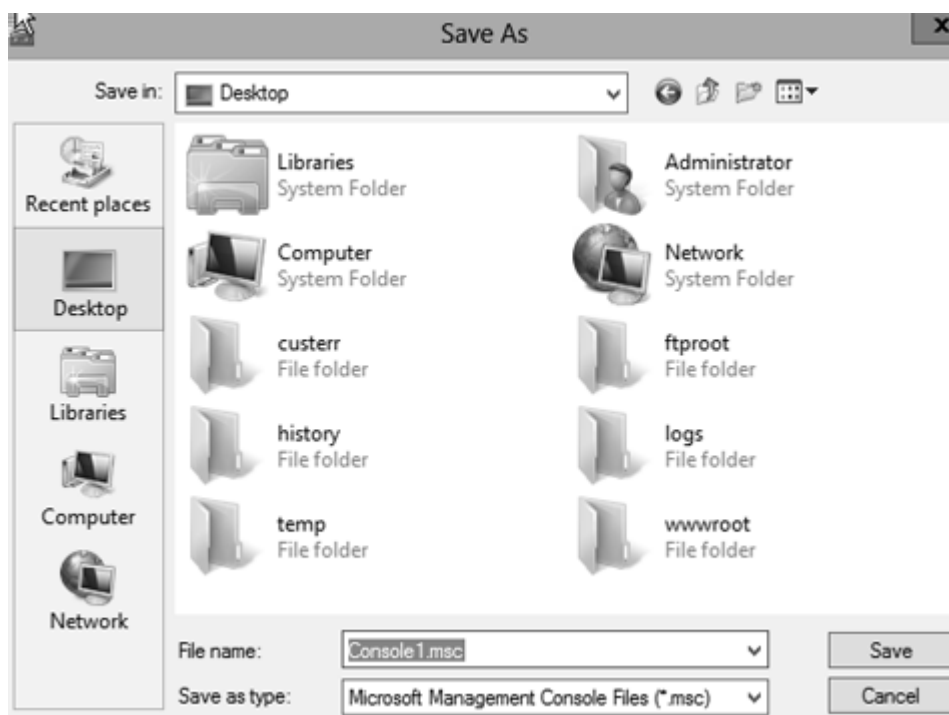


Pojawi się okno, w którym z listy po lewej stronie wybiera się które konsole mają być dołączone do obecnie tworzonej za pomocą guzika **Dodaj (Add)**.



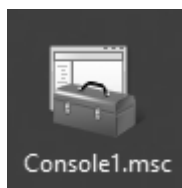


Tak przygotowaną konsolę należy zachować wybierając **Plik (File)**, a następnie **Zapisz (Save)**. Konsoli należy nadać przyjazną nazwę, tak aby odzwierciedlała to, co się w niej znajduje. Tym bardziej, że jej zawartość może składać się z kilku standardowych konsol np. może zawierać przystawki do zarządzania DNS, DHCP czy Active Directory itp.

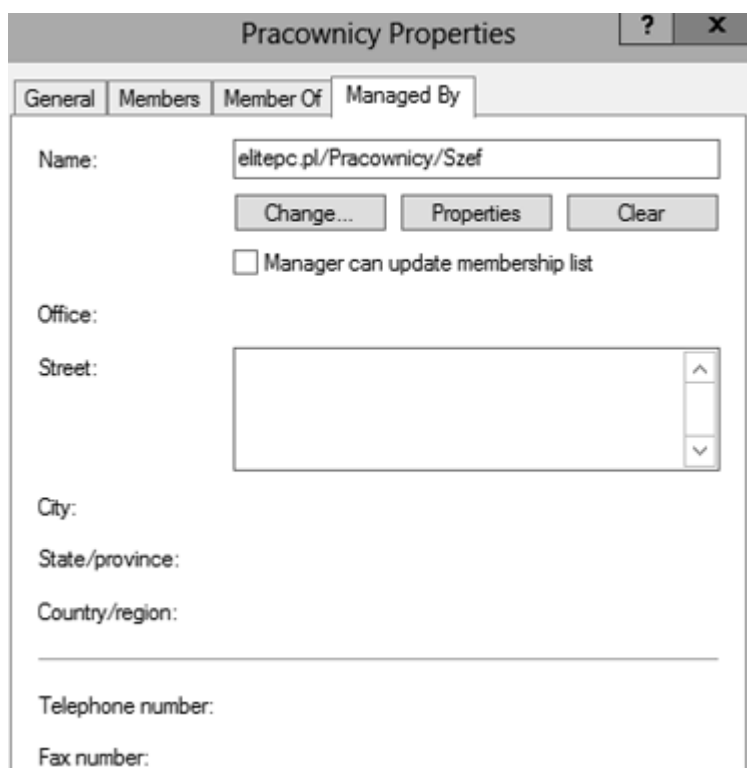


Tak przygotowany plik wystarczy przekazać użytkownikom docelowym. Musi on

zostać uruchomiony na komputerze wpiętym do sieci firmowej bezpośrednio bądź przez VPN. Uruchomienie następuje poprzez dwukrotne kliknięcie na konsoli, a sposób zarządzania nie odbiega od tego bezpośrednio z serwera.



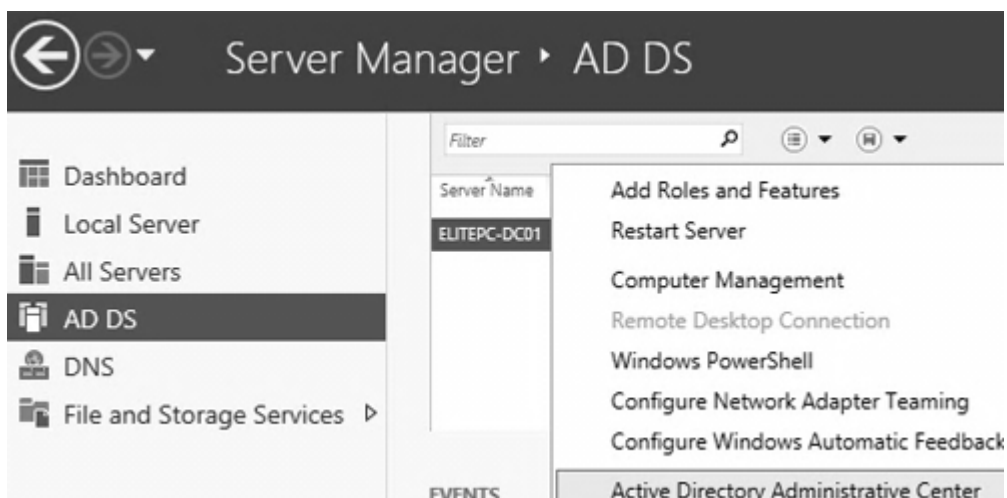
Inną opcją udzielenia komuś możliwości zarządzania np. nad pojedynczą grupą jest udzielenie władzy poprzez jej **Właściwości (Properties)** i wybranie zakładki **Zarządzany przez (Managed by)**. Karta ta pozwala na przypisanie jednego użytkownika do zarządzania jedną konkretną grupą.

The screenshot shows a Windows-style dialog box titled 'Pracownicy Properties'. It has four tabs: 'General', 'Members', 'Member Of', and 'Managed By', with 'Managed By' currently selected. The 'Name' field contains 'elitepc.pl/Pracownicy/Szef'. Below it are three buttons: 'Change...', 'Properties', and 'Clear'. There is an unchecked checkbox labeled 'Manager can update membership list'. The 'Office' section includes a 'Street' field with a list box below it, and 'City', 'State/province', and 'Country/region' fields. At the bottom are 'Telephone number' and 'Fax number' fields. The dialog box has standard Windows window controls (minimize, maximize, close) in the top right corner.

### 3.5. Active Directory Administrative Center

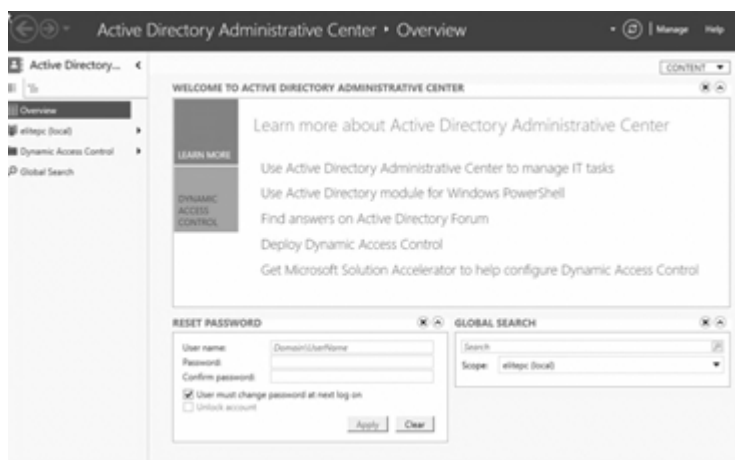
Chyba najlepszą i zarazem najbardziej popularną usługą katalogową jest Active Directory. Mimo, że jest ona wciąż na bieżąco rozwijana, to jednak należy pamiętać, że wywodzi się ona jeszcze z czasów Windows 2000. Nic więc dziwnego, że Microsoft stara się ciągle nie tylko dopracowywać starą, ale także tworzyć być może lepsze rozwiązania, które będą w stanie zastąpić swoich poprzedników. Jedną z takich nowości jest przystawka **Centrum Administracyjne Active Directory (Active Directory Administrative Center)**. Została ona wprowadzona w Windows Server 2008 R2, a w rozwiniętej wersji zaimplementowana również w Windows Server 2012.

Choć na pierwszy rzut oka wygląda ona do złudzenia podobna do tej z Windows Server 2008 to wprowadza kilka nowych możliwości. Podobnie jak inne konsolki znajduje się ona w narzędziach administracyjnych. Można się do niej dostać także poprzez Menadżera Serwera, analogiczne do Użytkowników i Komputerów usługi Active Directory.

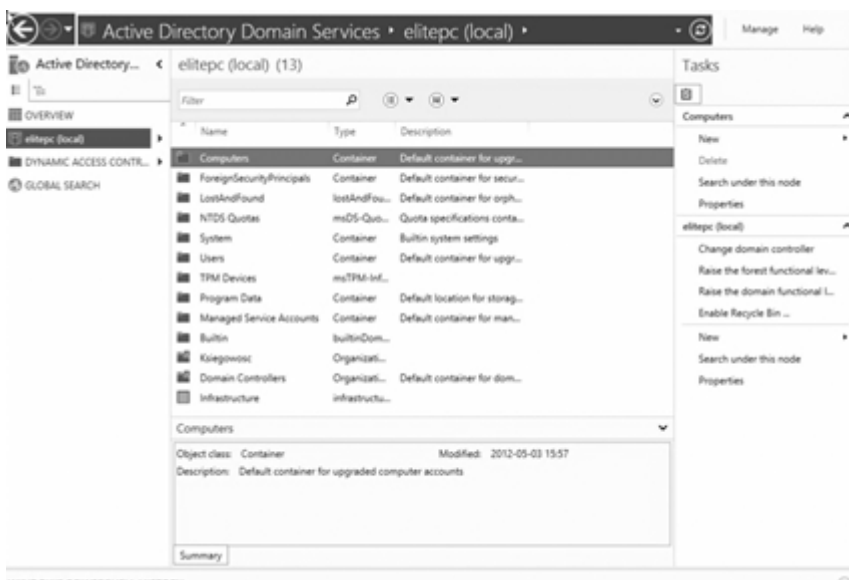


Celem jej wprowadzenia było uproszczenie, przyspieszenie i ułatwienie wykonywania najczęstszych czynności, jakie administrator napotyka na swojej

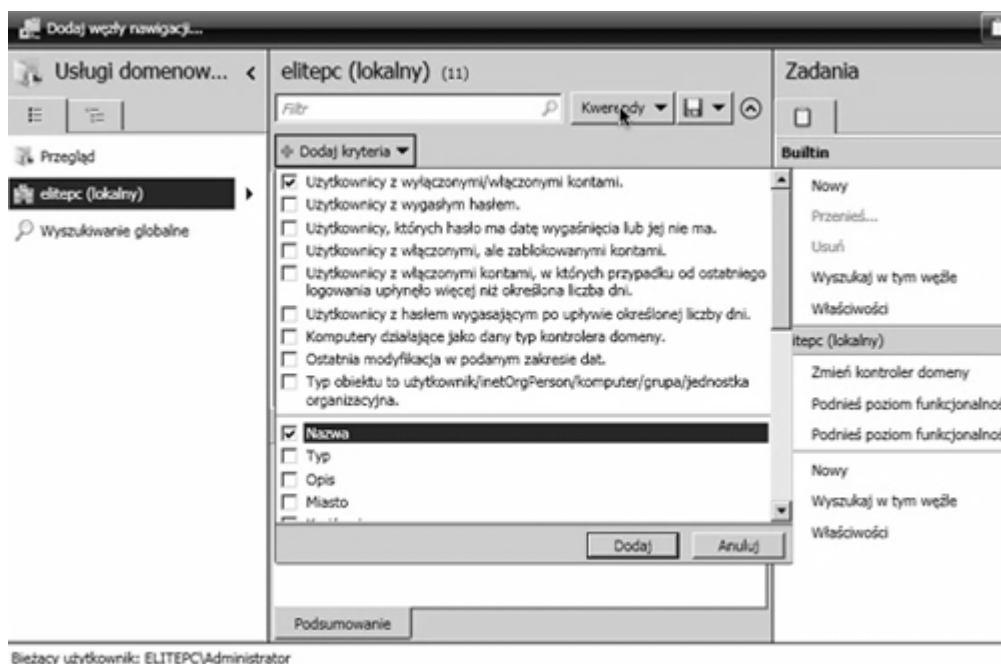
drodze. Zostaną więc tutaj stworzeni użytkownicy, grupy, kontenery, jednostki administracyjne itp. Można przy tym jednocześnie zarządzać więcej niż jedną domeną, używać filtrów wyszukiwania oraz powiązać jej pracę z PowerShell'em. Już pierwsza karta pozwala na zresetowanie hasła użytkownika czy przeszukanie domeny.



Po kliknięciu z lewej strony na pożądaną domenę w środkowej części ekranu pojawi się pasek z możliwością ręcznego pisania kwerend oraz zawartością domeny. Na pierwszy rzut oka wygląda podobnie do starej przystawki.

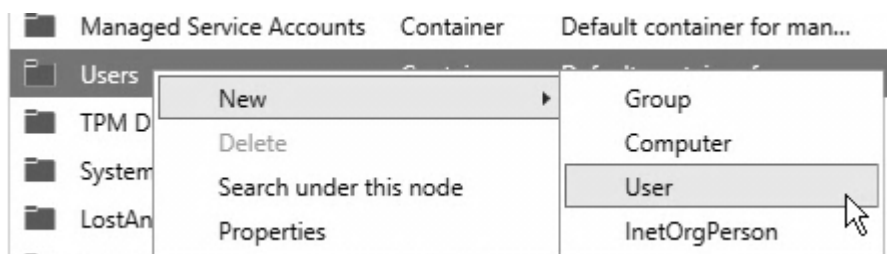


Klikając **Dodaj kryteria (Add Criteria)** można wybrać interesujące administratora właściwości obiektów, po których będą filtrowane wartości.



Ogólnie rzecz ujmując zarządzanie jest bardzo podobne do przystawki **Użytkownicy**

*i komputery usługi Active Directory*. Można np. kliknąć na danym kontenerze prawym guzikiem i dodać nowego użytkownika czy komputer.

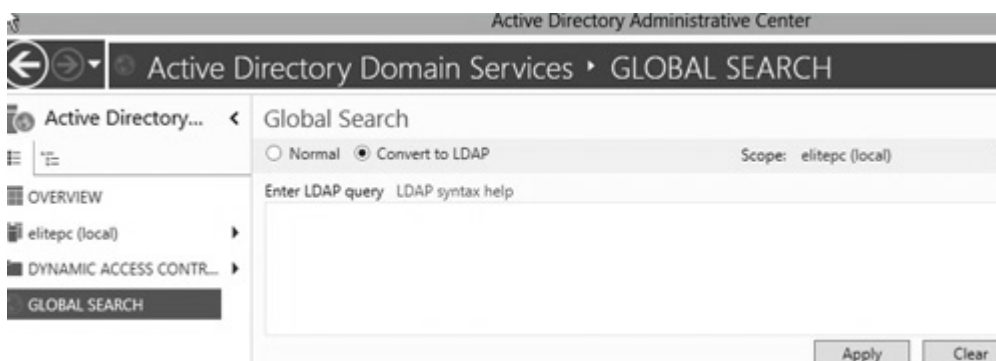


Zmianie uległy także kreatory. Teraz nie ma potrzeby przeglądania kilku zakładek jedna po drugiej, wszystkie właściwości zostały zebrane w formie formularza.

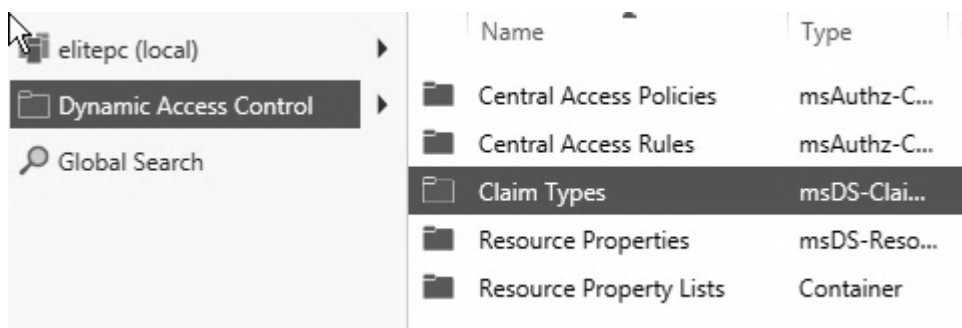
A screenshot of the 'Create User' wizard in Active Directory. The 'Account' tab is active, showing fields for user information, password settings, and organization details. The 'Organization' tab is also visible below the 'Account' tab. The 'Account' tab includes fields for First name, Middle initials, Last name, Full name, User UPN logon, User SamAccountName, Password, Confirm password, and Create in. It also has sections for Account expires, Password options, Encryption options, and Other options. The 'Organization' tab includes fields for Display name, Office, E-mail, Web page, Job title, Department, Company, Manager, and Direct reports. The 'More Information' section is expanded, showing a summary of the user being created: 'Bieżący użytkownik: ELITEPC\Administrator'. The 'OK' and 'Cancel' buttons are at the bottom right.

Na uwagę zasługuje także wyszukiwanie globalne, a właściwie ciekawa

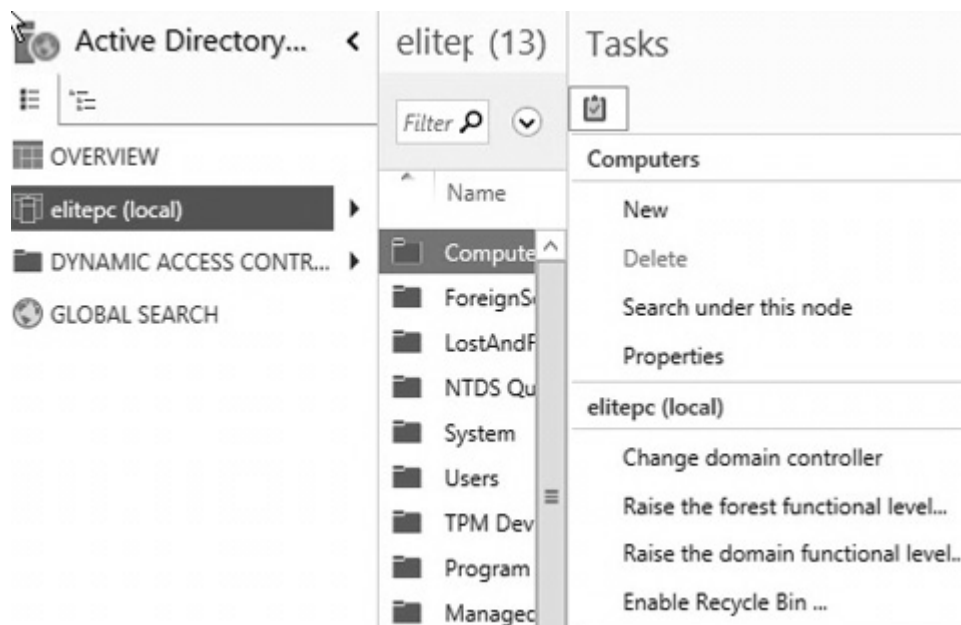
funkcjonalność, jaka się tam znalazła tj. możliwość skonwertowania zapytania na format LDAP.



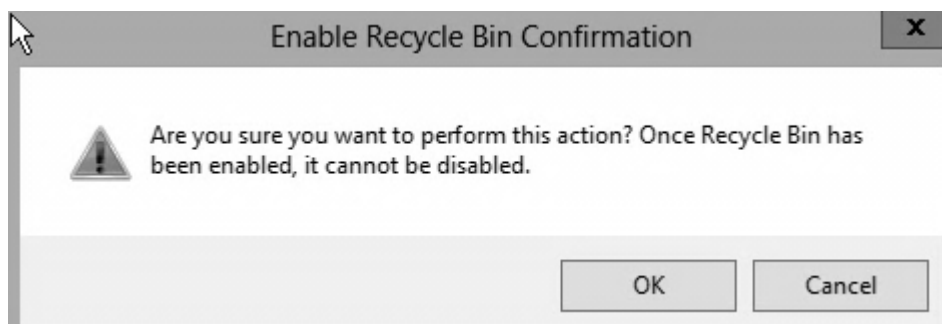
Wracając jednak do okna głównego nowej przystawki warto zauważyć, iż pojawił się kontener ***Dynamiczna Kontrola Dostępu (Dynamic Access Control)***, który powiązany jest z autoryzacją bazującą na mechanizmie Claim, o którym będzie więcej w dziale 8.3. Na tą chwilę wystarczy wiedza, iż ***Central Access Policies*** odpowiada za polisy autoryzacji w metodzie Claim, ***Central Access Rules*** posiada w sobie reguły autoryzacyjne niezbędne przy budowaniu polis dostępu, ***Claim Types*** zawiera uzgodnienia (Claim) pomiędzy obiektem a atrybutami obiektu, ***Resource Properties*** to miejsce na zdefiniowane ustawienia zasobów używane przy autoryzacji typu Claim, natomiast ***Resource Property List*** to nic innego jak listy własności zasobów używanych podczas autoryzacji Claim.



Warto teraz kliknąć na nazwie domeny i zerknąć na menu po prawej stronie.



Oprócz trzech opcji znanych z Windows Server 2008 R2, czyli *Zmiany kontrolera domeny* (*Change domain controller*) oraz *Zwiększania poziomu funkcjonalności domeny bądź lasu* (*Raise the forest functional level* oraz *Raise the domain functional level*), pojawił się także *Kosz dla usługi Active Directory* (*Enable Recycle Bin*). Po jego kliknięciu pojawi się komunikat o tym, że raz włączonego kosza nie można już wyłączyć. Należy go potwierdzić klikając **OK**.



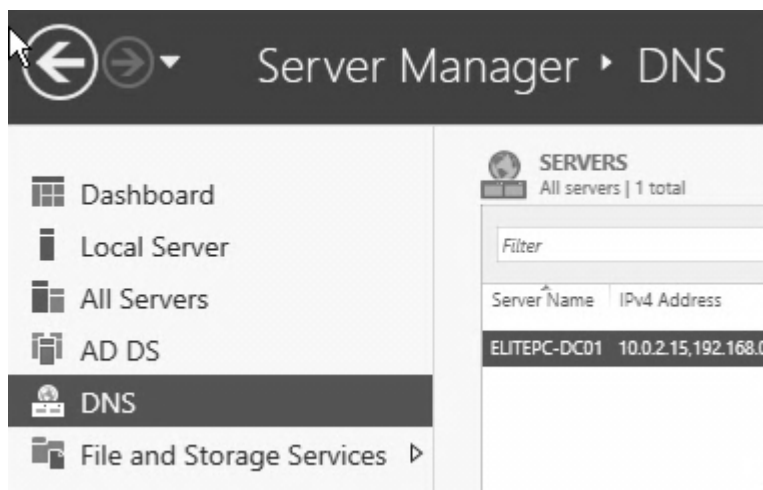


## 4. Serwer DNS


Działanie współczesnych sieci komputerowych byłoby niemożliwe bez użycia usługi DNS. To właśnie ona odpowiada za tłumaczenie nazw przyjaznych dla użytkowników na adresy IP. Dla przykładu odwołując się do ulubionej domeny internetowej to właśnie serwer DNS mówi komputerowi z jakim adresem IP ten ma się połączyć. Tłumaczenie oczywiście działa w obydwie strony. Czytelnik w tym rozdziale dowie się w jaki sposób Windows Server 2012 realizuje usługę DNS oraz jak nią zarządzać.

### 4.1. Zapoznanie z konsolą DNS Manager

Wraz z Active Directory automatycznie zainstalował się serwer DNS. Stało się tak, ponieważ Active Directory do prawidłowego działania wymaga serwera nazw. Gdyby w sieci przed instalacją AD DS istniał już inny serwer DNS najprawdopodobniej zostałby on użyty w zależności od kroków jakie zostałyby wybrane podczas instalacji AD DS. Ad współpracuje tylko z serwerami hostowanymi w Windows Server.



**DNS (Domain Name System)**, czyli system nazw domenowych to usługa zapewniająca zamianę adresów znanych użytkownikom na adresy, które staną się

zrozumiałe dla urządzeń wchodzących w skład sieci komputerowej. Na przykład zamiast odwoływać się do komputera w domenie poprzez podanie adresu IP 192.168.1.xxx będzie można napisać np. komputer01.Elitepc.pl. Na podobnej zasadzie działa cała globalna sieć. Aby sprawdzić, jaki adres IP kryje się pod daną nazwą wystarczy wejść w konsolę PowerShell .

W konsoli, która się pojawi wystarczy, że zostanie podana komenda ***ping adres strony www***. W przykładzie poniżej można się dowiedzieć, że wortal komputerowy in4.pl posiada adres IP 195.242.117.52. Zamiast wpisywać w przeglądarce adres strony www, jako in4.pl można podać powyższy ciąg cyfr. Efekt będzie taki sam.

```
PS C:\Users\Administrator> ping in4.pl

Pinging in4.pl [93.157.96.17] with 32 bytes of data:
Reply from 93.157.96.17: bytes=32 time=33ms TTL=56
Reply from 93.157.96.17: bytes=32 time=37ms TTL=56
Reply from 93.157.96.17: bytes=32 time=33ms TTL=56
Reply from 93.157.96.17: bytes=32 time=38ms TTL=56

Ping statistics for 93.157.96.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 38ms, Average = 35ms
```

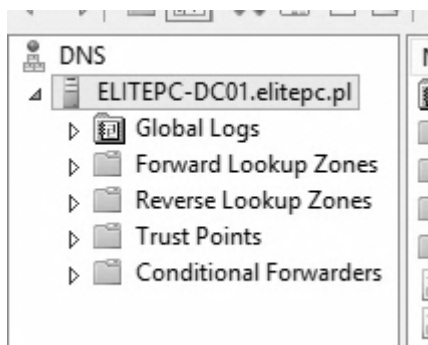
Ważną rzeczą, o której należy wspomnieć jest to, iż komputery obce, niebędące częścią domeny nie będą mogły się odwoływać do komputerów wewnątrz sieci adresem komputer01.Elitepc.pl. Natomiast komputery wewnątrz domeny nie tylko będą to potrafiły, ale jeszcze będą mogły korzystać z serwera DNS do tłumaczenia adresów internetowych. Jest to o tyle ważne, że przy dużych sieciach znacznie minimalizuje to obciążenie łącza internetowego. Przechodząc do konsoli zarządzania usługą, po znalezieniu na liście serwera należy kliknąć na nim prawym przyciskiem myszy, a następnie wybrać ***Menadżer Serwera DNS (DNS Manager)***.

Server Name	IPv4 Address	Manageability	Last Update
ELITEPC-DC01	10.0.2.15, 192.168.0.1	<ul style="list-style-type: none"> <li>Add Roles and Features</li> <li>Restart Server</li> <li>Computer Management</li> <li>Remote Desktop Connection</li> <li>Windows PowerShell</li> <li>Configure NIC Teaming</li> <li>Configure Windows Automatic Feedback</li> <li>DNS Manager</li> </ul>	

Usługa DNS podzielona jest na dwie strefy:

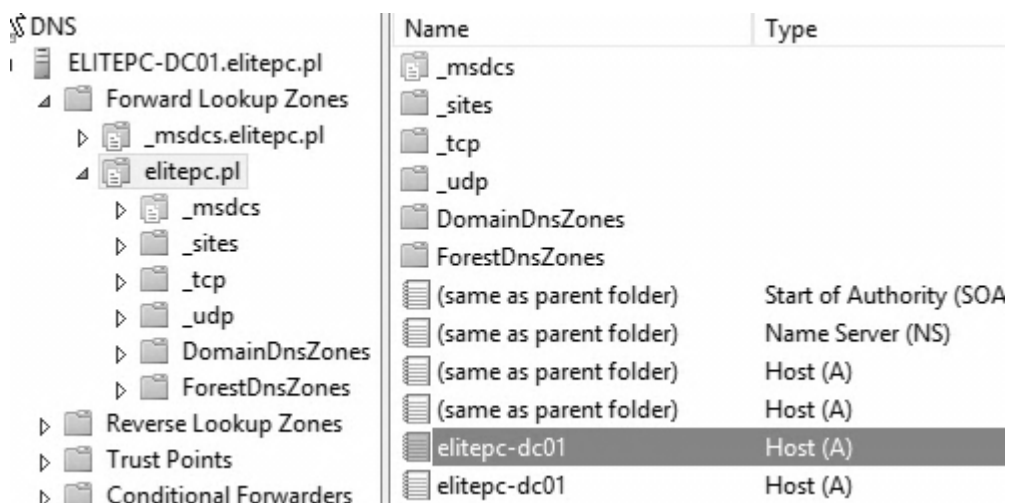
- wyszukiwania do przodu
- wyszukiwania wstecznego

Strefa wyszukiwania do przodu jest mniej więcej tym, co wcześniej zostało opisane i jest już ona skonfigurowana. Natomiast strefa wyszukiwania wstecznego działa jak sama nazwa wskazuje w stronę przeciwną, czyli posługując się przykładem zamieni adres IP 195.242.117.52 na in4.pl. DNS działa tylko wewnątrz sieci.



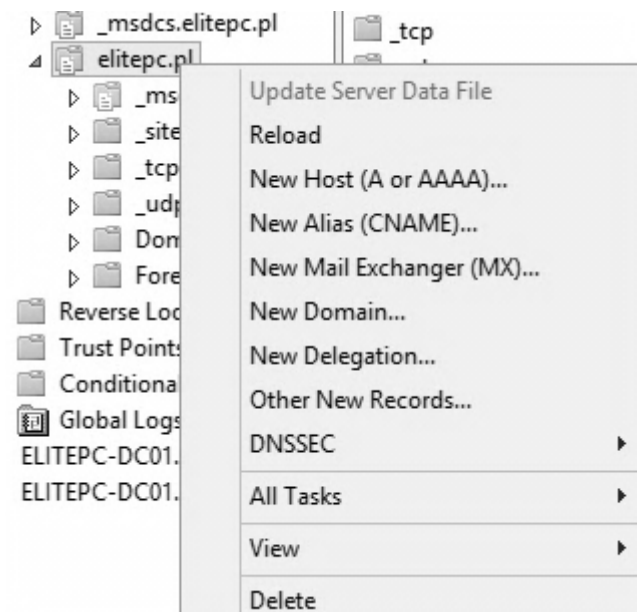
Należy rozwinąć strefę przewijania do przodu, a następnie zaznaczyć domenę, na serwerze przykładowym będzie to ElitePC.pl. Warto zwrócić uwagę, że po prawej stronie znajdują się różnego rodzaju wpisy, np. zaznaczony wpis typu *A (Host(A))* dla kontrolera domeny definiuje nam to, że nazwa ElitePC-DC01 w sieci lokalnej

będzie jednoznaczna z adresem IP 192.168.1.1

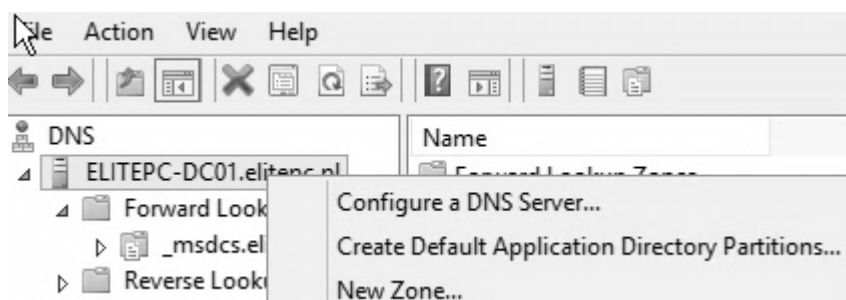


## 4.2. Ręczna konfiguracja strefy DNS

Na potrzeby treningowe zostanie skasowana główna strefa wyszukiwania do przodu, żeby pokazać jak ją ręcznie utworzyć. Należy kliknąć na niej prawym przyciskiem myszy i wybrać opcję *Usuń (Delete)*.



Następnie konieczne jest kliknięcie na nazwie serwera i wybranie opcji **Nowa Strefa (New Zone)**.



Otworzy się kreator, gdzie stronę powitalną należy pominąć klikając **Dalej (Next)**.



Kolejna plansza pozwoli wybrać rodzaj strefy. W tym przypadku zostanie wybrana **Strefa Podstawowa (Primary Zone)**, ponieważ serwer jest główną maszyną w sieci. Gdyby miał zostać zainstalowany dodatkowy serwer np. zapasowy lub do

zbilansowania obciążenia sieciowego, zostałaby wybrana *Strefa Pomocnicza (Secondary Zone)*. W lokalizacjach niezabezpieczonych najlepsza będzie *Strefa Skrótowa (Stub Zone)*. Jako, że serwer jednocześnie pełni rolę kontrolera domeny można wybrać opcję *Przechowywania strefy w usłudze Active Directory (Store the zone in Active Directory)* Należy kliknąć przycisk *Dalej (Next)*.



Kolejna karta określa sposób replikacji danych DNS. Można przekazywać rekordy *w całym lesie (To all DNS servers running on domain controllers in this forest)*, jedynie *w obrębie domeny (To all DNS servers running on domain controllers in this domain)* (co zostanie wybrane), bądź do *wszelkich kontrolerów domeny (To all domain controllers in this domain (for Windows 2000 compatibility))* (wymagane w przypadku starszych serwerów). Należy kliknąć *Dalej (Next)*.

### Active Directory Zone Replication Scope

You can select how you want DNS data replicated throughout your network.



Select how you want zone data replicated:

- ☐ To all DNS servers running on domain controllers in this forest: elitepc.pl
- ☒ To all DNS servers running on domain controllers in this domain: elitepc.pl
- ☐ To all domain controllers in this domain (for Windows 2000 compatibility): elitepc.pl
- ☐ To all domain controllers specified in the scope of this directory partition:

Następnie należy wybrać czy tworzona jest strefa wyszukiwania do przodu czy wstecznego. Zostanie wybrana opcja pierwsza.

Select the type of lookup zone you want to create:

- ☒ Forward lookup zone  
A forward lookup zone translates DNS names into IP addresses and provides information about available network services.
- ☐ Reverse lookup zone  
A reverse lookup zone translates IP addresses into DNS names.

Ponieważ jest to główny serwer naturalną nazwą strefy będzie elitepc.pl.

### Zone Name

What is the name of the new zone?



The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.


Zone name:

Na kolejnej planszy zostaną pozostawione opcje domyślne. Należy kliknąć przycisk

**Dalej (Next).** Ustawienia te zostaną zmienione za chwilę.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- ☒ Allow only secure dynamic updates (recommended for Active Directory)  
This option is available only for Active Directory-integrated zones.
- ☐ Allow both nonsecure and secure dynamic updates  
Dynamic updates of resource records are accepted from any client.  
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- ☐ Do not allow dynamic updates  
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

Na ostatniej planszy należy kliknąć **Zakończ (Finish)**.

### Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name:	elitepc.pl
Type:	Active Directory-Integrated Primary
Lookup type:	Forward

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

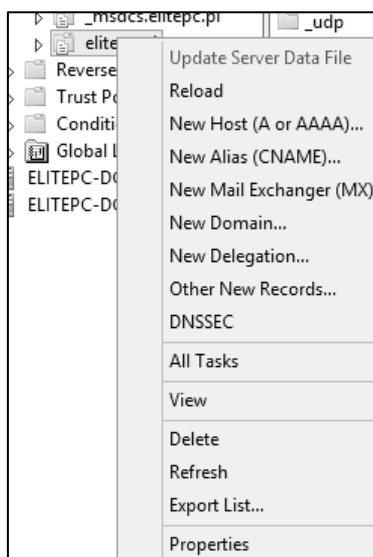
To close this wizard and create the new zone, click Finish.

< Back      Finish      Cancel

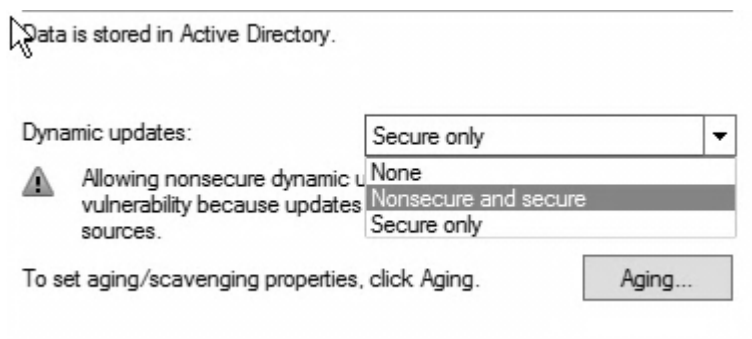


### 4.3. Zarządzanie serwerem DNS

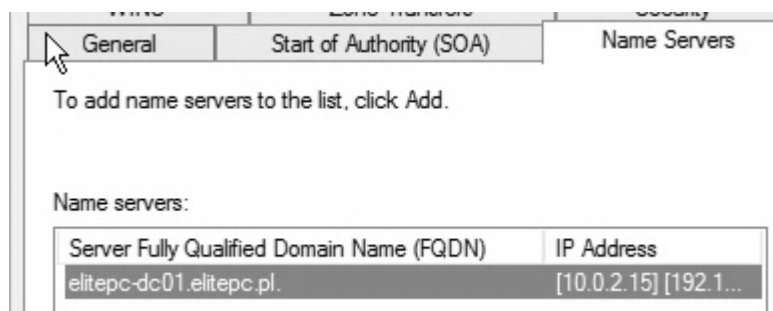
Usługa DHCP ma być ustawiona tak, aby aktualizowała przy okazji przyznania adresu rekordy DNS. Doda ona rekord A oraz PTR dla komputerów korzystających z sieci. Pojawią się one na liście pod serwerem. Gdyby jednak korzystano ze starszej wersji systemu Windows lub istniały jakieś inne problemy można kliknąć na nazwie domeny np. ElitePC.pl i wybrać **Właściwości (Properties)**.



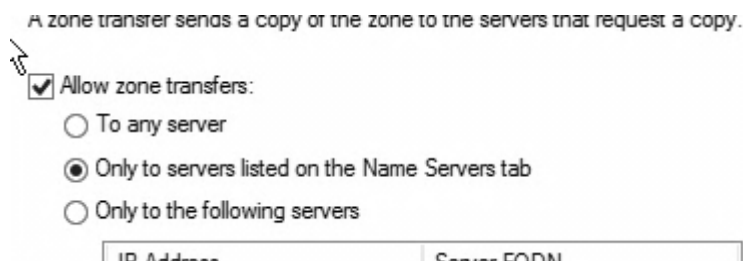
Niekiedy, choć nie jest to zalecane, konieczna będzie zmiana aktualizacji dynamicznych na **Niezabezpieczone i zabezpieczone (Nonsecure and secure)**.



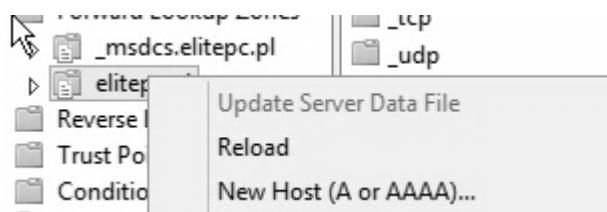
W zakładce *Serwery Nazw (Name Servers)* można dodać inne działające w sieci serwery DNS.



Dzięki temu można następnie w zakładce *Transfer Strefy (Zone transfer)* określić ustawienia tak, aby wszelkie zmiany w tym serwerze DNS były *propagowane do innych serwerów z poprzedniej karty Serwery Nazw (Only to servers listed on the Name Servers tab)*. Inną możliwością jest *Transfer strefy do dowolnego serwera w sieci (To any server)* lub *Dodanie serwerów poprzez podanie ich adresów IP (Only to the following servers)*. Ze względów bezpieczeństwa, jeżeli istnieje tylko taką możliwość zaleca się dzielenie rekordami DNS wyłącznie z członkami domeny.



Oczywiście można dodawać także nowe rekordy ręcznie. Do najbardziej popularnych należą rekordy A, AAAA, CNAME, MX i NS. Host A, czyli rekord adresu pozwala przypisać ręcznie dowolną nazwę pod dany adres IP jakiegoś urządzenia sieciowego.



Wystarczy podać nazwę hosta, a FQDN zostanie sam wygenerowany oraz adres IP, na który ma on wskazywać. Stworzenie rekordu PTR tworzy wpis odwrotny dla Hosta A, czyli wpis w strefie wyszukiwania wstecznego. Należy pamiętać o tym, że strefa wyszukiwania wstecznego musi być utworzona aby PTR powstał.

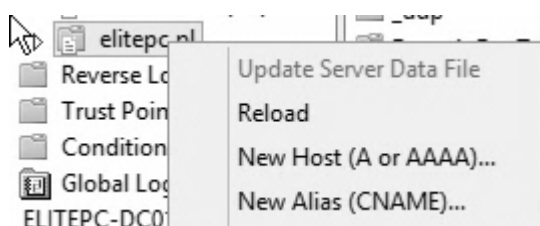
Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

☒ Create associated pointer (PTR) record

Host AAAA, czyli rekord adresu Ipv6 pozwala przypisać ręcznie dowolną nazwę pod dany adres IPv6 jakiegoś urządzenia sieciowego. CNAME tworzy alias dla istniejącego już wpisu, czyli wiele nazw może wskazywać na ten sam adres IP. Zaleca się tworzyć rekordy CNAME zamiast duplikować rekordy A, choćby z powodów ilości pamięci w bazie danych. Rekord MX jest używany do mapowania serwerów poczty, a NS serwerów DNS. Przechodząc przez kreator pojawi się rekord PTR zwany rekordem wskaźnika, który pozwala na implementację strefy wyszukiwania wstecznego. Dla przykładu zostanie utworzony rekord CNAME dla kontrolera domeny, który się przyda w kolejnych działach. W tym celu należy kliknąć prawym przyciskiem myszy na nazwie domeny i wybrać *Nowy Alias (CNAME) (New Alias (CNAME))*.



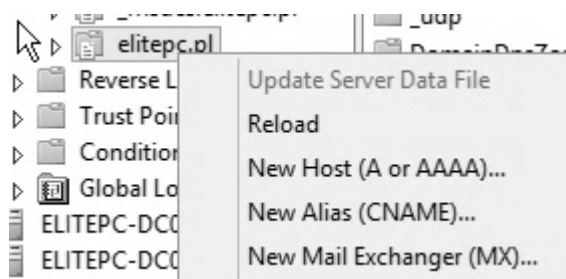
Nazwa aliasu jest dowolna, dla przykładu zostanie wpisane FTP. Należy także podać w pełni kwalifikowaną nazwę domeny dla hosta docelowego. Innymi słowy po prostu wskazać rekord A komputera, do którego alias ma się odwoływać. Sposób składania takiego adresu wydaje się być dość logicznym, jednak w przypadku problemów można użyć przycisku **Przeglądaj (Browse)** i wybrać odpowiedni komputer z listy.

A screenshot of a configuration dialog box titled 'Alias (CNAME)'. It contains three text input fields and a button. The first field is labeled 'Alias name (uses parent domain if left blank):' and contains the text 'ftp'. The second field is labeled 'Fully qualified domain name (FQDN):' and contains the text 'ftp.elitepc.pl.'. The third field is labeled 'Fully qualified domain name (FQDN) for target host:' and contains the text 'elitepc-dc01.elitepc.pl'. To the right of the third field is a button labeled 'Browse...'. The dialog box has a light gray background and a white border.

Zostaną także utworzone aliasy dla skrótów WWW oraz VPN. Pozwolą one użytkownikom łączyć się z serwerem podając adres `www.Elitepc.pl`, `vpn.Elitepc.pl`, `ftp.Elitepc.pl`, `elitepc.pl`. Dzięki temu nie tylko będzie to wyglądać bardziej profesjonalnie przy podawaniu różnego rodzaju danych do konfiguracji, ale także poprawi intuicyjność rozwiązania, mimo, że tak naprawdę połączenie następuje cały czas z jednym i tym samym komputerem. Co więcej gdyby każda rola serwera, tak jak ma to miejsce w profesjonalnych zastosowaniach, była zrealizowana na osobnych komputerach koniecznością byłoby utworzenie takich rekordów.

(same as parent folder)	Name Server (NS)	elitepc-dc01.elitepc.pl.
(same as parent folder)	Host (A)	192.168.0.1
(same as parent folder)	Host (A)	10.0.2.15
elitepc-dc01	Host (A)	192.168.0.1
elitepc-dc01	Host (A)	10.0.2.15
www	Host (A)	192.168.0.7
ftp	Alias (CNAME)	elitepc-dc01.elitepc.pl
vpn	Alias (CNAME)	elitepc-dc01.elitepc.pl

Rekordy MX – wymiany poczty przeznaczone są dla serwerów pocztowych np. z Microsoft Exchange.



Ich konfiguracja analogiczna jest do aliasów z tym, że posiadają one jeszcze pole na określenie priorytetu serwera pocztowego. Zaleca się priorytety zwiększać co 10 jeśli oczywiście jest taka możliwość w przedziale 1 do 100. Serwer o największym priorytecie będzie używany przez użytkowników sieci tak długo aż nie zostanie on przeciążony bądź nie ulegnie awarii.

Mail Exchanger (MX) Security

Host or child domain:  
mail

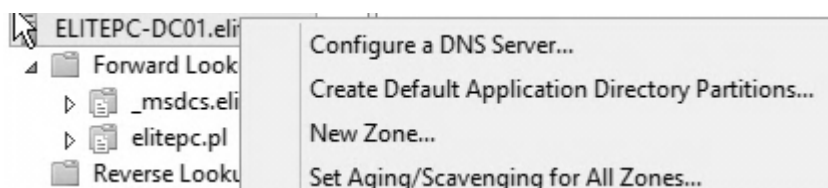
By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.

Fully qualified domain name (FQDN):  
mail.elitepc.pl

Fully qualified domain name (FQDN) of mail server:  
elitepc-dc01.elitepc.pl Browse...

Mail server priority:  
100

Serwer posiada także opcje oczyszczania samego siebie z nieaktualnych rekordów. Wystarczy na serwerze kliknąć prawym klawiszem myszy i wybrać opcję związaną z oczyszczaniem (*Set Aging/Scavenging for All Zones...*).



W oknie, które się pojawi należy wybrać jak długo nieodświeżony rekord może pozostać w serwerze DNS oraz co ile czasu serwer ma weryfikować swoje rekordy.

☐ Scavenge stale resource records

**No-refresh interval**

The time between the most recent refresh of a record timestamp and the moment when the timestamp may be refreshed again.

No-refresh interval:   ▼

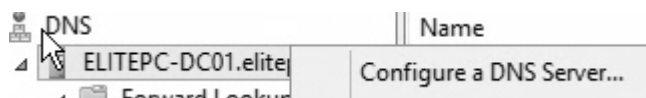
**Refresh interval**

The time between the earliest moment when a record timestamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period.

Refresh interval:   ▼

#### 4.4. Zapasowy serwer DNS

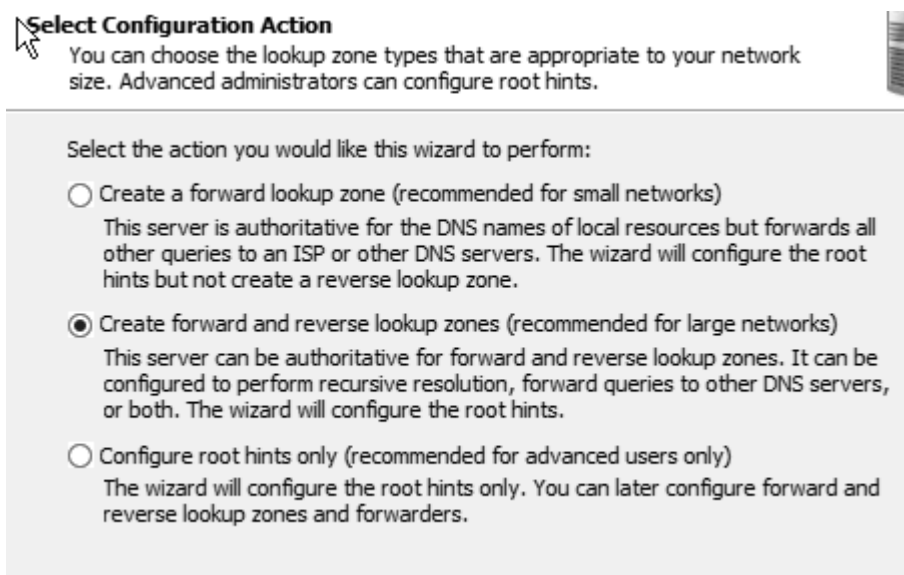
Naturalnie server DNS można zainstalować niezależnie od Active Directory np. na osobnym serwerze, do czego się zachęca, jeśli są ku temu odpowiednie środki. Najbezpieczniej i najwydajniej sieć będzie pracowała, **jeżeli na pojedynczym serwerze będzie jak naj mniej zainstalowanych ról**. Należy kliknąć na nazwie serwera prawym przyciskiem myszy i wybrać opcję *Skonfiguruj serwer DNS (Configure a DNS Server)*.



Kartę powitalną można pominąć klikając przycisk *Dalej (Next)*.



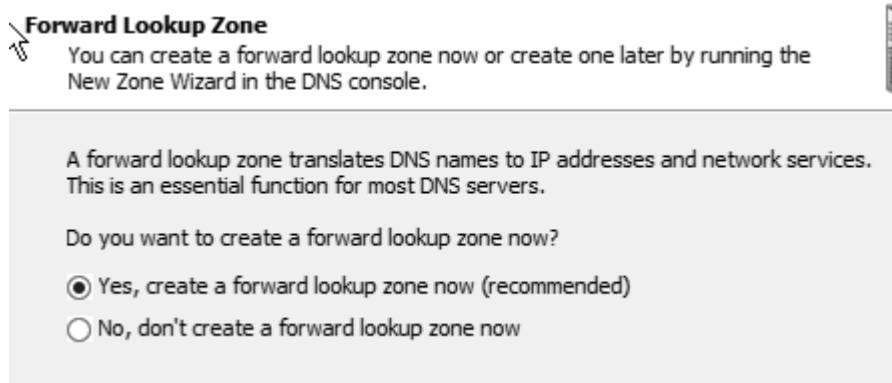
Do wyboru są trzy możliwości, z czego większość pewnie najbardziej zainteresują dwie pierwsze. Jedną z nich jest po prostu **stworzenie strefy wyszukiwania do przodu (Create a forward lookup zone)**, która świetnie sprawdza się w małych i średnich firmach. Lokalne zapytania będą rozwiązywane przez niego, natomiast te spoza sieci będą przekazywane do serwerów dostawcy Internetu. Dla dużych firm zaleca się **stworzyć strefę wyszukiwania do przodu oraz do tyłu (Create forward and reverse lookup zones)**. Serwer ten jest w pełni autorytatywny. Aby prześledzić dokładnie kreator konfiguracyjny należy wybrać opcję drugą.



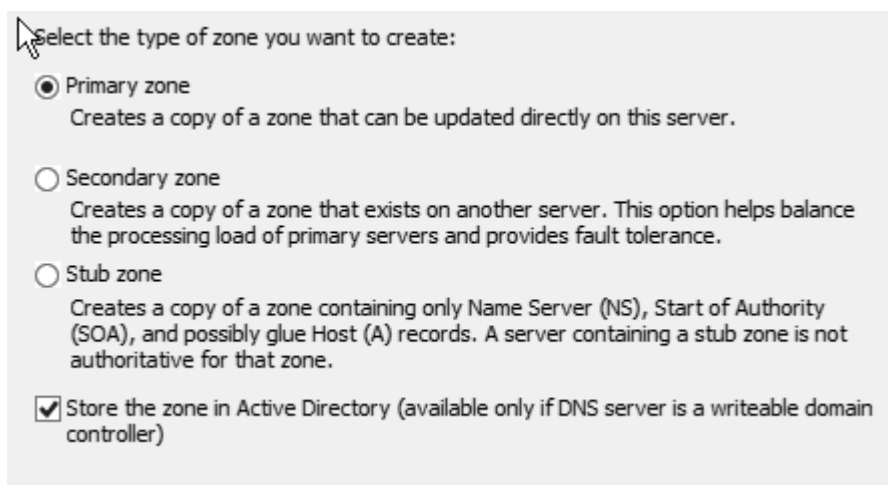
Na kolejnej karcie należy wybrać opcję zalecaną (**Yes, create a forward lookup zone**)



*now*), ponieważ ma zostać skonfigurowana strefa wyszukiwania do przodu.



Jako, że jest to pierwszy serwer stworzona zostanie **Strefę główną (Primary Zone)**. Gdyby był to serwer zapasowy zostałaby wybrana opcja druga. Zaznaczona także zostanie opcja **Przechowania strefy DNS w Active Directory (Store the zone in Active Directory)**.



Następnie należy określić metodę replikowania danych. Rekordy można propagować do wszystkich serwerów w lesie, tylko w domenie lub w partycji domenowej.

Select how you want zone data replicated:

☒ To all DNS servers running on domain controllers in this forest: elitepc.pl

☐ To all DNS servers running on domain controllers in this domain: elitepc.pl

☐ To all domain controllers in this domain (for Windows 2000 compatibility): elitepc.pl

☐ To all domain controllers specified in the scope of this directory partition:

▼

W kolejnym kroku należy podać nazwę strefy,.

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.


Zone name:

Należy określić opcje związane z aktualizacjami dynamicznymi, o których mowa była już wcześniej.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

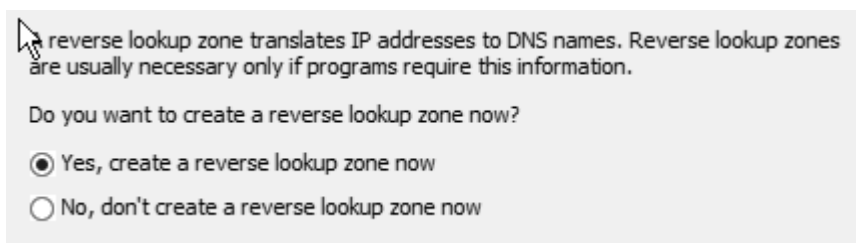
☒ Allow only secure dynamic updates (recommended for Active Directory)  
This option is available only for Active Directory-integrated zones.

☐ Allow both nonsecure and secure dynamic updates  
Dynamic updates of resource records are accepted from any client.  
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☐ Do not allow dynamic updates  
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

W kolejnym oknie definiuje się czy ma zostać skonfigurowana strefa wyszukiwania

wstecznego. Należy zaznaczyć **TAK** (*Yes, create a reverse lookup zone now*) i kliknąć **Dalej** (*Next*).



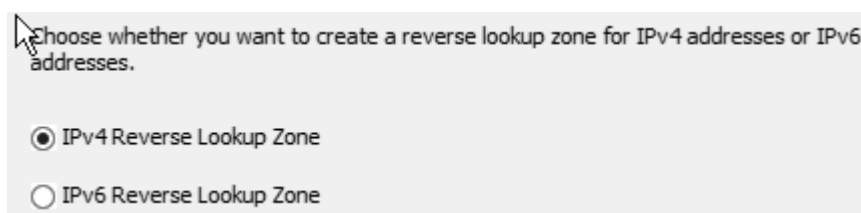
A reverse lookup zone translates IP addresses to DNS names. Reverse lookup zones are usually necessary only if programs require this information.

Do you want to create a reverse lookup zone now?

☒ Yes, create a reverse lookup zone now

☐ No, don't create a reverse lookup zone now

Kolejne trzy kroki są analogiczne do strefy wyszukiwania do przodu. Dochodzi się tak do planszy, na której należy zdefiniować czy strefa ma dotyczyć adresów **IPv4** (*IPv4 Reverse Lookup Zone*) czy **IPv6** (*IPv6 Reverse Lookup Zone*).

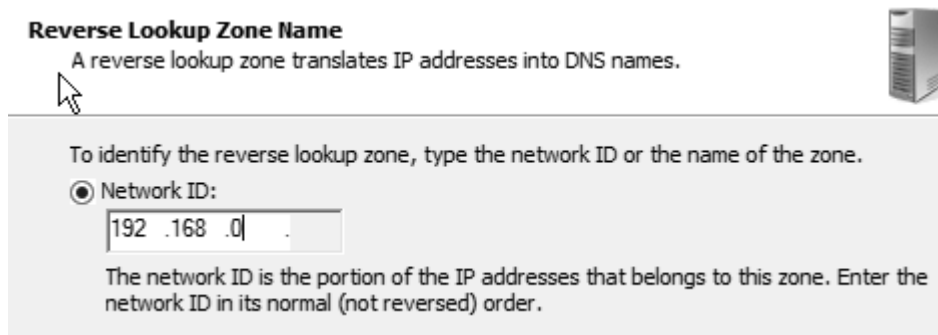


Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

☒ IPv4 Reverse Lookup Zone

☐ IPv6 Reverse Lookup Zone

Teraz należy zdefiniować adresację IP, jaka funkcjonuje w sieci.



**Reverse Lookup Zone Name**

A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:

192.168.0

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

Po raz kolejny należy skonfigurować aktualizacje dynamiczne.


## Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.



Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- ☐ Allow only secure dynamic updates (recommended for Active Directory)  
This option is available only for Active Directory-integrated zones.
- ☐ Allow both nonsecure and secure dynamic updates  
Dynamic updates of resource records are accepted from any client.  
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- ☒ Do not allow dynamic updates  
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

W kolejnym kroku definiuje się czy serwer ma przekazywać zapytania, których nie może rozwiązać do innego serwera, a jeśli tak to, do jakiego. W ćwiczeniowym przypadku przekazywanie zapytań dalej nie jest wymagane.

## Forwarders

Forwarders are DNS servers to which this server sends queries that it cannot answer.



Should this DNS server forward queries?

- ☐ Yes, it should forward queries to DNS servers with the following IP addresses:

IP Address	Server FQDN	Validated	
<Click here to ...			Delete
			Up
			Down

- ☒ No, it should not forward queries

If this server is not configured to use forwarders, it can still resolve names using root name servers.

Był to ostatni krok instalacji. Na karcie podsumowującej wystarczy kliknąć **Zakończ (Finish)**.

## Completing the Configure a DNS Server Wizard

You have successfully completed the Configure a DNS Server Wizard. When you click Finish, the following settings will be saved.

Settings:

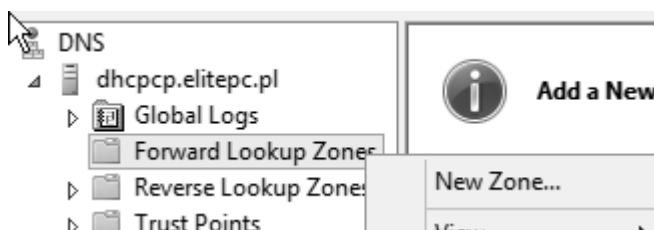
DNS server to configure: ELITEPC-DC01.elitepc.pl  
Forward lookup zone to create: elitepc.pl

Configure the hosts that will use this DNS server to point to this DNS server for name resolution, and then verify name resolution using nslookup. If you added a new primary zone, add resource records to it for the hosts whose names need to be resolved by this DNS server.

To close this wizard, click Finish.




Jeżeli ma istnieć zapasowy server DNS należy posiadać inny komputer z systemem Windows Server. Po zainstalowaniu na nim Roli serwera DNS należy w konsoli **DNS Manager** kliknąć prawym klawiszem myszy na strefie wyszukiwania i wybrać **New Zone (Nowa Strefa)**.




W kreatorze należy tym razem wybrać **Secondary Zone (Strefa Zapasowa)**. Dzięki temu obciążenie serwera DNS będzie nie tylko równoważone, ale także w razie awarii jednego serwera dane nie zostaną utracone, a jego rolę przejmie zapasowy serwer.

- ☒ **Secondary zone**  
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ **Stub zone**  
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

Należy wybrać odpowiednią nazwę strefy. Jest to o tyle ważne, iż jeżeli jest się w posiadaniu kilku domen można duplikować jedynie porcje danych, a nie całą zawartość serwera DNS.


 **Zone Name**  
What is the name of the new zone?




The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:


W kolejnym oknie należy podać adres IP komputera, na którym znajduje się już działający serwer DNS.

 **Master DNS Servers**  
The secondary zone is copied from one or more DNS servers.

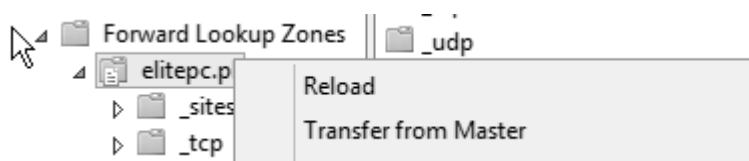


Specify the DNS servers from which you want to copy the zone. Servers are contacted in the order shown.

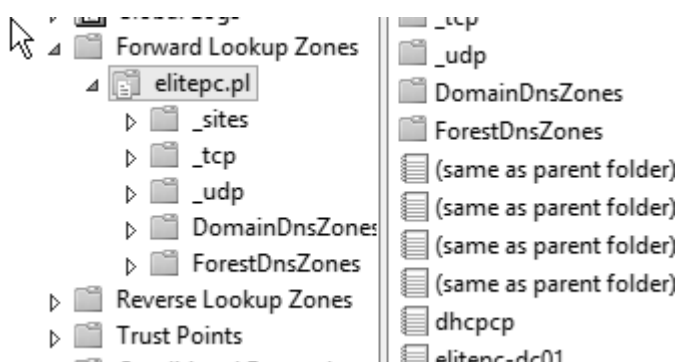
Master Servers:

IP Address	Server FQDN	Validated
<a href="#">&lt;Click here to add an IP Address or DNS Name&gt;</a>		
 192.168.0.1	elitepc-dc01	OK

Na karcie podsumowującej należy wybrać **Zakończ (Finish)**. Należy pamiętać, iż serwer główny musi mieć we właściwościach ustaloną zgodę na transfer strefy do docelowego serwera. Gdy zostanie to wykonane i wstępna synchronizacja zostanie wymuszona opcją **Transferuj z serwera głównego (Transfer From Master)** z menu kontekstowego, które jest dostępne po kliknięciu prawym przyciskiem myszy na nazwie domeny.



Po synchronizacji rekordy z głównego serwera DNS powinny pojawić się na serwerze zapasowym.

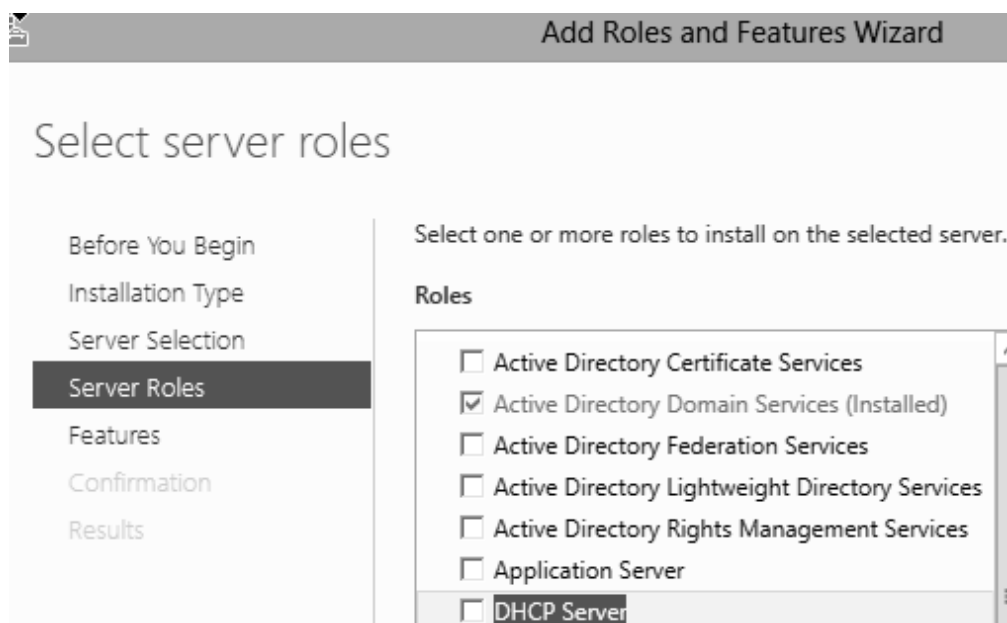


## 5. Serwer DHCP

Serwer DHCP mówiąc kolokwialnie przydziela adresy IP każdemu komputerowi, który się uruchomi podłączony do danej sieci. Jest to fundamentalny element każdej struktury sieciowej. Jedną z nowości w systemie Windows Server 2012 jest wprowadzenie funkcjonalności nazwanej polityką serwera DHCP (DHCP Policy). Czytelnik w tym dziale dowie się jak zainstalować i zarządzać serwerem DHCP.

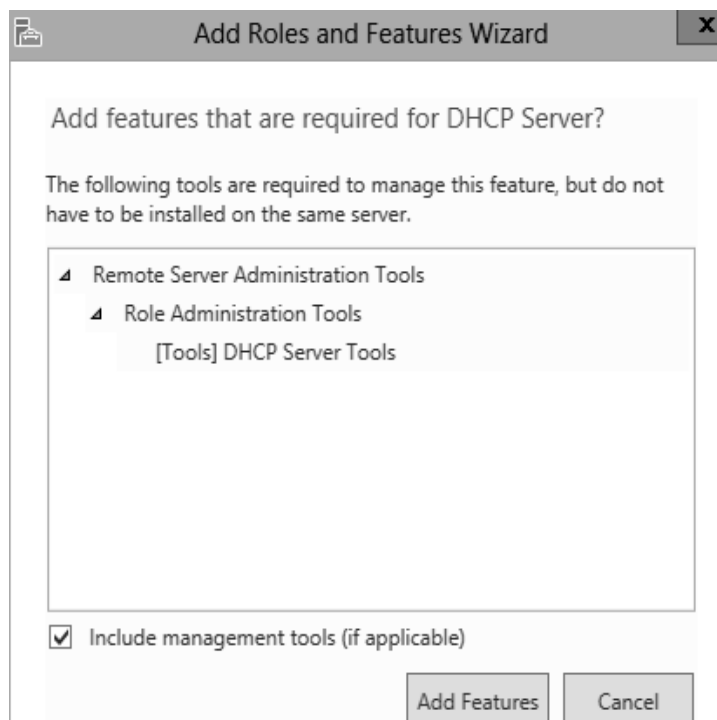
### 5.1. Instalacja pierwszego serwera DHCP

Podobnie jak w przypadku innych ról instalację serwera DHCP również rozpoczyna się z poziomu *Menadżera Serwera (Server Manager)*. Żeby zainstalować należy wybrać w kreatorze rolę *Serwer DHCP (DHCP Server)* i kliknąć *Dalej (Next)*.

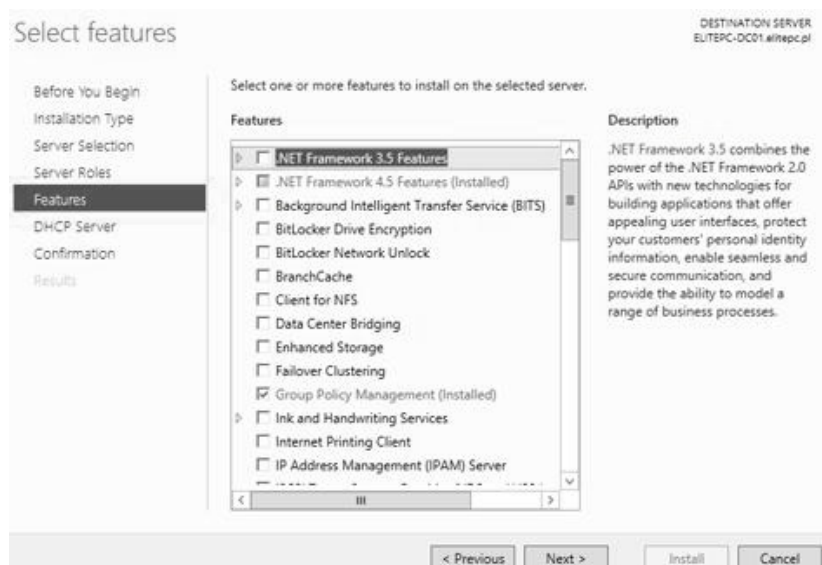


Następnie należy zaakceptować instalację wszelkich dodatkowych wymaganych funkcji.





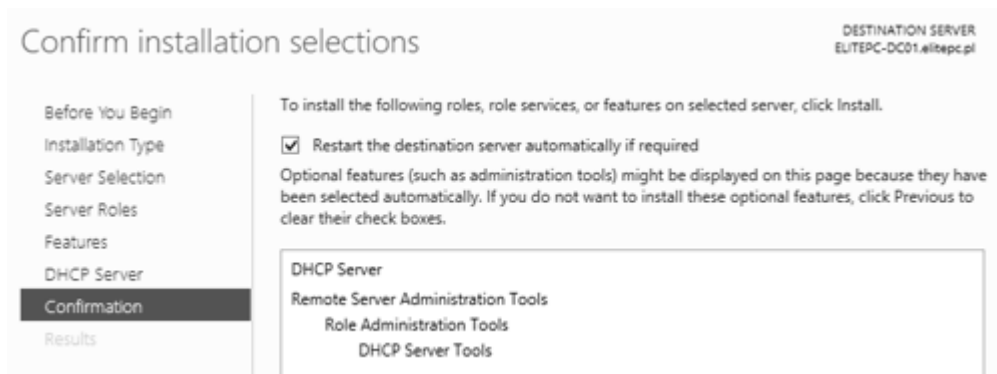
Na kolejnej planszy należy kliknąć **Dalej (Next)**.



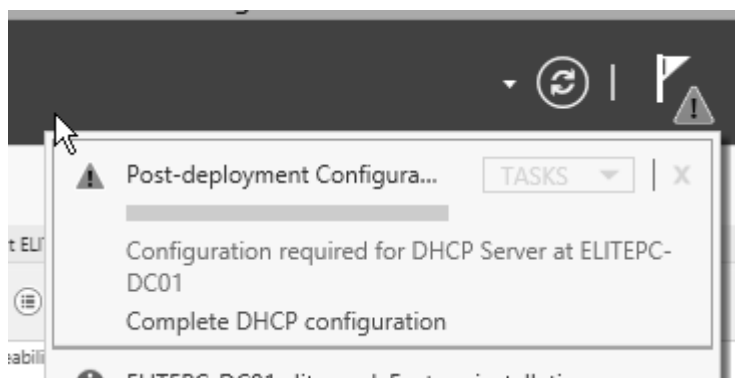
Następnie należy przejść **Dalej (Next)**.



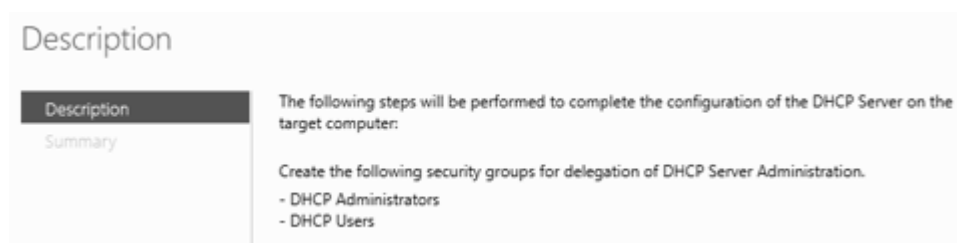
Na ostatniej karcie podsumowującej należy zaznaczyć opcję **Uruchom ponownie serwer docelowy jeśli wymagane (Restart the destination server automatically if required)**, aby w razie potrzeby serwer sam uruchomił się ponownie, a następnie należy kliknąć **Zainstaluj (Install)**.



Po ponownym uruchomieniu komputera i wejściu do konsoli **Menadżer Serwera (Server Manager)** w centrum akcji można zauważyć, że niezbędna jest dodatkowa konfiguracja serwera DHCP. Należy więc kliknąć **Dokończ konfigurację serwera DHCP (Complete DHCP Configuration)**.



Pojawi się kreator post instalacyjny. Jego zadaniem będzie utworzenie dwóch lokalnych grup bezpieczeństwa dla Administratorów i użytkowników DHCP. Należy kliknąć przycisk **Wykonaj (Commit)**.



Następnie należy podać dane użytkownika, który ma uprawnienia niezbędne do autoryzacji serwera DHCP w usłudze Active Directory (**Use the following user's credentials**). Można także pominąć autoryzację (**Skip AD authorization**).

☒ Use the following user's credentials

User Name:

☐ Use alternate credentials

UserName:

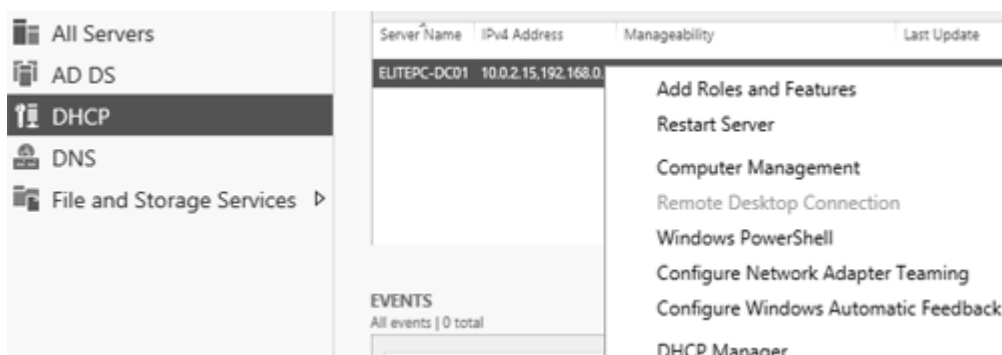
☐ Skip AD authorization

Wybór należy zaakceptować, a następnie zamknąć okno podsumowujące.

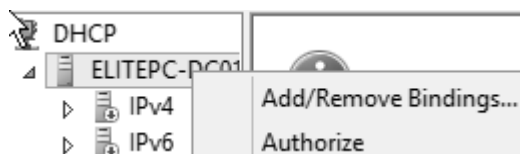


## 5.2. Konfiguracja serwera DHCP

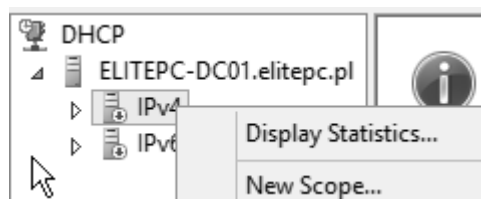
Kolejnym krokiem będzie wybranie DHCP w menu *Menadżera Serwera (Server Manager)* znajdującym się z lewej strony, a następnym kliknięcie prawym przyciskiem myszy na wybranym serwerze i wybranie opcji zarządzania nim *Menadżer DHCP (DHCP Manager)*.



Jeżeli serwer nie został jeszcze autoryzowany w Active Directory, wystarczy kliknąć na nim prawym przyciskiem myszy i wybrać opcję *Autoryzuj (Authorize)*. Jeżeli już jest autoryzowany można ten krok pominąć. Jeżeli AD i DHCP są instalowane na tej samej maszynie serwer autoryzuje się sam automatycznie



Kolejnym krokiem konfiguracji będzie stworzenie zakresów DHCP. Przykładowo niech będzie stworzony taki zakres dla protokołu IPv4. W tym celu należy rozwinąć drzewo serwera i klikając prawym przyciskiem myszy na IPv4 wybrać opcję **Nowy Zakres (New Scope)**.



W pierwszej karcie kreatora podaje się **Nazwę dla zakresu (Name)** oraz **Opis (Description)**, który będzie informował za co on odpowiada.

### New Scope Wizard

#### Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

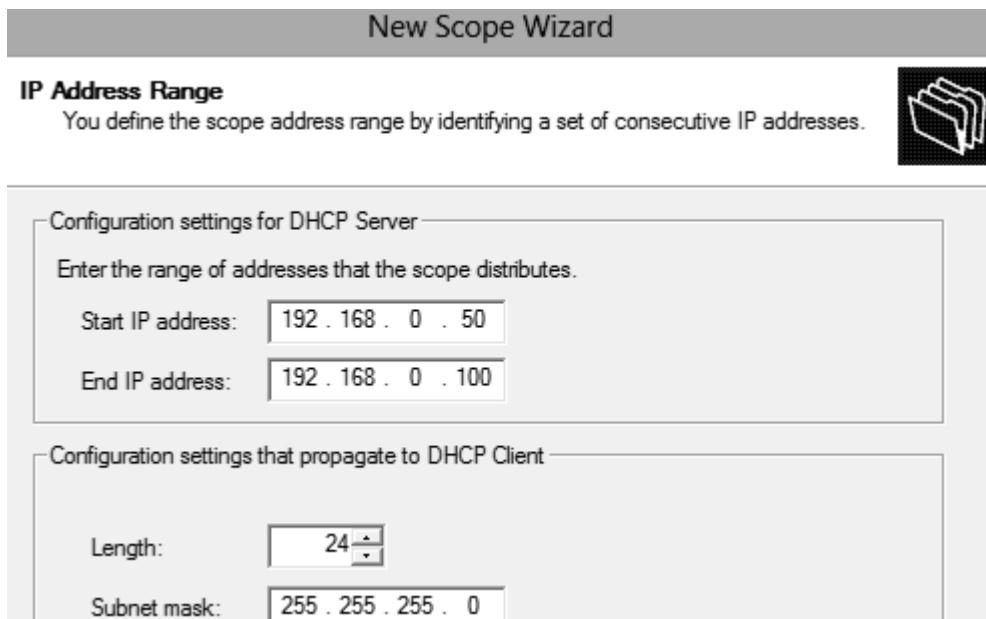
Jakaś nazwa

Description:

Opis

Na kolejnej karcie definiuje się dwa adresy IP. Jednym z nich będzie **Początkowy adres IP (Start IP address)**, począwszy od którego DHCP zacznie przydzielać klientom adresy IP, a drugi to **Końcowy adres IP (End IP address)**, na którym to serwer zakończy ich przydzielanie. Należy podać także **Maskę Podsięci (Subnet**

*Mask*), która ma być przypisywana klientom.



**New Scope Wizard**

**IP Address Range**

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 0 . 50

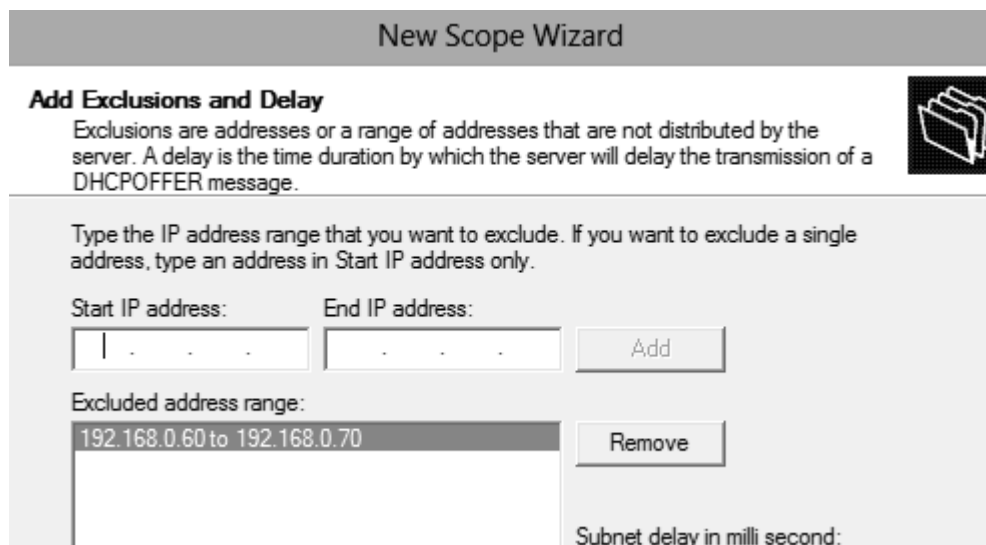
End IP address: 192 . 168 . 0 . 100

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

W kolejnym oknie analogicznie definiuje się zakres adresów IP z tym, że tym razem będą one dotyczyły puli adresów, które mają zostać wykluczone z wcześniej zdefiniowanej puli.



**New Scope Wizard**

**Add Exclusions and Delay**

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: . . . End IP address: . . . Add

Excluded address range:

192.168.0.60 to 192.168.0.70 Remove

Subnet delay in milli second:

W kolejnym kroku należy określić jak długo może trwać dzierżawa adresu. Domyślnie jest to 8 dni, po czym przydzielony adres jest zwalniany na potrzeby innego komputera.

### Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:	Hours:	Minutes:
<input type="text" value="8"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Można także skonfigurować opcje serwera DHCP. Na ogół ich konfiguracja jest zbędna do prawidłowego działania sieci. Dlatego też zostanie zaznaczona opcja pierwsza ***Tak chcę skonfigurować te opcje teraz (Yes, I want to Configure these options now)*** po to, aby je od razu skonfigurować z poziomu kreatora.

### Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

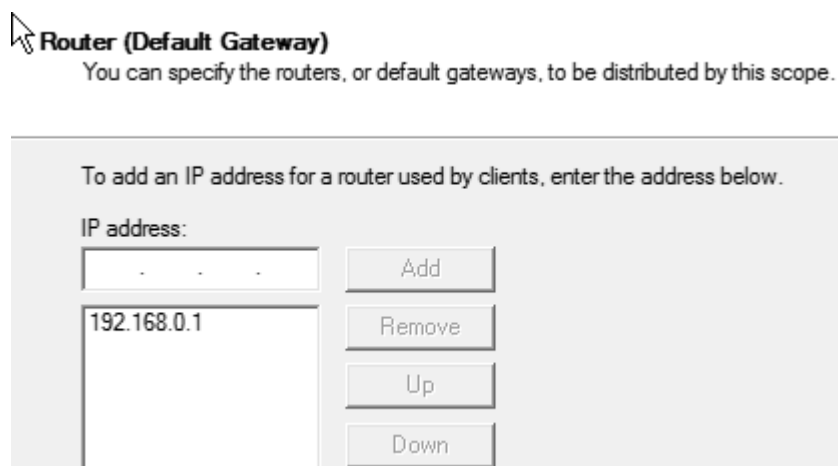
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- ☒ Yes, I want to configure these options now
- ☐ No, I will configure these options later

Jedną z nich będzie konfiguracja ***Routera (Bramki) (Router (Default Gateway))***,

gdzie wpisuje się adresy IP, pod którymi znajduje się wyjście z sieci na „świat”, np. Internet.



**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

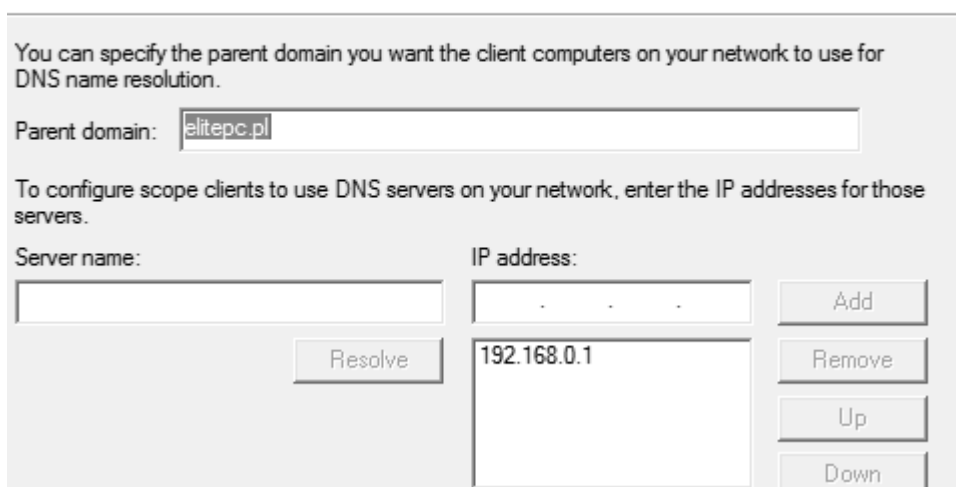
IP address:

- . -	Add
192.168.0.1	Remove
	Up
	Down

Następnie określa się adresy serwerów DNS z jakich ma się korzystać w sieci i opcjonalnie nazwę domeny. Należy pamiętać, że jeżeli maszyny mają prawidłowo pracować w domenie to niezbędne jest podanie wewnętrznych, firmowych adresów serwerów DNS powiązanych z Active Directory.

### Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:
<input type="text"/>	- . -
<input type="button" value="Resolve"/>	192.168.0.1
	Add
	Remove
	Up
	Down



Jeżeli korzysta się z serwerów WINS, w tym kreatorze także można określić ich sieciowe lokalizacje.

**WINS Servers**

Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:

IP address:

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

Ostatnim pytaniem, na jakie należy odpowiedzieć jest to, czy kreator ma uruchomić stworzony zakres czy też nie. Jeśli ma zostać uruchomiony należy wybrać, że się chce (*Yes, I want to deactivate this scope now*).

**Activate Scope**

Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

Przycisk **Zakończ** (*Finish*) zamyka kreatora.

## Completing the New Scope Wizard

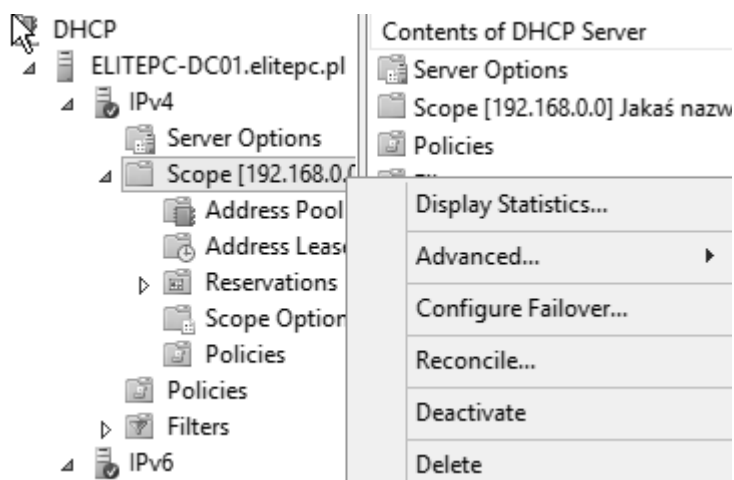
You have successfully completed the New Scope wizard.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

To close this wizard, click Finish.

### 5.3. Zarządzanie serwerem DHCP

Po chwili serwer powinien być gotowy do pracy. Obok jego ikonki powinna pojawić się zielona tarcza. Jeżeli nie pojawia się ona od razu należy chwilę poczekać i odświeżyć widok (opcja w menu kontekstowym bądź guzik F5 na klawiaturze). Stworzony zakres można zawsze skasować klikając na nim prawym przyciskiem myszy i wybierając *Usuń (Delete)*. Mniej inwazyjną metodą jego wyłączenia będzie *Dezaktywacja (Deactivate)*.



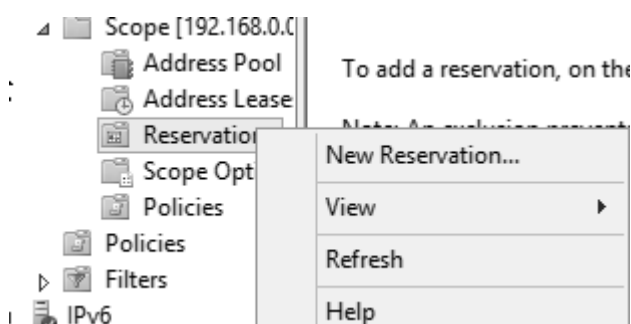
W ramach zakresu można między innymi wejść w jego **Właściwości (Properties)**. Znajdują się tam dodatkowe możliwości konfiguracyjne. We właściwościach znajduje się zakładka DNS, gdzie można skonfigurować pozostałe opcje związane z aktualizacjami dynamicznymi. Jest to krok niezbędny, aby dynamiczne aktualizacje działały. Należy więc zapamiętać, że ich konfiguracja jest dwu stopniowa. Należy je uruchomić zarówno po stronie serwera DNS jak i serwera DHCP.



W sekcji **Ochrona Nazwy (Name Protection)** można kliknąć przycisk **Konfiguruj (Configure)** i uruchomić ochronę, która sprawi, że duplikaty rekordów DNS nie wystąpią.

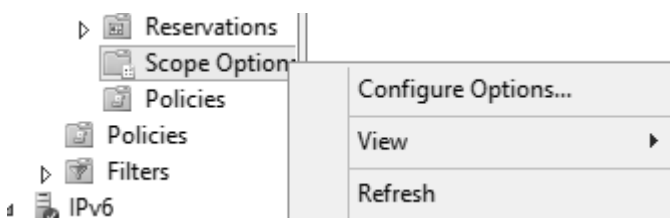


W bardzo łatwy sposób można także stworzyć zastrzeżenie, które będzie bardzo przydatne, kiedy dany adres IP ma być zarezerwowany dla drukarki czy innego komputera taki. Zawsze będzie on miał przypisany konkretny adres. Wystarczy na **Rezerwacje (Reservations)** kliknąć prawym przyciskiem myszy i wybrać **Nowe Zastrzeżenie (New Reservation)**.

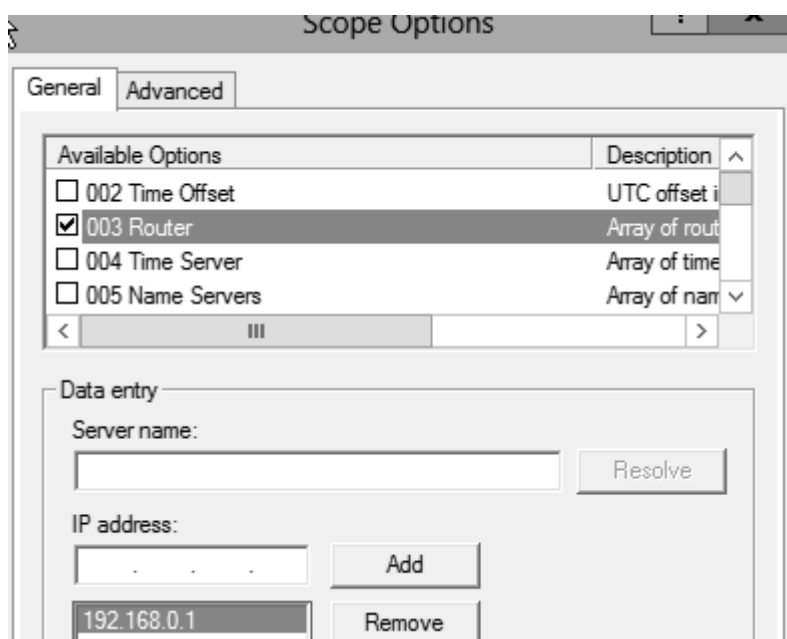


Pojawi się małe okienko, w którym należy podać **Nazwę zastrzeżenia (Reservation Name)**, **adres IP (IP address)**, który ma być przypisany temu urządzeniu, a także **Adres MAC (MAC address)** karty sieciowej tego urządzenia dzięki czemu serwer DHCP je rozpozna w sieci. Można także wprowadzić **Opis (Description)**.

Bardzo pożyteczne i przydatne są opcje zakresu. Trzy z nich zostały już skonfigurowane, lecz czasami może się to okazać niewystarczające. Należy więc kliknąć prawym klawiszem myszy na *Opcje zakresu (Scope Options)* i wybrać *Konfiguruj Opcje (Configure Options)*.

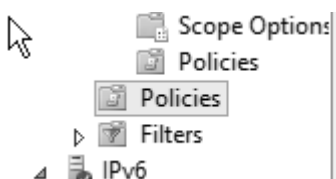


To właśnie w nich definiuje się adres IP routera, serwera czasu czy serwera PXE. Ustawienia te często są bardzo przydatne, a nierzadko niezbędne.



### 5.3.1. DHCP Policies

Omówione do tej pory moduły serwera DHCP nie uległy zmianie względem starszych wersji systemu Windows Server. W wersji 2012 pojawiły się jednak **Polityki (Policies)**. Warto zauważyć, że można je definiować na poziomie serwera (dla wszystkich zakresów) lub na poziomie jedynie wybranego zakresu. Na rysunku poniżej występują one w dwóch miejscach.



Polityki pozwalają na określenie zasad przydzielania adresów urządzeniom które, aby dostać adres IP będą musiały spełniać pewne predefiniowane kryteria. Aby takie kryterium określić Należy kliknąć na **Polityki (Policies)** prawym przyciskiem myszy i wybrać **Nowa Polityka (New policy)**.



W pierwszym oknie kreatora konieczne jest podanie nazwy oraz opisu polityki.

**Policy based IP Address and Option Assignment**

This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.

Policy Name:

Description:

W następnym oknie kreatora definiuje się kryteria, jakie dane urządzenie musi spełnić. Kryteriów może być kilka i mogą być połączone operatorem logicznym AND (urządzenie musi spełniać wszystkie) lub OR (urządzenie musi spełniać minimum jedno kryterium). Przyciskiem ADD dodaje się kryteria.

A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.

Conditions	Operator	Value

☐ AND
 ☒ OR

Następnie należy określić kryterium warunku, którego jest kilka klas. Jedną z nich jest **Vendor Class**, która pozwoli określić dolną granicę wersji systemu Windows,

*User*, która pozwala udzielać dostęp na podstawie uprawnień użytkowników, *MAC*, która pozwala na filtrowanie po adresach MAC oraz *Client Identifier* i *Relay Agent Information*.

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: Vendor Class

Operator: Vendor Class  
User Class  
MAC Address  
Client Identifier  
Relay Agent Information

Value(s):

Value: Microsoft Windows 2000 Options

☐ Append wildcard(\*)

Add

Remove

Microsoft Windows 2000 Options

Należy kliknąć **OK** aby powrócić do kreatora i a następnie kliknąć **Dalej (Next)**. Włączy się karta konfiguracji opcji serwera. W dalszej kolejności należy zdefiniować to, jakie opcje zostaną przypisane klientom, których obejmie kryterium. Można więc mieć inne opcje dla maszyn spełniających kryteria i dla tych, które ich nie spełniają.

#### Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.



Vendor class: DHCP Standard Options

Available Options	Description
<input type="checkbox"/> 003 Router	Array of router addresses order
<input type="checkbox"/> 004 Time Server	Array of time server addresses,
<input type="checkbox"/> 005 Name Servers	Array of name servers [IEN 114]

< III >

Data entry

Server name:

Resolve



Na karcie podsumowującej należy kliknąć **Zakończ (Finish)**.

A new IP address and option assignment policy will be created with the following:

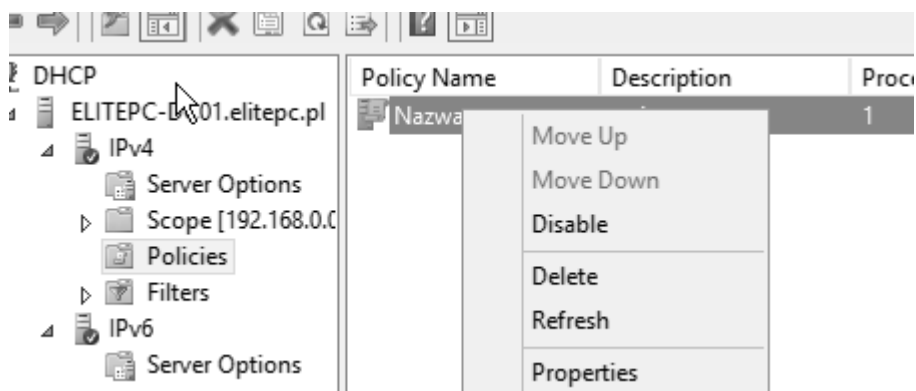
Name: Nazwa  
Description: opis  
Conditions: OR of

Conditions	Operator	Value
Vendor Class	Equals	Microsoft Windows 2000 Options

Settings:

Option Name	Vendor Class	Value
-------------	--------------	-------

Utworzona polityka zostanie wyświetlona na liście. Klikając na nią prawym klawiszem myszy w menu kontekstowym znajdują się opcje pozwalające ją **Wyłączyć (Disable)**, **Skasować (Delete)**, **Przenieść w górę (Move Up)** lub **w dół (Move Down)**, aby określić jej ważność. Im polityka znajduje się wyżej na liście tym jest ważniejsza.



Wchodząc we **Właściwości (Properties)** danej polityki można modyfikować jej właściwości.

**Nazwa Properties**

General Conditions Options DNS

Policy Name:

Description:

☐ Set lease duration for the policy

Lease duration for DHCP clients

☒ Limited to:

Days:  Hours:  Minutes:

☐ Unlimited

W przypadku polityki tworzonej po zmianie konkretnego zakresu w kreatorze pojawi się jeszcze jedna karta, która pozwala na stworzenie podzakresu adresów IP dla urządzeń, które są objęte daną polityką. „Mini” zakres musi znajdować się wewnątrz zakresu ogólnego.

A scope can be subdivided into multiple IP address ranges. Clients that match the conditions defined in a policy will be issued an IP Address from the specified range.

Configure the start and end IP address for the range. The start and end IP addresses for the range must be within the start and end IP addresses of the scope.

The current scope IP address range is 192.168.0.50 - 192.168.0.100

If an IP address range is not configured for the policy, policy clients will be issued an IP address from the scope range.

Do you want to configure an IP address range for the policy: ☒ Yes ☐ No

Start IP address:

End IP address:

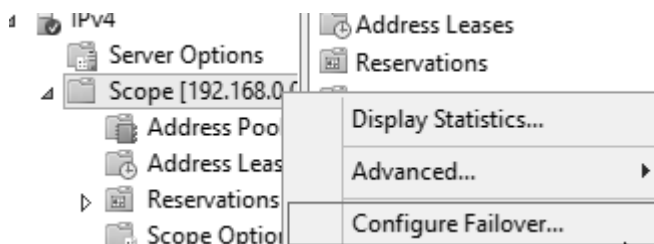
Percentage of IP address range: 21,6

## 5.4. Wysoka dostępność DHCP

Każdy serwer w tym także DHCP musi być dostępny 24h na dobę, 7 dni w tygodniu. Nawet podczas awarii serwera firma powinna móc dalej funkcjonować jak gdyby nic się nie stało z punktu widzenia użytkowników. Dlatego też tworzy się serwery zapasowe, które przejmują role głównych maszyn w razie ich awarii, przeciążenia lub niedostępności z innych powodów. Serwery te duplikują także dane. Za chwilę czytelnik dowie się jak zapewnić ciągłość i bezpieczeństwo działania serwera DHCP.

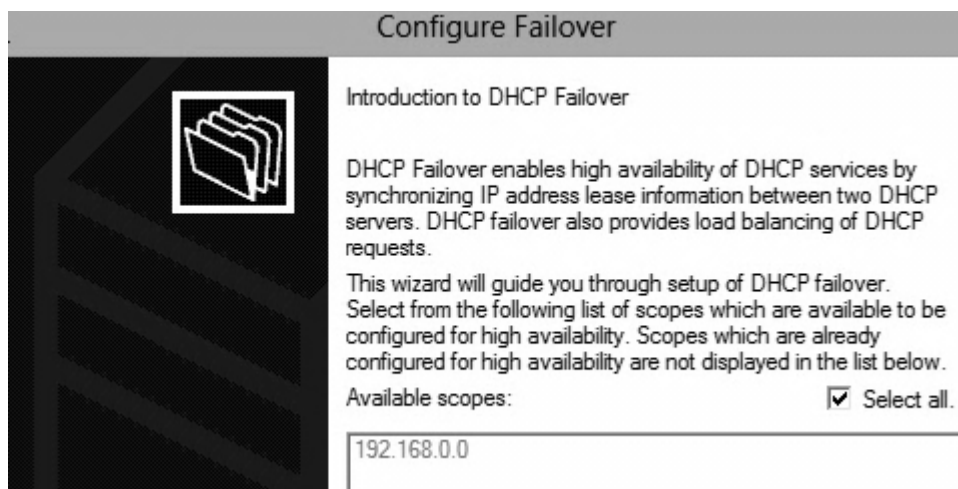
### 5.4.1. Konfiguracja klastra DHCP

Nowością w serwerze DHCP są elementy wysokiej dostępności związane z klastrami. Zostały one oparte na IETF-DHCP Failover Protocol. Przed kontynuacją należy pamiętać, że klastery wymaga systemu Windows Server w wersji Datacenter. Podobnie jak polityki, klastry można definiować dla zakresów jak i dla całego serwera. Pamiętać należy także o tym, aby w serwerze DHCP istniał przynajmniej jeden zakres. Jeżeli go nie będzie kreator konfiguracji nie do kolejnego kroku. Rzeczą naturalną jest to, że w sieci musi istnieć drugi serwer DHCP pod kontrolą Windows Server 2012, dlatego też dla utworzonego zakresu zostanie stworzony klastery. W tym celu należy kliknąć na zakresie prawym przyciskiem myszy i wybrać **Konfiguruj klastery (Configure Failover)**.



Na pierwszej karcie należy zdefiniować zakresy, które będą wykorzystywane bądź zaznaczyć opcję **Zaznacz Wszystko (Select All)**, aby wybrać wszystkie dostępne

zakresy. Należy kliknąć przycisk **Dalej (Next)**.



W kolejnym oknie konieczne jest wskazanie serwera partnerskiego, na którym replika będzie przechowywana. Będzie nią nie tylko baza danych DHCP, ale i konfiguracja serwera.

#### Specify the partner server to use for failover

Provide the host name or IP address of the partner DHCP server with which failover should be configured.

You can select from the list of servers with an existing failover configuration or you can browse and select from the list of authorized DHCP servers.

Alternatively, you can type the host name or IP address of the partner server.

Partner Server:

☐ Reuse existing failover relationships configured with this server (if any exist).

Przyciskiem **Dodaj Serwer (Add Server)** należy wybrać go. Serwer musi już być autoryzowany w domenie. Dla jednego zakresu można wybrać tylko jeden serwer partnerski.

Select a server you want to add to your console.

☐ This server:

☒ This authorized DHCP server:

Name	IP Address
dhccpc.elitepc.pl	192.168.0.5
elitepc-dc01.elitepc.pl	255.0.0.1

W kolejnym oknie relacji pomiędzy serwerami należy nadać nazwę. Wybiera się tu także **Tryb działania relacji (Mode)**. Do wyboru jest **Zrównoważenie Obciążenia (Load Balance)**, który będzie w określonym procentowo stopniu równoważył obciążenie serwera DHCP. Warto także ustawić czas w opcji **Maximum Client Lead Time**, która mówi o tym jak długo trwa czas dzierżawy dla klienta, który dostał dzierżawę adresu IP z dowolnego z serwerów. Jest on ważniejszy od czasu dzierżawy określonego dla zakresu. Warto także wybrać **Enable Message Authentication** i wprowadzić hasło o wysokiej złożoności. Dzięki temu komunikacja pomiędzy serwerami będzie szyfrowana funkcją SHA-2.

Create a new failover relationship with partner dhccpc.elitepc.pl

Relationship Name:

Maximum Client Lead Time:  hours  minutes

Mode:

Load Balance Percentage

Local Server: %

Partner Server: %

☐ Auto State Switchover Interval:  minutes

☒ Enable Message Authentication

Shared Secret:

Drugim trybem pracy jest **Hot Standby**. Tworzy on replikę, która przejmie rolę głównego serwera DHCP w razie jakichś problemów z dostępnością serwera

głównego. Warto w nim użyć opcji *Auto State Switchover Interval*, określa ona to, po jakim czasie od braku komunikacji z serwerem głównym zapasowy przejmie jego funkcje.

Relationship Name:	NAZWA
Maximum Client Lead Time:	1 hours 0 minutes
Mode:	Hot standby
Hot Standby Configuration	
Role of Partner Server:	Standby
Addresses reserved for standby server:	5 %
<input type="checkbox"/> Auto State Switchover Interval:	60 minutes
<input checked="" type="checkbox"/> Enable Message Authentication	
Shared Secret:	*****

Kolejna karta to podsumowanie, na której należy kliknąć *Zakończ (Finish)*.

Failover will be set up between elitepc-dc01.elitepc.pl and dhccp.elitepc.pl with the following parameters.

Scopes:

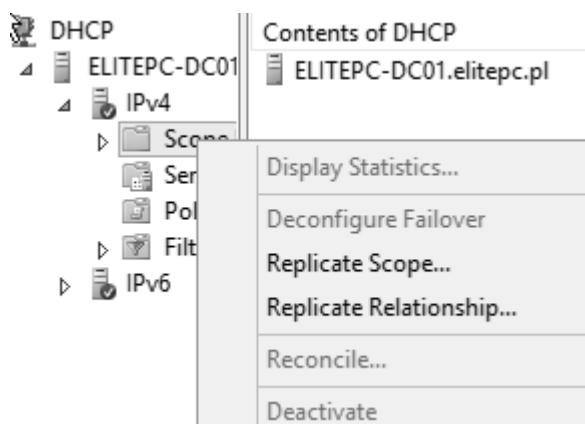
192.168.0.0

Relationship Name:	NAZWA
Maximum Client Lead Time:	1 hrs 0 mins
Mode:	Load balance
Auto Switchover Interval:	Disabled

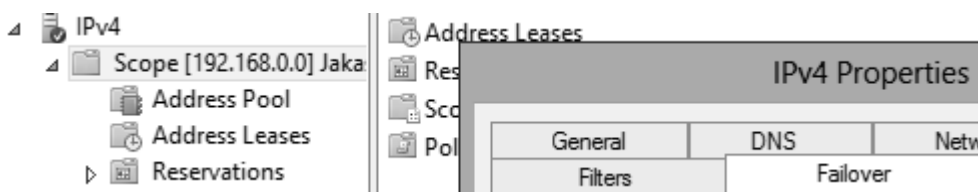
Load Balance Percentage

Local Server:	50 %
Partner Server:	50 %

Teraz dla zakresów pod prawym przyciskiem myszy dostępne będą dodatkowe funkcje związane z replikacją.

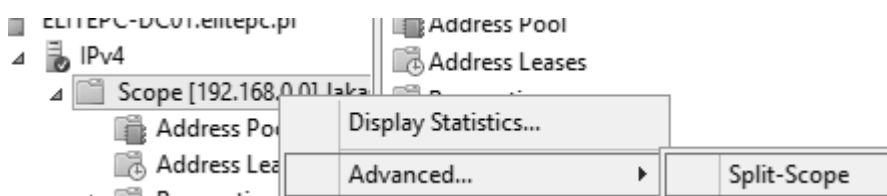


Aby skasować taką relację wystarczy wejść we właściwości IPv4, a następnie w zakładkę *Failover*.

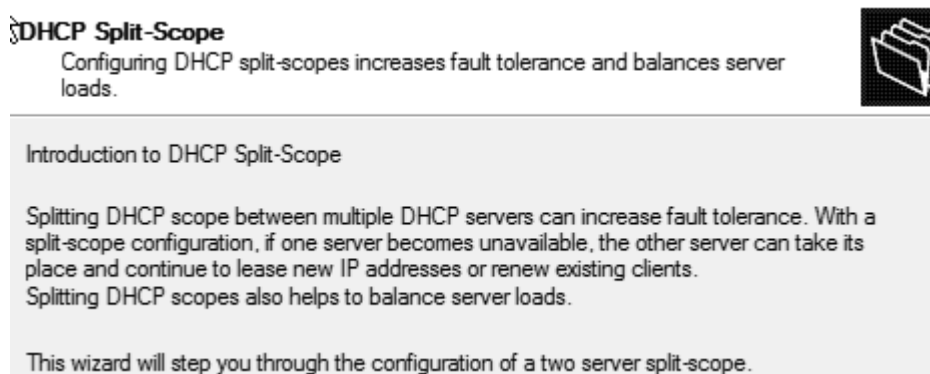


### 5.4.2. Split-Scope

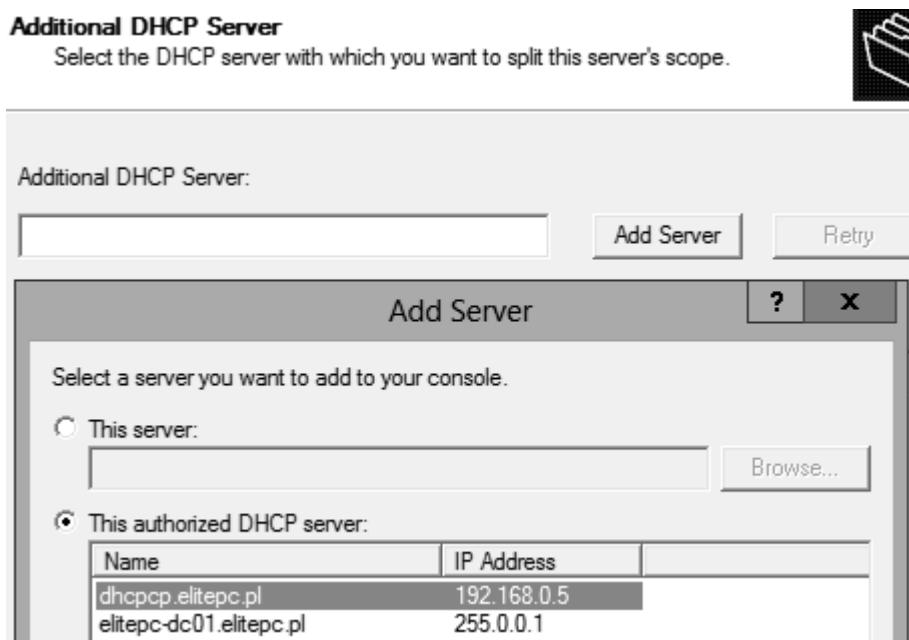
Jeżeli nie zostanie stworzony klaster można użyć funkcji znanej już z Windows Server 2008. Mowa tu o Split-Scope. Dzięki niej można stworzyć dwa serwery DHCP, pomiędzy którymi wybrany zakres zostanie rozdzielony, a w razie awarii serwera drugi przejmie jego rolę do czasu aż uszkodzony nie wróci do pełnej funkcjonalności. W tym celu wystarczy kliknąć prawym guzikiem na pożądanym zakresie, rozwinąć *Advanced (Zaawansowane)* i wybrać *Split-Scope*.



Na karcie powitalnej należy kliknąć **Dalej (Next)**.



Następnie podobnie jak w przypadku klastra należy określić serwer zapasowy. Również musi być autoryzowany w AD.





W kolejnym oknie konieczne jest określenie w procentach jaka część adresów będzie obsługiwana na głównym serwerze DHCP, a jaka na obecnie dodawanym (na zrzucie ekranu 20%).

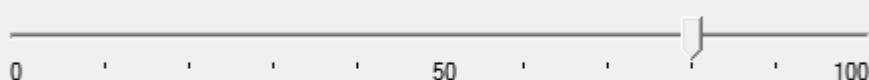
### Percentage of Split

Select the percentage of IP addresses that will be allocated to each of the split-scope servers.



Scroll the slider to choose the percentage of split of IPv4 address range of this scope:

192.168.0.50 192.168.0.100



	Host DHCP Server	Added DHCP Server
Percentage of IPv4 Addresses Served:	80	20

Following is the Exclusion IPv4 Address Range:

	Host DHCP Server	Added DHCP Server
Start IPv4 Address:	192 . 168 . 0 . 90	192 . 168 . 0 . 50
End IPv4 Address:	192 . 168 . 0 . 100	192 . 168 . 0 . 89

Note: The existing exclusions will also be configured appropriately on the DHCP Servers.

Następnie należy określić po jakim czasie DHCP zapasowy ma przydzielić adres, czyli ile czasu na reakcję dostaje serwer podstawowy.

### Delay in DHCP Offer

Specify the delay (in milli seconds) with which the added DHCP server distributes addresses.



	Host DHCP Server:	Added DHCP Server:
Delay in DHCP Offer (milli seconds):	<input type="text" value="10"/>	<input type="text" value="0"/>

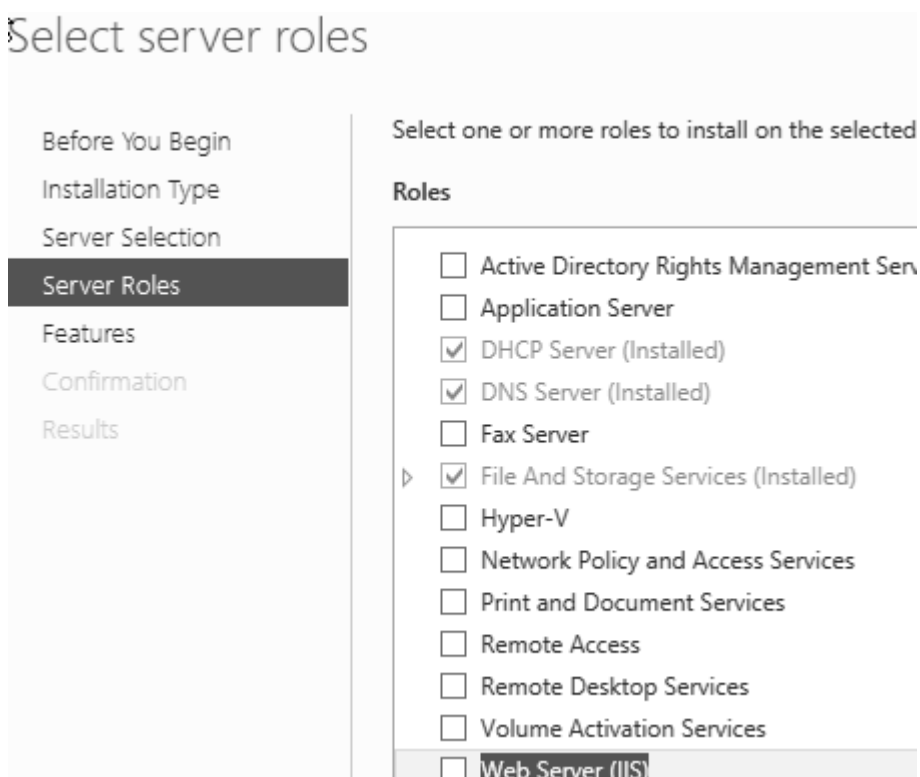
Na karcie podsumowującej należy kliknąć **Zakończ (Finish)**.

## 6. IIS z FTP oraz Urząd Certyfikacji

Internet Information Services, to rola serwera pozwalająca na hostowanie i publikowanie stron internetowych. Istnieje także możliwość publikacji witryn FTP. Obie te funkcje zostaną omówione w niniejszym rozdziale. Omówiony zostanie także Urząd Certyfikacji, ponieważ jego działanie i istnienie jest ściśle powiązane z serwerem www.

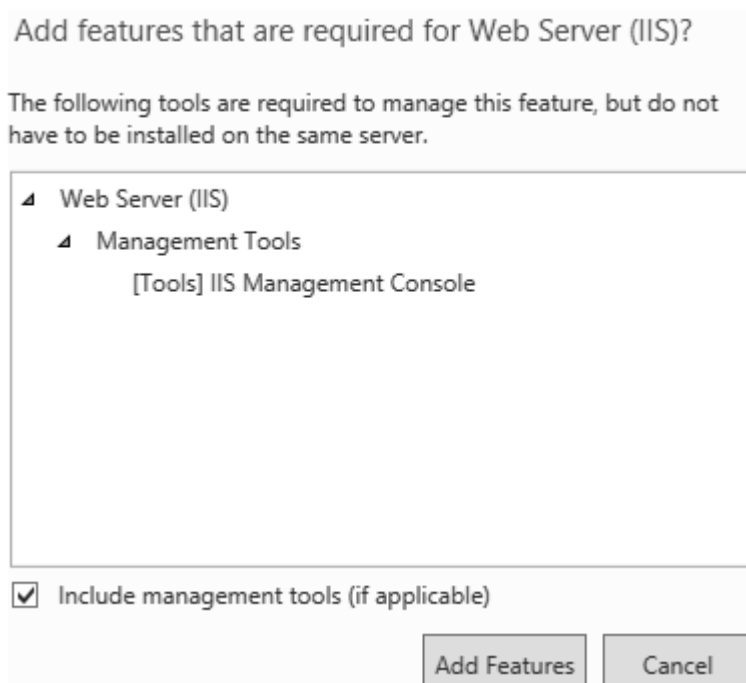
### 6.1. Instalacja roli Web Server (IIS)

Na początek należy zainstalować rolę *Web Server (IIS)* przy pomocy *Menadżera Serwera (Server Manager)*.

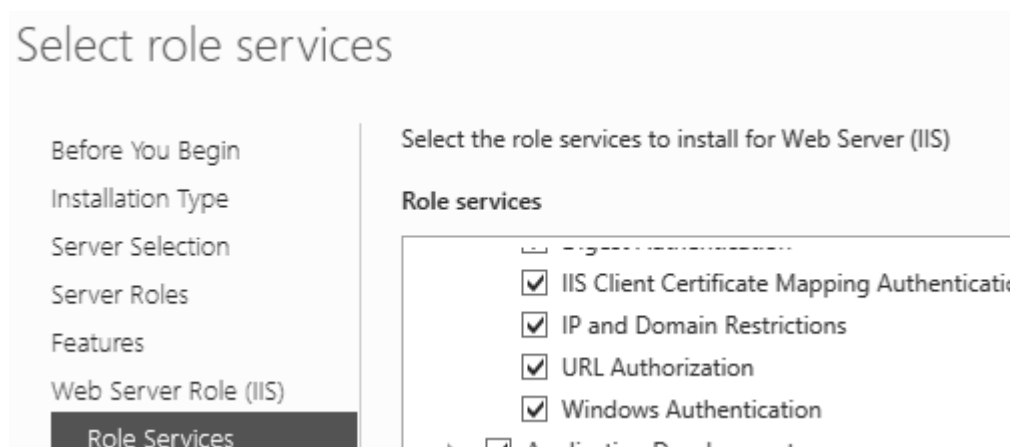


Należy zainstalować wymagane dodatki, a następnie zaakceptować je przyciskiem

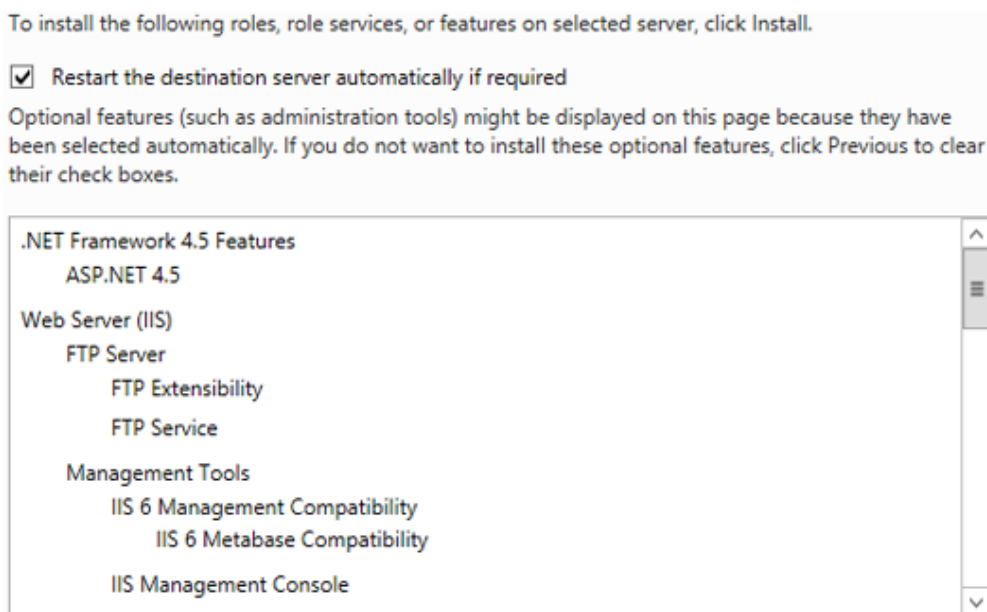
### ***Dodaj funkcję (Add Features).***



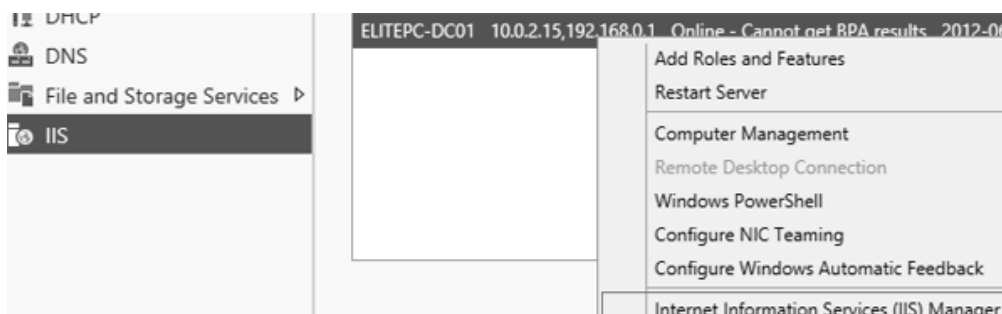
Spokojnie można zainstalować wszystkie usługi dostępne w serwerze IIS, aby w razie potrzeby nie musieć czegoś dodatkowo instalować. Można więc zaznaczyć wszystkie składniki IIS.



Proces instalacji tylu usług jednocześnie chwilę potrwa. Mimo, że kreator tego nie wymaga po instalacji warto uruchomić ponownie serwer.

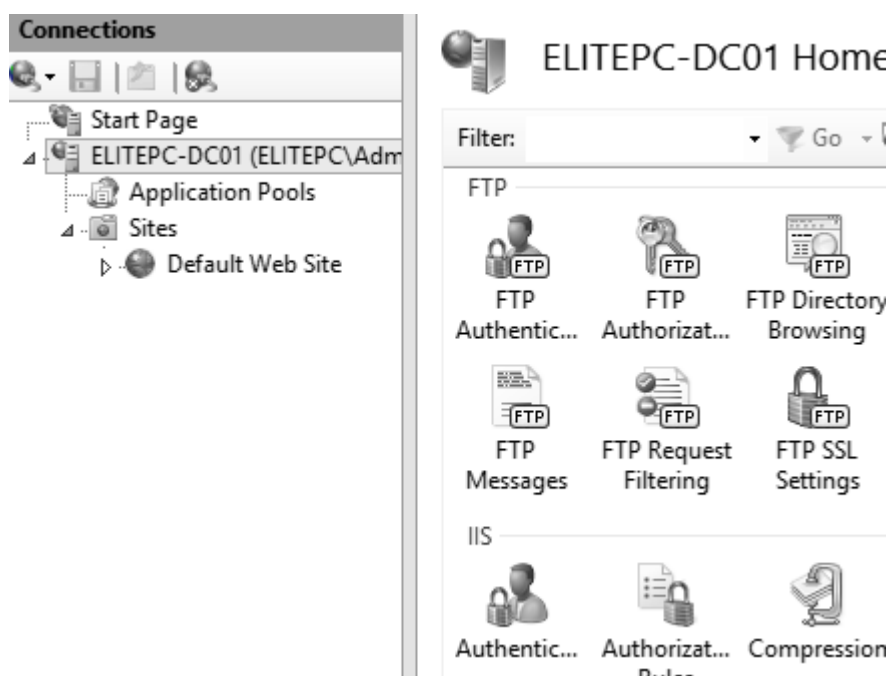


Menadżera IIS można odnaleźć w **Menadżerze Serwera (Server Manager)** w menu po lewej stronie. Podobnie jak i w przypadku innych ról po jego kliknięciu w centralnej części okna pojawi się lista serwerów, którymi można zarządzać. Po kliknięciu na wybranym prawym przycisku myszy należy wybrać **Menadżera IIS (Internet Information Services (IIS) Manager)**.



Standardowo uruchomiona jest już Domyślna Witryna. Najłatwiej jest wgrać swoją

stronę www do katalogu C:\inetpub\wwwroot, aby ona zadziałała. Jej możliwości będą ograniczone do najbardziej elementarnych funkcjonalności, a także nie będzie ona w żaden sposób zabezpieczona np. logowaniem. Co więcej doświadczeni użytkownicy Windows Server zauważą, że z punktu widzenia interfejsu użytkownika nie widać na pierwszy rzut oka zmian względem serwera IIS w Windows Server 2008.



## 6.2. Instalacja Active Directory Certificate Services

Po instalacji serwera IIS warto zainstalować *Urząd Certyfikacji (Certification Authority)*. IIS zawiera w sobie część składników wymaganych przez *Urząd Certyfikacji (CA, od Certification Authority)*, a same certyfikaty przydadzą się między innymi do zabezpieczenia witryny www. Zostanie więc zainstalowana rola *Active Directory Certificate Services* wraz ze wszystkimi dodatkami.

## Select server roles

Before You Begin

Installation Type

Server Selection

**Server Roles**

Features

AD CS

Role Services

Confirmation

Select one or more roles to install on the selected server.

**Roles**

- ☒ **Active Directory Certificate Services**
- ☒ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☒ DHCP Server (Installed)

Należy wybrać *Usługi Roli (Role Services)*.

## Select role services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD CS

**Role Services**

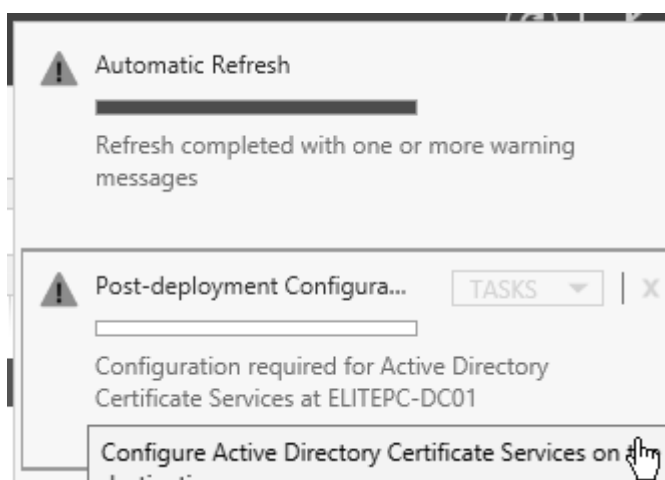
Confirmation

Select the role services to install for Active Directory Certificate Services.

**Role services**

- ☒ Certification Authority
- ☒ Certificate Enrollment Policy Web Service
- ☒ Certificate Enrollment Web Service
- ☒ Certification Authority Web Enrollment
- ☒ Network Device Enrollment Service
- ☒ **Online Responder**

Niezbędna będzie dodatkowa konfiguracja, do której wchodzi się poprzez *Centrum Akcji (Action Center)*.



W pierwszej karcie nowo otwartego kreatora należy podać dane użytkownika, który będzie miał stosowne uprawnienia do przeprowadzenia konfiguracji.

## Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: ELITEPC\Administrator

Change...

Na kolejnej karcie wystarczy, że zostanie skonfigurowany **Urząd Certyfikacji (Certification Authority)**, jednak wraz z nim można skonfigurować pozostałe usługi wybrane na zrzucie ekranowym. Dwie inne wybrane opcje wymagają odrębnej konfiguracji po uruchomieniu CA.

## Select Role Services to configure

- ☒ Certification Authority
- ☒ Certification Authority Web Enrollment
- ☒ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☒ Certificate Enrollment Policy Web Service

Następnie należy zdefiniować rodzaj CA. Enterprise wymaga do działania AD, natomiast w Standalone CA może nie być powiązany z AD i służyć np. jedynie jako uzupełnienie serwera hostingowego. Jako, że serwer ćwiczeniowy korzysta z AD zostanie wybrana opcja Enterprise.

## Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

### ☒ Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

### ☐ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

W następnym kroku należy zdefiniować to, czy jest to **Główny serwer CA (Root CA)** czy **Podrzędny (Zapasowy) (Subordinate CA)**. W tym przypadku jest to jednak serwer główny.



## Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the hierarchy.

☒ Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ Subordinate CA

Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates from the CA above them in the hierarchy.

W kolejnym zostanie stworzony **Klucz Prywatny (Private Key)**. Gdyby taki już istniał byłaby możliwość użycia go (*Use existing private key*). Jako, że ma zostać stworzony, należy wybrać opcję pierwszą **Stwórz nowy klucz prywatny (Create a new private key)**.

## Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ Create a new private key

Use this option if you do not have a private key or want to create a new private key.

☐ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

☐ Select a certificate and use its associated private key

Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

Na kolejnej karcie istnieje możliwość wybrania metody kryptografii. Jeżeli administrator nie zgłębił tego tematu i nie ma zbyt dużej wiedzy na temat metod

kryptografii, najlepiej będzie zostawić ustawienia domyślne.

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

W kolejnym oknie należy zdefiniować informacje i nazwy związane z CA, informacje te znajdują się w certyfikatach.

### Specify the name of the CA

Type a common name to identify this certification authority (CA). This name identifies certificates issued by the CA. Distinguished name suffix values are automatically modified.

Common name for this CA:

elitepc-ELITEPC-DC01-CA

Distinguished name suffix:

DC=elitepc,DC=pl

Preview of distinguished name:

CN=elitepc-ELITEPC-DC01-CA,DC=elitepc,DC=pl

Następnie konieczne jest zdefiniowanie okresu ważności certyfikatu. Domyślnie jest to 5 lat.

## Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

Years ▼

CA expiration Date: 2017-06-04 18:34:00

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

W następnym kroku należy wybrać miejsce przechowywania logów i bazy danych.

## Specify the database locations

Certificate database location:

C:\Windows\system32\CertLog

Certificate database log location:

C:\Windows\system32\CertLog

W kolejnym oknie konieczne jest zdefiniowanie metody autentykacji użytkowników. Dla komputerów pracujących w domenie najlepszym wyborem będzie ***Zintegrowanie uwierzytelnianie systemu Windows (Windows integrated authentication)***.

## Select the type of authentication

- ☒ Windows integrated authentication
- ☐ Client certificate authentication
- ☐ User name and password

W kolejnym oknie należy wybrać certyfikat, który będzie używany do szyfrowania połączenia pomiędzy klientami a serwerem.

## Specify a Server Authentication Certificate

When communicating with clients, the web service(s) uses Secure Sockets Layer encrypt network traffic.

- ☒ Choose an existing certificate for SSL encryption (recommended)

Issued To	Issued By	Expiration Date
WMSvc-ELITEPC-DC01	WMSvc-ELITEPC-DC01	2022-06-02
ELITEPC-DC01.elitepc.pl	ELITEPC-DC01.elitepc.pl	2013-06-04

Na karcie podsumowującej należy wybrać **Konfiguruj (Configure)**. Po tym kroku warto uruchomić ponownie serwer.

To configure the following roles, role services, or features, click Configure.

### ^ Active Directory Certificate Services

#### Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	2017-06-04 18:34:00
Distinguished Name:	CN=elitepc-ELITEPC-DC01-CA,DC=elitepc,DC=pl
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

#### Certification Authority Web Enrollment

#### Online Responder

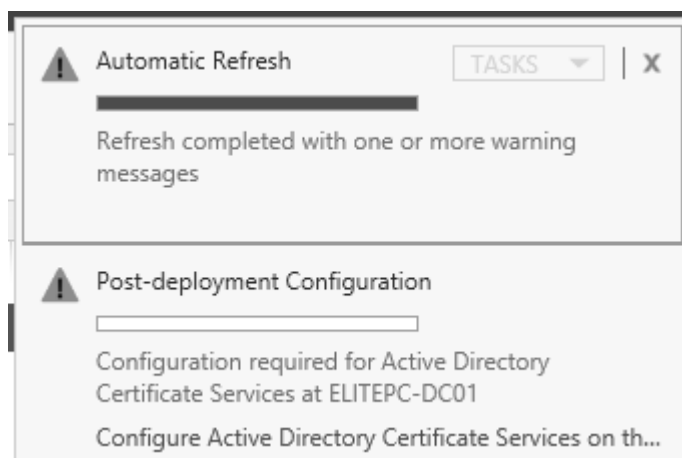
CA Web Enrollment Responder

< Previous

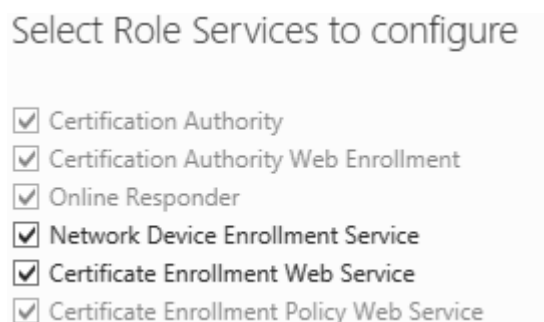
Next >

Configure

Teraz poprzez centrum akcji należy ponownie uruchomić kreatora konfiguracji CA.



Tym razem z listy usług konieczne jest wybranie dwóch opcji, których wcześniej nie można było zainstalować.



Następnie należy wybrać konto użytkownika, który ma uprawnienia do przeprowadzenia wymaganych zadań. Musi on należeć do grupy IIS\_IUSRS. Można więc dodać do tej grupy administratora i wykorzystać jego konto.

Select the identity the Network Device Enrollment Service (NDES) will use.

☒ Specify service account (recommended)

The account must be a member of the domain and must be added to the local IIS\_IUSRS group.

☐ Use the built-in application pool identity

W kolejnym oknie konieczne jest wprowadzenie informacji dotyczących przedsiębiorstwa.

Type the requested information to enroll for an RA certificate

A registration authority (RA) is required to manage the Network Device Enrollment Service (NDES) certificate requests.

Required information

RA Name:	<input type="text" value="ELITEPC-DC01-MSCEP-RA"/>
Country/Region:	<input type="text" value="PL (Poland)"/>

Optional information

E-mail:	<input type="text"/>
Company:	<input type="text"/>
Department:	<input type="text"/>
City:	<input type="text"/>
State/Province:	<input type="text"/>

Następnie należy wybrać **dostawcę (provider)** kryptografii wraz z długością klucza szyfrującego.

## Configure CSPs for the RA

Select the registration authority (RA) cryptographic service providers (CSPs) and key lengths for the signature and encryption keys.

Signature key provider:	Key length:
Microsoft Strong Cryptographic Provider ▼	2048
Encryption key provider:	Key length:
Microsoft Strong Cryptographic Provider ▼	2048

Teraz należy przejść do części kreatora odpowiedzialnej za konfigurację zapisów certyfikatów w sieci Web. Konieczne jest wybranie opcji *Nazwa komputera (Computer name)* i wybranie wcześniej skonfigurowanego CA.

## Specify CA for Certificate Enrollment Web Services

Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES).

Select:

☐ CA name

☒ Computer name

Target CA: ELITEPC-DC01.elitepc.pl\elitepc-ELITEPC-DC01-CA Select.

Kolejnym krokiem jest wybór metody autentykacji. Tak jak wcześniej należy pozostawić tą opcję domyślną tj. *Zintegrowane uwierzytelnianie systemu Windows (Windows integrated authentication)*.

## Authentication Type for CES

<ul style="list-style-type: none"> <li>Credentials</li> <li>Role Services</li> <li>Service Account for NDES</li> <li>RA Information</li> <li>Cryptography for NDES</li> <li>CA for CES</li> </ul>	<h3>Select the type of authentication</h3> <p> <input checked="" type="radio"/> Windows integrated authentication  <input type="radio"/> Client certificate authentication  <input type="radio"/> User name and password         </p>
---	---

Należy teraz zdefiniować konto użytkownika, który będzie odpowiadał za komunikację pomiędzy CES a CA. Na potrzeby książki będzie to Administrator. Następnie na karcie podsumowującej należy kliknąć **Konfiguruj (Configure)**, a po chwili **Zamknij (Close)**.

## Specify the service account

Select the identity that the Certificate Enrollment Web Service (CES) uses when communicating with the certification authority (CA) and other services on the network.

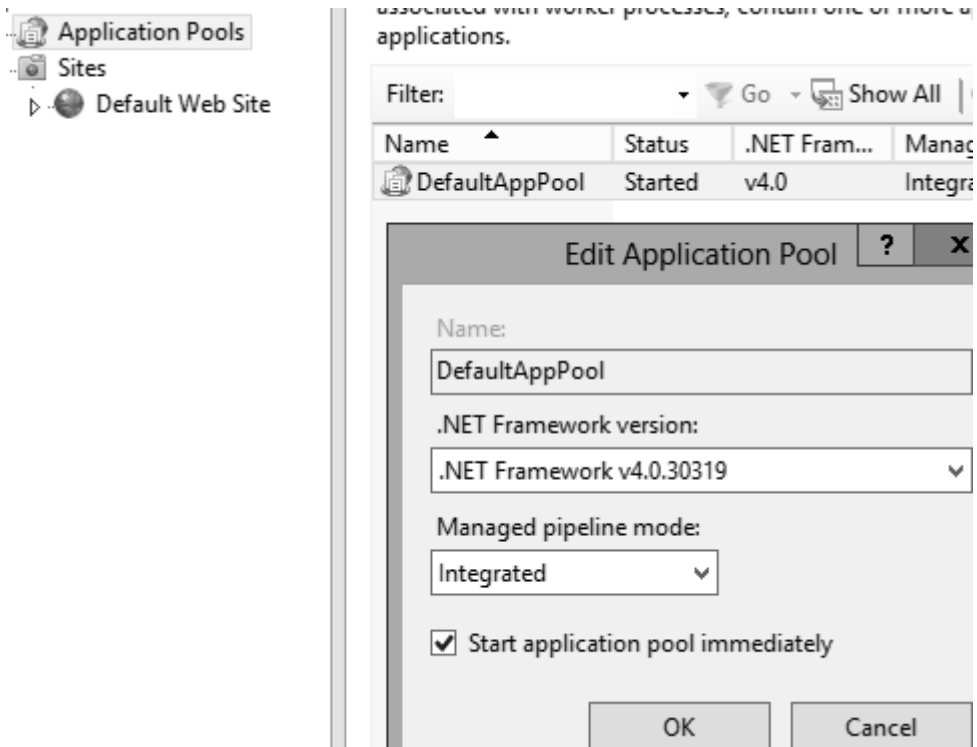
☒ Specify service account (recommended)

The account selected must be a member of the IIS\_USRS group. If Kerberos is selected as the authentication type, a service principal name is required for the service account.

### 6.3. Aktualizacja platformy .NET

Gdy urząd certyfikacji będzie już zainstalowany i skonfigurowany warto wrócić do menadżera IIS. W sekcji **Pule Aplikacji (Application Pool)** .NET można ustawić platformę .NET Framework jaką ma domyślnie używać serwer, będzie to wersja 4.0. Aby nowsza wersja była dostępna w tym oknie konieczne jest jej pobranie z Internetu i zainstalowanie.





Jeśli dana wersja nie będzie widoczna konieczne będzie wykonanie w konsoli odpowiedniego polecenia odpowiadającego za instalację ASP.NET.

```

Konto kontenera -pa Dodaj dostp konta do kontenera. Argumenty:
Kontener uytkownika [-pkul] zamiast kontenera
Dostawca Csp [-csp provider] do uycia.
[-full] Dodaj peny dostp (ustawieniem domylny
z prawem do odczytu).

konto kontenera -pr Usu dostp konta z kontenera. Argumenty:
Kontener uytkownika [-pkul] zamiast kontenera
Dostawca Csp [-csp provider] do uycia.

-- OPCJE KONFIGURACJI DOSTPU ZDALNEGO --

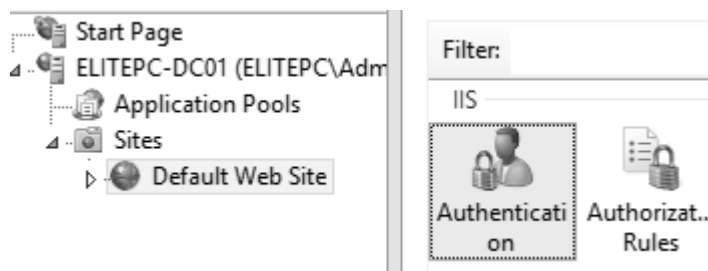
-config+ Wcz dostp zdalny do konfiguracji.
-config- Wycz dostp zdalny do konfiguracji.

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>aspnet_regiis.exe -i
Rozpoczto instalowanie platformy ASP.NET (2.0.50727).
.....
Zakoczono instalowanie platformy ASP.NET (2.0.50727).
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>

```

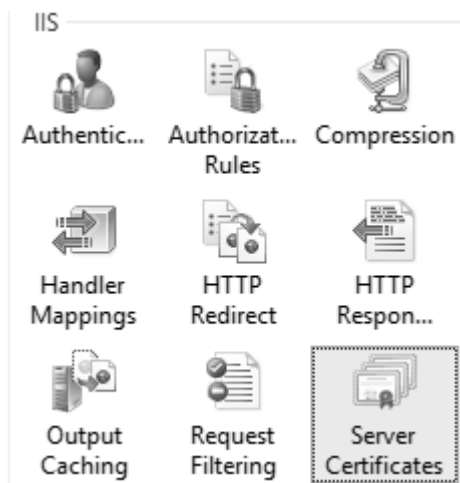
## 6.4. Tworzenie nowych Certyfikatów

Podstawowe opcje logowania można ustawić klikając w ikonę *Uwierzytelnianie (Authentication)* po wcześniejszym wybraniu w prawym menu pożądanej witryny sieci Web.

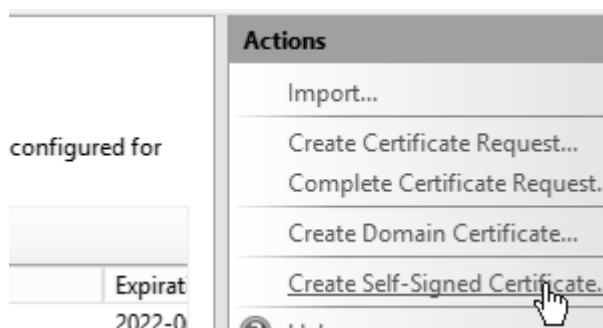


Warto jednak wcześniej wrócić poziom wyżej i klikając na nazwę serwera w drzewie po lewej stronie przejść do ogólnych ustawień serwera. Poza konfiguracją IIS znajduje się tam wiele innych opcji np. te związane z bezpieczeństwem, FTP oraz różne inne. W tym dziale strona zostanie zabezpieczona certyfikatem, a następnie logowaniem. Pierwszym krokiem będzie stworzenie jakiegoś certyfikatu

dla serwera. Należy kliknąć **Certyfikaty Serwera (Server Certificates)**.



Następnie należy kliknąć **Utwórz Certyfikat z Podpisem Własnym (Create Self-Signed Certificate)**. Dzięki temu uniknie się potrzeby odwoływania do głównego urzędu certyfikacji w domenie.



Pojawi się kreator, w którym należy podać nazwę oraz wybrać przeznaczenie certyfikatu, czyli na **Użytek własny (Personal)** lub **Hostingu www (Web Hosting)**.



## Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a signing:

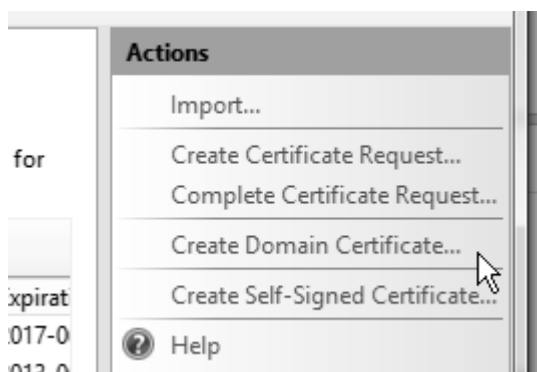
Specify a friendly name for the certificate:

Select a certificate store for the new certificate:

Personal	▼
Personal	
Web Hosting	

Następnie należy kliknąć **OK**.

Mając już zainstalowany CA łatwo jest także **utworzyć Certyfikat Domeny (Domain Certificate)**. Krok ten mogą pominąć osoby, którym wystarczy certyfikat z podpisem własnym, który wcześniej został utworzony. Certyfikat domeny tworzy się wybierając opcję **Stwórz Certyfikat Domeny (Create Domain Certificate)**.



W pierwszej karcie kreatora należy wypełnić dane dotyczące organizacji.



## Distinguished Name Properties

Specify the required information for the certificate. State/province and C official names and they cannot contain abbreviations.

Common name:	ElitePC Certyfikat IIS
Organization:	ElitePC
Organizational unit:	WAW
City/locality	Warsaw
State/province:	MZ
Country/region:	PL

Następnie definiuje się urząd certyfikacji, który ma zostać wykorzystany oraz należy podać przyjazną nazwę dla certyfikatu. W kolejnym kroku należy kliknąć **Zakończ (Finish)**.

Specify the certification authority within your domain that will sign the certificate and should be easy to remember.

Specify Online Certification Authority:

elitepc-ELITEPC-DC01-CA\ELITEPC-DC01.elitepc.pl

Example: CertificateAuthorityName\ServerName

Friendly name:

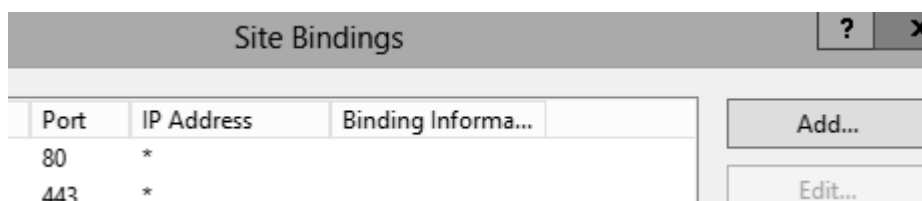
Certyfikat IIS

## 6.5. Zarządzanie Serwerem IIS

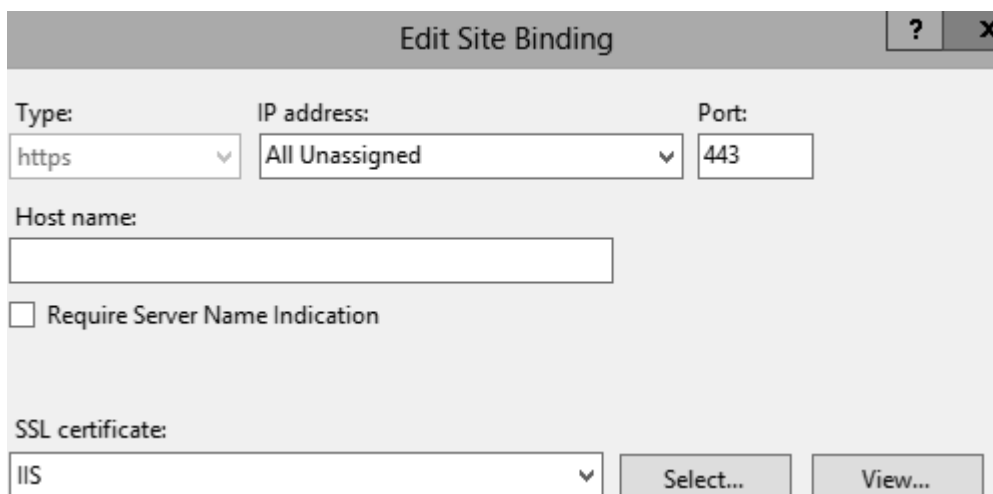
W przypadku książkowym pozostało już jedynie podłączyć certyfikat do danej witryny. Należy kliknąć najpierw na liście nazwę witryny, a następnie wybrać z menu po prawej opcję: **Powiązania (Bindings)**.



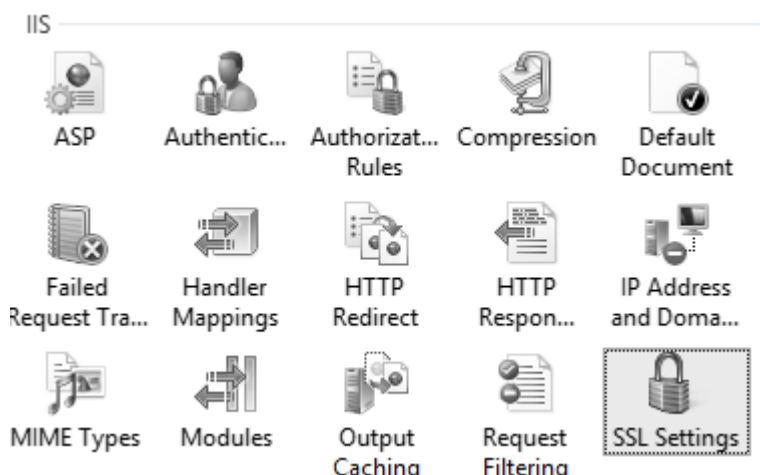
Na ekranie, jaki się pojawi należy kliknąć **Dodaj (Add)**.



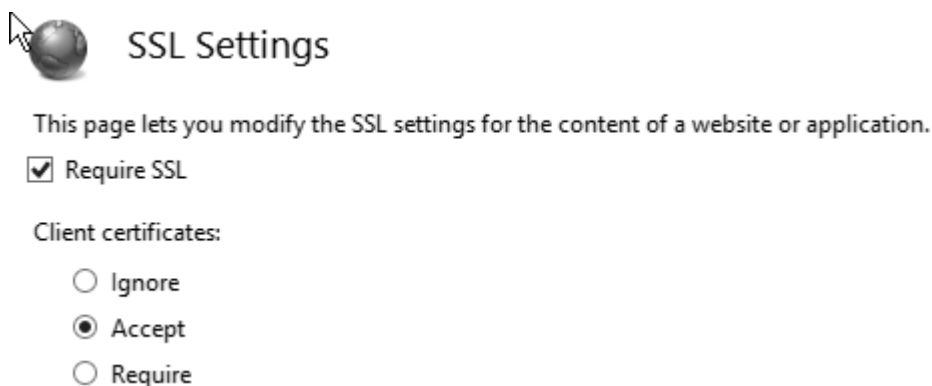
Jego typ należy ustawić na **https** i wybrać utworzony wcześniej certyfikat serwera. Wybranie w polu adres IP opcji **Wszystkie nieprzypisane (All unassigned)** powoduje tyle, iż na każdej karcie sieciowej na porcie **443** będzie używany ten, a nie inny certyfikat. Skasowanie powiązania HTTP sprawi, że nie będzie można podłączyć się do serwera w niezabezpieczony sposób. Warto też wtedy zablokować port w zaporze. Można także na zwykłej stronie stworzyć planszę informującą, że serwer wymaga certyfikatu wraz z przekierowaniem. Opcje te można zawsze zmienić przyciskiem edycji.



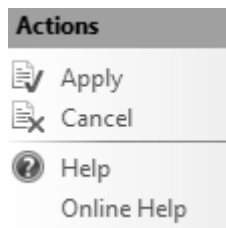
Inną metodą będzie wymuszenie wymagania certyfikatu SSL. Aby tego dokonać należy kliknąć w opcję ***Ustawienia Protokołu SSL (SSL Settings)***.



Na planszy, jaka się pojawi należy wybrać opcję ***Wymagaj Certyfikatu SSL (Require SSL)*** oraz zdefiniować dogodne ustawienia klienta. Zaleca się wybranie opcji ***Akceptuj (Accept)***.



Po wprowadzeniu ustawień należy kliknąć ***Zastosuj (Apply)*** w menu po prawej stronie.



Teraz każda próba wejścia na witrynę innym portem niż SSL zakończy się błędem i jednocześnie automatycznie wyświetli informacje na temat dalszego postępowania dla użytkownika.



## HTTP Error 403.4 - Forbidden

**The page you are trying to access is secured with Secure So**

### Most likely causes:

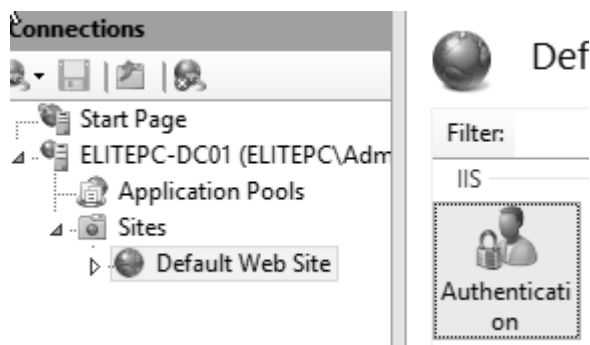
- Secure Sockets Layer (SSL) is enabled for the URL requested.
- The page request was made over HTTP, but the server requires the TPS.

Po wpisaniu w belce adresu przedrostka `https://` strona www powinna się załadować, a komunikacja powinna odbyć się w sposób szyfrowany. Naturalnie będzie konieczna akceptacja certyfikatu.



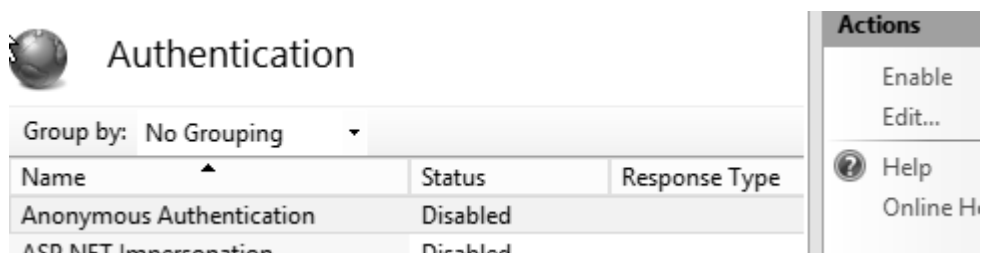


Warto się także zabezpieczyć stronę przed niepowołanymi odwiedzinami. W tym celu należy kliknąć dwukrotnie w ikonę *Uwierzytelnianie (Authentication)*.



Wyłączone także zostanie *Uwierzytelnianie anonimowe (Anonymous Authentication)*. Aby je wyłączyć należy kliknąć przycisk *Wyłącz (Disable)* z

prawej strony.



Uwierzytelnianie w sieci odbywa się na zasadzie komunikacji między serwerem a przeglądarką, podczas której przesyłane są nagłówki protokołu http oraz komunikaty o błędach.

Komunikacja przebiega następująco:

1. Przeglądarka zgłasza żądanie, np. HTTP-GET.
2. Serwer sprawdza, czy obowiązkowe jest uwierzytelnienie. Jeśli sprawdzenie się nie powiedzie, ponieważ uwierzytelnienie jest niezbędne, serwer odpowiada komunikatem o błędzie podobnym do tego poniżej:

***Brak upoważnienia do wyświetlania tej strony***

***Nie masz uprawnień, by przeglądać ten katalog lub tę stronę przy użyciu podanych poświadczeń. Komunikat ten zawiera informacje, których przeglądarka sieci Web może użyć do ponownego przesłania żądania, jako żądania uwierzytelnionego.***

3. Przeglądarka, na podstawie tego co odpowie serwer tworzy nowe żądania, które zawiera informacje o uwierzytelnianiu.
4. Serwer sieci Web dokonuje sprawdzenia uwierzytelnienia. Jeśli sprawdzenie powiedzie się, serwer sieci Web odsyła do przeglądarki

dane, których pierwotnie żądano.

***Istnieją następujące metody uwierzytelniania:***

- ***Uwierzytelnianie anonimowe (Anonymous Authentication)*** - w celu uwierzytelnienia użytkowników anonimowych, którzy żądają zawartości sieci, usługi IIS tworzą konto IUSR\_nazwa\_komputera. Konto to użytkownikowi daje uprawnienia do zalogowania się lokalnie. Istnieje możliwość zresetowania dostępu anonimowych użytkowników w sposób taki, aby używali dowolnego konta z systemu Windows.

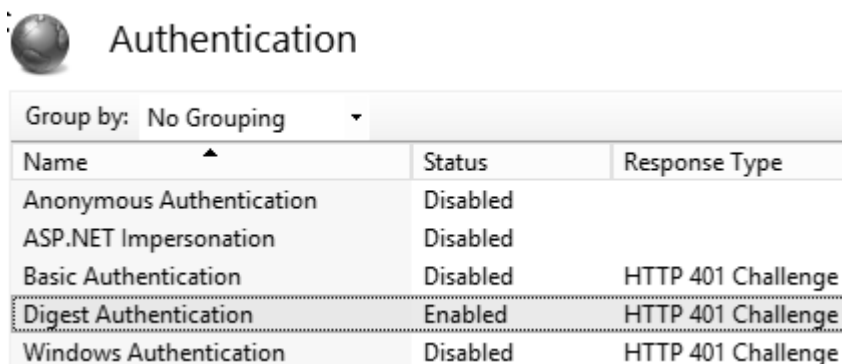
- ***Uwierzytelnienie podstawowe (Basic Authentication)*** – wykorzystywane jest do ograniczania dostępu do danych na serwerze znajdujących się na dysku sformatowanym w systemie NTFS. Jeśli używa się podstawowego uwierzytelniania, użytkownik ma obowiązek wprowadzenia poświadczeń, a możliwość dostępu jest zależna od identyfikatora użytkownika. Aby móc korzystać z podstawowego uwierzytelniania, każdy użytkownik musi mieć nadane prawo do logowania się lokalnie.

- ***Zintegrowane uwierzytelnianie systemu Windows (Windows Authentication)*** – uwierzytelnianie to zapewnia wyższy poziom bezpieczeństwa niż uwierzytelnianie podstawowe. Bardzo dobrze sprawdza się w środowisku intranetowym, w którym użytkownicy mają domenowe konta systemu Windows. W przypadku zintegrowanego uwierzytelniania systemu Windows przeglądarka w miarę możliwości używa bieżących poświadczeń użytkownika, które wcześniej były już używane do logowania się do domeny. Jeżeli nie powiedzie się użycie tych poświadczeń to wyświetlona zostanie odpowiednia informacja i użytkownik zostanie poproszony o podanie poprawnych danych logowania. Przy zintegrowanym uwierzytelnianiu systemu Windows, nie jest do serwera przesyłane hasło użytkownika. Jeżeli użytkownik został zalogowany do komputera jako użytkownik domeny, to próbując się dostać do sieciowego komputera w tej domenie, nie ma

konieczności ponownego uwierzytelniania.

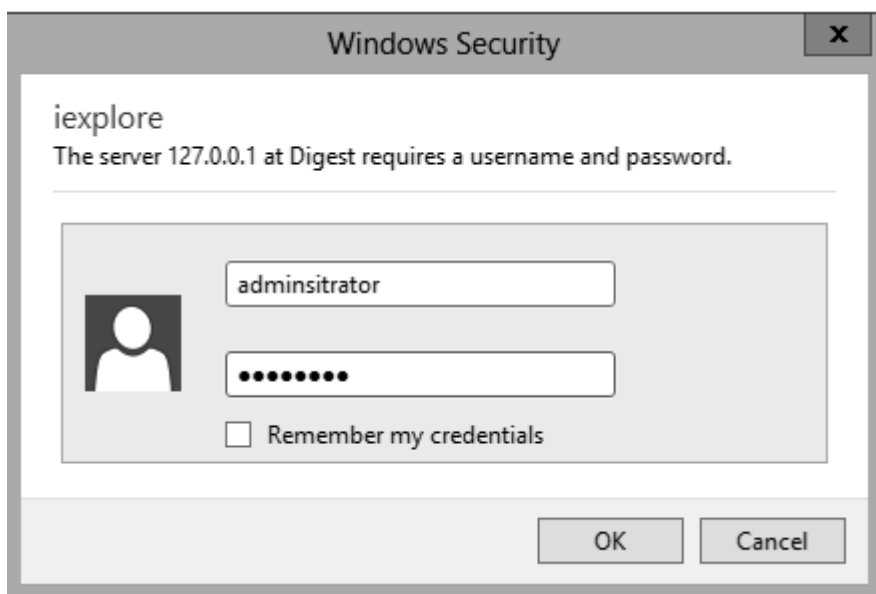
- **Uwierzytelnianie szyfrowane (Digest Authentication)** - eliminuje liczne wady uwierzytelnienia podstawowego. Podczas jego używania, uwierzytelnianie jest szyfrowane. W szyfrowanym uwierzytelnianiu używany jest mechanizm wezwania/odpowiedzi (identyczny mechanizm używany jest w zintegrowanym uwierzytelnianiu systemu Windows), a hasła są przesyłane w zaszyfrowanym formacie. Aby użyć uwierzytelniania szyfrowanego, koniecznością wszystkich kont użytkowników jest posiadanie odpowiedniej konfiguracji z włączoną opcją **Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego**. W momencie gdy została włączona ta opcja, należy zresetować lub wprowadzić ponownie hasło.

Zostanie wybrana jakaś metoda uwierzytelniania. Najlepsze będzie szyfrowanie. Zostanie więc ono włączone klikając **Włącz (Enabled)** po prawej stronie.

A screenshot of the 'Authentication' settings page in a web application. At the top left is a globe icon. The title 'Authentication' is centered. Below it is a 'Group by: No Grouping' dropdown menu. A table lists five authentication methods: Anonymous Authentication, ASP.NET Impersonation, Basic Authentication, Digest Authentication, and Windows Authentication. The 'Digest Authentication' row is highlighted with a dashed border. The 'Status' column shows 'Disabled' for the first four and 'Enabled' for Digest Authentication. The 'Response Type' column shows 'HTTP 401 Challenge' for the last three methods.

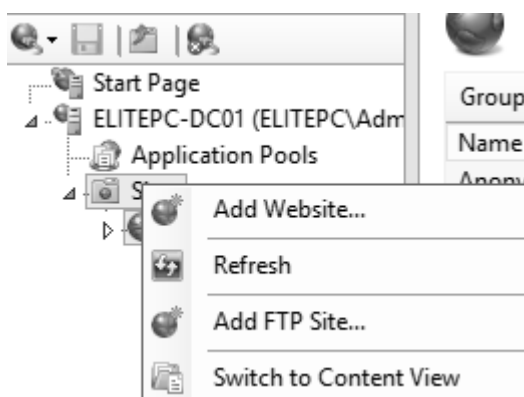
Group by: No Grouping ▾		
Name ▲	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Enabled	HTTP 401 Challenge
Windows Authentication	Disabled	HTTP 401 Challenge

Pojawi się ekran logowania po odświeżeniu strony. Należy wprowadzić swój login i hasło.



## 6.6. Uruchamianie Serwera FTP

Uruchomiony zostanie teraz serwer FTP, który także w dalszej części książki zostanie zabezpieczony. W tym celu należy kliknąć prawym przyciskiem myszy na napisie *Witryny (Site)* i dodać *Nową Witrynę FTP (Add FTP Site)*.



Na kolejnej karcie należy podać nazwę witryny oraz ścieżkę na dysku, gdzie będzie ona przechowywała swoje dane.



## Site Information

FTP site name:

Content Directory

Physical path:

Na kolejnej karcie pozostawione będą opcje domyślne.



## Binding and SSL Settings

Binding

IP Address:  Port:

☐ Enable Virtual Host Names:  
Virtual Host (example: ftp.contoso.com):

☒ Start FTP site automatically

SSL

☐ No SSL  
☐ Allow SSL  
☒ Require SSL

SSL Certificate:

Pozwolono też na *Uwierzytelnianie anonimowe (Anonymous)*.

Authentication

☒ Anonymous
   
☒ Basic

Authorization

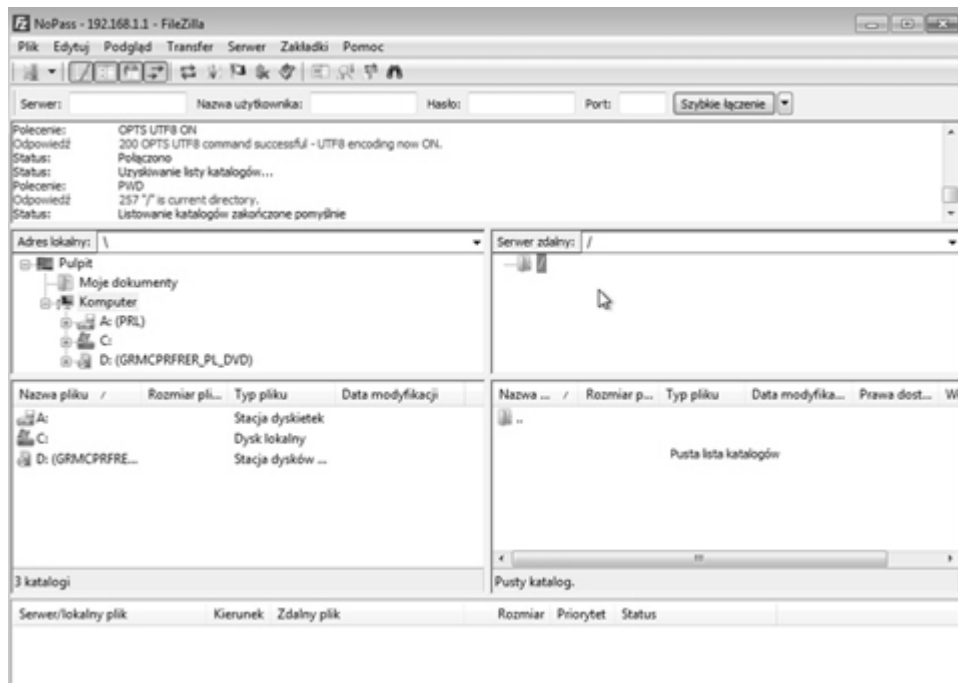
Allow access to:
   

All users

Permissions

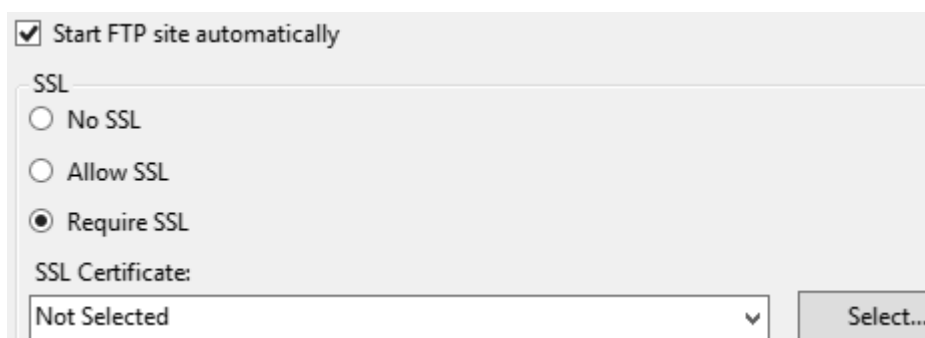
☒ Read
   
☒ Write

Do testów połączeń wykorzystany zostanie program FileZilla, zainstalowany na komputerze klienckim.

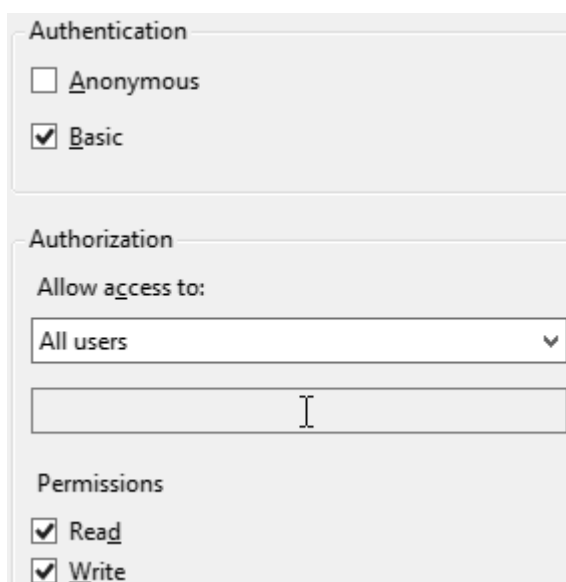


Warto także skupić się na zabezpieczeniu serwera FTP. Ponownie zostanie stworzony certyfikat z własnym podpisem tym razem dla serwera FTP.

Zostanie skasowana strona FTP, będzie trzeba przejść kreator raz jeszcze. Tym razem zostanie włączony certyfikat SSL i zaznaczony zostanie podany wcześniej certyfikat.



Uwierzytelnianie anonimowe nie jest pożądane, zostanie więc wyłączone.



Należy wejść w *Ustawienia SSL usługi FTP (FTP SSL Settings)*, wybrać *Wymagaj*



*połączeń SSL (Require SSL Connections) i zaznaczyć Szyfrowanie 128 bitowe (Use 128-bit encryption for SSL connections).*



## FTP SSL Settings

SSL Certificate:

WMSVC

SSL Policy

☐ Allow SSL connections

☒ Require SSL connections

☐ Custom

Advanced...

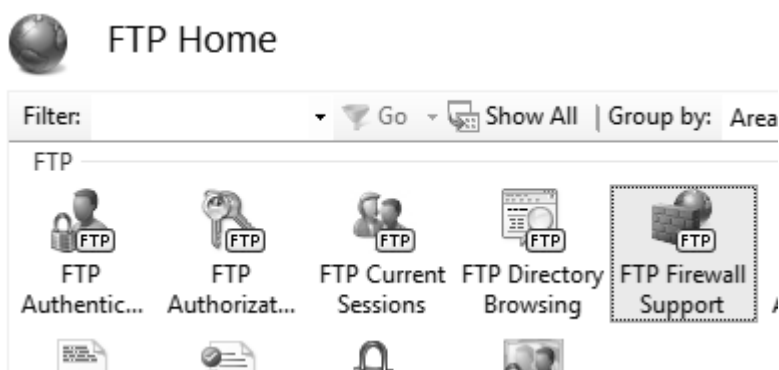
☒ Use 128-bit encryption for SSL connections

Klienta FTP konfiguruje się w następujący sposób:

Należy zaakceptować certyfikat i po chwili następuje bezpieczne połączenie z FTP.



To jednak nie wszystko, aby FTP działał poza siecią lokalną należy jeszcze skonfigurować Firewall. Należy znaleźć **Obsługę zapory FTP (FTP Firewall Support)**.



Należy skonfigurować tak, że adres IP to publiczny adres IP. Zakres portów, jaki należy ustawić to: 49152-65535. Gdyby pojawiły się problemy z routingiem czasami

pomogą konsolowe komendy:

#### **Dla FTP niezabezpieczonego:**

```
netsh advfirewall firewall add rule name="FTP (non-SSL)" action=allow  
protocol=TCP dir=in localport=21
```

```
netsh advfirewall set global StatefulFtp enable
```

#### **Dla zabezpieczonego SSL'em:**

```
netsh advfirewall firewall add rule name="FTP for IIS7" service=ftpsvc  
action=allow protocol=TCP dir=in
```

```
netsh advfirewall set global StatefulFtp disable
```

## **6.7. IIS i PHP**

We wcześniejszych działach został zainstalowany IIS oraz serwer FTP. Ten serwer jednak nie wspierał stron napisanych w języku PHP. Można to jednak łatwo zmienić.

PHP może funkcjonować przy użyciu protokołu ISAPI lub CGI. Wadą CGI jest to, że dla każdego żądania tworzony jest w systemie osobny proces, co przy wielu użytkownikach podłączonych jednocześnie w znacznym stopniu obciąża komputer. ISAPI jest wolne od tej wady, ponieważ wykorzystuje wewnętrzne procesy serwera IIS. Jego wadą jest to, że nie radzi on sobie z wielowątkowością, do której obsłużenia używa się bibliotek PHP, co znów prowadzi do utraty wydajności. Dlatego też w Windows Server 2008 Microsoft zaimplementował trzecie i najlepsze rozwiązanie FastCGI, zostało ono również przeniesione do Windows Server 2012.

Pierwszym krokiem instalacji będzie dodanie roli serwera IIS. Jako, że wcześniej

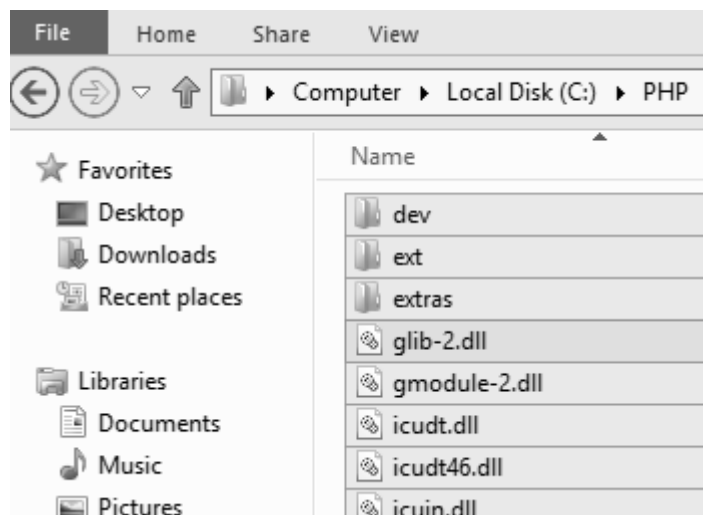
zostały już zainstalowane wszystkie możliwe komponenty ten krok można pominąć. Jeżeli jednak zaczyna się od początku należy zaznaczyć Serwer Sieci Web i kliknąć Dalej (Next).

Na kolejnych kartach należy zaznaczyć opcję CGI. FastCGI nie jest osobnym elementem, lecz modulem zawartym w najnowszej wersji CGI.

Należy także pobrać PHP ze strony PHP.net, polecić można wersję non-thread-safe, ponieważ jest lepiej zoptymalizowana pod kątem wielowątkowości.



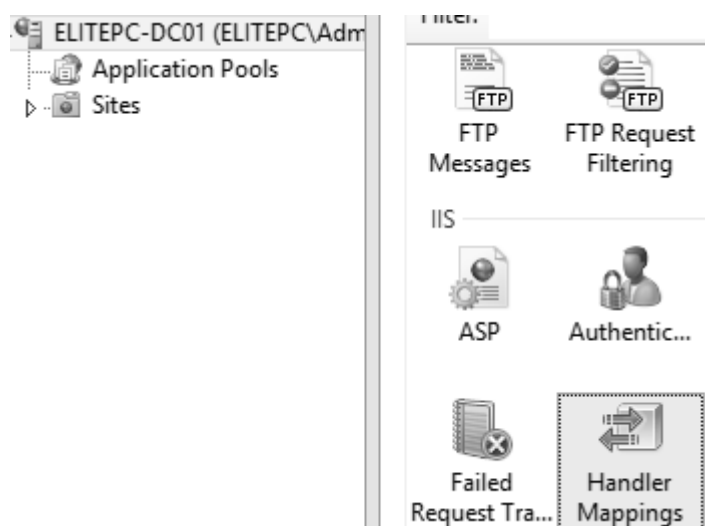
Należy rozpakować zawartość archiwum ZIP do katalogu PHP umieszczonego na dysku C.



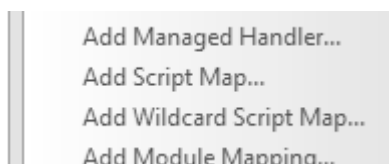
Należy zmienić rozszerzenie pliku ze zdjęcia na \*.ini



W Menadżerze IIS należy wybrać **Mapowania Obsługi (Handler Mappings)**, przy zaznaczonym serwerze w menu po lewej stronie.



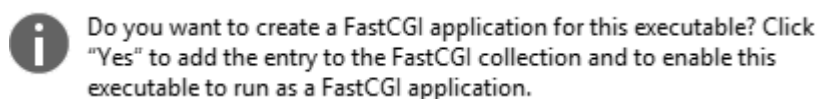
Następnie należy kliknąć w menu po prawej stronie na ***Dodaj Mapowanie Modułu (Add Module Mapping)***.



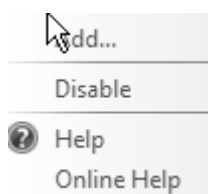
Planszę, która się pojawi należy wypełnić tak, jak na poniższym zrzucie z ekranu:

Request path:	
<input type="text" value="*.php"/>	
Example: *.bas, wsvc.axd	
Module:	
<input type="text" value="FastCgiModule"/>	
Executable (optional):	
<input type="text" value="C:\PHP\php-cgi.exe"/>	<input type="button" value="..."/>
Name:	
<input type="text" value="PHP"/>	

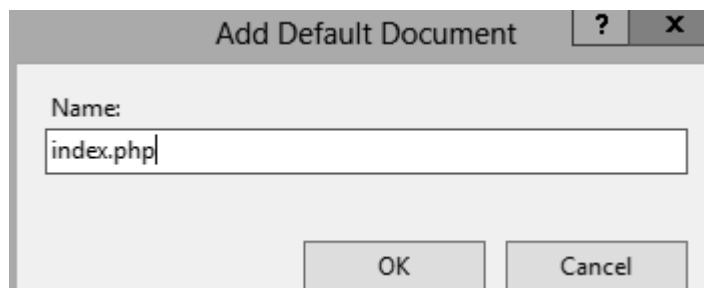
Należy kliknąć **OK**, a komunikat, który się pojawi należy potwierdzić przyciskiem **Tak (Yes)**.



W menu po prawej stronie należy kliknąć **Dodaj (Add...)**.



Aby strony napisane języku PHP prawidłowo się wczytywały należy także dodać domyślny dokument o nazwie index.php



Gdy dokument zostanie już dopisany do listy, aby strona w języku PHP była wczytywana jako pierwsza powinno się ustawić jej priorytet na najwyższy ustawiając ją na szczycie listy domyślnych dokumentów.

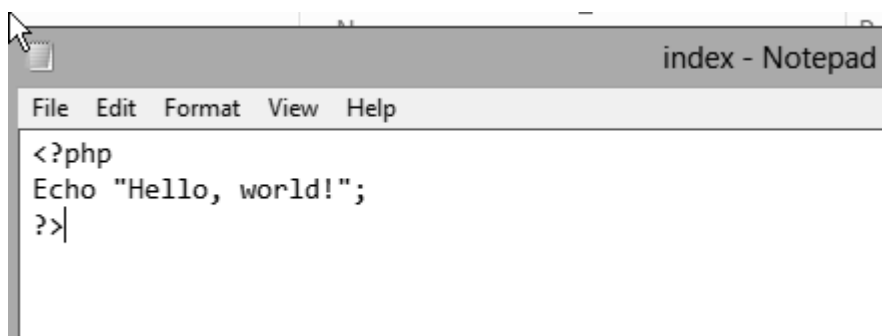


## Default Document

Use this feature to specify the default file(s) to return w documents in order of priority.

Name	Entry Type
index.php	Local
Default.htm	Local
Default.asp	Local
index.htm	Local
index.html	Local

Następnie należy otworzyć notatnik i stworzyć bardzo prostą stronę www, a także zapisać ją w katalogu C:\inetpub\wwwroot\ jako index.php



Następnie trzeba zresetować serwer, a po jego ponownym rozruchu sprawdzić czy strona działa.

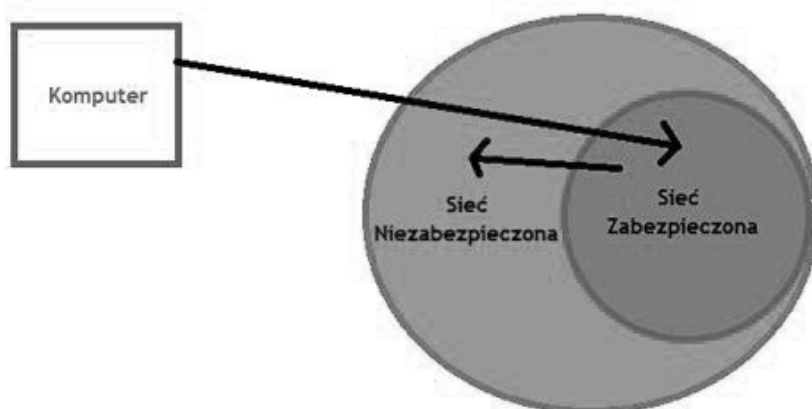




## 7. Network Access Protection

Jedną z nowości wprowadzonych do Windows Server 2008 był Network Access Protection (NAP), służący do zwiększenia bezpieczeństwa sieci. Pozwala on przeskanować zdalnie komputery i tym, które nie spełniają norm bezpieczeństwa zabronić połączenia się z siecią. Schemat działania tego systemu przedstawia diagram poniżej. Ta sama funkcjonalność znajduje się także w Windows Server 2012.

### 7.1. Network Policy and Access Services

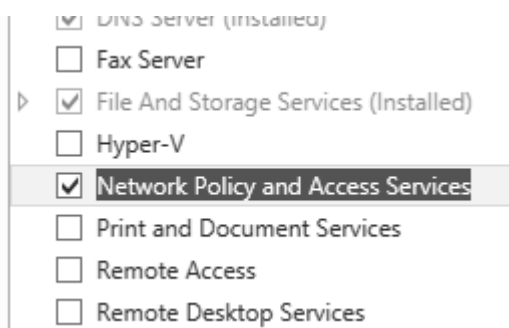


Zewnętrzny okrąg przedstawia niezabezpieczoną sieć firmową. Wewnętrzny okrąg natomiast pokazuje fragment sieci, w której działają tylko i wyłącznie komputery spełniające normy bezpieczeństwa. Maszyna spoza sieci, która próbuje uzyskać dostęp do zasobów kontaktuje się z serwerem w sieci zabezpieczonej. Jeżeli spełniła ona warunki, czyli np. ma zainstalowany aktualny program antywirusowy oraz najnowsze aktualizacje bezpieczeństwa, nie będzie stanowiło problemu przyłączenie komputera do sieci. W przeciwnym wypadku maszyna zostanie prze delegowana do komputerów w sektorze niezabezpieczonym, gdzie będzie mogła uzyskać dostęp do witryny WWW z pomocą, czy też niezbędnych aktualizacji lub programów.

Należy skonfigurować taką polisę dla każdego rodzaju połączenia. W ramach tej publikacji posłużono się przykładem konfiguracji dla klientów DHCP. Uruchomiono także routing, aby komputery z sieci lokalnej miały dostęp do Internetu, jak również zapewniono zdalny dostęp do komputerów firmowych spoza siedziby za pośrednictwem bezpiecznego połączenia VPN.

Filter:	Go	Show All	Group by: No Grouping
Name	Issued To	Issued By	
Certyfikat IIS IIS	ELITEPC-DC01.elitepc.pl	elitepc-ELITEP	
	elitepc-ELITEPC-DC01-CA	elitepc-ELITEP	
	ElitePC Certyfikat IIS	elitepc-ELITEP	
	ELITEPC-DC01.elitepc.pl	ELITEPC-DC01	
SSTP	SSTP	elitepc-ELITEP	
WMSVC	WMSvc-ELITEPC-DC01	WMSvc-ELITE	

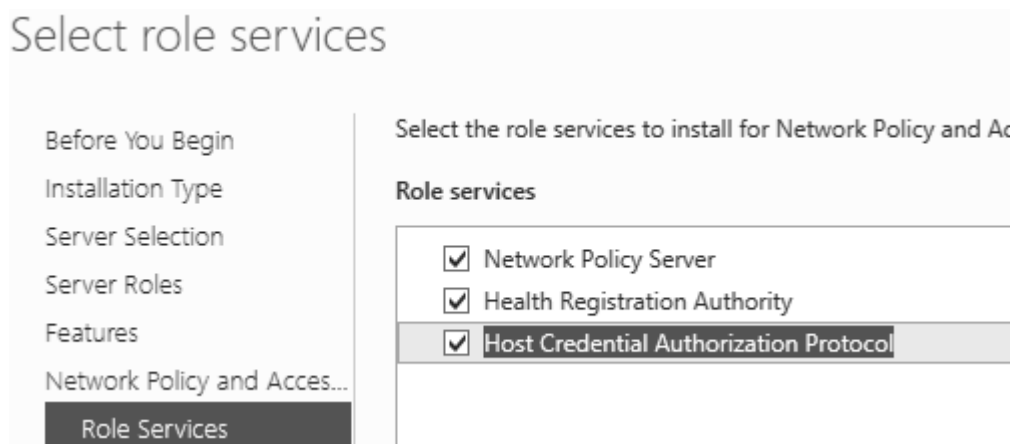
Następnie należy zainstalować rolę *Usługi Zasad i Dostępu Sieciowego (Network Policy and Access Services)* i wybór zatwierdzić klikając przycisk *Dalej (Next)*.



Na kolejnej planszy należy kliknąć *Dalej (Next)*.



W ramach roli można zainstalować wszystkie usługi, ponieważ prędzej czy później okażą się one przydatne. Trzeba kliknąć **Dalej (Next)**.



Jeżeli na komputerze nie ma jeszcze urzędu certyfikacji, teraz jest dobry moment by go zainstalować. Jeżeli urząd już jest należy wybrać go z listy. Można wybrać także opcję ze zrzutu ekranu, czyli skorzystanie z lokalnego CA.

Health Registration Authority (HRA) requires that at least one Certification Authority (CA) be associated with it.

- ☒ Use the local CA to issue health certificates for this HRA server.

There is an existing CA on this computer. If you choose to use it, it will be dedicated to issuing health certificates.

- ☐ Use an existing remote CA.

If you choose to use an existing CA it should be one dedicated to issuing health certificates.

- ☐ Select a CA later using the HRA console.



You will not be able to issue health certificates to NAP client computers until this CA is configured.

Dla większego bezpieczeństwa powinno się wymagać, aby *Użytkownicy uwierzytniali się jako członkowie domeny (Yes, require requestors to be authenticated as members of a domain)*.

Health Registration Authority can be configured to ensure that only users authenticated to the domain can get health certificates.

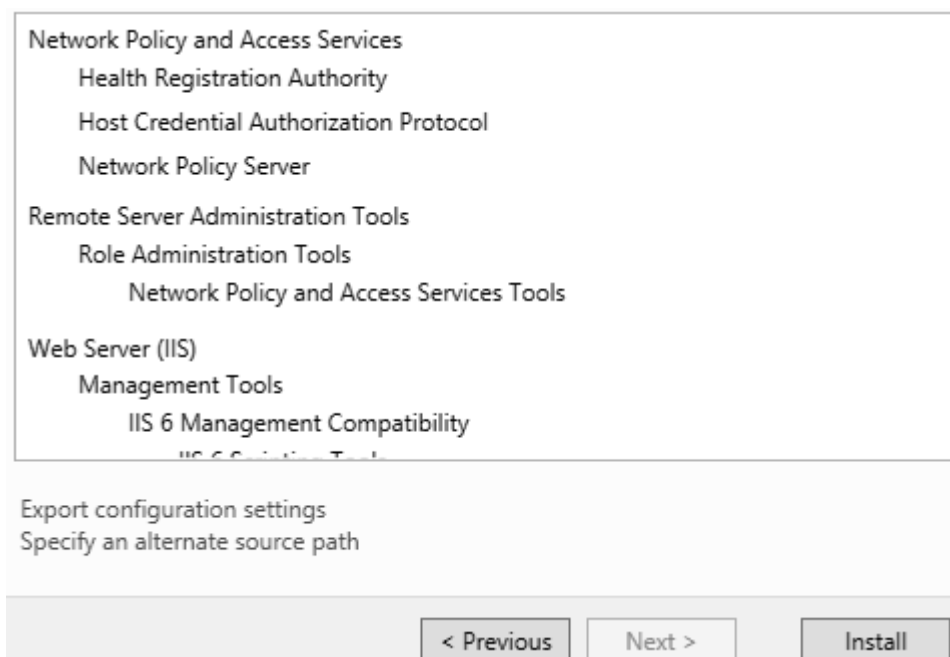
Do you want to require that users be authenticated in order to get a health certificate?

- ☒ Yes, require requestors to be authenticated as members of a domain. (recommended)

This option is only available when the computer is joined to a domain.

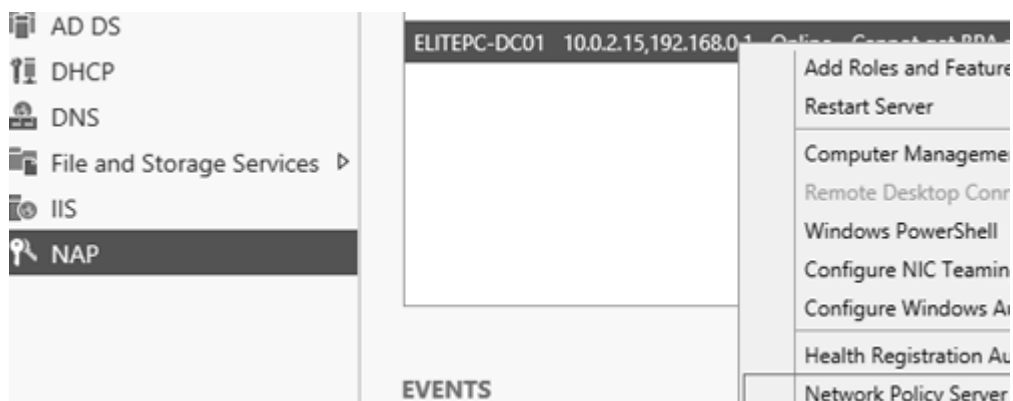
- ☐ No, allow anonymous requests for health certificates.

Na karcie podsumowującej należy kliknąć *Zainstaluj (Install)*.



## 7.2. Zarządzanie Network Policy Server

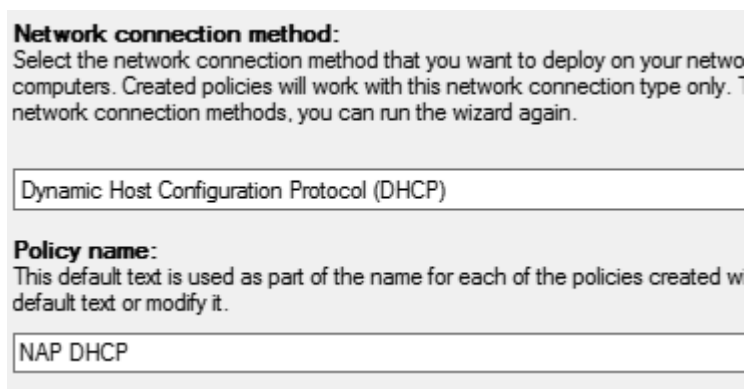
W *Menadżerze Serwera (Server Manager)* znajduje się serwer zasad sieciowych NAP. Należy wybrać opcję *Serwer Zasad Sieciowych (Network Policy Server)* znajdującą się pod prawym przyciskiem myszy.



Po jego uruchomieniu można skorzystać z kreatora klikając napis *Konfiguruj Ochronę Dostępu do Sieci (Configure NAP)*.



Na pierwszej karcie kreatora należy wybrać metodę połączenia sieciowego, w tym przypadku będzie to **DHCP (Dynamic Host Configuration Protocol)**, a także określić **nazwę dla polity (Policy name)** i kliknąć przycisk **Dalej (Next)**.



Jeśli w sieci nie istnieje Serwer Radius, należy w kreatorze przejść do następnego kroku klikając przycisk **Dalej (Next)**.

RADIUS clients are network access servers, not client computers. If the local computer is running DHCP Server, you can skip this step and click Next.

If you want to add remote DHCP servers as RADIUS clients, click Add. All remote DHCP servers that add must also run NPS. Also, remote DHCP/NPS servers must forward connection requests to this NPS server (the local computer).

**RADIUS clients:**

	Add...
	Edit...
	Remove

Pragnąc uruchomić osłonę tylko dla wybranego zakresu (karty sieciowej itp.) należy kliknąć przycisk **Dodaj (Add)**, zaś chcąc uruchomić ją dla wszystkich zakresów trzeba pozostawić kartę pustą i kliknąć **Dalej (Next)**.

When you specify one or more NAP-enabled scopes, NPS evaluates client health and performs authorization for client computers requesting an IP address from the designated scopes.

If you do not specify any scopes, the policy applies to all NAP-enabled scopes at the selected DHCP server. If you specify a scope that is not NAP-enabled, you must enable NAP for the scope after completing this wizard.

To specify one or more scopes, click Add.

**DHCP scopes:**

	Add...
	Edit...
	Remove

Na następnej karcie można wybrać konkretne grupy komputerów lub pozostawić pole puste.

To grant or deny access to groups of computers, add groups to Machine Groups.

If no groups are selected, this policy applies to all users.

**Machine Groups:**

Add...  
Remove...

Konkretnych zmian można dokonać na kolejnej karcie. Można tutaj skonfigurować serwery, do których użytkownik zostanie oddelegowany, jeżeli nie spełni wszystkich norm bezpieczeństwa. W tym celu należy kliknąć ***Nowa Grupa (New Group)***.

**Remediation Server Group:**  
Remediation servers store software updates for NAP clients that need them. Remediation Server Groups contain one or more remediation servers.

Select a Remediation Server Group that you have already configured or, to create a new group, click New Group.

<none>

New Group...

**Troubleshooting URL:**  
If you have a Web page that provides users with instructions to users on how to bring computers and devices in compliance with NAP health policy, type the Uniform Resource Locator (URL) for the Web page.

If you do not have a Help Web page, do not type a URL.

http://

W kolejnym oknie trzeba wprowadzić nazwę grupy oraz komputery, które znajdują się w sieci niezabezpieczonej i udostępniają niezbędne oprogramowanie i aktualizacje.



**Add New Server**

Friendly name:

IP address or DNS name:

To use an IP address to identify the server, select one from the following list

IP address:

Można także wprowadzić adres strony internetowej, na której zostanie umieszczona np. instrukcja dla użytkowników.

**Troubleshooting URL:**  
 If you have a Web page that provides users with instructions to users on how compliance with NAP health policy, type the Uniform Resource Locator (URL)

If you do not have a Help Web page, do not type a URL.

Kolejną kartę należy skonfigurować według schematu przedstawionego na zdjęciu w celu odcięcia komputerów nie spełniających norm bezpieczeństwa od sieci. Służy ku temu opcja **Odmów pełnego dostępu do sieci NAP niekwalifikowalnym komputerom klienckim** (*Deny full network access to NAP – ineligible client computers*). Pragnąc jedynie monitorować komputery nie spełniające norm bezpieczeństwa należy wybrać opcję **Pozwól na pełen dostęp do sieci NAP niekwalifikowalnym komputerom klienckim** (*Allow full network access to NAP –*

*ineligible client computers).*

The installed System Health Validators are listed below. Select only the System Health Validators that you enforce with this health policy.

Name
<input checked="" type="checkbox"/> Windows Security Health Validator

☒ Enable auto-remediation of client computers

If selected, NAP-capable client computers that are denied full access to the network because they are compliant with health policy can obtain software updates from remediation servers.

If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot full network access until they are manually updated.

**Network access restrictions for NAP-ineligible client computers:**

☒ Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only

☐ Allow full network access to NAP-ineligible client computers.

Po przeczytaniu podsumowania trzeba kliknąć **Zakończ (Finish)**.

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

**Health Policies:**

NAP DHCP Compliant  
NAP DHCP Noncompliant

**Connection Request Policy:**

NAP DHCP

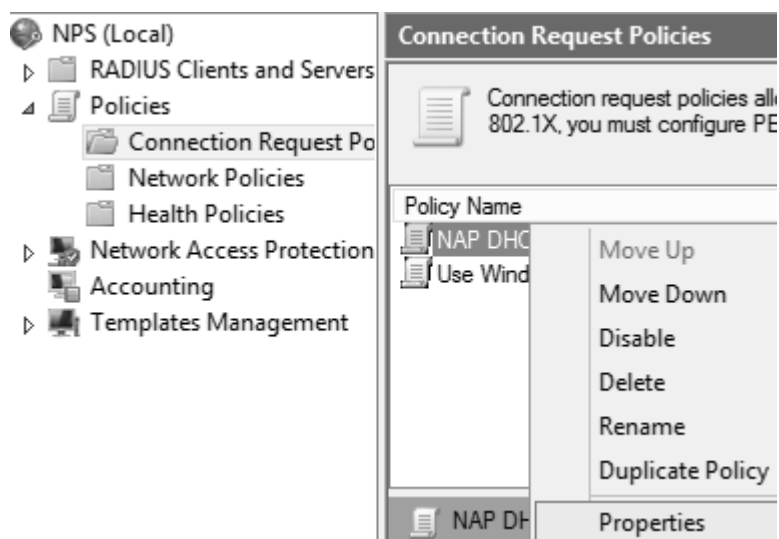
**Network Policies:**

NAP DHCP Compliant  
NAP DHCP Noncompliant  
NAP DHCP Non NAP-Capable

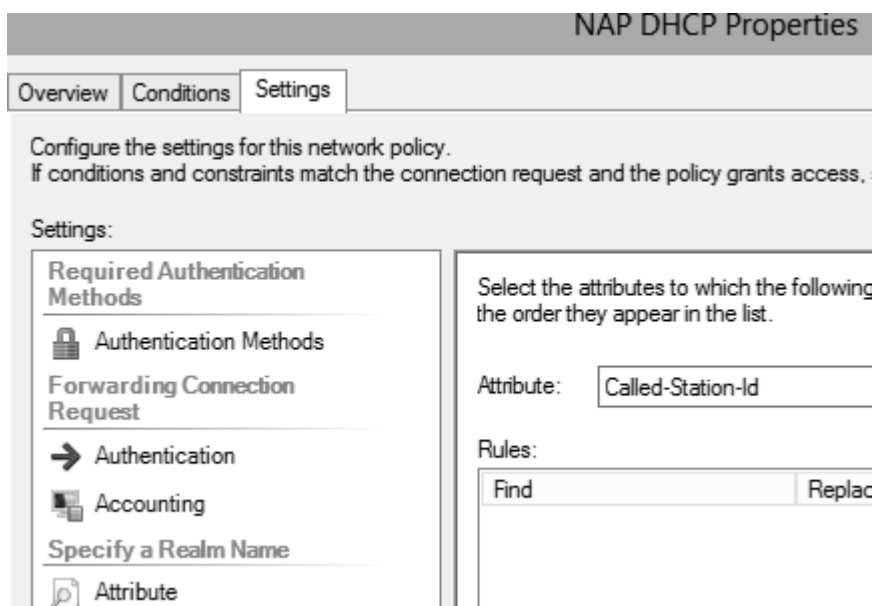
**Remediation Server Group:**

Poza siecia wew.

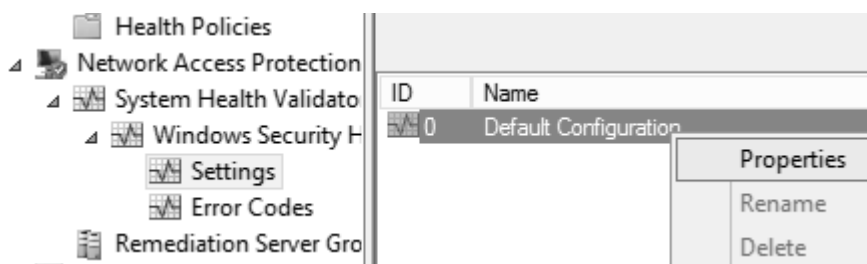
W sekcji **Zasady (Policies)/Zasady żądań połączeń (Connection request Policies)** pojawiła się wcześniej ustawiona zasada, klikając na niej prawym guzikiem należy wejść w jej **Właściwości (Properties)**.



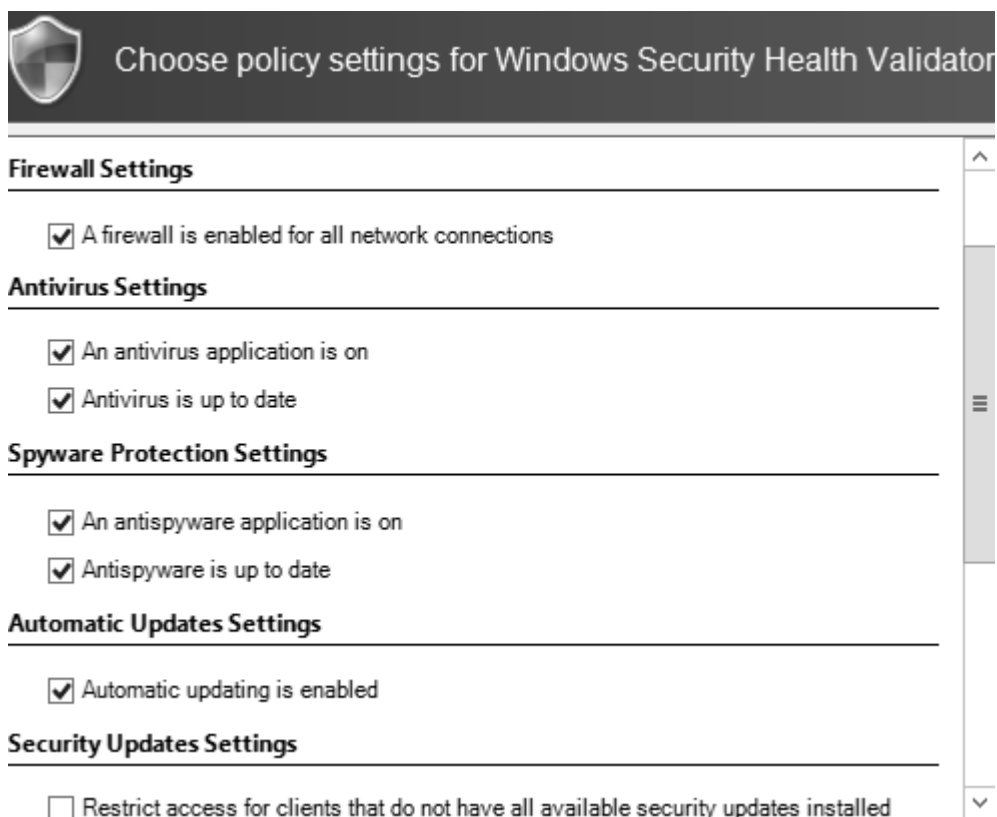
Można w nich konfigurować różne opcje związane z połączeniem czy dostępem.



W ustawieniach *Modułu Sprawdzania Kondycji (Windows Security Health)* znajduje się konfiguracja domyślna, należy wybrać jej *Właściwości (Properties)*.

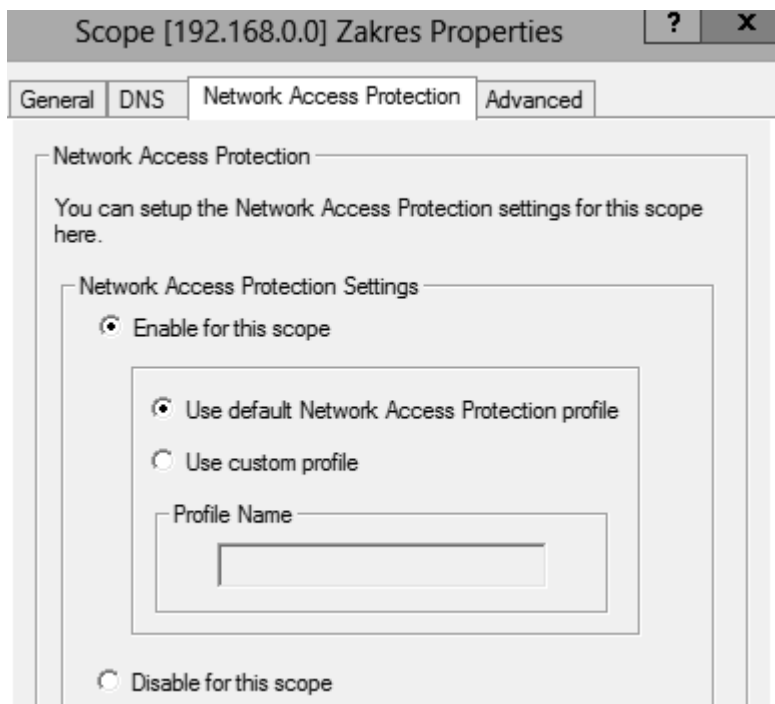


W oknie, które się pojawi można ustalić jakie aspekty komputerów klienckich są sprawdzane. Do wyboru jest Firewall, AV, Antispyware (Windows Defender), a także Update.



Skoro NAP jest już skonfigurowany należy zmusić serwer DHCP do jego używania.

W tym celu koniecznym jest wejście we właściwości zakresu, do zakładki ***Ochrona Dostępu Do Sieci (Network Access Protection)*** oraz wybranie opcji ***Włącz ochronę dla tego zakresu (Enable for this scope)***, a następnie ***Użyj domyślnego profilu ochrony dostępu do sieci (Use Default Network Access Protection Profile)***.

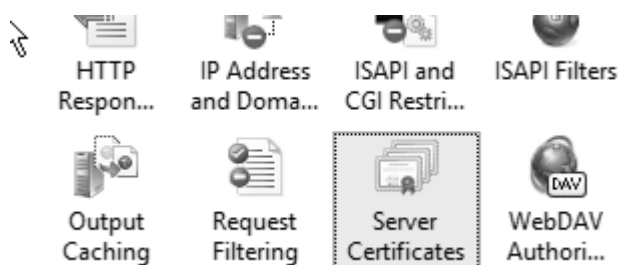


## 8. VPN, Direct Access i NAT

Funkcje VPN i Direct Access zapewniają użytkownikowi spoza domeny swobodną pracę z wykorzystaniem zasobów wewnątrz firmy. Z kolei NAT uruchamia translację adresów sieciowych, czyli w przypadku, gdy bramką sieciową jest Windows Server, NAT pozwala na połączenie komputerów wewnątrz sieci z siecią zewnętrzną.

### 8.1. Instalacja roli Remote Access

Zostanie teraz skonfigurowane połączenie VPN typu SSTP, czyli szyfrowane z certyfikatem, które jest znacznie bezpieczniejsze od PPTP. Pierwszym najważniejszym krokiem będzie więc zainstalowanie certyfikatu. Bardzo ważnym jest, aby zrobić to przed instalacją Routingu. W przeciwnym wypadku nie osiągnie się celu. Wymagana będzie instalacja wcześniej roli IIS. Aby tego dokonać należy wejść do Menadżera IIS i kliknąć dwukrotnie w *Certyfikaty Serwera (Server Certificates)*.



Następnie należy wybrać opcję Utwórz Certyfikat Domeny. Pojawi się kreator, w którym pierwszą planszę trzeba wypełnić wedle uznania, gdyż są to tylko nieznaczające informacje i wcisnąć przycisk *Dalej (Next)*.

Specify the required information for the certificate. State/province and official names and they cannot contain abbreviations.

Common name:	SSTP
Organization:	ElitePC
Organizational unit:	WAW
City/locality	Warsaw
State/province:	MZ
Country/region:	PL

Na kolejnej planszy należy kliknąć przycisk **Wybierz (Choose)** i z listy wybrać serwer, na którym zainstalowany jest główny urząd certyfikacji.

Select a certificate authority you want to use:

Certificate Authority	Computer
elitepc-ELITEPC-DC01-CA	ELITEPC-DC01.elitepc.pl

Należy nazwać wprowadzony certyfikat, dlatego powinno się wypełnić pole dotyczące jego **Przyjaznej nazwy (Friendly name)**, a następnie kliknąć w przycisk **Zakończ (Finish)**.

Specify the certification authority within your domain that will sign the certificate, and should be easy to remember.

Specify Online Certification Authority:

elitepc-ELITEPC-DC01-CA\ELITEPC-DC01.elitepc.pl

Example: CertificateAuthorityName\ServerName

Friendly name:

SSTP

Certyfikat pojawi się na liście. Można teraz przystąpić do instalacji. W **Menadźerze Serwera (Server Manager)** należy dodać rolę **Zdalny Dostęp (Remote Access)**.

## Select server roles

Before You Begin	Select one or more roles to install on the selected server.
Installation Type	
Server Selection	
<b>Server Roles</b>	<b>Roles</b>
Features	<input type="checkbox"/> Active Directory Rights Management Services
Remote Access	<input type="checkbox"/> Application Server
Role Services	<input checked="" type="checkbox"/> DHCP Server (Installed)
Confirmation	<input checked="" type="checkbox"/> DNS Server (Installed)
Results	<input type="checkbox"/> Fax Server
	▶ <input checked="" type="checkbox"/> File And Storage Services (Installed)
	<input type="checkbox"/> Hyper-V
	▶ <input checked="" type="checkbox"/> Network Policy and Access Services (Installed)
	<input type="checkbox"/> Print and Document Services
	<input checked="" type="checkbox"/> <b>Remote Access</b>
	<input type="checkbox"/> Remote Desktop Services

Należy pamiętać o tym, iż w przypadku Windows Server, VPN jest nierozzerwalny z Routingiem (RRAS). W Windows Server 2008 usługi, które są omawiane były włączone do roli NAP, w Windows Server 2012 zostały rozdzielone. W czasie instalacji konieczne jest kliknięcie przycisku **Dalej (Next)** na karcie powitalnej.

## Remote Access

Before You Begin	Remote Access combines DirectAccess and RRAS.
Installation Type	
Server Selection	
Server Roles	
Features	Deploy DirectAccess to allow managed domain-joined client computers to connect to the corporate network as DirectAccess clients. Connectivity is secured by IPsec. DirectAccess ensures that mobile computers are kept up-to-date with the latest security requirements.
<b>Remote Access</b>	Deploy VPN to allow client computers running operating systems configured in a workgroup, to remotely access corporate resources.
Role Services	
Confirmation	



W kolejnym oknie można zainstalować DirectAccess i VPN, które są ze sobą połączone, jak również Routing, dzięki któremu będzie możliwe udostępnienie Internetu stacjom klienckim poprzez protokół IPv4.

Warto więc wybrać wszystkie opcje. Wymagane będą także pojedyncze komponenty serwera IIS, które także należy zainstalować, jeżeli to wcześniej nie zostało wykonane. Jeżeli natomiast jest już zainstalowany IIS to można przejść od razu do podsumowania i kliknąć **Zainstaluj (Install)**.

To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because been selected automatically. If you do not want to install these optional features, click Pre their check boxes.

RAS Connection Manager Administration Kit (CMAK)

Remote Access

- DirectAccess and VPN (RAS)
- Routing

Remote Server Administration Tools

- Role Administration Tools
  - Remote Access Management Tools
    - Remote Access GUI and Command-Line Tools
    - Remote Access module for Windows PowerShell

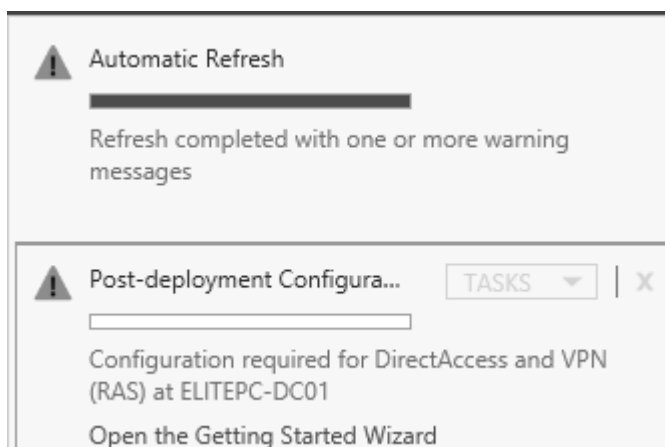
Windows Internal Database

Export configuration settings  
Specify an alternate source path

< Previous      Next >      Install

## 8.2. Konfiguracja VPN i NAT

Po zakończeniu instalacji, z poziomu *Centrum Akcji (Action Center)* należy uruchomić konfigurację zainstalowanej roli.



Do wyboru są trzy opcje. Konfiguracja serwera VPN i Direct Access jednocześnie, bądź jedynie wybranego z nich. W przykładzie zostanie skonfigurowany na razie tylko VPN, ponieważ jest to proces analogiczny względem wcześniejszych wersji systemu Windows Server.

### Deploy both DirectAccess and VPN (recommended)

Configure DirectAccess and VPN on the server, and enable DirectAccess client computers. Allow remote client computers not supported for DirectAccess to connect over VPN.

### Deploy DirectAccess only

Configure DirectAccess on the server, and enable DirectAccess client computers.

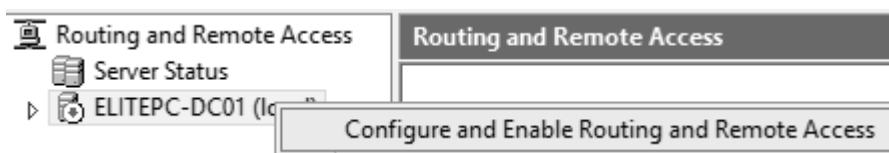
### Deploy VPN only

Configure VPN using the Routing and Remote Access console. Remote client computers can connect over VPN, and multiple sites can be connected using VPN site-to-site connections. VPN can be used by clients not supported for DirectAccess.

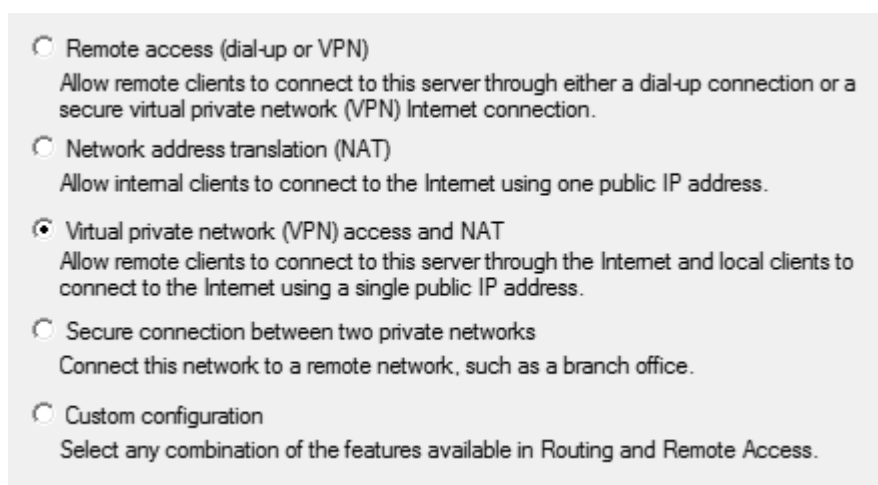
Po kliknięciu trzeciej opcji pojawi się znana administratorom z Windows Server

2003 i 2008 konsola **Routing i Dostęp Zdalny (Routing and Remote Access)**.

Należy kliknąć prawym guzikiem myszy na nazwie komputera i wybrać opcję **Konfiguruj i Włącz Routing i Dostęp Zdalny (Configure and Enable Routing and Remote Access)**.



Następnie należy kliknąć **Dostęp prywatnej sieci wirtualnej i translator adresów sieciowych (Virtual private network (VPN) access and NAT)**, a potem przycisk **Dalej (Next)**.



Należy wybrać interfejs sieciowy, który będzie łączył z Internetem.

Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
Ethemet	Intel(R) PRO/1000 MT ...	10.0.2.15 (DHCP)
Ethemet 2	Intel(R) PRO/1000 MT ...	192.168.0.1

Przypisywanie adresów można wybrać ***Automatyczne (Automatically)***, ponieważ w sieci jest już skonfigurowany serwer DHCP, więc nie ma konieczności używania serwera DHCP wbudowanego w RRAS.

### IP Address Assignment

You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

☒ Automatically  
If you use a DHCP server to assign addresses, confirm that it is configured properly.  
If you do not use a DHCP server, this server will generate the addresses.

☐ From a specified range of addresses

W sieci testowej nie ma serwera Radius, dlatego też należy wybrać opcję pierwszą.

Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.

If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.

Do you want to set up this server to work with a RADIUS server?

☒ No, use Routing and Remote Access to authenticate connection requests

☐ Yes, set up this server to work with a RADIUS server

Na karcie z podsumowaniem należy wybrać ***Zakończ (Finish)***.

## ❖ Completing the Routing and Remote Access Server Setup Wizard

You have successfully completed the Routing and Remote Access Server Setup Wizard.

Summary:

VPN clients connect to the following public interface: Ethernet	^ ≡ v
RAS and VPN clients are assigned the following network for addressing: Ethernet 2.	
Client connections are accepted and authenticated	

Before clients can connect, user accounts must be added locally or through Active Directory. For more information about user accounts, see [Routing and Remote Access Help](#).

To close this wizard, click Finish.

Pojawią się dwa komunikaty. Oba należy zatwierdzić przyciskiem **OK**.



Remote Access Service is unable to enable Routing and Remote Access for the probable reason like: unable to open ports for Routing and Remote Access in Windows Firewall service. In this case RAS may not accept vpn connections.

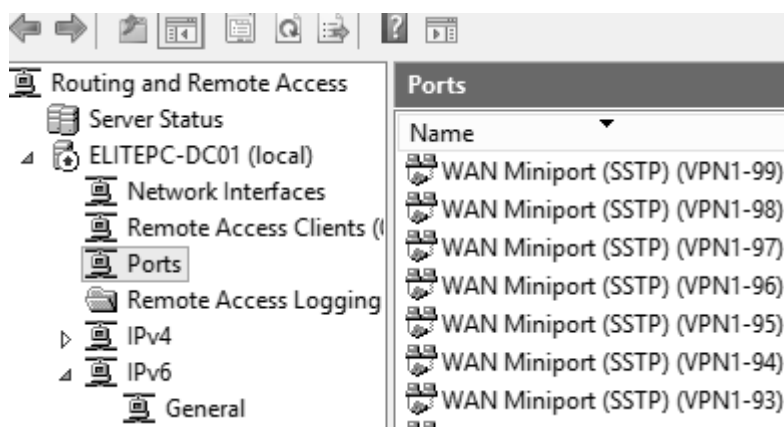
User Action: Manually open the port of Routing and Remote Access in the windows firewall.

To support the relaying of DHCP messages from remote access clients, you must configure the properties of the DHCP Relay Agent with the IP address of your DHCP server. Click Help for more information.

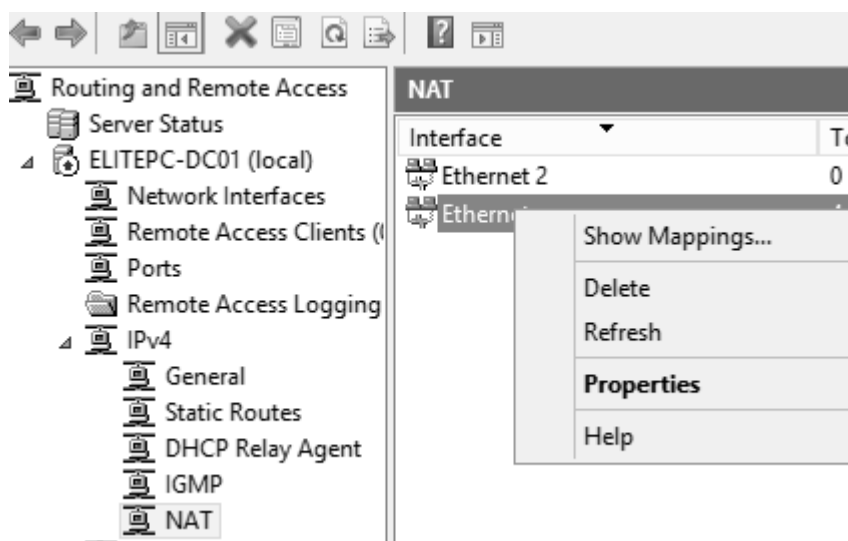
OK

Help

Po chwili oczekiwania, jeżeli wszystko się powiedzie, w sekcji **Porty (Ports)** zostaną utworzone mini porty SSTP.



Konieczne jest jeszcze odblokowanie w *zaporze systemowej (Firewallu)* portu 80, aby klienci mogli odbierać certyfikat. Na połączeniu WAN należy więc kliknąć prawym klawiszem myszy i wybrać *Właściwości (Properties)*.



Następnie należy wejść w zakładkę *Usługi i Porty (Services and Ports)* i zaznaczyć *Serwer WWW (Web Server)*, a jako adres prywatny podać *Localhost* i kliknąć *OK*.



Designate the port and address to which packets should be sent when they arrive on a special port on this interface's address or on a specific address pool entry.

Description of Service:

Web Server (HTTP)

Public address

☒ On this interface

☐ On this address pool entry: . . .

Protocol

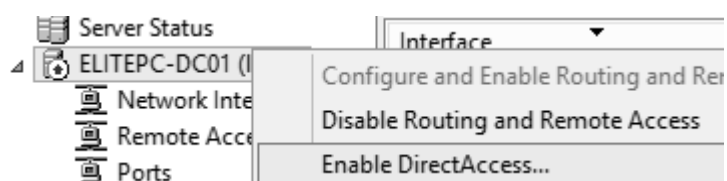
☒ TCP ☐ UDP

Incoming port: 80

Private address: 127 . 0 . 0 . 1

Outgoing port: 80

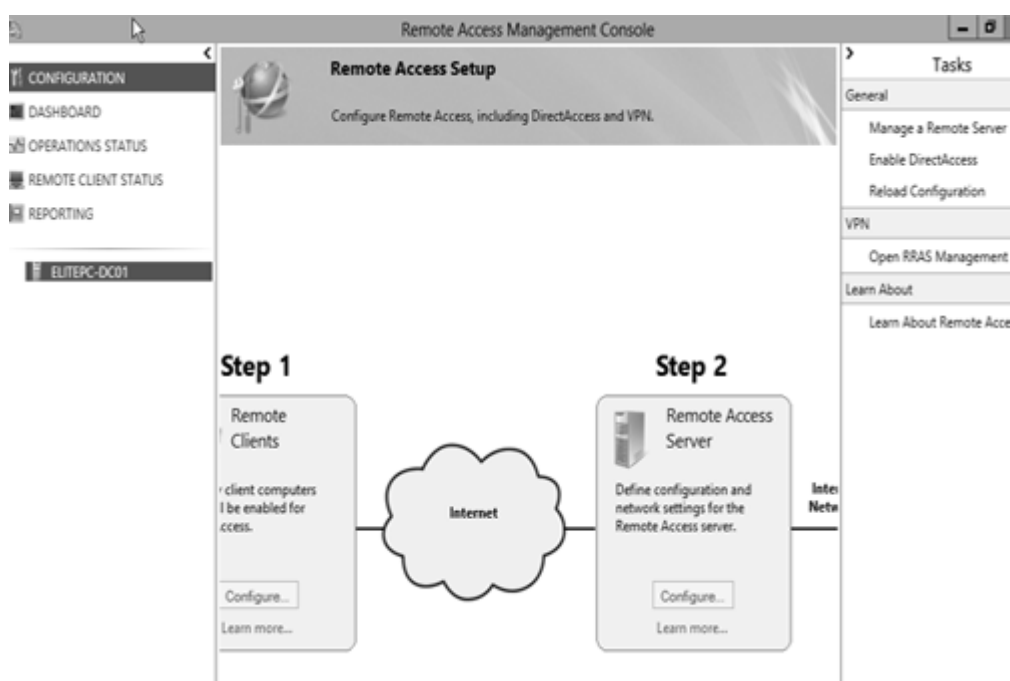
Nowością względem starszych wersji systemu Windows Serwer jest przycisk umożliwiający uruchomienie *Zdalnego Dostępu (Direct Access)* z poziomu menu kontekstowego serwera RRAS.



Warto teraz zajrzeć do *Menadżera Serwera (Server Manager)*, gdzie również pojawił się *Zdalny Dostęp (Remote Access)*. Po wybraniu serwera istnieje możliwość uruchomienia konsoli *Menadżer Zdalnego Dostępu (Remote Access Management)*.



W sekcji **Konfiguracja (Configuration)** znajduje się schemat przedstawiający działanie roli. Za pomocą przycisku **Konfiguruj (Configure)** można w każdej chwili przejść do konfiguracji danego elementu. W menu po prawej stronie okna znajduje się także przycisk **Uruchom DirectAccess (Enable DirectAccess)**.



W sekcji **Dashboard** znajduje się podgląd na działanie serwera RRAS. W menu po prawej stronie znajdują się cztery opcje: **Odśwież (Refresh)**, służąca do odświeżania



widoku, **Konfiguruj harmonogram odświeżania (Configure Refresh Interval)**, która tworzy harmonogram odświeżania, **Włącz śledzenie (Start Tracing)**, która włącza zaawansowane śledzenie oraz **Generuj raport użycia (Generate Usage Report)**, która generuje raport z działania użytkowników zdalnych.

Tasks
Monitoring
Refresh
Configure Refresh Interval
Start Tracing
Generate Usage Report
Learn About
Learn About Remote Access

Na poziomie **Stan klientów zdalnych (Remote Clients Status)** istnieje możliwość wglądu do obecnej aktywności użytkowników zdalnych oraz możliwość rozłączenia danego klienta opcją **Odlącz klienta VPN (Disconnect VPN Client)**.

Refresh
Configure Refresh Interval
Disconnect VPN Clients
Learn About
Learn About Remote Access

Pod **Raportowanie (Reporting)** kryją się opcje dotyczące raportowania, które domyślnie nie są skonfigurowane. W celu ćwiczeniowym, aby skonfigurować raportowanie należy kliknąć odnośnik **Konfiguruj Raportowanie (Configure Accounting)**.

## Remote Access Reporting



Inbox accounting must be configured before reporting can be used.

[Configure Accounting](#)

Po wybraniu dogodnych opcji należy kliknąć **Zastosuj (Apply)**.

### Configure Accounting

Configure accounting settings for Remote Access data logging.

Configure settings for Remote Access accounting.

#### Select Accounting Method

☒ Use RADIUS accounting

Select this setting to store logs and generate reports using a local or remote RADIUS server.

☒ Use inbox accounting

Select this setting to store logs using the Windows Internal Database (WID) and generate reports on this server.

#### Configure Accounting Settings

Accounting method: Inbox accounting

Store accounting logs for last 12 months

Used space:

0 bytes

0 MB

Free space:

52953780224 bytes

50501 MB



#### Manage Accounting

☐ Delete all accounting logs

☒ Delete accounting logs for specified period

From:

2012-06-04 15

To:

2012-06-04 15

Empty

### 8.3. Konfiguracja DirectAccess

Należy pamiętać, że DirectAccess wymaga IPv6 wprowadzonego i działającego globalnie, a więc jest to funkcja raczej przyszłościowa. Dzięki tej technologii użytkownicy zdalni będą zawsze mieli dostęp do wewnętrznej sieci firmowej bez potrzeby nawiązywania połączenia VPN. Co więcej taki zdalny użytkownik jest cały czas podłączony do sieci firmowej nawet przed zalogowaniem się na własne konto użytkownika, jedyny wymóg to połączenie z Internetem. Z kolei administrator sieci może takim komputerem zarządzać na odległość tak samo jakby był on wpięty do sieci. Cała komunikacja odbywa się w sposób bezpieczny po IPSec. W celu ćwiczeniowym proszę więc wcisnąć przycisk **Włącz Zdalny Dostęp (Enable DirectAccess)**, aby zobaczyć ekran powitalny, który między innymi informuje o tym, że DirectAccess może spokojnie działać „obok” VPN.

Welcome to the Enable DirectAccess Wizard

This wizard helps you to configure DirectAccess using recommended settings. Select computers that will be configured as DirectAccess clients, specify how client computers access the Internet, and configure a network topology.

Remote client computers that are not configured as DirectAccess clients can continue to connect over a VPN connection.


The Enable DirectAccess Wizard configures DirectAccess with default settings. Additional settings can be configured after completing the wizard.

☐ Do not show this again

Po kliknięciu przycisku **Dalej (Next)** kreator sprawdzi czy komputer spełnia wszelkie wymagania, jeżeli tak to przejdzie do karty, na której trzeba określić, które grupy komputerów z usługi katalogowej mają mieć dostęp przez DirectAccess. Ponadto można tu przefiltrować wybrane grupy tak, aby tylko maszyny mobilne

miały dostęp przez DA, a także wymusić tunelowanie połączenia.

Select one or more security groups containing client computers that will be enabled for DirectAccess

 komputery zdalne (ELITEPC\komputery zdalne)	<input type="button" value="Add..."/>
	<input type="button" value="Remove"/>

☒ Enable DirectAccess for mobile computers only

With this setting enabled, all mobile computers in the specified security groups will be enabled as DirectAccess clients.

☒ Use force tunneling

DirectAccess clients connect to the internal network and to the Internet via the Remote Access server

Kolejnym krokiem jest określenie topologii sieci serwera. Edge to topologia, gdzie serwer dostępu zdalnego stoi na pograniczu sieci zewnętrznej i sieci wewnętrznej, na ogół posiada dwa lub więcej adapterów sieciowych, gdzie jeden łączy z Internetem, a drugi z siecią firmową. Drugi rodzaj Behind an Edge device występuje w wersji posiadającej jedną lub dwie karty sieciowe. Scenariusz z dwiema kartami sieciowymi zakłada, że klientów spoza sieci i serwer dzieli jeszcze jakieś inne urządzenie jak na przykład firewall, do którego wpięty jest serwer, podczas, gdy druga karta komunikuje się z siecią wewnętrzną. Ostatni scenariusz z jedną kartą sieciową zakłada, że serwer nie pełni roli bramki, tylko jest po prostu wpięty bezpośrednio do sieci firmowej.

Select the network topology of the server.

- ☒ Edge
- ☐ Behind an edge device (with two network adapters)
- ☐ Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.

Type the public name or IPv4 address used by clients to connect to the Remote Access server:

ELITEPC-DC01.elitepc.pl

W kolejnym oknie należy zdefiniować listę serwerów DNS, z których mają korzystać maszyny klienckie. Gdy jedna maszyna nie umie rozwiązać zapytania, będzie ono kierowane do kolejnego na liście. Serwery firmowe powinny zajmować czołowe miejsce.

Add additional suffixes to search for short unqualified name in multiple locations. If a query fails for a suffix, the other suffixes are appended to the name and the DNS query is repeated for the alternate FQDN.

☒ Configure DirectAccess clients with DNS client suffix search list

Detected domain suffixes:

Add ->

<- Remove

Domain suffixes to use:

<Primary DNS suffix of client>  
elitepc.pl

^

v

New Suffix:

Add



The primary domain DNS suffix appears first in the list.

Kolejne okno informuje o zmianach w polisach bezpieczeństwa, które muszą być

wprowadzone, aby komputery klienckie prawidłowo funkcjonowały.

#### DirectAccess client GPO

GPO containing DirectAccess client settings:

ELITEPC

DirectAccess Client Settings

Browse.

#### DirectAccess server GPO

GPO containing DirectAccess server settings:

ELITEPC

DirectAccess Server Settings

Browse.

Następna karta jest kartą podsumowującą, na której należy kliknąć **Zakończ (Finish)**.

You have successfully completed the Enable DirectAccess Wizard. DirectAccess is configured with default settings.

[Click here to edit the wizard settings. Configuration settings that can be modified include GPO settings, the DirectAccess client security group, server adapters, and DNS properties.](#)

**Please Note:** This wizard configures DirectAccess with default settings.

To configure additional settings, click the Configuration node after completing this wizard. If Network Access Protection (NAP) or Network Load Balancing (NLB) is already configured for

Click Finish to apply the configuration.

Należy także pamiętać, że aby użytkownik mógł się zdalnie połączyć, na jego karcie w zakładce **Telefonowanie (Dial-in)** trzeba zezwolić na dostęp bądź skonfigurować dostęp zarządzany przez NPS.

Remote control		Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment		Sessions

Network Access Permission

☐ Allow access  
☐ Deny access  
☒ Control access through NPS Network Policy

☐ Verify Caller-ID:

Callback Options

☒ No Callback  
☐ Set by Caller (Routing and Remote Access Service only)  
☐ Always Callback to:

☐ Assign Static IP Addresses

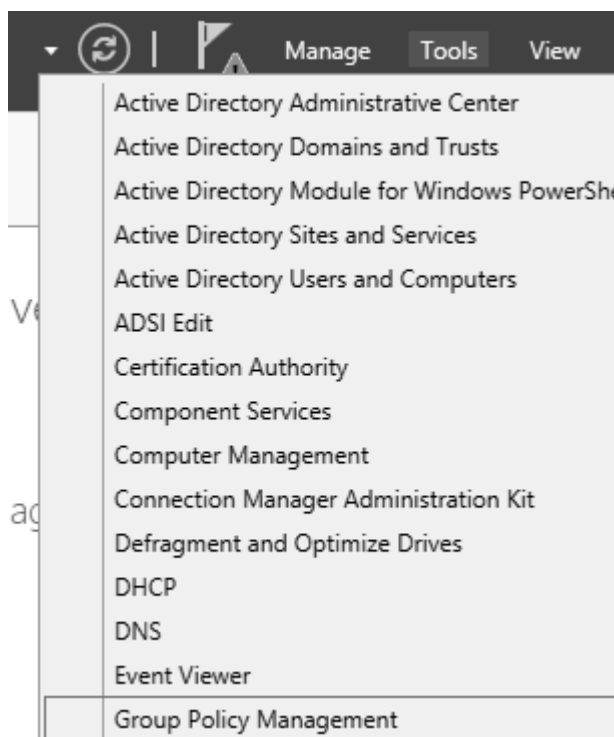
Define IP addresses to enable for this Dial-in connection.

☐ Apply Static Routes

Define routes to enable for this Dial-in connection.

## 9. Polisy (Zarządzanie Zasadami Grupy)

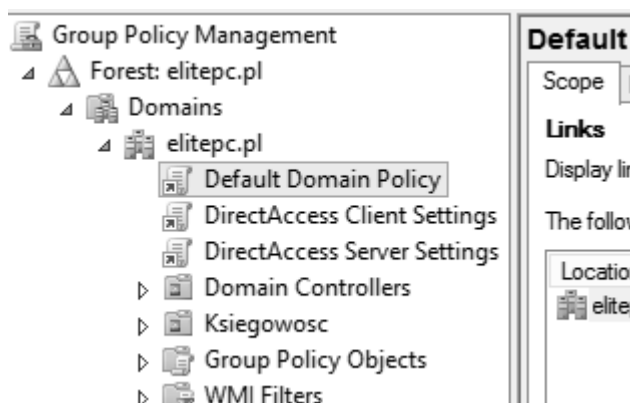
Polisy pozwalają na scentralizowane zarządzanie i konfigurowanie praktycznie całego systemu. Innymi słowy pozwalają na kontrolowanie tego, co użytkownicy mogą robić, a czego nie. Administrator może swobodnie kontrolować funkcje dostępne użytkownikom, nawet zabronić im takich drobnostek jak zmiana tapety. Aby wejść do konsoli **Zarządzania Zasadami Grupy (Group Policy Management)** należy kliknąć z poziomu **Menadżera Serwera (Server Manager)** guzik **Narzędzia (Tools)**, a następnie wybrać **Zarządzanie Zasadami Grupy (Group Policy Management)**.



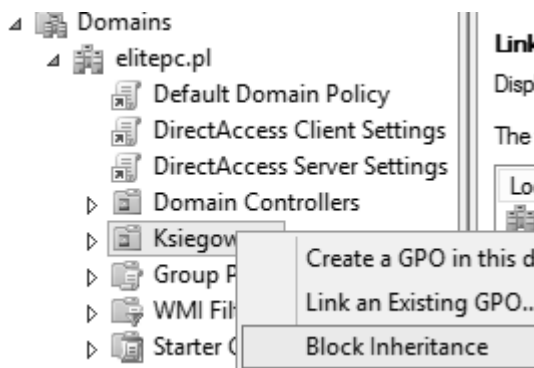
Po rozwinięciu drzewa z lewej strony można dostrzec tam domenę, a także utworzone wcześniej jednostki organizacyjne. Jest też **Domyślna Polisa Domeny (Default Domain Policy)**, co tak jak nazwa wskazuje, jest domyślną polisą dla domeny. Wszystko, co znajduje się w drzewie pod nią dziedziczy po niej, czyli



mówiąc krótko korzysta z niej. Ponieważ we wcześniejszych rozdziałach był konfigurowany DirectAccess również i dla tej roli pojawiły się dwie polisy. Gdyby nie był zainstalowany DirectAccess, nie byłoby ich tu (*DirectAccess Client Settings* oraz *DirectAccess Server Settings*).

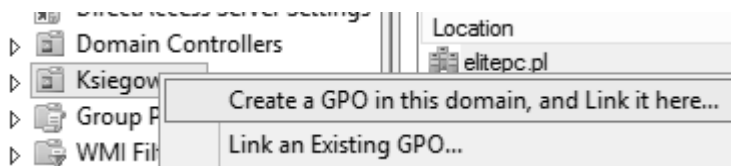


Jeżeli zajdzie taka potrzeba, dziedziczenie można zawsze wyłączyć poprzez kliknięcie prawym przyciskiem na odpowiedniej jednostce organizacyjnej i wybraniu opcji *Zablokuj Dziedziczenie (Block Inheritance)*.

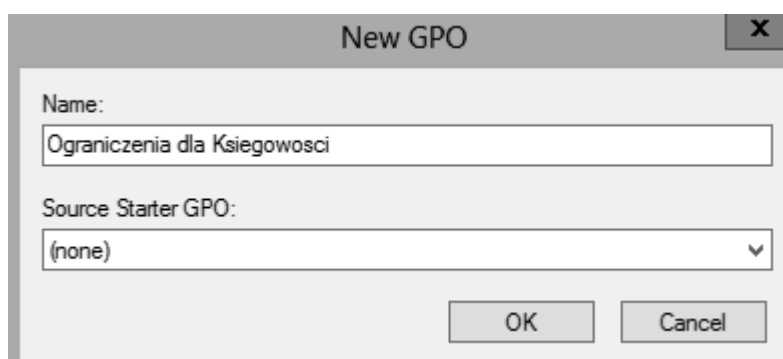


W tym przypadku jednak nie ma takiej potrzeby. W celach ćwiczeniowych zostanie stworzona nowa polisa dla Księgowości. W tym celu należy kliknąć ponownie prawym przyciskiem i wybrać opcję *Utwórz obiekt zasad grupy w tej domenie i umieść tu łącze (Create a GPO in this domain, and Link it here)*. Warto też

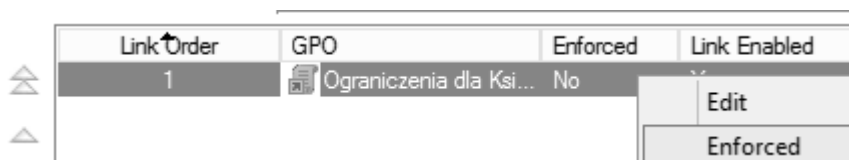
zwrócić uwagę, że jeżeli już wcześniej została stworzona polisa, która spełniała by odpowiednie wymagania, można ją podłączyć wybierając ***Połącz z istniejącym obiektem zasad grupy (Link an Existing GPO)***.



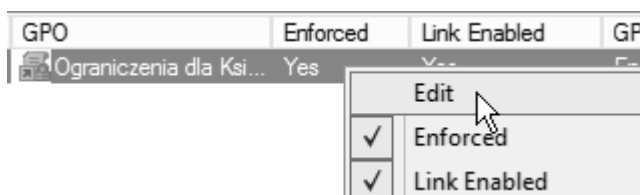
Pojawi się ekran, w którym należy podać nazwę dla nowej polisy. Dobrze, aby była ona intuicyjna np. ***Ograniczenia dla Księgowości*** i zatwierdzić wybór przyciskiem ***OK***.



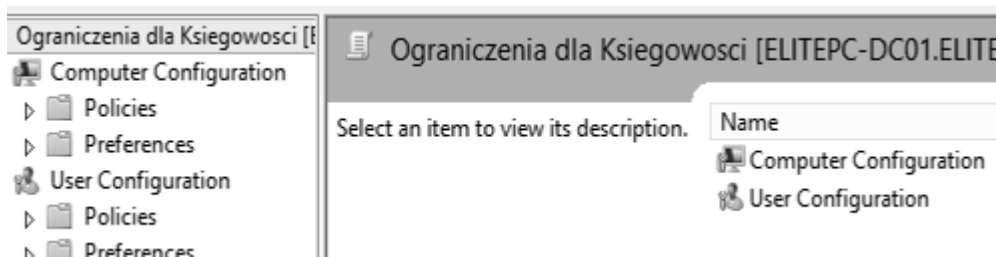
Po wybraniu kontenera Księgowość pojawi się ona na liście po prawej stronie okienka jak i w drzewie pod kontenerem. Jeżeli ma być ona zawsze wymuszona należy kliknąć na niej prawym przyciskiem myszy i zaznaczyć opcję ***Wymuszone (Enforced)***, a następnie zatwierdzić wybór klikając ***OK***. Dzięki temu pomimo, że wybrana polisa jest niżej w hierarchii będzie ona ważniejsza.



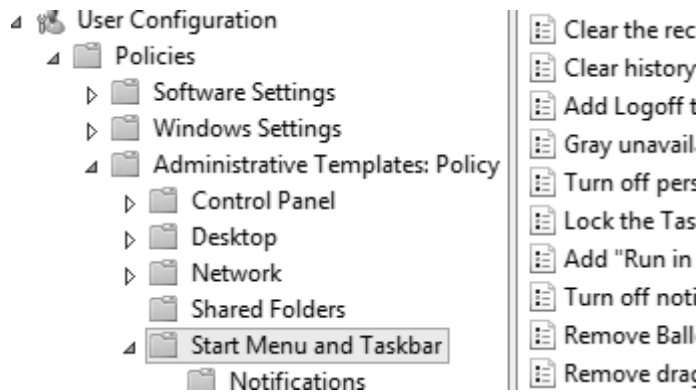
Teraz nadszedł czas na podjęcie decyzji, co ta polisa ma robić. Po raz kolejny należy kliknąć na niej prawym przyciskiem myszy, wybierając opcję **Edytuj (Edit)**.



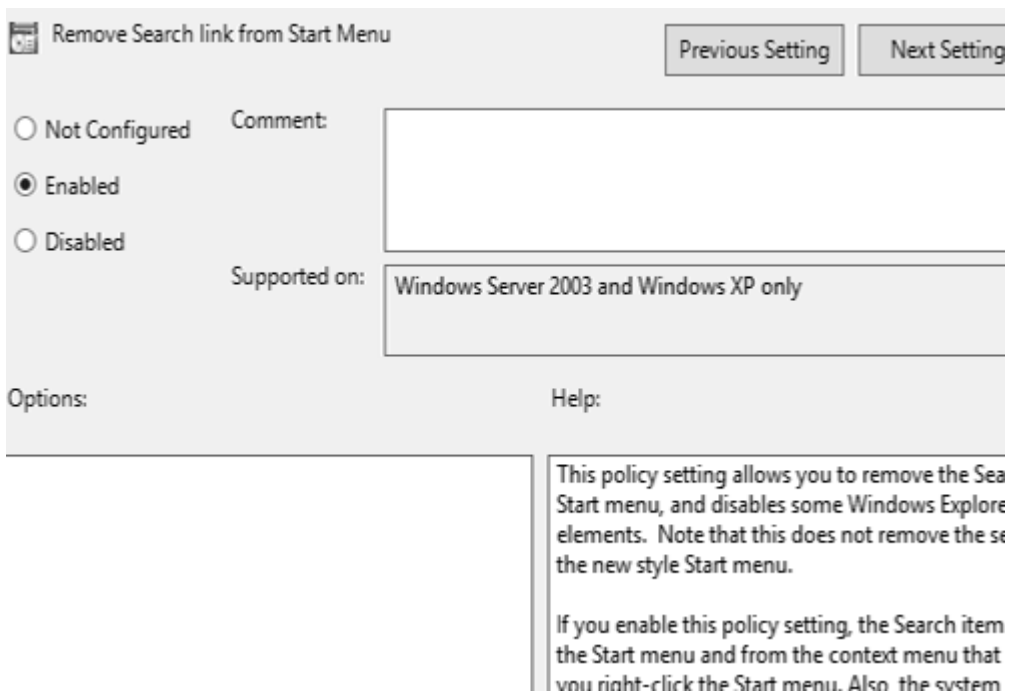
Otworzy się **Edytor Zarządzania Zasadami Grupy (Group Policy management Console)**. W książce zostanie jednak pominięta informacja do czego służy jaka zasada i gdzie się ona znajduje. Jest to narzędzie na tyle intuicyjne, że wystarczy przeczytać opisy pojedynczych opcji, aby zorientować się bez problemu co dana zasada robi. Nie mniej jednak przy odrobinie cierpliwości uda się odnaleźć odpowiednie elementy i skutecznie ograniczyć użytkowników.



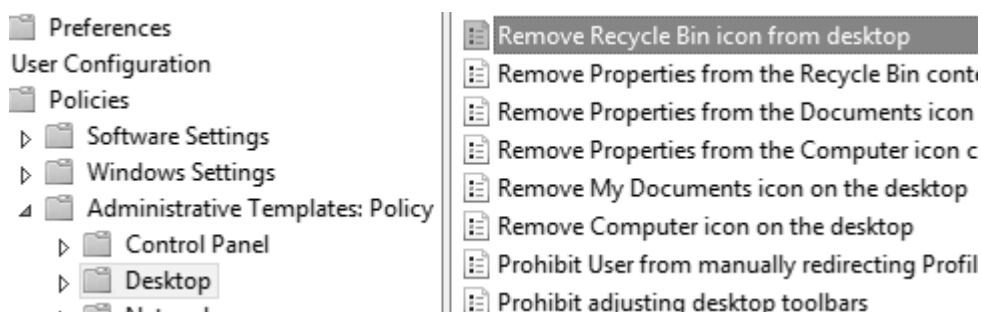
W celach ćwiczeniowych można trochę odchudzić za pomocą polisy menu Start. Aby tego dokonać należy rozwinąć listę w następujący sposób **Konfiguracja użytkownika > Zasady > Szablony administracyjne > Menu Start i pasek zadań (Computer Configuration > Policies > Administrative Templates > Start Menu and Taskbar)**.



Następnie należy dwukrotnie kliknąć na *Usuń menu Pomoc z Menu Start (Remove Search link from Start Menu)*. W oknie, które się pokaże należy zaznaczyć opcję *Włączone (Enabled)*, a potem *Zastosuj (Apply)* i potwierdzić wybór przyciskiem *OK*. Tak samo można zrobić dla opcji *Usuń menu Uruchom z menu start (Remove Run menu from Start Menu)*. Można jeszcze dla przykładu wyłączyć opcję *Wyloguj z menu start (Remove Logoff on the Start Menu)*.



W sekcji **Pulpit (Desktop)** można uruchomić opcję **Usuń ikonę Kosz z pulpitu (Remove Recycle Bin icon from desktop)**.



Dzięki takim poczynaniom użytkownik straci dostęp do pomocy, nie będzie mógł korzystać z opcji „uruchom”, a także już nigdy nie zostawi włączonego komputera w pracy, bo aby się wylogować będzie musiał wyłączyć komputer. Kiedy dokonywanie zmian zostanie ukończony należy kliknąć **Plik (File)** i wybrać opcję **Zakończ (Finish)**. Zostanie ona zastosowana do wszystkich maszyn i użytkowników znajdujących się we wnętrzu kontenera Księgowość.

Warto zauważyć, że stworzona chwilę temu polisa została dodana tuż obok napisu Księgowość w GPO. Po kliknięciu na nią, a następnie po wybraniu **Ustawień (Settings)** z zakładek po prawej stronie, pojawi się dość intuicyjny wgląd do zmian, jakie dana polisa wprowadza.



Aby sprawdzić czy powyższe zabiegi odniosły jakikolwiek skutek należy zalogować się na komputerze klienta, w tym przypadku można zalogować się np. jako Kasjer. W następnej kolejności należy uruchomić konsolę CMD lub PowerShell, a w niej wpisać polecenie „gpupdate /force”, które to spowoduje pobranie z kontrolera domeny najnowszych polis bezpieczeństwa i ich zastosowanie. Można to samo osiągnąć po prostu uruchamiając komputer ponownie. Co więcej odświeżenie polis przez automat nie zawsze skutkuje od razu, dlatego warto je wymusić.

Odświeżanie zasad bezpieczeństwa chwilę potrwa, jeżeli wszystko zostało prawidłowo skonfigurowane zakończy się sukcesem.

```
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
```

Podsumowując polisy stanowią bardzo potężne narzędzie w rękach administratora. Używa się ich nie tylko do dostosowywania takich banałów jak te przedstawione w

przykładzie, ale przede wszystkim do zabezpieczania komputera. Na przykład można blokować różne kombinacje klawiszy, strony internetowe, dołączać lokacje sieciowe, można zablokować możliwość instalowania różnych aplikacji, korzystania z gier itp. Bez problemu także można wymusić, aby na pulpicie pojawiły się skróty do niezbędnych firmowych aplikacji, a całą resztę funkcjonalności systemu Windows włącznie z używaniem niepotrzebnych przycisków po prostu zablokować. Podobnie ma się sprawa aspektów sprzętowych jak blokowanie napędu optycznego, nośników USB itp. To tak jakby administrator sam budował swój własny system operacyjny, idealnie spersonalizowany do potrzeb i upodobań użytkowników. Co najważniejsze można tego dokonać w sposób łatwy i przyjemny. Także istotne jest to, że polisy można wdrożyć na potrzeby pojedynczego komputera bez konieczności korzystania z domeny. Na przykład wbudowane w system konto gościa pozostawia użytkownikom zbyt duże pole do manewru, a na komputerze domowym jest zbyt wielu gości - wystarczy więc w odpowiedni sposób zająć się polisami lokalnymi.

## 9.1. Wybrane nowości w GPO

Warto omówić nowości, jakie zostały wprowadzone Windows Server 2012. Większość elementów nie uległa zmianie, jednak jest kilka różnic. Jedną z nich jest ***Name Resolution Policy***, gdzie pojawiły się dwie dodatkowe zakładki ***Generic DNS Server*** oraz ***Encoding***, które są związane z ***DNS SEC*** oraz rolą ***DirectAccess***.

**Description**

Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).

**Create Rules**

To which part of the namespace does this rule apply?

Suffix

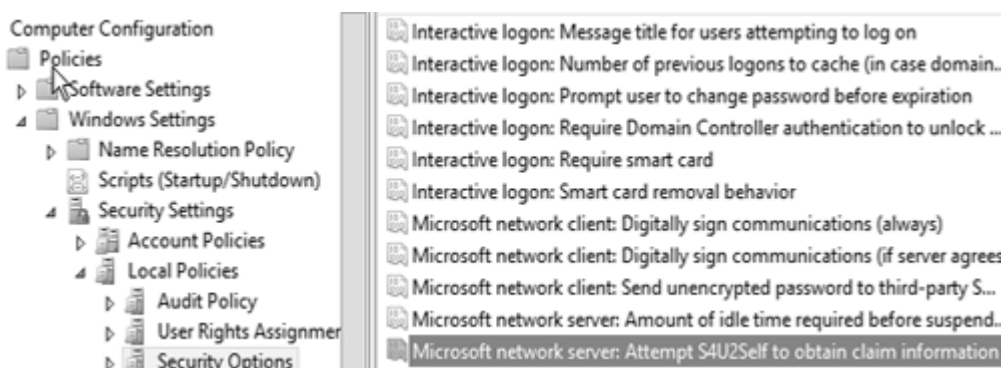
Certification authority: (Optional)

**DNSSEC** **DNS Settings for DirectAccess** **Generic DNS Server** **Encoding**

☐ Enable DNS settings

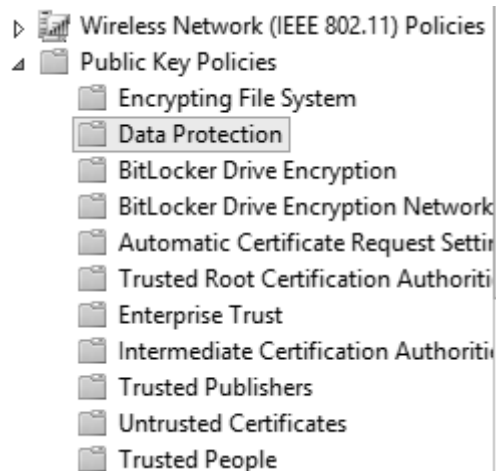
Generic DNS Server settings

Pojawiła się także zasada związana z autoryzacją metodą Claim dla systemów starszych niż Windows Server 2012 o nazwie **Microsoft network server: Attempt S4USelf to obtain claim information**.

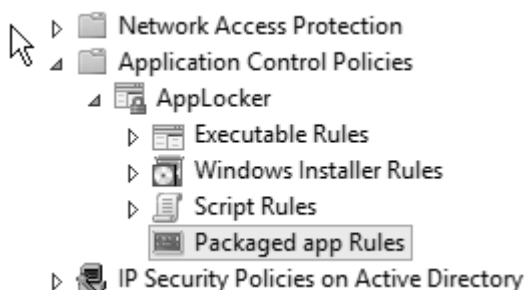


W gałęzi **Public Key Policies** pojawiły się dwa nowe kontenery. Jednym z nich jest **BitLocker Drive Encryption Network Unlock Certificate**, gdzie znajdują się ustawienia związane z napędami szyfrowanymi BitLockerem. Drugim jest **Protection**, który przechowuje ustawienia agenta odzyskiwania **Data Protection Recovery Agent**.





W funkcji **AppLocker** pojawiła się także pewna nowość. Jest nią **Packaged app Rules**, który odpowiada za blokowanie aplikacji napisanych dla interfejsu Metro, które Między innymi można nabyć za pośrednictwem Microsoft AppStore.



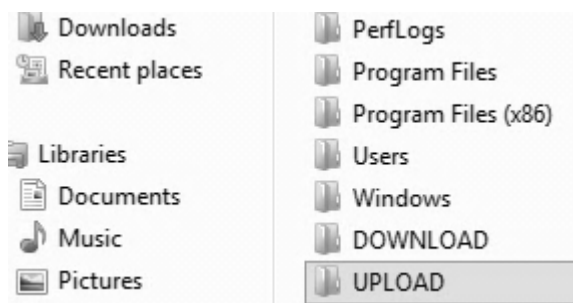
Bardzo duże zmiany zaszły w **Administrative Templates**, co ma związek z nowym interfejsem i możliwościami systemu Windows Server 2012.

## 10. Uprawnienia Sieciowe i na systemie plików

Jedną z największych zalet systemu plików NTFS jest możliwość szczegółowego zarządzania dostępem do zasobów. Dzięki grupom wcześniej utworzonym w usłudze Active Directory można swobodnie zarządzać tym, która z nich, jakie będzie miała uprawnienia. Nie mówiąc tu tylko o ustawieniach dostępu do plików, ale także do urządzeń np. drukarek. Można tylko określonym osobom pozwolić z niej korzystać, a nawet ustawić priorytety wydruku. Na przykład, jeśli kierownik będzie miał wyższy priorytet, to drukowanie wywołane przez pracowników zostanie wstrzymane po to, aby dokumenty kierownika mogły zostać wcześniej wydrukowane. Kiedy to się stanie, wznowione zostaną wydruki o niższym priorytecie. W tym dziale przedstawione także zostanie nadawanie uprawnień dla zasobów sieciowych. Na koniec udostępniony zasób zostanie zamapowany jako dysk twardy na komputerze klienta oraz narzucona zostanie quota na zasobie, czyli ograniczenie ilości danych, jakie będzie można w nim przechowywać.

### 10.1. Uprawnienia sieciowe

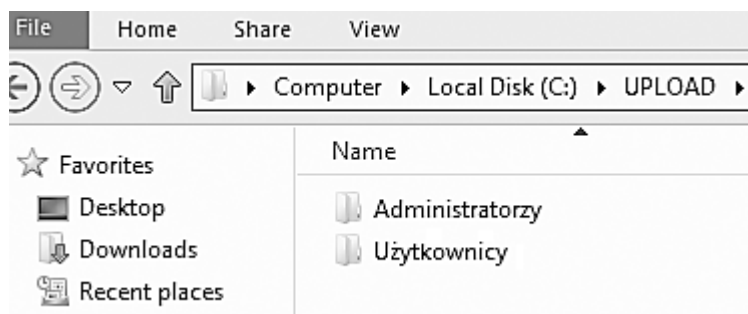
Aby przećwiczyć nadawanie uprawnień sieciowych warto stworzyć na dysku C katalogi UPLOAD i DOWNLOAD, które w miarę prosty sposób uda się skonfigurować.



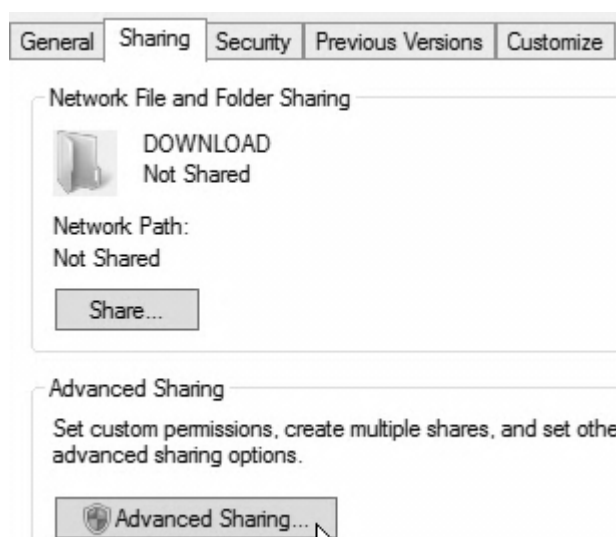
Wewnątrz obu katalogów zostaną stworzone foldery o nazwach:

- Administratorzy

- Użytkownicy

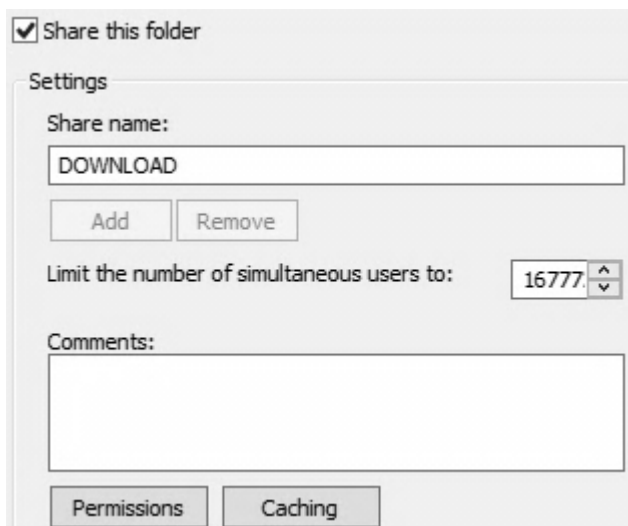


Należy kliknąć prawym przyciskiem myszy na folderze DOWNLOAD, wybrać jego **Właściwości (Properties)** i przejść do zakładki **Udostępnianie (Sharing)**. Następnie należy kliknąć w **Udostępnianie Zaawansowane (Advanced Sharing)**.



Aby folder udostępnić konieczne jest zaznaczenie opcji **Udostępnij ten folder (Share this folder)**. W polu **Nazwa udziału (Share name)** należy wpisać nazwę, pod jaką będzie on widoczny w sieci np. DOWNLOAD. Gdyby jego nazwa została zapisana następująco DOWNLOAD\$, czyli na końcu nazwy dopisany by został symbol dolara, folder ten byłby udostępniony jako ukryty. Można by było się do niego dostać np. poleceniem \\serwer\DOWNLOAD\$, natomiast nie byłby on

widoczny z poziomu Otoczenia sieciowego.



☒ Share this folder

Settings

Share name:

DOWNLOAD

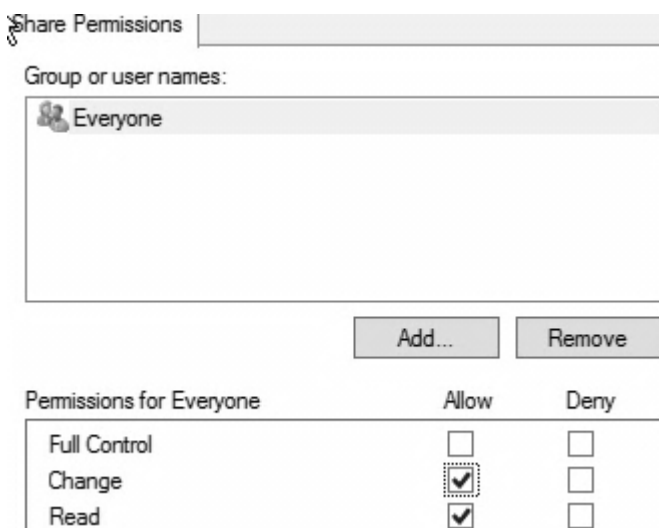
Add Remove

Limit the number of simultaneous users to: 16777

Comments:

Permissions Caching

Klikając przycisk **Uprawnienia (Permissions)** można nadawać uprawnienia sieciowego dostępu. Jest to **Odczyt (Read)** i **Zmiana (Change)** lub **Pełna Kontrola (Full Control)**. Uprawnienia te można nadawać zarówno pojedynczym użytkownikom jak i grupom użytkowników. Dodaje się ich przyciskiem **Dodaj (Add)**.



Share Permissions

Group or user names:

Everyone

Add... Remove

Permissions for Everyone	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Warto zauważyć, że nadając uprawnienia administrator ma dwie opcje **Zezwól (Allow)** oraz **Odmów (Deny)**. Ta druga opcja jest silniejsza i służy ona do tworzenia wykluczeń. Dla przykładu grupie **Wszyscy (Everyone)** dano możliwość Odczytu i Zmiany, a pojedynczy użytkownik np. kasjer\_01 ma nie mieć dostępu. W tym celu kasjerowi\_01 zamiast w sekcji Allow nadać odpowiednie uprawnienia, zabiera się je w sekcji Deny. Pomimo, że należy on do grupy Wszyscy i tak nie będzie miał dostępu do zasobów. Podobnie sprawa wygląda w przypadku nadawania innych uprawnień w systemie Windows Server 2012.

Group or user names:

Everyone
kasjer_01 (kasjer_01@elitepc.pl)

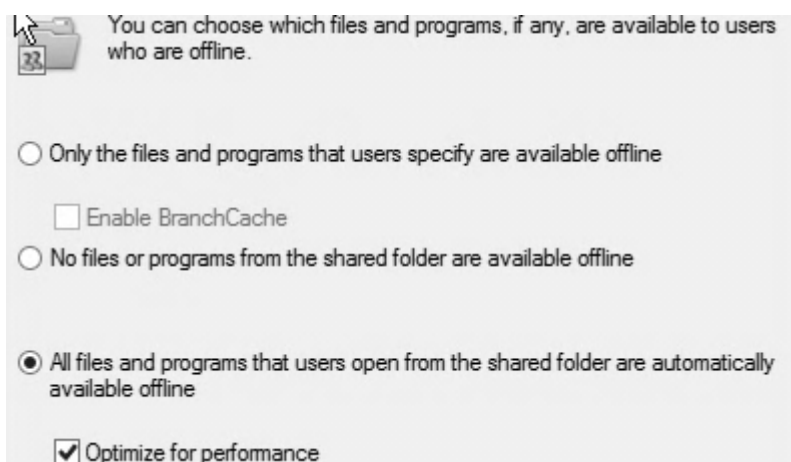
Add... Remove

Permissions for kasjer\_01

	Allow	Deny
Full Control	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Change	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Read	<input type="checkbox"/>	<input checked="" type="checkbox"/>

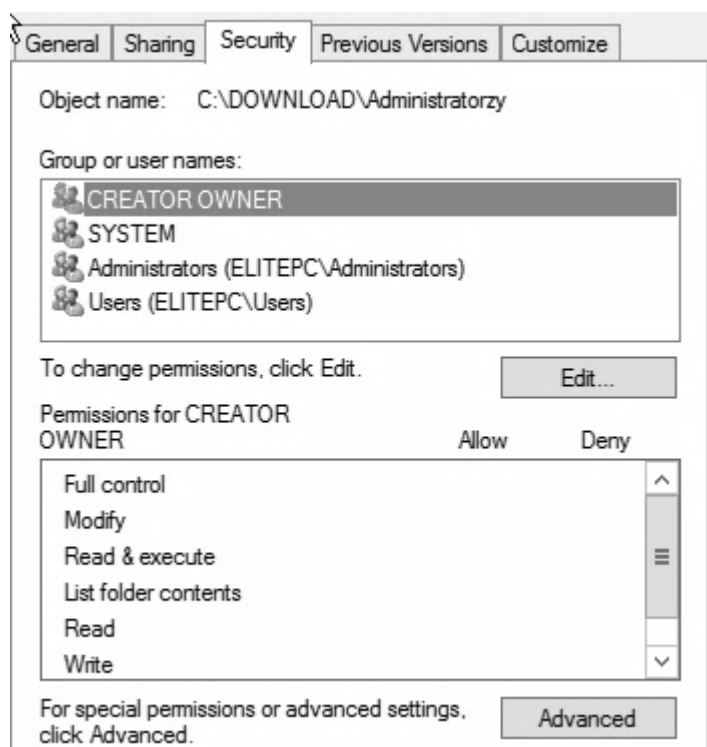
### 10.1.1. Dodatkowe ustawienia udostępnianych plików

Po powrocie do okna udostępniania zasobów warto kliknąć **Buforowanie (Caching)**. Uruchomienie tej opcji i zoptymalizowanie jej dla wydajności spowoduje, że użytkownik będzie miał dostęp do swoich plików nawet, gdy nie będzie podłączony przez sieć do serwera. Natomiast w momencie podpięcia dane zostaną zsynchronizowane.

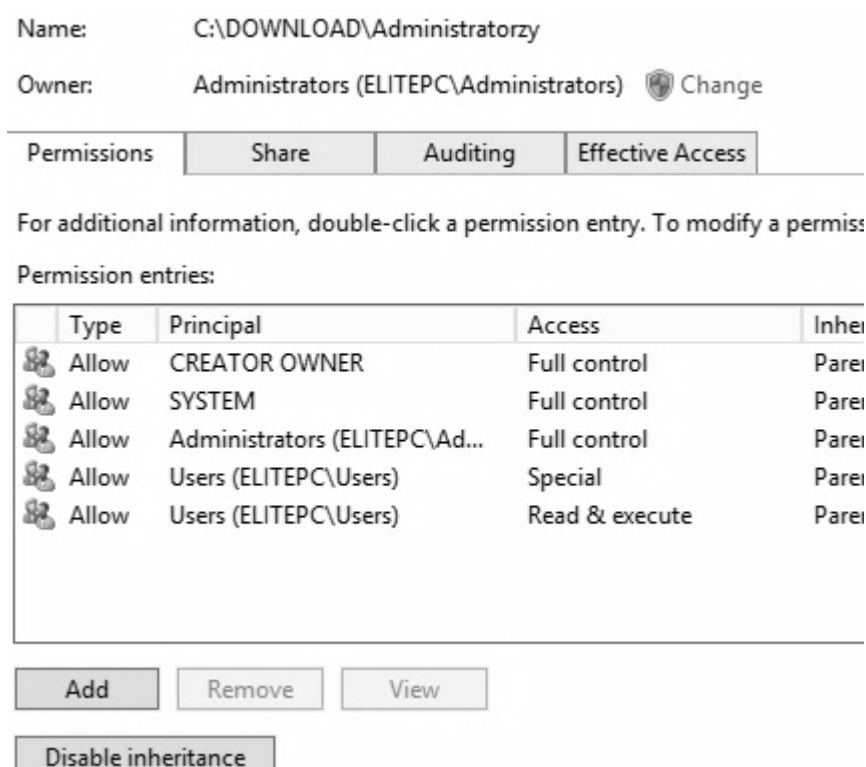


## 10.2. Uprawnienia NTFS

Uprawnienia na systemie plików NTFS są znacznie bezpieczniejsze jak i bardziej zaawansowane. W celu ich edycji, we właściwościach pliku bądź folderu należy kliknąć zakładkę **Zabezpieczenia (Security)**.



Aby można było swobodnie edytować uprawnienia NTFS należy wyłączyć dziedziczenie z katalogu nadrzędnego. Domyślnie w systemie Windows nowo utworzony folder przejmuje uprawnienia z folderu nadrzędnego, w przypadku książkowym bezpośrednio z Dysku C. Należy wejść we właściwości folderu Administratorzy, a następnie w zakładkę **Zabezpieczenia (Security)** i kliknąć przycisk **Zaawansowane (Advanced)**, a tam wybrać opcję **Wyłącz dziedziczenie (Disable inheritance)** po to, aby móc swobodnie edytować uprawnienia.



W komunikacie, który się pojawi należy kliknąć **Przekształć odziedziczone uprawnienia do jawnych uprawnień do tego obiektu (Convert inherited permissions into explicit permissions on this object)**. Spowoduje to przekopiowanie uprawnień tak, aby te już istniejące zostały zachowane.



What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

→ Convert inherited permissions into explicit permissions on this object.

→ Remove all inherited permissions from this object.

Teraz po powrocie do zakładki **Zabezpieczenia (Security)** i przyciśnięciu guzika **Edytuj (Edit)** istnieje możliwość edycji uprawnień NTFS. Jest ich więcej, są to **Zapis (Write)**, **Odczyt (Read)**, **Listowanie zawartości folderu (List folder contents)**, **Odczyt i Wykonanie (Read & Execute)**, **Modyfikacja (Modify)** oraz **Pełna kontrola (Full Control)**, która między innymi pozwala na edycję uprawnień.

Object name: C:\DOWNLOAD\Administratorzy

Group or user names:

CREATOR OWNER
SYSTEM
Administrators (ELITEPC\Administrators)
Users (ELITEPC\Users)

Add... Remove

Permissions for CREATOR OWNER

	Allow	Deny	
Full control	<input type="checkbox"/>	<input type="checkbox"/>	^
Modify	<input type="checkbox"/>	<input type="checkbox"/>	≡
Read & execute	<input type="checkbox"/>	<input type="checkbox"/>	
List folder contents	<input type="checkbox"/>	<input type="checkbox"/>	
Read	<input type="checkbox"/>	<input type="checkbox"/>	▼

Warto zwrócić uwagę, że w razie potrzeby nie ma potrzeby ograniczania się do grup, gdyż uprawnienia można także spersonalizować dla pojedynczego użytkownika. Czasami np. dla kierownika działu jest to pożądane. Często zdarzają



się sytuacje, gdy pliki czy foldery tylko jedna osoba ma mieć możliwość ich edycji, a jej współpracownicy jedynie mogą ten plik odczytywać. W taki sposób można, więc łatwo nadać uprawnienia pojedynczemu użytkownikowi do edytowania.

Twórca-właściciel ma nadane specjalne uprawnienia, których też lepiej nie edytować bez doświadczenia w tej kwestii. Należy też pamiętać, że wcześniej modyfikowane były uprawnienia dostępu przez sieć, a teraz modyfikowany jest dostęp do plików na dysku, a nie zasobów udostępnionych. Trzeba także uważać i wiedzieć, co się robi. Dla przykładu Użytkownikom odmówiona zostanie możliwość odczytu, a Administratorowi będzie to pozwolone. Pojawia się pytanie, czy Administrator będzie mógł odczytać zasoby, bo przecież on też jest Użytkownikiem. W ramach książki zostaną zmodyfikowani Użytkownicy tak, aby nie mieli żadnych uprawnień do zasobów. Resztę można zostawić bez zmian.

W przypadku katalogu Download w celach testowych zwykli użytkownicy nie dostaną żadnych praw.

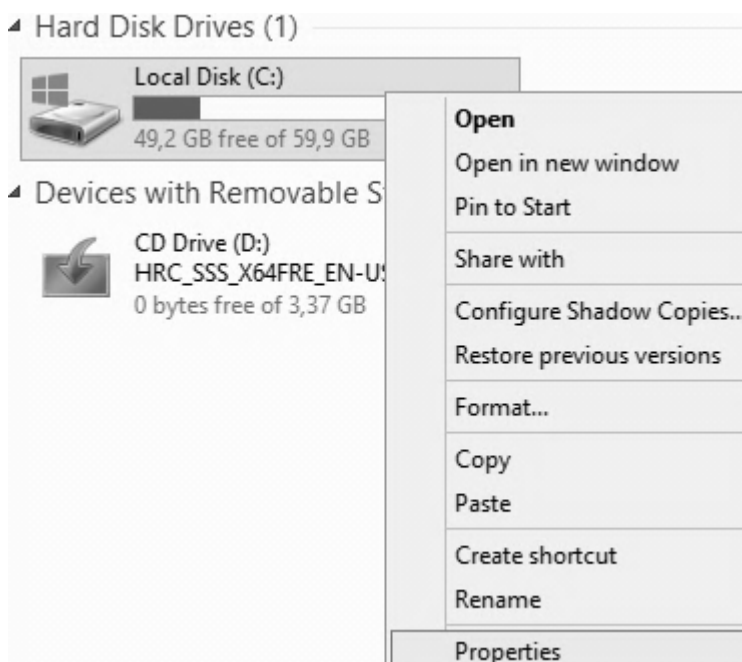
W przypadku katalogu Upload użytkownicy dostaną jedynie możliwość Zapisu i wykonania. Modyfikować nie muszą, a Pełna Kontrola by im pozwoliła zmieniać uprawnienia folderów i plików. Nie tylko byłoby to niebezpieczne ze względu na brak umiejętności z ich strony, ale Administrator powinien być jedyną osobą z takimi możliwościami. Na stronach technet można znaleźć dokładny opis tego, za co dane uprawnienie odpowiada. Warto się temu zagadnieniu przyjrzeć, gdyż pozwala to na wygodne zarządzanie dostępem do plików dowolną drogą. Nie ważne czy przez sieć lokalną, FTP czy stronę www, te ustawienia zawsze są brane pod uwagę.

**UWAGA!!!**

Gdy folder kopiowany jest do innej lokalizacji nałożone na niego uprawnienia są tracone i dziedziczy on nowe uprawnienia z folderu nadrzędnego. W przypadku, gdy


folder jest przenoszony uprawnienia są zachowywane.

Aby włączyć limit na dysku należy kliknąć prawym przyciskiem myszy na dysku wybranej literze dysku i wybrać **Właściwości (Properties)**.



Następnie należy wybrać **Przydział (Quota)**. Zostanie uruchomione zarządzanie przydziałami i skonfigurowane tak, jak na ilustracji poniżej. Spowoduje to, że użytkownik nie będzie mógł na dysku C serwera przechowywać więcej niż 5000MB danych, a gdy przekroczony zostanie 4500MB pojawi się komunikat z ostrzeżeniem. Co więcej nie ważne, gdzie dany użytkownik ma umieszczone swoje pliki, ważna jest suma ich rozmiarów. System je odnajdzie po właściwości zasobu mówiącej o jego właścicielu. Należy kliknąć **Zastosuj (Apply)** i **OK**.

General	Tools	Hardware	Sharing	Security
Shadow Copies		Previous Versions		Quota

 Status: Disk quotas are disabled

☒ Enable quota management

☒ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

☐ Do not limit disk usage

☒ Limit disk space to

Set warning level to

Select the quota logging options for this volume:

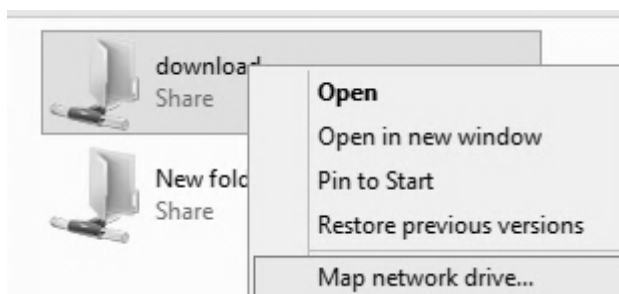
☐ Log event when a user exceeds their quota limit

☐ Log event when a user exceeds their warning level

[Quota Entries...](#)

Warto wykonać kilka testów czy nałożone wcześniej uprawnienia i Quota działają, przechodząc do komputera klienckiego i logując się na nim jako Kasjer. Konieczne jest wejście w **Mój Komputer (My Computer)** i w panelu z lewej strony okna wybranie z menu **Sieć (Network)** nazwy komputera, do którego zasobów można się dostać. Pojawi się lista udostępnionych zasobów. Przykładowo można więc wybrać Download. Niestety zwykły użytkownik nie ma praw dostępu do tego katalogu, co jest prawidłowe we wcześniejszej konfiguracji.

Teraz pora zapewnić łatwy dostęp do tych katalogów. Najlepiej będzie je zamapować jako dyski sieciowe. W przypadku książkowym najprościej jest to zrobić klikając na danym folderze prawym guzikiem i wybierając opcję **Mapuj Dysk Sieciowy (Map Network Drive)**.



Można wybrać literę dysku i ewentualnie wprowadzić poświadczenia innego użytkownika, aby to z jego uprawnieniami zmapowany był dysk. Na koniec należy kliknąć **Zamknij (Finish)**.

### What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive:

Folder:

Example: \\server\share

☒ Reconnect at sign-in

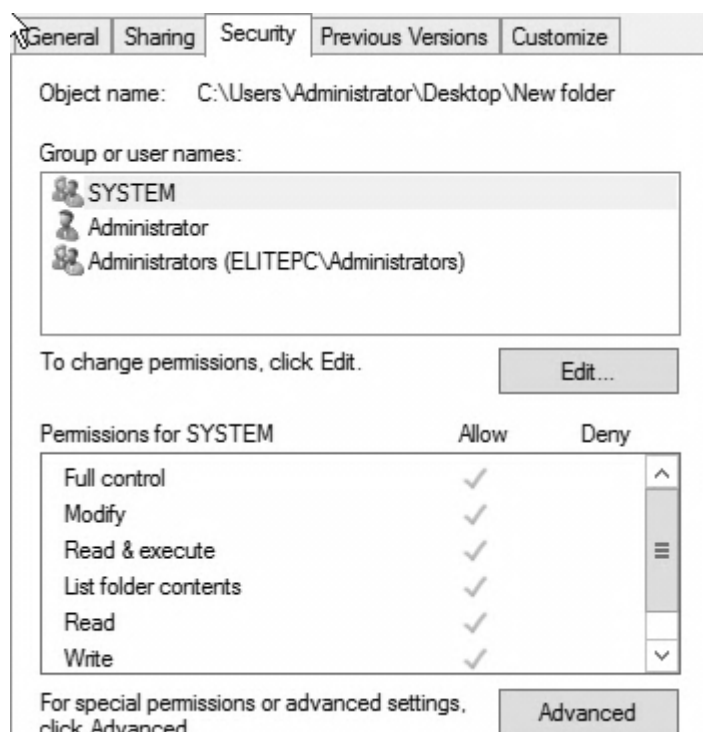
☐ Connect using different credentials

## 10.3. Autoryzacja Metodą CLAIM

W tym rozdziale omówiony zostanie mechanizm autoryzacji metodą Claim. Sam w sobie nie jest on nowością. Wcześniej był on z powodzeniem używany w Active Directory Federation Services w Windows Server 2008 R2. To, co się zmieniło to to, iż teraz może on być używany w obrębie lasu czy też domeny. Nowy mechanizm rzuca całkowicie nowe światło na metody autoryzacji. Może on być używany np. podczas autoryzacji dostępu do danych udostępnianych przez serwer plików przy użyciu tzw. **Uzgodnień (Claim)** zapisanych w atrybutach konkretnego obiektu, które mogą być zdefiniowane na poziomie Active Directory.


### 10.3.1. Nakładanie uprawnień Claim

Do tej pory uprawnienia były nadawane za pomocą tzw. *List Kontroli Dostępu (Access Control List)*. Określano było jacy użytkownicy, grupy czy komputery mają mieć dostęp do zasobów i z jakimi uprawnieniami (Allow/Deny). Następnie te dane były przekazywane jako token w protokole Kerberos. To w systemie Windows Server 2012 się nie zmieniło.



Okno zaawansowanego udostępnienia pozornie uległo jedynie zmianom kosmetycznym. Lecz to nie do końca prawda.




Name: C:\Users\Administrator\Desktop\New folder

Owner: Administrators (ELITEPC\Administrators)  Change

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify permissions

Permission entries:

	Type	Principal	Access	Inheritance
	Allow	SYSTEM	Full control	None
	Allow	Administrators (ELITEPC\Ad...	Full control	None
	Allow	Administrator	Full control	None

Add Remove Edit

Enable inheritance

Zostanie wyłączone dziedziczenie. Warto zauważyć, że po podwójnym kliknięciu w użytkownika czy też grupę lub przy dodawaniu nowej pozycji do listy DACL pojawiają się nowe opcje związane z autoryzacją metodą CLAIM.

Permission Entry for New folder

Principal: Administrators (ELITEPC\Administrators) Select a principal

Type: Allow ▼

Applies to: This folder, subfolders and files ▼

Permissions:

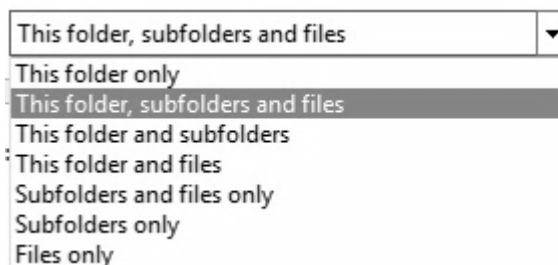
- ☒ Full control
- ☒ Modify
- ☒ Read & execute
- ☒ List folder contents
- ☒ Read
- ☒ Write
- ☐ Special permissions

☐ Only apply these permissions to objects and/or containers within this container

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

Add a condition

Na powyższym zrzucie ekranu widać nowe okno nadawania uprawnień do obiektu. W pierwszej kolejności należy wybrać podmiot, którym może być dowolny użytkownik lub dowolna grupa użytkowników. Po wybraniu podmiotu należy zdefiniować czy reguła będzie pozwalała wykonywać jakąś czynność czy też nie (Allow/Deny), a także zdefiniować jaki jest zasięg reguły.



Może się ona dotyczyć kolejno:

- Tylko tego folderu
- Tego folderu, pod folderów oraz plików
- Tego folderu i podfolderów
- Tego folderu i Plików.
- Tylko podfolderów i plików
- Tylko podfolderów
- Tylko plików

Następnie w sekcji ***Uprawnienia (Permissions)*** należy zdefiniować odpowiednie uprawnienia. Do wyboru jest ***Pełna Kontrola (Full Control)***, która między innymi pozwala zarządzać uprawnieniami, możliwość ***Modyfikowania (Modify)*** zawartości folderu, ***Odczytu i Wykonania (Read & Execute)***, ***Przeglądania zawartości folderu (List folder contents)***, ***Odczytu (Read)***, a także ***Zapisu (Write)***.

Permissions:

- ☒ Full control
- ☒ Modify
- ☒ Read & execute
- ☒ List folder contents
- ☒ Read
- ☒ Write
- ☐ Special permissions



Jeżeli są nie wystarczające można także skorzystać z **uprawnień zaawansowanych** (*Show advanced permissions*). Są one dużo bardziej precyzyjne. Zdefiniować można podobnie jak wcześniej **pełną kontrolę** (*Full control*) lub jedynie wybrać któreś z pozostałych możliwości, którymi są kolejno, **przechodzenie pomiędzy folderami i wykonywanie plików** (*Traverse folder/ execute folder*), **listowanie zawartości folderów i odczyt danych** (*List folder /read data*), **odczyt atrybutów** (*Read attributes*), **odczyt atrybutów rozszerzonych** (*Read extended attributes*), **tworzenie plików i zapis danych** (*Create files/ write data*), **tworzenie folderów i dołączanie danych** (*Create folders /append data*), **zapisywanie atrybutów** (*Write attributes*), **zapisywanie rozszerzonych atrybutów** (*Write extended attributes*), **kasowanie podfolderów i plików** (*Delete subfolders and files*), **kasowanie** (*Delete*), **możliwość odczytu** (*Read permissions*), **możliwość zmiany** (*Change permissions*), **możliwość przejmowania na własność** (*Take ownership*).

#### Permissions:

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Full control                   | <input checked="" type="checkbox"/> Write attributes            |
| <input checked="" type="checkbox"/> Traverse folder / execute file | <input checked="" type="checkbox"/> Write extended attributes   |
| <input checked="" type="checkbox"/> List folder / read data        | <input checked="" type="checkbox"/> Delete subfolders and files |
| <input checked="" type="checkbox"/> Read attributes                | <input checked="" type="checkbox"/> Delete                      |
| <input checked="" type="checkbox"/> Read extended attributes       | <input checked="" type="checkbox"/> Read permissions            |
| <input checked="" type="checkbox"/> Create files / write data      | <input checked="" type="checkbox"/> Change permissions          |
| <input checked="" type="checkbox"/> Create folders / append data   | <input checked="" type="checkbox"/> Take ownership              |

Ostatnia trzecia już sekcja okna dotyczy tworzenia reguły autoryzacyjnej. To właśnie one stanowią metodę autoryzacji CLAIM. Standardowo żadna reguła nie jest zdefiniowana i brane są pod uwagę uprawnienia nadane w zwykły sposób. Aby taką regułę dodać należy kliknąć **Dodaj Warunek** (*Add Condition*)

 Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

Add a condition

Spowoduje to pojawianie się dodatkowej listy, w której istnieje możliwość zdefiniowania warunków dostępowych. W pierwszym polu określa się czy reguła będzie dotyczyła użytkownika (User) czy urządzenia, czyli konta komputera (Device). W drugim polu należy określić czy reguła dotyczyć będzie jakiejś grupy.

 Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

User ▼ Group ▼ Member of any ▼ Value ▼ 1 item(s) selected ▼ Add items

Add a condition

W trzecim określa się czy reguła będzie obowiązywała użytkowników należących do jednej z grup wyznaczonych w polu piątym, czy też użytkowników należących do każdej z grup, lub nie będących członkami ani jednej z tych grup lub nie będących członkami wszystkich tych grup.

Member of any ▼  
Member of any  
Member of each  
Not member of any  
Not member of each

Przyciskiem **Dodaj obiekty** (*Add items*) można zdefiniować jakich grup będzie dotyczyła reguła.

1 item(s) selected ▼ Add items Remove  
☒ Administrators (ELITEPC\Administrat...

Tak utworzona reguła pojawi się na liście.

Permission entries:

	Type	Principal	Access	Condition
	Allow	SYSTEM	Full control	
	Allow	Administrator	Full control	
	Allow	Administrators (ELITEP...	Full control	Member of any({Admin

W zakładce *Efektywne Uprawnienia (Effective Access)* istnieje możliwość podejrzenia jaki użytkownik ma uprawnienia do konkretnego folderu.

Name: C:\Users\Administrator\Desktop\New folder

Owner: Administrators (ELITEPC\Administrators) Change

Permissions Auditing Effective Access

Select a user, group, or device to view the permissions that would be granted on this object.

User/ Group: admin (ELITEPC\admin) Select a user

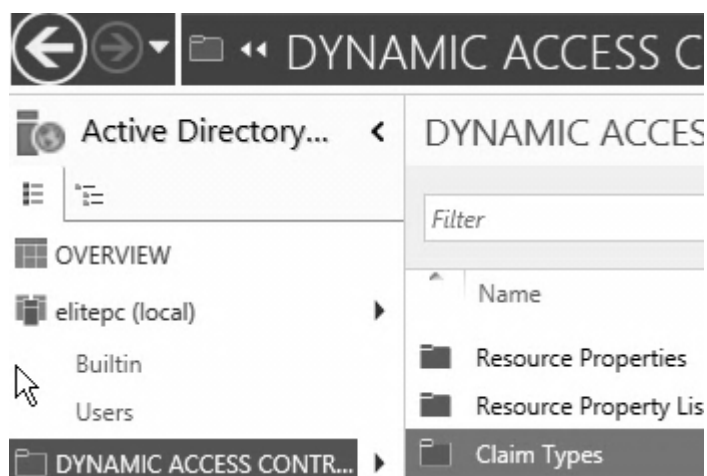
Device: Select a device

View effective access

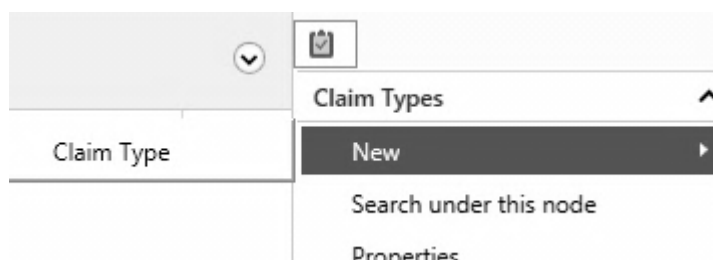
Effective access	Permission	Access
	Full control	File Perr

### 10.3.2. Definiowanie Claim Types

Innym sposobem definiowania uzgodnień Claim jest użycie konsoli *Centrum Administracyjnego Active Directory (Active Directory Administrative Center)*. Należy w nim rozwinąć *Dynamiczną kontrolę dostępu (DYNAMIC ACCESS CONTROL)* i wybrać z listy *Typy uzgodnień (Claim Types)*.



Następnie w menu po prawej stronie należy wybrać *Nowy > Typ uzgodnień (New > Claim Type)*.



Zamiast bazować na grupach komputerów i użytkowników można stworzyć uzgodnienie, które będzie brało pod uwagę konkretne atrybuty obiektów znajdujących się w bazie Active Directory. Dla przykładu zostanie wybrana opcja *Prawo Jazdy (CarLicense)*. Należy kliknąć *OK*.

## Create Claim Type: carLicense

Source Attribute

### Source Attribute

A claim type is an assertion about the object with which it is associated. The claim type is used to filter objects when authoring central access rules.

Select an AD attribute to base this claim type on:

<div>Filter</div>			
Display Name	Value Type	Belongs To (Class)	ID
carLicense	Multi-Valued String	user, inetOrgPerson	carLicense
catalogs	Multi-Valued String	computer, msDirectoryObject	Catalog
cn	String	user, inetOrgPerson	CommonName
co	String	user, inetOrgPerson	TextCountryCodeName
codePage	Integer	user, inetOrgPerson	CodePage
comment	String	user, inetOrgPerson	UserComment
company	String	user, inetOrgPerson	CompanyName
countryCode	Integer	user, inetOrgPerson	CountryCode

Wracając do właściwości udostępnionego folderu i próbując raz jeszcze dodać regułę Claim, do wyboru poza grupą pojawił się stworzony przez chwilę carLicense.

Add a condition to limit access. The principal will be granted

User	Group	Memb
Add a condition		
carLicense		
Group		

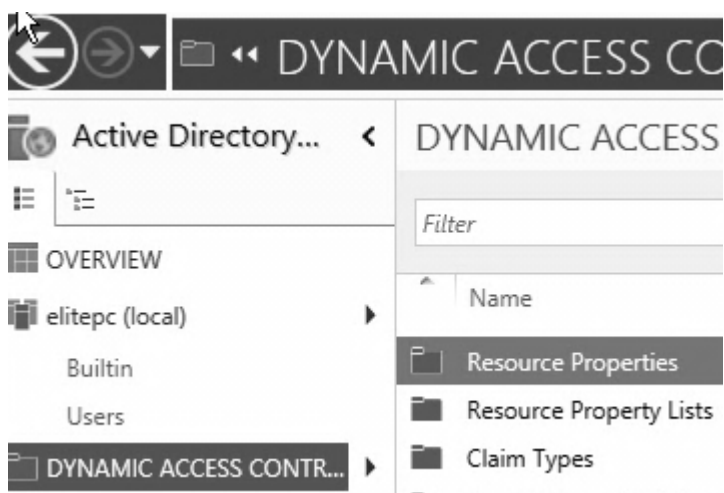
Po jego wybraniu definicja reszty reguły ulega dynamicznej zmianie w zależności od wybranych atrybutów w Centrum Administracyjnym.

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met

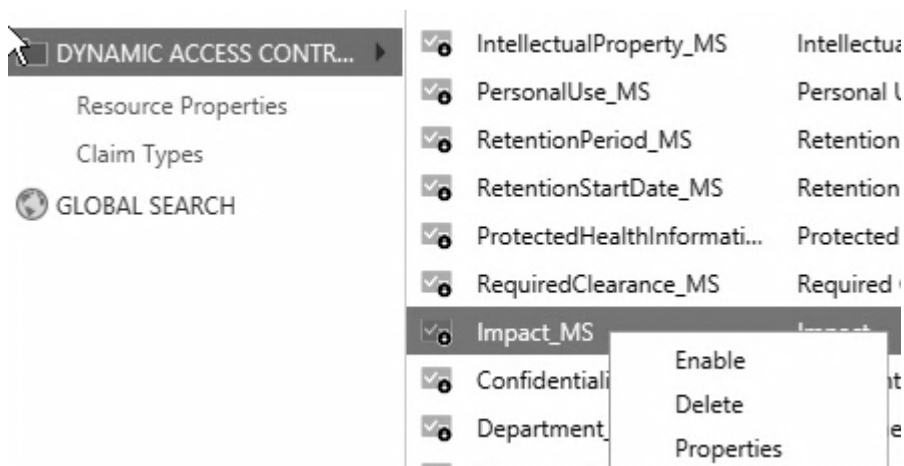
User	carLicense	Contains each of	Value	DSW
------	------------	------------------	-------	-----

Add a condition

Co więcej w podobny sposób można zdefiniować konkretne typy zasobów.



Na konkretnym typie zasobu wystarczy kliknąć prawym guzikiem i wybrać opcję **Włącz (Enable)**.



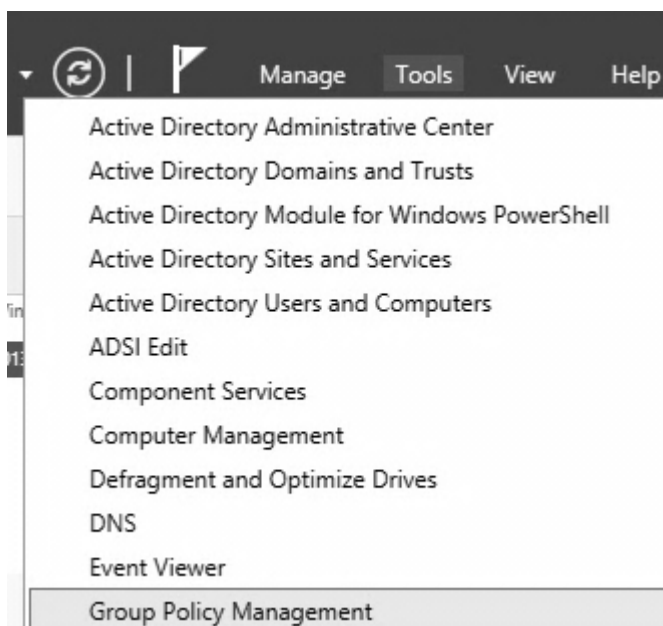
Zasób pojawi się do wyboru we właściwościach pliku/folderu.

Add a condition to limit access. The principal will be granted the specifi

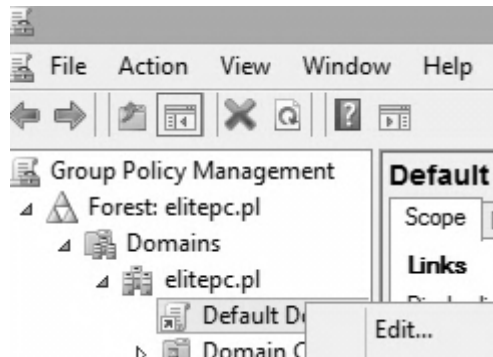
Resource	▼	Impact	▼	Equals
----------	---	--------	---	--------

Add a condition

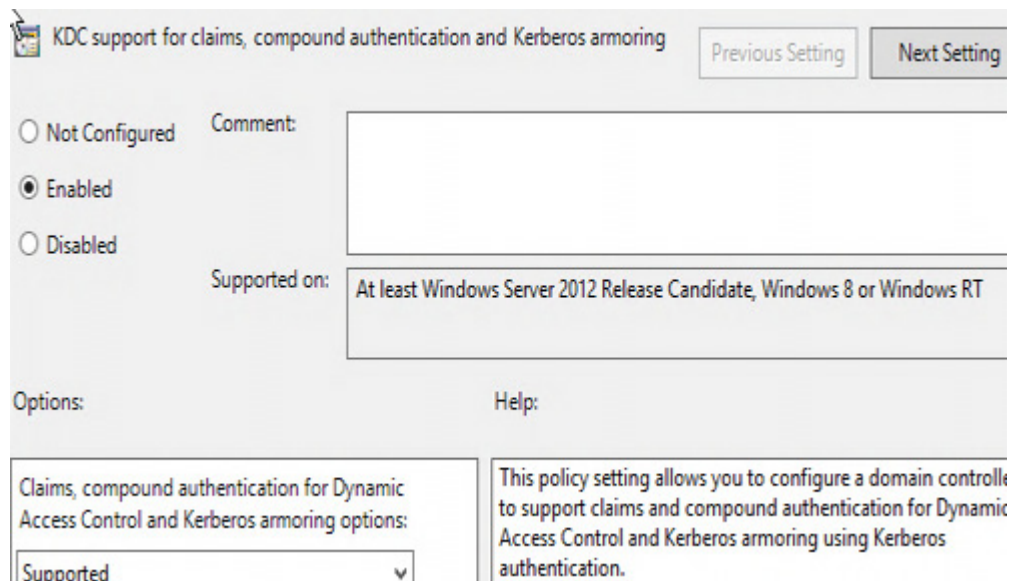
Aby dodatkowo zdefiniowane uzgodnienia Claim działały należy jeszcze uruchomić odpowiednią polisę. Z poziomu *Menadżera Serwera (Server Manager)* należy wybrać *Narzędzia (Tools)*, a następnie *Group Policy Management*.



Należy zedytować *Domyślną polisę domeny (Default Domain Policy)* i przejść kolejno *Computer Configuration > Policies > Administrative Templates > System > KDC*



Należy włączyć opcję ***KDC support for claims, compound authentication and Kerberos armoring***. W testowym środowisku są kontrolery domeny pracujące na Windows Server 2012 – zatem wybrano ustawienie Support w ***Claims, compound authentication for Dynamic Access Control and Kerberos armoring***. Modyfikacje tego ustawienia pokazuje rysunek poniżej.



## 10.4. Uprawnienia na systemie plików ReFS

System Windows Server 2012 wprowadza jeszcze jedną znaczącą nowość. Mianowicie nowy system plików. Choć NTFS sprawdza się dobrze to ma on już

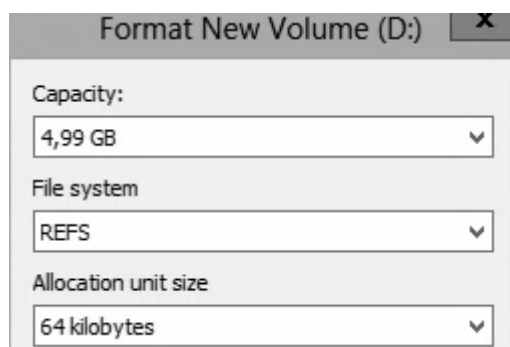


swoje lata, bo zadebiutował w 1993 roku. Nowy system plików trudno nazwać rewolucją w zarządzaniu danymi, jest to raczej ewolucja i spokojnie można by było go oznaczyć jako kolejną wersję NTFS'a. Właściwie to jest to bardziej dopracowany i zoptymalizowany NTFS.

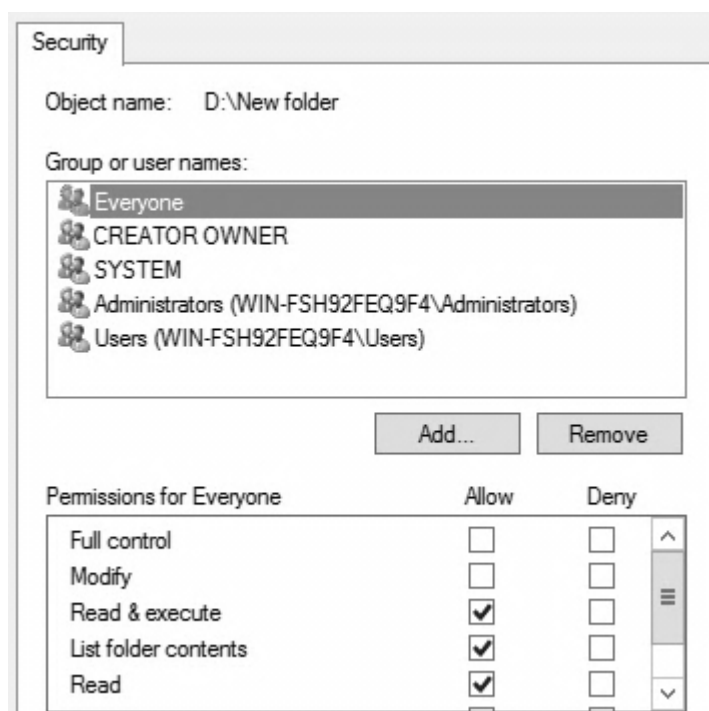
Nazwa ReFS to skrót od Resilient File System, czyli jak sama nazwa sugeruje odporny system plików. Jest on odporniejszy na uszkodzenia zarówno te logiczne jak i fizyczne nośników.

Oferuje on zarówno własne mechanizmy ochronne takie jak sumy kontrolne, rozproszony log transakcyjny, przeprowadzanie zapisu w separacji od oryginalnego pliku, itd., ale też współpracuje z mechanizmem Storage Spaces w Windows Server 2012. Dane i metadane są przechowywane w formie bardzo podobnej do relacyjnych baz danych. Dodatkowe zabezpieczenie stanowi kopiowanie przy zapisie, a także możliwość skasowania uszkodzonego pliku przez potrzeby odłączania dysku. Limity rozmiarów zostają zwiększone do 64 potęgi liczby 2. Z systemu NTFS pozostanie większość elementów interfejsu dostępu do danych, a co za tym idzie zmianom uległ głównie wewnętrzny mechanizm działania, a nie sposób zarządzania z punktu widzenia administratora systemu. Choć interfejs jest wręcz identyczny jak w przypadku NTFS, to zniknęły niektóre funkcje np. brakło szyfrowania EFS i kompresji plików bądź folderów. Na tą chwilę nie ma możliwości zainstalowania systemu operacyjnego na partycji ReFS. Microsoft prawdopodobnie chce system najpierw dokładnie przetestować dlatego wdraża go fazami. Najpierw nowy system plików zagości Windows Server 2012, potem na systemach klienckich, a na samym końcu zostanie możliwość pracy jako system plików na dysku rozruchowym.

W ramach ćwiczeń można jednak sformatować wybraną partycję do nowego systemu plików.



Gdy proces dobiegnie końca można wejść we właściwości jakiegoś folderu utworzonego na tym dysku, aby zobaczyć iż zarządzanie uprawnieniami na systemie plików ReFS nie różni się niczym od tego znanego z NTFS.

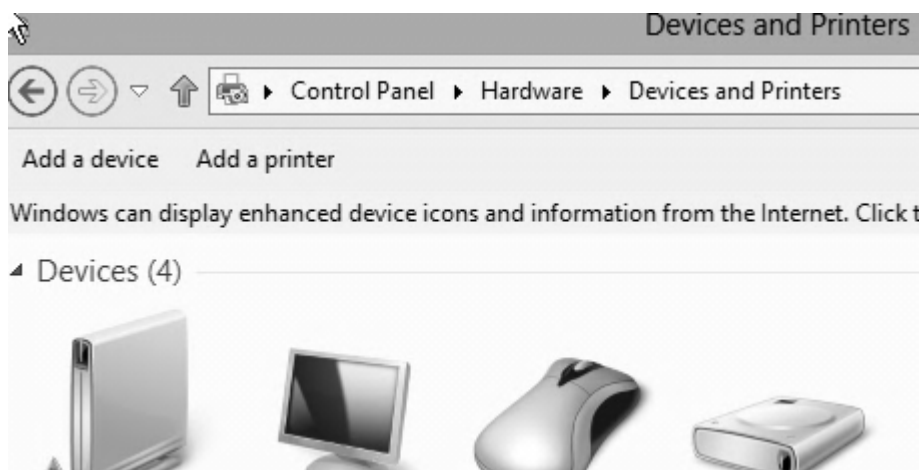


## 10.5. Zarządzanie drukarkami


Podobnie jak i w przypadku plików uprawnienia można również nakładać na urządzenia pracujące bądź udostępnione w sieci. Dzięki funkcjom dostępnym w Windows Server 2012 administrator może efektywnie zarządzać dostępem do urządzeń i drukarek, wydajnie je udostępniać zapewniając bezpieczeństwo działania i hermetyczność przekazywanych danych. Co więcej może on także nadawać różne priorytety dla mniej i bardziej uprzywilejowanych pracowników przedsiębiorstwa.

### 10.5.1. Instalowanie drukarek

W pierwszej kolejności należy otworzyć *Panel Sterownia (Control panel)*, wybrać *Sprzęt (Hardware)*, a następnie *Urządzenia i Drukarki (Devices and Printers)*.



Aby zainstalować drukarkę należy kliknąć przycisk *Dodaj Drukarkę (Add a printer)*. W pierwszej karcie kreatora system przeskanuje urządzenia w poszukiwaniu drukarki, jeżeli takowej nie znalazł bądź istnieje potrzeba instalacji drukarki, która fizycznie nie jest podpięta do komputera należy kliknąć opcję *Drukarka, którą pragnę zainstalować nie znajduje się na liście (The printer that I want isn't listed)*.

 Add Printer

No printers were found.

Printer Name	Address
--------------	---------

→ The printer that I want isn't listed

W kolejnej karcie kreatora w ramach ćwiczenia w środowisku wirtualnym powinno się wybrać opcję ***Dodaj drukarkę lokalną lub sieciową z ustawieniami ręcznymi*** (*Add a local printer or network printer with manual Settings*).

### Find a printer by other options

☐ Find a printer in the directory, based on location or feature

☐ Select a shared printer by name

Example: \\computername\printername or  
<http://computername/printers/printername/.printer>

☐ Add a printer using a TCP/IP address or hostname

☐ Add a Bluetooth, wireless or network discoverable printer

☒ Add a local printer or network printer with manual settings

Na kolejnej karcie warto zostawić ustawienia domyślne.

## Choose a printer port

A printer port is a type of connection that allows your computer to

☒ Use an existing port:

LPT1: (Printer Port)

☐ Create a new port:

Type of port:

Local Port

Z listy sterowników przykładowo można wybrać drukarkę firmy HP Color LaserJet 2700PS Class Driver.

## Install the printer driver



Choose your printer from the list. Click Windows Update to see more models.

To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
Fuji Xerox	HP Color LaserJet 2605 PS Class Driver
Generic	HP Color LaserJet 2700 PCL6 Class Driver
Gestetner	HP Color LaserJet 2700 PS Class Driver
HP	HP Color LaserJet 2800 series AiO PCL6 Class Driver
InfoPrint	

This driver is digitally signed.  
[Tell me why driver signing is important](#)

Windows Update

Na kolejnej karcie należy nadać drukarce nazwę np. Drukarka Szefa. Następnie można zainstalować raz jeszcze tą samą drukarkę nadając jej nazwę np. Drukarka Pracownika.

Type a printer name

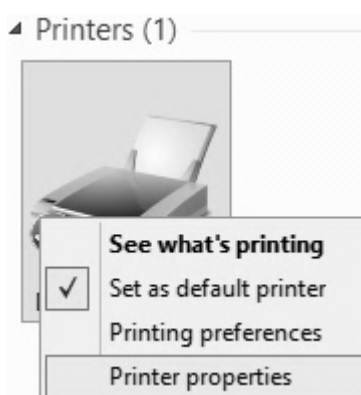
Printer name:

Drukarka Szefa

This printer will be installed with the HP Color LaserJet 2700 PS Class Driver driver.

### 10.5.2. Zarządzanie dostępem do drukarek sieciowych

Należy wejść we *Właściwości drukarki (Printer Properties)*.



W zakładce *Udostępnianie (Sharing)* można udostępnić drukarkę w sieci (analogicznie jak w przypadku plików), a także dodać sterowniki. Np. urządzenia często wymagają innych sterowników w zależności od wersji systemu Windows. Jeśli wszystkie zostaną tutaj dodane to instalacja na klienckich komputerach przebiegnie bez potrzeby dostarczania CD producenta.

Zakładka *Zaawansowane (Advanced)* pozwala na ograniczenie godzin w jakich można korzystać z urządzenia za pomocą opcji *Dostępna od (Available from)* (podobne ograniczenia można też nakładać na użytkowników). Jest także możliwość ustawiania priorytetów. Im wyższy priorytet tym urządzenie ważniejszy. O zastosowaniu było wspomniane wcześniej, za chwilę pokazane będzie jak wdrożyć system kolejowania zleceń.

General | Sharing | Ports | **Advanced** | Color Management | Security

☐ Always available  
☒ Available from 12:00 To 20:00  
 Priority: 50  
 Driver: Microsoft XPS Document Writer v4 New Driver...

---

☒ Spool print documents so program finishes printing faster  
     ☐ Start printing after last page is spooled  
     ☒ Start printing immediately  
☐ Print directly to the printer

---

☐ Hold mismatched documents  
☒ Print spooled documents first  
☐ Keep printed documents  
☒ Enable advanced printing features

Printing Defaults...    Print Processor...    Separator Page...

Zakładka **Zabezpieczenia (Security)** odpowiada za dostęp do zasobów drukarki. Działa to podobnie jak w przypadku plików.

General | Sharing | Ports | Advanced | Color Management | **Security**

Group or user names:

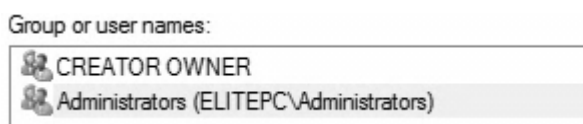
- Everyone
- ALL APPLICATION PACKAGES
- CREATOR OWNER
- Administrator
- Administrators (ELITEPC\Administrators)

Add... Remove

Z posiadaną wiedzą i dwa razy zainstalowaną tą samą drukarką można wdrożyć pewną ciekawą funkcjonalność. Należy wejść we właściwości drukarki szefa. W jej właściwościach ustawia się priorytet na większy niż był wcześniej czyli np. 50.

A screenshot of a printer's properties window. The 'Priority' field is highlighted, showing a numeric value of 50. To the right of the field is a small button with up and down arrows for adjusting the value.

W zabezpieczeniach zostawia się jedynie administratorów (zakłada się, że szef jest administratorem) oraz twórców-właścicieli.

A screenshot of the 'Group or user names' list in a printer's security settings. The list contains two entries: 'CREATOR OWNER' and 'Administrators (ELITEPC\Administrators)'. The 'Administrators (ELITEPC\Administrators)' entry is highlighted with a grey background.

Dla drukarki pracowników można zrobić dokładnie to samo z tym, że im można ustawić niższy priorytet np. 10.

Teraz na każdym komputerze szefa należy zainstalować drukarkę używając tej o wyższym priorytecie, a na innych komputerach tej o niższym. Oba sterowniki odnoszą się fizycznie do tego samego urządzenia, dzięki czemu wydruki szefa są ważniejsze. Gdy szef zapragnie coś wydrukować, wydruki pracowników zostaną wstrzymane na tak długo aż szef skończy drukować.

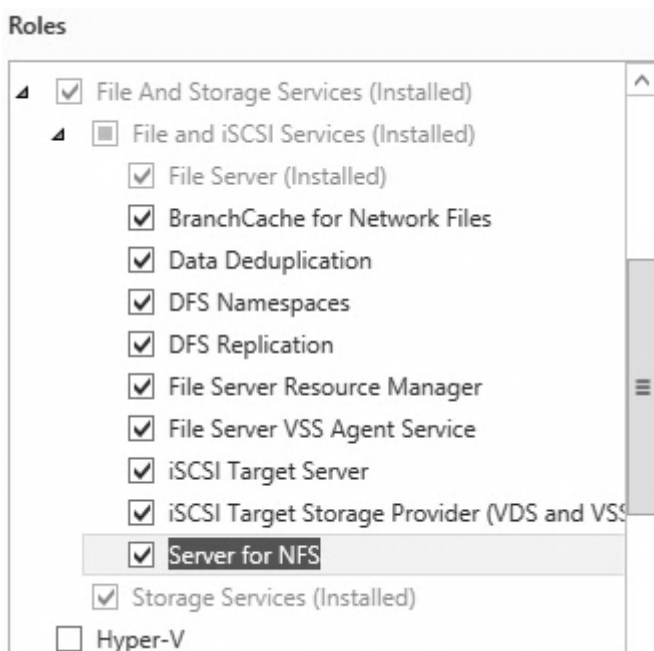


## 11. Serwer Plików

Serwer plików stanowi najbardziej potrzebną rolę serwera. Służy on nie tylko do scentralizowanego zarządzania danymi i dostępem do nich, ale także dba o bezpieczeństwo danych. Wiążą się z nim takie pojęcia jak rozproszony system plików, czy klastry, lecz w tym przypadku ćwiczeniowym zajęto się jego podstawowymi właściwościami.

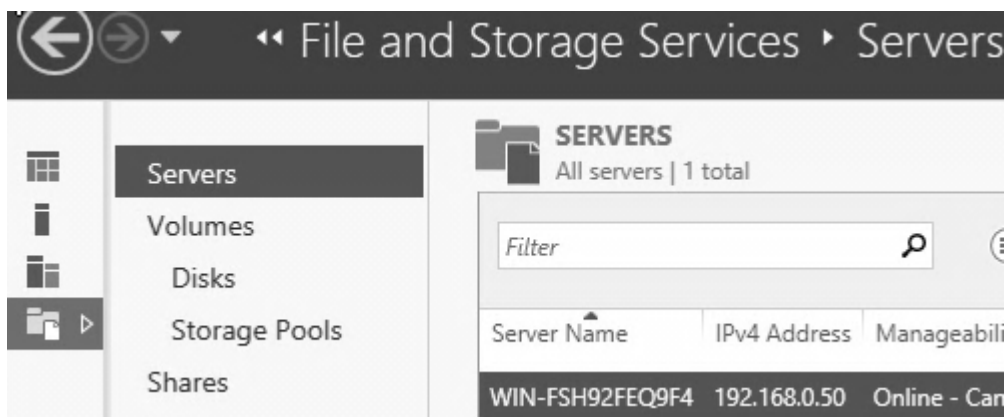
### 11.1. Instalacja roli Serwera Plików

Należy zatem wejść do kreatora dodawania ról i dodać składniki serwera plików, które nie zostały jeszcze zainstalowane. Część z nich (Storage Pool , Volumes, Shares , iSCSI Virtual Disks) standardowo jest zainstalowana, ponieważ nawet prosta funkcjonalność jak udostępnianie plików tego wymaga. Należy wybrać wszystkie brakujące składniki i kliknąć *Dalej (Next)*.



## 11.2. Zapoznanie z nowym podejściem do usług plików

Po instalacji w *Menadżerze Serwera (Server Manager)* pojawi się nowy wpis *Usługi plików (Files and Storage Services)*, po jego zaznaczeniu i wybraniu opcji *Serwery (Servers)* można dostać się do głównej konsoli zarządzania serwerami plików. W sekcji *Serwery (Servers)* widać listę serwerów i można nimi zarządzać.



Przesuwając ekran coraz niżej można znaleźć sekcję *Zdarzenia (Events)*, która wypisuje zdarzenia jakie zaszły na serwerze. Używając pobliskiego przycisku *Zadania (Tasks)* można zdefiniować jakiego rodzaju zdarzenia są istotne. Do wyboru są *błędy krytyczne (Critical)*, *błędy zwyczajne (Error)*, *ostrzeżenia (Warning)* oraz *informacje (Informational)*. Można też określić z jakiego przedziału czasu zdarzenia mają być prezentowane.

These settings determine how Server Manager gathers event data from servers in the server group that you are currently managing. Changes to defaults that significantly increase the number of events in the Events tile can result in delayed responses from Server Manager.

Show events with these severity levels




☒ Critical ☒ Error ☒ Warning ☐ Informational

Get events that have occurred within the past

24 hours ▼

Jeszcze niżej znajduje się sekcja **Usługi (Services)**. Są to usługi powiązane z serwerem plików, administrator może z tego poziomu podejrzeć co się z nimi dzieje i uruchomić je ponownie.




**SERVICES**  
All services | 8 total


Filter   

Server Name	Display Name	Service Name
WIN-FSH92FEQ9F4	File Server Storage Reports Manager	srmreports
WIN-FSH92FEQ9F4	Server	LanmanServer
WIN-FSH92FEQ9F4	Microsoft iSCSI Software Target	WinTarget
WIN-FSH92FEQ9F4	DFS Namespace	dfs
WIN-FSH92FEQ9F4	DFS Replication	DFSR

Poniżej znajduje się opcja **Best Practices Analyzer**, która sprawdza konfigurację serwera plików i wyświetla porady dotyczące ewentualnych zmian w jego konfiguracji. Pod guzikiem **Zadania (Tasks)** kryje się opcja BPA Scan, która przeanalizuje wybrany przez administratora serwer.

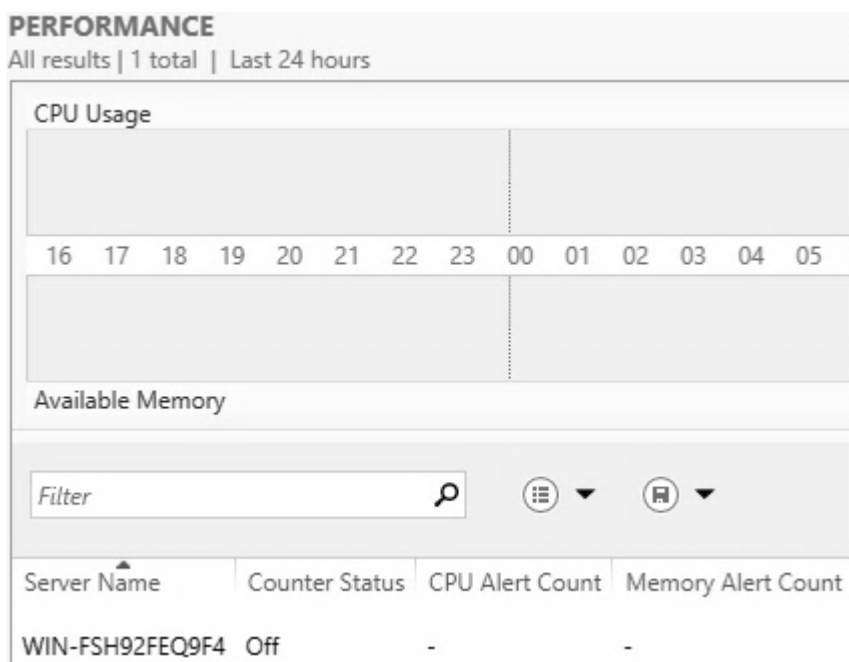
**BEST PRACTICES ANALYZER**  
Warnings or Errors | 5 of 142 total

Filter   

Filter applied.  Clear All

Server Name	Severity	Title
WIN-FSH92FEQ9F4	Warning	title EnableThroughputSchedule_Title
WIN-FSH92FEQ9F4	Warning	Enable Checksum Offload on a network adapter
WIN-FSH92FEQ9F4	Warning	Short file name creation should be disabled
WIN-FSH92FEQ9F4	Warning	Server for Network File System should be used on
WIN-FSH92FEQ9F4	Error	The domain functional level should be Windows :

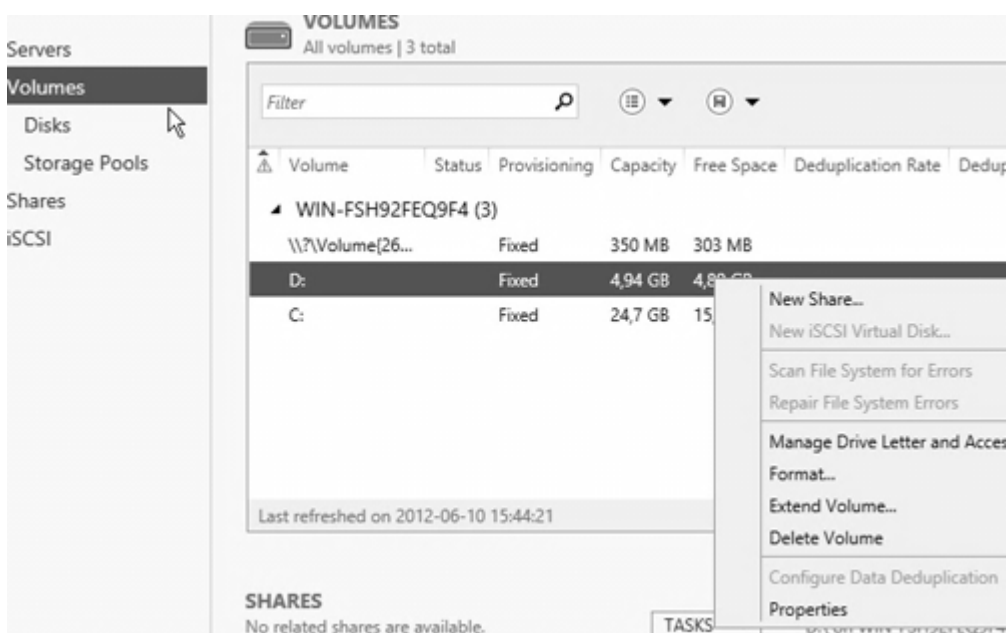
W sekcji *Wydajność (Performance)* znajduje się *Monitor Wydajności (Performance Monitor)*. Do jego funkcjonalności zalicza się tworzenie Alertów wydajności opcją *Konfiguruj Alerty Wydajności (Configure Performance Alerts)*.



Na samym dole okna znajduje się sekcja Roles and Features gdzie wypisane są składniki serwera plików jakie funkcjonują na nim. Wśród ról można znaleźć m.in. elementy, które wcześniej zostały już zainstalowane tj. File Server, który w systemie Windows odpowiada za udostępnianie plików w sieci, BranchCache for Network Files, czyli sieciowe buforowanie plików za pomocą technologii BranchCache, Data Duplication, który skanuje dyski twarde w poszukiwaniu duplikatów plików po to, aby je skasować, DFS Name Spaces, DFS Replication odpowiedzialna za replikację danych pomiędzy rozproszonymi serwerami, File Server Resource Manager będącą przystawką do bardziej zaawansowanego zarządzania udziałami, File Server VSS Agent Service agent niezbędny do archiwizacji używanych plików przez inne aplikacje, SI Target Server, Server for NFS służący do udostępniania plików komputerów bazujących na Unixie oraz Storage Service odpowiedzialny za obsługę

urządzeń fizycznych.

Po kliknięciu w menu na **Woluminy (Volumes)** zostanie się przeniesionym do ekranu, w którym ma się podgląd na woluminy istniejące na danym serwerze. Poprzez menu kontekstowe wolumin można naprawić, przeskanować, stworzyć na nim nowy udział, sformatować itp. Jest też podgląd jego podstawowych parametrów, a także co ważniejsze, w sekcji **Udziały (Shares)** znajduje się lista wszystkich udziałów sieciowych jakie się na nim znajdują.

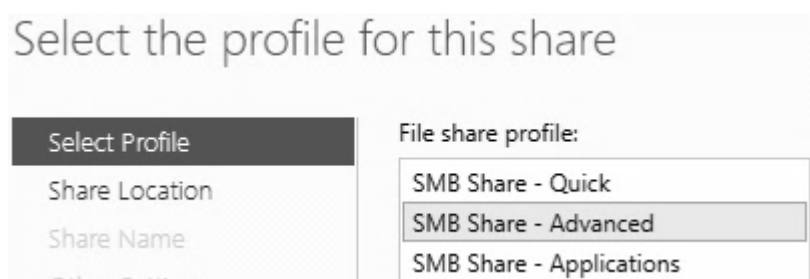


Należy kliknąć przycisk **Nowy Udział (New Share)** w obrębie sekcji **Udziały (Shares)**.

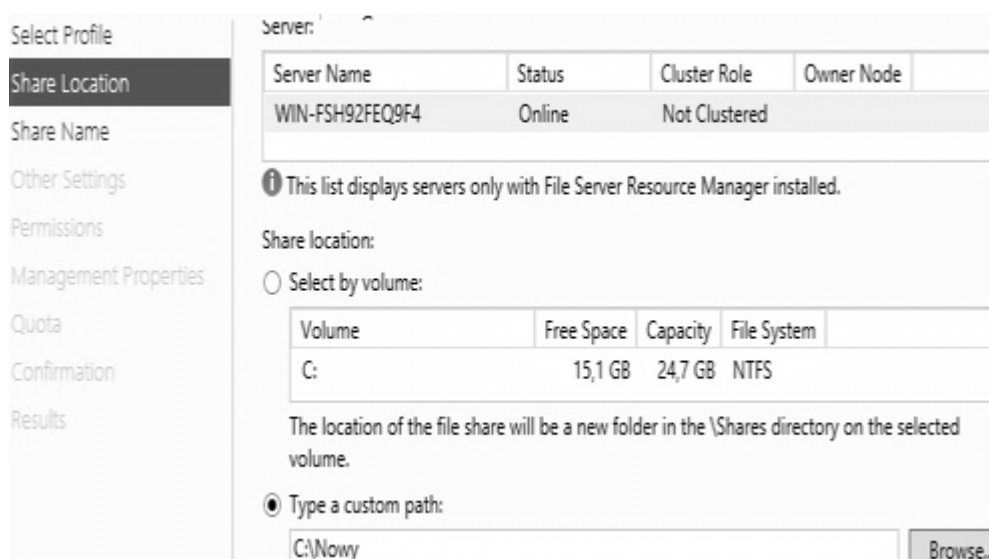


Pojawi się kreator udostępniania, który pozwala wybrać kilka opcji. Te oznaczone

przypisem *Szybkie (Quick)* pozwalają szybko udostępnić udział protokołem SMB (dla Windows) lub NFS (dla UNIX). Opcje *Zaawansowane (advanced)* pozwalają dodatkowo w kreatorze zarządzać quotami oraz właściwościami udziału. Istnieje jeszcze udział sieciowy dla aplikacji. Jest on dostosowany do tworzenia udziałów z ustawieniami odpowiednimi dla serwerów aplikacji, serwera Hyper-V czy baz danych. W ramach ćwiczeń zostanie wybrana zaawansowana droga kreatora dla udziału SMB tj. **SMB Share – Advanced**.



W kolejnym oknie należy wybrać serwer, na którym dany udział ma zostać utworzony, a także zdefiniować czy udziałem będzie cały dysk twardy czy jedynie jakiś folder. W przykładzie poniżej zdecydowano się jedynie na folder.



W następnej kolejności należy określić nazwę dla udziału sieciowego, można zaopatrzyć go w opis, a także konieczne jest zdefiniowanie jego ścieżki sieciowej. Praktycznie wszystkie pola poza opisem domyślnie powinny zostać automatycznie wygenerowane.

Select Profile	Share name: Nowy
Share Location	Share description: jakiś opis
<b>Share Name</b>	
Other Settings	
Permissions	
Management Properties	Local path to share: C:\Nowy
Quota	<b>i</b> If the folder does not exist, the folder is created.
Confirmation	Remote path to share: \\WIN-FSH92FEQ9F4\Nowy
Results	

Kolejnym krokiem będzie zdefiniowanie dodatkowych ustawień. Można włączyć **Listowanie folderu oparte na uprawnieniach użytkownika (Enable access based enumeration)**. Rezultat będzie taki, że użytkownik będzie miał wgląd jedynie do tych plików i folderów, do których ma uprawnienia dostępowe.

Opcja **Pozwól na buforowanie udziału (Allow Caching of share)**, pozwoli na buforowanie zawartości udziału sieciowego tak, aby był on dostępny, nawet jeżeli użytkownik jest offline. Dodatkowo można włączyć usługę **BranchCache**, wymaga ona jednak globalnej dostępności IPv6.

Ostatnią opcją jest **Szyfrowany dostęp (Encrypt data access)**, która to spowoduje szyfrowanie danych podczas połączenia pomiędzy klientem i serwerem w celu uniknięcia przechwycenia danych przez niepowołaną osobę.

☒ **Enable access-based enumeration**  
 Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☒ **Allow caching of share**  
 Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

☐ **Enable BranchCache on the file share**  
 BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.  
[Learn more about configuring SMB cache settings](#)

☒ **Encrypt data access**  
 When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

W kolejnym oknie można podejrzeć uprawnienia, jakie będą standardowo przypisane. Przyciskiem **Dostosuj Uprawnienia** (*Customize Permissions*) można je modyfikować.

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Read Only

Folder permissions:

Type	Principal	Access	Applies To
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files

[Customize permissions...](#)

W kolejnym oknie kreatora należy określić przeznaczenie udziału, czyli to, jakiego rodzaju dane będzie on przechowywał.



The Folder Usage property specifies the purpose of the folder and the type is used by data management policies such as classification rules.

Select the Folder Usage value for this folder:

- ☐ User Files
- ☒ Group Files
- ☐ Application Files
- ☐ Backup and Archival Files

W następnym oknie można nałożyć ograniczenie co do ilości danych, jakie może wgrać użytkownik, czyli tzw. Quoty. Można wybrać dowolną ze wcześniej zdefiniowanych Quot lub utworzyć nową.

☐ Do not apply a quota

☒ Apply a quota based on the template:

100 MB Limit

200 MB Limit Reports to User

Monitor 200 GB Volume Usage

Monitor 500 MB Share

200 MB Limit with 50 MB Extension

250 MB Extended Limit

Summary of template:




Template name:	100 MB Limit
Limit:	100 MB Hard
Notification thresholds:	3
	85% - Event
	95% - Email, Event
	100% - Email, Event

Na oknie podsumowania należy kliknąć **Utwórz (Create)**.

Confirm that the following are the correct settings,

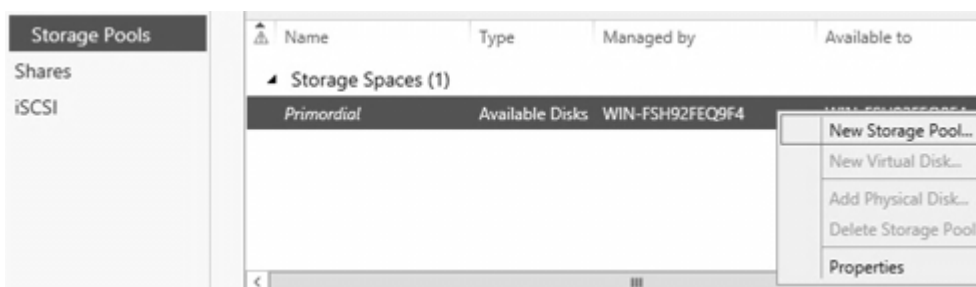
<b>SHARE LOCATION</b>	
Server:	WIN-FSH92FEQ9F4
Cluster role:	Not Clustered
Local path:	C:\Nowy
<b>SHARE PROPERTIES</b>	
Share name:	Nowy
Description:	jakiś opis
Protocol:	SMB
Access-based enumeration:	Enabled
Caching:	Enabled
BranchCache:	Disabled
Encrypt data:	Enabled
<b>MANAGEMENT PROPERTIES</b>	
Folder usage:	Group Files
Quota template:	None applied

Następnie należy powrócić do widoku *Menadżera Serwera (Server Manager)* i z *Woluminów (Volumes)* przejść na *Dyski (Disks)*. Widok jego zawartości jest analogiczny do Woluminów jednak dotyczy już fizycznie całych dysków.

Servers Volumes <b>Disks</b> Storage Pools Shares iSCSI	<b>DISKS</b> All disks   2 total				
	Filter <input type="text"/>   				
	Disk ID	Virtual Disk	Status	Capacity	Unallocated
	▲ WIN-FSH92FEQ9F4 (2)				
	0		Online	25,0 GB	0,00 B
	1		Online	5,00 GB	1,00 MB

### 11.3. Storage Pools

W menu po lewej stronie należy przejść do Storage Pools. Jeżeli komputer spełnia minimalne wymagania sprzętowe wewnątrz okna powinny być dostępne jakieś urządzenia magazynujące. Po kliknięciu w któreś z nich należy wybrać **New Storage Pool**.



Storage Pools pozwala na połączenie przestrzeni dyskowych relacjami, aby zapewnić zarówno wydajność jak i bezpieczeństwo wraz z wysoką dostępnością danych. W ramach ćwiczenia zostanie stworzony jeden wirtualny dysk z kilku fizycznych dysków. Nie może być to używany dysk, na którym zainstalowany jest już system operacyjny, więc wymagany jest przynajmniej jeden odrębny dysk na głównym serwerze lub dwa w przypadku użycia trybu wysokiej dostępności 2-way Mirror, który klonuje zawartość dysku i trzy w trybie 3-way Mirror, gdzie na każdym przechowywana jest kopia danych. Takie dyski powinny być czyste i nie sformatowane o rozmiarze minimum 10GB. Dyski muszą być zainicjowane i online. Mogą być podłączone fizycznie do komputera przez SCSI, iSCSI, SAS czy nawet USB.

Po pominięciu karty powitalnej należy wprowadzić nazwę i ewentualnie opis.

## Specify a storage pool name and subsystem

Before You Begin

**Storage Pool Name**

Physical Disks

Confirmation

Results

Name:

Description:

Select the group of available disks (also known as a storage subsystem):

Managed by	Available to
WIN-FSH92FEQ9F4	WIN-FSH92FEQ9F4

W następnym oknie kreatora zaznacza się dyski, które mają być użyte.

## Select physical disks for the storage pool

Before You Begin

Storage Pool Name

**Physical Disks**

Confirmation

Select unused physical disks for the storage pool. You can also select disks for managed disks.

Physical disks:

<input checked="" type="checkbox"/>	Slot	Name	Capacity	Free Space
<input checked="" type="checkbox"/>		PhysicalDisk1 (...)	11,0 GB	11,0 GB

Na koniec należy kliknąć **Utwórz (Create)**.

## Confirm that the following are the correct settings,

STORAGE POOL LOCATION

Server: WIN-FSH92FEQ9F4

Cluster role: Not Clustered

Storage subsystem: Storage Spaces

STORAGE POOL PROPERTIES

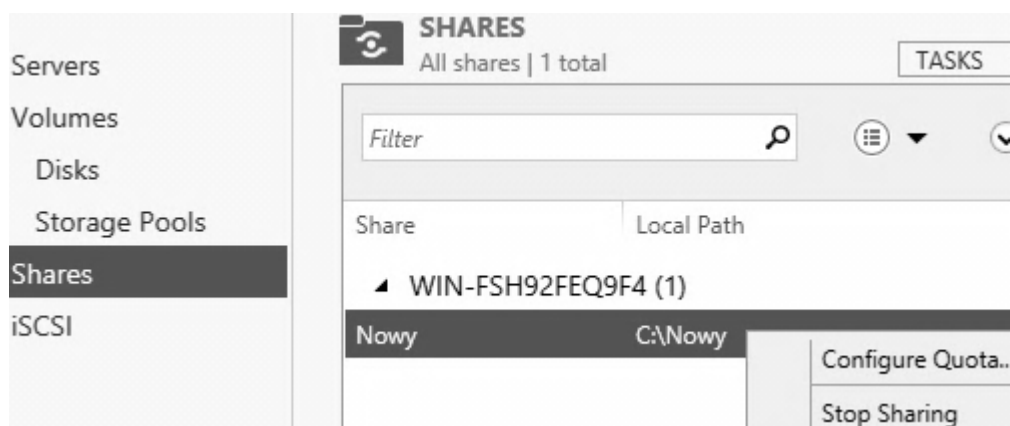
Name: Pool

Capacity: 11,0 GB

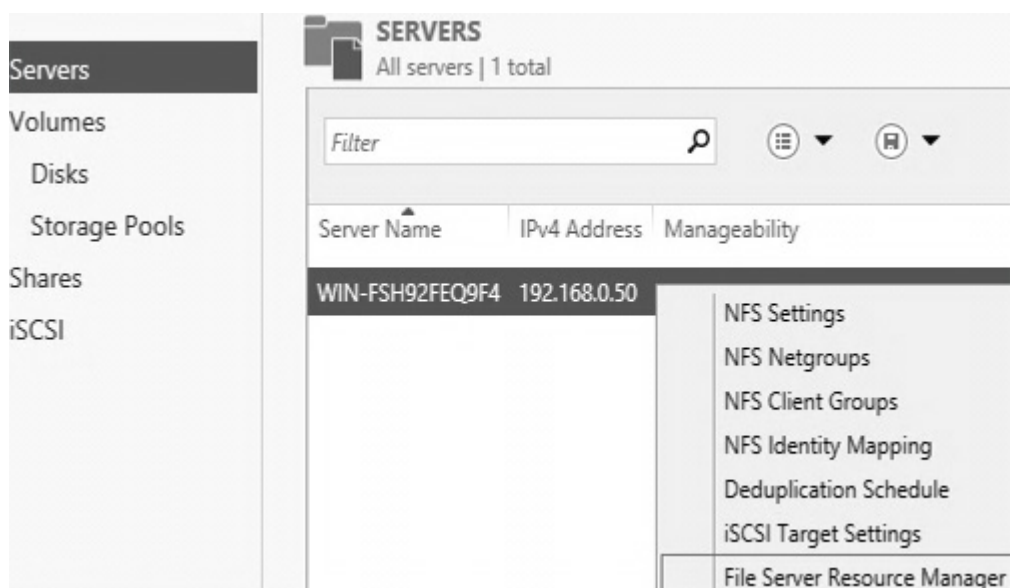
PHYSICAL DISKS

PhysicalDisk1 (WIN-FSH92FEQ9F4) 11,0 GB

Klikając przycisk **Udostępnione (Shares)** znajdujący w menu się po lewej stronie można przenieść się do widoku, w którym widać będzie wszystkie udziały sieciowe na danym serwerze zebrane w jednym miejscu. W każdej chwili można modyfikować Quoty, wyłączyć udostępnianie czy edytować właściwości udziału.

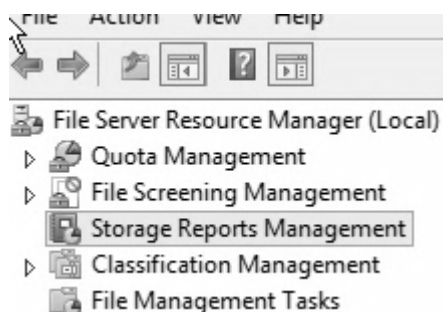


Powróciwszy do pierwszego okna oznaczonego jako **Serwery (Servers)** i po kliknięciu prawym przyciskiem myszy na serwerze należy wybrać **File Server Resource Manager**.



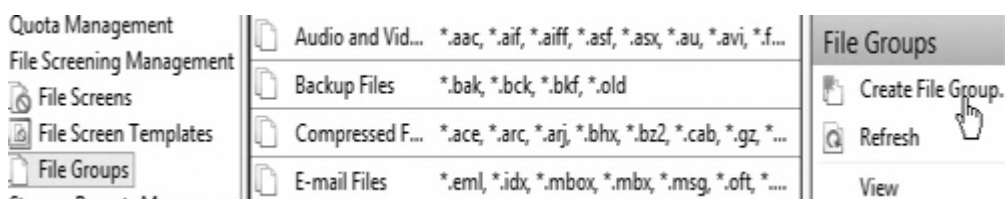
## 11.4. Zarządzanie przez Menadżera Serwera Plików

Skupiając się na *Menadżerze Zasobów Serwera Plików (File Server Resource Manager)*, raporty o tym, jakie pliki i w jaki sposób były używane można obejrzeć w sekcji *Zarządzanie Raportami Magazynowymi (Storage Reports Management)*.



### 11.4.1. Zarządzanie Osłonami Plików

*File Screening Management*, czyli Zarządzanie Osłonami Plików z kolei pozwala nie tylko monitorować, ale na przykład zakazywać otwierania jakichś rodzajów plików. W pierwszej kolejności należy utworzyć *Grupę plików (File Group)*. W menu z lewej strony należy wybrać *Grupy plików (File Groups)*, a następnie w menu po prawej opcję *Utwórz Grupę Plików (Create File Group)*.



W oknie jakie się pojawi należy podać nazwę dla tworzonej grupy plików, a także rozszerzenia plików jakich będzie ona dotyczyć w postaci \*.rozszerzenie.

Settings

File group name:











To select a set of files, type a file name pattern, and click Add.  
 Examples: \*.exe or Q4FY2002\*.\*

Files to include:

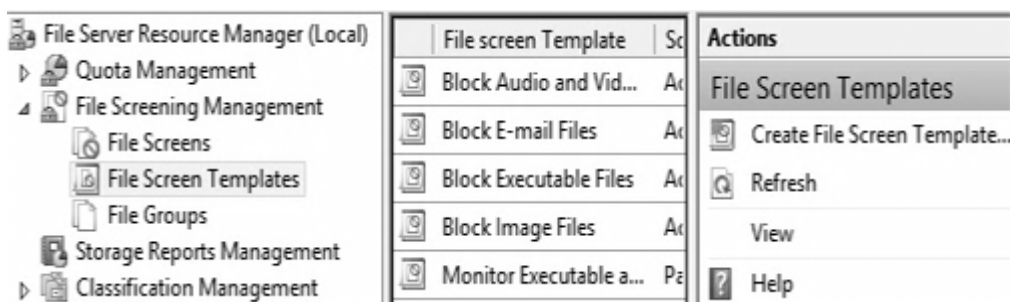
\*.plik

Files to exclude:

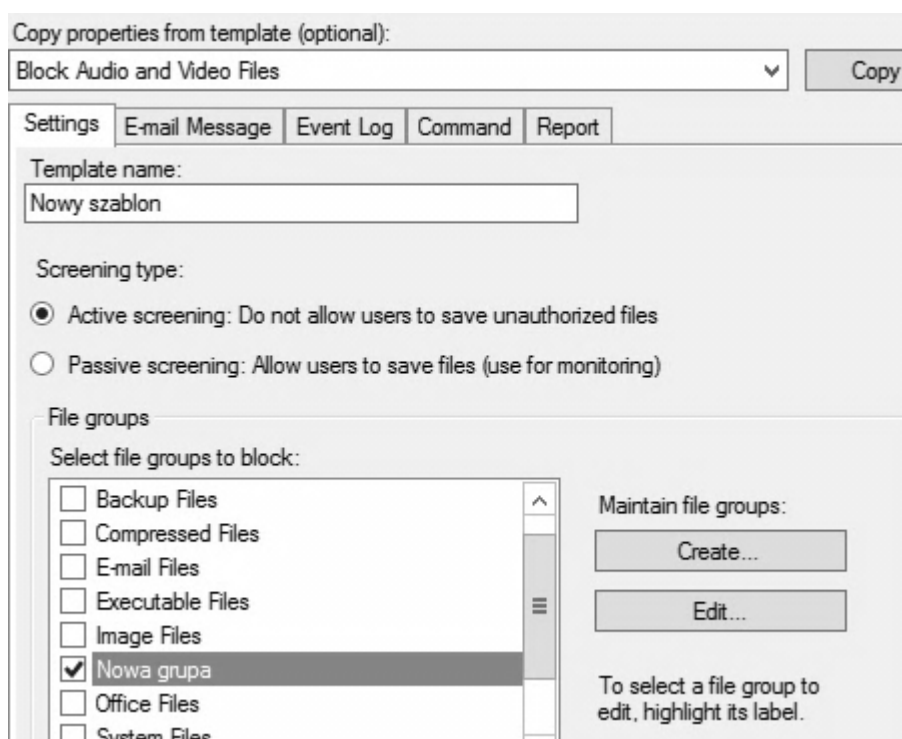
Po kliknięciu **OK** grupa pojawi się na liście.

	Compressed F...	*.ace, *.arc, *.arj, *.bhx, *.bz2, *.cab, *.gz, *...
	E-mail Files	*.eml, *.idx, *.mbox, *.mbx, *.msg, *.oft, *...
	Executable Files	*.bat, *.cmd, *.com, *.cpl, *.exe, *.inf, *.js, ...
	Image Files	*.bmp, *.dib, *.eps, *.gif, *.img, *.jif, *.jpe...
	Nowa grupa	*.plik
	Office Files	*.accdb, *.accde, *.accdr, *.accdt, *.adn, *...
	System Files	*.acm, *.dll, *.ocx, *.sys, *.vxd
	Temporary Files	*.temp, *.tmp, ~*
	Text Files	*.asc, *.text, *.txt
	Web Page Files	*.asp, *.aspx, *.cgi, *.css, *.dhtml, *.hta, *...

Kolejnym krokiem będzie utworzenie szablonu osłony plików. Należy kliknąć więc na **Szablony osłony plików (File Screen Templates)** i w menu po prawej stronie wybrać opcję **Utwórz szablon osłony plików (Create File Screen Template)**.

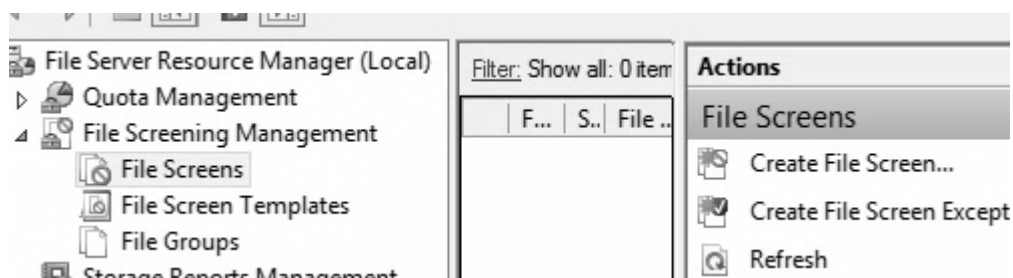


W oknie, które się pojawi należy zdefiniować nazwę dla szablonu oraz to, czy będzie to osłanianie **Aktywne (Active Screening)** czy **Pasywne (Passive Screening)**. Aktywne nie pozwoli użytkownikom wgrać do danego folderu określonych przez administratora typów plików, z kolei pasywne pozwoli, lecz wyśle mu informacje o tym, więc będzie służyło bardziej do monitoringu. To, czy zostanie wysłany email z notyfikacją czy też informacja trafi do logów, definiuje się w zakładkach okna. W ćwiczeniu tym zostanie wybrane osłanianie Aktywne.

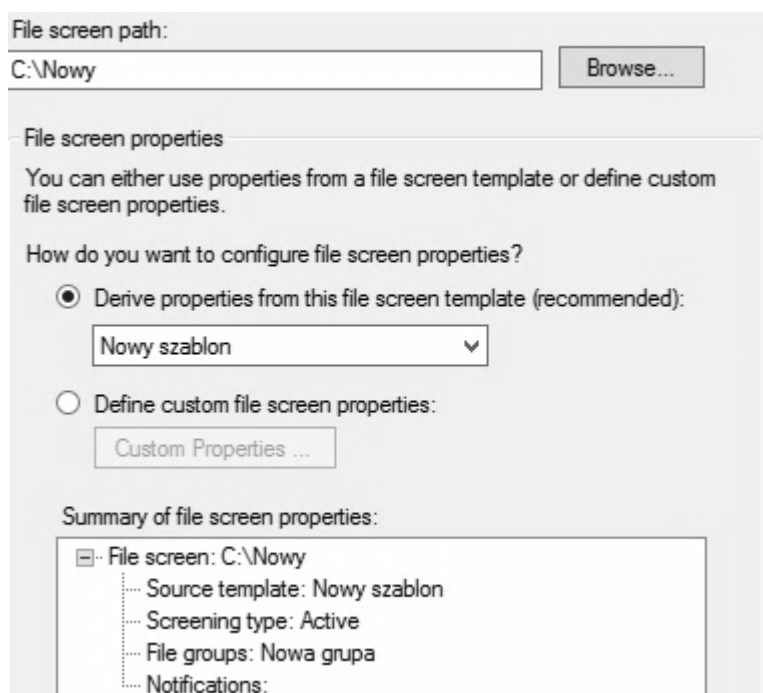




Na koniec należy zaznaczyć **Oslony Plików (File Screen)** i w menu po prawej stronie wybrać **Utwórz osłonę plików (Create file Screen)**.

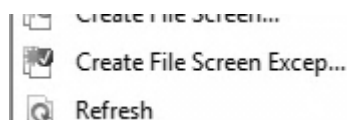


W oknie, jakie się pojawi należy wybrać udostępniony folder jakiego ma dotyczyć osłona oraz jaka osłona jest na niego narzucana. Wybór finalizuje się przyciskiem **Utwórz (Create)**.



Od tej pory użytkownicy w wybranym folderze nie będą mieli prawo zapisywania plików o określonych rozszerzeniach. Na dany folder można narzucić kilka różnych osłon, powtarzając kroki, które zostały pokazane powyżej. Wewnątrz danego

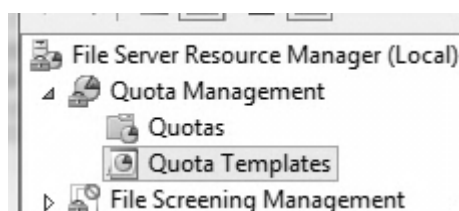
folderu można także stworzyć wyjątek od osłony jeżeli w pojedynczym folderze ma zaistnieć pozwolenie na zapisywanie zabronionych plików przyciskiem **Stwórz wyjątek osłony plików (Create File Screen Exception)**.



Przykładem z życia wziętym dla zastosowania takiego rozwiązania jest na przykład zakazanie włączania plików wykonywalnych, dzięki czemu użytkownicy nie będą w stanie instalować niepożądanych aplikacji.

### 11.4.2. Zarządzanie Przydziałami

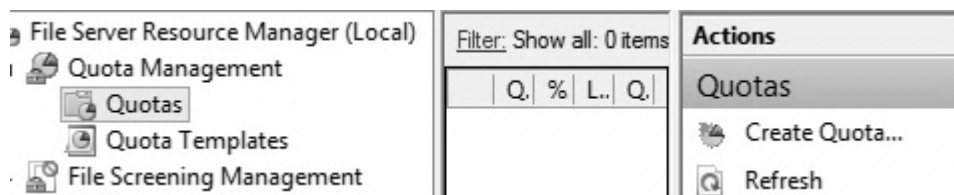
Zarządzanie przydziałami to także bardzo pożyteczna funkcjonalność. Wcześniej został nałożony limit na rozmiar plików użytkownika na dysku. Co jednak jeśli limit miałby dotyczyć jednego użytkownika, albo konkretnego katalogu, lub użytkownicy mieliby mieć różne limity? Kilka działów wcześniej został uruchomiony serwer FTP, wypadaloby jednak jakoś ograniczyć użytkownikom powierzchnię dyskową jaką mogą oni wykorzystać. Tu właśnie można to zrobić. Istnieją oczywiście predefiniowane szablony, są one raczej poglądowe i przykładowe. To są te same szablony, które kilka stron wcześniej zostały użyte. Aby utworzyć własny szablon w lewym menu należy rozwinąć **Zarządzanie Przydziałami (Quota Management)** i kliknąć **Szablony Przydziałów (Quota Templates)**.



W menu po prawej stronie należy wybrać opcję **Utwórz Szablon Przydziału (Create Quota Template)**. Pojawi się okno, w którym nadaje się szablonowi nazwę, następnie w sekcji Space limit określa się rozmiar dozwolonej pamięci i definiuje

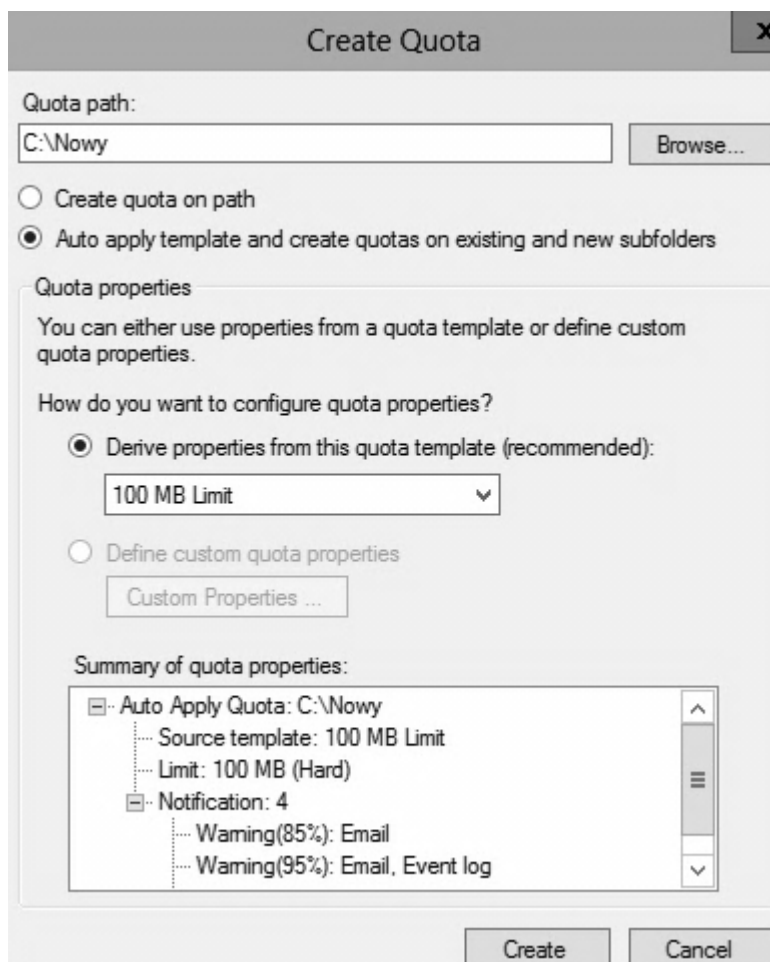
czy przydział będzie *Sztywny (Hard Quota)* czy *Elastyczny (Soft Quota)*. Pierwszy nie pozwoli wgrać więcej danych niż zakłada limit, drugi pozwoli, lecz będzie komunikował o tym użytkownika. Wybrana zostanie Hard Quota i nadany limit np. 2 GB.

Z drzewa kategorii z lewej strony należy wybrać *Przydziały (Quotas)*, a następnie po prawej kliknąć w przycisk *Utwórz przydział (Create Quota)*.



Należy wybrać ścieżkę do jakiegoś katalogu z przygotowanego szablonu. Użytkownicy teraz nie będą mogli przechowywać tam więcej danych niż przewiduje limit np. jeżeli limit wynosi 100MB, to każdy użytkownik może wgrać maksymalnie 100MB własnych danych. Warto też zaznaczyć opcję *Auto apply template and*

*create quotas on existing and new subfolders*, ponieważ dzięki temu przydziały będą również nakładane na nowo tworzone foldery.



**Create Quota**

Quota path:  
C:\Nowy Browse...

☐ Create quota on path  
☒ Auto apply template and create quotas on existing and new subfolders

**Quota properties**  
You can either use properties from a quota template or define custom quota properties.

How do you want to configure quota properties?

☒ Derive properties from this quota template (recommended):  
100 MB Limit

☐ Define custom quota properties  
Custom Properties ...

**Summary of quota properties:**

- [-] Auto Apply Quota: C:\Nowy
  - Source template: 100 MB Limit
  - Limit: 100 MB (Hard)
  - [-] Notification: 4
    - Warning(85%): Email
    - Warning(95%): Email, Event log

Create Cancel

## 12. Praca zdalna

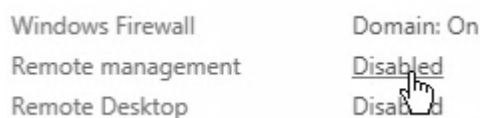
Serwer powinien dawać administratorowi możliwość zarządzania zdalnego. Dlatego też skonfigurowane zostanie połączenie pulpitu zdalnego. Proces ten jest relatywnie łatwy, a funkcja pulpitu zdalnego dobrze zaimplementowana. Dzieje się tak, ponieważ elementy interfejsu Windows zawierają się już w systemach czy aplikacjach klienckich. Co więcej klienta dostępu zdalnego Microsoft przygotował także na inne platformy jak Linux, OS X, a nawet urządzenia mobilne, dzięki czemu w awaryjnej sytuacji można odratować serwer nawet przez komórkę jadąc pociągiem.

### 12.1. Wstępna konfiguracja serwera

Należy kliknąć na *Serwer Lokalny (Local Server)* w *Menadźerze Serwera (Server Manager)*.



Zostanie wybrane i uruchomione *Zdalne Zarządzanie (Remote Management)* znajdujące się po prawej stronie okna.



W okienku, które się pojawi należy zaznaczyć *Zezwalaj na zdalne zarządzanie tym serwerem z innych komputerów (Enable remote management of this server from other computers)*, co pozwoli na zarządzanie tą maszyną choćby przez *Menadżera Serwera (Server Manager)* uruchomionego na innym komputerze bądź za pomocą

PowerShella.

☒ Enable remote management of this server from other computers.

Enable applications or commands that require Windows Management Instrumentation (WMI) and Windows PowerShell remote access to manage this server.

If you disable remote management, applications or commands that require WMI or Windows PowerShell remote access will fail.

You might not be able to manage this computer remotely from a different local subnet because of firewall settings.

Local administrator accounts other than the built-in Administrator account may not have rights to manage this computer remotely, even if remote management is enabled.

Tuż poniżej należy uruchomić dostęp poprzez połączenie **Pulpitu zdalnego (Remote Desktop)**.

Remote management	Enabled
Remote Desktop	<u>Disabled</u>
NIC Teaming	Disabled

W oknie, które się pojawi należy wybrać opcję **Pozwól na zdalne łączenie z tym komputerem (Allow remote connections to this computer)**. Można także zaznaczyć zgodę na połączenia zdalne wyłącznie z komputerów, które są zautentykowane na poziomie sieci, co zwiększa bezpieczeństwo.

Remote Desktop

Choose an option, and then specify who can connect.

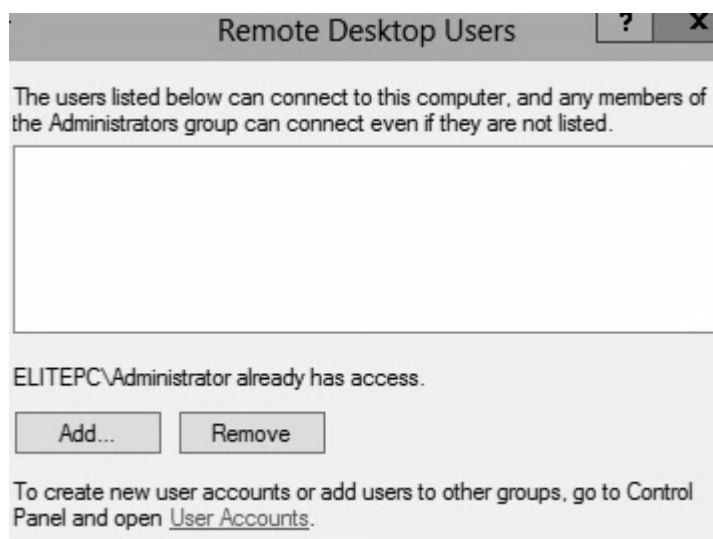
☐ Don't allow remote connections to this computer

☒ Allow remote connections to this computer

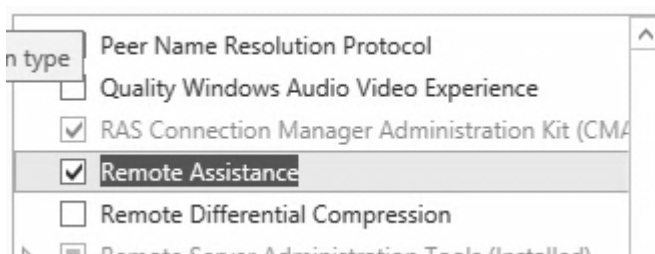
☒ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

[Help me choose](#) Select Users...

Kliknąwszy w opcję **Wybierz użytkowników (Select Users)** można dodać użytkowników, którzy będą mieli możliwość zdalnego łączenia się z tą maszyną. Administratorów nie trzeba tu wprowadzać, ponieważ oni już domyślnie mają stosowne uprawnienia.

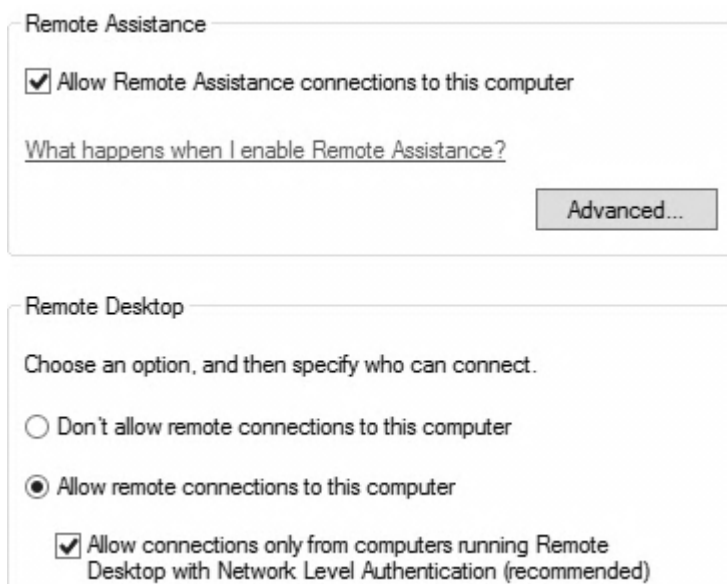


Zanim się przejdzie do konfiguracji klienta i testowania połączenia warto zainstalować i skonfigurować pomoc zdalną. W pierwszym kroku należy doinstalować funkcję **Zdalna Pomoc (Remote Assistance)**.



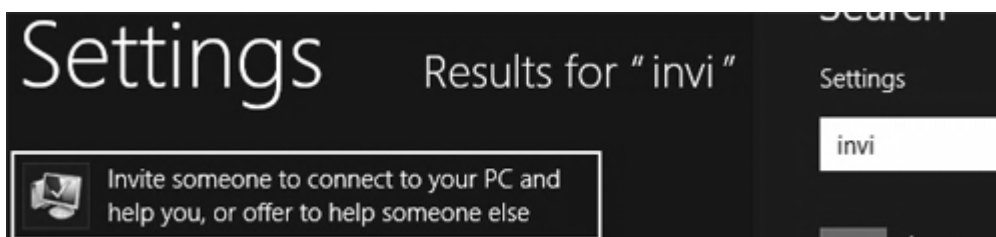
Gdy proces instalacji dobiegnie końca należy wrócić do okna, w którym został uruchomiony **Pulpit Zdalny (Remote Desktop)**. Teraz będzie możliwość uruchomienia również **Zdalnej Pomocy (Remote Assistance)**. Należy zaznaczyć opcję **Zezwól na połączenia zdalnej pomocy z tym komputerem (Allow Remote**

*Assistance connections to this computer).*



## 12.2. Korzystanie z Pomocy Zdalnej

Zanim przystąpi się do prezentacji działania systemu po stronie klienta należy wysłać zaproszenie do pomocy. W wyszukiwarce dla sekcji *Ustawienia (Settings)* należy wpisać słowo *Zaproś (Invite)* i z listy wyników wybrać *Zaproś kogoś do połączenia z twoim PC na pomoc tobie, lub zaoferuj swoją pomoc komuś innemu (Invite someone to connect to your PC and help you, or offer to help someone else)*.



Zostanie otwarte nowe okno, w którym pojawiają się dwie opcje. Pierwsza to prośba o pomoc, druga to pomoc innej osobie. Dla przykładu zostanie wybrana opcja



pierwsza ***Zaproś kogoś komu ufasz żeby ci pomógł (Invite someone you trust to help you)***.

Do you want to ask for or offer help?

Windows Remote Assistance connects two computers so that one person can help tri problems on the other person's computer.

→ **Invite someone you trust to help you**  
Your helper can view your screen and share control of your computer.

→ **Help someone who has invited you**  
Respond to a request for assistance from another person.

Należy kliknąć przycisk ***Poproś kogoś komu ufasz o pomoc (Invite someone you trust to help you)*** znajdujący się w centrum ekranu. Pojawią się trzy opcje. Jedna z nich to stworzenie odpowiedniego pliku z danymi, który trzeba dostarczyć we własnym zakresie danej osobie (***Save this invitation as file***), kolejna opcja to zaproszenie poprzez e-mail (***Use email to sen dan invitation***), a ostatnia opcja to łatwe połączenie (***Use easy connect***).

How do you want to invite your trusted helper?

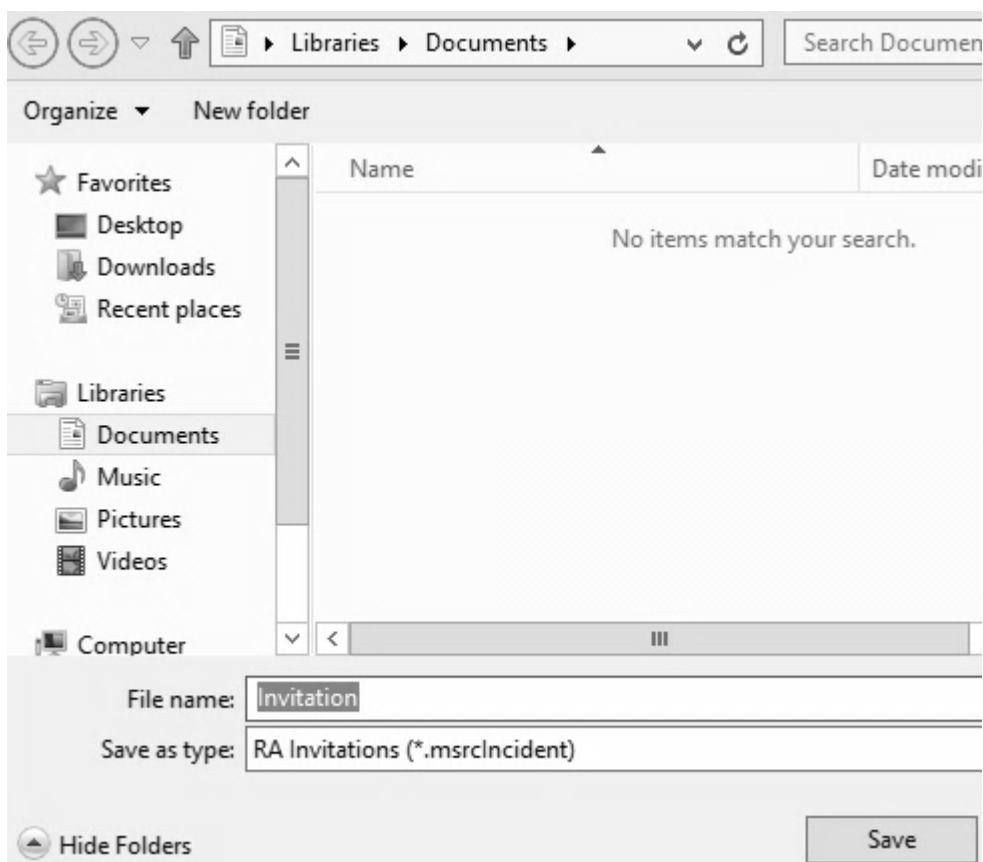
You can create an invitation and send it to your helper. You can also use Easy Connect to simplify connections to your helper.

→ **Save this invitation as a file**  
You can send this invitation as an attachment if you use web-based email.

→ **Use email to send an invitation**  
If you use a compatible email program this will start the email program and attach the invitation file.

→ **Use Easy Connect**  
Use this option if Easy Connect is also available to your helper.

Najwygodniej będzie oczywiście to zrobić zapisując zaproszenie jako plik. Potem go należy udostępnić po sieci i w przypadku książkowym zostanie użyty komputer zdalny.



Wygenerowane zostanie hasło, które trzeba ręcznie przekazać osobie, która będzie udzielała pomocy.

Give your helper the invitation file and password

**SC3DV8BQ5DTR**

Jeśli nie zostało to wcześniej zrobione, aby można było odnaleźć komputer w sieci należy na serwerze wprowadzić następujące ustawienia:

## Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private ▼

Guest or Public ▼

Domain (current profile) ▲

Network discovery ▼

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

☒ Turn on network discovery  
☐ Turn off network discovery

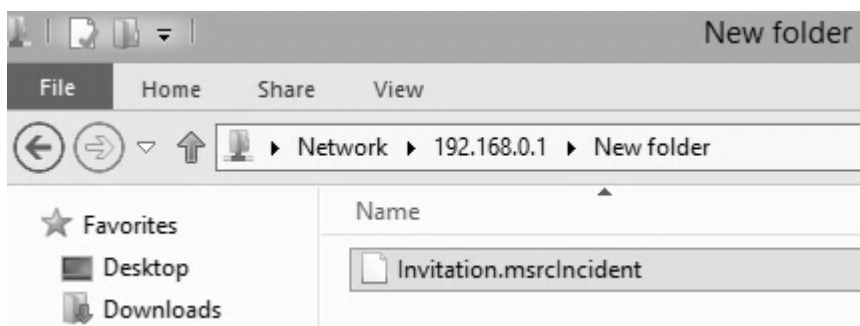
File and printer sharing ▼

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

☒ Turn on file and printer sharing  
☐ Turn off file and printer sharing

All Networks ▼

Należy udostępnić w sieci plik z zaproszeniem. Następnie należy wejść do udostępnionego folderu z drugiego komputera.



Należy wybrać udostępnione wcześniej zaproszenie i uruchomić je podwójnym kliknięciem. Trzeba pamiętać o tym, iż na zdalnym komputerze także musi być zainstalowana funkcja zdalnej pomocy. Będzie także konieczność wprowadzenia wygenerowanego na serwerze hasła.

Enter the password to connect to the remote computer

You can get this password from the person requesting assistance. A Remote Assistance session will start after you type the password and click OK.

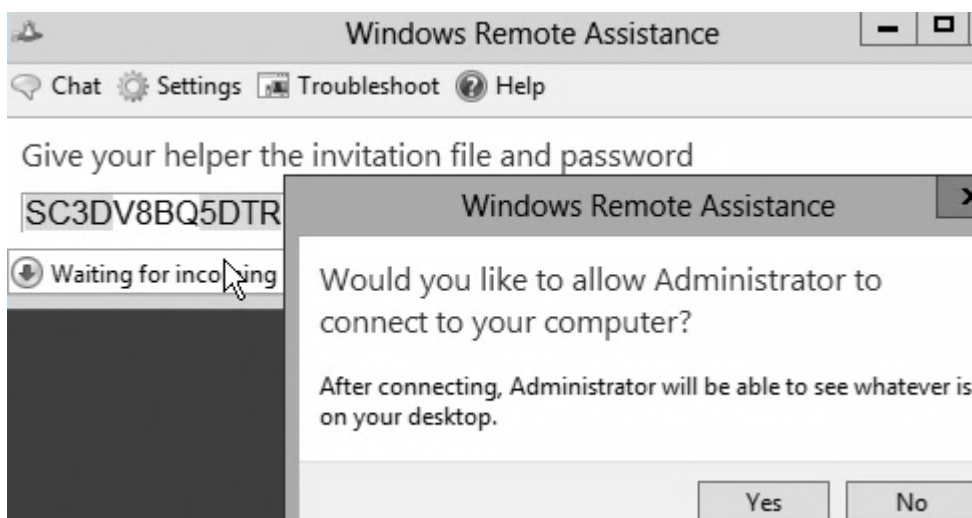
Enter password:

SC3DV8BQ5DTR

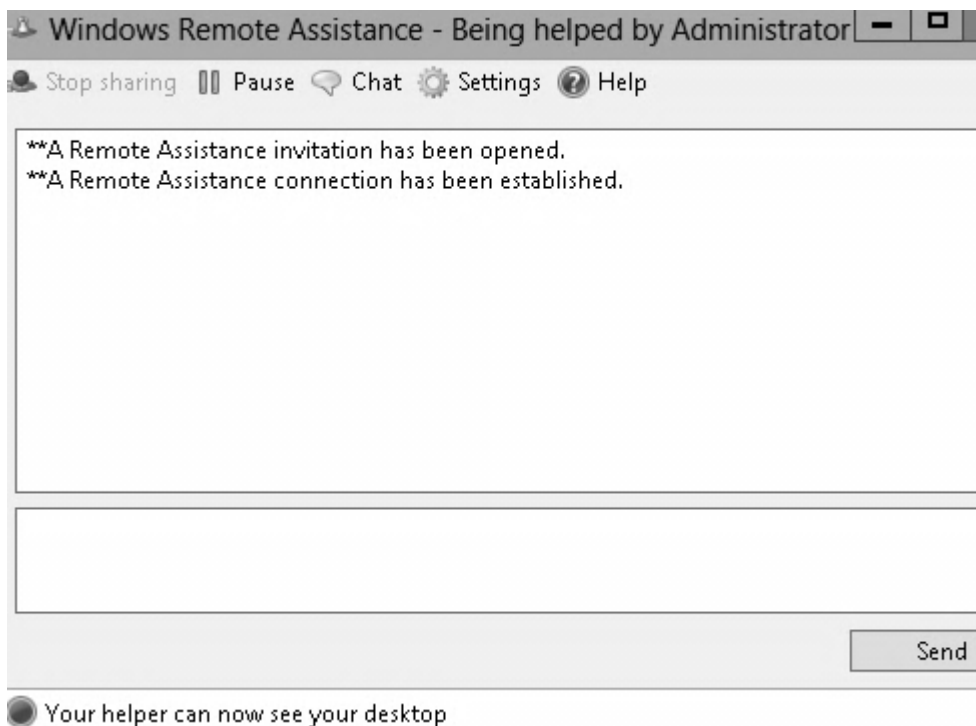
OK

Cancel

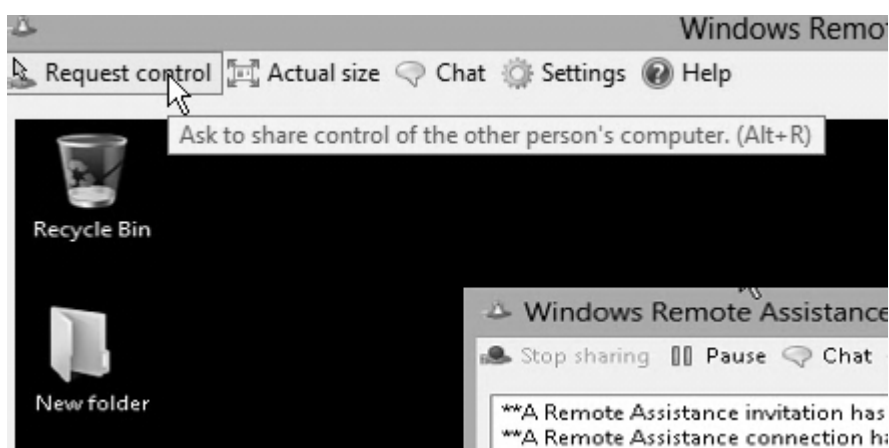
W tej chwili na komputerze nadawcy pojawi się komunikat, który należy potwierdzić klikając **Tak (YES)**, dopóki nie zostanie to zrobione osoba pomagająca nie będzie w stanie nic zrobić.



Na komputerze, który potrzebuje pomocy pojawi się okienko czatu, dzięki któremu można rozmawiać z pomocnikiem itp.

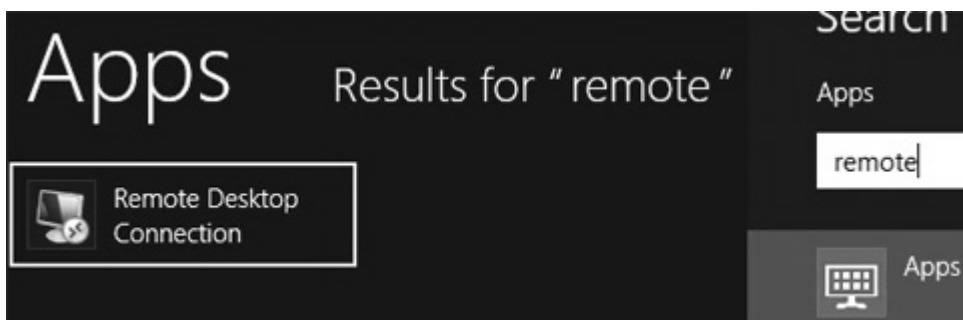


Obie strony pracują jednocześnie na jednym pulpicie i widzą go, w związku z czym pomocnik może albo nauczyć czegoś drugą osobę wydając jej polecenia i patrząc jak je realizuje lub po prostu przejąć kontrolę nad komputerem, do którego się podłączył i samemu wykonać powierzone zadanie.



### 12.3. Nawiązywanie połączenia pulpitu zdalnego

W tym poddziale zostanie nawiązane połączenie z serwerem za pomocą **Pulpitu Zdalnego (Remote Desktop)**. Należy wyszukać program **Połączenie Pulpitu Zdalnego (Remote Desktop Connection)**, a następnie go uruchomić.

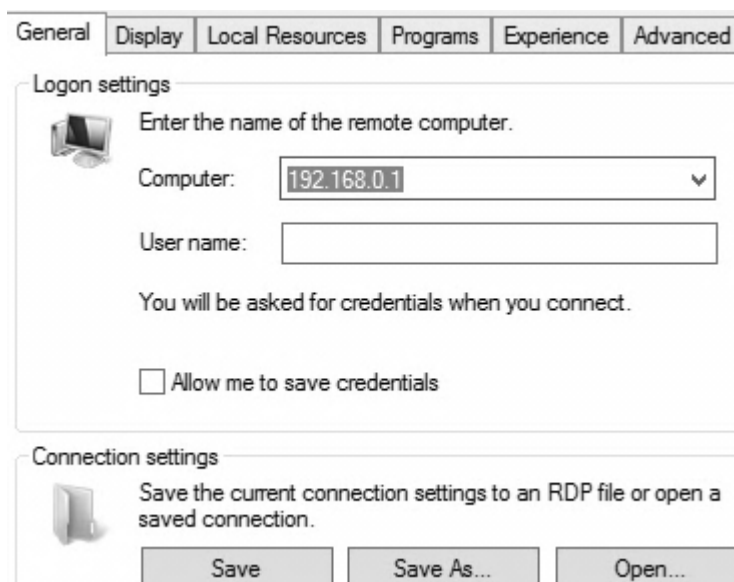


Pojawi się małe okno dialogowe, w którym de facto wystarczy podać adres serwera. Nie ważne czy będzie to adres IP czy nazwa domeny np. elitepc.pl. Będąc w domenie można po prostu wpisać nazwę komputera docelowego.

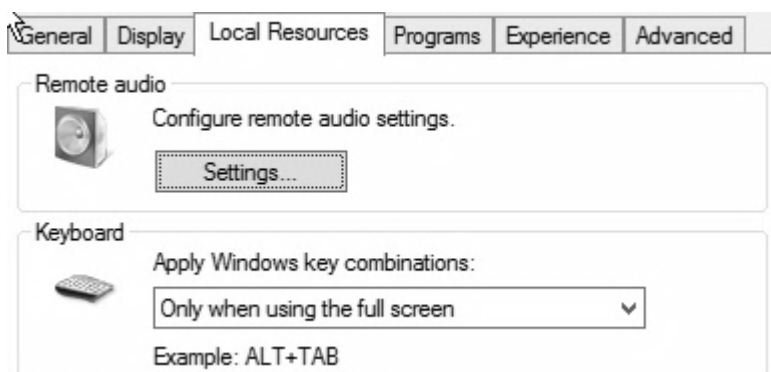


Przed połączeniem warto także rozwinąć opcje przyciskiem **Pokaż Opcje (Show Options)**. Między innymi znajduje się tam możliwość zapisania ustawień połączenia pulpitu zdalnego w formie pliku, dzięki czemu następnym razem wystarczy kliknąć,

aby zdalnie połączyć się z serwerem.




W zakładce **Zasoby lokalne (Local Resources)** znajdują się opcje związane z dostępem do zasobów lokalnych. Będzie można na komputerze zdalnym między innymi przenieść dźwięk, skróty klawiaturowe, zawartość schowka, drukarki czy inne urządzenia Plug and Play.




Po kliknięciu **Podłącz (Connect)** należy zalogować się do docelowego komputera. Konieczne będzie podanie danych do logowania.

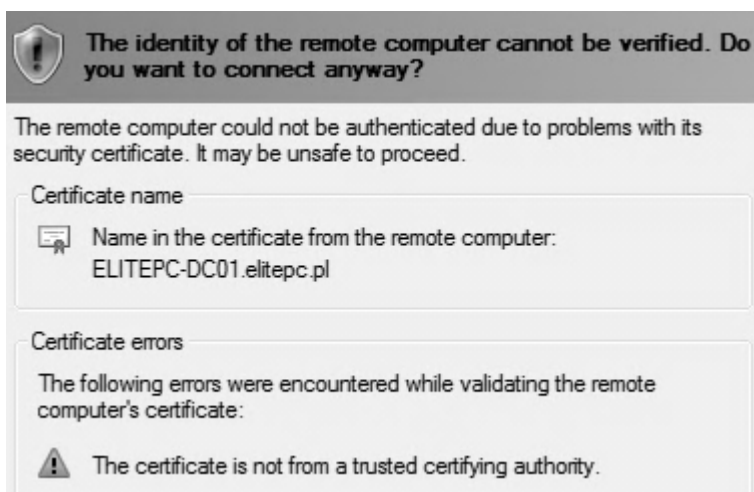
## Enter your credentials

These credentials will be used to connect to 192.168.0.1.

 administrator

 Use another account

Należy potwierdzić certyfikat. Jest to krok niezbędny, ponieważ połączenie pulpitem zdalnym ze względów bezpieczeństwa musi być szyfrowane.



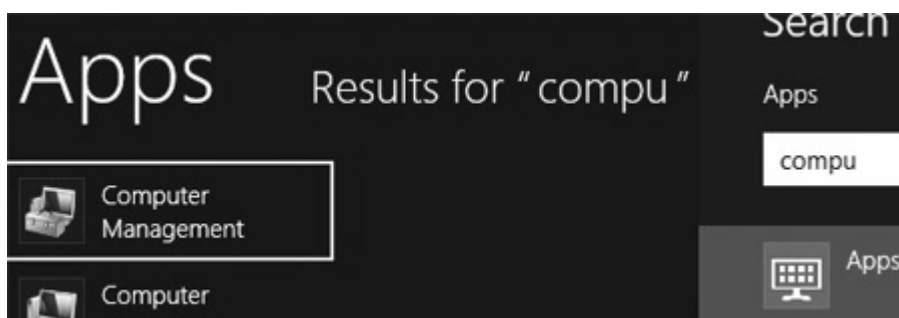
Połączenie powinno zostać nawiązane. Ten sposób logowania na serwerze pozwala na taką pracę na serwerze, jak gdyby administrator pracował na nim bezpośrednio. Pracę w trybie zdalnym można rozpoznać po dodatkowym pasku na górze ekranu.





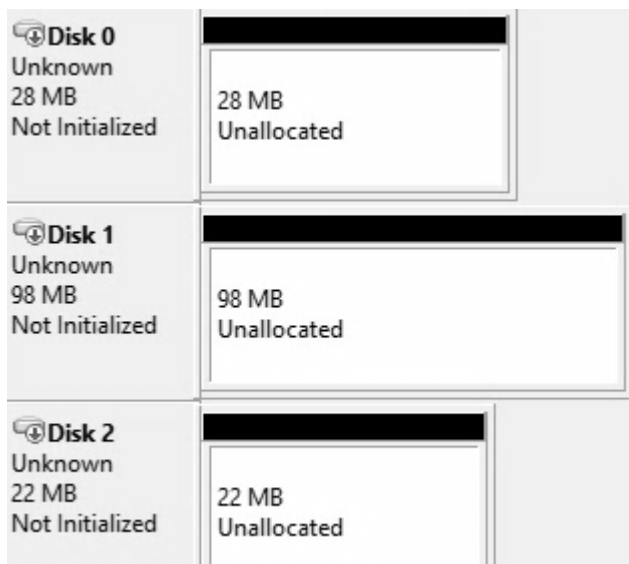
## 13. Zarządzanie dyskami

W systemie Windows Server 2012 można przekonwertować dyski na tak zwane dyski dynamiczne, które oferują zwiększone możliwości. Dyski dynamiczne zapewniają funkcje niedostępne na dyskach podstawowych, takie jak możliwość tworzenia woluminów obejmujących wiele dysków (woluminy łączone i rozłożone) czy odpornych na uszkodzenia (woluminy dublowane i RAID-5). Wszystkie woluminy na dyskach dynamicznych są nazywane woluminami dynamicznymi. Istnieje pięć typów woluminów dynamicznych: proste, łączone, rozłożone, dublowane i RAID-5. Woluminy dublowane i RAID-5 cechują się odpornością na uszkodzenia i są dostępne wyłącznie na komputerach z systemem Windows 2000 Server, Windows 2000 Advanced Server, Windows2000 Datacenter Server lub z systemami operacyjnymi Windows Server2003 i nowszych. Za pomocą komputera z systemem Windows 7 Professional można jednak zdalnie tworzyć woluminy dublowane na komputerach z tymi systemami operacyjnymi. Bez względu na to, czy używanym stylem partycjonowania dysku dynamicznego jest główny rekord rozruchowy (MBR), czy tabela partycji GUID (GPT), można utworzyć nawet 2000 woluminów dynamicznych. Zalecana liczba woluminów dynamicznych to 32 lub mniej. Należy wejść więc do *Konsoli Zarządzania Komputerem (Computer Management)*.

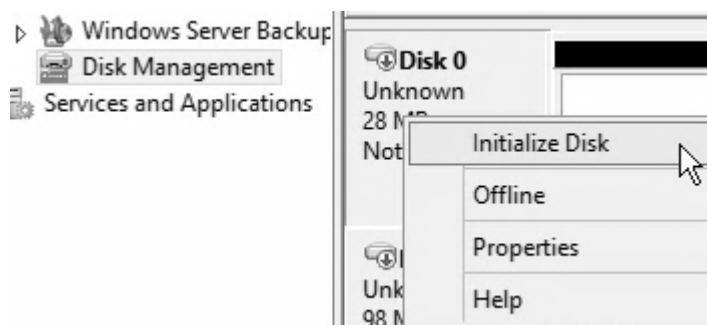


Należy kliknąć na *Zarządzanie Dyskami (Disk Management)*, po prawej stronie pojawi się lista partycji, a pod nią lista fizycznie podłączonych do komputera

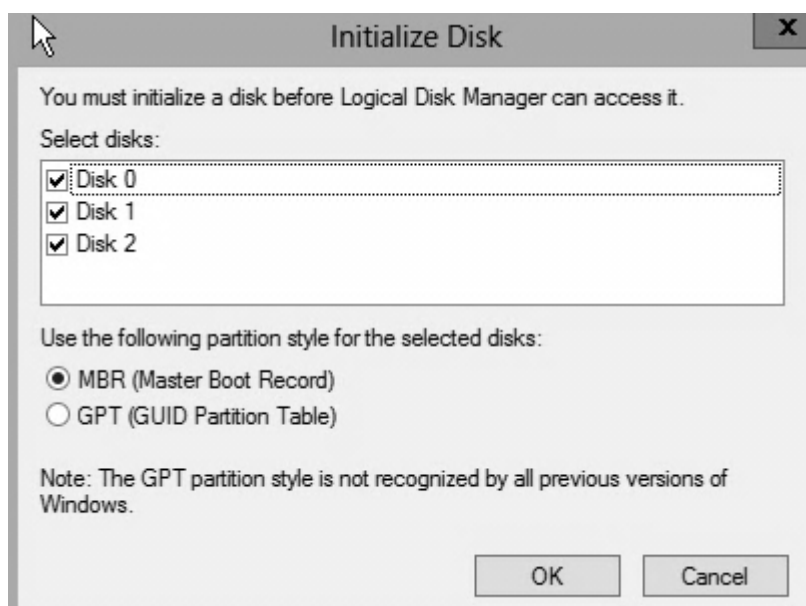
dysków. Jak widać są to trzy dyski, o których wspomniano w dziale opisującym środowisko, w którym Windows Server 2012 został zainstalowany. Nie były one jeszcze ani formatowane ani inicjalizowane.



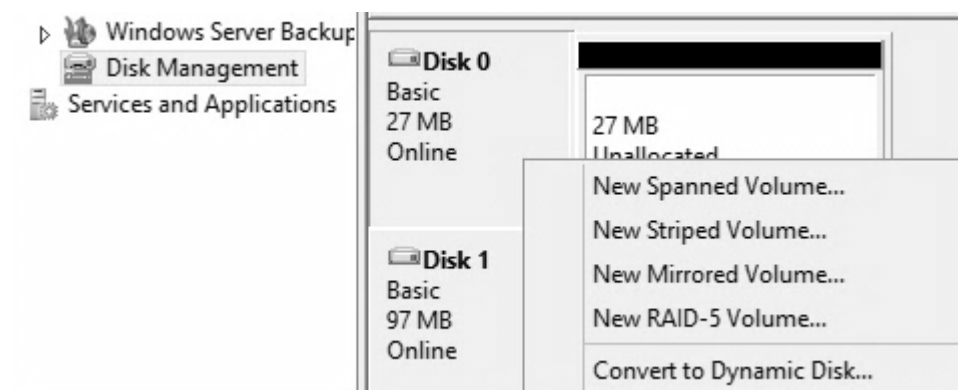
Teraz na wybranym nieaktywnym dysku należy kliknąć **Zainicjuj Dysk (Initialize Disk)**, po to, aby zaczął działać.



Należy pamiętać, że inicjowanie jest nieodwracalne. W oknie, które się pojawi należy wybrać wszystkie dyski twarde i kliknąć **OK**. Warto zauważyć, że drzewo partycji jakie zostanie na nim utworzone może być typu zarówno MBR jak i nowego typu GUID. Dla systemów Windows standardem jest MBR.

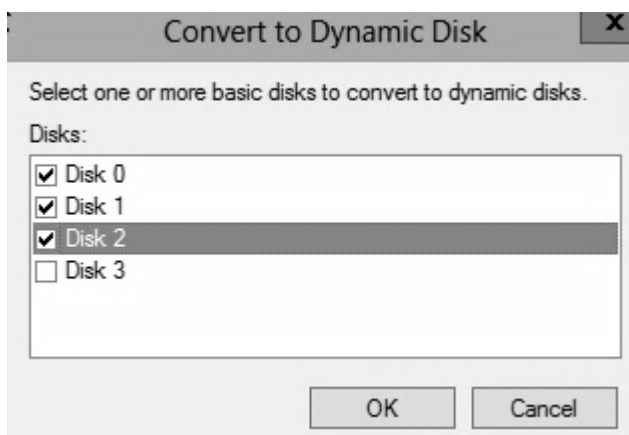


Następnie Należy przekonwertować dyski na dyski dynamiczne. Dzięki temu zyskuje się możliwość ich zaawansowanych ustawień i tworzenie macierzy dyskowych. Należy jednak pamiętać, iż macierze z racji na to, że nie są sprzętowe, lecz programowe będą wolniejsze od sprzętowych. Co więcej dysku skonwertowanego na dynamiczny nie uda się bez problemów odczytać na innym komputerze. Na wybranym dysku należy kliknąć prawym przyciskiem myszy i wybrać opcję **Konwertuj dysk na dynamiczny (Convert to Dynamic Disk)**.



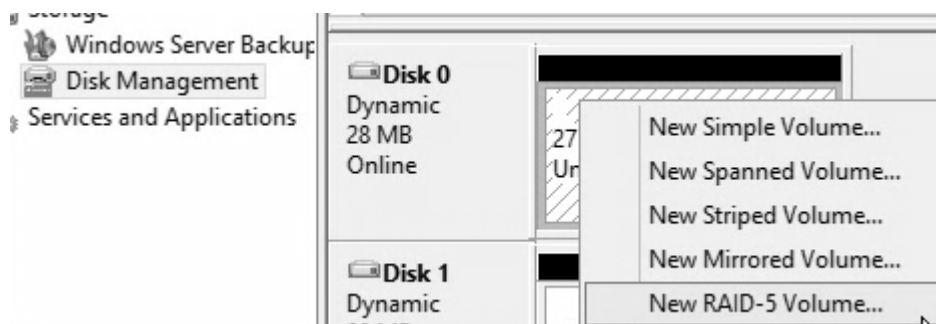
W oknie, które się pojawi należy wybrać dyski. Zostaną wybrane tylko trzy

dodatkowe dyski służące ćwiczeniu, a wybór zostanie potwierdzony kliknięciem **OK**.



Teraz klikając na wybranym dysku prawym przyciskiem myszy można utworzyć jeden z 5 woluminów. **Wolumin Prosty (Simple Volume)** jest odpowiednikiem zwyczajnej partycji, z tym, że w przyszłości będzie się dało swobodnie modyfikować jego rozmiar jeżeli pozwoli na to dysk twardy. **Wolumin Łączony (Spanned Volume)** pozwala połączyć ze sobą kilka dysków twardych w jeden duży, jego zaletą jest to, iż dyski mogą mieć różne rozmiary. Nie daje on żadnego przyrostu szybkości pracy dysków ani bezpieczeństwa przed utratą danych. **Wolumin Rozłożony (Stripped Volume)** z kolei jest alternatywą dla RAID 0. Łączy on dwa dyski o identycznej pojemności i zapisując jednocześnie na obu z nich fragmenty danych sprawia iż dysk działa szybciej. **Wolumin Dublowany (Mirrored Volume)** łączy dwa dyski ze sobą w taki sposób, że na jednym z nich przechowywana jest kopia drugiego, podobnie jak w RAID 1. Dla przykładu zostanie stworzony nowy wolumin RAID-5. Stanowi on jakby połączenie RAID 0 i RAID 1. Wymaga on co najmniej 3 dysków. Dwa z nich łączone są tak, jak w przypadku woluminu rozłożonego, natomiast trzeci dysk przechowuje część danych uzyskaną przez operację arytmetyczną XOR. Na podstawie tych danych w razie awarii jednego z dwóch pierwszych dysków można dane odzyskać i serwer dalej

działa.



W oknie powitalnym należy kliknąć **Dalej (Next)**, następnie wybrać dyski i ustawić odpowiedni rozmiar woluminu. Może on być tak duży jak duży jest najmniejszy z dysków. Należy kliknąć przycisk **Dalej (Next)**.

#### Select Disks

You can select the disks and set the disk size for this volume.

Select the disks you want to use, and then click Add.

Available:		Selected:
	Add >	Disk 0 19 MB
	< Remove	Disk 1 19 MB
	< Remove All	Disk 2 19 MB

Total volume size in megabytes (MB): 38

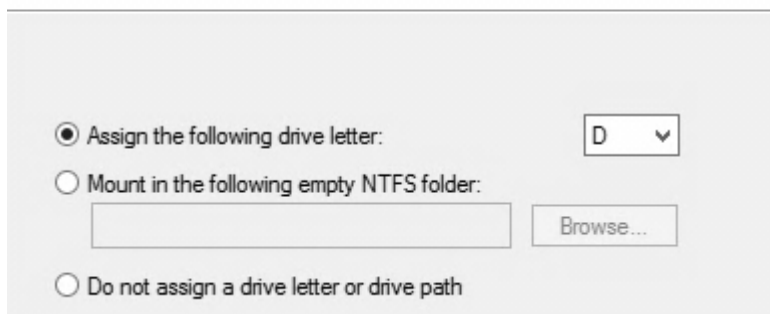
Maximum available space in MB: 19

Select the amount of space in MB: 19

Następnie konieczne jest wybranie litery, która będzie oznaczała dysk.

### Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your volume.



☒ Assign the following drive letter: D ▼

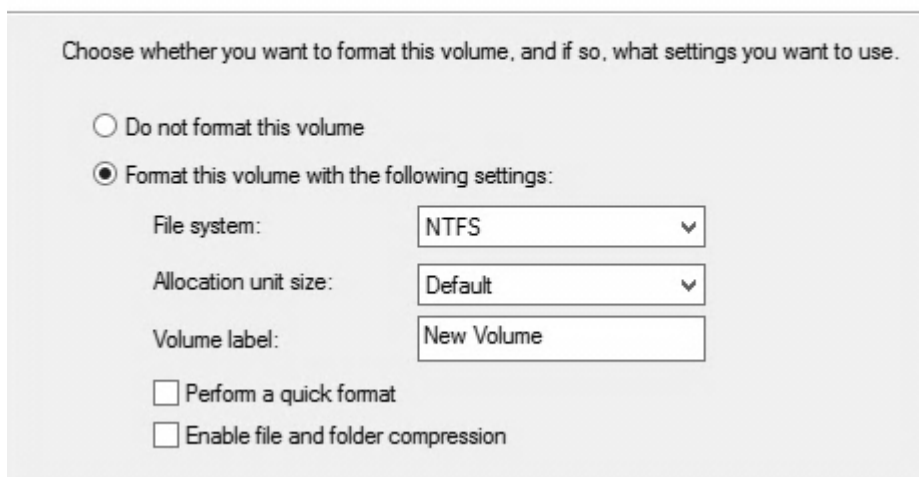
☐ Mount in the following empty NTFS folder:  Browse...

☐ Do not assign a drive letter or drive path

Na kolejne karcie można sformatować wolumin, wybrać odpowiedni system plików, a także nadać mu odpowiednią etykietę. Należy kliknąć ***Dalej (Next)***.

### Format Volume

To store data on this volume, you must format it first.



Choose whether you want to format this volume, and if so, what settings you want to use.

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS ▼

Allocation unit size: Default ▼

Volume label: New Volume

☐ Perform a quick format

☐ Enable file and folder compression

W okienku podsumowującym należy kliknąć ***Zakończ (Finish)***.

## Completing the New RAID-5 Volume Wizard

You have successfully completed the Wizard.

You selected the following settings:

Volume type: RAID-5	^
Disks selected: Disk 0, Disk 1, Disk 2	
Volume size: 38 MB	
Drive letter or path: D:	≡
File system: NTFS	
Allocation unit size: Default	
Volume label: New Volume	
Quick format: No	v

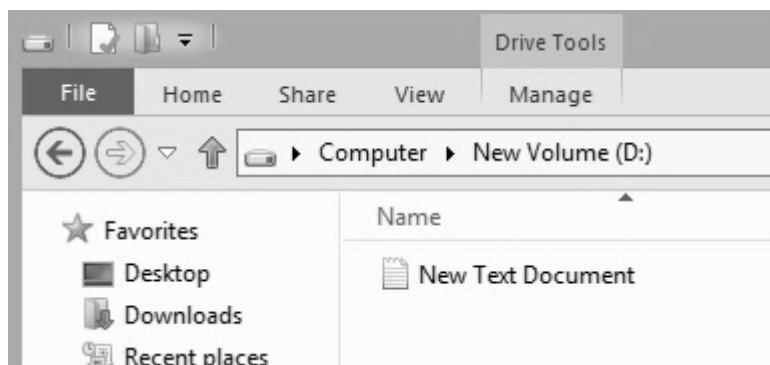
To close this wizard, click Finish.



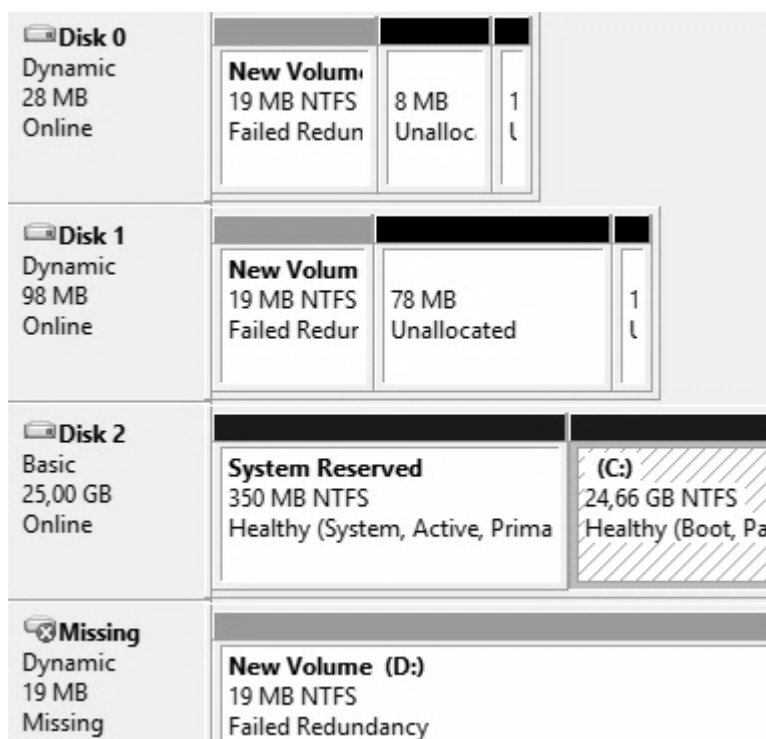
Nastąpi synchronizacja dysków.

<b>Disk 0</b> Dynamic 28 MB Online	<table><tr><td><b>New Volume</b> 19 MB NTFS Healthy</td><td>8 MB Unallocated</td></tr></table>	<b>New Volume</b> 19 MB NTFS Healthy	8 MB Unallocated
<b>New Volume</b> 19 MB NTFS Healthy	8 MB Unallocated		
<b>Disk 1</b> Dynamic 98 MB Online	<table><tr><td><b>New Volume</b> 19 MB NTFS Healthy</td><td>78 MB Unallocated</td></tr></table>	<b>New Volume</b> 19 MB NTFS Healthy	78 MB Unallocated
<b>New Volume</b> 19 MB NTFS Healthy	78 MB Unallocated		
<b>Disk 2</b> Dynamic 22 MB Online	<table><tr><td><b>New Volume (D:)</b> 19 MB NTFS Healthy</td><td></td></tr></table>	<b>New Volume (D:)</b> 19 MB NTFS Healthy	
<b>New Volume (D:)</b> 19 MB NTFS Healthy			

Dla testu zostanie stworzony plik na tym dysku.

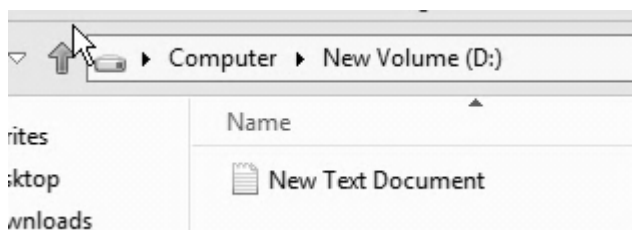


W celach testowych maszyna zostanie wyłączona i jeden dowolny dysk zostanie od niej odłączony. Po ponownym uruchomieniu komputera i wejściu do konsoli **Computer Management** można zobaczyć, że jednego dysku brakuje.



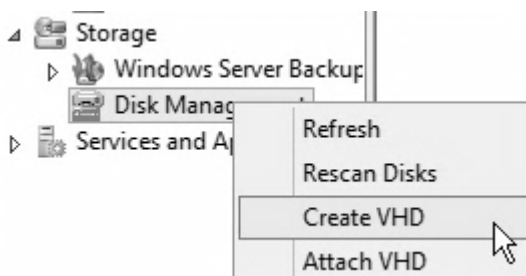
Jednak jak widać plik dalej istnieje i ma się dobrze.





## 12.4. Wirtualne dyski

Dysk wirtualny to określenie zasobów pamięci masowej w komputerze niedostępnych bezpośrednio w systemie, lecz emulowanych przez oprogramowanie w taki sposób, jakby były fizycznie obecne. Najczęściej dysk taki jest realizowany w postaci pliku na fizycznym dysku twardym, który potem jest montowany, dzięki czemu z punktu widzenia użytkownika działa dokładnie tak samo jak gdyby był to fizyczny dysk twardy. Po kliknięciu prawym przyciskiem myszy na **Disk Management** w konsoli **Computer Management**, w menu kontekstowym można ujrzeć dwie opcje związane z tworzeniem wirtualnych dysków: **Utwórz (Create)** oraz **Przylącz (Attach)**. Pierwsza z nich, służy do tworzenia dysków wirtualnych, druga z kolei do ich podłączania do komputera.



W oknie, które się pojawi należy podać ścieżkę lokalizacji, w jakiej ma zostać utworzony wirtualny dysk twardy, a także określić jego rozmiar i format. Nowością w systemie Windows Server 2012 jest wprowadzenie formatu zapisu VHDX, który znosi ograniczenia dysków w formacie VHD. Teraz wirtualny dysk może posiadać objętość do 64TB, co więcej VHDX jest bardziej odporny na uszkodzenia, które

mogłyby powstać podczas awarii zasilania.

Ostatnim krokiem jest określenie typu dysku wirtualnego. **Stały rozmiar (Fixed size)** od razu zaalokuje sobie odpowiednią ilość pamięci na dysku fizycznym. Jest rekomendowany ze względu na stabilność oraz szybkość działania. Typ **Alokowany Dynamicznie (Dynamically allocated)** stworzy dysk, którego rozmiar będzie zwiększany przyrostowo. Im więcej danych zostanie na nim umieszczonych tym większy będzie rozmiar jego pliku.

Specify the virtual hard disk location on the machine.

Location:  
C:\nowy.vhd Browse...

Virtual hard disk size: 200 MB

Virtual hard disk format

☒ VHD  
Supports virtual disks up to 2040 GB in size.

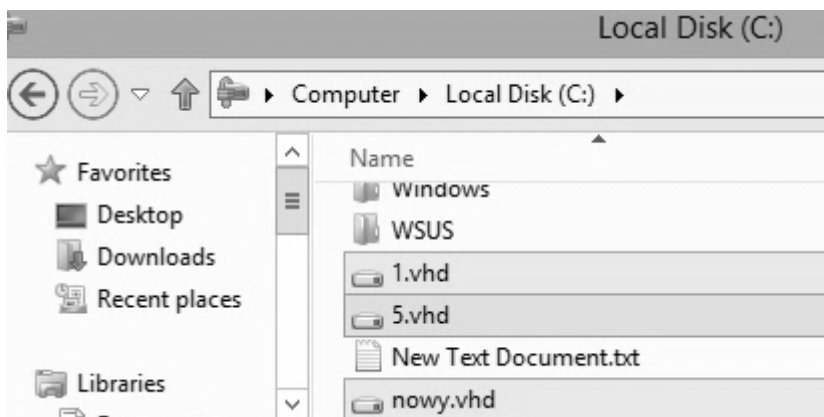
☐ VHDX  
Supports virtual disks larger than 2040 GB in size (Supported maximum of 64 TB) and is resilient to power failure events. This format is not supported in operating systems earlier than Windows Server 2012 Release Candidate.

Virtual hard disk type

☒ Fixed size (Recommended)  
The virtual hard disk file is allocated to its maximum size when the virtual hard disk is created.

☐ Dynamically expanding  
The virtual hard disk file grows to its maximum size as data is written to the virtual hard disk.

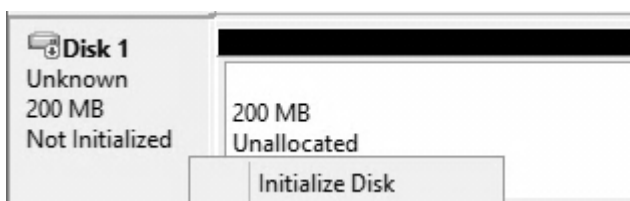
Po kliknięciu przycisku **OK** i chwili oczekiwania zależnej od wielkości tworzonego dysku w podanej lokalizacji powinien zostać utworzony plik dysku wirtualnego.



Zostanie on także automatycznie podłączony do komputera. Jeżeli jednak wirtualny dysk został skopiowany z innej maszyny należy go podłączyć opcją **Przylącz (Attach)** z menu kontekstowego. Wystarczy, że zostanie podana ścieżka i zostanie kliknięty przycisk **OK**.



Dyskami VHD i VHDX zarządza się tak samo jak dyskami fizycznymi i również należy je inicjalizować.



Dzięki dyskom wirtualnym można bardzo swobodnie przenosić dane, a nawet całe systemy operacyjne. Co więcej zwiększają one hermetyczność danych. Wydajnościowo dyski Fizyczne i VHD są porównywalne. VHD nieco lepiej wypadają przy zapisie danych.

## **12.5. Instalacja systemu na wirtualnym dysku**

Windows 2012 podobnie jak i Windows 8, Windows 7 czy Windows Server 2008 R2, oferują możliwość instalacji na wirtualnym dysku twardym. Istniała również możliwość takiej instalacji w systemie Windows Vista, lecz nie była ona ani wspierana przez Microsoft, ani w 100% działająca.

Instalacja na dysku wirtualnym polega na tym, że jest tworzony na istniejącej już partycji z zainstalowanym (choć nie koniecznie, wystarczy, że będzie nim sformatowana partycja) systemem operacyjnym plik VHD. Dzięki temu nie ma konieczności dokupowania dysku, ani zmniejszania partycji na obecnym dysku twardym, aby można było zainstalować system operacyjny obok już istniejącego.

Pierwszym pytaniem jakie powinno się nasunąć jest celowość takiego zabiegu oraz to, czy jest i jaki jest spadek wydajności. Maszyny wirtualne nie oferują pełnej funkcjonalności systemu jak na przykład wsparcie 3D oraz są zdecydowanie wolniejsze niż zwykłe instalacje. W ten sposób można spokojnie przetestować system pod każdym kątem oraz jak będzie działał na fizycznym sprzęcie, a nie tym wirtualnym.

Aby rozpocząć instalację wystarczy tradycyjnie uruchomić komputer z płyty instalacyjnej Windows 7, na pierwszym ekranie należy wybrać odpowiedni język, lokalizację i klawiaturę.

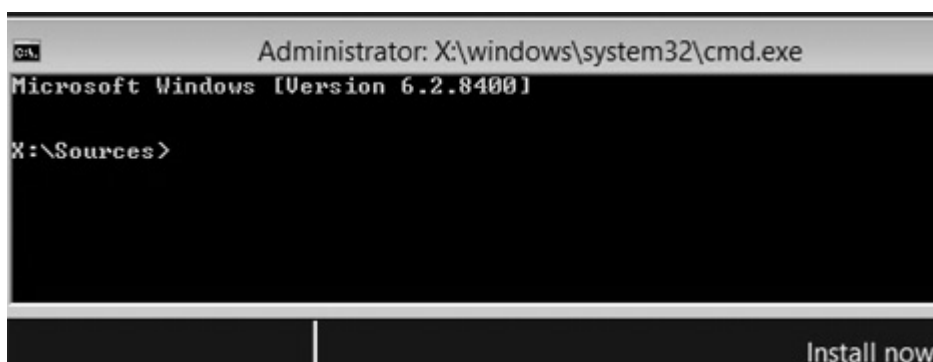


Language to install: English (United States)

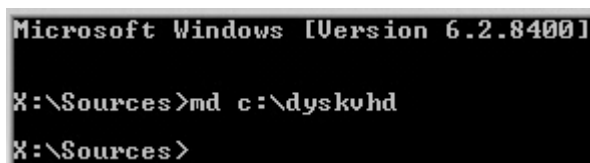
Time and currency format: Polish (Poland)

Keyboard or input method: Polish (Programmers)

Następnie należy wybrać kombinację klawiszy SHIFT+F10, aby pojawiła się konsola CMD. Instalator to nic innego jak system Windows w wersji PE, czyli polecenia jak regedit do edycji rejestru itp. zadziałają.



Na komputerze zainstalowany jest już standardowo jeden system. Na dysku 250GB jest stworzona jedynie jedna partycja. Na początek warto stworzyć na dysku systemowym C folder, w którym zostaną umieszczone wirtualne dyski.



```
Microsoft Windows [Version 6.2.8400]
X:\Sources>md c:\dyskvh
X:\Sources>
```

W następnej kolejności należy uruchomić narzędzie do zarządzania dyskami twardymi, wpisując w konsoli polecenie **diskpart**. Trzeba będzie chwilę poczekać aż program się załaduje z płyty DVD.

```
Microsoft Windows [Version 6.2.8400]

X:\Sources>md c:\dyskvh

X:\Sources>diskpart

Microsoft DiskPart version 6.2.8400

Copyright (C) 1999-2012 Microsoft Corporation.
On computer: MINWINPC

DISKPART>
```

Kiedy program zostanie wczytany do pamięci należy stworzyć wirtualny dysk twardy. Typ *fixed* oznacza, że dysk nie będzie dynamicznie się rozszerzał, tylko będzie miał stały rozmiar. Jest to lepsze rozwiązanie, gdyż dyski dynamiczne czasami w tym zastosowaniu powodują pojawianie się niebieskich ekranów. Parametr maximum określa maksymalny rozmiar jaki dysk będzie miał (Przyjmuje on wartości w MB).

```
Microsoft Windows [Version 6.1.7600]

X:\Sources>notepad

X:\Sources>md c:\virtualne

X:\Sources>diskpart

Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: MINWINPC

DISKPART> create vdisk file=c:\virtualne\win7.vhd type=fixed maximum = 200

10 percent completed
```

Tworzenie dysku chwilę potrwa, gdyż program w razie potrzeby zdefragmentuje miejsce tak, aby wirtualny nośnik zajmował jedną dużą wolną przestrzeń, która także jest zapisywana zerami przy jej tworzeniu. Gdy dysk zostanie przygotowany należy go „zaznaczyć”, aby móc na nim operować.

```
DiskPart successfully created the virtual disk file.  
DISKPART> select vdisk file c:\wirtualne\win7.vhd  
DiskPart successfully selected the virtual disk file.  
DISKPART> _
```

Ostatnim już krokiem będzie przyłączenie dysku poleceniem *attach*. Jest ono jednoznaczne z fizycznym podłączeniem dysku do komputera.

```
DISKPART> attach vdisk  
100 percent completed  
DiskPart successfully attached the virtual disk file.  
DISKPART> _
```

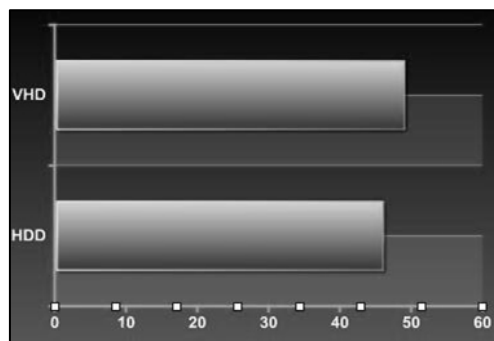
W dalszym kroku należy zamknąć program poleceniem *exit*, konsolę krzyżykiem i wrócić do instalatora klikając *Dalej (Next)*.

```
DiskPart successfully attached the virtual disk file.  
DISKPART> exit  
Leaving DiskPart...
```

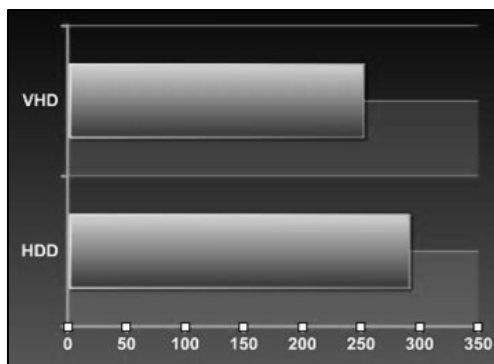
Dalsza instalacja jest analogiczna jak w przypadku zwykłej instalacji. Wirtualne dyski zostaną automatycznie wykryte przez instalator tak samo jak dyski fizyczne.

Pora przejść do pomiarów wydajności. System działa tak, jakby był normalnie zainstalowany, jedyną różnicą jest to, że mieści się on na sztucznie stworzonym dysku. Dla porównania poniżej zostały przedstawione wyniki kilku syntetycznych jak i normalnych testów.

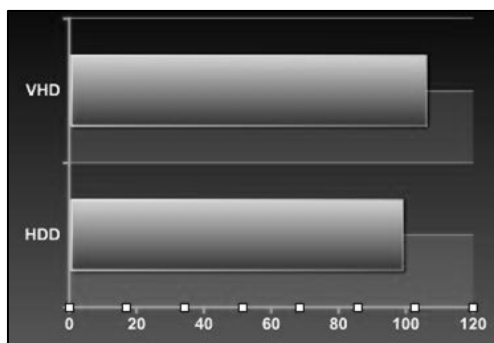
### 1) Start Windows 7



### 2) Kopiowanie pliku 6GB

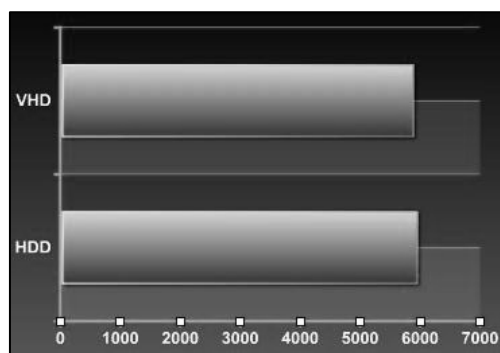


### 3) Tworzenie pliku 6GB

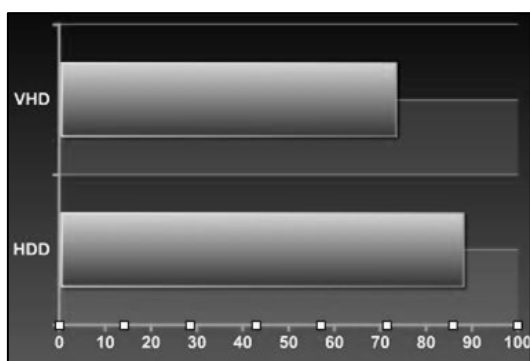




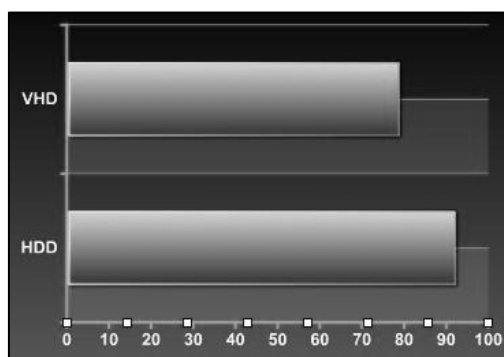
#### 4) PCMark HDD Suite



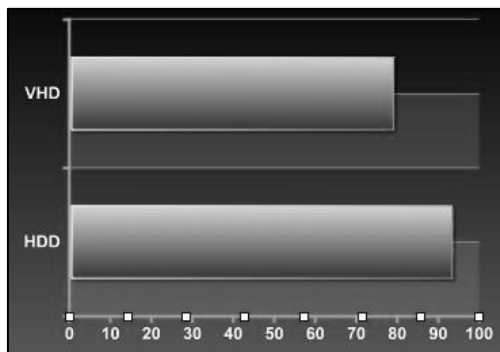
#### 5) HDTune (Mb/s)



#### 6) HDTach 8MB (MB/s)



## 7) HdTach 32MB (MB/s)

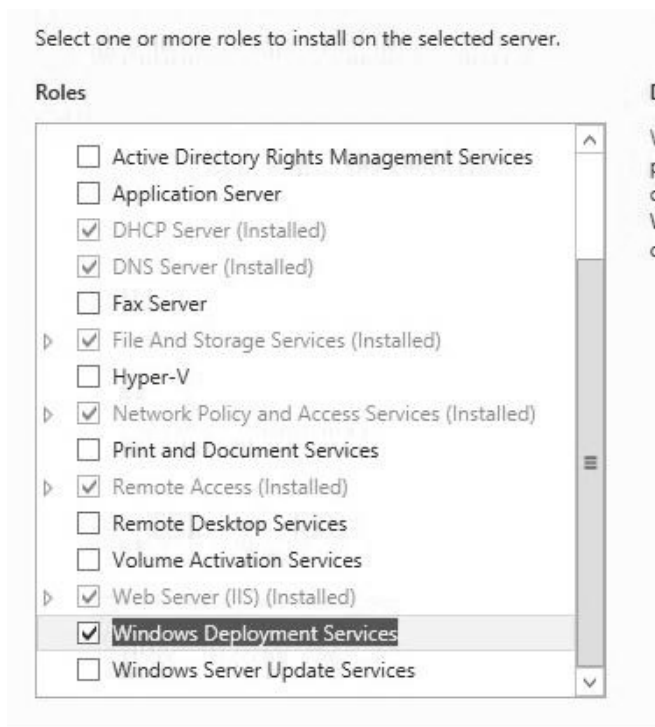


Jak widać za wyjątkiem kopiowania pliku dyski VHD są nieco wolniejsze. Nie jest to jednak spadek wydajności na tyle zauważalny, aby się nim bardzo przejmować. Kopiowanie wyszło natomiast nieco lepiej dlatego, że cały obszar pamięci jest dysku wirtualnego jest za alokowany jako jeden ciągły obszar. Co za tym idzie głowica dysku nie musiała daleko się przemieszczać w celu odczytania i ponownego zapisu danych. Wyciągając średnią arytmetyczną z reszty testów okazuje się, że wydajność dysku wirtualnego jest niższa od zwykłego jedynie o około 10,1%.

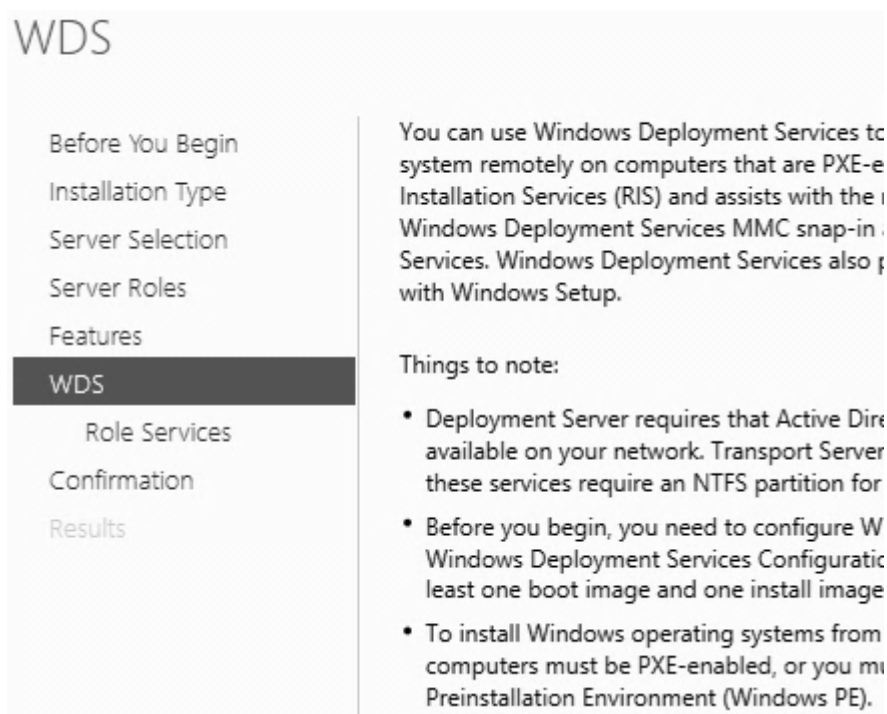
Zainteresowanym można także polecić jedną bardzo przydatną aplikację *disk2vhd*, którą można pobrać ze strony: <http://technet.microsoft.com/en-us/sysinternals/ee656415.aspx>. Dzięki niej uda się dowolną partycję przekonwertować na dysk VHD. Dla przykładu jeśli na komputerze jest wgrany Windows XP i użytkownik nie chce go stracić, można wtedy przeprowadzić taką operację. Następnie dysk VHD ze starym systemem można użyć pod Windows 7 do pracy w trybie XP Mode lub jako zwykłą maszynę wirtualną w programie Microsoft Virtual PC.

## 14. WDS – Zdalna Instalacja

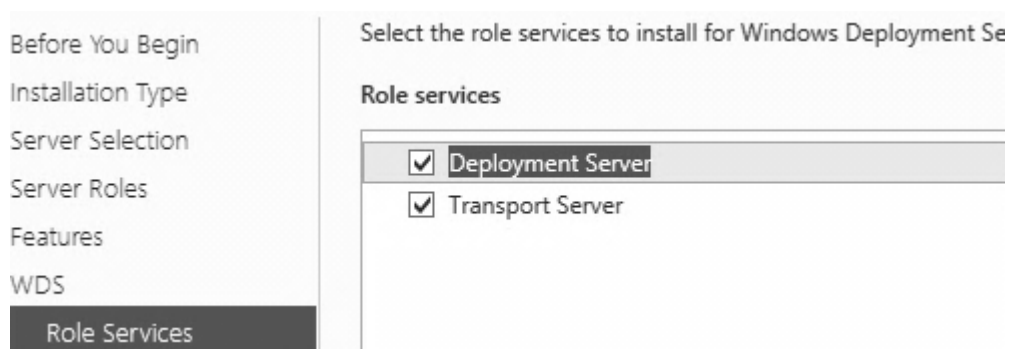
Windows Deployment Services, czyli usługi wdrażania systemu Windows pozwalają na zdalną instalację systemu na wielu maszynach na raz bez potrzeby używania CD. Komputer uruchamia się za pomocą połączenia sieciowego, łączy się z serwerem i uruchamia pożądany program instalacyjny np. Windows Server 2012. Za pomocą aplikacji WAIK można przygotować instalator systemu nie wymagający interakcji z użytkownikiem, co znacznie upraszcza wdrożenie oprogramowania na wielu komputerach. W tym celu należy zainstalować rolę systemu Windows o nazwie **Usługi wdrażania systemu Windows (Windows Deployment Services)**. Po wybraniu roli w kreatorze należy kliknąć **Dalej (Next)**.



Na kolejnej karcie należy ponownie kliknąć **Dalej (Next)**.



Na następnej karcie należy wybrać odpowiednie *Usługi Ról (Role Services)* i kliknąć przycisk *Dalej (Next)*.



Wybrane wcześniej ustawienia potwierdza się klikając *Instaluj (Install)*.

To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they were selected automatically. If you do not want to install these optional features, click their check boxes.

Remote Server Administration Tools

Role Administration Tools

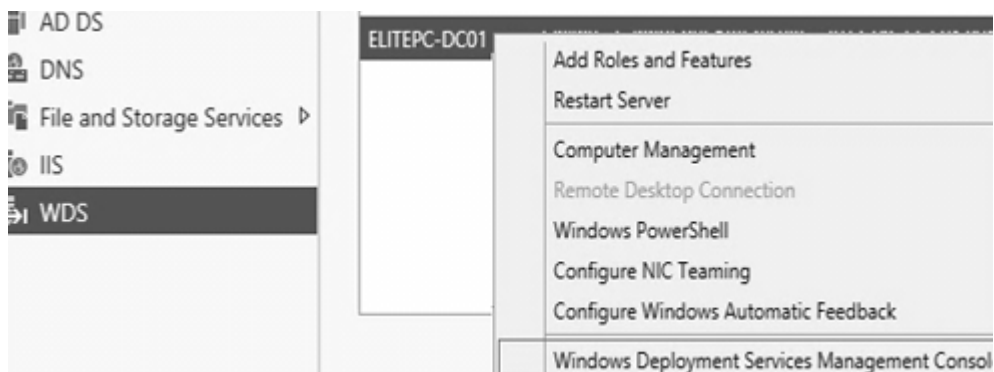
Windows Deployment Services Tools

Windows Deployment Services

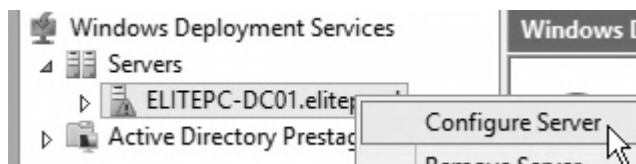
Deployment Server

Transport Server

W *Menadżerze Serwera (Server Manager)* pojawi się wpis WDS, po jego wybraniu i kliknięciu prawym klawiszem na nazwie serwera, można na nim uruchomić konsolę *Usług wdrażania systemu Windows (Windows Deployment Services Management Console)*.



Na serwerze należy kliknąć prawym przyciskiem myszy i wybrać *Skonfiguruj Serwer (Configure Server)*.



Na ekranie powitalnym należy kliknąć **Dalej (Next)**.

You can use this wizard to configure Windows Deployment Services. Once the server is configured, you will need to add at least one boot image and one install image to the server before you will be able to install an operating system.

**Before you begin, ensure that the following requirements are met:**

- The server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain. If the server supports Standalone mode, it can be configured without having a dependency on Active Directory.
- There is an active DHCP server on the network. This is because Windows Deployment Services uses Pre-Boot Execution Environment (PXE), which relies on DHCP for IP addressing.
- There is an active DNS server on your network.
- This server has an NTFS file system partition on which to store images.

To continue, click Next.

W kolejnym oknie trzeba zdefiniować to, czy serwer będzie działał niezależnie czy w ramach usługi Active Directory.

Select one of the following options:

☒ Integrated with Active Directory  
This server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain.

☐ Standalone server  
Configure the server so that it is standalone, operating independently of Active Directory.


Na kolejnym należy wybrać folder, w którym obrazy systemów mają być przechowywane i kliknąć **Dalej (Next)**.

The remote installation folder will contain boot images, install images, PXE boot files, and the Windows Deployment Services management tools. Choose a partition that is large enough to hold all of the images that you will have. This partition must be an NTFS partition and should not be the system partition.

Enter the path to the remote installation folder.

Path:

Na komunikacie, który się pojawi należy kliknąć **Tak (Yes)**.

 The volume selected is also the Windows system volume. For best performance and data reliability, the remote installation folder should be stored on a separate volume, and, where possible, on a separate disk from the system volume.  
Do you want to continue?

W następnej kolejności wymagane jest zaznaczenie opcji niezbędnych do odpowiadania wszystkim komputerom oraz kliknięcie **Zakończ (Finish)**.

PXE Response Policy

Define which client computers this server will respond to. Known clients are clients that appear in the list of prestaged devices.

☒ Do not respond to any client computers

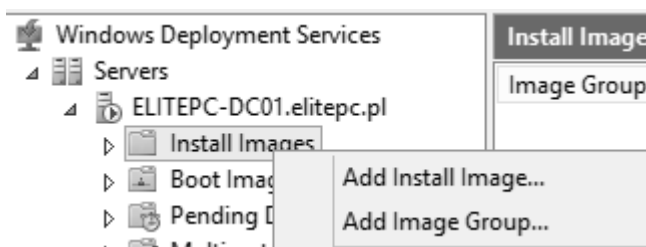
☐ Respond only to known client computers

☐ Respond to all client computers (known and unknown)

☐ Require administrator approval for unknown computers. When you select this option, you must approve the computers using the Pending Devices node in the snap-in. Approved computers will be added to the list of prestaged clients.

Po kliknięciu prawym przyciskiem myszy na Install Images w konsoli WDS są do

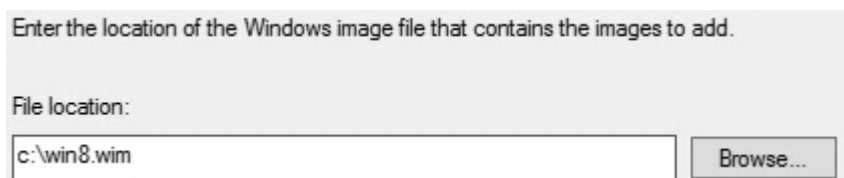
wyboru dwie opcje: **Dodaj obraz instalacji (Add Install Image)** oraz **Dodaj grupę obrazów (Add Image Group)**.



Jeżeli zostanie wybrana opcja **Dodaj grupę obrazów (Add Image Group)** konieczne będzie podanie nazwy dla grupy.



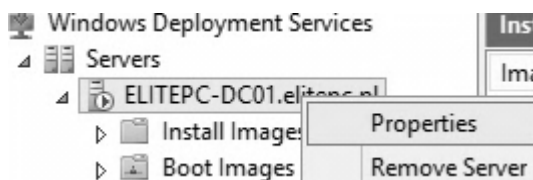
Konieczne jest wybranie ścieżki do obrazu lub obrazów systemu. Nie chodzi tu o plik ISO, lecz folder, do którego na przykład zostanie przekopiowana zawartość instalacyjnego CD. Należy go przygotować narzędziem WAIK.



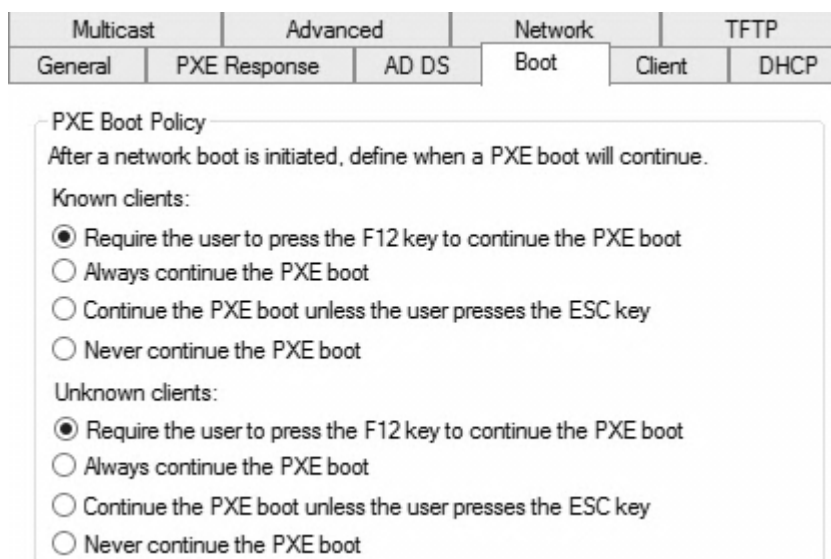
Server jest gotowy, aby dało się z niego uruchamiać instalację za pośrednictwem sieci lokalnej. Można też przygotować Windows'a w wersji PE czy Linux'a w



wersji Live CD.



Gdy serwer jest już skonfigurowany przez kreatory można zawsze dokonać ręcznych zmian jego konfiguracji. Po wejściu we właściwości serwera z poziomu konsoli WDS i wybraniu zakładki **Boot** można określić parametry związane z rozruchem przez sieć. Definiuje się je osobno dla znanych jak i nie znanych komputerów klienckich. Między innymi definiuje się to, czy uruchamianie ma być automatyczne czy na żądanie poprzez wciśnięcie klawisza F12 oraz czy użytkownik będzie mógł przyciskiem ESC anulować proces uruchamiania z sieci. Można także określić domyślne obrazy rozruchowe w zależności od architektury sprzętowej komputera.



W zakładce DHCP należy zaznaczyć obie dostępne opcje jeżeli każdy komputer, któremu zostanie przypisany adres IP ma jednocześnie znać adres serwera PXE.

Jeżeli w sieci jest DHCP pod kontrolą Windows Server zostanie on automatycznie skonfigurowany, w przeciwnym razie odpowiednie opcje zakresu należy ustawić ręcznie.

Multicast	Advanced	Network	TFTP
General	PXE Response	AD DS	Boot
		Client	DHCP

If Dynamic Host Configuration Protocol (DHCP) is running on this server, check both of the following check boxes and use DHCP tools to add appropriate PXE options to all DHCP and DHCPv6 scopes.

If a non-Microsoft DHCP server is running on this server, then check the first box and manually configure DHCP option 60 and DHCPv6 Vendor Class for Proxy DHCP.

If DHCP is installed on a server that is located in a different subnet, click the link below for more information.

☐ Do not listen on DHCP ports

☐ Configure DHCP options to indicate that this is also a PXE server

Warto także zapoznać się z zakładką Client, gdzie można określić czy każda maszyna czy tylko ta o określonej architekturze sprzętowej może korzystać z danego obrazu nienadzorowanej instalacji. Nowością w Windows Server 2012 jest wsparcie dla komputerów, które zamiast Biosu używają UEFI. Można tutaj także zabronić podłączania komputera do domeny w sposób automatyczny po instalacji oraz uruchomić logowanie.

## 15. Hyper - V

Ostatnie lata rozwoju branży IT prześlągnięte są słowem wirtualizacja, na, której to zaczyna opierać się coraz więcej rozwiązań branżowych. Polega ona na tym, że na fizycznie działającym systemie operacyjnym za pomocą odpowiedniego oprogramowania, w tym przypadku Hyper-V instaluje się dodatkowy system operacyjny, który zachowuje się dokładnie tak samo jak gdyby był zainstalowany na zwykłym komputerze.

Hyper-V został wprowadzony w Windows Server 2008, został on także rozwinięty o wiele znaczących funkcjonalności w Service Pack 1 do Windows Server 2008 R2. Windows Server 2012 udoskonala istniejące już funkcjonalności, a także wprowadza nowe. W Windows Server 2012 możliwe jest utrzymanie 1024 aktywnych maszyn wirtualnych zamiast wcześniejszych 384. Maksymalna ilość wirtualnych procesorów dostępnych dla maszyny wirtualnej zwiększono z 4 do 32. Pojedyncza maszyna wirtualna może korzystać z maksymalnie 512 GB pamięci (wcześniej 64GB), a sama rola Hyper-V bez problemu zagospodaruje moc 160 procesorów logicznych.

### a. Instalacja

W celu zainstalowania roli Hyper-V należy użyć *Menadżera Serwera (Server Manager)*, w którym podczas dodawania nowych ról wybiera się Hyper-V.

## Select server roles

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
Hyper-V  
Virtual Switches  
Migration  
Default Stores  
Confirmation  
Results

Select one or more roles to install on the selected server.

**Roles**

- ☐ Active Directory Rights Management Services
- ☐ **Application Server**
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☒ File And Storage Services (Installed)
- ☒ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Żadne dodatkowe funkcje nie będą wymagane, więc w oknie ich wyboru można kliknąć przycisk **Dalej (Next)**.

## Select features

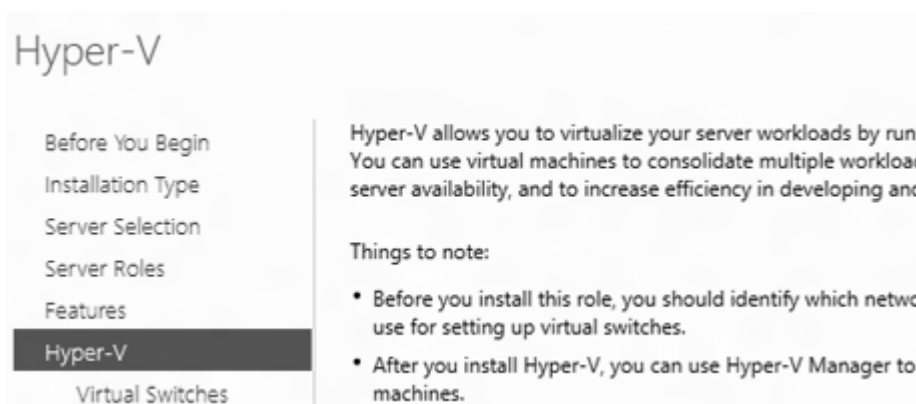
Before You Begin  
Installation Type  
Server Selection  
Server Roles  
**Features**  
Hyper-V  
Virtual Switches  
Migration  
Default Stores

Select one or more features to install on the selected server.

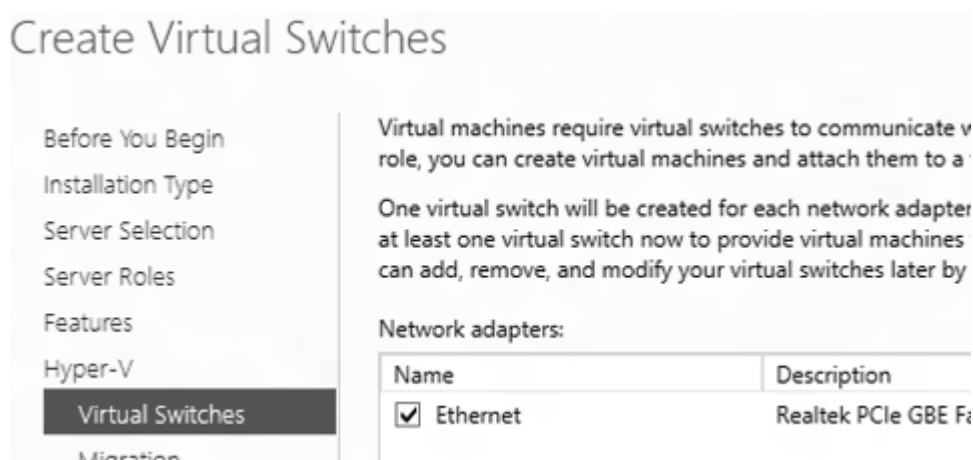
**Features**

- ☐ **.NET Framework 3.5 Features**
- ☒ .NET Framework 4.5 Features (Installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS

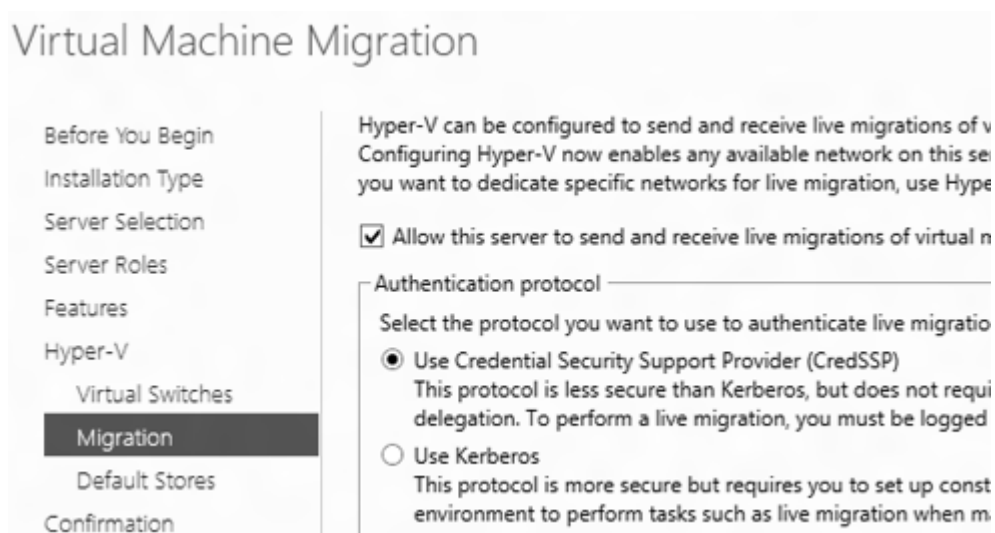
Kolejne okno kreatora to karta informacyjna, która powiadamia o tym iż potrzebna będzie wiedza na temat tego, które interfejsy sieciowe będą współdzielone z maszynami wirtualnymi oraz do tego, że do zarządzania maszynami wirtualnymi będzie używana konsola Hyper-V Manager. Naturalnie jeżeli maszyny wirtualne mają mieć dostęp do sieci firmowej muszą być połączone z interfejsem sieciowym, który jest wpięty do tej sieci.



W kolejnym oknie zaznacza się adaptory sieciowe, które mają być użyte. Microsoft rekomenduje pozostawienie jednego interfejsu nieużywanego na potrzeby zdalnej administracji.



Następna karta kreatora dotyczy ustawień związanych z migracją maszyn wirtualnych. Jest to nowość w systemie Windows Server 2012. Do tej pory niezbędne było używanie funkcji Failover clustering. Do wyboru są dwa rodzaje autentykacji podczas migracji. Jednym z nich jest CredSSP, który jest mniej bezpieczny niż protokół Kerberos, lecz nie wymaga tworzenia delegacji, a do przeprowadzenia migracji administrator musi być zalogowany na źródłowym serwerze. W przypadku Kerberosa autentykacja jest bezpieczniejsza, natomiast wymaga stworzenia delegacji, za to pozwala na zdalne wykonanie migracji. Jeżeli serwer ma być częścią klastra nie należy uruchamiać migracji, lecz zrobić to podczas tworzenia klastra.



W kolejnym oknie kreatora definiuje się to, gdzie serwer maszyn wirtualnych ma przechowywać wirtualne dyski twarde oraz pliki konfiguracyjne tychże maszyn. Zaleca się je trzymać na szybkich macierzach dyskowych zabezpieczonych przed utratą danych.

## Default Stores

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Hyper-V

Virtual Switches

Migration

Default Stores

Hyper-V uses default locations to store virtual hard disk files unless you specify different locations when you create them now, or you can change them later by modifying Hyper-V settings.

Default location for virtual hard disk files:

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

Default location for virtual machine configuration files:

C:\ProgramData\Microsoft\Windows\Hyper-V

Na karcie podsumowującej należy kliknąć przycisk Install, aby instalacja się rozpoczęła. Wymagane będzie ponowne uruchomienie komputera. Na serwerze, na którym zainstalowano Hyper-V nie zaleca się instalowania innych ról.

## Confirm installation selections

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Hyper-V

Virtual Switches

Migration

Default Stores

Confirmation

To install the following roles, role services, or features or

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might have been selected automatically. If you do not want to install them, uncheck their check boxes.

Hyper-V

Remote Server Administration Tools

Role Administration Tools

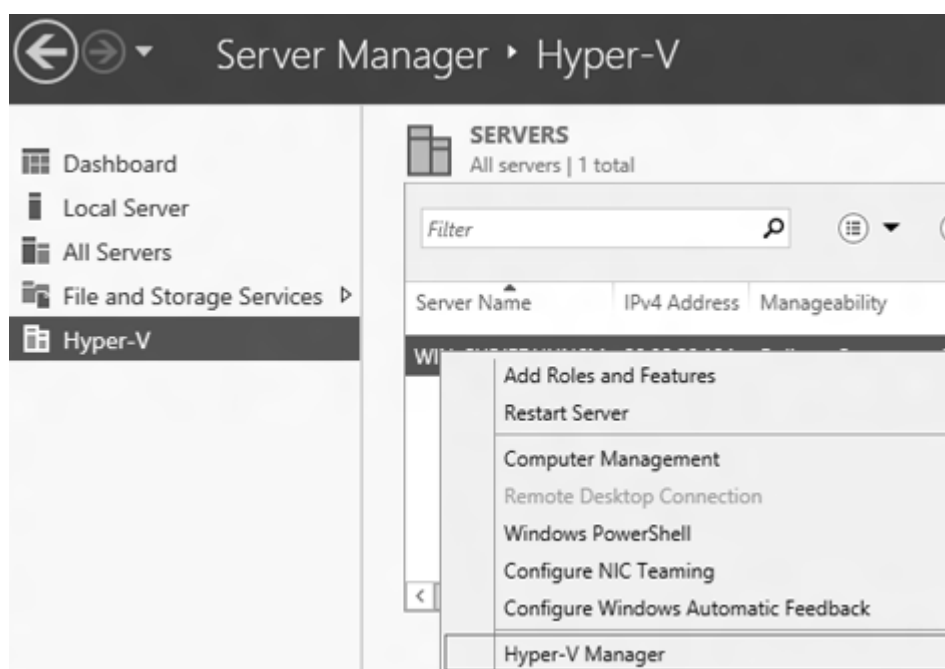
Hyper-V Management Tools

Hyper-V Module for Windows PowerShell

Hyper-V GUI Management Tools

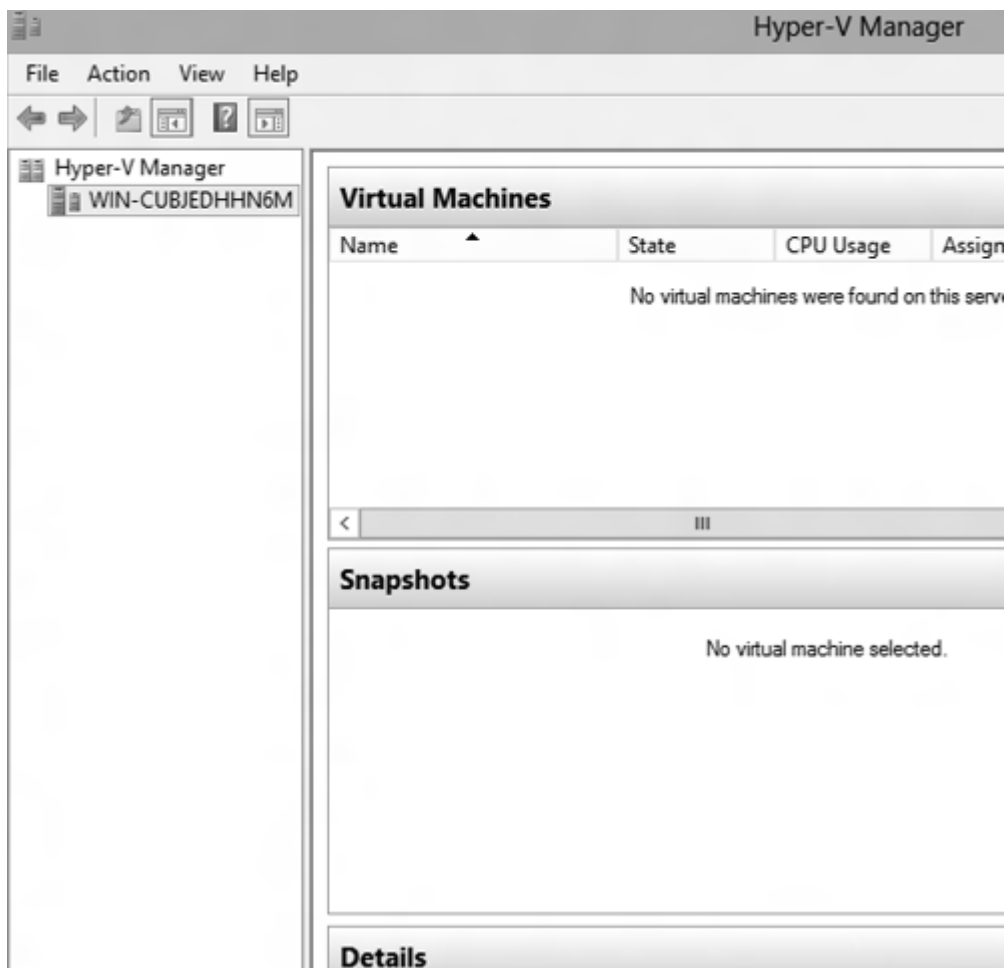
## b. Zarządzanie Hyper-V

Z poziomu Menadżera Serwera należy do konsoli wejść Hyper-V Manager. Jest to główna konsola zarządzania rolą Hyper-V, w której będzie można wykonywać większość zadań administracyjnych z nią związanych.

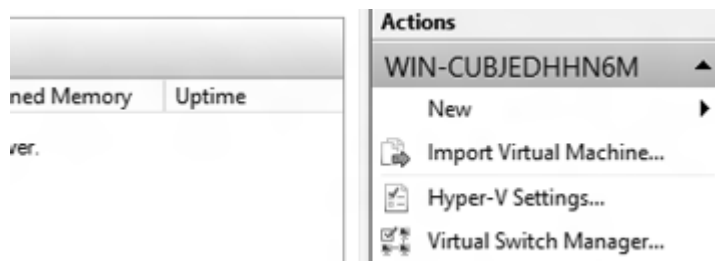


Okno Menadżera Hyper-V składa się z trzech sekcji. Pierwsza z nich to drzewo serwerów pozwalające zarządzać różnymi serwerami, po prawej stronie znajduje się menu, natomiast w centralnej sekcji znajdują się maszyny wirtualne oraz ich migawki. Aby wszystkie funkcje jak na przykład zarządzanie RemoteFX i kartami graficznymi były dostępne musi zostać zainstalowana także rola Remote Desktop Virtualization, co zostało uczynione w rozdziale 12.

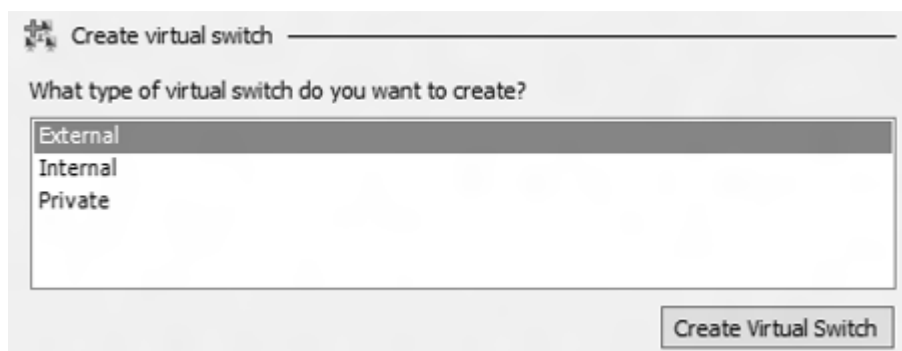




Pierwszym krokiem jaki powinno się zrobić jest stworzenie wirtualnych sieci, aby zapewnić łączność ze „światem” dla maszyn wirtualnych. Robi się to przyciskiem Virtual Switch Manager.



Stworzyć można trzy rodzaje sieci. Jednym z nich jest połączenie zewnętrzne, **mostkowane (Bridged)** nazwane **External**. Symuluje ono wpięcie maszyny wirtualnej do fizycznej sieci. Drugim jest połączenie **wewnętrzne (Internal)**, które tworzy sieć niemającą wyjścia na świat i działającą tylko i wyłącznie w obrębie maszyn wirtualnych w taki sposób, że maszyny do niej wpięte będą się między sobą komunikowały. Zapewniona będzie także komunikacja z komputerem hosta (serwerem Hyper-V). Ostatnim rodzajem wirtualnego przełącznika jest sieć prywatna, charakteryzująca się tym, że tylko i wyłącznie maszyny wirtualne mają ze sobą łączność. Po wybraniu odpowiedniego wirtualnego przełącznika należy kliknąć **Utwórz Wirtualny Przełącznik (Create Virtual Switch)**.



Pojawi się okno, w którym można nadać danemu przełącznikowi nazwę oraz opis, także typ połączenia może zostać zmieniony w każdej chwili. W przypadku **połączenia zewnętrznego (External)** można także z rozwijanej listy określić, do której karty sieciowej połączenie będzie mostkowane. Tylko i wyłącznie w tym momencie, czyli podczas tworzenia nowego przełącznika można skorzystać z funkcji **SR-IOV**, która jest jedną z nowości w Hyper-V 2012, zaznaczając opcję **Enable single – root I/O virtualization**. Funkcja ta daje możliwość przypisania karty sieciowej wspierającej standard single root I/O virtualization, co z kolei wpływa na zmaksymalizowanie przepustowości sieci oraz zmniejszenie opóźnień sieciowych. Dzięki temu maszyna wirtualna jest bezpośrednio wpięta do fizycznej karty sieciowej bez użycia pośredniczącego wirtualnego przełącznika.

**Virtual Switch Properties**

Name:  
SR-IOV

Notes:

**Connection type**  
What do you want to connect this virtual switch to?

☒ External network:  
Realtek PCIe GBE Family Controller

☒ Allow management operating system to share this network adapter  
☒ Enable single-root I/O virtualization (SR-IOV)

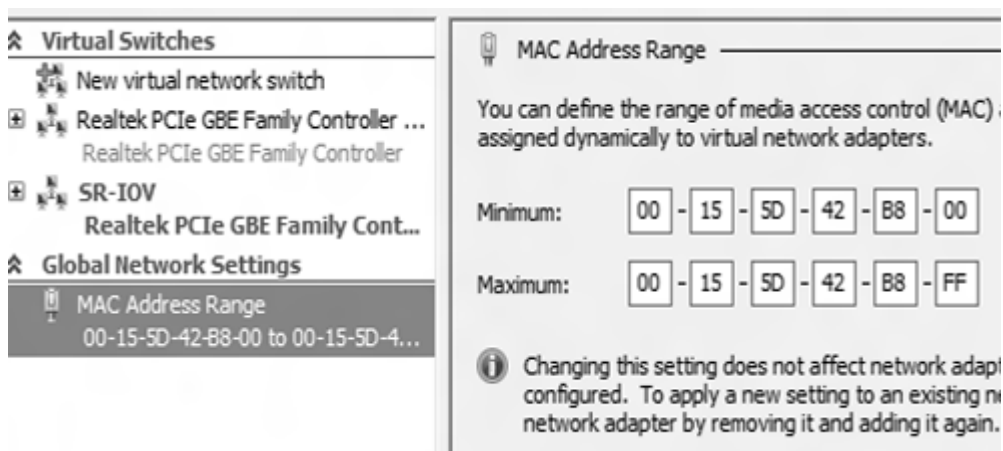
☐ Internal network  
☐ Private network

**VLAN ID**  
☐ Enable virtual LAN identification for management operating system

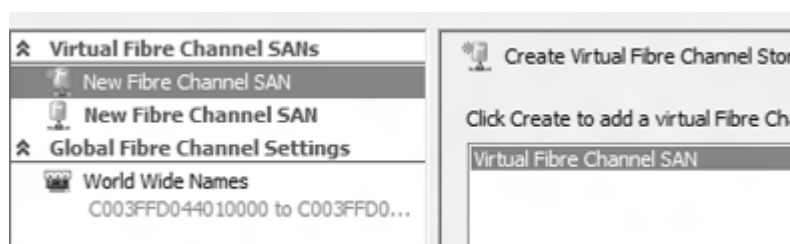
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

Wybranie w lewym menu **MAC-Address Range** umożliwia zdefiniowanie zakresów adresacji MAC dla wirtualnych kart sieciowych poprzez określenie minimalnych i maksymalnych wartości adresu MAC. Przy użyciu przycisku **OK** należy zapisać i zatwierdzić wybór, jednocześnie zamykając okno i wracając do głównego menu Hyper-V.

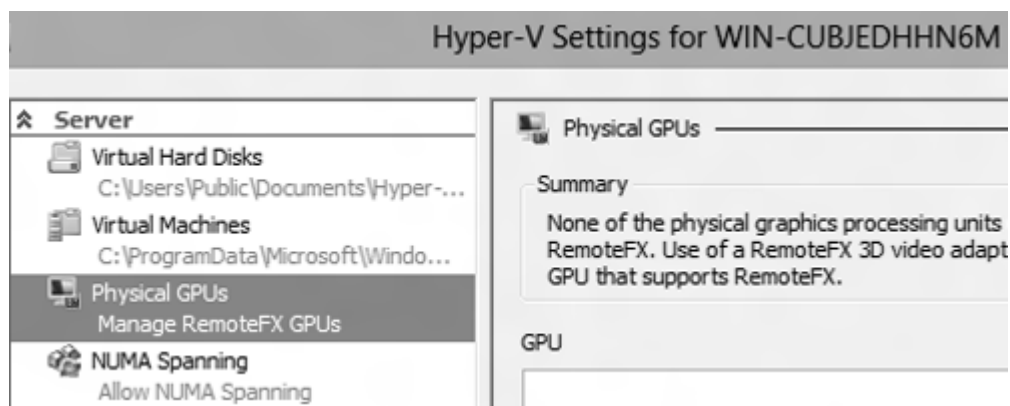


W menu po prawej stronie należy kliknąć **Virtual San Manager**, aby zapoznać się z kolejną nowością w Hyper-V. Pozwala ona na stworzenie wirtualnego kanału typu fibre-channel, dzięki któremu maszyny wirtualne mogą mieć dostęp do magazynów typu fibre-channel. Naturalnie wymogiem jest posiadanie portów typu fibre-channel w komputerze hostującym. Należy kliknąć **OK**.

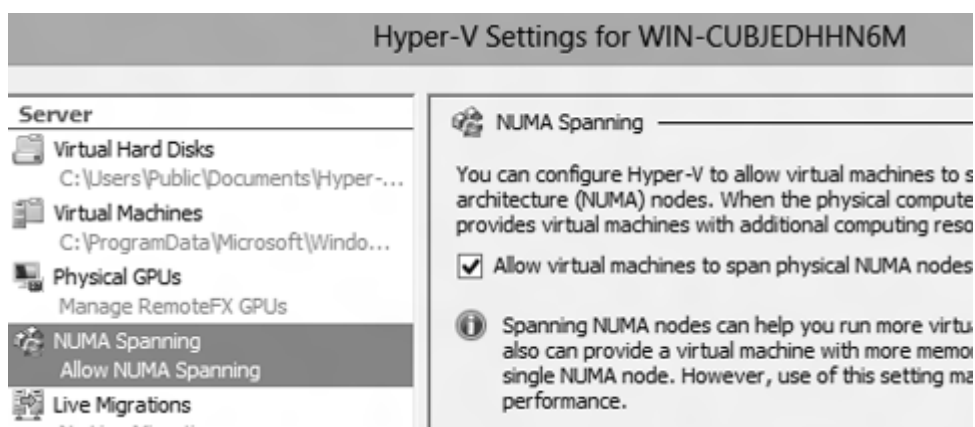


Wracając do Menadżera Hyper-V można wybrać przycisk **Ustawienia Hyper-V (Hyper-V Settings)**. Pierwsze dwie opcje, czyli **Wirtualne Dyski Twarde (Virtual Hard Disks)** oraz **Maszyny Wirtualne (Virtual Machines)** pozwalają na zmianę miejsca przechowywania wirtualnych dysków twardych oraz plików konfiguracyjnych maszyn wirtualnych. Opcja **Physical GPUs** pozwala na zdefiniowanie, która karta graficzna może być używana przez RemoteFX, a także na włączenie wsparcia GPU dla RemoteFX. RemoteFX jest technologią wprowadzoną w Service Pack 1 do Windows Server 2008 R2. Daje możliwość wirtualizacji karty

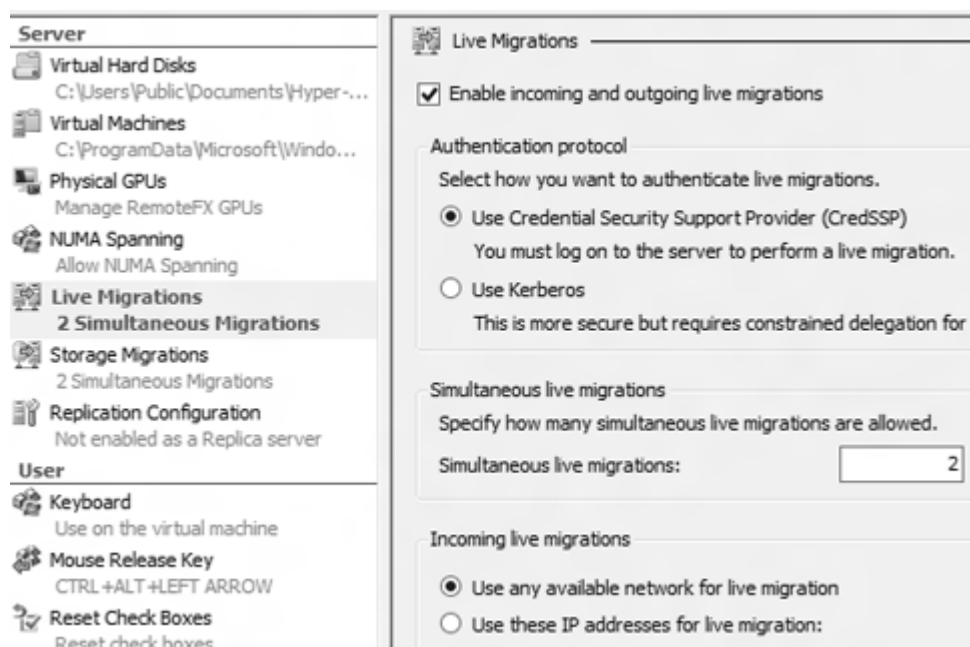
graficznej w maszynach wirtualnych, dzięki czemu zyskują one możliwość akceleracji sprzętowej. Pozwala to na renderowanie materiałów 3D, a nawet uruchamianie gier komputerowych. Umożliwia także przekierowanie portów USB do maszyn wirtualnych, a także zapewnia wysoką jakość wideo oraz tekstu.



Kolejną opcją wartą omówienia jest **NUMA Spanning**, którą także można uruchomić w Hyper-V Settings. Technologia ta pozwala na przydzielenie dodatkowych zasobów dla maszyn wirtualnych, a także pomaga w jednoczesnym uruchomieniu wielu maszyn wirtualnych, dzięki dynamicznemu przydzielaniu zasobów, jednak w niektórych przypadkach negatywnie wpływa na ogólną wydajność. Jak skorzystać z technologii Virtual NUMA powiedziane będzie za chwilę przy tworzeniu maszyny wirtualnej. Technologia NUMA nazywana jest także przetwarzaniem współbieżnym nierównomiernym. Stosowane jest ona w szczególności w serwerach wieloprocessorowych, gdzie czas dostępu do pamięci operacyjnej zależy od odległości od procesora, który na przykład szybciej odwoła się do swojej pamięci lokalnej niż do pamięci współdzielonej między procesorami.

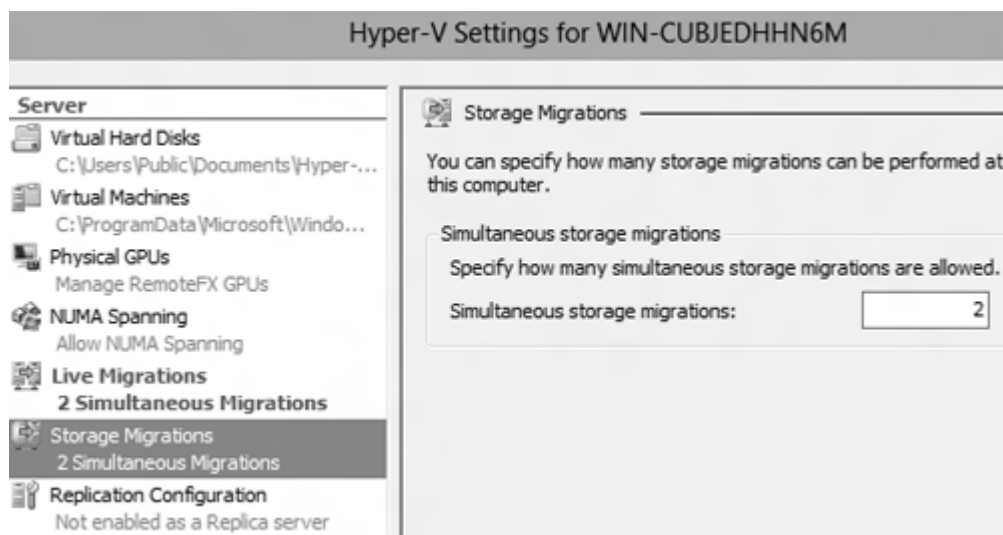


Wybierając opcję **Migracja w czasie rzeczywistym (Live Migration)** ma się dostęp do opcji, które zostały skonfigurowane w kreatorze instalacji. Można tutaj dodatkowo określić ile migracji może być jednocześnie przeprowadzanych oraz przez jakie sieci mogą się one odbywać.

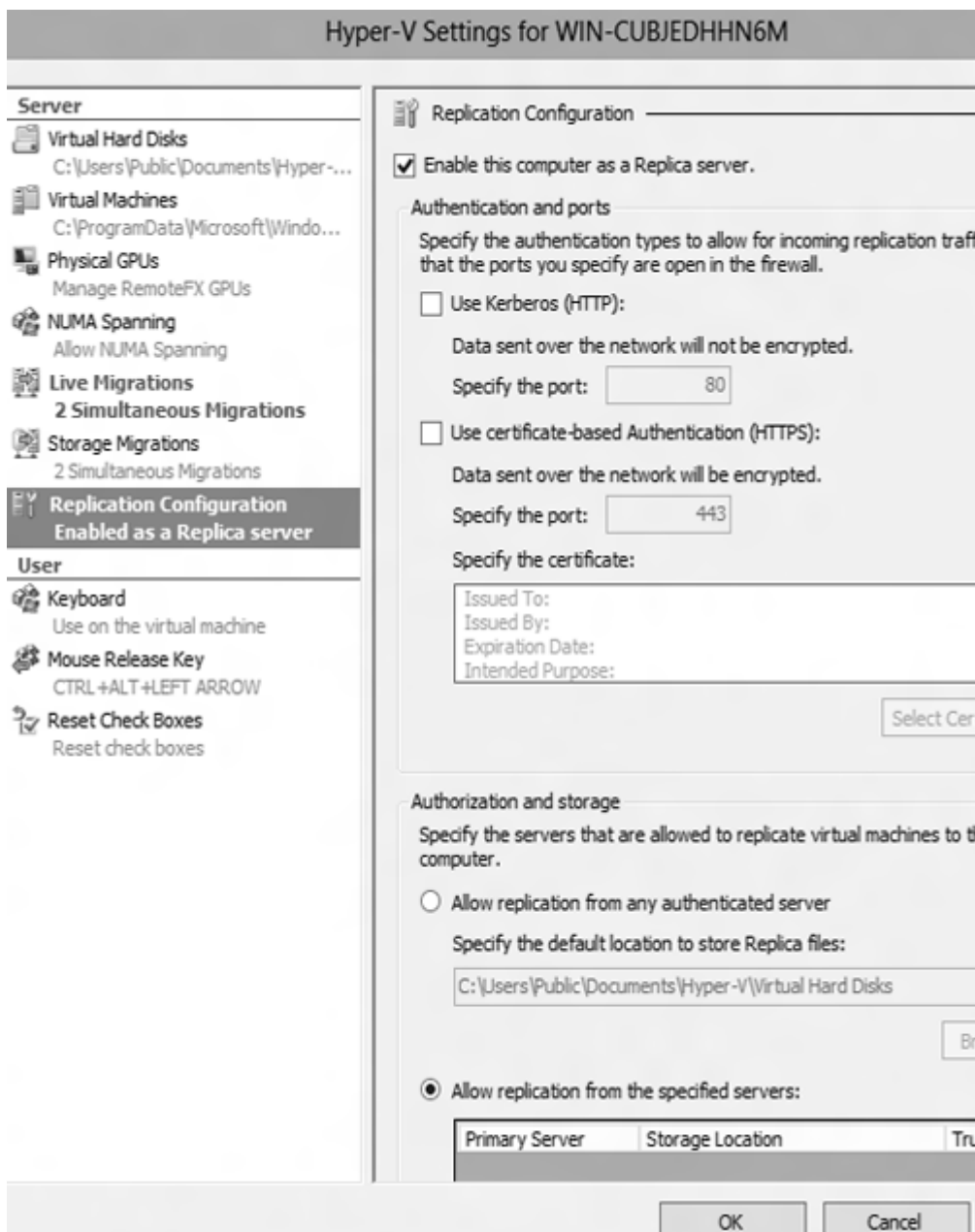


Opcja **Migracja Magazynów (Storage Migrations)** pozwala na określenie jak wiele

migracji magazynów danych może być jednocześnie wykonywana.



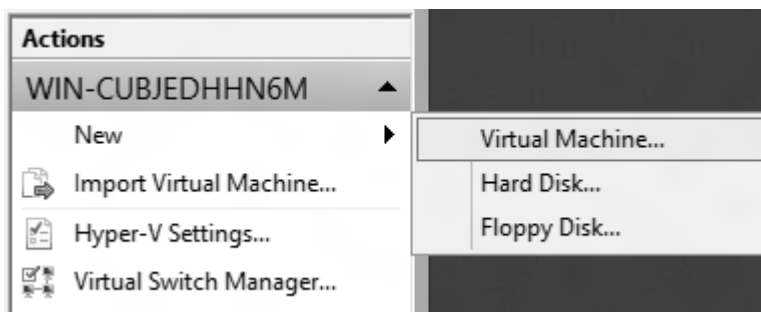
Użycie przycisku **Konfiguracja Replikacji (Replication Configuration)** pozwala na skonfigurowanie serwera Hyper-V jako serwera przechowującego replikę innych serwerów. Komunikacja pomiędzy serwerami może odbywać w sposób nie szyfrowany przy użyciu protokołu Kerberos oraz http, lub w sposób szyfrowany przy użyciu certyfikatów. Jest także możliwość określenia tego, czy mają być przyjmowane repliki z dowolnego serwera czy z określonej listy, którą można zdefiniować.



Nową maszynę można stworzyć z poziomu Menadżera Hyper-V, importując ją bądź tworząc nową przy użyciu przycisku *Nowy (New)*, a następnie wybierając *Wirtualna Maszyna (Virtual Machine)*. Można stworzyć także obraz dyskiety czy



wirtualny dysk twardy.




Otworzy się okno kreatora, kliknięcie przycisku **Zakończ (Finish)** spowoduje stworzenie maszyny wirtualnej z predefiniowanymi ustawieniami, stworzonymi przez firmę Microsoft. Jeżeli jednak administrator pragnie mieć większy wpływ na konfigurację wirtualnego komputera powinien kliknąć przycisk **Dalej (Next)**.



W kolejnym oknie kreatora określa się nazwę maszyny wirtualnej i ewentualną inną lokalizację na dysku twardym. Warto też zauważyć, że w każdej chwili można użyć przycisku **Zakończ (Finish)**, aby zakończyć kreatora pozostawiając pozostałe opcje domyślne. W przypadku książkowym zostanie kliknięty przycisk **Dalej (Next)**.



## Specify Name and Location

Before You Begin	Choose a name and location for this virtual machine.
<b>Specify Name and Location</b>	The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.
Assign Memory	Name: <input type="text" value="Windows 8"/>
Configure Networking	You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.
Connect Virtual Hard Disk	<input checked="" type="checkbox"/> Store the virtual machine in a different location
Installation Options	Location: <input type="text" value="C:\ProgramData\Microsoft\Windows\Hyper-V\"/> <input type="button" value="Browse..."/>
Summary	 If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.

Na kolejnej karcie określa się ile pamięci RAM zostanie przydzielone tej maszynie wirtualnej. Można także włączyć dynamiczne alokowanie pamięci, o czym więcej będzie za chwilę.



## Assign Memory

Before You Begin	Specify the amount of memory to allocate to this virt MB through 7346 MB. To improve performance, spec for the operating system.
Specify Name and Location	Startup memory: <input type="text" value="1024"/> MB
<b>Assign Memory</b>	<input type="checkbox"/> Use Dynamic Memory for this virtual machine.
Configure Networking	
Connect Virtual Hard Disk	

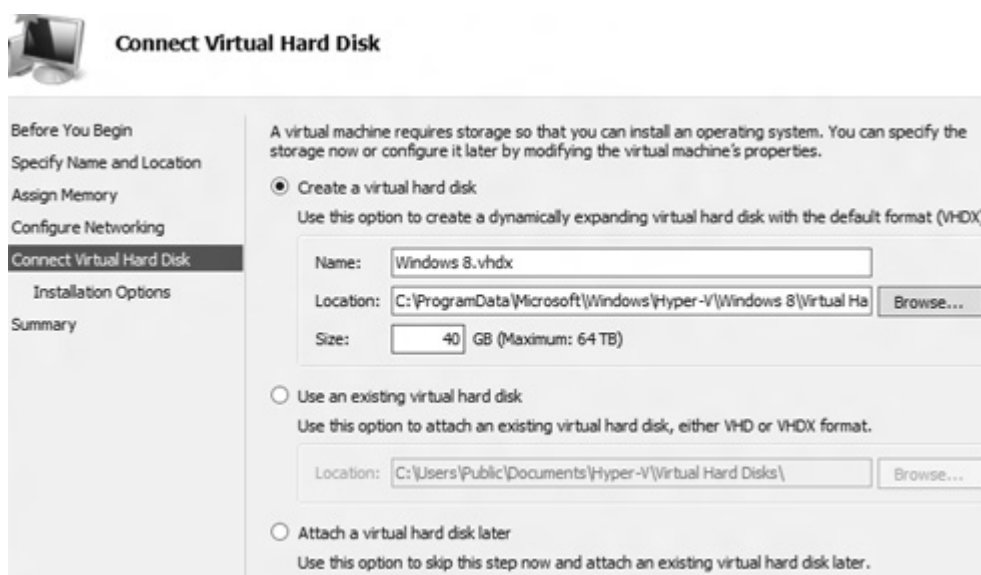
Następnie określa się wirtualny przełącznik, który zapewni komunikację z siecią.



## Configure Networking

Before You Begin	Each new virtual machine includes a network adapter. You can co virtual switch, or it can remain disconnected.
Specify Name and Location	Connection: <input type="text" value="Realtek PCIe GBE Family Controller - Virtual Switch"/>
Assign Memory	
<b>Configure Networking</b>	

Kolejny krok to tworzenie lub przyłączanie wirtualnego dysku twardego. Są trzy opcje do wyboru. Pierwsza - ***Utwórz wirtualny dysk twardy (Create a virtual hard disk)*** to stworzenie dysku twardego w formie pliku. W tym przypadku wystarczy podać jego rozmiar w GB. Druga opcja – ***Użyj istniejącego wirtualnego dysku twardego (Use an existing virtual hard disk)*** to wykorzystanie istniejącego już wirtualnego dysku twardego w formacie VHD lub VHDX. Trzecia – ***Przylącz wirtualny dysk twardy później (Attach a virtual hard disk later)*** to przyłączenie wirtualnego dysku w czasie późniejszym. Jako, że nie został wcześniej stworzony żaden dysk twardy – należy stworzyć go teraz.



Następny krok dotyczy instalacji systemu operacyjnego w maszynie wirtualnej. Można albo wykonać to w późniejszej chwili, lub podmontować napęd CD gospodarza zamiennie z obrazem ISO płyty, jak również zainstalować system operacyjny z obrazu dyskietki lub sieciowego serwera rozruchu. W tym przypadku zdecydowano się na instalację systemu Windows Server 2012 z obrazu ISO.



## Installation Options

Before You Begin  
Specify Name and Location  
Assign Memory  
Configure Networking  
Connect Virtual Hard Disk  
**Installation Options**  
Summary

You can install an operating system now if you have access to the setup media, or you can install it later.

☐ Install an operating system later

☒ Install an operating system from a boot CD/DVD-ROM

Media

☐ Physical CD/DVD drive: E: ▾

☒ Image file (.iso): F:\Windows8-ReleasePreview-32bit-English.iso Browse...

☐ Install an operating system from a boot floppy disk

Media

Virtual floppy disk (.vfd): Browse...

☐ Install an operating system from a network-based installation server

Ostatnim krokiem kreatora będzie wyświetlenie karty podsumowującej, na, której należy kliknąć przycisk **Zakończ (Finish)**.



## Completing the New Virtual Machine Wizard

Before You Begin  
Specify Name and Location  
Assign Memory  
Configure Networking  
Connect Virtual Hard Disk  
Installation Options  
**Summary**

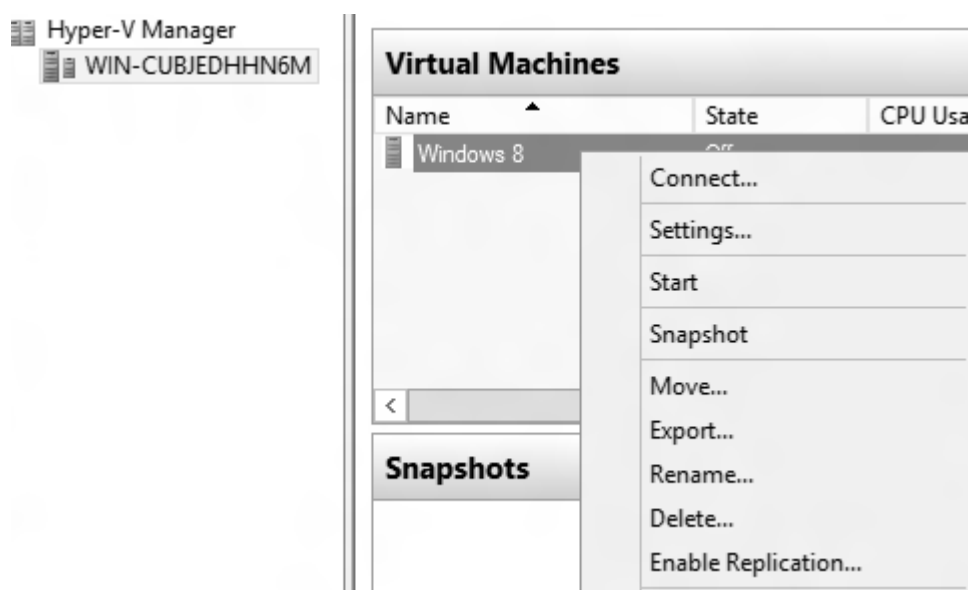
You have successfully completed the New Virtual Machine Wizard. The following virtual machine.

Description:

Name:	Windows 8
Memory:	1024 MB
Network:	Realtek PCIe GBE Family Co
Hard Disk:	C:\ProgramData\Microsoft\
Operating System:	Will be installed from F:\Win

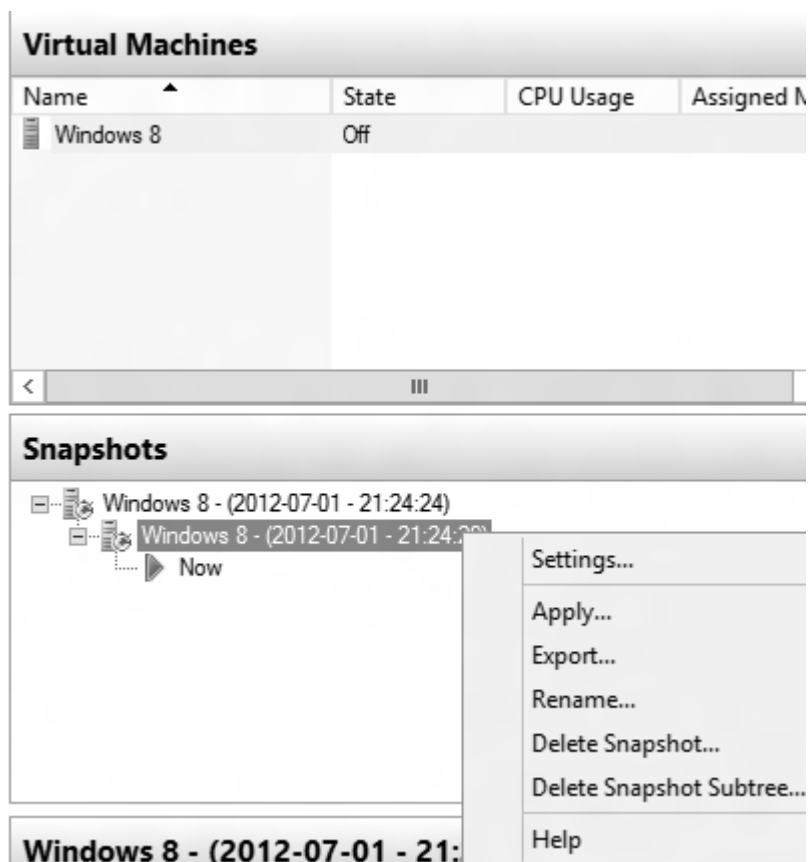
Wirtualna maszyna pojawi się w Menadżerze Hyper-V w sekcji **Maszyny Wirtualne (Virtual Machines)**. W menu kontekstowym myszy bądź po wybraniu maszyny wirtualnej w menu po prawej stronie ekranu wyświetlą się dodatkowe opcje. Pierwszą z nich jest **Połącz (Connect)**, który pozwoli na wyświetlenie okna maszyny wirtualnej, które jest realizowane na zasadzie połączenia pulpitu zdalnego.

To samo można uzyskać dwukrotnym kliknięciem na maszynie wirtualnej. Opcja **Start (Start)** uruchamia maszynę wirtualną. Opcja **Przenieś (Move)** uruchamia kreator przenoszenia maszyny wirtualnej. Opcja **Eksportuj (Export)** pozwala na wyeksportowanie maszyny wirtualnej w celu jej zaimportowania na innych komputerach. Opcja **Zmień Nazwę (Rename)** zmienia nazwę, a opcja **Usuń (Delete)** usuwa maszynę. Przydatna może się także okazać opcja **Włącz Replikację (Enable Replication)**, która uruchomi kreator ustawień replikacji dla tej maszyny wirtualnej. W kreatorze między innymi będzie konieczne wskazanie serwera docelowego bądź brokera replikacji w przypadku klastra.

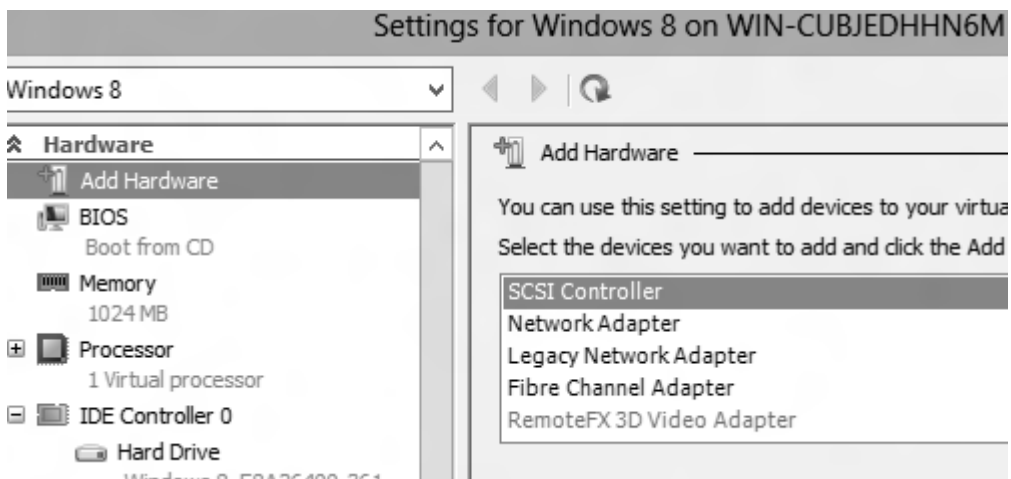


W menu kontekstowym znajduje się także opcja **Migawka (Snapshot)**, która tworzy migawki stanowiące jakby „zamrożone” wersje zainstalowanego systemu. Migawki pojawiają się w sekcji **Migawki (Snapshots)**, a w ich menu kontekstowym można migawkę zastosować przyciskiem **Zastosuj (Apply)**, co spowoduje wyzerowanie stanu maszyny wirtualnej do stanu z migawki. W menu kontekstowym znajduje się także opcja **Eksportuj (Export)** do eksportowania migawek, **Zmień Nazwę (Rename)** do zmiany ich nazwy oraz możliwość usunięcia samej migawki lub

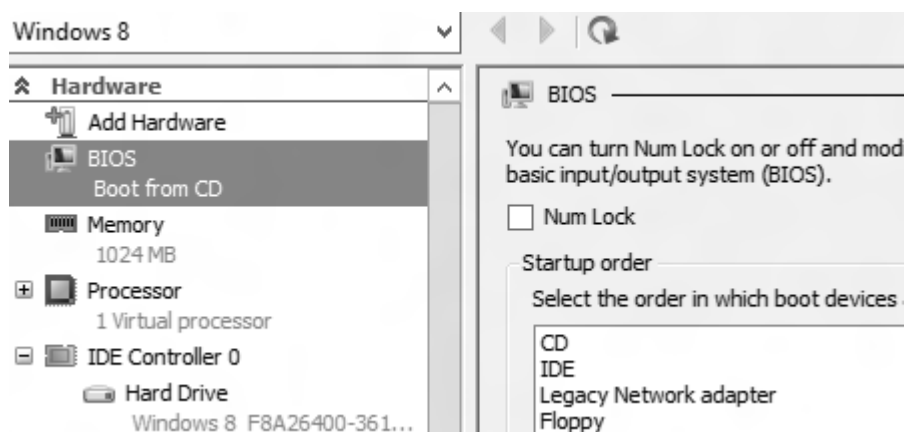
całego drzewa migawek opcjami **Usuń (Delete)**.



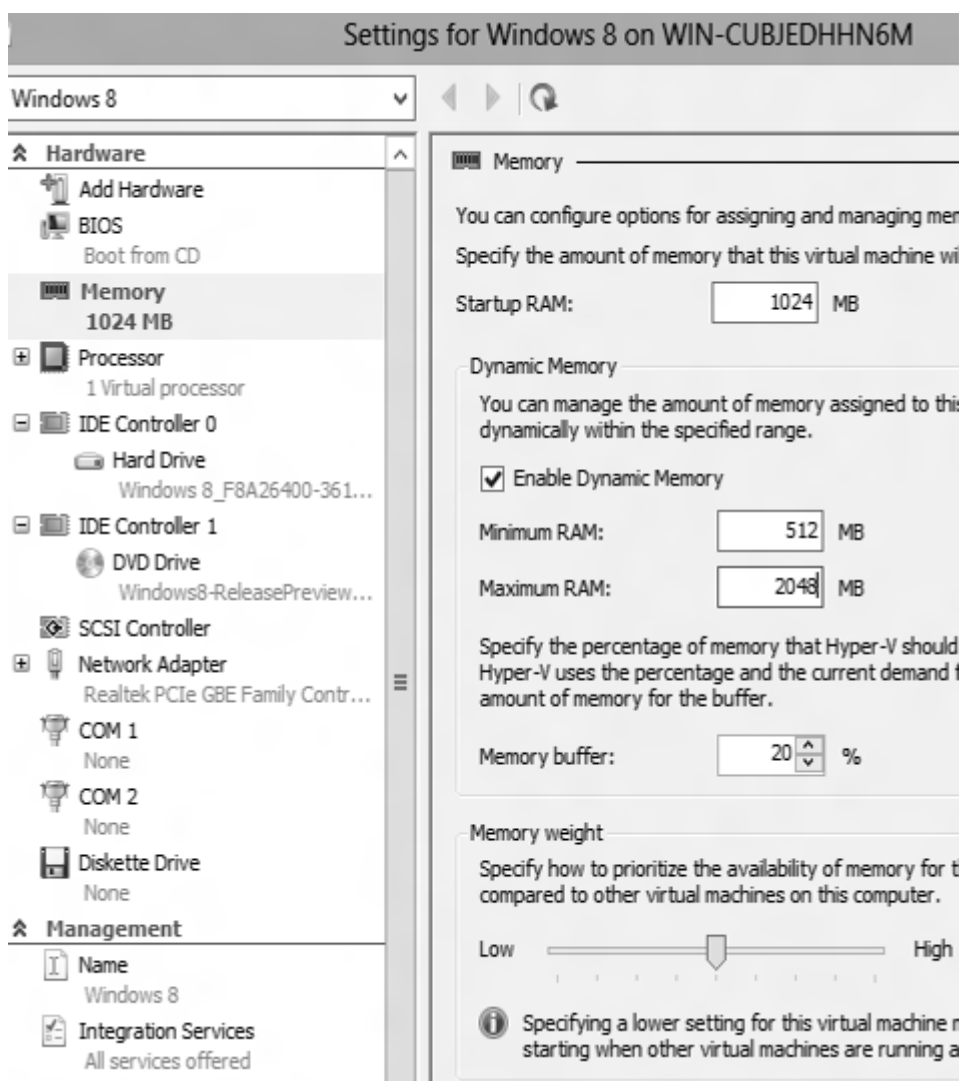
Kliknąwszy na maszynie wirtualnej prawym klawiszem myszki i wybierając opcję **Ustawienia (Settings)**, można dostać się do ustawień wirtualnego komputera. Zostanie otwarte okno konfiguracji, a w nim zaznaczona opcja **Dodaj sprzęt (Add hardware)**, pozwalająca na przypisanie maszynie wirtualnej dodatkowych urządzeń. Są nimi kontroler SCSI, karta sieciowa, stara karta sieciowa, która może być zainstalowana na starych komputerach, adapter fibre-channel oraz karta graficzna 3D poprzez funkcję RemoteFX.



W sekcji Bios definiuje się kolejność urządzeń startowych w komputerze.

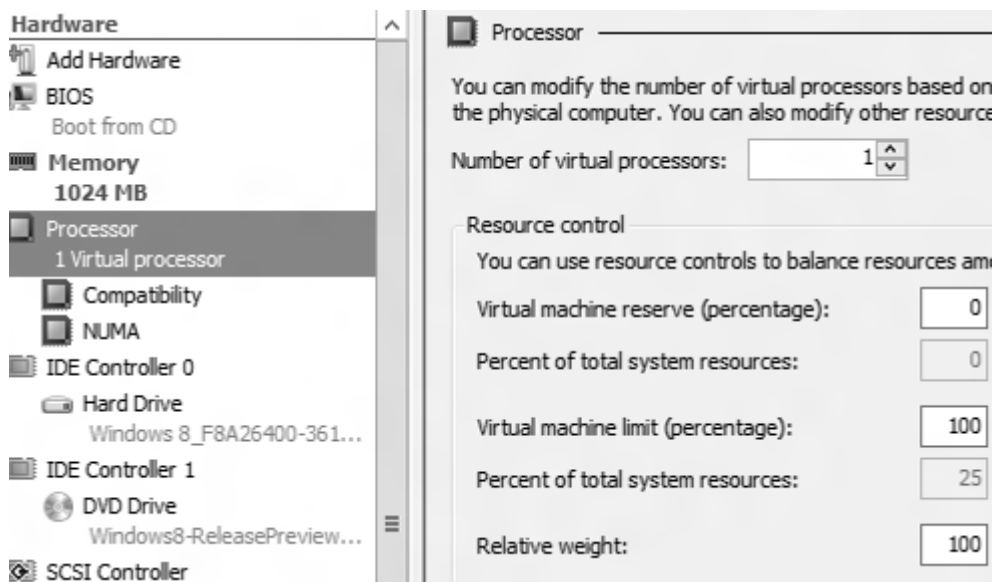


Klikając na odnośnik **Pamięć (Memory)** można ustawić stałą ilość pamięci RAM przypisaną danej maszynie, bądź uruchomić pamięć dynamiczną i określić minimum jakie maszyna musi mieć przydzielone oraz maksimum, które będzie mogła mieć przydzielone gdy zajdzie taka potrzeba i obciążenie innych maszyn na to pozwoli. Za pomocą suwaka w sekcji **Priorytet Pamięci (Memory Weight)** określa się priorytet dla tej maszyny wirtualnej. Maszyna o najwyższym priorytecie będzie miała przydzielaną pamięć w pierwszej kolejności.

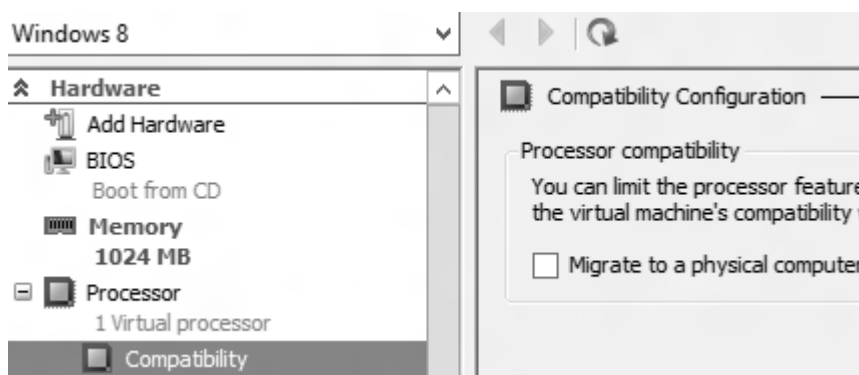


Po kliknięciu w **Procesor (Processor)** administrator ma możliwość określenia ilości wirtualnych procesorów przydzielonych maszynie, a także ustawienia kontroli zasobów, ponieważ te same procesory prawdopodobnie będą dzielone z innymi maszynami. Między innymi można także określić procentową rezerwację mocy procesora oraz procentowo maksymalne zużycie procesora, jak również priorytet, który działa analogicznie do pamięci dynamicznej pod parametrem **Relatywny Priorytet (Relative Weight)**.

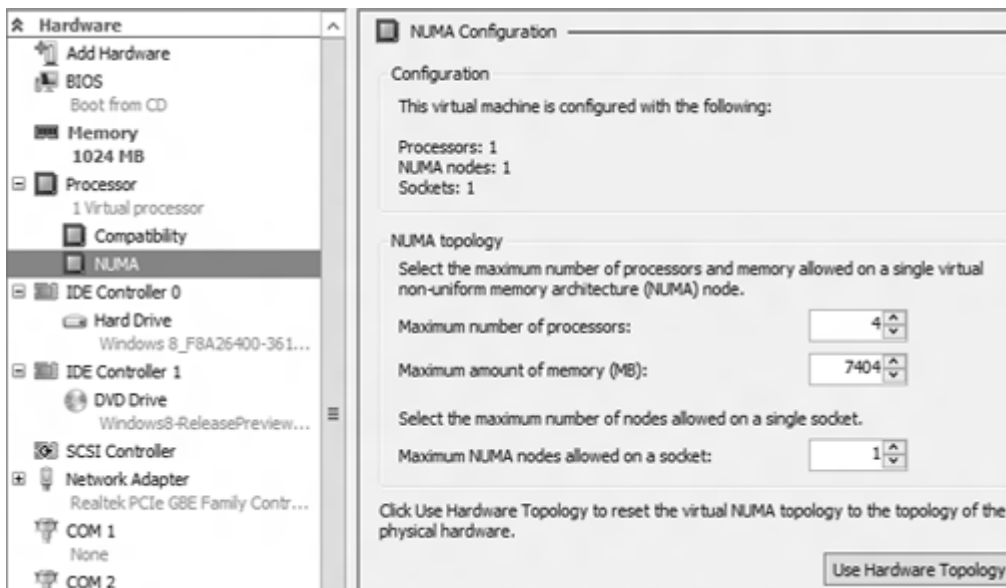




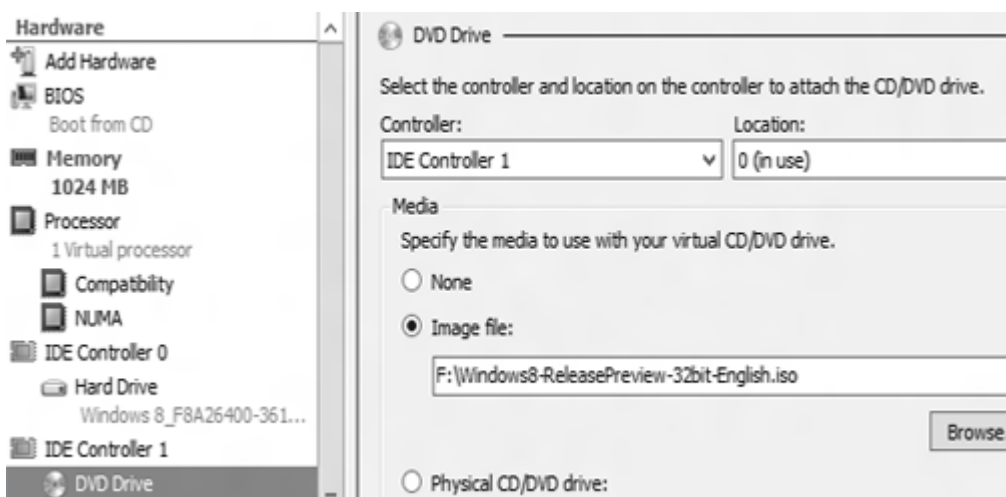
W momencie gdy zostanie rozwinięte drzewo procesor i wybrana opcja **Kompatybilność (Compatibility)**, istnieje możliwość wybrania opcji migracji na komputer z innym procesorem. Przydaje się ona wtedy gdy maszyna została zaimportowana na innym hoście.



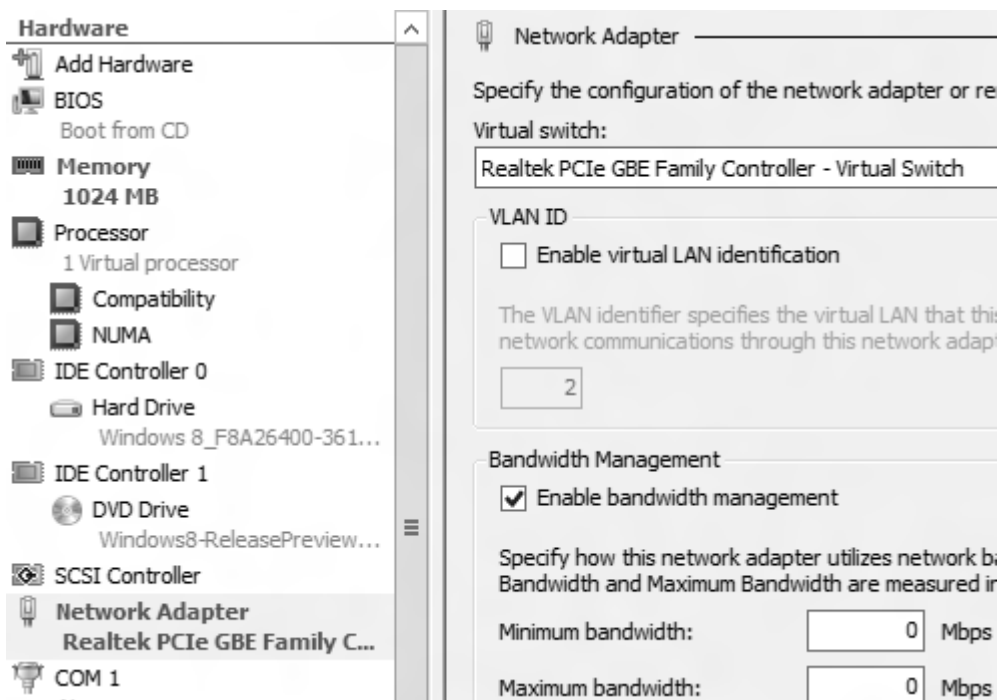
Pole niżej w menu to opcja NUMA, w ramach której określa się maksymalną ilość procesorów z jakich maszyna może korzystać oraz maksymalną ilość pamięci operacyjnej.



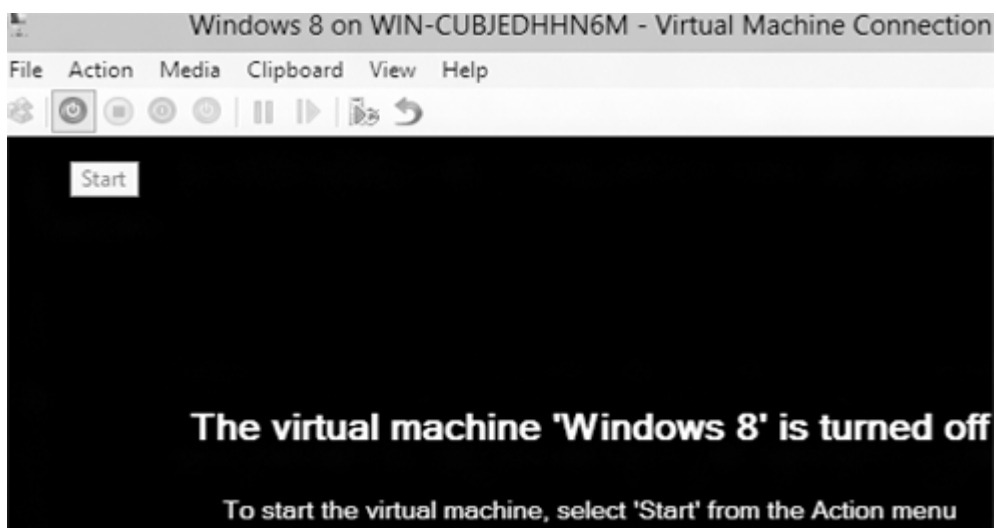
Znajdują się także kontrolery IDE, do każdego z nich można podpiąć dwa urządzenia. Będzie to albo dysk twardy albo napęd optyczny, do którego można podmontować obraz ISO lub fizyczny napęd gospodarza.



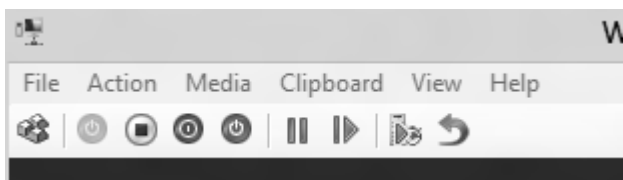
Poniżej znajdują się także ustawienia kontrolera sieci, gdzie można ustalić minimalną oraz maksymalną przepustowość adaptera w tej maszynie wirtualnej.



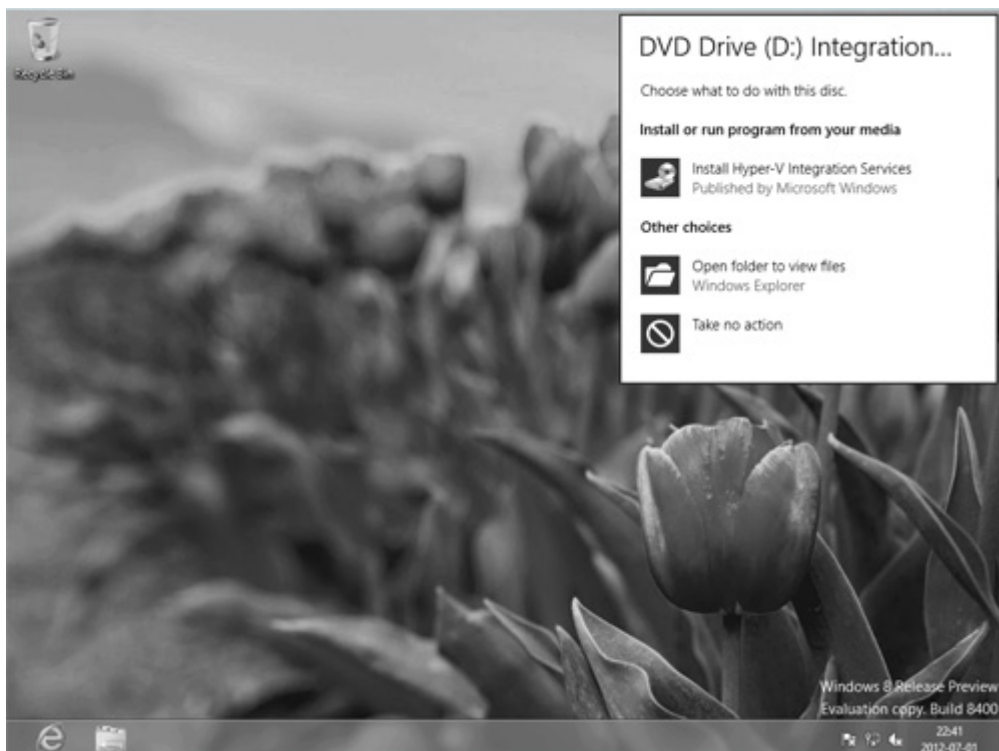
Przyciskiem OK należy zatwierdzić ustawienia i wrócić do Menadżera Hyper-V, w którym dwukrotnie należy kliknąć na utworzonej maszynie wirtualnej, a w oknie, które się pojawi nacisnąć przycisk **Start** w celu uruchomienia komputera.



Ładuje się system operacyjny z płyty. Można na nim pracować tak jak na zwykłym systemie operacyjnym. Natomiast myszkę, która zostanie uwięziona w oknie maszyny wirtualnej można uwolnić kombinacją klawiszy CTRL+Shift+strzałka w lewo. W górnym menu obok przycisku Start znajduje się ikonka symbolizująca trzy guziczki służące do wysłania do maszyny wirtualnej kombinacji klawiszy CTRL+ALT+Delete. Po prawej stronie guzika Start znajdują się kolejno przycisk **Turn Off** powodujący wyłączenie maszyny wirtualnej, jednoznaczny z odłączeniem prądu, przycisk **Shut Down**, wysyłający sygnał wyłączenia do maszyny wirtualnej, przycisk **Save** pauzujący i zapisujący stan maszyny wirtualnej, przycisk **Pause** wstrzymujący maszynę wirtualną oraz przyciski **Reset**, **Snapshot** i **Revert**.



W górnym menu rozwijając przycisk **Widok (View)** istnieje możliwość uruchomienia maszyny w trybie pełnoekranowym. Przycisk **Schowek (Clipboard)** daje możliwość skopiowania do maszyny wirtualnej zawartości schowka oraz wykonania zrzutu ekranu maszyny wirtualnej. Pod przyciskiem **Nośniki (Media)** kryje się możliwość szybszego niż przez ustawienia podmontowania obrazu ISO lub napędu optycznego gospodarza. W menu **Akcje (Action)** znajdują się te same opcje, za które odpowiadają ikony. Istnieje także opcja **Włóż dysk narzędzi integracji maszyny wirtualnej (Insert integration services setup disk)**, którą bezwzględnie należy uruchomić po zainstalowaniu systemu operacyjnego w celu lepszego zintegrowania go z serwerem Hyper-V oraz wgrania sterowników.

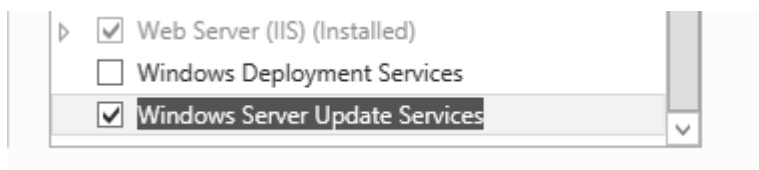


Nowością w Hyper-V jest także stworzenie nowej lokalnej grupy zabezpieczeń o nazwie *Administratorzy Hyper-V (Hyper-V Administrators)*. Wystarczy dodać do niej użytkownika, aby ten miał pełen dostęp do funkcji Hyper-V.

## 16. Windows Server Update Services

Należy dodać nową rolę do serwera, wybierając z listy Windows Server Update Services i następnie kliknąć **Dalej(Next)**. Wymagany będzie IIS. Niniejsza usługa pobiera z oficjalnej witryny Microsoft Windows Update bądź z innego lokalnego serwera WSUS aktualizacje produktów Microsoft, które zostaną wybrane w kreatorze konfiguracji. Następnie są one propagowane do innych komputerów w sieci tak, aby nie musiały one korzystać z oficjalnej witryny Windows Update i nadmiernie obciążać firmowych łącz.

Po wybraniu Windows Server Update Services klika się **Dalej (Next)**.



Karta powitalna kreatora informuje o tym, za co odpowiada serwer WSUS, a także o tym jakie wymagania sieci muszą być zapewnione na maszynie hostującej tą rolę. Informuje także o tym iż komunikacja pomiędzy komputerami klienckimi a serwerem oraz pomiędzy serwerami powinna być szyfrowana protokołem SSL.

Windows Server Update Services (WSUS) allows administrators to manage the download and installation of updates from the Microsoft Update website to the local network.

### Things to note:

- At least one WSUS server in a network must be able to download updates from Microsoft Update. Other WSUS server can get updates either from that server or from Microsoft Update.
- WSUS server-to-server and server-to-client communications should be set up to use the Secure Sockets Layer (SSL).

W kolejnym oknie kreatora należy wybrać składniki roli Windows Server Update Services, które powinny zostać zainstalowane. Niezbędne będą WSUS Services oraz

jedna z baz danych (obu nie można zainstalować jednocześnie).

Select the role services to install for Windows Server Update Services

Role services	Description
<input checked="" type="checkbox"/> WID Database	
<input checked="" type="checkbox"/> <b>WSUS Services</b>	
<input type="checkbox"/> Database	

Installs the services used by Windows Server Update Services: Update Service, the Reporting Web Service, the API Remoting Web Service, the Client Web Service, the Simple Web Authentication Web Service, the Server Synchronization Service, and the DSS Authentication Web Service.

W kolejnym oknie kreatora należy podać miejsce, gdzie mają być przechowywane pobrane aktualizacje. Musi być to partycja o rozmiarze wynoszącym minimum 6GB oraz sformatowana w systemie plików NTFS. Zaleca się użycie szybkiej macierzy dyskowej, aby wysyłać aktualizacje do maszyn klienckich bez opóźnień, o rozmiarze dostosowanym do ilości wybranych produktów Microsoft dla których mają zostać pobrane aktualizacje.

If you have a drive formatted with NTFS and at least 6 GB of free disk space, you can use it to store updates for client computers to download quickly.

If you need to save disk space, clear the check box to store updates on Microsoft Update; downloads will be slower.

If you choose to store updates locally, updates are not downloaded to your WSUS server until you approve them. By default, when updates are approved, they are downloaded for all languages.

☒ Store updates in the following location (choose a valid local path on ELITEPC-DC01.elitepc.pl, or a remote path) :

C:\WSUS

W oknie podsumowującym należy kontynuować instalację klikając przycisk **Zainstaluj (Install)**.

To install the following roles, role services, or features on sel

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be di  
been selected automatically. If you do not want to install the  
their check boxes.

Remote Server Administration Tools

Role Administration Tools

Windows Server Update Services Tools

API and PowerShell cmdlets

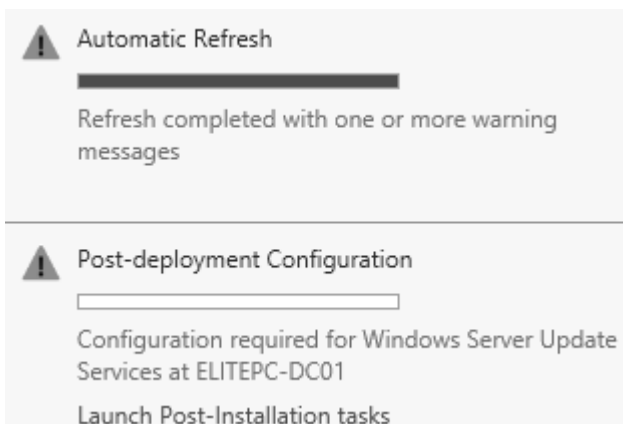
User Interface Management Console

Windows Server Update Services

WSUS Services

WID Database

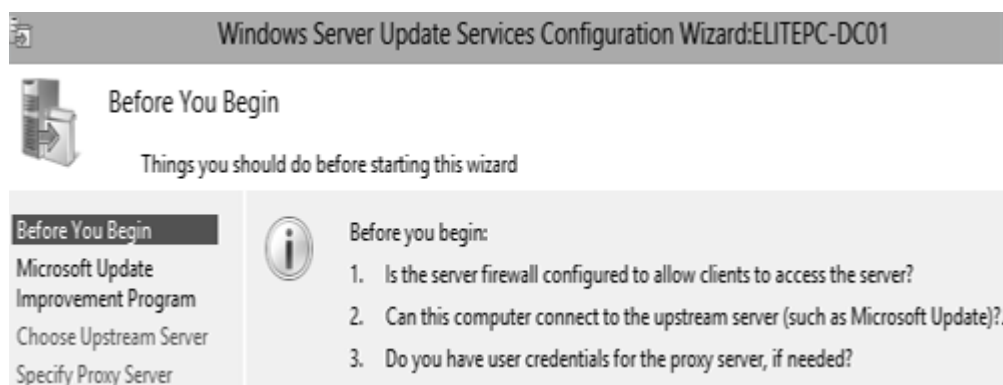
Gdy wszystkie wymagane pliki zostaną zainstalowane w Menadżerze Serwera, a dokładniej w Centrum Akcji należy kliknąć ***Uruchom czynności post instalacyjne (Launch Post Installation Tasks)*** w sekcji ***Konfiguracja powdrożeniowa (Post-deployment Configuration)*** dla Windows Server Update Services.



W ten sposób uruchomiony zostanie kreator konfiguracji roli, która właśnie została zainstalowana. Informuje on o tym, że zanim rozpocznie się proces konfiguracji, powinna zostać skonfigurowana zapor systemowa tak, aby umożliwiała klientom



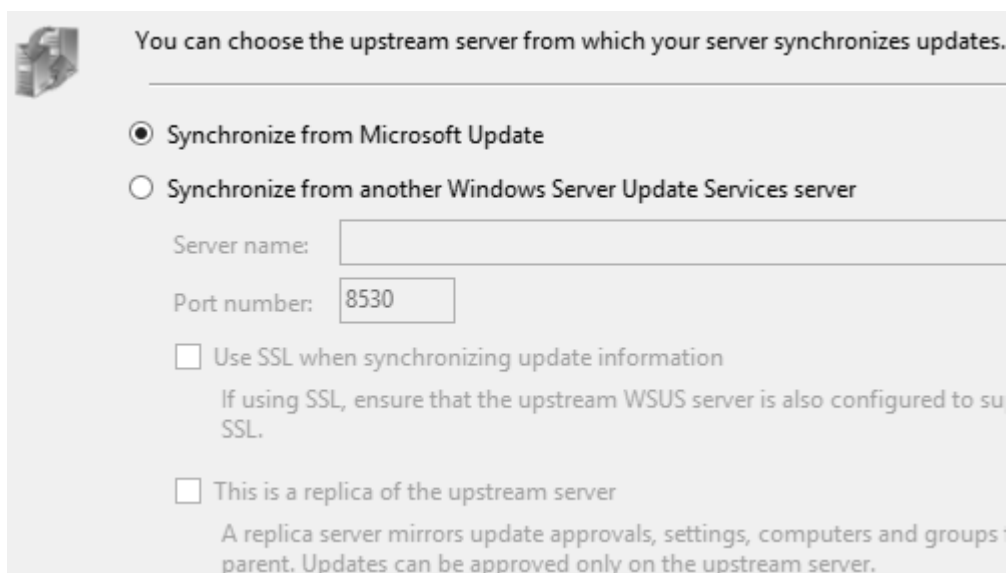
łączenie się z tym serwerem, temu serwerowi na łączenie się z witryną Microsoft Windows Update oraz uzyskać informacje dotyczące serwera Proxy jeżeli taki jest używany.



W kolejnym oknie kreatora można przystąpić do programu poprawy jakości produktów Microsoft, nie jest to jednak obligatoryjne.



Następnie określa się czy serwer ma się synchronizować z oficjalną witryną Microsoft Update czy z innym serwerem WSUS.



This screenshot shows a configuration window titled "You can choose the upstream server from which your server synchronizes updates." It features two radio button options. The first option, "Synchronize from Microsoft Update", is selected. The second option, "Synchronize from another Windows Server Update Services server", is unselected. Below the second option, there are input fields for "Server name:" and "Port number:" (containing "8530"). There are also two checkboxes: "Use SSL when synchronizing update information" (unchecked) and "This is a replica of the upstream server" (unchecked). A note explains that a replica server mirrors update approvals, settings, computers and groups, and that updates can only be approved on the upstream server.

You can choose the upstream server from which your server synchronizes updates.

☒ Synchronize from Microsoft Update

☐ Synchronize from another Windows Server Update Services server


Server name:

Port number:

☐ Use SSL when synchronizing update information  
If using SSL, ensure that the upstream WSUS server is also configured to support SSL.

☐ This is a replica of the upstream server  
A replica server mirrors update approvals, settings, computers and groups on the upstream server. Updates can be approved only on the upstream server.

Kolejna karta kreatora to opcjonalne ustawienia serwera Proxy.



This screenshot shows a configuration window titled "If this server requires a proxy server to access the upstream server, you can configure proxy server settings here." It features a checkbox "Use a proxy server when synchronizing" which is unchecked. Below it are input fields for "Proxy server name:" and "Port number:" (containing "80"). There is another checkbox "Use user credentials to connect to the proxy server" which is unchecked. Below it are input fields for "User name:", "Domain:", and "Password:". At the bottom, there is a checkbox "Allow basic authentication (password is sent in cleartext)" which is unchecked.

If this server requires a proxy server to access the upstream server, you can configure proxy server settings here.

☐ Use a proxy server when synchronizing

Proxy server name:

Port number:

☐ Use user credentials to connect to the proxy server

User name:

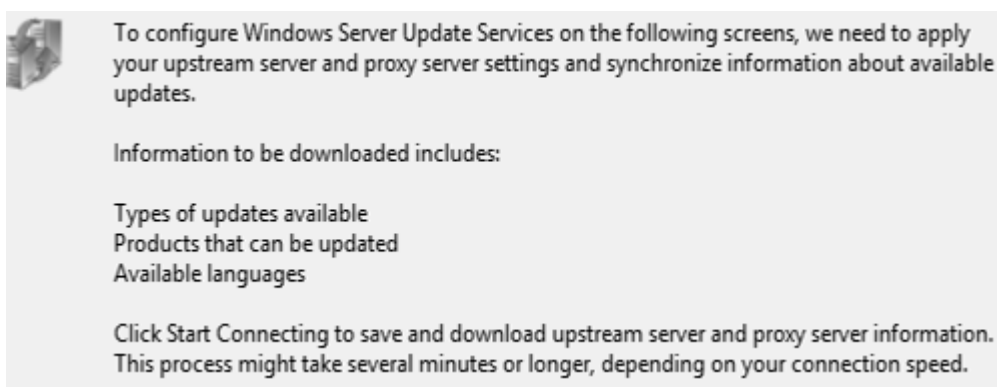
Domain:

Password:

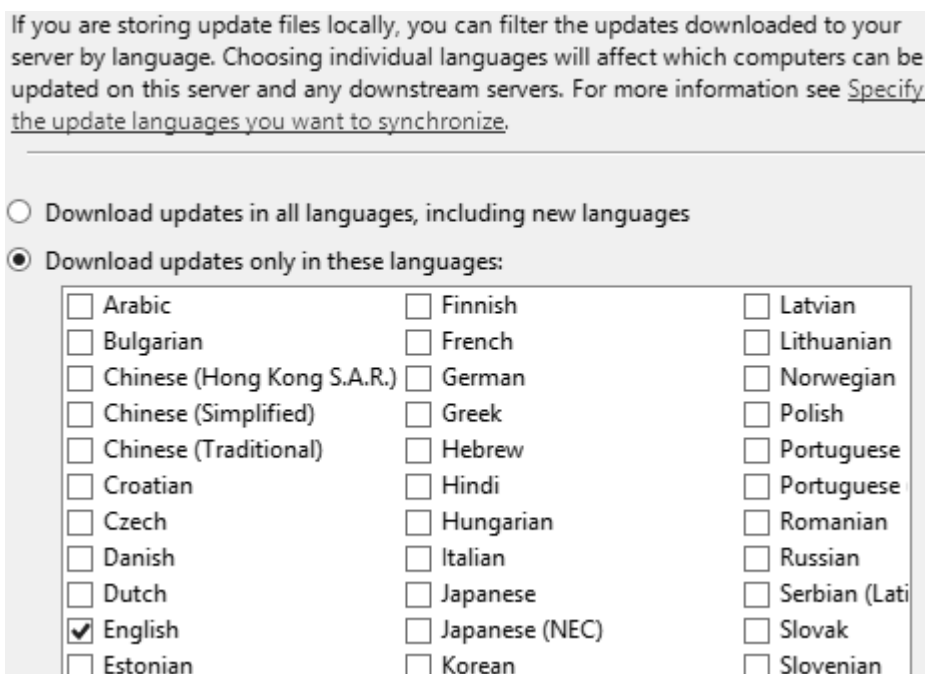
☐ Allow basic authentication (password is sent in cleartext)

Następnie kreator spróbuje nawiązać połączenie z witryną Microsoft Update w celu

pobrania informacji na temat rodzajów dostępnych aktualizacji, listy produktów które mogą być aktualizowane oraz języków w jakich te produkty są dostępne.

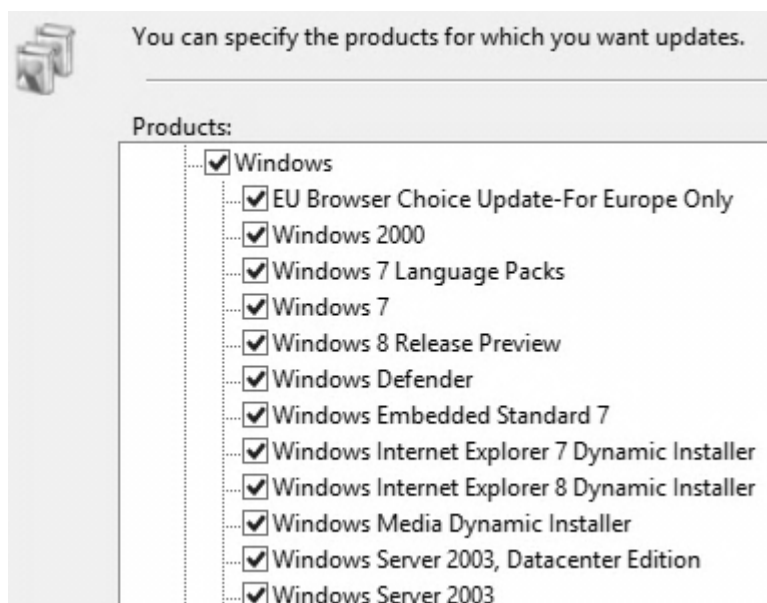


Gdy niezbędne informacje zostaną już pobrane w pierwszej kolejności należy wybrać języki produktów dla jakich będą pobierane aktualizacje.

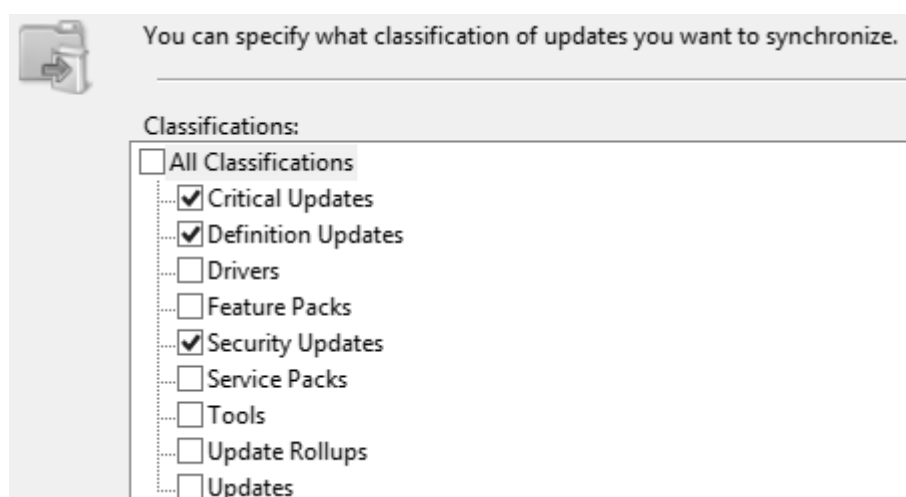


Po wybraniu języków koniecznej jest wybranie z listy produktów, które są używane

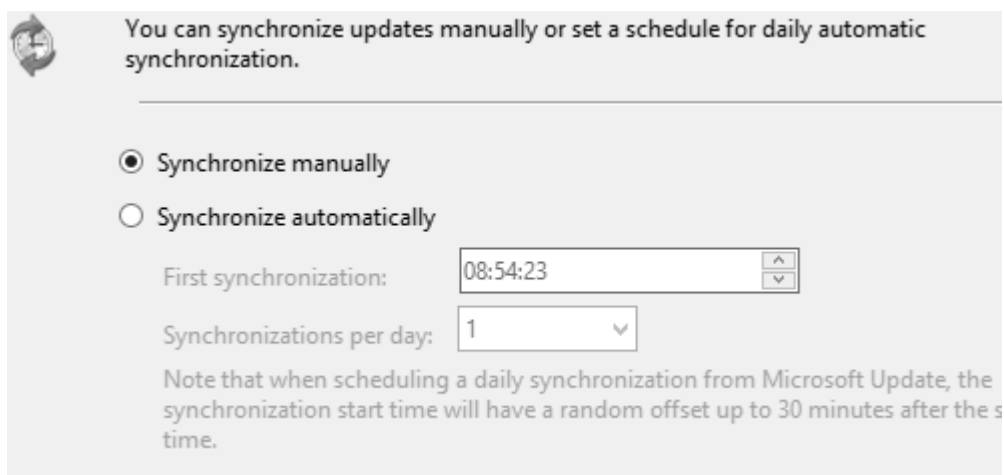
w przedsiębiorstwie, tak aby pobierać wyłącznie te aktualizacje, które są niezbędne.



W kolejnym kroku określa się rodzaje aktualizacji, jakie mają być pobierane z witryny Microsoft Update. Do wyboru są aktualizacje krytyczne, aktualizacje definicji, sterowniki, pakiety funkcji, aktualizacje zabezpieczeń, aktualizacje zbiorcze Service Pack, narzędzia, aktualizacji Rollupów oraz zwykłe aktualizacje.

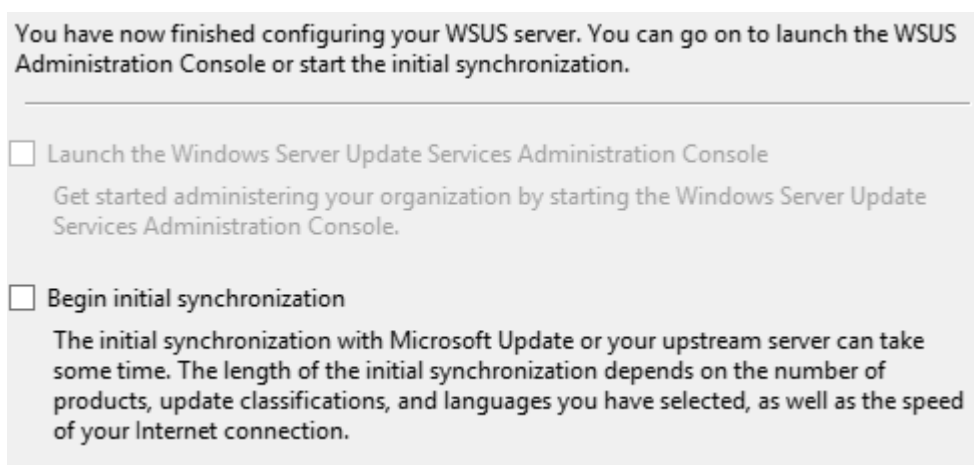


Gdy uda się przefiltrować pożądane pliki do pobrania należy określić czy serwer WSUS będzie synchronizowany z witryną Windows Update ręcznie czy automatycznie. Zaleca się aby aktualizacje pobierać w godzinach nocnych.



The screenshot shows a configuration window titled "You can synchronize updates manually or set a schedule for daily automatic synchronization." It features two radio buttons: "Synchronize manually" (selected) and "Synchronize automatically". Below the "Synchronize automatically" option, there are two input fields: "First synchronization:" with a time value of "08:54:23" and "Synchronizations per day:" with a value of "1". A note at the bottom states: "Note that when scheduling a daily synchronization from Microsoft Update, the synchronization start time will have a random offset up to 30 minutes after the time."

Kończąc kreator konfiguracji opcją **Rozpocznij pierwszą synchronizację (Begin initial synchronozation)** można rozpocząć wstępną synchronizację. Z racji tego, że do pobrania będzie pokaźna ilość danych, należy uzbroić się w cierpliwość.



The screenshot shows a configuration window titled "You have now finished configuring your WSUS server. You can go on to launch the WSUS Administration Console or start the initial synchronization." It features two checkboxes: "Launch the Windows Server Update Services Administration Console" and "Begin initial synchronization". Below the "Begin initial synchronization" checkbox, there is a paragraph of text: "The initial synchronization with Microsoft Update or your upstream server can take some time. The length of the initial synchronization depends on the number of products, update classifications, and languages you have selected, as well as the speed of your Internet connection."

W karcie podsumowującej należy kliknąć **Zakończ (Finish)**.

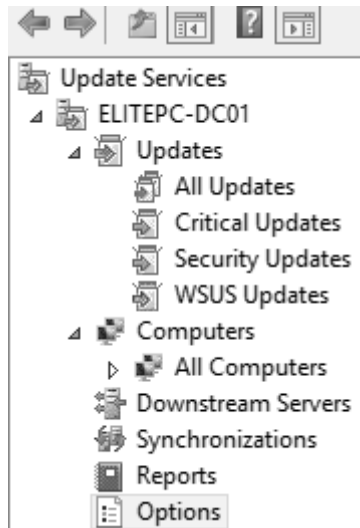
Next Steps: To fully configure your system, you should explore the following topics:

1. [Using SSL with WSUS](#)
2. [Create computer groups](#)
3. [Assign computers to groups using Group Policy](#)
4. [Configure auto-approval rules](#)

Po zakończeniu kreatora rola WSUS pojawi się w Menadżerze Serwera, aby nią zarządzać należy na wybranym serwerze kliknąć prawym przyciskiem myszy i wybrać Windows Server Update Services.



W konsoli zarządzania rolą Windows Server Update Services warto szczególną uwagę zwrócić na **Opcje (Options)**.



W tym miejscu znajdują się dodatkowe ustawienia WSUS. Opcja Automatic Approvals pozwala określić jak automatycznie zatwierdzić instalację updateów dla wybranych grup. Synchronization Schedule pozwala zarządzać automatycznymi synchronizacjami bądź synchronizować się manualnie. Computers określa w jaki sposób maszyny przypisywane są do grup. Warto także zaznajomić się z innymi ustawieniami. Na szczególną uwagę zasługuje Server Cleanup Wizard, czyli kreator oczyszczania serwera.



### Automatic Approvals

You can specify how to automatically approve installation of updates for selected groups and how to approve revisions to existing updates.



### Synchronization Schedule

You can choose to synchronize manually or set a schedule for daily automatic synchronization.



### Computers

You can specify how to assign computers to groups.



### Server Cleanup Wizard

You can use server cleanup to free up old computers, updates and update files from your server.



### Reporting Rollup

You can choose to have replica downstream servers roll up update and computer status.



### E-Mail Notifications

You can have Windows Server Update Services send e-mail notifications of new updates and status reports.



### Microsoft Update Improvement Program

You have the option of joining the Microsoft Update Improvement Program to improve the quality, reliability, and performance of Microsoft software.



### Personalization

You can choose how downstream server rollup data is displayed, which items are shown in the To Do list, and how validation errors are displayed.



### WSUS Server Configuration Wizard

You can configure several of the basic Windows Server Update Services settings by running this wizard. Each of the settings here can be configured separately, using

Kreator oczyszczania serwera pozwala na automatyczne kasowanie nieużywanych i nieaktualnych plików. W oknie, które się pojawi określa się elementy, które mają zostać oczyszczone.




Welcome to the WSUS Server Cleanup Wizard. With the help of this wizard, you can remove out-of-date and unused update files, old revisions of updates, superseded updates, and computers that are no longer active.

What would you like to clean up?

- ☒ Unused updates and update revisions  
Delete updates that are expired and have not been approved for 30 days or more, and delete older update revisions that have not been approved for 30 days or more.
- ☒ Computers not contacting the server  
Delete computers that have not contacted the server in 30 days or more.
- ☒ Unneeded update files  
Delete update files that aren't needed by updates or downstream servers.
- ☒ Expired updates  
Decline updates that aren't approved and have been expired by Microsoft.
- ☒ Superseded updates  
Decline updates that have not been approved for 30 days or more, are not currently needed by any clients, and are superseded by an approved update.

Gdy WSUS jest odpowiednio skonfigurowany należy zadbać o rzecz najważniejszą, czyli o to, aby maszyny klienckie wiedziały, że mają korzystać z tego serwera zamiast oficjalnej witryny Microsoft Update. Aby wymusić aktualizację z lokalnego serwera należy dokonać odpowiedniej edycji polisy związanej z intranetową witryną Windows Update. W anglojęzycznej wersji systemu Windows Server 2012 nosi ona nazwę ***Allow signed updates from an intranet Microsoft updates service location***.

 Allow signed updates from an intranet Microsoft update service location Previous Setting

☒ Not Configured      Comment:

☐ Enabled

☐ Disabled

Supported on:

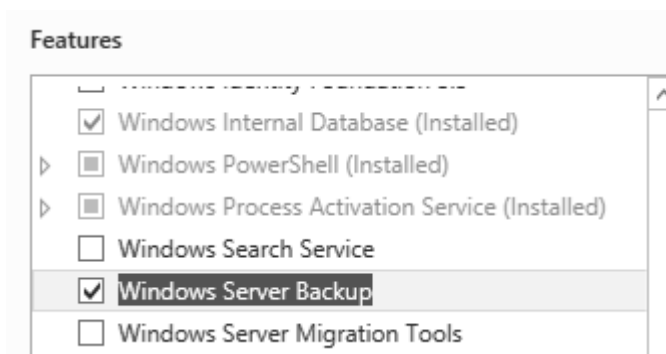
Options:       Help:

## 17. Bezpieczeństwo danych i komputera

Backup to rzecz podstawowa w pracy administratora. Dane jak i same systemy trzeba nieustannie archiwizować na bezpiecznych nośnikach danych.

### a. Windows Backup

Należy dodać funkcję do serwera, mianowicie *Kopia zapasowa systemu Windows Serwer (Windows Server Backup)* i kliknąć *Dalej (Next)*. Resztę instalacji przechodzi się analogicznie do instalacji innych ról.



Po zainstalowaniu powyższej funkcji można teraz wejść w *Narzędzia Administracyjne > Kopia zapasowa Systemu Windows Serwer (Tools > Windows Server Backup)*.



Uruchomiona w ten sposób zostanie konsola backupu w systemie Windows Server.

## Windows Server Backup (Local)

Backup your important data to a local or online location

### Local Backup

**Last Backup Status:** -

**Next Backup Time:** -

**Number of available backups:** -

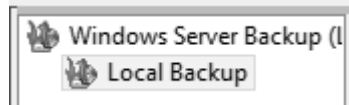
### Online Backup

You can now backup your critical data to online storage automatically. [More Information](#)

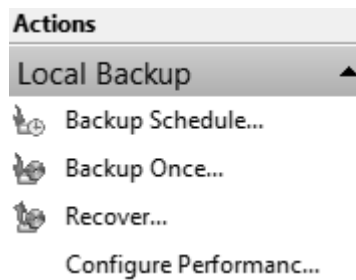
Kopię zapasową można wykonywać standardowo na nośnikach lokalnych. Nowością w Windows Server 2012 jest możliwość backupu danych w chmurze.

Microsoft Online Backup Service — strona główna	<h2>Microsoft Online</h2> <div><b>Beta feedback</b></div> <div><b>Discussion forum</b></div> <div><b>Downloads</b></div> <div><b>Updates</b></div> <div>Microsoft Online Backup provide a low cost choice for customers. With no up connection), customer against disasters.</div> <div>Before we make this p small group of you to t</div>
Pliki do pobrania	
Ankiety	

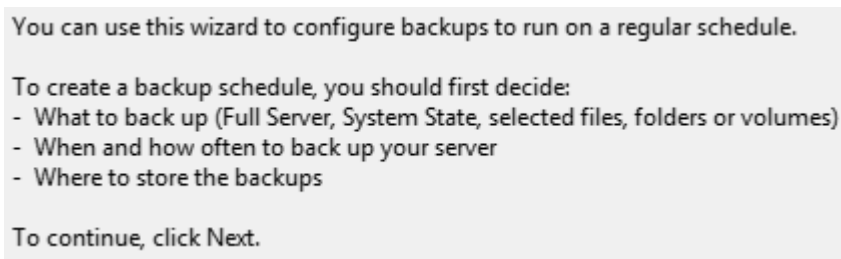
W drzewie po lewej stronie znajdują się listy dostępnych kopii zapasowych.



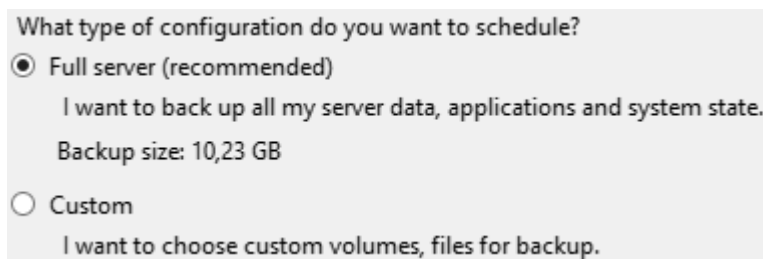
Następnie należy kliknąć opcję **Harmonogram wykonywania (Backup Schedule)**, która znajduje się w prawym panelu na samej górze.



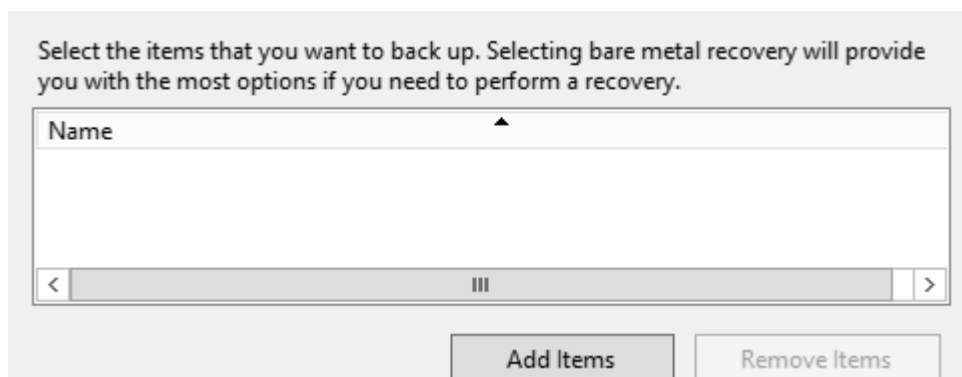
Otworzy się kreator harmonogramu wykonywania kopii zapasowych, w którym zachodzi potrzeba kliknięcia przycisku **Dalej (Next)**.



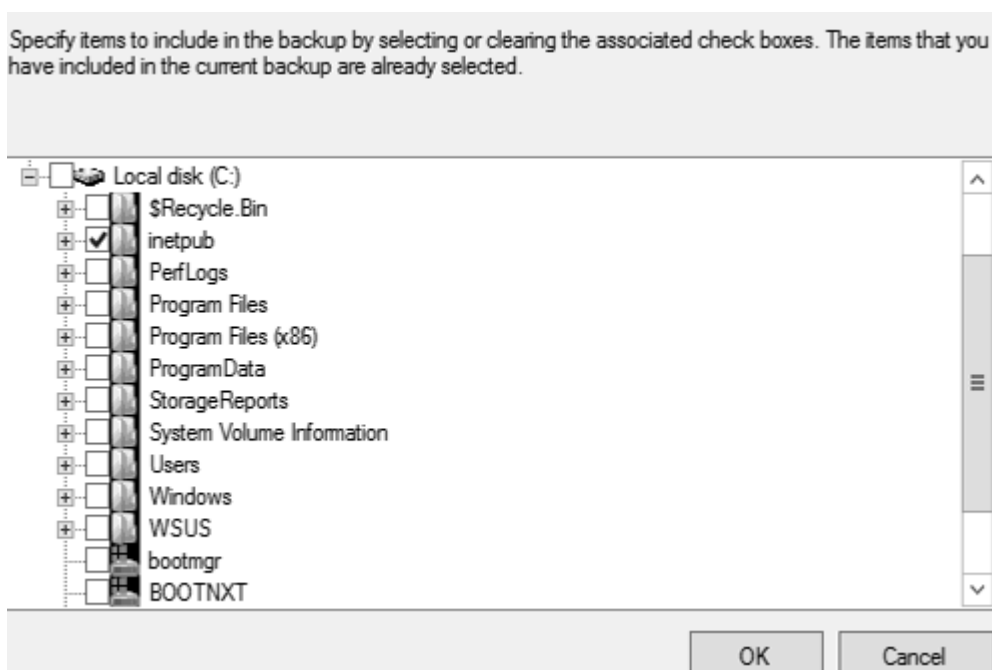
Następnie należy wybrać **Konfigurację Niestandardową (Custom)** i kliknąć **Dalej (Next)**.



Należy kliknąć **Dodaj Elementy (Add Items)**, dzięki czemu możliwe jest dodanie tylko określonych elementów do skopiowania zamiast wykonywania kopii całego serwera. Jest to przydatne gdy administrator pragnie przechowywać różnego rodzaju dane w różnych bezpiecznych lokalizacjach.



Na następnej karcie wybiera się elementy do wykonania kopii zapasowej.



W następnym kroku należy określić harmonogram wykonywania kopii, czyli w

jakich godzinach ma być wykonana kopia zapasowa.

How often and when do you want to run backups?

☐ Once a day  
Select time of day: 21:00

☒ More than once a day  
Click an available time and then click Add to add it to the backup schedule.

Available time:		Scheduled time:
18:30	<div>Add &gt;</div> <div>&lt; Remove</div>	21:00
19:00		23:30
19:30		
20:00		
20:30		
21:30		
22:00		
22:30		
23:00		

Następnie należy określić typ miejsca docelowego. Do wyboru jest **kopia na dysku lokalnym** (*Back up to a hard disk that is dedicated for backups*), **na woluminie** (*Back up to a volume*) oraz w **lokalizacji sieciowej** (*Back up to a shared network folder*)

Where do you want to store the backups?

☒ Back up to a hard disk that is dedicated for backups (recommended)  
Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups.

☐ Back up to a volume  
Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume.

☐ Back up to a shared network folder  
Choose this option if you do not want to store backups locally on the server. Note that you will only have one backup at a time because when you create a new backup it overwrites the previous backup.

Jeżeli administrator zdecyduje się na wykorzystanie całych dysków, w zależności od ich ilości kreator połączy je w macierz Raid oraz je sformatuje i przygotuje do przechowywania kopii zapasowej.

Select one or more disks to store your backups. You can use multiple backup disks if you want to store disks offsite.

Available disks:

Disk	Name	Size	Used Space	Volumes in D...
------	------	------	------------	-----------------

Show All Available Disks...

W ćwiczeniowym wirtualnym środowisku znajdują się dwa dyski po 500MB każdy. Można zaznaczyć wszystkie dyski i kliknąć OK.

On the wizard page (by default), only the disk you are most likely to use is shown. In the list below, all the disks that are attached to this server are shown, both internal and external disks. The list excludes critical disks that contain system files, and cluster shared volume disks.

Select the check box for a disk to make it appear in the list of available disks in the wizard page.

Available disks:

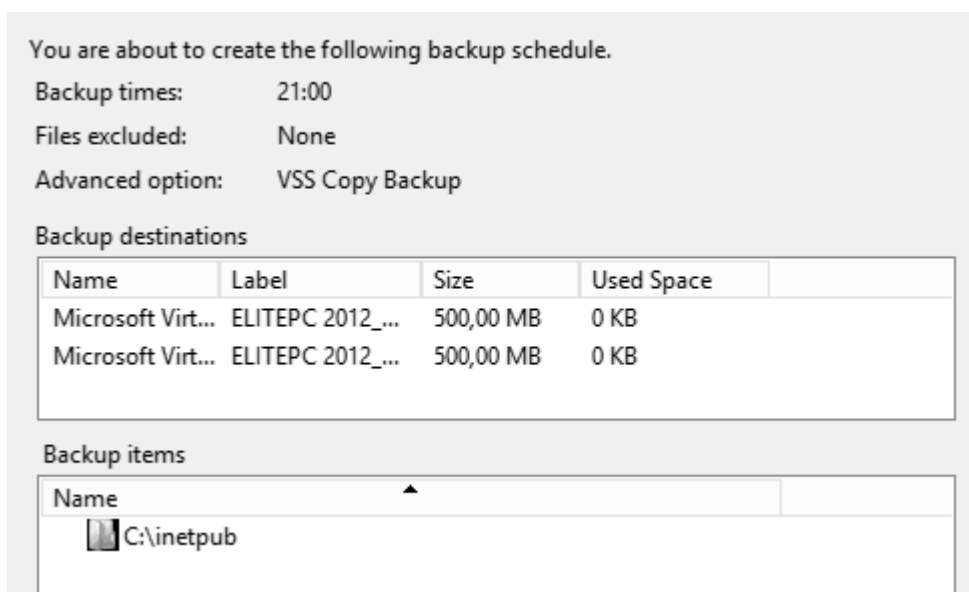
Disk	Name	Size	Used Space	Volumes
<input checked="" type="checkbox"/> 1	Microsoft Virtual ...	500,00 MB	0 KB	
<input checked="" type="checkbox"/> 2	Microsoft Virtual ...	500,00 MB	0 KB	

Na komunikacie, który się pojawi należy kliknąć **TAK (Yes)**. Informuje on czytelnika o tym, iż wybrane dyski zostaną sformatowane, a dane już na nich zebrane zostaną utracone.

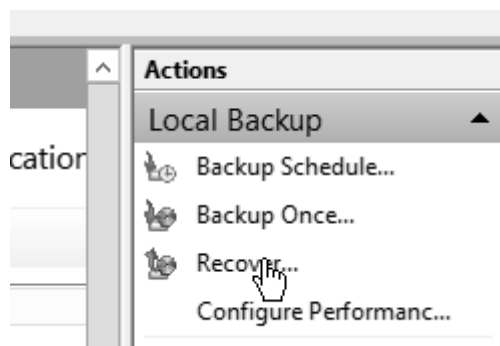




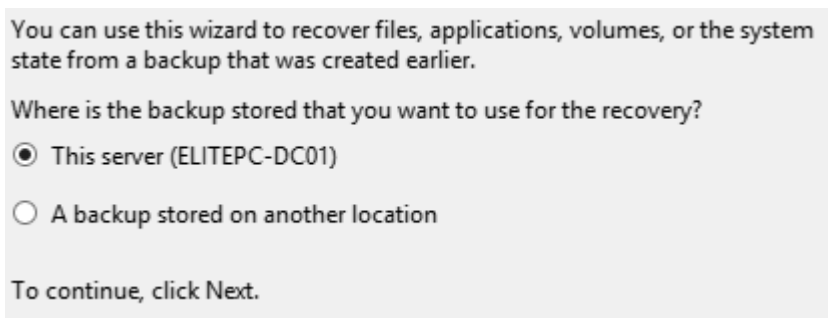
Następnie należy potwierdzić kartę podsumowującą kreatora klikając **Zakończ (Finish)**.



W celach treningowych można odzyskać dane. Należy więc kliknąć na **Odzyskaj (Recover)**.



Otworzy się kreator odzyskiwania, w którym należy wybrać lokalizację, w której przechowywana jest kopia oraz kliknąć ***Dalej (Next)***. Do wyboru jest kopia w na ***Lokalnym serwerze (This server)*** oraz w ***Innej lokalizacji (A backup stored on another location)***.



Następnie wybiera się datę, z której mają zostać przywrócone pliki.

Oldest available backup: 2012-06-12 18:14  
 Newest available backup: 2012-06-12 18:14

Available backups  
 Select the date of a backup to use for recovery. Backups are available for dates shown in bold.

czerwiec 2012						
Pn	Wt	Śr	Cz	Pt	So	N
					1	2
4	5	6	7	8	9	10
11	<b>12</b>	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Backup date: 2012-06-12  
 Time: 18:14  
 Location: ELITEPC 2012\_06\_12 18:11  
 Status: Available online  
 Recoverable items: Local disk (C:)(Sele...

Należy wybrać typ odzyskiwania i kliknąć **Dalej (Next)**. Do wyboru jest **Odzyskiwanie plików i folderów (Files and folders)**, w którym administrator może ręcznie wybrać pojedyncze pliki lub folder, **Przywracanie maszyn wirtualnych Hyper-V (Hyper-V)**, przywracanie całych **Woluminów (Volumes)** oraz **Aplikacji (Applications)**. Można także przywrócić wcześniej zapisany stan systemu operacyjnego.

What do you want to recover?

☒ **Files and folders**  
 You can browse volumes included in this backup and select files and folders.

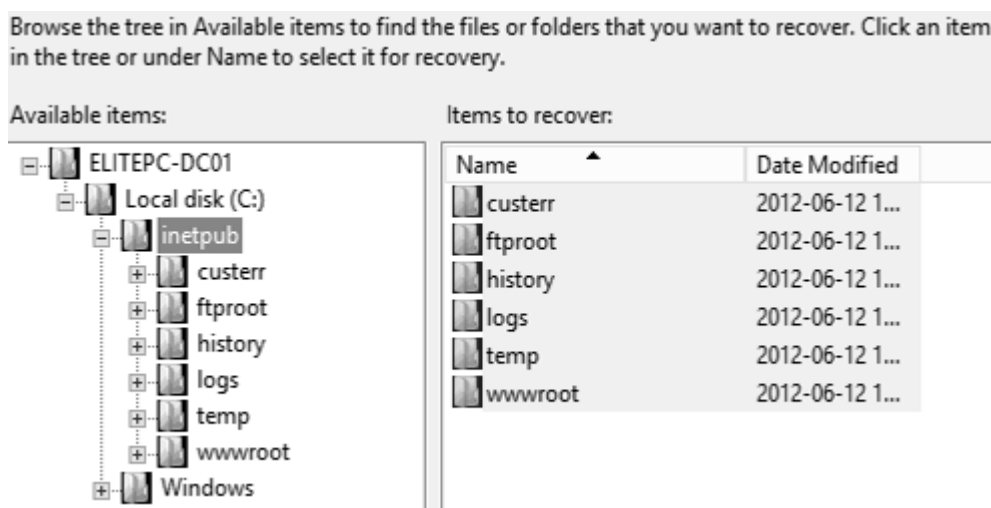
☐ **Hyper-V**  
 You can restore virtual machines to their original location, another location or copy the virtual hard disk files of a virtual machine.

☐ **Volumes**  
 You can restore an entire volume, such as all data stored on C:.

☐ **Applications**  
 You can recover applications that have registered with Windows Server Backup.

☐ **System state**  
 You can restore just the system state.

Po wybraniu pierwszej opcji tj. **przywracanie pojedynczych plików i folderów (Files and folders)** należy zaznaczyć elementy do odzyskania i kliknąć **Dalej (Next)**.



W kolejnym kroku określa się opcje odzyskiwania. Przede wszystkim należy określić czy dane mają być odzyskane w swoim oryginalnym miejscu, a co za tym idzie nowe pliki zostaną nadpisane czy też w lokalizacji alternatywnej, co pozwoli zachować obie wersje plików. Należy także określić jak ma się zachować kreator, jeżeli w docelowej lokalizacji napotka już jakieś wersje plików oraz to, co ma on zrobić z uprawnieniami ACL.

Recovery destination

☐ Original location  
☒ Another location

---


When this wizard finds items in the backup that are already in the recovery destination

☒ Create copies so that you have both versions  
☐ Overwrite the existing versions with the recovered versions  
☐ Do not recover the items that already exist on the recovery destination

---

Security settings

☒ Restore access control list (ACL) permissions to the file or folder being recovered

 File recovery to a non-NTFS target volume might fail due to unsupported file properties.

Na karcie podsumowującej należy użyć przycisku **Przywróć (Recover)**, aby rozpocząć przywracanie plików.

Recovery destination: C:\Users\Administrator\Desktop

Recovery option: Create copies of recovered files

Security settings: Recover

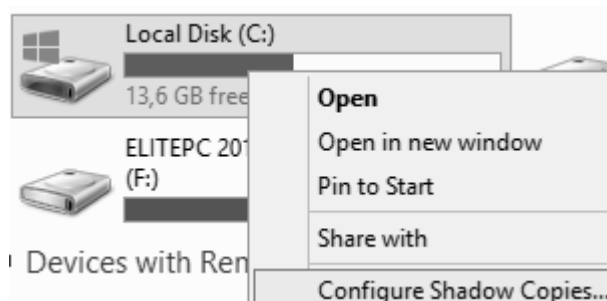
## b. Shadow Copies

Funkcja **kopiowania w tle (Shadow Copies)** folderów udostępnionych umożliwia tworzenie bieżących kopii plików należących do zasobów udostępnionych, takich jak serwer plików. Dzięki tej funkcji można przeglądać udostępnione pliki i foldery w stanie, w jakim znajdowały się w określonym czasie w przeszłości.

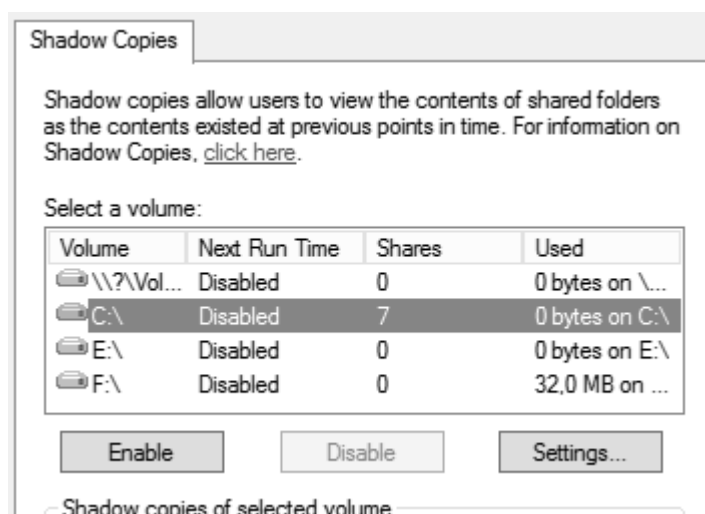
Za pomocą funkcji **kopiowania w tle (Shadow Copies)** można odzyskiwać pliki,

które zostały przypadkowo usunięte lub zastąpione, oraz porównywać różne wersje plików.

W celu ich uruchomienia należy otworzyć Mój Komputer i kliknąć prawym przyciskiem myszy na lokalnym dysku komputera, a następnie wybrać **Konfiguruj Kopie w tle (Configure Shadow Copies)**.

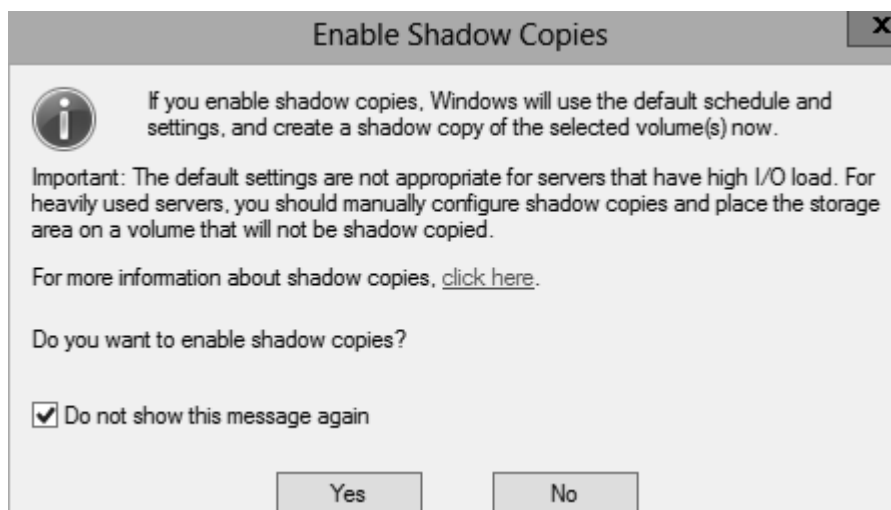


Następnie należy kliknąć na wybrany wolumin i kliknąć opcję **Włącz (Enable)**. Spowoduje to uruchomienie na nim kopii w tle. Za chwilę przeprowadzony zostanie demonstracyjny proces, który ma na celu pokazanie w jaki sposób działają kopie w tle i jak nich korzystać oraz jak je prawidłowo skonfigurować.

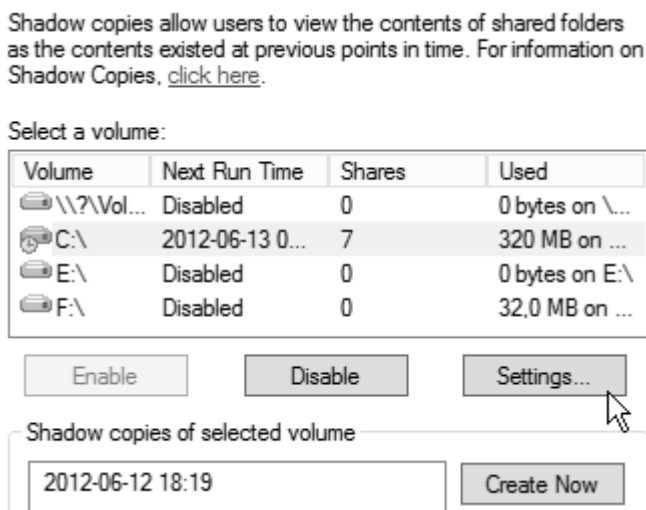


Należy kliknąć **Tak (Yes)** w komunikacie jaki się pojawi. Informuje on o tym iż nie

zaleca się uruchamiania kopii w tle na maszynach o dużym obciążeniu.



Następnie konieczne jest wejście w *Ustawienia (Settings)* w celu dokonania dalszej konfiguracji m. in. ustawienia harmonogramu wykonywania kopii.



W następnym kroku ustawia się limit miejsca na dysku jakie będzie zarezerwowane dla kopii w tle np. wynoszący 600MB. Gdy limit zostanie osiągnięty kasowane będą

najstarsze wersje plików. Następnie należy wybrać **Harmonogram (Schedule)**.

Maximum size: ☐ No limit ☒ Use limit: 600 MB

Note: You need at least 300MB free space to create a shadow copy.

Schedule

Schedule...

Note: The default schedule creates two shadow copies per day. Avoid creating shadow copies more frequently than once per hour.

Harmonogram określa jak często wykonywana jest kopia plików, które uległy zmianie. Można np. wybrać wykonywanie kopii przy logowaniu dzięki czemu użytkownicy zawsze będą mieli dostęp do swoich plików z poprzedniego dnia pracy.

Schedule

1. At 07:00 every Pn, Wt, Śr, Cz, Pt of every week, starting 2012-06-12

New Delete

Schedule Task: Weekly Start time: 07:00 Advanced...

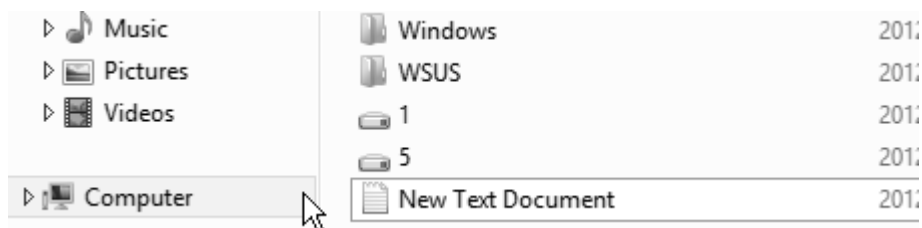
Schedule Task Weekly

Every 1 week(s) on: ☒ Mon ☐ Sat ☒ Tue ☐ Sun ☒ Wed ☒ Thu ☒ Fri

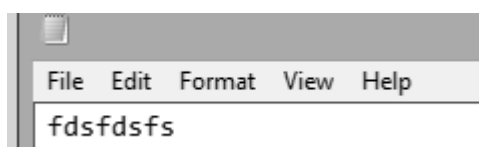
W celu przeprowadzenia pokazu działania kopii w tle należy na wcześniej



wybranym woluminie utworzyć nowy dokument tekstowy.



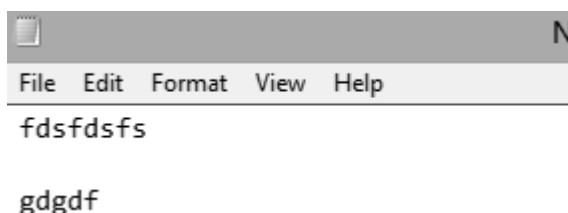
Następnie w utworzonym dokumencie należy wprowadzić jakąkolwiek treść.



W karcie konfiguracyjnej kopii w tle można kliknąć *Utwórz Teraz (Create Now)* co spowoduje wymuszenie wykonania kopii w tle.

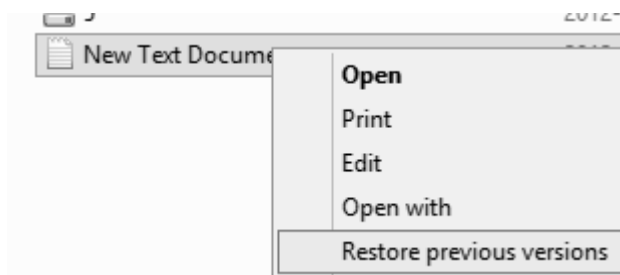


Czynności te należy powtórzyć kilkakrotnie po to, aby utworzyć kilka wersji tego samego pliku.

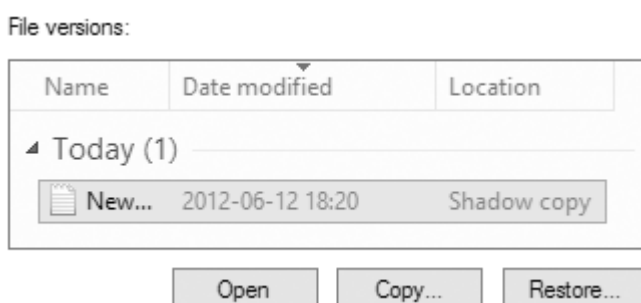


Gdy kopie są już przygotowane, użytkownik na komputerze łączącym się do swojego zasobu będzie miał pod prawym klawiszem myszy opcję *Przywróć*

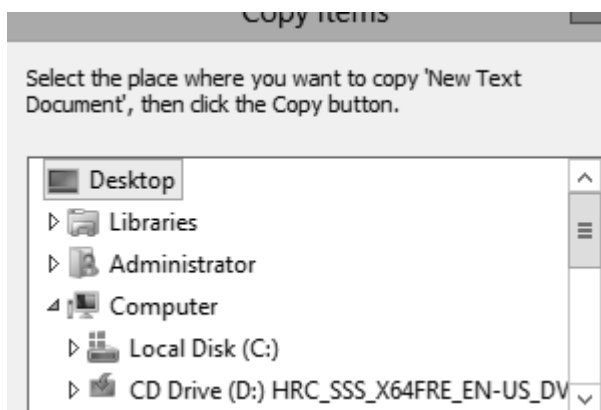
*poprzednie wersje (Restore previous versions)*. Należy kliknąć tę opcję.



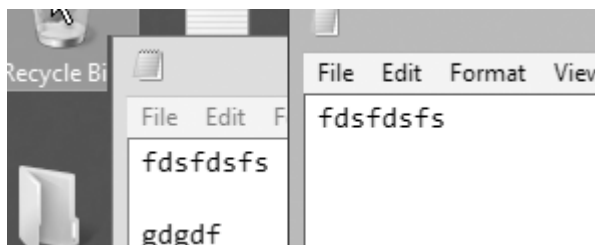
W oknie które się pojawi można wybrać dowolną poprzednią wersję pliku.



Poprzedni plik użytkownik może otworzyć w celu podglądu, skopiować w dowolne inne miejsce lub przywrócić w jego oryginalnej lokalizacji, co spowoduje nadpisanie najnowszej wersji pliku.



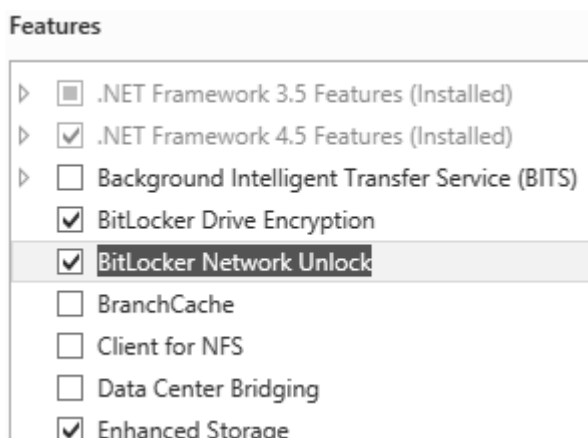
Jak widać została przywrócona poprzednia wersja pliku sprzed edycji treści.



### c. BitLocker

**BitLocker** to rozwiązanie wbudowane w niektórych systemach operacyjnych firmy Microsoft. Pozwala on na kryptograficzną ochronę danych na dyskach. Można także wykorzystywać sprzętowe moduły Trusted Platform Module dostępne na coraz to większej ilości płyt głównych.

Pierwszym krokiem będzie dodanie funkcji *Szyfrowanie danych funkcją BitLocker (BitLocker Network Unlock)*.



Niezbędne będzie ponowne uruchomienie komputera.

## Confirm installation selections

Before You Begin

Installation Type

Server Selection

Server Roles

Features

WDS

Role Services

Confirmation

Results

To install the following roles, role services, or features on selected server:

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed. If you do not want to install them, uncheck their check boxes.

BitLocker Drive Encryption

BitLocker Network Unlock

Enhanced Storage

Remote Server Administration Tools

Feature Administration Tools

BitLocker Drive Encryption Administration Utilities

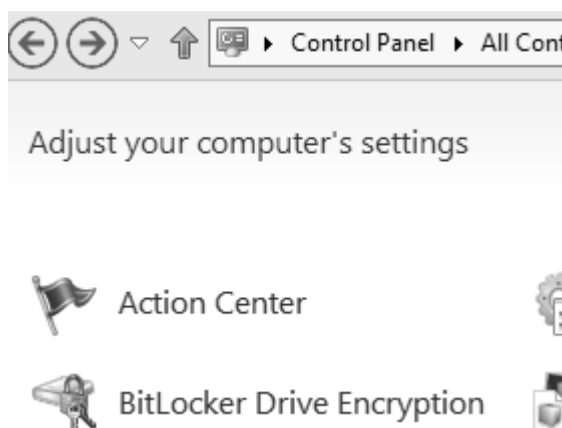
BitLocker Recovery Password Viewer

BitLocker Drive Encryption Tools

Role Administration Tools

Windows Deployment Services Tools

Należy włączyć **Zarządzanie funkcją BitLocker (BitLocker Drive Encryption)**, co można uczynić z poziomu **Panelu Sterowania (Control Panel)**.



W oknie konsoli, która się otworzy można zarządzać modułami TPM, to jednak nie

zostanie zrobione. Zostanie jednak włączone szyfrowanie na dysku C. Należy kliknąć *Włącz funkcję BitLocker (Turn on BitLocker)*.

## BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

### Operating system drive

C: BitLocker off



 Turn on BitLocker

### Fixed data drives

Na komunikacie, który się pojawi należy kliknąć *Tak (Yes)*. Szyfrowanie jest dość obciążające dla komputera i trzeba mieć to na uwadze.



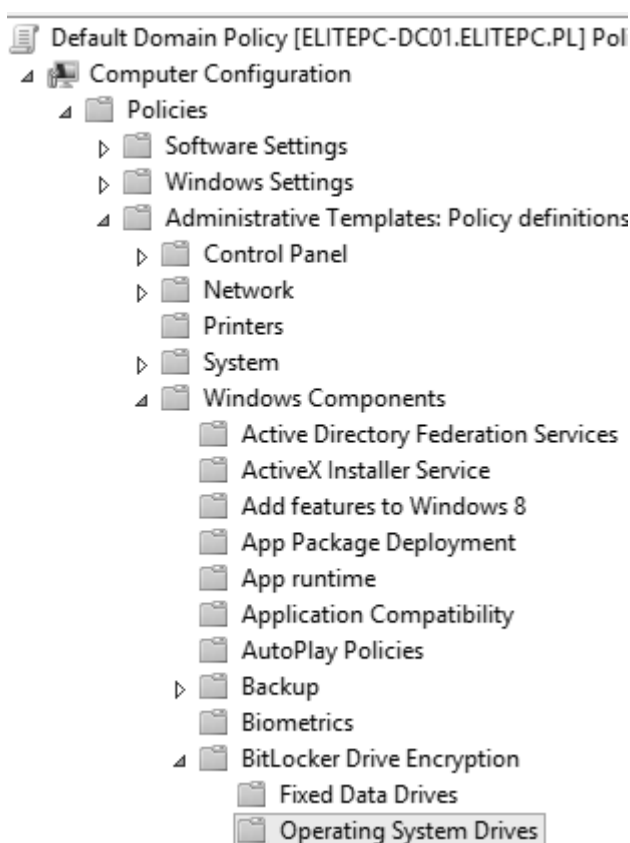
Chwilę to potrwa, pod warunkiem, że w systemie zainstalowany jest moduł TPM.

Jeżeli takiego modułu nie ma konsola zwróci błąd.

## Starting BitLocker

- ❌ This device can't use a Trusted Platform Module. Your administrator must set the "Allow BitLocker without a compatible TPM" option in the "Require additional authentication at startup" policy for OS volumes.

Informuje on o tym, iż na komputerze nie ma modułu TMP i aby uruchomić szyfrowanie można uruchomić odpowiednią zasadę. Należy więc rozwinąć drzewo GPO jak na poniższym zrzucie ekranu.



Następnie należy skonfigurować zasadę *Wymagaj dodatkowej autentykacji przy starcie (Require additional authentication at startup)* jak na zrzucie ekranu poniżej.

Require additional authentication at startup

Require additional authentication at startup

Previous Setting

Next Setting

☐ Not Configured
 

Comment:

☒ Enabled
 

Supported on:

Windows 7 operating systems

☐ Disabled
 

Options:

Allow BitLocker without a compatible TPM

☒ (requires a password or a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup:

Allow TPM

Configure TPM startup PIN:

Allow startup PIN with TPM

Configure TPM startup key:

Allow startup key with TPM

Configure TPM startup key and PIN:

Allow startup key and PIN with TPM

Help:

This policy setting allows you to configure whether requires additional authentication each time the co and whether you are using BitLocker with or without Platform Module (TPM). This policy setting is appli turn on BitLocker.

Note: Only one of the additional authentication op required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without select the "Allow BitLocker without a compatible TI box. In this mode either a password or a USB drive i start-up. When using a startup key, the key informa encrypt the drive is stored on the USB drive, creatin When the USB key is inserted the access to the driv authenticated and the drive is accessible. If the USB unavailable or if you have forgotten the password t need to use one of the BitLocker recovery options t drive.


On a computer with a compatible TPM, four types

Teraz po odświeżeniu zasad bezpieczeństwa poprzez *gpupdate /force* dyski powinny się szyfrować. Przy ponownej próbie szyfrowania pojawi się pytanie czy będzie używany klucz szyfrujący w formie napędu USB czy hasła.

354

Ebookpoint.pl kopia dla: Pawel Domanski pawel@dexterteam.eu

## Choose how to unlock your drive at startup

 Some settings are managed by your system administrator.

To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.

---

➔ Insert a USB flash drive

---

➔ Enter a password

W przykładzie zdecydowano się na hasło.

### BitLocker Drive Encryption (C:)

## Create a password to unlock this drive

You should create a strong password that uses uppercase and lowercase letters, numbers, symbols, and spaces.

Enter your password

Reenter your password

W kreatorze konieczne jest wykonanie kopii zapasowej hasła dowolną metodą np. poprzez zapis do pliku, jego wydruk bądź zapisanie na nośniku USB.



How do you want to back up your recovery key?

**i** Some settings are managed by your system administrator.

A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

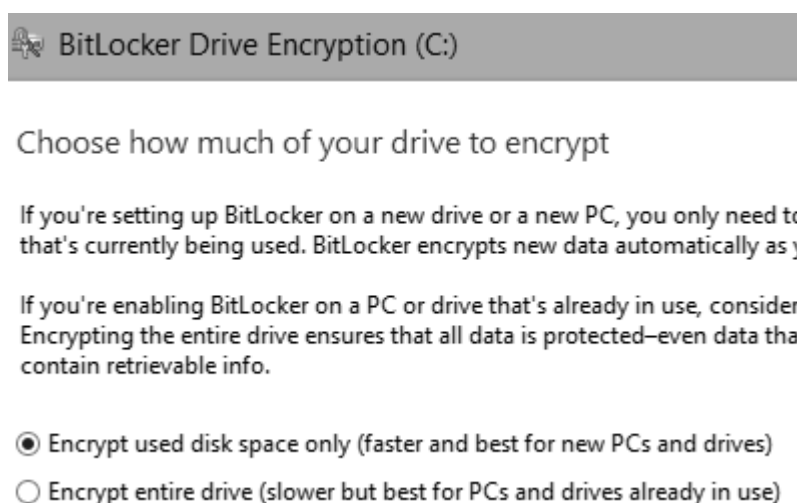


→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

Następnie konieczne jest zdefiniowanie czy szyfrowany będzie cały dysk czy jedynie zajęta przestrzeń.



**BitLocker Drive Encryption (C:)**

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt that's currently being used. BitLocker encrypts new data automatically as you use it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that contain retrievable info.

☒ Encrypt used disk space only (faster and best for new PCs and drives)

☐ Encrypt entire drive (slower but best for PCs and drives already in use)

Następnie pojawi się karta podsumowująca. Informuje ona o tym, iż za chwilę rozpocznie się proces szyfrowania dysku twardego podczas którego komputer spowolni, po czym BitLocker zostanie uruchomiony. Komputer zostanie ponownie uruchomiony.

Are you ready to encrypt this drive?

This drive (C:) has been encrypted for use with BitLocker and now just needs to be activated. This will take a few seconds.

You can keep working while the drive is being encrypted, although your PC might run more slowly.

☒ Run BitLocker system check

The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.

BitLocker will restart your computer before encrypting.

Note: This check might take a while, but is recommended to ensure that your selected unlock method works without requiring the recovery key.

Podczas ponownego uruchomienia komputera system Windows nie udzieli dostępu do dysku twardego bez podania wcześniej zdefiniowanego hasła.



Po pierwszym logowaniu od uruchomienia szyfrowania HDD, pojawi się okienko obrazujące postępy szyfrowania dysku twardego.



Encrypting...

Drive C: 19.5% Completed

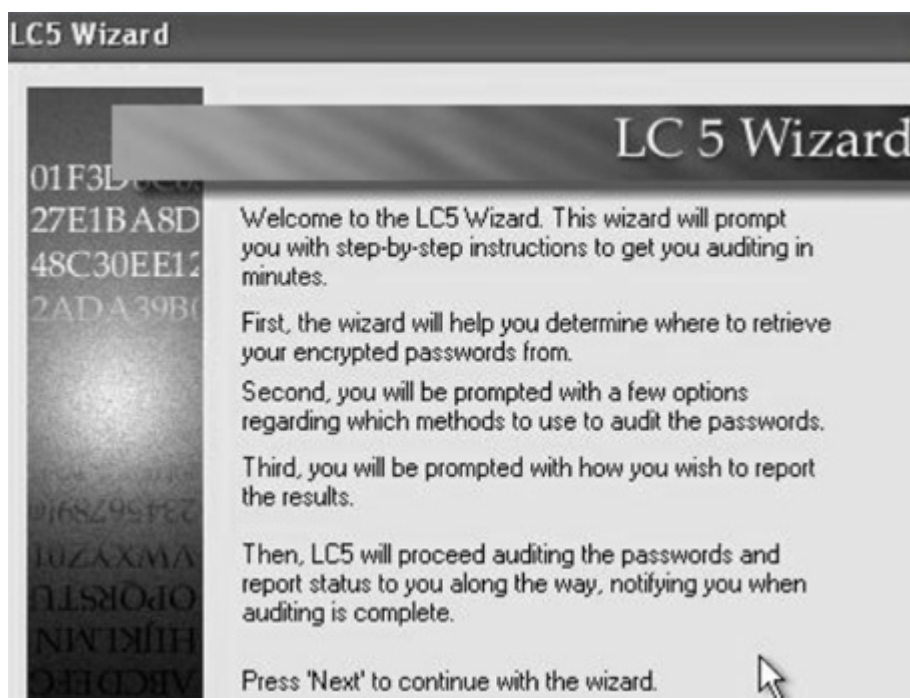


## d. Kilka uwag ogólnych

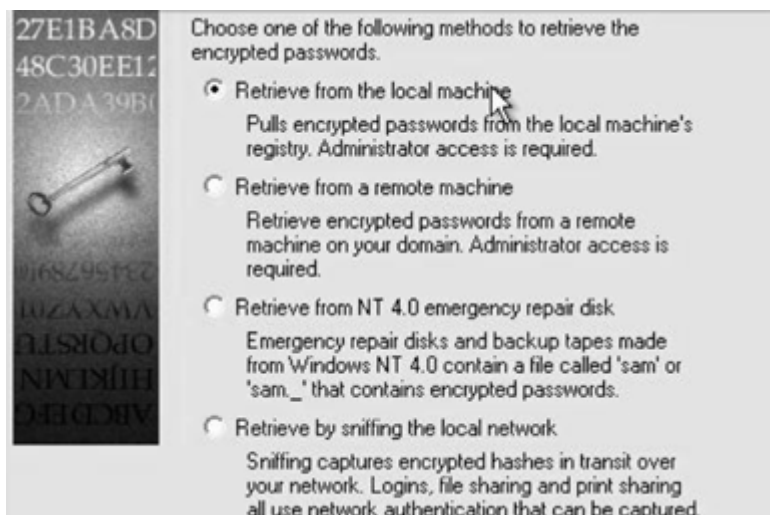
W najbliższych podziałach czytelnik dowie się kilku ciekawostek na temat systemu Windows oraz najlepszych praktyk związanych z bezpieczeństwem. Wyjaśni one także niektóre polityki bezpieczeństwa dyktowane przez Default Domain Policy.

### i. Polityka haseł

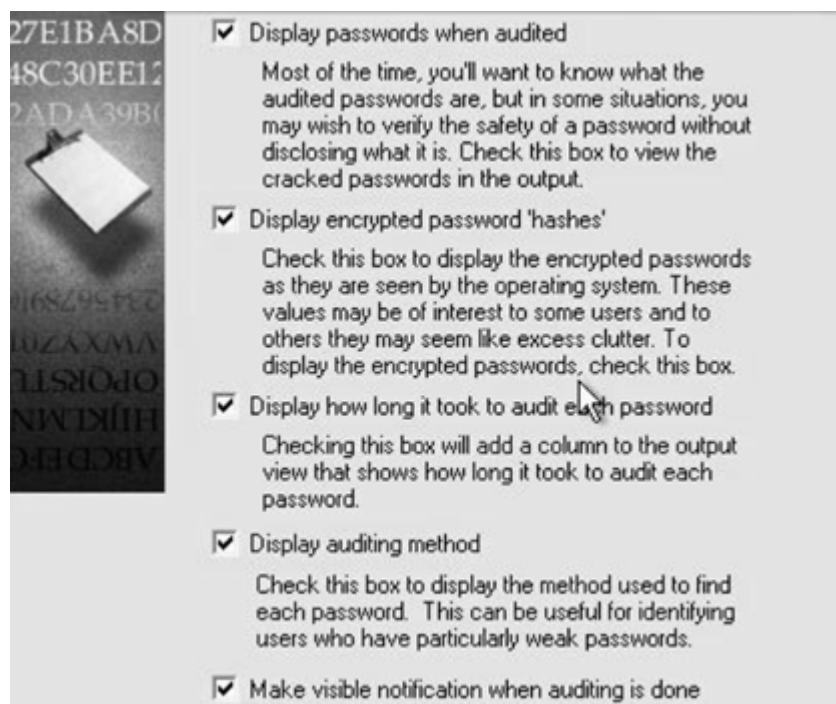
Nadeszła pora na zajęcie się komputerem klienta. W tym momencie w celach ćwiczeniowych należy stworzyć dowolnych 4 użytkowników i dać im następujące hasła „a”, „aaa”, „abc”, „kował”, a także zainstalować program LC5, postępując zgodnie z kreatorem.



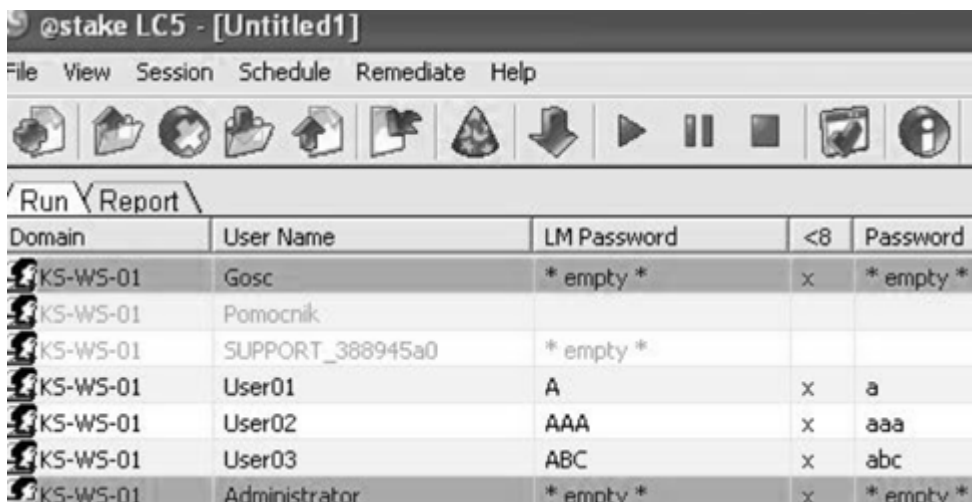
Należy wybrać pierwszą opcję ***Komputer Lokalny (Retrieve from the local machine)***.



W przykładzie zostanie wybrana najprostsza metoda łamania haseł.



Resztę ustawień należy zostawić domyślną.



The screenshot shows the @stake LC5 - [Untitled1] application window. It has a menu bar with File, View, Session, Schedule, Remediate, and Help. Below the menu is a toolbar with various icons. A tab labeled 'Run' is selected, and below it is a table with the following data:

Domain	User Name	LM Password	<8	Password
KS-WS-01	Gosc	* empty *	x	* empty *
KS-WS-01	Pomocnik			
KS-WS-01	SUPPORT_388945a0	* empty *		
KS-WS-01	User01	A	x	a
KS-WS-01	User02	AAA	x	aaa
KS-WS-01	User03	ABC	x	abc
KS-WS-01	Administrator	* empty *	x	* empty *

Tak proste hasła zostały złamane w ułamku sekundy najprostszą metodą. Dłuższe hasło "kowal" nie zostało złamane, gdyż nie było go w słowniku. Dlatego tak ważne jest wdrożenie odpowiedniej polityki haseł. Polecieć można do przetestowania programy takie jak IRIS do przechwytywania haseł podczas logowania do usług np. FTP czy Telnet, a także WireShark do podsłuchiwanie ruchu w sieci. Dlatego też ważne jest, aby hasła w sieci miały odpowiednią złożoność, a sama komunikacja wewnątrz sieci była jak najlepiej zabezpieczona.

## ii. Podmiana logon.scr

Można teraz spróbować nieco podnieść swoje uprawnienia, jeśli ma się dostęp do dysku C. Aby to zrobić należy.

1. Zalogować się jako administrator, uruchomić program regedit i zmienić wartość klucza:

ScreenSaveTimeOut na wartość 15 (sekund) oraz ScreenSaveActive na wartość 1. (HKEY\_USERS\DEFAULT\Control Panel\Desktop).

2. W katalogu %systemroot%\System32 skopiować następujące pliki:

logon.scr na logon.old.scr

cmd.exe na logon.scr.

3. Wylogować się i odczekać około 15 sekund.

4. Po pojawieniu się konsoli (okna poleceń) wykonać następujące próby (uwaga: niektóre z nich należy powtórzyć kilkakrotnie, ograniczając do niezbędnego minimum ilość otwartych okien):

A. Określić kontekst użytkownika (wykorzystać program whoami z Resource Kit);

B. Uruchomić konsolę lusrmgr.msc i wypróbować możliwości:

- zmiany hasła dla konta administratora,
- utworzenia nowego konta użytkownika,
- zmiany składu grup Administrators.

C. Po zamknięciu konsoli lusrmgr.msc, uruchomić program explorer.exe i zbadać możliwości wykorzystania Narzędzi administracyjnych (np. wyczyścić plik dziennika systemowego).

D. Zamknąć okno poleceń.

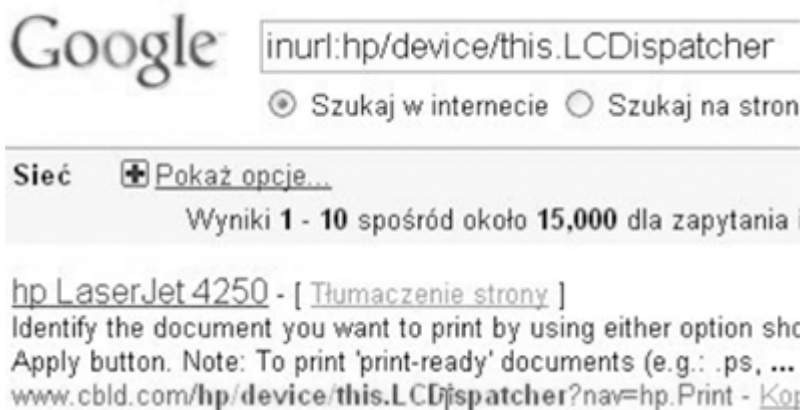
5. Zalogować się jako administrator.

6. Przywrócić pierwotne wartości kluczy w rejestrze, zmienione podczas realizacji punktu 1.

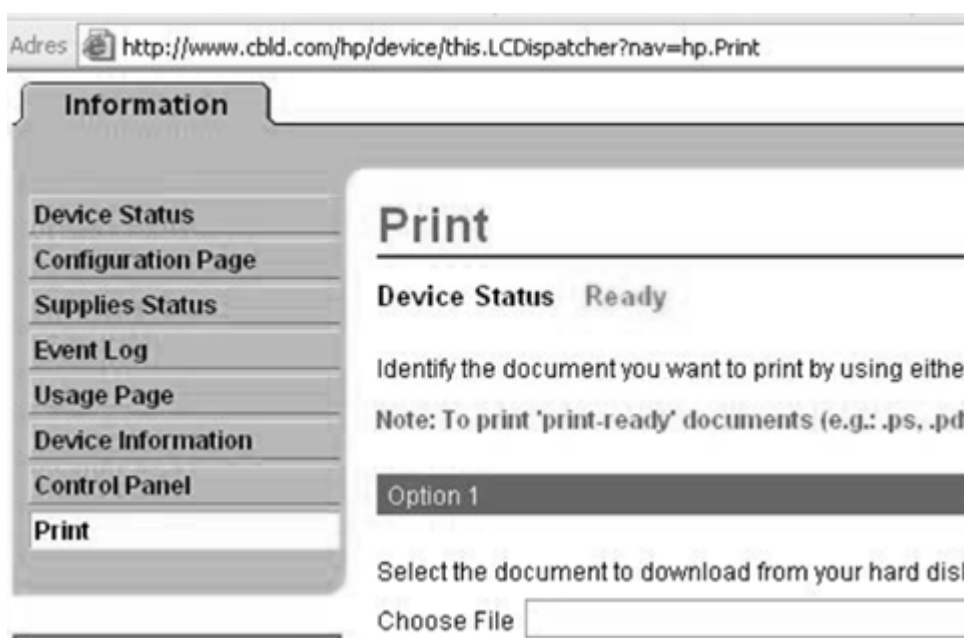
7. Przywrócić pierwotny stan plików zmieniony podczas realizacji punktu 2.

### **iii. Niezabezpieczone serwery wydruku**

Należy teraz wpisać w wyszukiwarce internetowej Google.pl takie zapytanie inurl:hp/device/this.LCDDispatcher, jest to adres własny dla serwera wydruku dla drukarek HP.



Często administratorzy nie zabezpieczają serwerów, a dodając stronę do wyszukiwarek automatycznie Google zapisuje rekord drukarek. Wystarczy wejść w jakiś znaleziony link.



Można teraz zrobić komuś żarcik i coś wydrukować na jego drukarce.

Na koniec stron godnych polecenia:

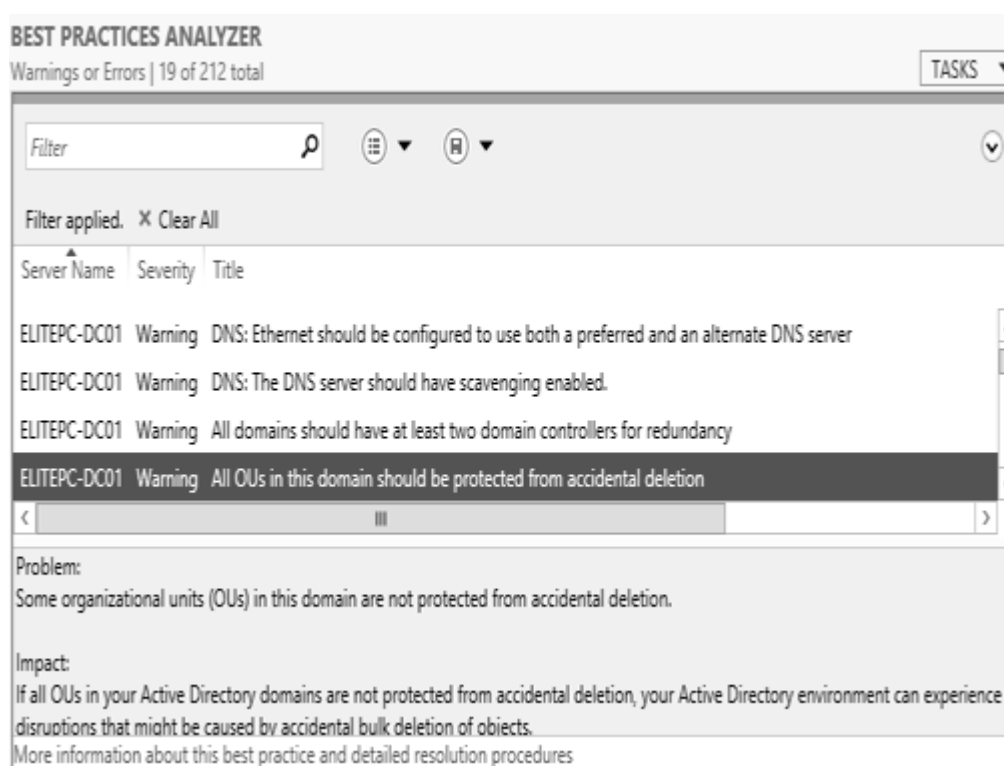
<http://www.auditmypc.com/security-scan.asp> Gdzie łatwo będzie sprawdzić bezpieczeństwo systemu z zewnątrz.

Linux naszpikowany hakerskimi programami <http://www.backtrack-linux.org/>

#### iv. Best Practices Analyzer

Po zainstalowaniu i skonfigurowaniu wszystkich niezbędnych komponentów serwera warto jeszcze użyć narzędzia, które znajduje się w Menadżerze Serwera po kliknięciu **Serwer Lokalny (Local Server)** w lewym menu.

Jest nim okno zarządzania najlepszymi praktykami. Są to wytyczne, uważane za idealny sposób konfiguracji środowiska Windows Server, w normalnych warunkach.

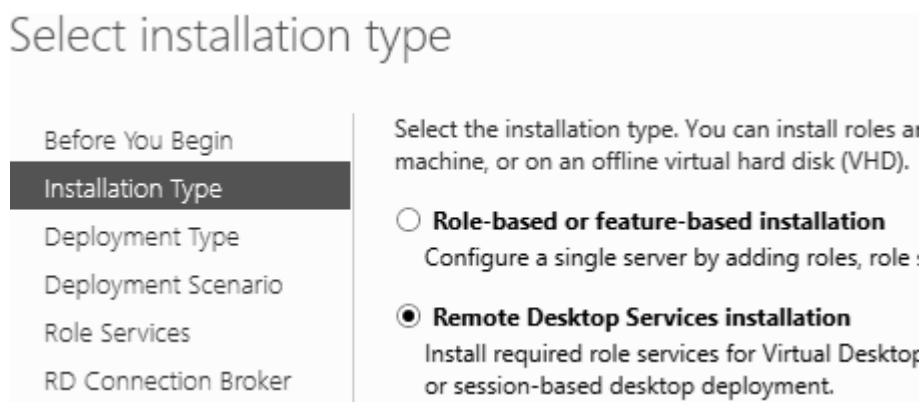




## 18. Remote Desktop Services

Przed rozpoczęciem instalacji usług terminalowych, jeżeli dokonywane były istotne zmiany w konfiguracji IIS w ramach tego kursu najrozsądniej będzie odinstalować tę rolę, a następnie przystąpić do instalacji serwera terminali (w Windows'ie 2012 nazywa się to *Usługą pulpitu zdalnego (Remote Desktop Services)*). Do instalacji tej roli niezbędne są takie składniki jak NPS, IIS, Usługi Certyfikatów oraz Active Directory. Wdrożenie nie może mieć miejsca na kontrolerze domeny, a komputer musi być przyłączony do domeny.

Należy uruchomić kreatora dodawania ról i funkcji serwera. Tym razem nie wybiera się jednak instalacji opartych na rolach lub funkcjach, lecz zaznacza opcję Instalacja *Usługi Pulpitu Zdalnego (Remote Desktop Services Installation)*.



Kolejnym krokiem będzie określenie typu wdrożenia. Do wyboru jest *Wdrożenie Standardowe (Standard Deployment)*, które pozwala na instalację na wielu serwerach jednocześnie. W przypadku ćwiczeniowym można zdecydować się na opcję *Szybki Start (Quick Start)*, która pozwoli zainstalować szybko i w prosty sposób *Usługi Pulpitu Zdalnego* na jednym serwerze, skonfigurować kolekcję i opublikować *Zdalne Aplikacje (RemoteApp)*.

## Select deployment type

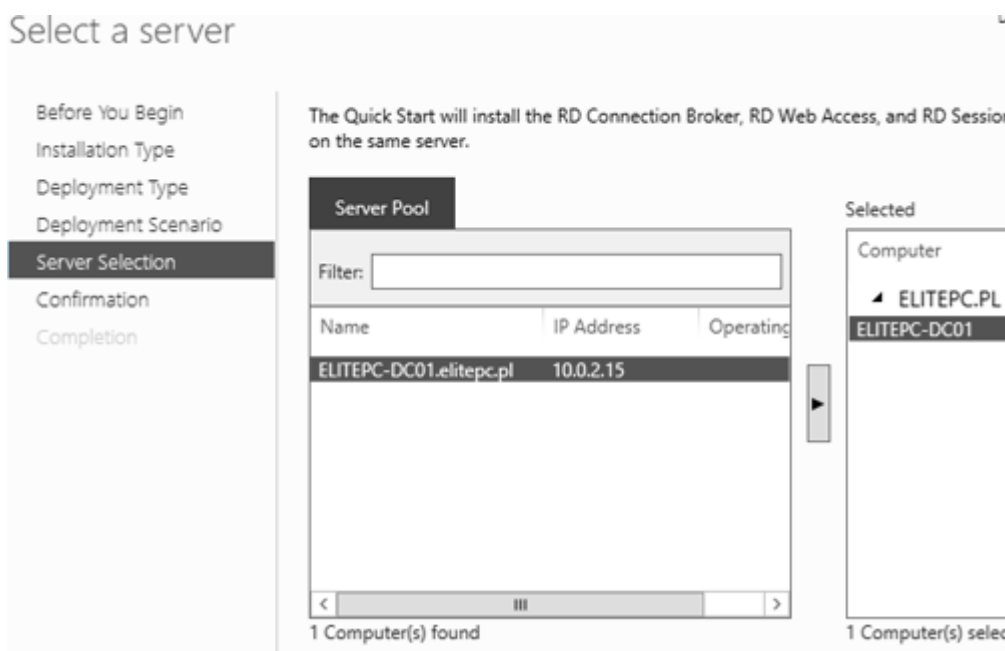
Before You Begin	Remote Desktop Services can be configured to allow users to connect to published RemoteApp programs and session-based desktops.
Installation Type	<input type="radio"/> Standard deployment A standard deployment allows you to deploy Remote Desktop Services on a single server.
<b>Deployment Type</b>	<input checked="" type="radio"/> Quick Start A Quick Start allows you to deploy Remote Desktop Services on a single server and publishes RemoteApp programs.
Deployment Scenario	
Server Selection	
Virtual Desktop Template	

W kolejnym oknie kreatora należy zdefiniować scenariusz wdrożenia. Do wyboru są dwie opcje. Wdrożenie *oparte na maszynach wirtualnych (Virtual Machine – Based Desktop Deployment)*, które to pozwala użytkownikom na łączenie się z przygotowanymi wcześniej maszynami wirtualnymi i korzystać z zainstalowanych na nich aplikacji. Drugą opcją, która zostanie wybrana w ramach ćwiczenia jest *wdrożenie oparte na sesjach (Session – Based Desktop Deployment)*, które tak naprawdę jest utożsamiane z usługami terminalowymi. W tym podejściu użytkownicy nie potrzebują maszyn wirtualnych, ponieważ instancje ich aplikacji mogą wykonywać się niezależnie na jednym serwerze.

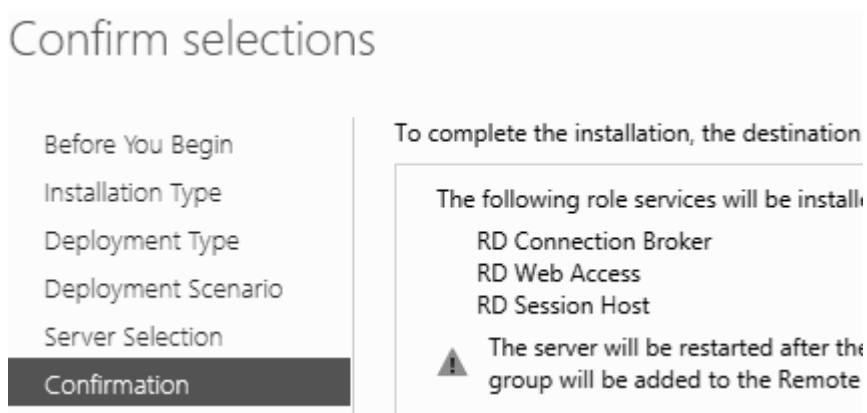
## Select deployment scenario

Before You Begin	Remote Desktop Services can be configured to allow users to connect to published RemoteApp programs and session-based desktops.
Installation Type	<input type="radio"/> Virtual machine-based desktop deployment Virtual machine-based desktop deployment allows users to connect to published RemoteApp programs and session-based desktops that include published RemoteApp programs and virtual machines.
Deployment Type	<input checked="" type="radio"/> Session-based desktop deployment Session-based desktop deployment allows users to connect to published RemoteApp programs and session-based desktops.
<b>Deployment Scenario</b>	
Server Selection	
Confirmation	
Completion	

W kolejnym kroku określa się serwer, na którym będzie dokonywane wdrożenie.



Następnie pojawi się okno podsumowania, gdzie po zaznaczeniu opcji umożliwiającej automatyczne ponowne uruchamianie serwera można użyć przycisku **Wdroż (Deploy)**, który rozpocznie cały proces.



Proces instalacji składa się z trzech etapów. Wdrażania usług systemu zdalnego (**Remote Desktop Services role services**), następnie tworzenia kolekcji sesji (**Session collection**) oraz uruchamiania programów RemoteApp (**RemoteApp programs**).

Podczas tego procesu komputer kilkakrotnie uruchomi się ponownie.

#### Remote Desktop Services role services

ELITEPC-SR01.elitepc.pl  Succeeded

#### Session collection

ELITEPC-SR01.elitepc.pl  Succeeded

#### RemoteApp programs

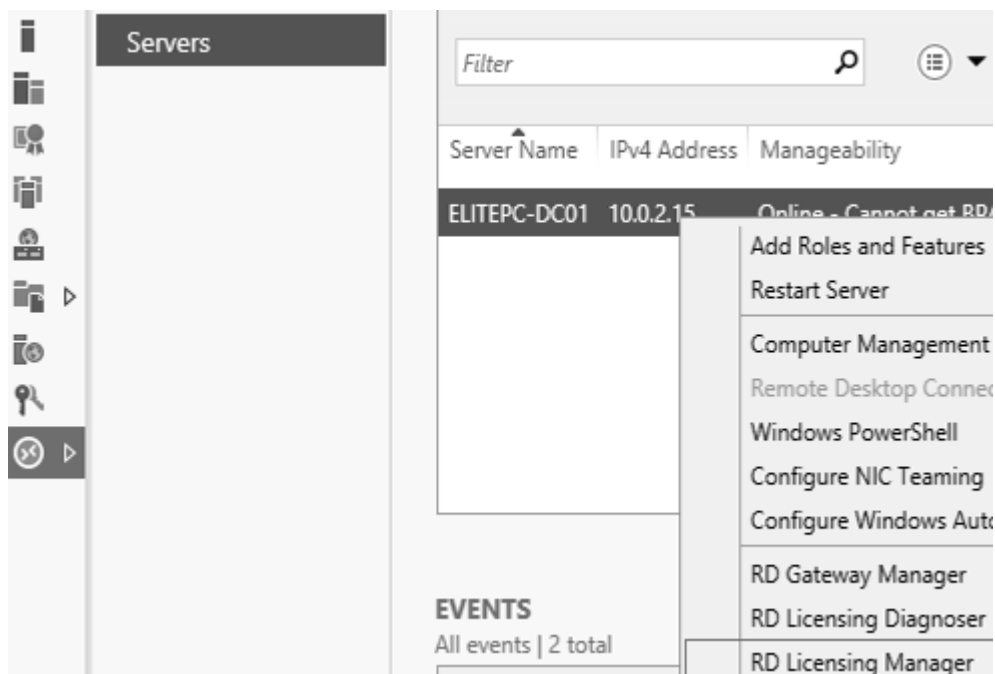
ELITEPC-SR01.elitepc.pl  Succeeded

Po jakimś czasie RDS będą zainstalowane. Należy je jeszcze skonfigurować. Jeżeli nie zostanie wprowadzona żadna licencja (kupuje się je osobno w firmie Microsoft) zyska się 120dni okresu próbnego. Można ściągnąć teraz z Internetu jakiś program, np. CDBurnerXP służący do nagrywania płyt CD. Po jego ściągnięciu program należy zainstalować. Ważne jest to, aby aplikację instalować dopiero po zainstalowaniu roli serwera.

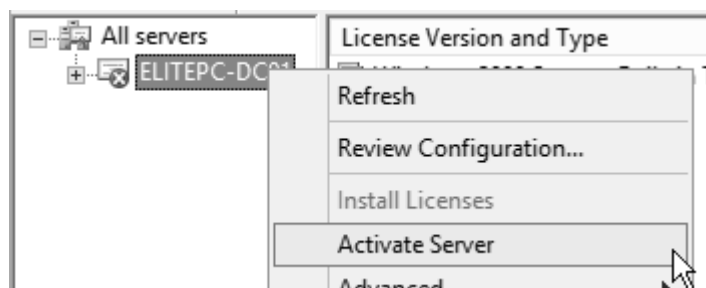


Gdy wgrane są już wszystkie aplikacje, które docelowo będą udostępniane w sieci, warto pomyśleć o konfiguracji licencjonowania serwera terminali. Można jej dokonać z poziomu Menadżera Serwera, rozwijając Remote Desktop Services, następnie wybierając z listy serwerów ten, który jest interesujący i wybierając z

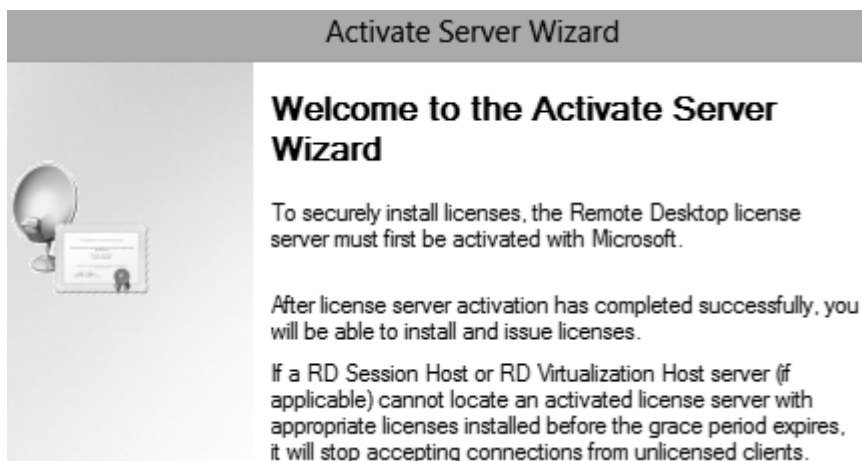
menu kontekstowego RD Licensing Manager.



Domyślnie serwer licencjonowania nie jest aktywny, aby go uaktywnić klika się na nim prawym przyciskiem myszy i wybiera **Aktywuj Serwer (Activate Server)**.



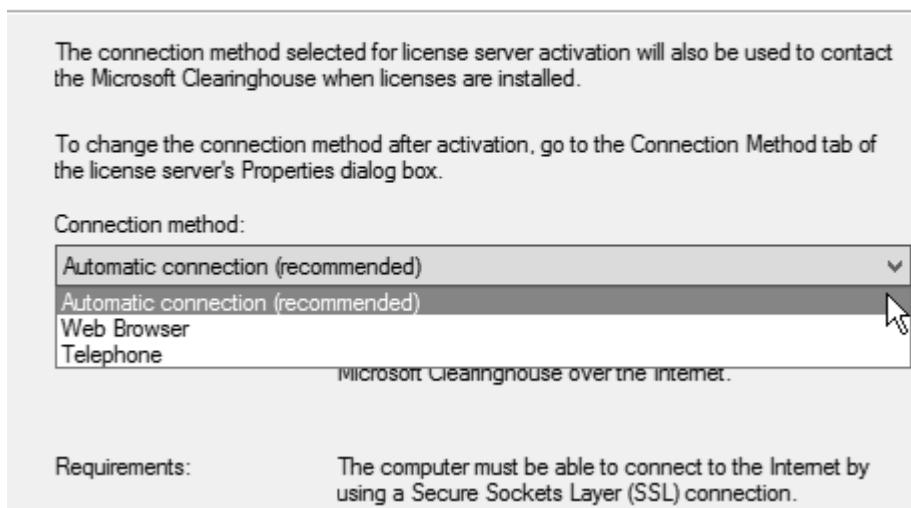
Pierwszym krokiem przed wprowadzeniem licencji jest aktywacja serwera w firmie Microsoft o czym informuje pierwsza karta kreatora.



W kolejnym kroku się określa czy aktywacja ma się odbyć przez Internet czy telefon, bądź też pozostawia opcje domyślne, czyli wybór automatyczny, który w pierwszej kolejności dokona próby aktywacji przez Internet.

#### Connection Method

Select the most appropriate connection method.



W kolejnym oknie wypełnia się informacje dotyczące osoby dokonującej aktywacji, firmy oraz kraju pochodzenia.

### Company Information

Provide the requested company information.

Enter your name, company name, and country/region information.

This information is required to proceed.

First name:	<input type="text" value="Imie"/>
Last name:	<input type="text" value="Nazwisko"/>
Company:	<input type="text" value="Firma"/>
Country or Region:	<input type="text" value="Poland"/>

Następna karta stanowi uzupełnienie danych przedsiębiorstwa.

### Company Information

Enter this optional information.

Email:	<input type="text" value="kontakt@elitepc.pl"/>
Organizational unit:	<input type="text" value="WAW"/>
Company address:	<input type="text" value="Warszawska 1337"/>
City:	<input type="text" value="Warsaw"/>
State/province:	<input type="text" value="MZ"/>
Postal code:	<input type="text" value="01-459"/>

Po kliknięciu przycisku **Dalej (Next)** nastąpi aktywacja i wyświetli się karta podsumowująca, gdzie można uruchomić kreatora instalacji licencji poprzez zaznaczenie opcji **Rozpocznij Kreatora Instalacji Licencji (Start Install Licenses Wizard Now)**, i wybranie przycisku **Dalej (Next)**.

## Completing the Activate Server Wizard

You have completed the Activate Server Wizard.

Status:

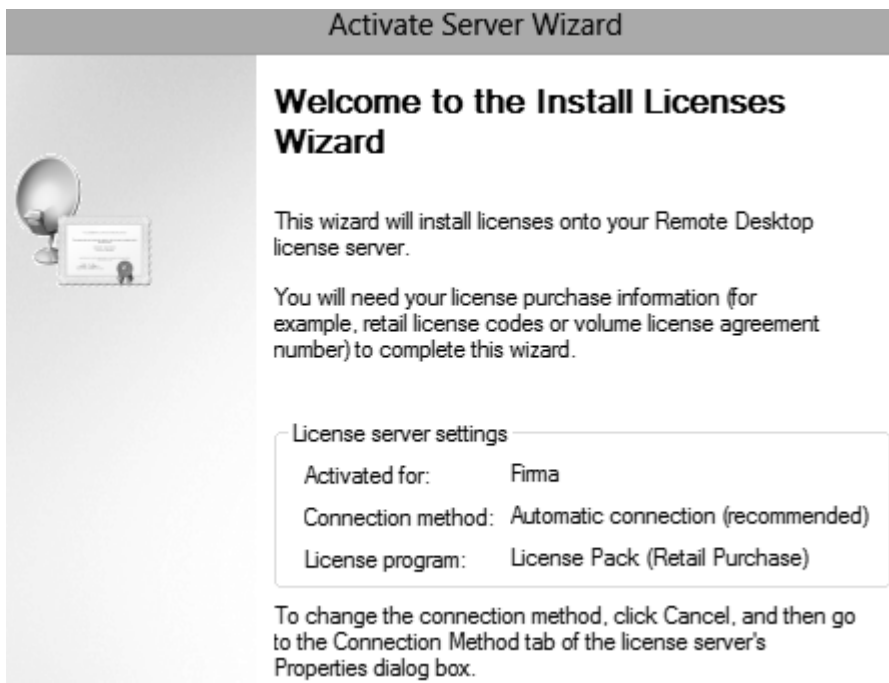
The license server has been successfully activated.

To install licenses, click Next.

To postpone license installation, clear the Start Install Licenses Wizard now check box, and then click Finish.

☒ Start Install Licenses Wizard now

Decydując się na tę opcję pojawi się pierwsze okno nowego kreatora informujące o jego zadaniu i wymaganiach.



W kolejnym oknie wybiera się obejmujący firmę program licencjonowania i podaje



na kolejnych kartach niezbędne dane.

### License Program

Choose the appropriate license program.

Every client that is connecting to a Remote Desktop Session Host server or a virtual desktop in a Microsoft Virtual Desktop Infrastructure must have a valid license. Select the license program through which you purchased your licenses.

License program:

Description:

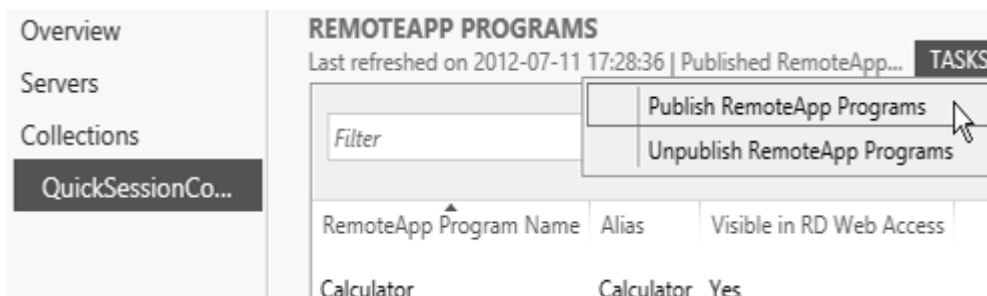
Format and location:

Sample:

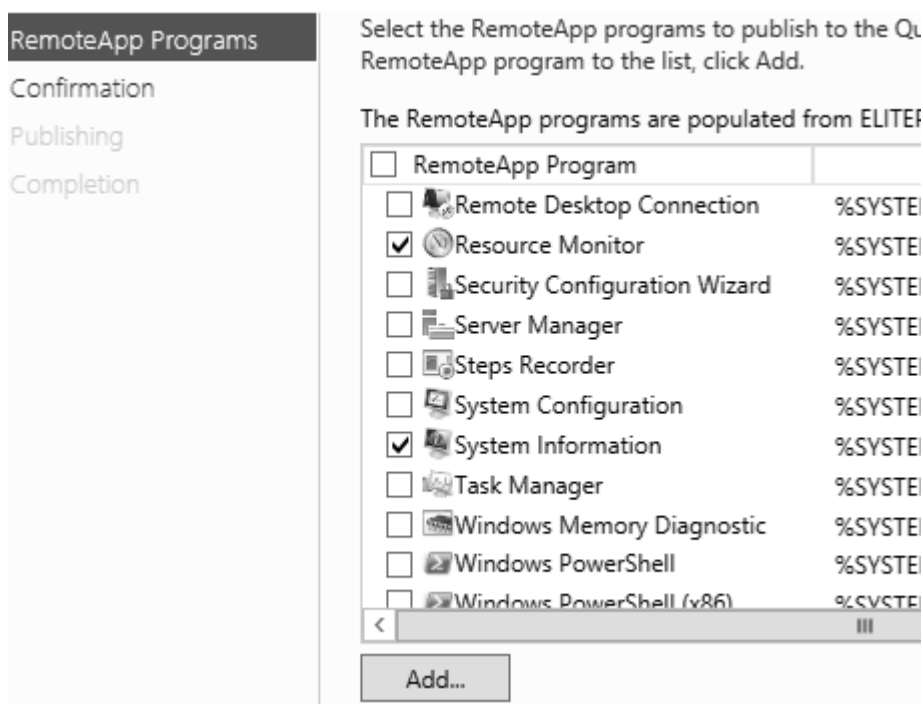
Verify that your license information is similar to the sample before continuing.

Jeżeli zostanie pominięty ten krok uzyska się 120 dni okresu próbnego.

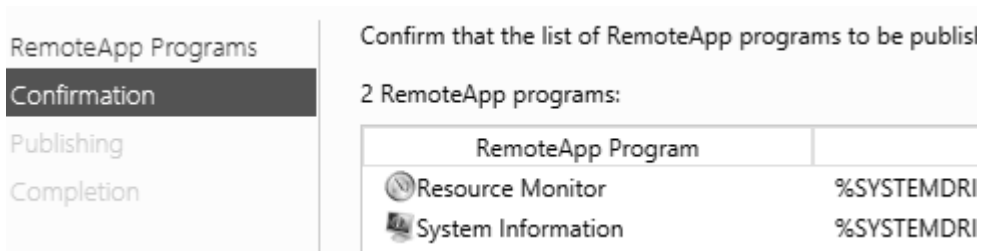
Na serwerze, na którym został zainstalowany RDS po uruchomieniu Menadżera Serwera, rozwinięciu *Usługi Pulpitu Zdalnego (Remote Desktop Services)* z menu po lewej stronie, rozwijając następnie *Kolekcje (Collections)*, a potem *Kolekcja Szybkiej Sesji (Quick Session Collection)*, która jest kolekcją utworzoną przez kreatora w czasie instalacji. W sekcji *Zdalne Aplikacje (RemoteApp Programs)* za pomocą przycisku *Zadania (Tasks)* wybiera się opcję *Opublikuj Zdalne Aplikacje (Publish RemoteApp Programs)* w celu udostępniania programów w trybie *RemoteApp*. Standardowo udostępniony jest Kalkulator, Paint oraz Wordpad.



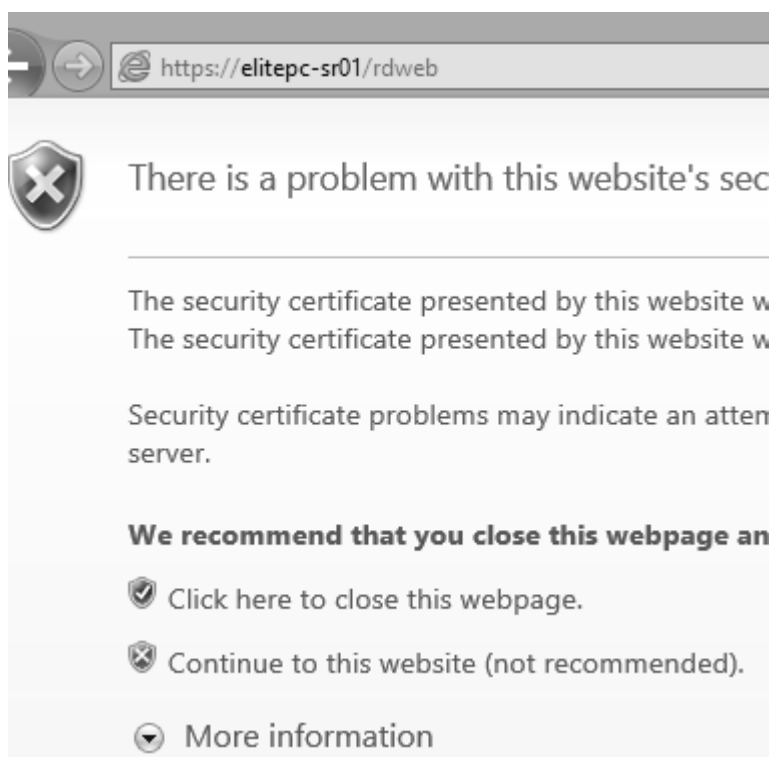
Pojawi się kreator, w którym należy zaznaczyć aplikacje, które mają zostać udostępnione lub przyciskiem **Dodaj (Add)** dodaje się aplikacje, których nie ma na liście.



Pojawi się karta podsumowująca, w której należy kliknąć przycisk **Publikuj (Publish)**, a po chwili przycisk **Zamknij (Close)**.



Po wpisaniu w przeglądarce adresu ***https://adres\_serwera.pl/RDWeb/*** nastąpi przeniesienie na stronę, która oferuje możliwość uruchomienia wcześniej udostępnionych aplikacji, jak również dostępu za pomocą terminali do komputerów wewnątrz sieci. Ważnym aspektem tych działań jest to, że aplikacje uruchamiane w ten sposób działają w kontekście serwera, czyli nie obciążają komputerów klienckich.



Nie posiadając certyfikatu z podpisem cyfrowym konieczne będzie zaakceptowanie wyjątku bezpieczeństwa. Gdy zostanie potwierdzony pojawi się ekran logowania,

gdzie należy podać hasło użytkownika oraz jego nazwę poprzedzoną nazwą domeny. Określa się także czy komputer wpięty jest do bezpiecznej sieci prywatnej czy publicznej.

Domain\user name:  X

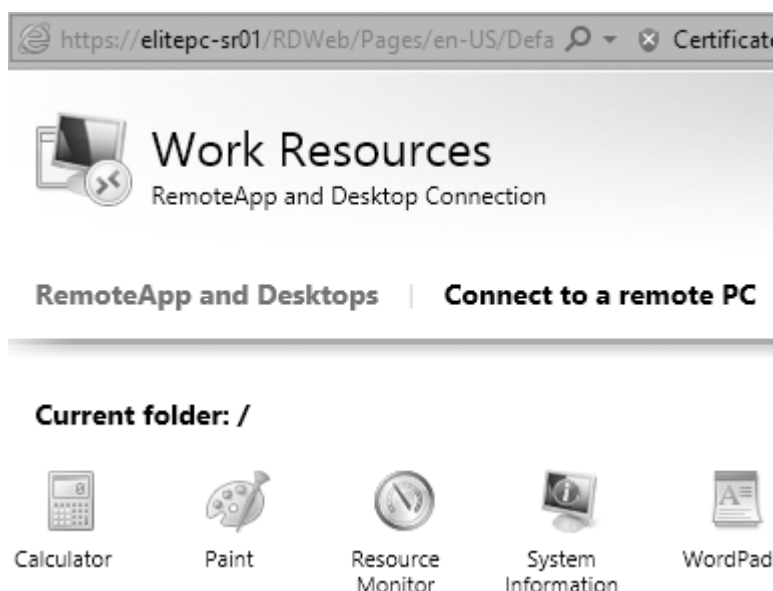
Password:

You must enter a valid domain name.

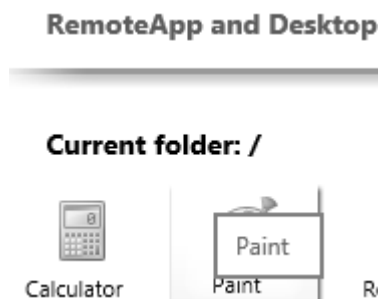
Security ([show explanation](#))

- ☐ This is a public or shared computer
- ☒ This is a private computer

Wchodząc do zakładki **Zdalne Aplikacje i Pulpity (RemoteApps and Desktops)** można znaleźć aplikacje udostępnione na serwerze, zarówno te dostępne w samym systemie jak i te dodatkowo zainstalowane, w tym ściągnięty z internetu CD Burner XP.



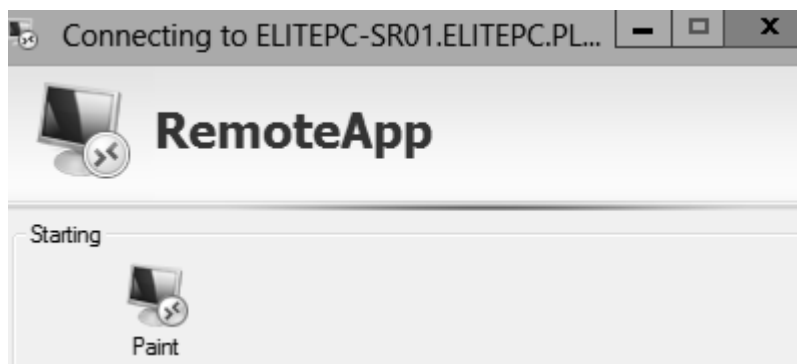
Aby uruchomić jakąś aplikację wystarczy kliknąć na niej myszką.



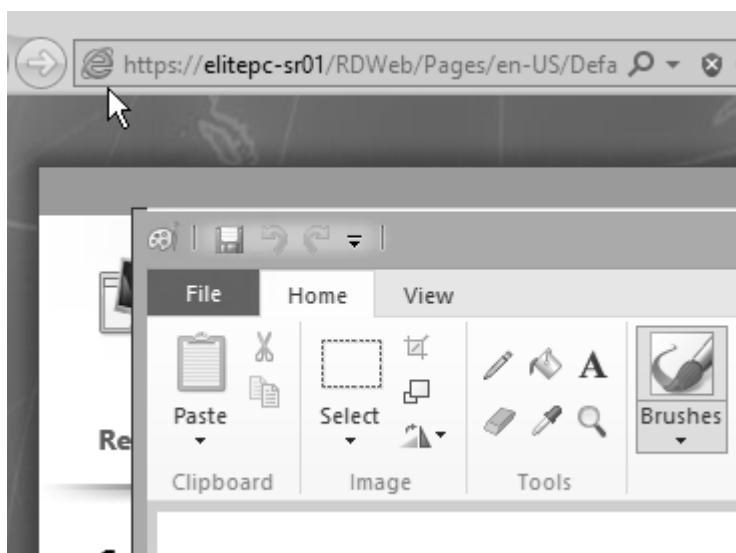
Pojawi się ekran przypominający połączenie pulpitu zdalnego, na którym pozostawiając opcje domyślne należy kliknąć przycisk **Połącz (Connect)**.



Rozpocznie się przygotowywanie połączenia z serwerem, które może potrwać kilka chwil. O postępie w tworzeniu połączenia informuje okienko połączenia.



Gdy aplikacja zostanie uruchomiona, mimo, że działa ona w kontekście serwera na systemie klienckim nie widać różnicy od pracy jak gdyby ta aplikacja była zainstalowana na komputerze klienckim.



Aplikację uruchomioną w trybie RemoteApp rozpoznać można na pasku Start poprzez znaczek symbolizujący połączenie zdalne, narzucony na ikonę programu.



Wchodząc w zakładkę **Połącz się ze zdalnym komputerem (Connect to a Remote PC)** można połączyć się do komputera znajdującego się w sieci firmowej poprzez połączenie pulpitu zdalnego, można określić rozdzielczość okienka, w którym ma być nawiązane połączenie oraz inne opcje znane już z nawiązywania tradycyjnego połączenia pulpitu zdalnego. Aby się połączyć wystarczy podać adres serwera oraz użyć przycisku **Połącz (Connect)**.

## RemoteApp and Desktops | Connect to a remote PC

Enter the name of the remote computer that you want to connect to, specify options,

### Connection options

Connect to:

Remote desktop size:

### Devices and resources

Select the devices and resources that you want to use in your remote session.

- ☒ Printers ☒ Clipboard  
☐ Drives ☐ Supported Plug and Play devices  
☐ Serial ports

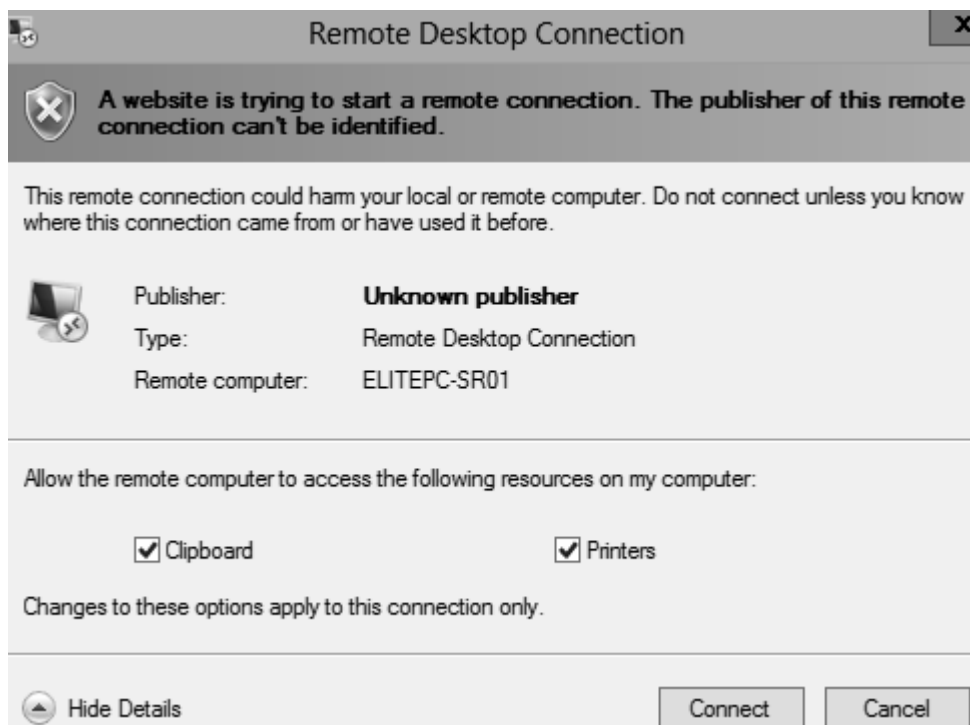
### Additional options

Remote computer sound:

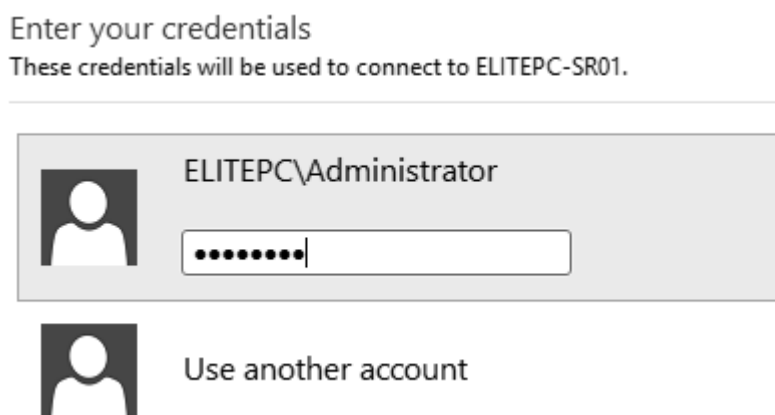
Apply keyboard shortcuts:

Performance:

Pojawi się okno połączenia pulpitu zdalnego, w którym należy nacisnąć przycisk **Połącz (Connect)**.



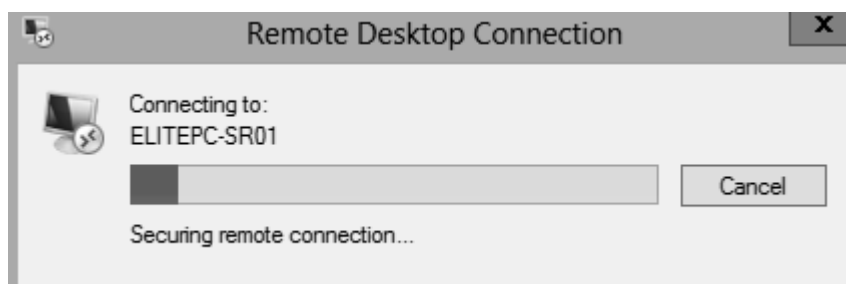
Należy podać dane do logowania, które mają zostać użyte do nawiązania połączenia z komputerem zdalnym.



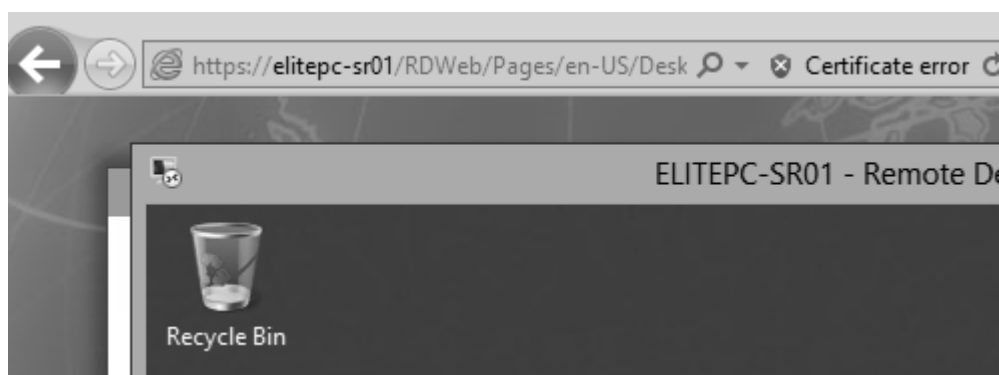
Nastąpi przygotowywanie i nawiązywanie połączenia zdalnego, które musi zostać



zabezpieczone, dlatego też proces ten może chwilę zająć.



Jeżeli zostało wybrane połączenie pulpitu zdalnego w trybie pełnoekranowym praca zdalna będzie wyglądać analogicznie do tej znanej z pracy ze zwykłym połączeniem pulpitu zdalnego. W przeciwnym razie jeżeli zostanie wybrana mniejsza rozdzielczość zostanie otworzone okienko w tym rozmiarze, a obraz pulpitu komputera zdalnego dostosowany do jego wymiarów.



## 19. Serwer Wydruku

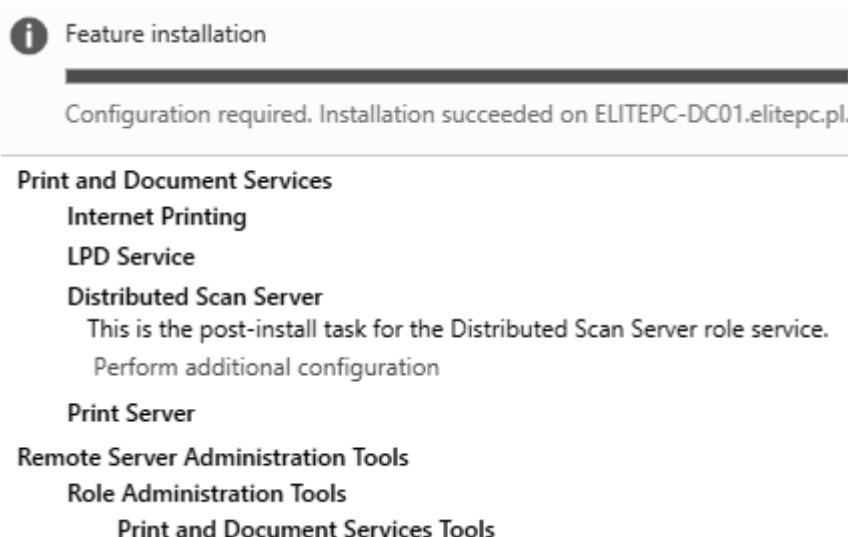
Na początek należy dodać nową rolę do serwera, wybierając z listy *Usługi drukowania i zarządzania dokumentami (Print and Document Services)*. Należy kliknąć *Dalej (Next)*.

- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☒ DNS Server (Installed)
- ☐ Fax Server
- ☒ File And Storage Services (Installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☒ **Print and Document Services**
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☒ Web Server (IIS) (Installed)
- ☐ Windows Deployment Services
- ☒ Windows Server Update Services (Installed)

Należy wybrać wszystkie usługi i kliknąć *Dalej (Next)*.

- Role services
- ☒ Print Server
  - ☒ Distributed Scan Server
  - ☒ Internet Printing
  - ☒ **LPD Service**

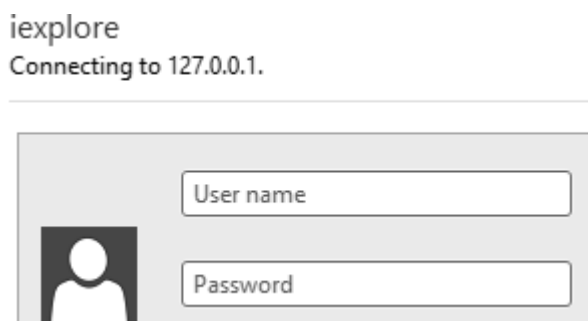
Po wgraniu niezbędnych plików powinno się ponownie uruchomić komputer, szczególnie jeżeli dodatkowo była instalowana rola IIS.



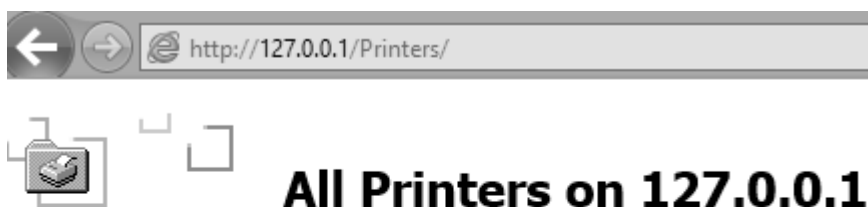
Po wpisaniu adresu <http://127.0.0.1/Printers> można wejść na stronę, na której zarządza się wydrukami.



System Windows poprosi użytkownika o uwierzytelnienie przed udzieleniem mu dostępu do serwera wydruków.



Jeżeli wszystko przebiegnie pomyślnie użytkownik otrzyma dostęp do udostępnionych drukarek.



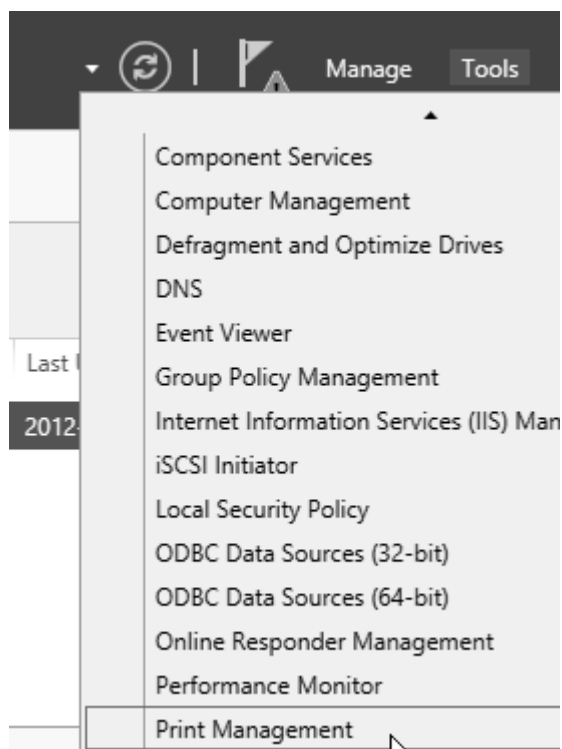
Name	Status	Location
<u>Brother Color Leg Type1 Class Driver</u>	Ready	

Po wybraniu dowolnej z nich strona www przeniesie użytkownika do podstrony drukarki, na której można nią zarządzać.



Opcje serwera wydruku można skonfigurować wchodząc do Menadżera serwera i wybierając *Narzędzia (Tools)*, a następnie *Zarządzanie Wydrukami (Print*

*Management).*



## 20. Serwer Faksów

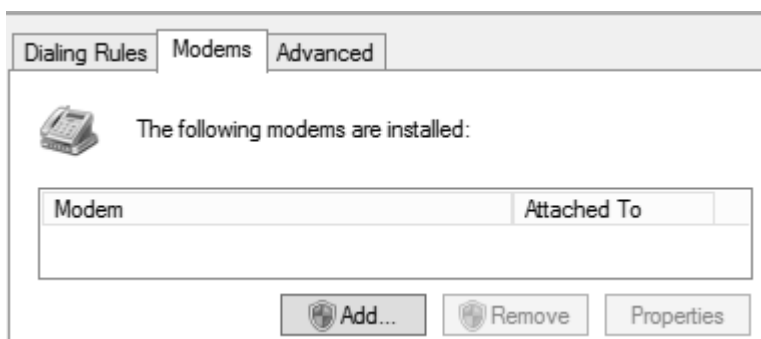
W tym rozdziale zostanie skonfigurowany serwer faxów. Przydatna będzie drukarka. Dla ćwiczeń zostanie zainstalowana wirtualna drukarka, która będzie zapisywać wydruki w formacie PDF np. BullZIP PDF Printer.

Drugim niezbędnym urządzeniem będzie sam modem. Potrzebny jest fizycznie zainstalowany modem, aby serwer działał, a także należy podpiąć linię telefoniczną pod niego.

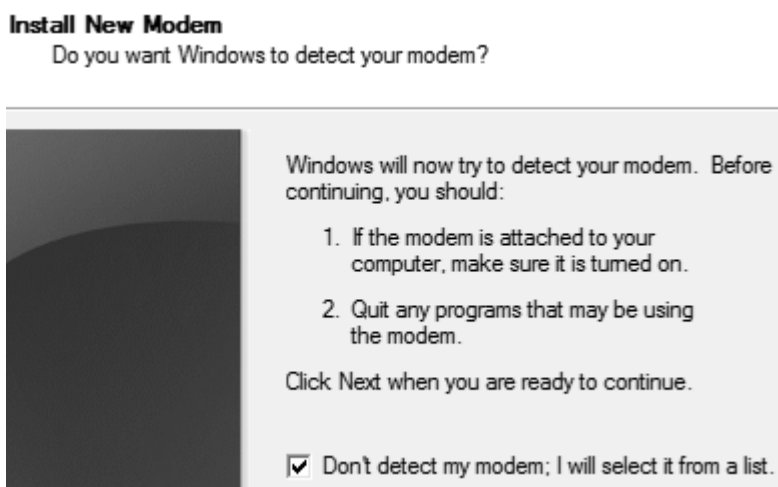
W ten sposób można oszukać system wymuszając na nim instalację modemu, którego nie jest podpięty fizycznie. W panelu sterowania wybiera się opcję **Telefon i Modem (Phone and Modem)**.



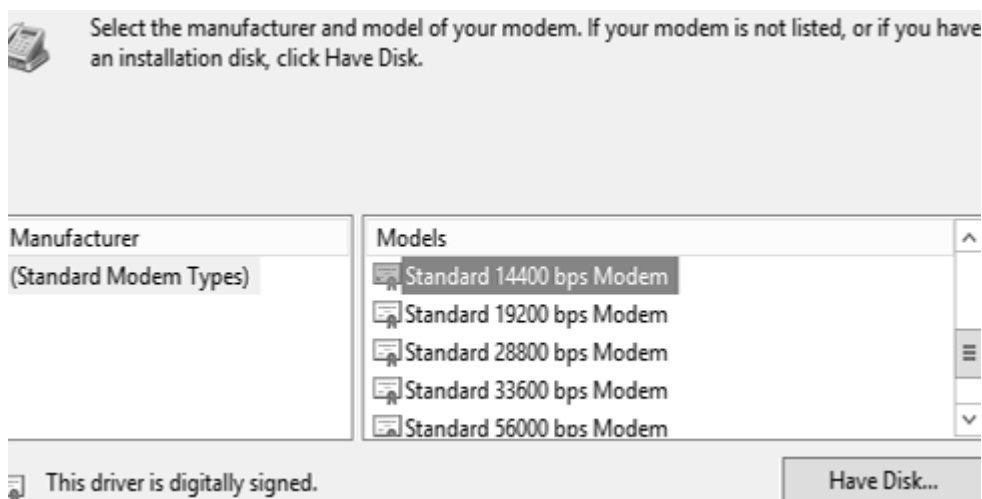
Następnie w zakładce modem należy kliknąć **Dodaj (Add)**.



Należy zaznaczyć *Nie wykrywaj mojego modemu (Don't detect my modem: I will select it from a list)* i kliknąć *Dalej (Next)*.



Należy chwilę poczekać aż lista się wygeneruje, a następnie wybrać modem z listy.



Gdy na komputerze zainstalowane są wszelkie niezbędne urządzenia można przystąpić do właściwej instalacji serwera wydruku. Należy wybrać i zainstalować rolę Serwer Faksów.



Następnie należy kliknąć ***Dalej (Next)***.

You can use a Fax Server to share and manage network fax resources from a central location, which enables users to send and receive faxes. By setting up a Fax Server, you can define routing policies and rules for faxes, provide access to faxes that have been previously sent or received, and configure activity logging to track the user of fax resources. You can use the Fax Service Manager to install, view, and manage all of the faxes in your organization.

#### Things to Note

- To set up a Fax Server, you must also set up a Print Server.
- To finish installing the Fax and Print server roles, you must complete post-deployment configuration for both roles. The Fax Server role is configured from the Microsoft Fax Service Manager. To configure additional fax server properties from the Microsoft Fax Service Manager, click Action on the menu bar and then click Properties.

Następnie należy zaznaczyć opcję ***Uruchom ponownie serwer docelowy jeśli wymagane (Restart the destination server automatically if required)*** i kliknąć przycisk ***Instaluj (Install)***.



To install the following roles, role services, or features on selected server, click Install.

☒ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click their check boxes.

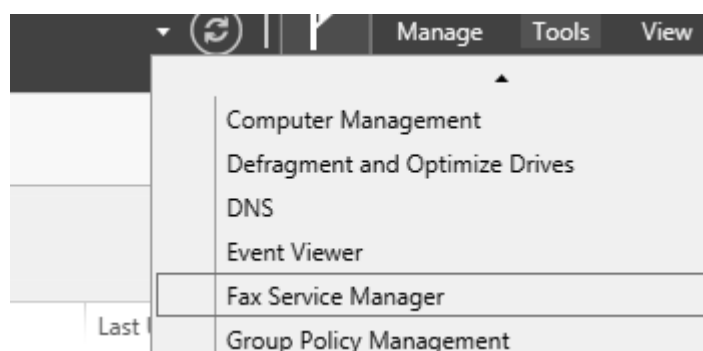
Fax Server

Remote Server Administration Tools

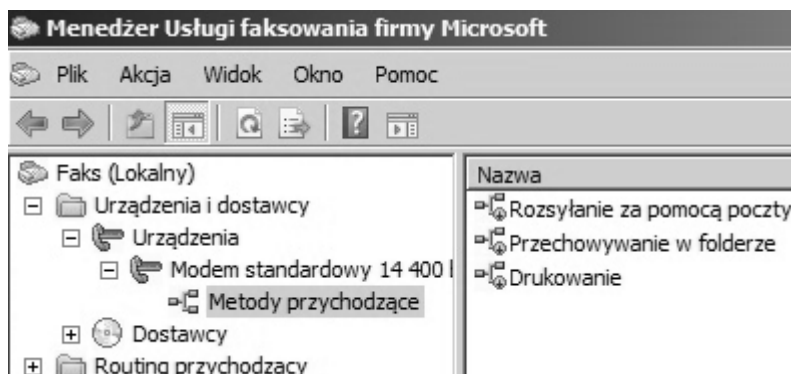
Role Administration Tools

Fax Server Tools

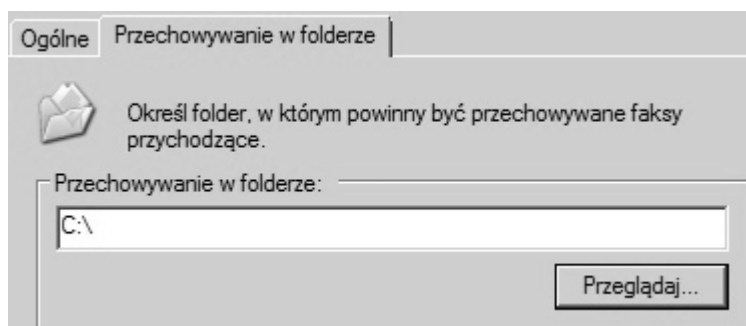
Aby przystąpić do wstępnej konfiguracji serwera należy wybrać **Menadżer Usług Faksowania (Fax Service Manager)**. Konsola ta jest identyczna jak w systemie Windows Server 2008 R2. Poniższe zrzuty ekranu demonstrują możliwości konfiguracyjne serwera faksów w Windows Server w wersji 2008.



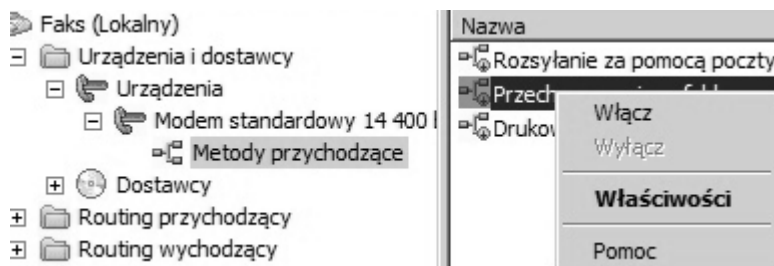
W dalszej kolejności rozwinąwszy drzewko menu zgodnie z obrazkiem poniżej można znaleźć trzy metody odbierania faksów. Pierwsza z nich przekaże fax na podany adres email, ostatnia spowoduje wydruk na drukarce, a środkowa zapisze wiadomość w formie pliku. W ćwiczeniu wybrano właśnie tę opcję.



W zakładce **Przechowywanie w folderze** należy wskazać ścieżkę do folderu, gdzie mają być zapisywane pliki i kliknąć **OK**.

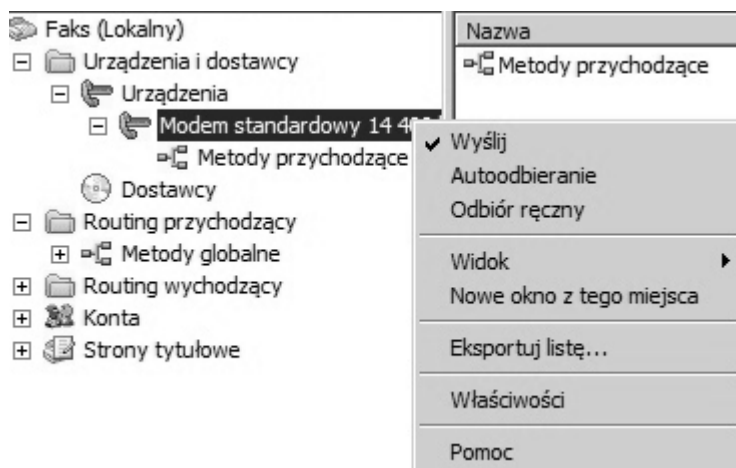


Należy pamiętać, aby użytkownicy wcześniej zdefiniowani mieli dostęp do tego folderu czy też do drukarki, która byłaby konfigurowana. Na koniec należy kliknąć prawym guzikiem na wybranej opcji i kliknąć **Włącz (Enable)**.

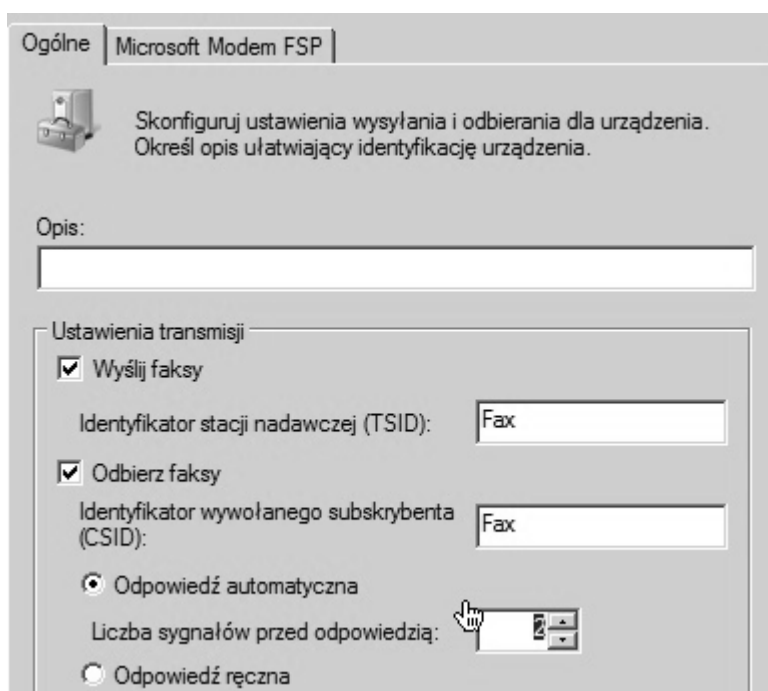


W następnym kroku konieczne jest kliknięcie na modemie i wejście w jego

### ***Właściwości (Properties).***

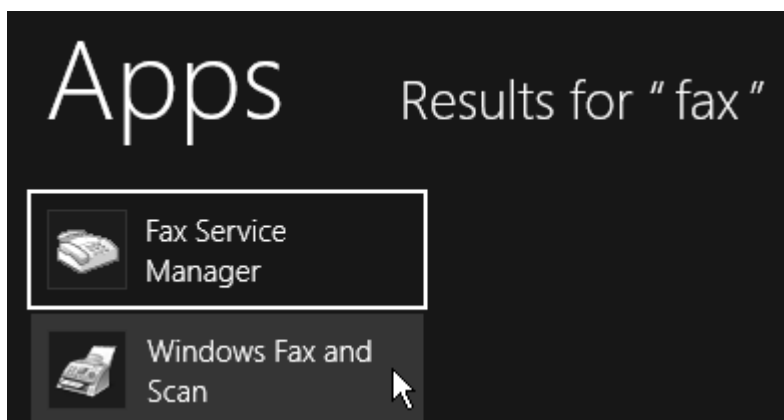


Na karcie **Ogólne** należy zaznaczyć opcję odbierz fax, a następnie ustawić liczbę sygnałów po jakich fax zostanie odebrany np. 2.

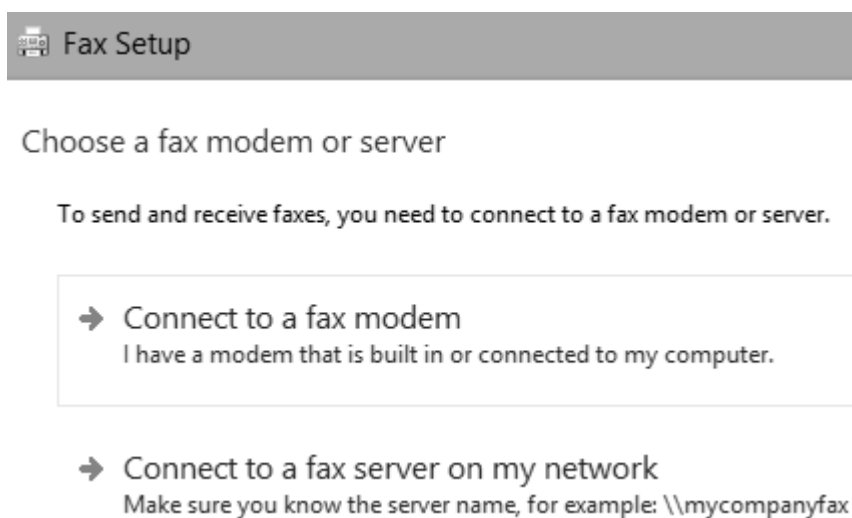


Odbieranie faksów jest już zapewnione, a co z wysyłaniem? Należy kliknąć **START**

i uruchomić *Faksowanie i skanowanie w systemie Windows (Windows Fax and Scan)*.



Na ekranie jaki się pojawi należy wybrać *Połącz z serwerem faksów w mojej sieci (Connect to a fax server on my network)*.



Następnie należy wpisać nazwę serwera i kliknąć *Dalej (Next)*.

## Fax Setup

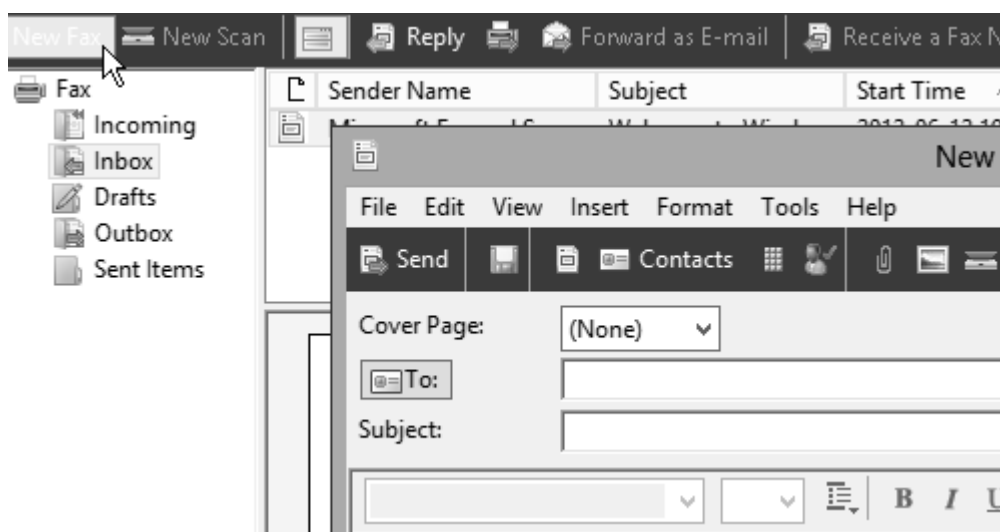
### Type the fax server location

Make sure you know the name and network address of the fax server.  
You also need permission from your network administrator to use it.

Name:

For example: \\mycompanyfax

Za pomocą tej aplikacji można tworzyć dokumenty, które będą wysłane za pomocą faksu.



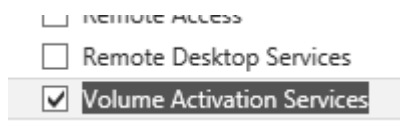
Należy także pamiętać, aby każdy użytkownik, który ma mieć dostęp do usług faksowania został dodany do grupy *Użytkownicy Faksu (Fax Users)*.

## 21. Volume Activation Services

Volume Activation Services jest rolą, która zastąpiła Key Management Service (KMS). Daje ona możliwość aktywacji systemów klienckich, serwerowych oraz innych aplikacji firmy Microsoft w obrębie przedsiębiorstwa bez konieczności nawiązywania bezpośredniego połączenia z serwerami aktywacyjnymi firmy Microsoft. Niniejszy rozdział omawia proces instalacji oraz jej wstępnej konfiguracji.

### a. Instalacja

Aby użytkownik mógł zainstalować Volume Activation Services musi posiadać uprawnienia administratora lokalnego do komputera docelowego oraz być członkiem grupy zabezpieczeń *Administratorzy Przedsiębiorstwa (Enterprise Administrators)*. Instalacji dokonuje się poprzez Menadżera Serwera, używając kreatora dodawania ról i funkcji.



W pierwszej karcie kreatora instalacji Volume Activation Services pojawiają się informacje o tym, za co ta rola odpowiada oraz jakie są wymagania do jej instalacji. Między innymi można się tutaj dowiedzieć o tym, iż niezbędny będzie klucz aktywacji woluminowej.

## Volume Activation Services

Before You Begin	<p>Volume Activation Services enables you to automate the installation of Volume Activation Service (KMS) host keys and the volume key activation process. You can install and manage a KMS host, or configure the volume activation for domain-joined systems.</p> <p>Things to Note:</p> <ul style="list-style-type: none"><li>• To install and enable Volume Activation Service, you must be a member of the Volume Activation Service Administrators group for the domain.</li><li>• To install and enable Volume Activation Service, you must have the appropriate permissions to install and manage a KMS host.</li></ul>
Installation Type	
Server Selection	
Server Roles	
Features	
<b>Volume Activation Services</b>	
Confirmation	

Bezpośrednio po użyciu przycisku **Dalej (Next)** zostanie wczytana karta podsumowująca, gdzie w celu zainstalowania roli należy wybrać przycisk **Instaluj (Install)**.

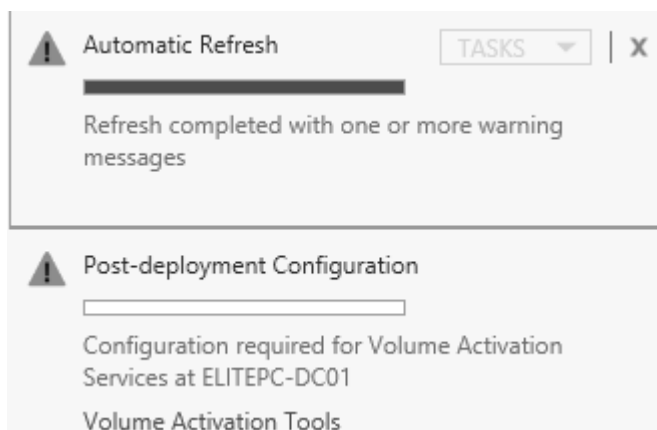
## Confirm installation selections

Before You Begin	To install the following roles, role services, and features, you must have the appropriate permissions to install and manage a KMS host.
Installation Type	<input checked="" type="checkbox"/> Restart the destination server automatically after installation.
Server Selection	Optional features (such as administration tools) have been selected automatically. If you do not want to install them, uncheck their check boxes.
Server Roles	
Features	
Volume Activation Services	Remote Server Administration Tools
<b>Confirmation</b>	Role Administration Tools
Results	Volume Activation Tools
	Volume Activation Services

### b. Wstępna konfiguracja VA Services

W Menadżerze Serwera w menu po lewej stronie pojawi się rola VA Services. Nie jest jednak ona jeszcze uruchomiona, niezbędna jest wstępna konfiguracja serwera. Można tego dokonać poprzez **Centrum Akcji**, gdzie klika się na nośnik **Volume**

*Activation Tools* w sekcji *Post-deployment Configuration*.



Pojawi się kreator, który składa się z czterech kroków. Pierwszym z nich jest wprowadzenie do usługi. Znajdują się tam informacje na temat samej roli, jak i wymagań jakie muszą zostać spełnione przed dalszą konfiguracją.

## Introduction to Volume Activation Services

Introduction	Volume Activation Services enables you to automate the installation and activation of Microsoft software volume licenses for a variety of devices. With Volume Activation Services, you can install and activate a variety of volume licenses for Windows clients and servers. After this service is installed, you can configure the KMS. After this service is installed, you can configure the KMS. After this service is installed, you can configure the KMS.
Activation Type	
Product Key Management	
Configuration	<b>Things to Note</b> To install and enable Volume License Services, the following are required: - Local administrator permissions on the computer (separate) where you intend to install keys and manage licenses. - Permissions to write data to the Activation Objects in the Active Directory Domain Services (AD DS) database. - You also must have a unique Key Management Service (KMS) host name. For more information about volume licensing options, see <a href="#">Volume Licensing Overview</a> .

W kolejnym kroku należy określić metodę aktywacji. W przypadku domeny



najwygodniej będzie wybrać *Autentykacja oparta na Active Directory (Active Directory – Based Activation)*. Dzięki temu nowa rola dostosuje się do infrastruktury AD i nie będzie wymagana żadna dodatkowa konfiguracja np. Firewalla. W tym oknie istnieje też możliwość podania nazwy użytkownika i hasła, gdyby obecnie zalogowany użytkownik na komputerze nie miał odpowiednich uprawnień do przeprowadzenia instalacji.

## Select Volume Activation Method

Introduction

Activation Type

Product Key Management

Configuration

You can modify an existing volume activation method you want to manage and, for the Key Management Service (KMS) installed.

If you need to use credentials other than your current user, you can specify them here before proceeding.

☒ Active Directory-Based Activation

☐ Key Management Service (KMS)

☐ Alternate credentials (optional)

User name:

Password:

Na kolejnej karcie konieczne jest wprowadzenie numeru licencji klienta na podstawie, której dokonywane będą aktywacje.

## Manage Activation Objects

Introduction

Activation Type

**Product Key Management**

Configuration

Install your Key Management Service (KMS) host Key to create a new Activation Object

☒ Install your KMS host key

☐ Enter a display name for your new Activation Object (optional)

☐ Skip to Configuration

Niezbędne będzie połączenie z serwerami Microsoft w celu weryfikacji i aktywacji tego klucza, podobnie jak w przypadku systemów operacyjnych można tego dokonać online lub telefonicznie zatwierdzając swój wybór przyciskiem **Wykonaj (Commit)**.

## Activate Product

Introduction

Activation Type

**Product Key Management**

Configuration

Activate the Key Management Service (KMS) host Key to create a new Activation Object

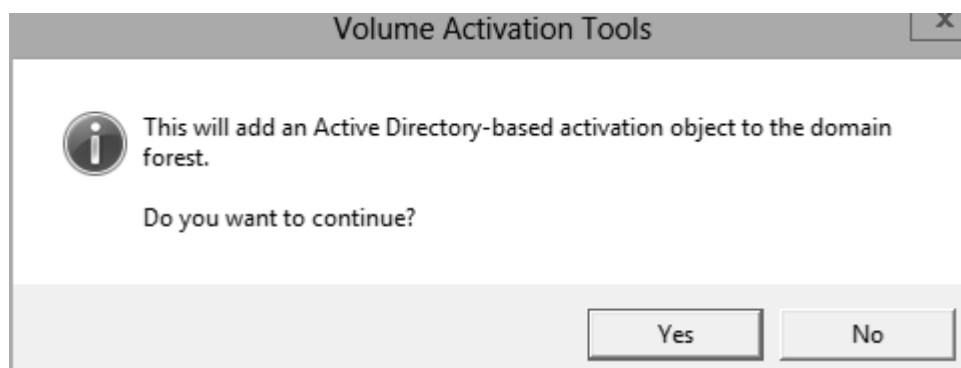
☒ Activate online

☐ Activate by phone

Select location

Afghanistan

Pojawi się komunikat informujący o tym, że do Active Directory zostanie dodany nowy obiekt, który należy zatwierdzić przyciskiem **Tak (Yes)**.



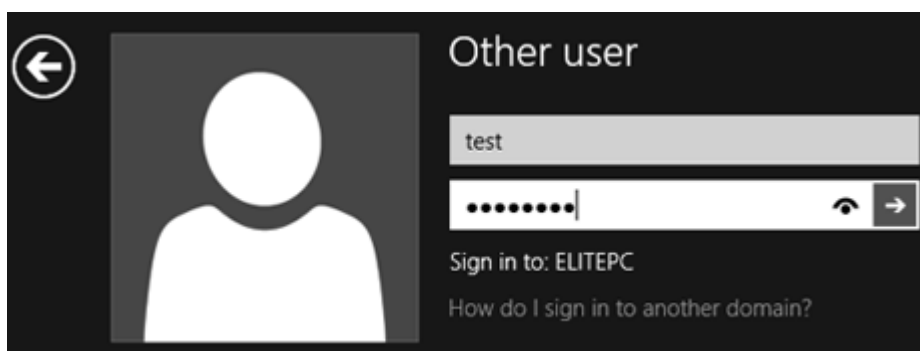
Po pomyślnej aktywacji rola będzie zainstalowana i uruchomiona.

## 22. Triki

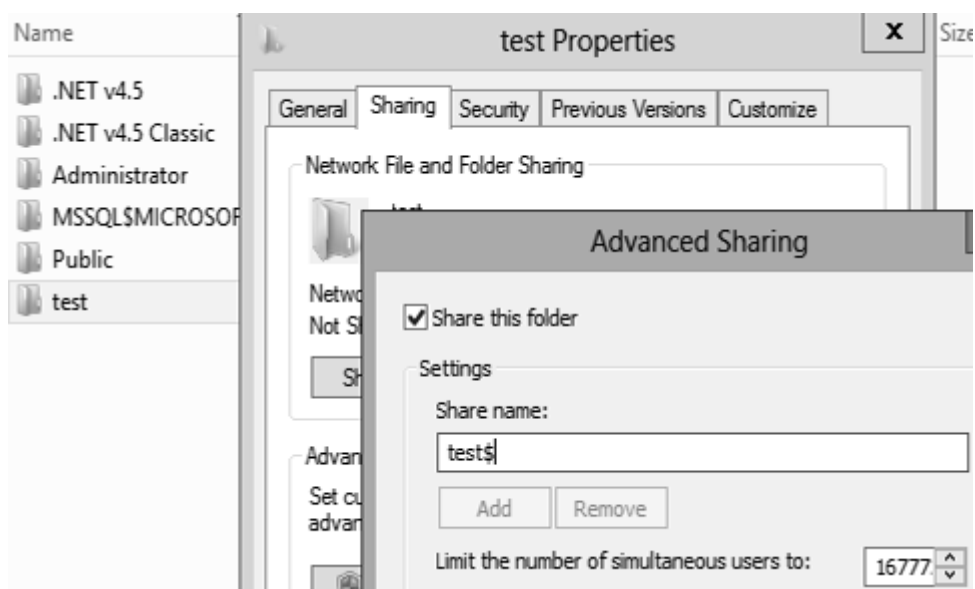
### a. Wędrujący i wymuszony profil użytkownika

Należy stworzyć profil użytkownika, który nie będzie mógł samodzielnie edytować ustawień konta, a wprowadzone przez niego zmiany będą automatycznie kasowane. Na początek konieczne będzie stworzenia jakiegoś konta użytkownika, a następnie dostosowanie go do własnych potrzeb. Kolejnym krokiem będzie wylogowanie się z komputera i zalogowanie się na nim jako administrator.

Dla przykładu na samym początku można stworzyć nowy profil dla użytkownika test, następnie zalogować się na nim po to, aby system utworzył jego domyślny profil. Można ten profil dostosować tak, aby spełniał on odpowiednie oczekiwania (np. posiadał odpowiednie pliki czy skróty na pulpicie).



Następnie należy wylogować się z konta użytkownika test i zalogować jako administrator. Warto zauważyć, że na dysku lokalnym C w folderze Users powstał nowy katalog o nazwie test. Powinien on zostać teraz udostępniony. Aby to uczynić należy kliknąć na tym folderze prawym klawiszem myszy i we właściwościach udostępnić go tak, aby tylko docelowa grupa użytkowników miała do niego dostęp. Warto też sprawić, aby folder był ukryty w otoczeniu sieciowym.



Następnie należy otworzyć konsolę *Użytkownicy i Komputery Usługi Active Directory (Active Directory Users and Computers)*. We właściwościach pożądanego użytkownika w zakładce profile podaje się na sztywno ścieżkę dla profilu użytkownika (ścieżkę sieciową). Nie ma znaczenia czy zostanie użyta adresacja IP czy rekordy serwera DNS.

Member Of		Dial-in	Environment		Sessions
Remote control		Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	Organization

User profile

Profile path:

Logon script:

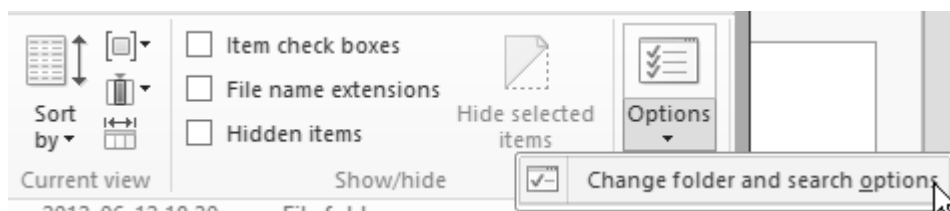
Home folder

☒ Local path:

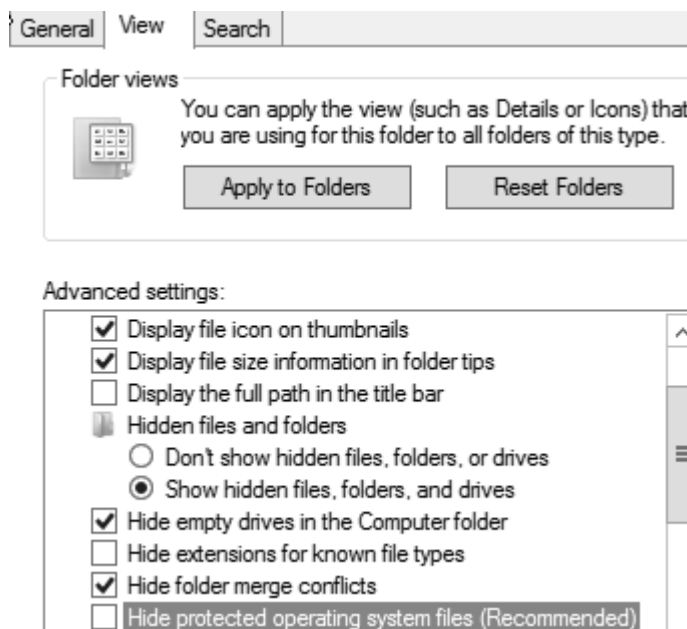
☐ Connect:  To:

To jednak nie wszystko. Tak przygotowany profil użytkownicy będą mogli

edytować i zapisywać w nim zmiany. Należy zmienić profil na tzw. **Profil Wymuszony (Mandatory)**. W tym celu w oknie zawierającym zawartość profilu użytkownika w górnym menu należy kliknąć guzik **Widok (View)**, następnie rozwinąć **Opcje (Options)** i wybrać **Zmień opcje przeszukiwania folderów (Change folder and search options)**.









Teraz należy wejść w zakładkę **Widok (View)**, gdzie należy wybrać **Pokaż ukryte pliki i foldery (Show hidden files, folders and drives)** i odznaczyć, **Ukryj rozszerzenie znanych typów plików (Hide extensions for known file types)** oraz **Ukryj chronione pliki systemowe (Hide protected operating system files)**.

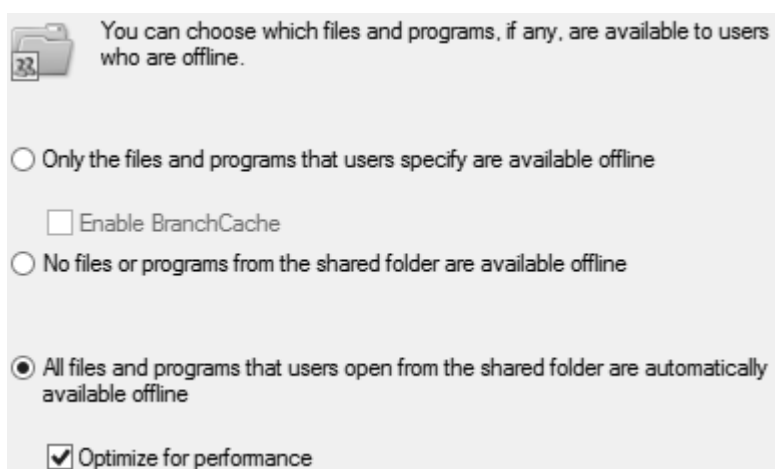


W katalogu użytkownika pojawi się teraz więcej plików oraz ich rozszerzenia.

Zmiana rozszerzenia pliku NTUSER.DAT na NTUSER.MAN, spowoduje to, że żadne zmiany wprowadzone w profilu użytkownika, jak na przykład utworzenie nowego pliku na pulpicie czy zmiana tła pulpitu nie zostaną zachowane. Po wylogowaniu po prostu zmiany wprowadzone przez użytkownika będą tracone.

 Saved Games	2012-06-12 18:30	File fo
 Searches	2012-06-12 18:30	File fo
 SendTo	2012-06-12 18:30	File fo
 Start Menu	2012-06-12 18:30	File fo
 Templates	2012-06-12 18:30	File fo
 NTUSER.MAN	2012-06-12 18:30	DAT F

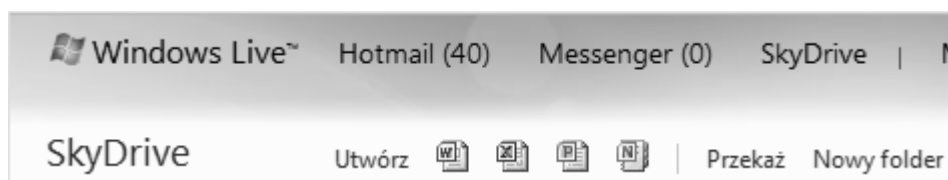
Obecna konfiguracja zakłada jednak to, że użytkownicy przy każdym logowaniu będą ściągali z serwera swoje dane. Jest to o tyle kłopotliwe że może prowadzić do zbyt dużego obciążenia sieci. Wracając więc do właściwości udostępnionego folderu i uruchamiając jeszcze pliki trybu offline z optymalizacją dla wydajności można osiągnąć to, że dane użytkowników będą ściągane nie zawsze lecz np. wtedy gdy użytkownik przesiądzie się na inny komputer. W przypadku zwykłych kont użytkownika również warto pomyśleć o takiej optymalizacji jeżeli są one przechowywane w lokalizacji sieciowej.



## b. Dane w chmurze - mapowanie SkyDrive

Windows Live SkyDrive to wirtualny dysk autorstwa firmy Microsoft i jednocześnie część serwisu Windows Live. SkyDrive w darmowej wersji udostępnia 25 GB miejsca, ograniczeniem wysyłanych plików jest ich rozmiar nie przekraczający 100 MB na plik (z racji nieustannie doskonalącej się oferty firmy Microsoft liczby te mogą ulec zmianie). Te wartości jednak zmieniają się bardzo szybko. Teraz zostanie przedstawione jak podmontować w swoim komputerze lub serwerze dysk Skydrive tak, aby był widoczny w Moim Komputerze tak samo jak inne dyski. Dzięki temu będzie można zabezpieczyć w chmurze najważniejsze dane. Analogiczne kroki można podjąć posiadając wykupione płatne usługi w chmurze w firmie Microsoft. Konfiguracja dla ułatwienia w przykładzie zostanie przedstawiona na systemie klienckim Windows 7. W innych systemach proces przebiega analogicznie.

Pierwszym krokiem jest udanie się na stronę [skydrive.live.com](http://skydrive.live.com) gdzie należy albo się zalogować albo zarejestrować. Po zalogowaniu tworzy się folder bądź foldery.

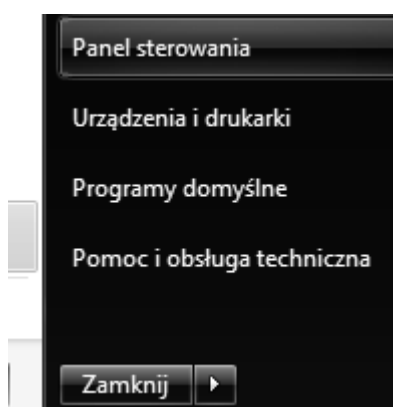


Warto zwrócić uwagę na to, aby uprawnienia folderów były adekwatne do celu. Innymi słowy jeżeli foldery mają nie być nikomu udostępniane prawidłowym parametrem udostępniania powinno być „*Tylko ja*”

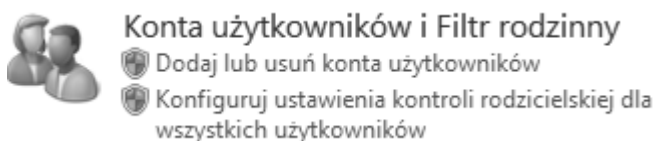


<b>Nazwa *</b>	Data modyfikacji	Autor ostatniej mo...	Udostępnione użyt...
BackupAlien	2012-04-21	ElitePC Kursy Sieci ...	Tylko ja
Dokumenty	2012-02-19	ElitePC Kursy Sieci ...	Tylko ja
AE2420	2010-09-24	ElitePC Kursy Sieci ...	Wszyscy (publiczne)

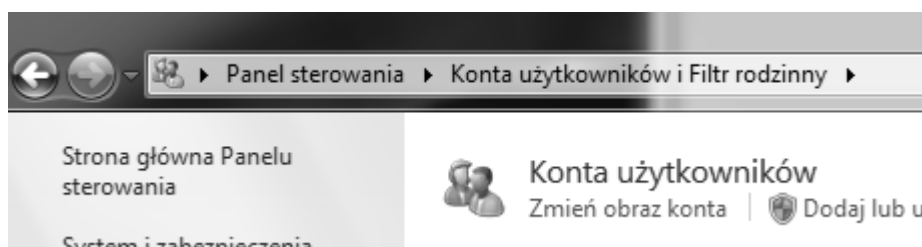
W Windows 7 należy wejść do panelu sterowania.



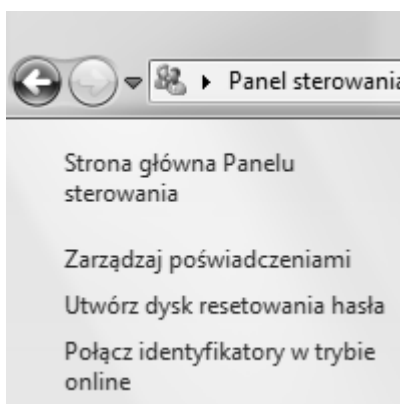
Następnie należy wybrać **Konta użytkowników i Filtr rodzinny**.



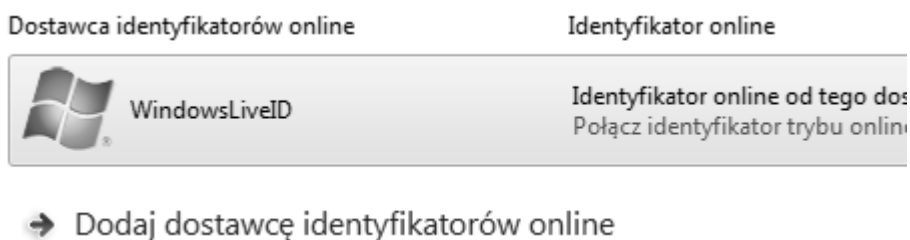
W dalszej kolejności konieczne jest wejście w **Konta Użytkowników**.




W końcu w menu po lewej stronie okna należy kliknąć ***Połącz identyfikatory w trybie online.***



Na poziomie loga Windows Live ID konieczne jest kliknięcie na link ***Połącz identyfikator trybu online.***



Jeżeli są wgrane dodatki Microsoft Live Essentials pojawi się od razu ekran logowania do usługi Windows Live, w przeciwnym razie najpierw nastąpi przekierowanie do strony www, na której będzie możliwość pobrania niezbędnego pliku instalacyjnego.

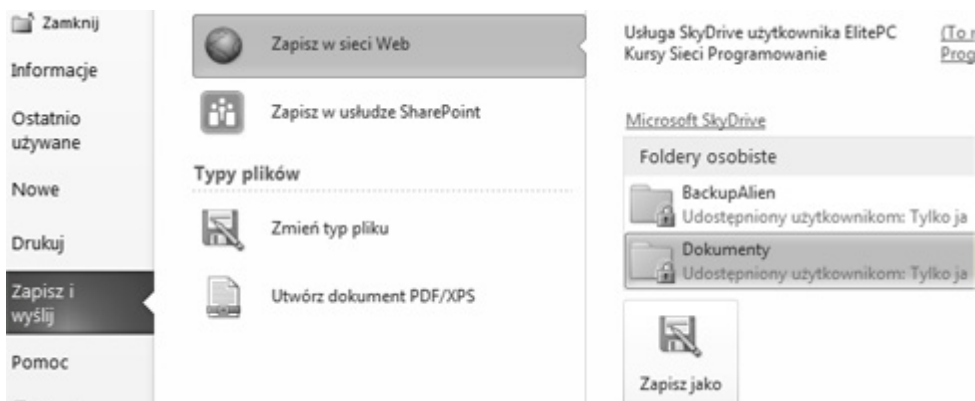


[Nie pamiętasz swojego hasła?](#)

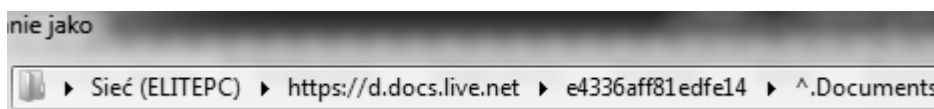
Dostawca identyfikatorów online	Identyfikator online
 WindowsLiveID	elitepc@windowslive.com <a href="#">Aktualizuj poświadczenie</a>

➔ Dodaj dostawcę identyfikatorów online

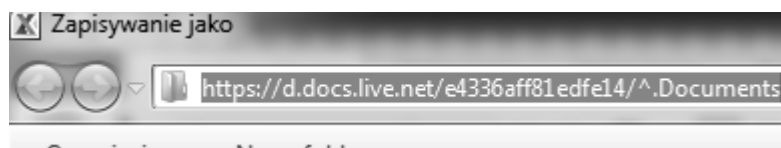
Teraz programy jak Microsoft Office uzyskały możliwość zapisu do dowolnego folderu na dysku Skydrive. Aby taki folder zamapować potrzebna będzie jego dokładna ścieżka sieciowa. W tym celu należy włączyć np. Excel, z menu **Plik** wybrać opcję **Zapisz i Wyślij**, a następnie w rozwiniętym menu **Zapisz w sieci Web**, aby po chwili po prawej stronie pojawiły foldery dostępne w usłudze Skydrive. Konieczne jest wybranie folderu, który ma zostać zmapowany i kliknięcie **Zapisz Jako**.



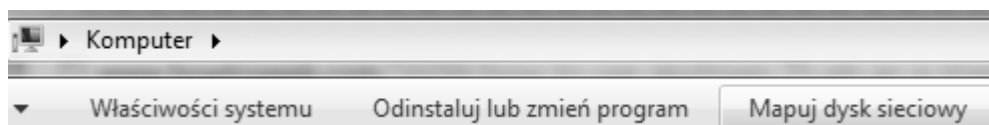
Po kliknięciu w górny pasek adresu się możliwość skopiowania adresu dysku.



Po wyłuskaniu fizycznej ścieżki internetowej do dysku Skydrive dysk ten można zamontować w tradycyjny sposób na dowolnym komputerze pod kontrolą Windows lub innego systemu operacyjnego.

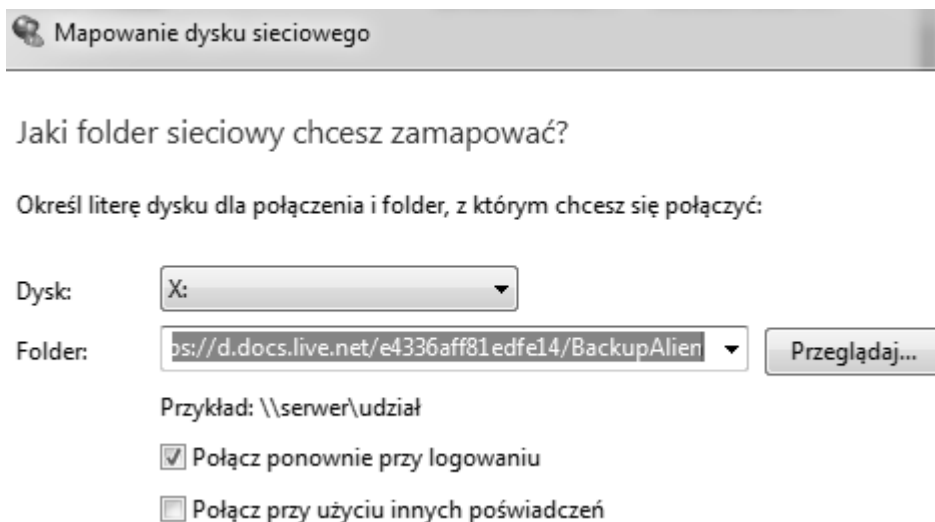


Należy wejść w *Mój Komputer* i w górnym menu wybrać opcję *Mapuj Dysk Sieciowy*.



W oknie, które się pojawi konieczne jest określenie litery dysku oraz wklejenie

wcześniej skopiowanego linku. Całą akcję należy zatwierdzić klikając **Zakończ**.



Mapowanie dysku sieciowego

Jaki folder sieciowy chcesz zamapować?

Określ literę dysku dla połączenia i folder, z którym chcesz się połączyć:

Dysk: X:

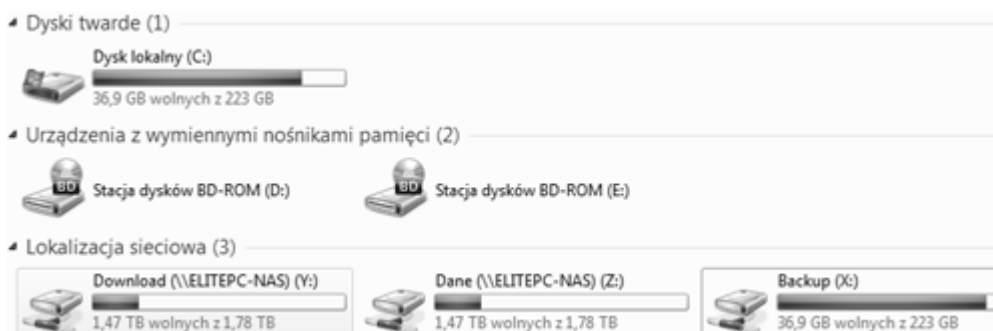
Folder: ps://d.docs.live.net/e4336aff81edfe14/BackupAlien Przeglądaj...

Przykład: \\serwer\udział

☒ Połącz ponownie przy logowaniu

☐ Połącz przy użyciu innych poświadczeń

Jeżeli wszystko przebiegnie pomyślnie dysk sieciowy pojawi się w Moim Komputerze i będzie automatycznie podłączany przy każdym uruchomieniu komputera. Teraz pozostaje tylko zabezpieczać swoje dane. Można to robić ręcznie bądź użyć np. darmowej aplikacji Comodo Backup.

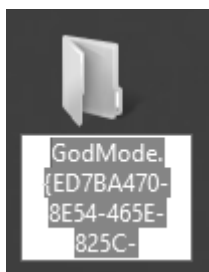


### c. GodMode

W Windows Server 2012 można stworzyć specjalny folder, który pozwoli zebrać wszystkie narzędzia konfiguracyjne systemu w jednym miejscu. Aby utworzyć taki folder należy postępować tak, jak w przypadku tworzenia zwykłego folderu, czyli

kliknąć na pulpicie prawym klawiszem myszki i wybrać opcję *Nowy -> Folder*, a następnie nadać nazwę folderowi, musi być dokładnie taka jak poniżej:

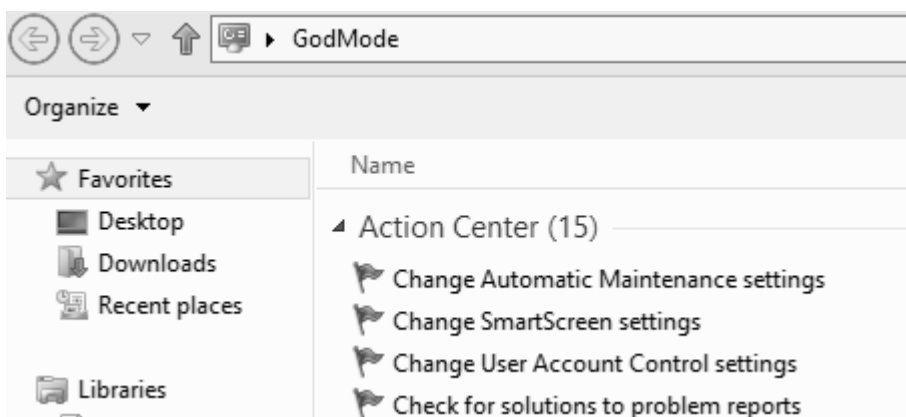
**GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}**



Folder został utworzony i zmieniła się jego ikona oraz nazwa, a mianowicie wygląda jak na ilustracji poniżej:



Jego zawartość jest imponująca i daje administratorowi duże możliwości wprowadzania przeróżnych konfiguracji dla systemu.

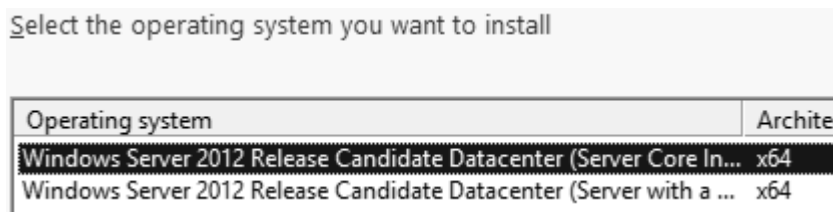


## 23. Windows 2012 Core

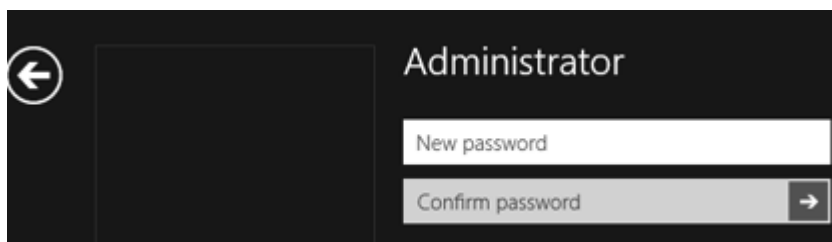
Windows Server 2012 podobnie jak jego poprzednik może zostać zainstalowany w trybie Core. Tryb ten charakteryzuje się tym, że nie instaluje on graficznej powłoki systemu Windows. Nie są instalowane także programy korzystające z graficznego interfejsu użytkownika za wyjątkiem kilku programów jak na przykład notatnik. Systemem zainstalowanym w wersji Core można zarządzać za pomocą wiersza poleceń PowerShell'a, lub zdalnie za pomocą Microsoft Management Console. W dziale tym czytelnik dowie się w jaki sposób zainstalować system w wersji Core oraz poznać podstawy zarządzania takim systemem na podstawie kilku wybranych ról.

### a. Instalacja wstępna konfiguracja

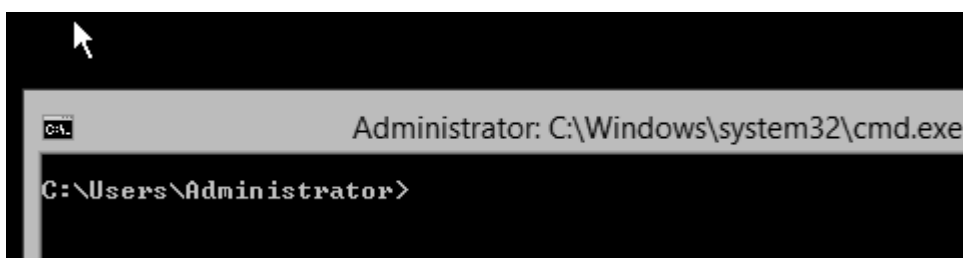
Proces instalacji systemu Windows Server 2012 w wersji Core praktycznie nie różni się od standardowej instalacji. Podczas wyboru systemu operacyjnego, który ma zostać zainstalowany wystarczy wybrać ten, w którego nazwie w nawiasie występuje sformułowanie Server Core.



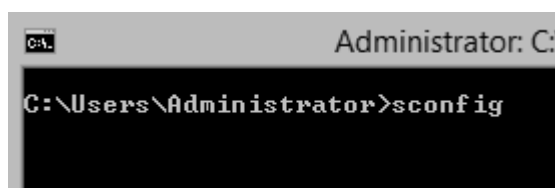
Pozostałe kroki instalatora są analogiczne do tych opisanych w rozdziale 1. Podobnie jak i w tym rozdziale instalator zakończy się prośbą podania nowego hasła dla administratora.



Duże zmiany w interfejsie można dostrzec dopiero po zalogowaniu się do systemu operacyjnego. Zamiast standardowego GUI jest czarny ekran z uruchomioną konsolą CMD.



Podstawowym poleceniem, które będzie wykorzystywane jest *sconfig*, który uruchamia *Narzędzie Konfiguracji Serwera (Server Configuration)*.



Narzędzie to pozwala na konfigurację podstawowych ustawień komputera takich jak:

- Domena/grupa robocza
- Nazwa komputera
- Dodawanie administratorów
- Konfigurowanie zdalnego zarządzanie



- Konfigurowanie aktualizacji
- Ściągnięcie i instalacja aktualizacji
- Zdalny pulpit
- Ustawienia sieci
- Ustawienia daty i czasu
- Konfiguracja ustawień związanych z programem raportowania błędów w firmie Microsoft
- Aktywacja systemu
- Wylogowanie użytkownika
- Ponowne uruchomienie serwera
- Wyłączenie serwera
- Wyjście do wiersza poleceń

Aby dostać się do jakichś ustawień wystarczy podać numer wybranej opcji, a wybór zatwierdzić klawiszem **Enter**.

```

Administrator: C:\Windows\system32\cmd.exe - sc

=====
                        Server Configuration
=====

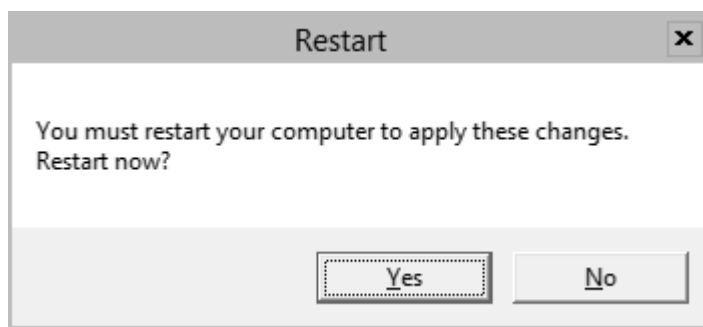
1> Domain/Workgroup:                Workgroup:  WORKGR
2> Computer Name:                  WIN-TRDOG30UU33
3> Add Local Administrator
4> Configure Remote Management      Enabled
5> Windows Update Settings:         Manual
6> Download and Install Updates
7> Remote Desktop:                  Disabled
8> Network Settings
9> Date and Time
10> Help improve the product with CEIP  Not participating
11> Windows Activation

12> Log Off User
13> Restart Server
14> Shut Down Server
15> Exit to Command Line

Enter number to select an option:

```

Pierwszym krokiem będzie nadanie komputerowi odpowiedniej nazwy. Dokonuje się tego poprzez wybranie opcji numer 2 i wprowadzenie pożądanej nazwy komputera. Po zatwierdzeniu jej klawiszem **Enter** pojawi się okienko informujące o tym, że wymagany jest ponowny rozruch komputera.



Gdy komputer ponownie się uruchomi, należy ponownie włączyć narzędzie konfiguracji serwera, aby tym razem skonfigurować sieć za pomocą opcji numer 8. Po jej wybraniu wylistowana zostanie tablica dostępnych interfejsów sieciowych. Aby dostać się do konfiguracji, któregoś z nich należy podać jego indeks, a wybór potwierdzić przyciskiem **Enter**. Do wyboru pojawią się cztery opcje. Są nimi konfiguracja adresów sieciowych, konfiguracja serwerów DNS, oczyszczenie ustawień serwerów DNS oraz powrót do poprzedniego menu.

```
1> Set Network Adapter Address
2> Set DNS Servers
3> Clear DNS Server Settings
4> Return to Main Menu
```

Za pomocą opcji pierwszej należy przypisać serwerowi statyczny adres IP. Komputer najpierw zapyta czy adres IP ma być przypisywany z serwera DHCP (opcja D) czy adres będzie statycznych (opcja S). Następnie poprosi o wprowadzenie kolejnych adresów IP. Jeżeli jakieś mają nie zostać podane zostawia się pole puste.

```

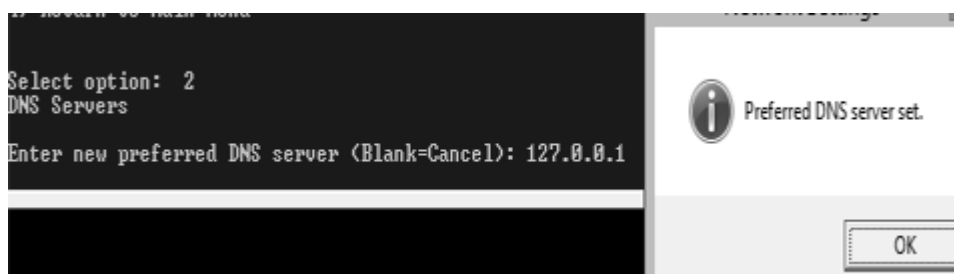
Select option: 1

Select <D>HCP, <S>tatic IP <Blank=Cancel>: S

Set Static IP
Enter static IP address: 192.168.0.1
Enter subnet mask <Blank = Default 255.255.255.0>: 255.255.255.0
Enter default gateway:
Setting NIC to static IP...

```

Należy także skonfigurować serwery DNS jeżeli będą takowe wymagane. W przykładowym laboratoryjnym przypadku Windows Server sam w sobie będzie serwerem DNS, więc należy wprowadzić adres IP localhosta, czyli **127.0.0.1**.



Oprócz korzystania z poleceń PowerShell'a oraz przygotowanych programów można korzystać także z wiersza poleceń. Za pomocą polecenia **md Share** należy stworzyć na dysku C komputera folder o nazwie **Share**. Poleceniem **dir** należy wylistować zawartość dysku C w celu weryfikacji czy folder został utworzony.

```

C:\>md Share

C:\>dir
Volume in drive C has no label.
Volume Serial Number is 9E39-E83B

Directory of C:\

2012-05-19  10:58    <DIR>          PerfLogs
2012-05-19  10:45    <DIR>          Program Files
2012-05-19  11:25    <DIR>          Program Files (x86)
2012-07-12  11:21    <DIR>          Share
2012-07-12  10:40    <DIR>          Users
2012-07-12  11:15    <DIR>          Windows
                0 File(s)        0 bytes
                6 Dir(s)  20 238 585 856 bytes free

```

Aby folder udostępnić należy wydać polecenie **NET SHARE** z odpowiednim parametrem.

```
C:\>NET SHARE sharename=C:\Share  
sharename was shared successfully.
```

Naturalnie poznanie wszystkich poleceń oraz wszystkich możliwych parametrów jest możliwym tematem dla kilku oddzielnych publikacji. Tym o czym będzie teraz wspomniane jest możliwość skorzystania z podpowiedzi dla każdej z komend, które można wyświetlić za pomocą sformułowania *nazwa\_polecenia /?*

```
C:\>NET SHARE /?  
The syntax of this command is:  
  
NET SHARE  
sharename  
sharename=drive:path [/GRANT:user,[READ | CHANGE | FULL]]  
[ /USERS:number | /UNLIMITED]  
[ /REMARK:"text"]  
[ /CACHE:Manual | Documents | Programs | BranchCache | None]  
sharename [/USERS:number | /UNLIMITED]  
[ /REMARK:"text"]  
[ /CACHE:Manual | Documents | Programs | BranchCache | None]  
{sharename | devicename | drive:path} /DELETE  
sharename \\computername /DELETE
```

## b. Zarządzanie systemem w wersji Core

W tym podrozdziale największa waga zostanie przywiązana do nauki podstaw zarządzania systemem Windows Server 2012 w wersji Core. Przede wszystkim zostaną przedstawione różne interfejsy użytkowników oraz możliwości przełączania się między nimi oraz różnice pomiędzy nimi. Następnie zostanie zainstalowanych kilka podstawowych ról serwera za pomocą wiersza poleceń zamiast trybu graficznego.

### i. Interfejsy użytkownika

Jedną z nowości w Windows Server 2012 jest możliwość swobodnego przełączania

się pomiędzy graficznym interfejsem użytkownika, a tekstowym. Wymagany będzie jedynie restart komputera, aby tego dokonać. Wcześniej taka zmiana wymagała reinstalowania całego systemu operacyjnego. Jest to ukłon w stronę administratorów, którzy są początkujący w PowerShell i pragną dokonać konfiguracji w trybie graficznym, a następnie przełączyć się do trybu tekstowego, dzięki czemu serwer nie straci na prostocie konfiguracji, a jednocześnie będzie lepiej zabezpieczony. Aby przełączyć się z trybu tekstowego na graficzny należy wydać polecenie: ***Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell –Restart***. Przed jego wpisaniem należy uruchomić PowerShell komendą ***PowerShell***.

```
C:\>powershell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\> Install-WindowsFeature Server-Gui-Mgmt-Infra, Server-Gui-Shell -restart
```

Rozpocznie się proces instalacji i pojawi się pasek postępu. Instalacja może trwać od kilku do kilkunastu minut w zależności od wydajności komputera.

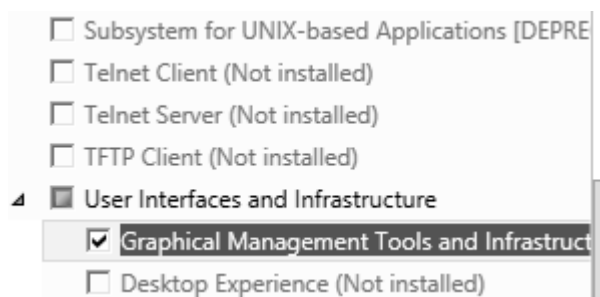
```
The syntax of this command is:

Start Installation...
 68%
[oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]
```

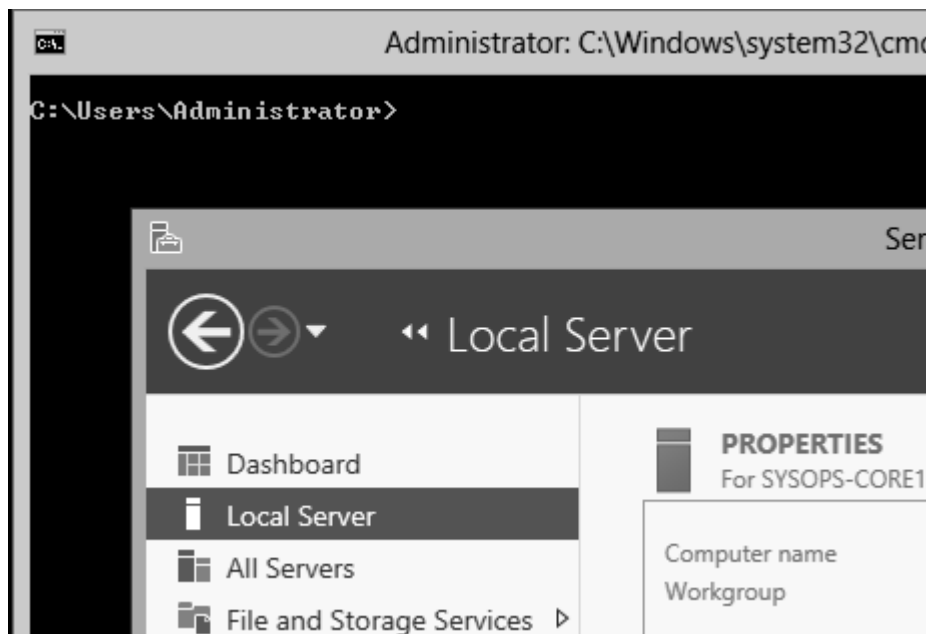
Aby z trybu graficznego powrócić do trybu tekstowego należy wpisać polecenie ***Uninstall-WindowsFeature Server-Gui-Mgmt-Infra –Restart***.

W Windows Server 2012 została jeszcze wprowadzona opcja pośrednia, tzw. ***Minimalny interfejs serwera (Minimal Server Interface)*** zwany również ***MinShell***. Stanowi on coś pośredniego pomiędzy trybem w pełni graficznym, a w pełni tekstowym. Administrator w tym trybie ma dostęp do graficznej konsoli menadżera serwera. W części panelu sterowania konsoli MMC oraz wiersza poleceń PowerShell administrator nie ma dostępu do Explorera Windows, Internet Explorera

oraz interfejsu startowego metra. Poza zwiększeniem wygody MinShell zwiększa także bezpieczeństwo systemu Windows Server zmniejszając obszary potencjalnych ataków. Aby uruchomić system operacyjny w tym trybie należy odinstalować wszystkie role i funkcje za wyjątkiem ***Graphical Management Tools and Infrastructure***. Kolejnym krokiem będzie ponowne uruchomienie komputera.



Po ponownym uruchomieniu komputera interfejs, który się wczyta będzie hybrydowy. Pojawią się zarówno elementy z trybu graficznego jak i tekstowego.



## **ii. Podstawowe role serwera**

Windows Server 2012 daje możliwość instalacji większej ilości ról niż w przypadku swoich poprzedników. Oprócz tego wprowadza większą liczbę poleceń PowerShell. Nowością jest także możliwość instalacji Microsoft SQL Server 2012 w serwerze w wersji Core, co znaczy, że serwer IIS ma możliwość hostowania aplikacji ASP.NET. Możliwe do zainstalowania role to:

- Active Directory Certificate Services (AD CS)
- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Rights Management Server (AD RMS)
- DHCP Server
- DNS Server
- File and Storage Services
- Hyper-V
- Print and Document Services
- Remote Desktop Services (RDS)
  - Remote Desktop Connection Broker
  - Remote Desktop Licensing
  - Remote Desktop Virtualization Host
- Routing and Remote Access Server (RRAS)
- Web Server
- Windows Server Update Server (WSUS)

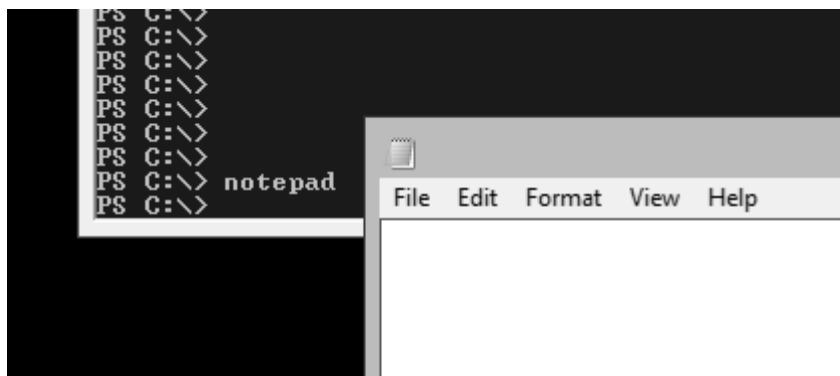
Windows Server 2008 dawał możliwość instalacji następujących ról:

- Active Directory Domain Services (AD DS)
- Active Directory Certificate Services (AD CS)
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP Server

- DNS Server
- File Services
- Print Services
- Streaming Media Services
- Internet Information Services (IIS)
- Hyper-V

### ***1. Nienadzorowana instalacja Active Directory***

Podobnie jak w przypadku trybu graficznego należy wcześniej skonfigurować odpowiednią nazwę komputera oraz adresację IP., aby instalacja przebiegła pomyślnie niezbędny będzie serwer DNS. Wprawdzie Windows Server 2012 wprowadza nowe narzędzie konfiguracji domeny, jednak podejście znane ze starszych wersji Windows Server również się sprawdzi.



Pierwszym krokiem będzie uruchomienie notatnika poleceniem notepad w celu przygotowania pliku konfiguracyjnego dla nienadzorowanej instalacji. To z niego instalator pobierze informacje i w sposób automatyczny przeprowadzi awans serwera do pierwszego kontrolera domeny w nowym lesie.



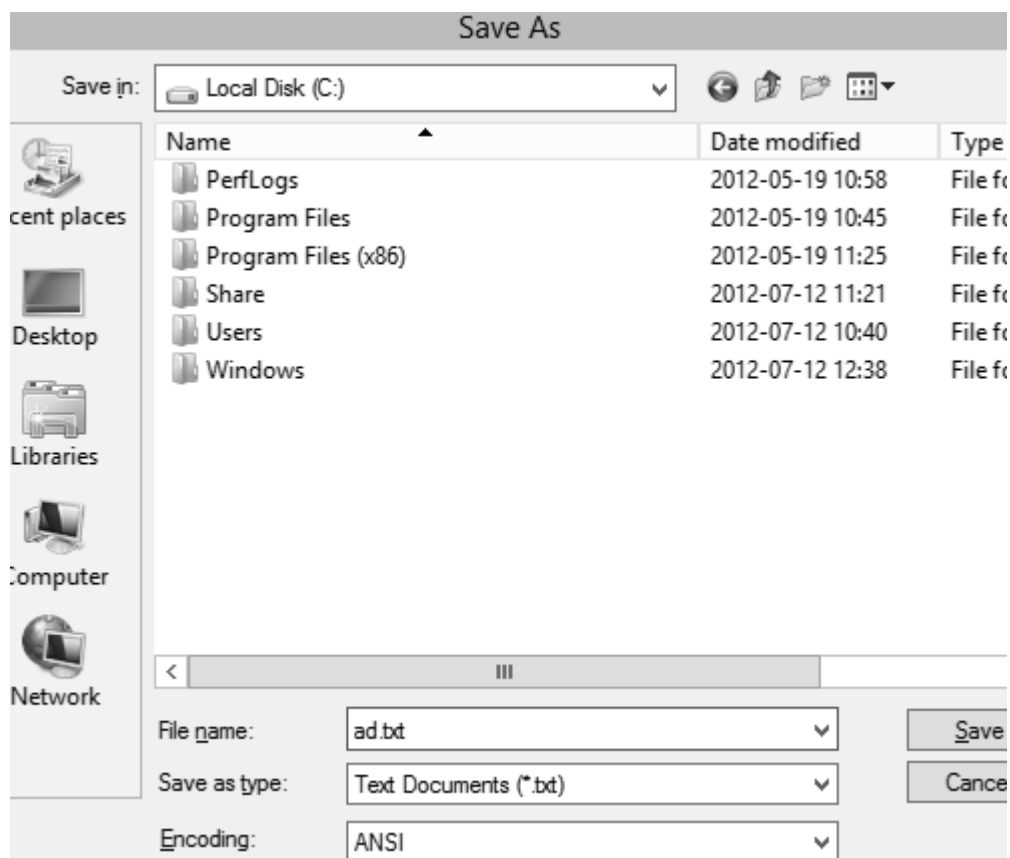
```
uter has at least one physical network  
ess(es) assigned to its IP Properties.  
etw  
h I  
ss<  
le  
  
ion  
can  
th  
is  
th  
  
tor  
eme  
se  
  
ad  
  
[DCINSTALL]  
InstallDNS=yes  
NewDomain=forest  
NewDomainDNSName=elitepc.pl  
DomainNetBiosName=ELITEPC  
SiteName=Default-First-Site-Name  
ReplicaOrNewDomain=domain  
ForestLevel=5  
DomainLevel=5  
DatabasePath="%systemroot%ntds"  
LogPath="%systemroot%ntds"  
RebootOnCompletion=yes  
SYSVOLPath="%systemroot%sysvol"  
SafeModeAdminPassword=Pa$$w0rd
```

Plik tekstowy powinien zaczynać się poleceniem DCINSTALL, które mówi o tym jakiego typu dane się tutaj znajdują. Kolejne wiersze tego pliku to polecenia odpowiadające kolejno za:

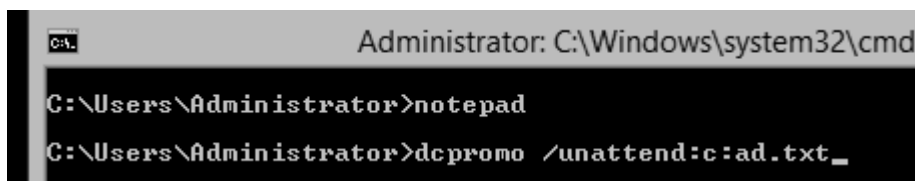
- Określenie czy ma być zainstalowany serwer DNS
- Określenie czy tworzony jest nowy las czy nowa domena
- Określenie DNSowej nazwy domeny
- Określenie netbiosowej nazwy domeny
- Nazwa lokalizacji
- Określenie czy tworzona jest nowa domena czy replika
- Określenie poziomu funkcjonalności lasu (1 – Windows 2000, 2 – Windows 2003, 3 – Windows 2008, 4 - Windows 2008 R2, 5 – Windows 2012)
- Określenie poziomu funkcjonalności domeny
- Lokalizacja bazy danych
- Lokalizacja logów

- Zgoda na zresetowanie komputera po zakończeniu
- Lokalizacja folderu Sysvol
- Hasło administratora trybu przywracania

Tak przygotowany plik należy zachować na dysku C, np. AD.txt.



Kolejnym krokiem jest podanie polecenia *dcpromo /unattend:c:unattend.txt*.



Pojawi się informacja o tym, że *dcpromo* zostało zastąpione przez *ADDSDeployment*, a instalacja zostanie kontynuowana. Niezbędny będzie ponowny rozruch komputera. Gdy to nastąpi Windows Server będzie miał zainstalowaną rolę DNS oraz Active Directory Domain Services.

```
C:\Users\Administrator>notepad
C:\Users\Administrator>dcpromo /unattend:c:\ad.txt
The dcpromo unattended operation is replaced by the ADDSDeployment module for Windows PowerShell. For more information, see http://go.microsoft.com/fwlink/?LinkId=220924
```

Następnym krokiem będzie instalacja serwera DHCP przy użyciu PowerShell. Po uruchomieniu konsoli PowerShell należy wydać polecenie *Add-WindowsFeature DHCP*.

```
C:\Users\Administrator>powershell
Start Installation...
86%
[oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
PS C:\> Add-WindowsFeature DHCP
```

Rola serwera DHCP została zainstalowana. Należy jedynie ją skonfigurować.

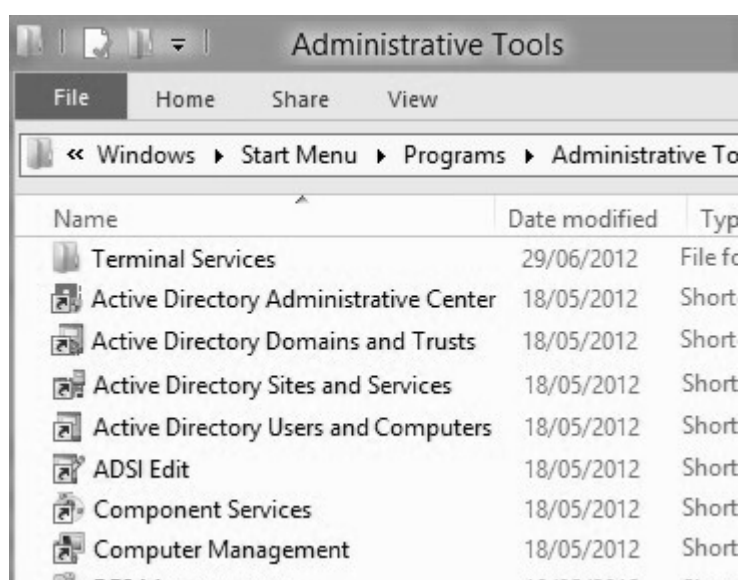
Inną rolę, którą warto zainstalować na serwerze w wersji Core jest Hyper-V. Służy temu polecenie *dism /online /enable-feature /FeatureName:Microsoft-Hyper-V*

```
PS C:\> dism /online /enable-feature /FeatureName:Microsoft-Hyper-V
Deployment Image Servicing and Management tool
Version: 6.2.8400.0
Image Version: 6.2.8400.0
Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Restart Windows to complete this operation.
Do you want to restart the computer now? (Y/N)
```

W analogiczny sposób można zainstalować pozostałe role serwera. Każdą z tych ról można zarządzać na kilka sposobów, ponieważ każda rola posiada szereg poleceń

PowerShell służących do zarządzania nimi. Po więcej informacji w tej materii warto zajrzeć na stronę Microsoft Technet. Innym sposobem zarządzania jest zarządzanie z poziomu Menadżera Serwera na innej maszynie z systemem Windows Server bądź za pomocą dodatku na stacje robocze zwanego *Narzędziami Administracyjnymi Serwera (Remote Server Administration Tools)*.

Pakiet Administration Tools można znaleźć za darmo w Internecie bądź na płycie instalacyjnej Windows Server.



Zawiera on przygotowane konsole, po włączeniu których za pomocą adresu IP nastąpi połączenie się z serwerem. Jest to sposób wygodny i bezpieczny, pozwalający także na zdalne zarządzanie nawet spoza przedsiębiorstwa przy użyciu połączenia VPN.



Jest magistrem inżynierem informatyki, absolwentem Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych. Obecnie doktorant i ćwiczeniowca na powyższej uczelni, a zawodowo trener IT. Jego specjalnością są produkty serwerowe firm Apple oraz Microsoft, a także aplikacje graficzne firmy Adobe. Od 2009 roku redaktor portalu informatycznego [in4.pl](http://in4.pl) oraz własnego bloga [www.wolk.pl](http://www.wolk.pl), na łamach których opublikował kilkadziesiąt artykułów oraz poradników w dziedzinie informatyki. Tworzy także autorskie materiały szkoleniowe, udziela się na portalu [e-biotechnologia.pl](http://e-biotechnologia.pl), a także autor niektórych artykułów dla magazynu iCoder Magazine. Posiada liczne certyfikaty firm Apple i Microsoft, między innymi Apple Certified System Administrator (ACSA), Microsoft Certified System Administrator (MCSA) oraz Microsoft Certified IT Professional (MCITP).

Prowadzę portal IT [in4.pl](http://in4.pl) już od 12 lat. Od kilku współpracuje z autorem niniejszej książki. Podczas naszej wieloletniej współpracy, Krzysztof dał się poznać jako wybitny specjalista i pasjonat w dziedzinie różnych systemów operacyjnych. Zawsze dokładnie zgłębiał te nie łatwe tematy po to aby później w sposób łatwy i przystępny podzielić się zdobytą wiedzą na łamach portalu. Jego artykuły cieszą się u nas dużą popularnością, a jego książka jest naturalnym rozwinięciem jego talentu i pracowitości.

*Sebastian Wiśniewski, Redaktor Naczelny in4.pl*

Niniejszą publikację opiniuję z dużą przyjemnością. Jestem świadom tego, że biorę udział w przygotowaniu publikacji, która ma gwarantowane duże powodzenie u czytelników. Rzadko kiedy spotyka się książki, które w tak doskonałym stopniu balansują wiedzę praktyczną niezbędną do codziennej pracy z teorią wymaganą na egzaminach. Z czystym sumieniem mogę ją polecić jako jedną z najlepszych i najłatwiej przyswajalnych pozycji tego typu.

*Michał Maciej Kasprzak, Microsoft Certified Technology Specialist*

Publikacja stanowi bardzo wartościowe opracowanie szerokiej gamy zagadnień związanych z Windows Server 2012. Recenzowanie tej książki stanowiło dla mnie naprawdę wielką przyjemność, ponieważ sama chciałam zgłębić tajniki nowego systemu w formie takiej kwintesencji. Jestem pewna iż książka ma bardzo duże znaczenie dla rozwoju polskiej branży IT i życzę jej dużego sukcesu. Jest to pozycja godna polecenia nie tylko dla profesjonalistów, ale także dla początkujących, a przede wszystkim dla osób, które pragną szybko zdobyć praktyczne umiejętności.

*Agnieszka Kaczmarek, Microsoft Certified IT Professional*

ISBN 978-83-63548-08-7



9 788363 548087 >



Wydawnictwo  
**PSYCHOSKOK**