

Narzędzia administracyjne. Zdalne zarządzanie stacjami roboczymi.

System Windows, zarówno w wersji klienckiej jak i serwerowej, dostarcza szereg narzędzi do zarządzania i administrowania poszczególnymi opcjami i zachowaniami systemu. Do narzędzi administracyjnych zalicza się m.in. defragmentator dysku, skanowanie powierzchniowe dysku, monitor wydajności, podgląd zdarzeń, zarządzanie komputerem, menedżer zadań czy zasady zabezpieczeń lokalnych. Nie każda wersja systemu będzie zawierać dokładnie te same narzędzia – przykładowo Windows 8.x Pro zawiera dodatkowe zakładki w Zarządzaniu komputerem, takie jak Użytkownicy i grupy, pozwala na dodanie narzędzia Hyper-V (prócz tego musimy posiadać wersję 64bitową; inaczej otrzymujemy jedynie narzędzie do administracji Hyper-V na maszynach zdalnych) oraz pozwala także na Zarządzanie zasadami lokalnymi komputera. Ponadto wersje standardowe Windows nie pozwalają np. na przyłączaniu komputerów do domeny (opcja zarezerwowana dla wersji Professional bądź wyższych).

W przypadku systemów z linii Server opcja Standard nie posiada ograniczonego zasobu narzędzi. W tym konkretnym przypadku systemu w każdej wersji dostajemy niemal te same narzędzia. Różnica polega na „możliwościach” systemu – ilości połączeń pulpitów zdalnych, maksymalnej ilości obsługiwanych rdzeni procesora/procesorów, możliwości łączenia w klastry itp.

Posiadacze klienckich wersji systemu Windows wszelkie narzędzia administracyjne bez problemu odnajdą w Panelu sterowania. Od wersji Vista z mało wiadomych powodów dostęp do nich został ukryty – aby zobaczyć ikonę narzędzi administracyjnych trzeba przestawić opcję Widok według na Małe/Duże ikony (Kategoria nie pokazuje narzędzi w sposób jawny). Innym sposobem jest wpisanie w pole Szukaj frazy „narzędzia administracyjne” bądź wpisać w linii poleceń cmd/PowerShell

control admintools

Poszczególne narzędzia także można wywoływać przy pomocy linii poleceń; niekiedy może to być bardzo użyteczne (klikanie myszą bywa nad wyraz uciążliwe). Pełna lista wszystkich poleceń pozwalających korzystać z poszczególnych narzędzi znajduje się tutaj: <http://spece.it/windows-serwer-artykuly/narzedzia-administracyjne-windows> .

System Windows Server pozwala także na wybieranie narzędzi bezpośrednio z okna Menedżer serwera – wystarczy kliknąć przycisk Narzędzia a wyświetli się lista wszystkich dostępnych narzędzi zainstalowanych w systemie. Proszę pamiętać, że dodawanie nowych ról/składników systemu bądź ich usuwanie bezpośrednio wpływa na ilość dostępnych narzędzi. Przykładowo usługa AD dodaje ok. 7 narzędzi dostępnych w systemie.

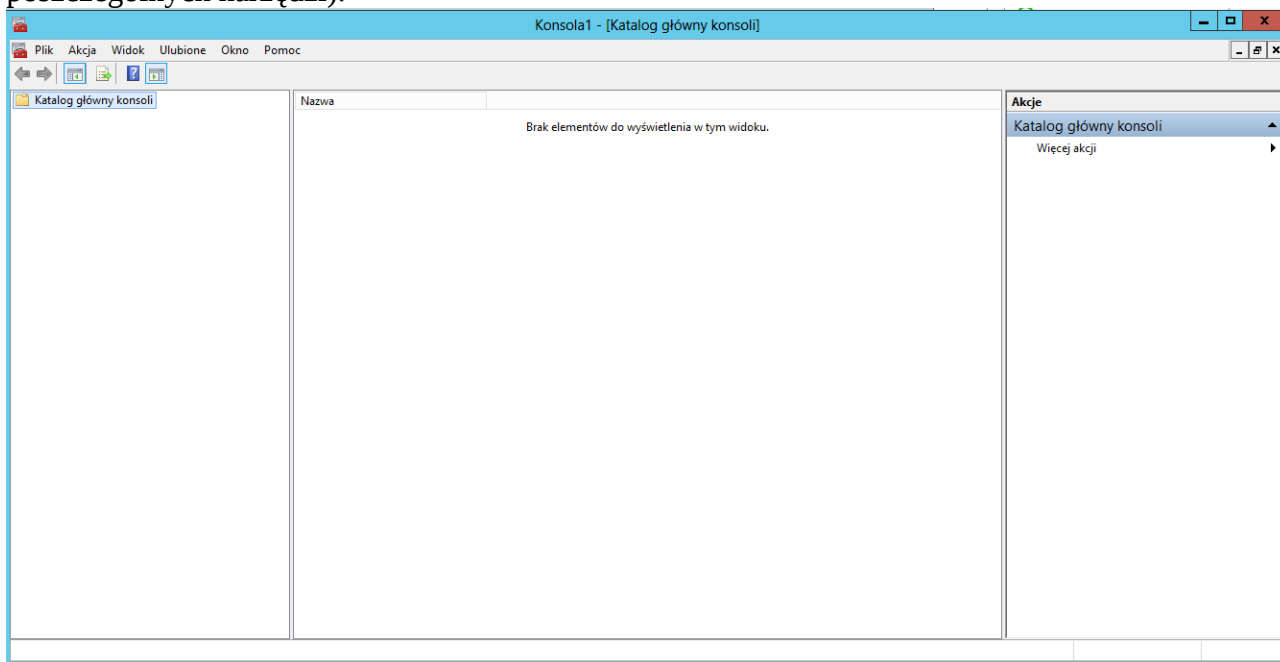
Wszystkie systemy z rodziny NT, w tym systemy klienckie od wersji XP pozwalają także na inny, o wiele wygodniejszy sposób dostępu do narzędzi administracyjnych. Nazywa się Microsoft Management Console – Konsola Zarządzania. W systemie Windows 2012 dołączona jest jej 3, najnowsza wersja. Większość użytkowników korzysta z niej często nawet o tym nie wiedząc – niemal wszystkie narzędzia są jej „dziećmi” - przystawkami (snap-in); przystawka to narzędzie, które nie posiada swojego interfejsu graficznego, a jedynie odpowiednie funkcje. Jako takie nie może istnieć w systemie (brak jej macierzystego okna), którym właśnie staje się MMC. Tak więc MMC to nic innego jak interfejs zbiorczy dla poszczególnych narzędzi administracyjnych. Przykładowo narzędzie Zarządzanie komputerem jest odpowiednio przygotowaną konsolą, do której dodane zostały przystawki Harmonogramu zadań, Użytkowników i grup lokalnych, Zarządzania magazynami danych itd.

Bardzo pożyteczną funkcję opisywanej konsoli stanowi możliwość zapisania jej stanu – tym sposobem administrator może zapisać sobie własny zestaw narzędzi np. na pulpicie. Gdy będzie chciał skorzystać ze swojego zestawu narzędzi nie będzie musiał uruchamiać iluś okien narzędzi (bądź wybierać ich ręcznie) – po prostu kliknie na utworzony skrót i będzie miał dostęp do stworzonej przez siebie konsoli.

W celu uruchomienia konsoli MMC należy wykonać jedną z powyższych czynności:

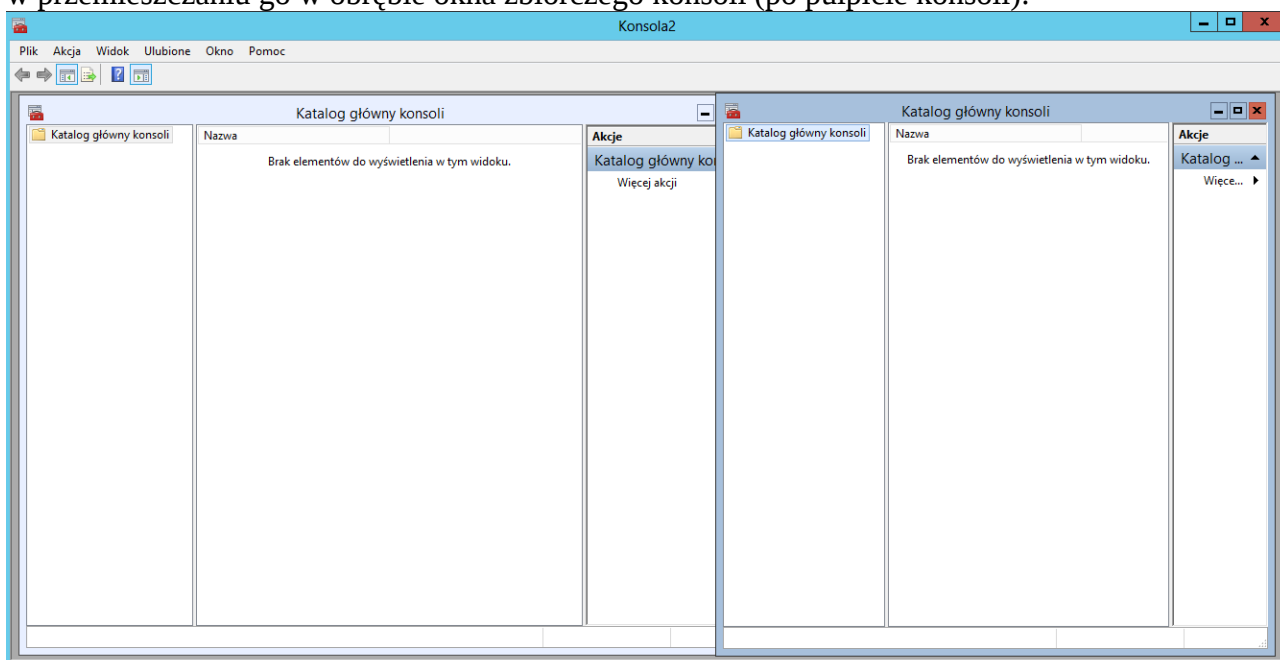
- 1) wcisnąć klawisz [WINDOWS]+F, wpisać frazę mmc i wybrać znaleziony program
- 2) wcisnąć klawisz [WINDOWS]+R wpisać frazę mmc i wcisnąć [ENTER] (bądź przycisk Uruchom)
- 3) w oknie cmd/PowerShell wpisać frazę mmc i zatwierdzić [ENTER]

Okno konsoli na pewno jest bardzo typowe dla większości narzędzi – posiada lewą część (lista narzędzi) część środkową (ustawienia i konfiguracja narzędzia) oraz prawą część (dostępne akcje poszczególnych narzędzi).



Nazwę „Katalog główny konsoli” możemy dowolnie zmieniać.

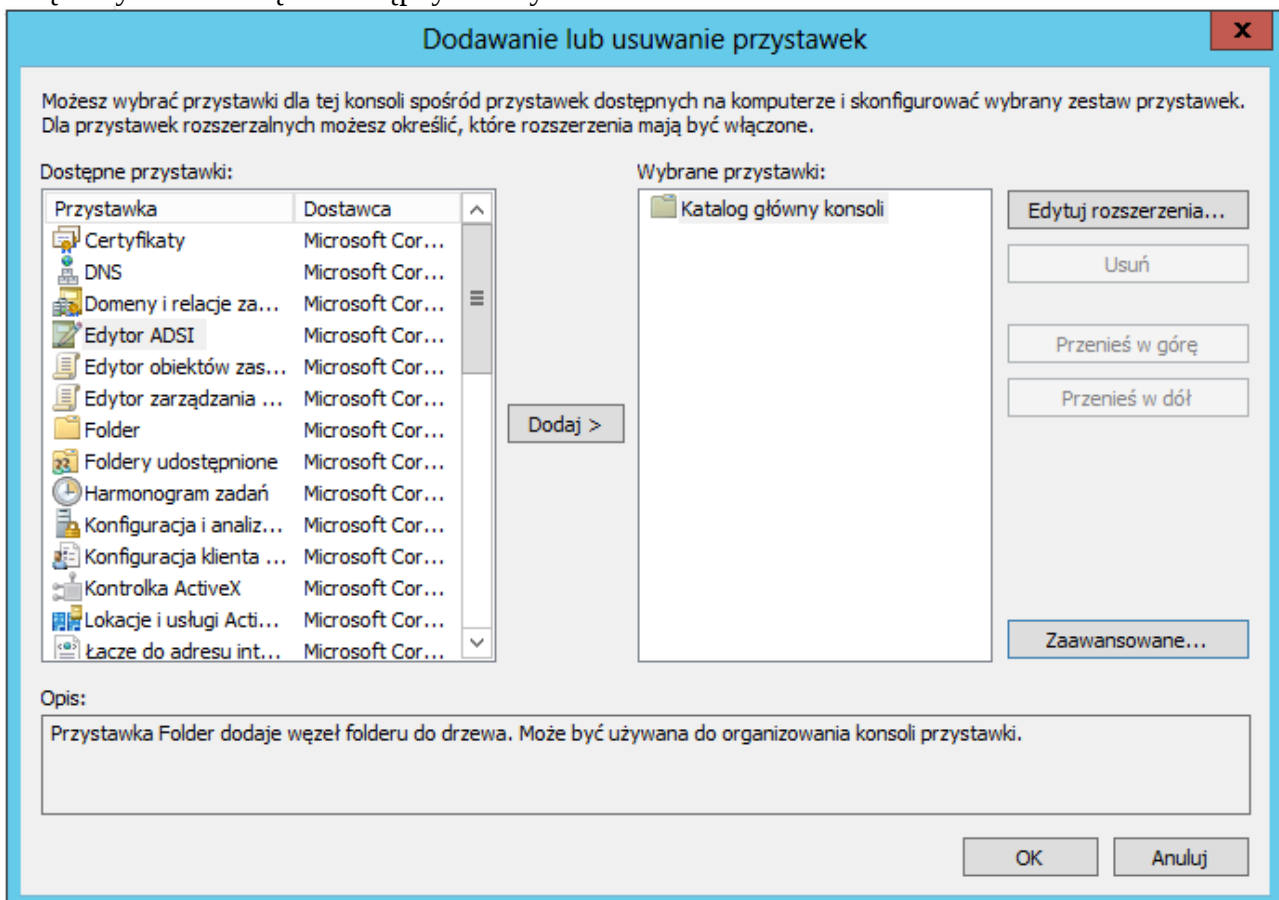
Konsola jako taka jest tylko zbiorem (kontenerem) dla poszczególnych „podkonsol”. W dowolnej chwili możemy Otworzyć nowe okna poprzez polecenie Okno->Nowe okno (lub poprzez [CTRL]+[W]). Każde okno możemy maksymalizować/minimalizować bądź zamykać. Mamy także swobodę w przemieszczaniu go w obrębie okna zbiorczego konsoli (po pulpicie konsoli):



Powyżej widać odpalone narzędzie MMC z dwiema niezależnymi konsolami w ramach jednego

okna.

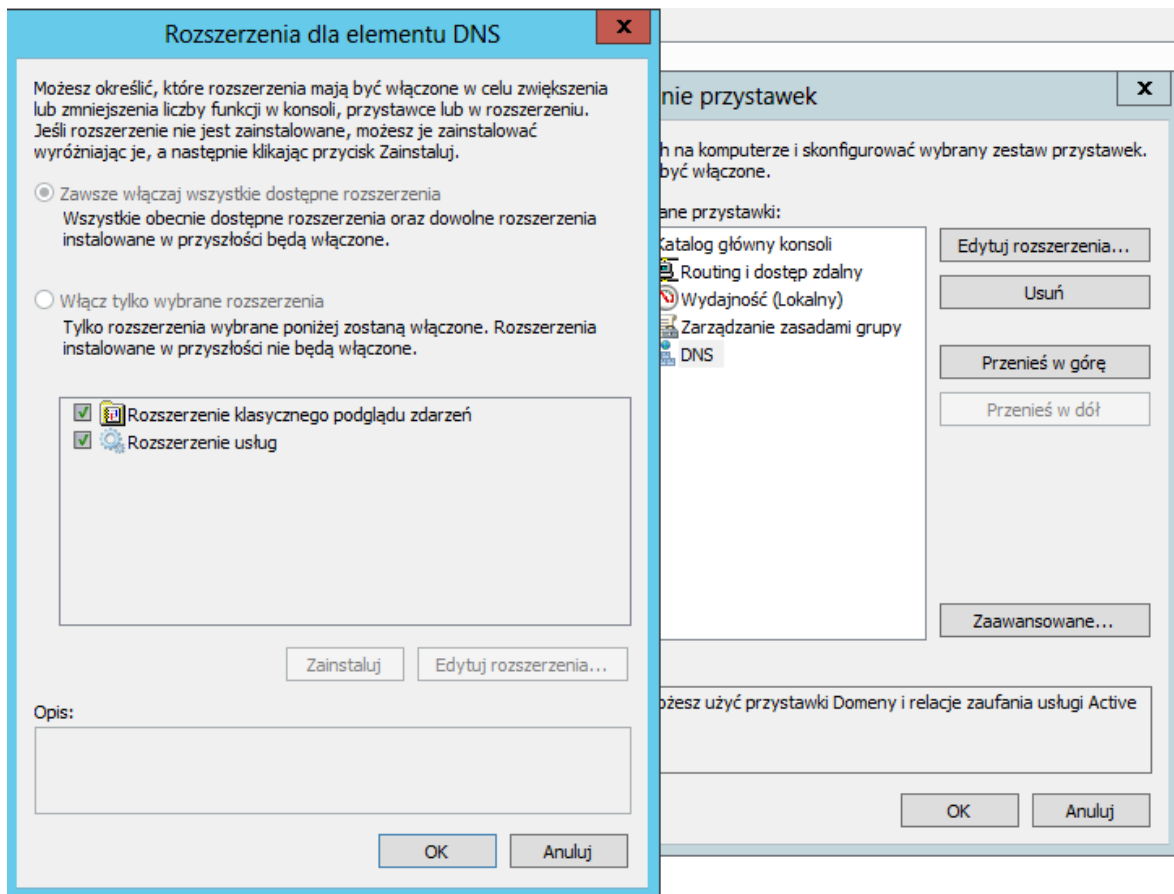
Kolejnym ważnym aspektem (w zasadzie najważniejszym) jest możliwość dodawania/modyfikacji listy dostępnych narzędzi w konsoli. Dokonuje się tego poprzez opcję Plik->Dodaj/usuń przystawkę... (skrót [CTRL]+[M]). Powoduje wywołanie nowego okna dialogowego z dostępną listą wszystkich narzędzi dostępnych w systemie:



Niemal każda dostępna przystawka posiada swój opis oraz graficzną ikonę, która ją reprezentuje. Podany jest także jej dostawca – przystawki mogą być dostarczane przez podmioty trzecie (przykładowo firmy takie jak Adobe, Symantec czy Kaspersky).

Gdy dodamy jakieś przystawki do naszej listy (można klikać dwa razy lewym przyciskiem myszy na wybranej przystawce, można zaznaczyć wybraną przystawkę i kliknąć przycisk Dodaj >) i klikniemy je w liście Wybrane przystawki to niektóre z przycisków zostaną odblokowane.

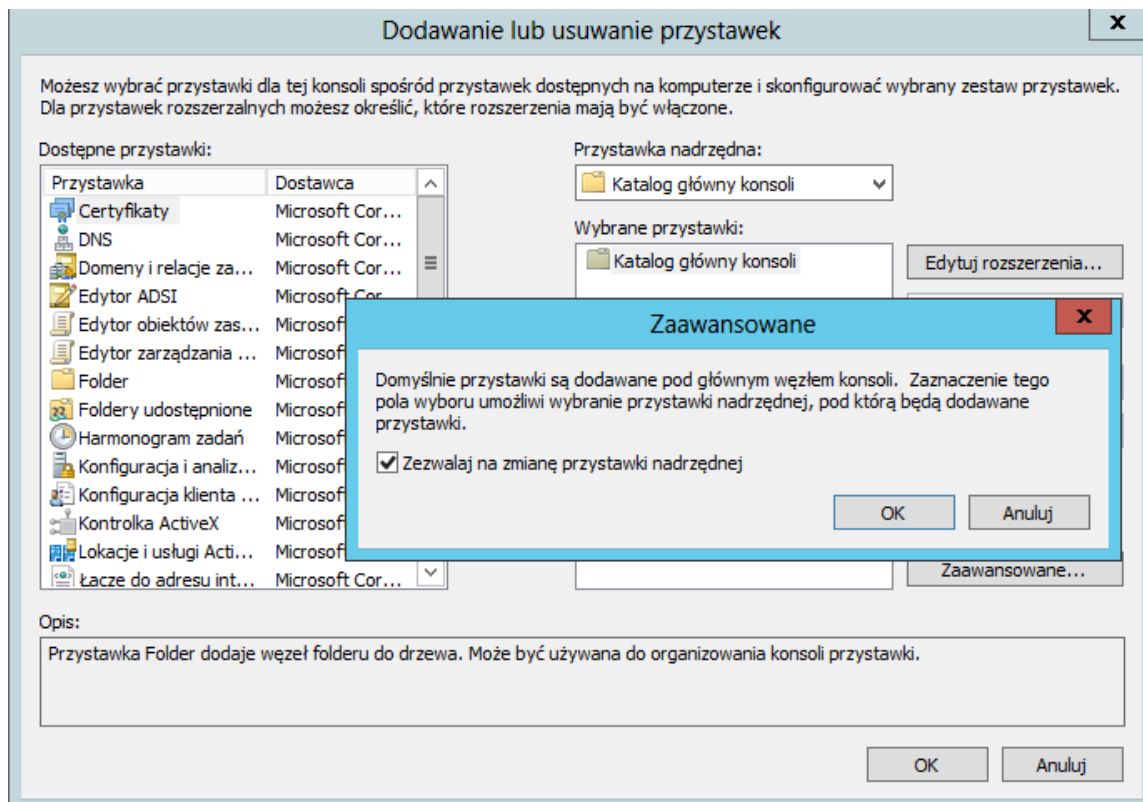
Edytuj rozszerzenia... - przycisk pozwala na włączanie/wyłączanie wskazanych rozszerzeń przystawki. Niektóre przystawki są rozbudowane o dodatkowe moduły. Tworząc swoją konsolę administracyjną możemy rezygnować z poszczególnych modułów i zabraniać dodawania ich do wskazanej przystawki w przyszłości (w ramach tworzonej konsoli, nie samej przystawki jako takiej). Przystawka pokazana na poniższym zrzucie – zarządzanie serwerem DNS posiada dwa dodatkowe moduły. Proszę jednak zauważyć, że jej projektant zabronił nam odłączania od niej jakichkolwiek modułów. Jeżeli nie byłoby nałożonego ograniczenia, można by było wybrać „Włącz tylko wybrane rozszerzenia” po czym istniałaby możliwość odłączenia wskazanych modułów, instalacji nowych (przycisk Zainstaluj) bądź edycji wskazanego rozszerzenia (proszę zwrócić uwagę na to, że rozszerzenie to nic innego jak dodatkowa przystawka, która także może posiadać swoje opcje!). Przykładem przystawki, która umożliwia wyłączenie wskazanego rozszerzenia jest Zarządzanie dyskami



Usuń – usuwa wskazaną przystawkę

Przenieś w górę/Przenieś w dół – pozwala przemieszczać wybraną przystawkę na szczyt/na dół listy z dostępnymi przystawkami. Nie ma innej możliwości na zmianę pozycji przystawek na liście (jedynie skróty klawiaturowe [ALT]+[G] przeniesienie w górę, [ALT]+[N] przeniesienie w dół).

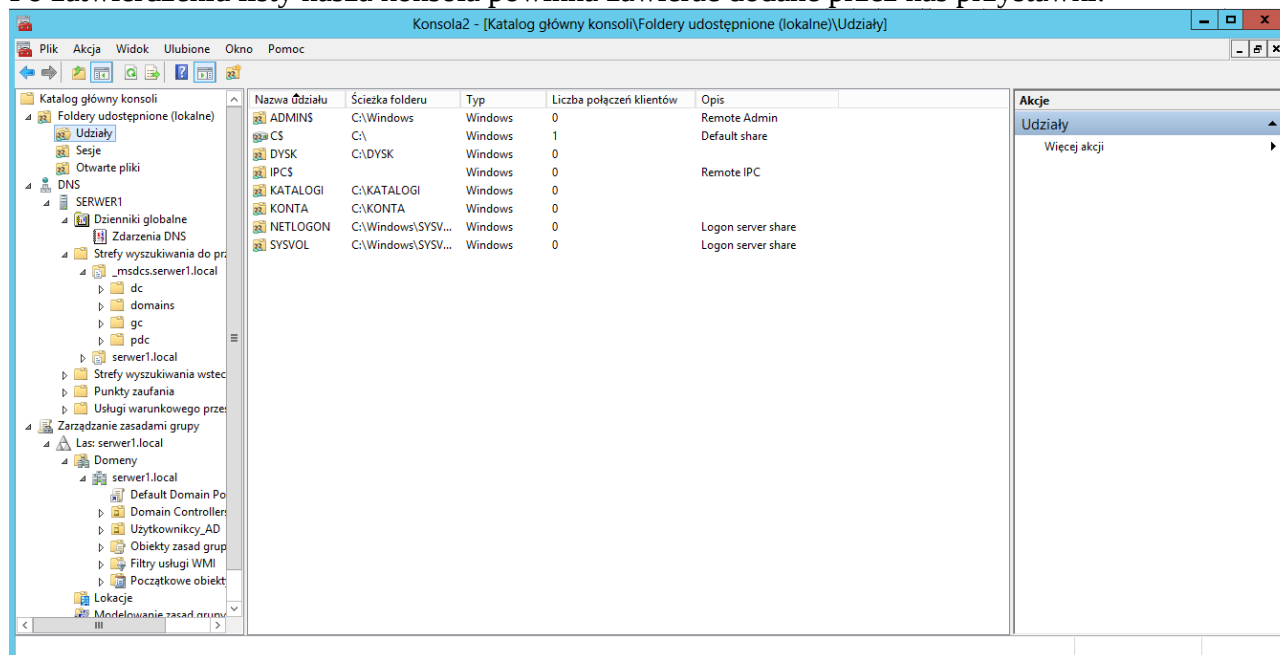
Zaawansowane – przycisk pozwala na zmianę dosłownie jednej, aczkolwiek dosyć pożytecznej opcji. Domyślnie wszystkie przystawki dodawane są do folderu Katalog główny konsoli. Nie ma możliwości na zmianę korzenia dodawania kolejnych przystawek – nawet gdy dodamy z listy po lewej przystawkę Folder (pozwala na gromadzenie dodatkowych przystawek).



Jeżeli zaznaczymy Zezwalaj na zmianę przystawki nadrzędnej (jak na zrzucie powyżej) to system pozwoli nam na wybranie przystawki, która ma być „korzeniem” dla nowo dodawanych przystawek. W oknie dodawania pojawi się nowa, rozwijalna lista „Przystawka nadrzędna” z której to właśnie wybieramy przystawkę-korzeń.

**INFORMACJA:** Tak naprawdę każda przystawka może stać się katalogiem dla kolejnych przystawek – nie musi to być folder. Należy jednak pamiętać, że może to być nieintuicyjne rozwiązanie i należy je stosować jedynie w przypadku, gdy jest nam to niezbędne.

Po zatwierdzeniu listy nasza konsola powinna zawierać dodane przez nas przystawki:

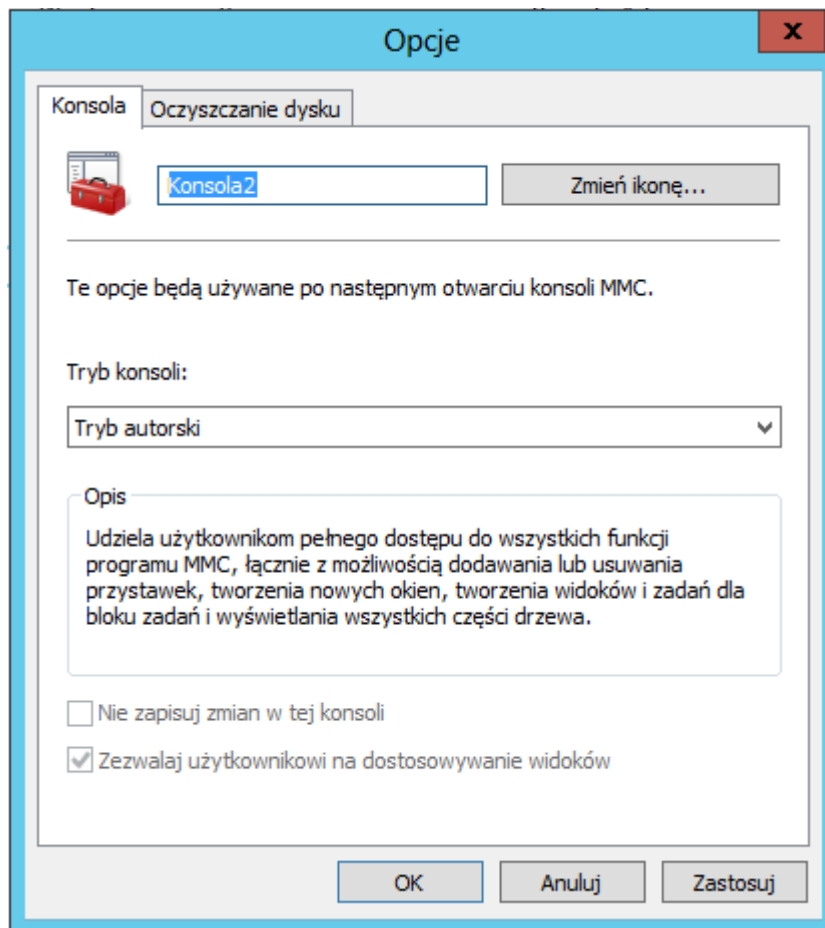


Dodane zostały trzy przystawki – Foldery udostępnione, DNS oraz Zarządzanie zasadami grupy.

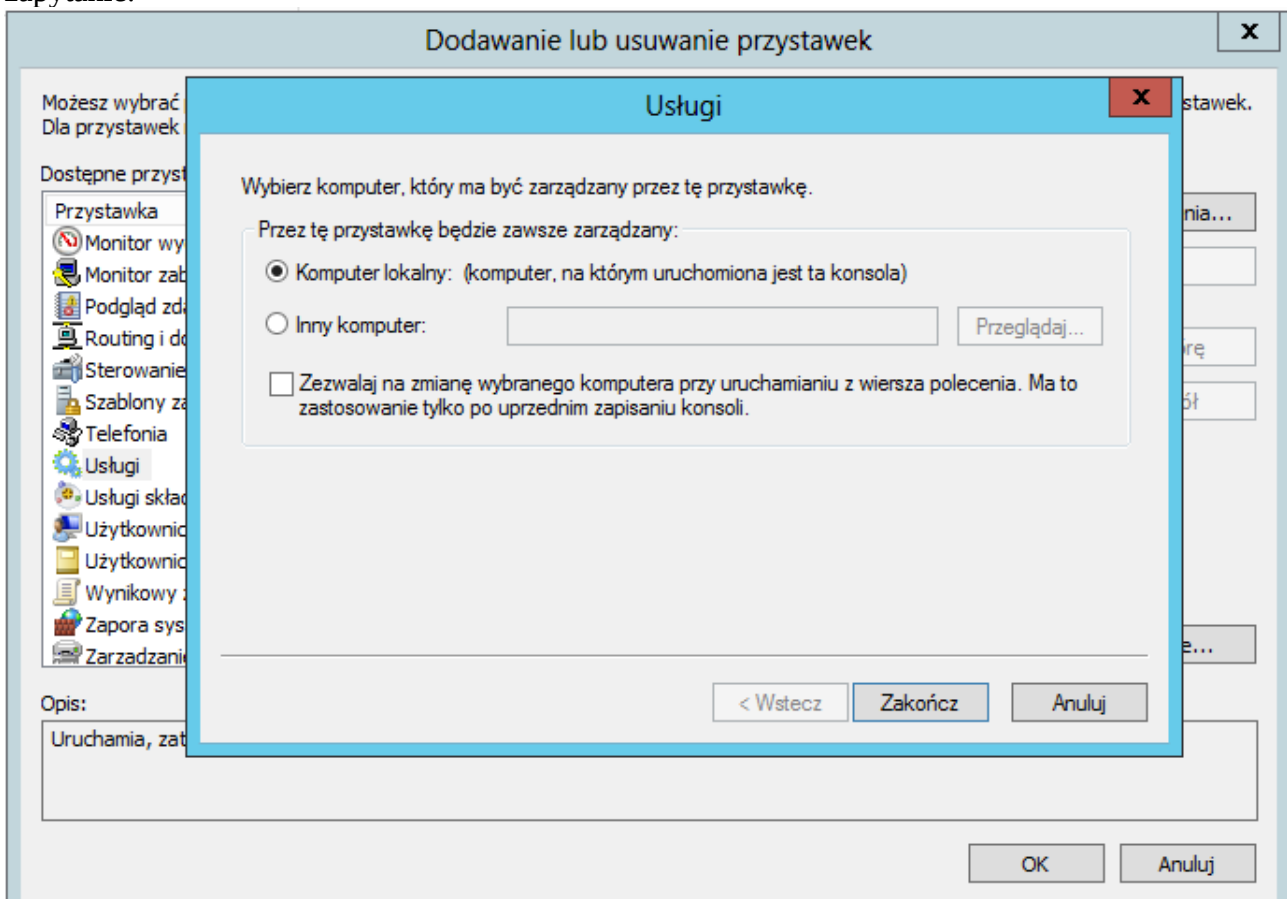
Zanim przejdziemy dalej do użytkowania konsoli, proszę zauważyć iż okno MMC zawiera także menu Widok oraz Ulubione. Poprzez pierwsze menu możemy zmieniać sposób prezentacji wyników. Domyślnie wybrany jest widok Szczegóły, przez co każdy element okna wyświetlany jest w kolejnych wierszach, a jego poszczególne właściwości rozmieszczone są w kolumnach. Zmiana widoku działa tak samo jak w oknie folderów (Eksplorator Windows).

Menu Ulubione pozwala dodać aktualną konsolę do biblioteki konsol. Funkcja przydatna w przypadku, gdy potrzebujemy korzystać z kilku narzędzi jednocześnie i szukamy sposobu na sprawne przełączanie się pomiędzy nimi.

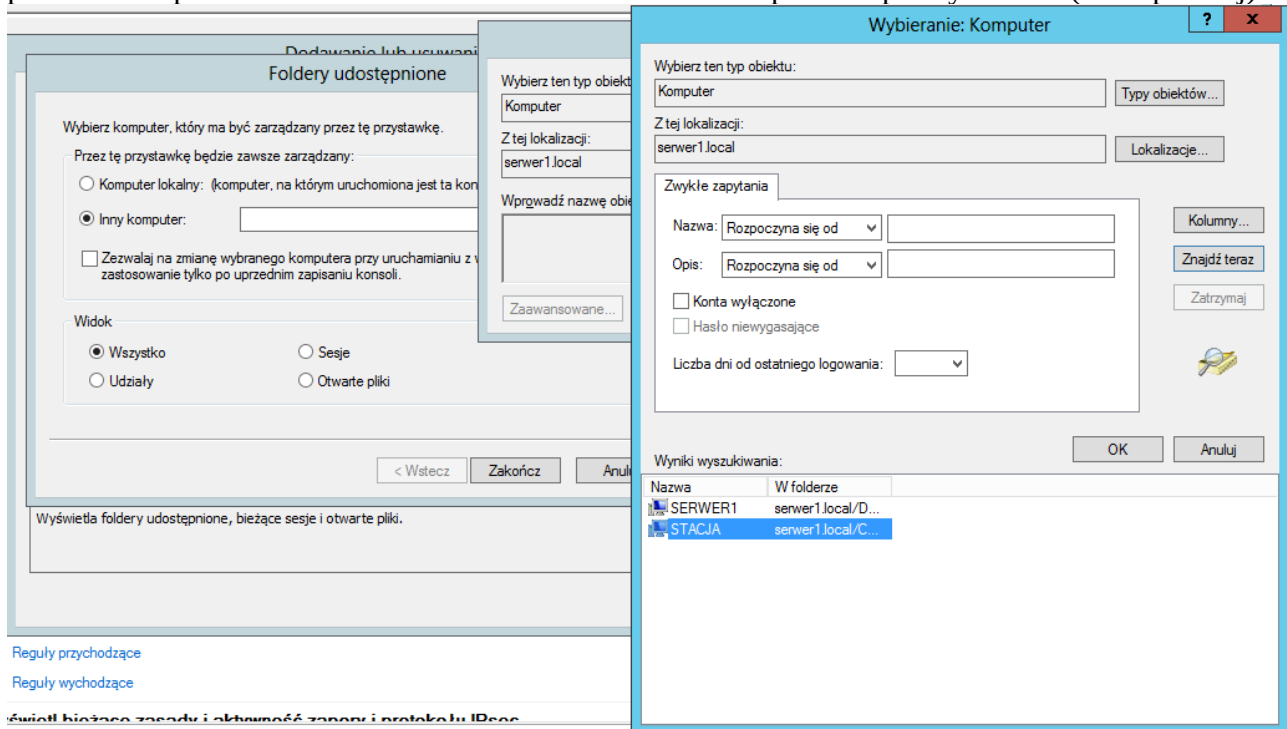
MMC posiada swoje dodatkowe opcje (menu Plik->Opcje...). Pozwalają one na zmianę nazwy projektowanej konsoli, zmianę ikony (po kliknięciu Zmień ikonę... możemy wybrać dowolny symbol graficzny dla naszej konsoli – tak jak w przypadku np. standardowych plików czy skrótów). Tryb konsoli pozwala nam decydować do innej użytkownicy mogą z nią robić (od pełnych praw po jedynie możliwość wyświetlania przygotowanej listy). Zakładka Oczyszczanie dysku pozwala na usunięcie z dysku (naszego profilu) plików tymczasowych konsoli.



Proszę zauważyć, że większość przystawek, które chcemy dodać do konsoli wyświetlają takie oto zapytanie:

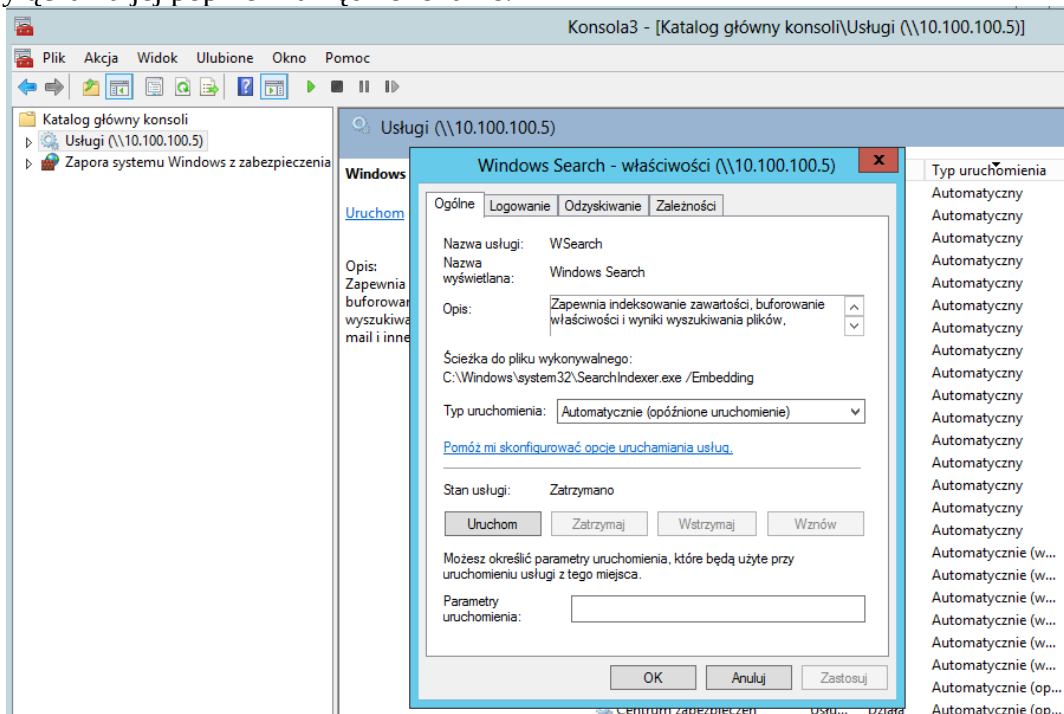


Wybierając Inny komputer możemy przeszukać sieć w celu znalezienia komputera, którego zasobami chcemy zarządzać. Istnieje możliwość podawania nazwy komputera (NETBIOS), można podawać bezpośredni adres IP lub można odszukiwać dostępne komputery w sieci (zrzut poniżej)



Jakkolwiek tego nie dokonamy, od tej chwili będziemy mieli dostęp do ustawień komputera poprzez narzędzie zdalne – zmiany dokonane poprzez narzędzie będą miały skutki na działanie systemu odległego.

W celach demonstracyjnych poprzez przystawkę Usługi spróbujemy wyłączyć jakąś usługę komputera zdalnego (Windows Search – nie ma wpływu na działanie systemu). Najpierw należy się upewnić jaki stan ma usługa na maszynie zdalnej. Włączanie/wyłączanie samej usługi nie różni się od wyłączenia jej poprzez narzędzie lokalne.



**WAŻNE!** Należy pamiętać, funkcja zarządzania zdalnego nie będzie poprawnie funkcjonować z systemami „niższymi” niż Windows serii Professional. Tyczy się to wszystkich wydań Windows od

XP wyłącznie. Reguła nie dotyczy systemów Windows Server!

Dostęp zdalny do serwera/systemów lokalnych

Najpopularniejszym dostępem zdalnym do maszyn z systemem Windows jest usługa pulpitu zdalnego. Dzięki niej użytkownik, jeżeli ma do tego uprawnienia, może zalogować się na swoje konto poprzez dostarczaną w każdym systemie Windows (od XP wzwyż) aplikację Podłączenie pulpitu zdalnego. W przypadku sukcesu użytkownik otrzymuje dostęp do swojego pulpitu, na którym może normalnie pracować.

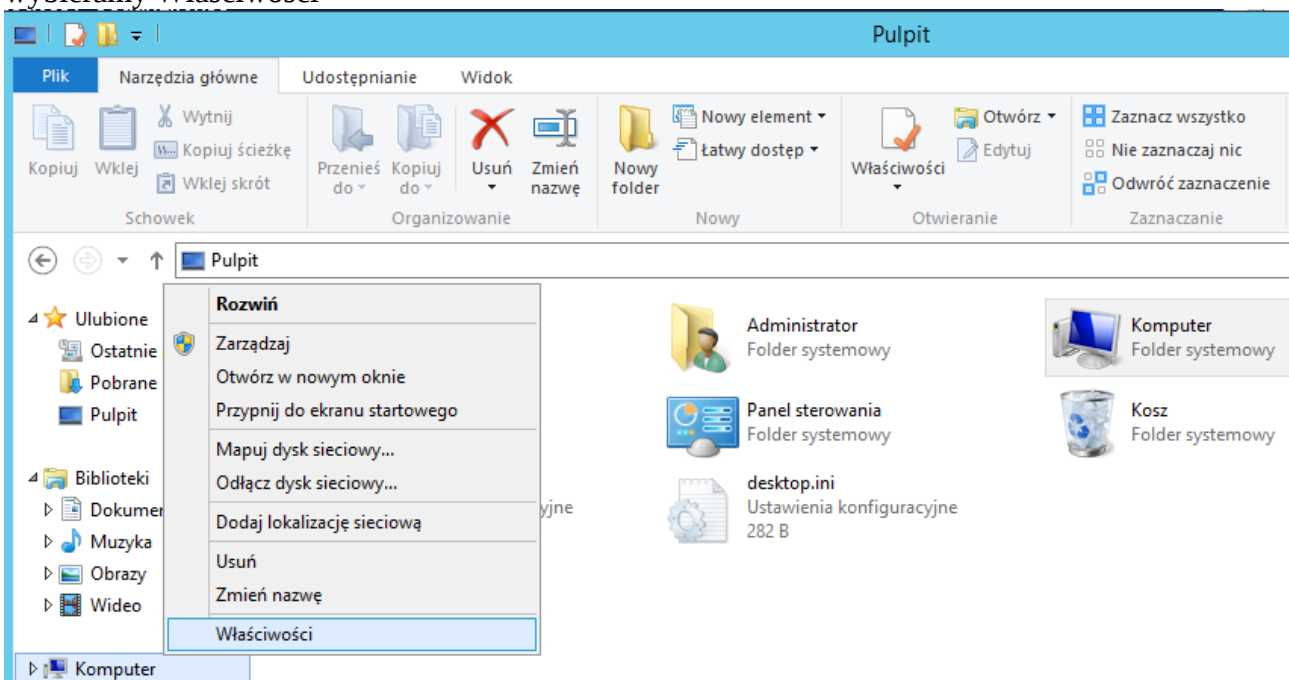
Oczywiście ze względów bezpieczeństwa domyślnie usługa pulpitu zdalnego jest wyłączona. Aby ją włączyć należy:

1) Wpisujemy w cmd/PowerShell polecenie

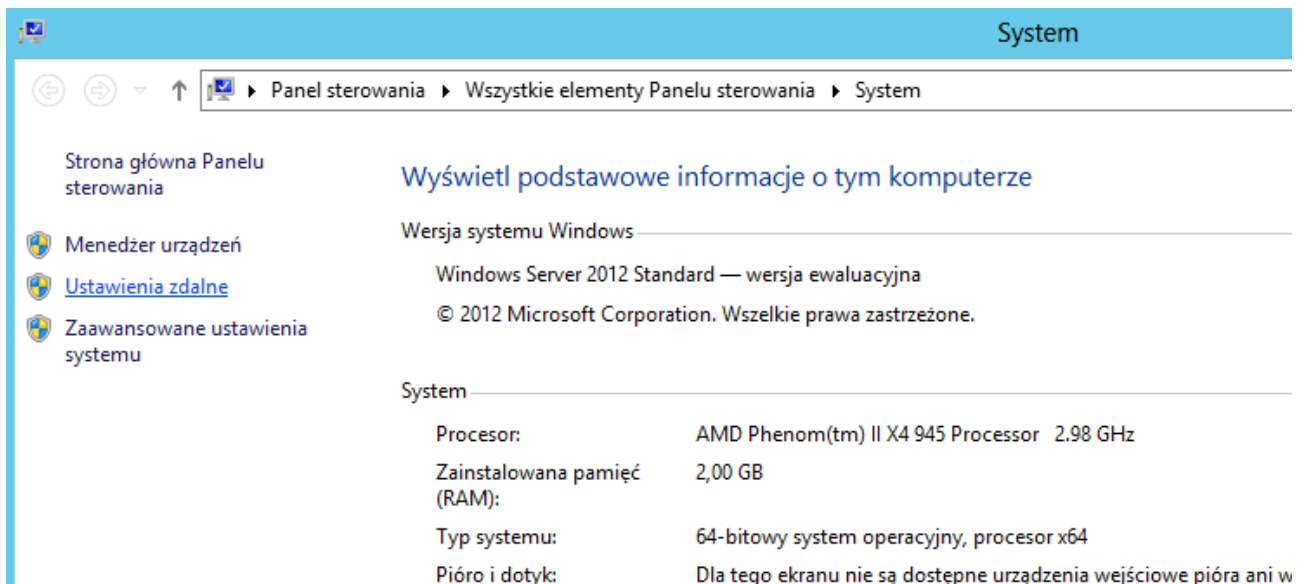
```
sysdm.cpl
```

i przechodzimy na zakładkę Zdalny

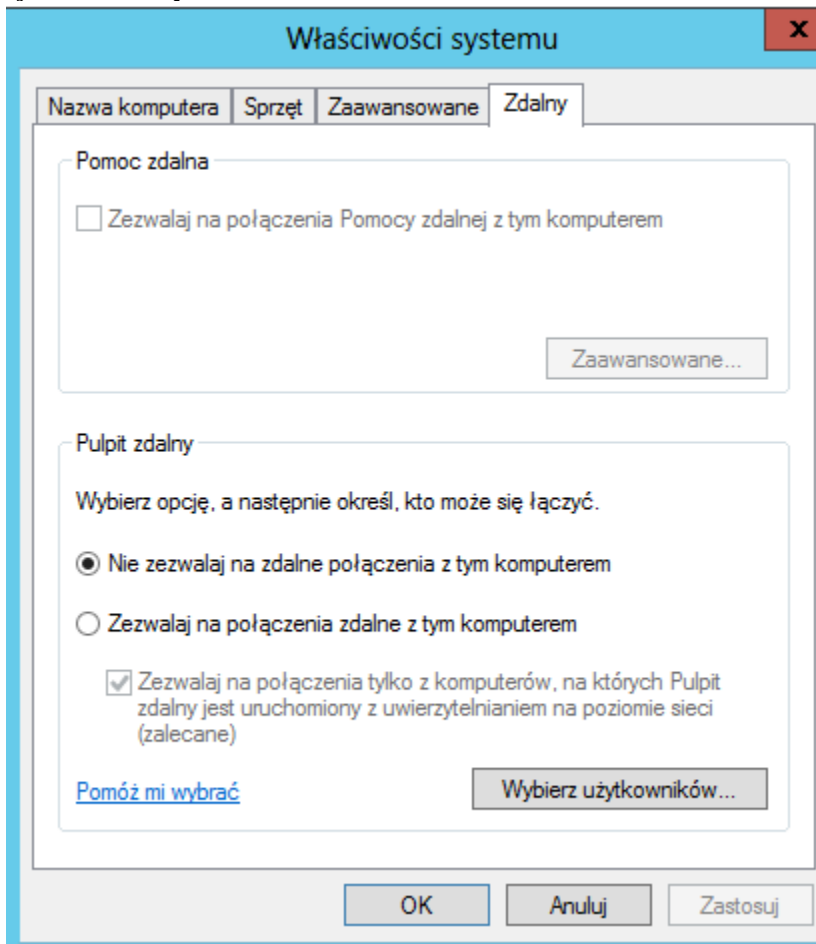
2) Uruchamiamy Eksploratora plików. Klikamy na Komputer prawym przyciskiem myszy i wybieramy Właściwości



W oknie, które się pojawi klikamy na Ustawienia zdalne



Którękolwiek sposobu nie wybierzemy, będziemy dokładnie w tym samym punkcie (oczywiście istnieje także możliwość dotarcia do tego punktu przez Panel sterowania). Na ekranie powinno wyświetlać się takie okno:



Okno to wygląda tak samo jak w Windows 7/8.x Professional bądź wyższych. Pozwala na zarządzanie połączeniami pulpitu zdalnego do tego komputera. Proszę pamiętać, że połączenia wychodzące (serwer także posiada narzędzie Podłączenie pulpitu zdalnego) NIE WYMAGA interwencji na tej karcie.

Na górze okna mamy ustawienia pomocy zdalnej. Funkcja ta jest dostępna w wersjach klienckich systemu Windows i pozwala na „zaproszenie” technika do pomocy z obsługą systemu operacyjnego/naprawienia ustawień systemu operacyjnego. W edycji serwerowej nie jest on potrzebny – mamy pełną implementację protokołu RDP.

Część Pulpit zdalny pozwala na włączanie/wyłączanie zezwolenia na łączenie się z tym systemem

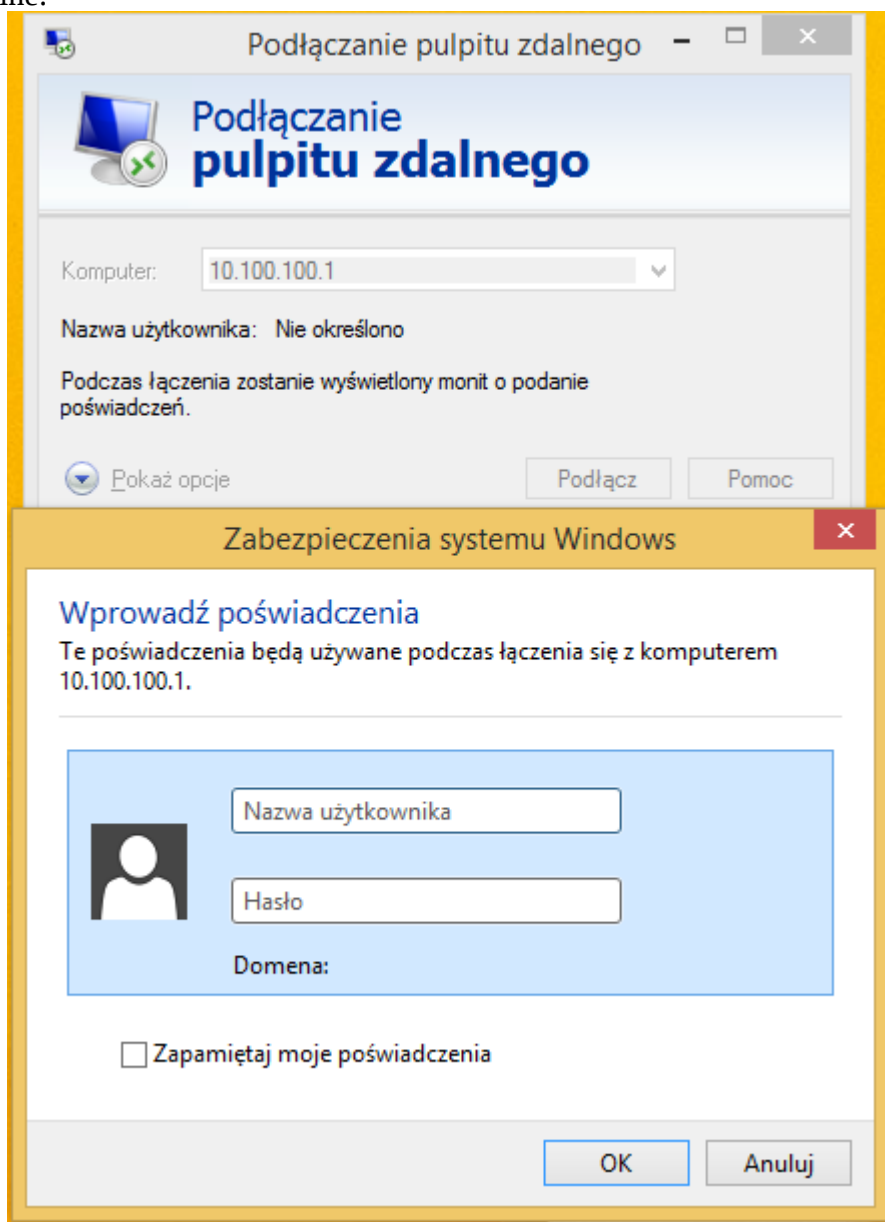
poprzez protokół RDP. Opcja Zezwalaj na połączenia tylko z komputerów, na których Pulpit zdalny jest uruchomiony z uwierzytelnianiem na poziomie sieci (zalecane):

- 1) wymusza na kliencie, który loguje się do systemu włączenie tej opcji w swoim systemie (domyślnie obsługiwana od systemu XP Service Pack 3).
- 2) powoduje, że klient musi zostać najpierw uwierzytelniony (sprawdzenie loginu/hasła), a dopiero po tym następuje proces logowania go do systemu. Pozwala to na lepszą ochronę przed nieautoryzowanym przejściem sesji zdalnej (brak dostępu do niej).

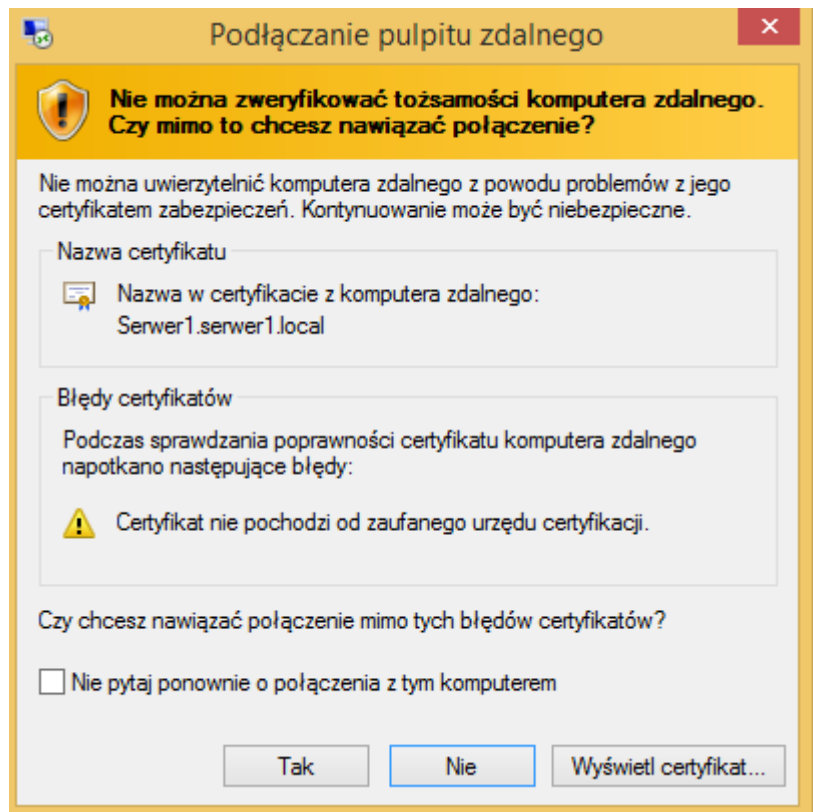
Domyślnie Administrator dodany jest jako użytkownik, który może dokonywać zdalnych połączeń do systemu. Zawsze możemy dodać nowych użytkowników poprzez wybranie przycisku Wybierz użytkowników...

Gdy zaakceptujemy zmiany będziemy mieli możliwość łączenia się z naszym serwerem za pomocą innych komputerów w sieci/internecie (jeżeli nasz serwer posiada zewnętrzny adres IP).

Przykładowo logując się z Windows 8 podajemy adres IP komputera (bądź jego nazwę sieciową jeżeli łączymy się w obrębie sieci LAN) po czym po weryfikacji (Login/hasło) nawiązywane jest połączenie zdalne:

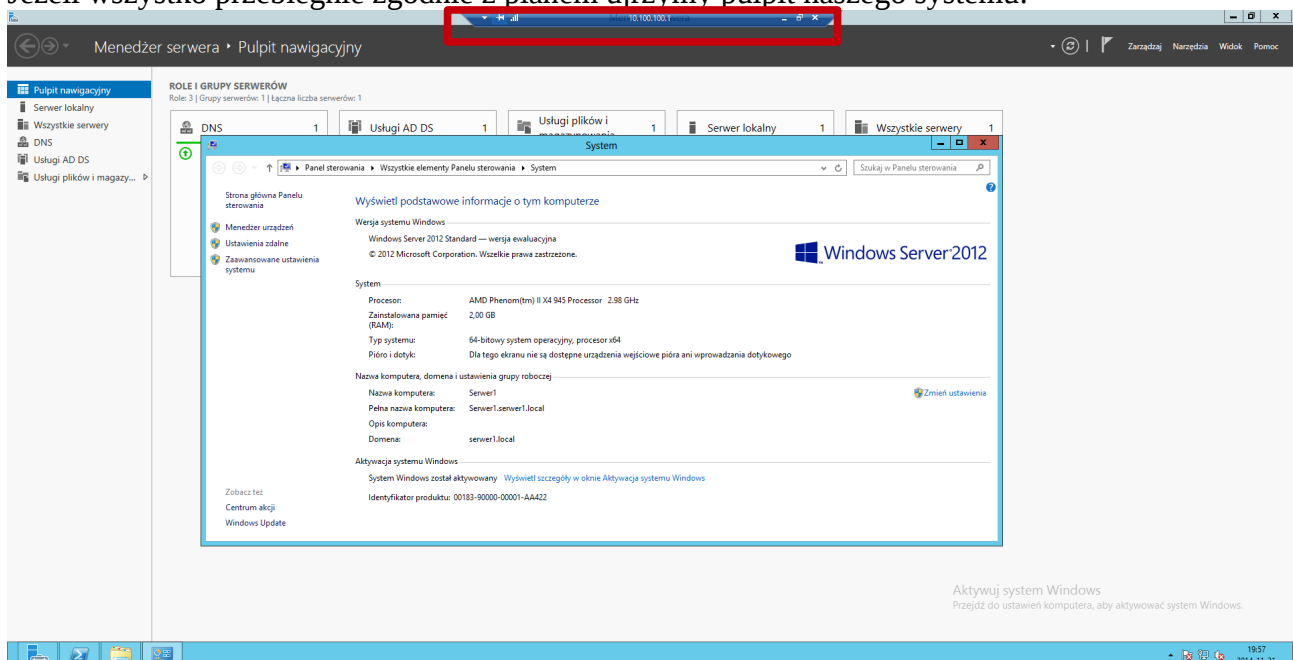


W trakcie logowania narzędzie może się nas zapytać, czy w pełni ufamy komputerowi zdalnemu (kwestia problemu z uwierzytelnieniem certyfikatu). Ponieważ nie podpisywaliśmy certyfikatu cyfrowo (i pewnie nie będziemy bo po co to nam na własny użytek) toteż wystarczy zaakceptować ten komunikat (a można nawet zaznaczyć by więcej się to powiadamienie nie pojawiało).



**OSTRZEŻENIE!** W naszym przypadku oczywiście można to poświadczenie domyślnie akceptować, proszę jednak pamiętać iż przy odległych połączeniach zdalnych NIGDY nie należy tego robić (zawsze trzeba sprawdzić certyfikat). W przeciwnym wypadku napastnicy mogą wykorzystać nasze poświadczenia do przejścia kontroli nad naszym (klienckim) systemem!

Jeżeli wszystko przebiegnie zgodnie z planem ujrzymy pulpit naszego systemu:



Zaznaczony na czerwono fragment świadczy o nawiązanym połączeniu. Oczywiście okno możemy pomniejszyć (ikona minimalizowania w zaznaczonym fragmencie). Pulpit zdalny pozwala na kopiowanie/wklejanie plików, treści i innych danych poprzez takie połączenie (jednak nie działa przeciągnij i upuść).

Aby zakończyć sesję najlepiej jest się wylogować; w przeciwnym wypadku system zawiesi naszą sesję i będzie ona w trybie uśpienia czekać do naszego następnego logowania zdalnego (co

niekoniecznie musi być bezpieczne – zależy od ustawień naszej sieci).

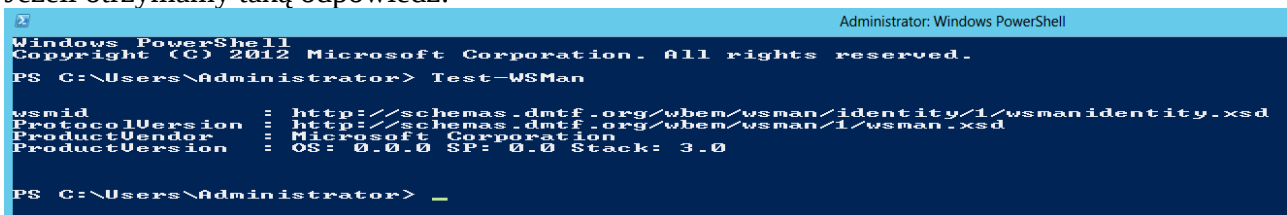
## INNE SPOSOBY POŁĄCZEŃ ZDALNYCH

Od wprowadzenia do systemu nowej generacji konsoli poleceń PowerShell istnieje także możliwość wykonywania połączeń zdalnych w trybie poleceń tekstowych. Tego typu rozwiązanie pozwala przede wszystkim na łączenie się do serwera nawet ze słabego połączenia sieciowego – nie nakłada się dodatkowego obciążenia na połączenie ze względu przesyłania dodatkowych danych dla potrzeb obsługi środowiska graficznego. Innym udogodnieniem tego typu połączenia jest możliwość obsłużenia instalacji serwera Core – serwer ten nie przyjmuje połączeń pulpitu zdalnego.

Domyślnie usługa ta, podobnie zresztą jak usługa pulpitu zdalnego, jest nieaktywna. W przypadku systemów z powłoką graficzną włączenie jej następuje wraz z pulpitem zdalnym. Sprawdzenie czy możemy korzystać z połączenia WinRM można wpisać w PowerShell:

Test-WSMan

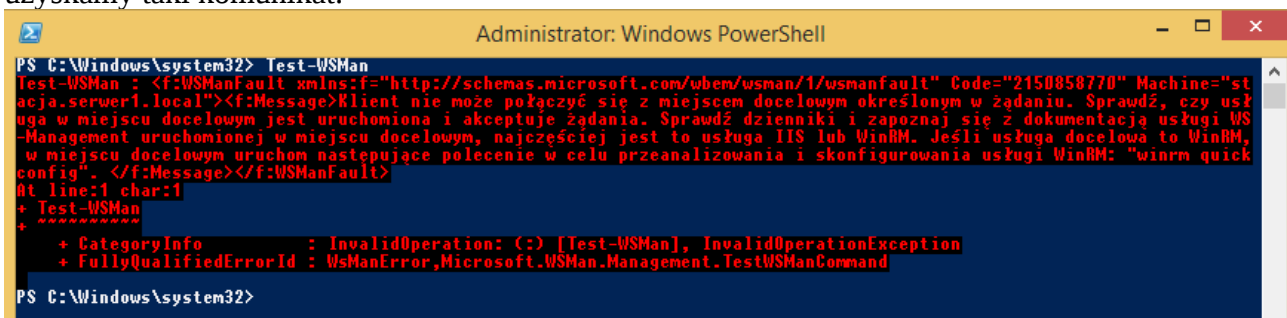
Jeżeli otrzymamy taką odpowiedź:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> Test-WSMan

wsmanid           : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion  : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor    : Microsoft Corporation
ProductVersion   : OS: 0.0.0 SP: 0.0 Stack: 3.0
PS C:\Users\Administrator> _
```

to usługa jest aktywna i nie ma najmniejszego problemu by z niej korzystać. Jeżeli natomiast uzyskamy taki komunikat:



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Test-WSMan
Test-WSMan : <f:WSManFault xmlns:f="http://schemas.microsoft.com/wbem/wsman/1/wsmanfault" Code="2150858770" Machine="st
acja.serwer1.local"><f:Message>Klient nie może połączyć się z miejscem docelowym określonym w żądaniu. Sprawdź, czy usł
uga w miejscu docelowym jest uruchomiona i akceptuje żądania. Sprawdź dzienniki i zapoznaj się z dokumentacją usługi WS
-Management uruchomionej w miejscu docelowym, najczęściej jest to usługa IIS lub WinRM. Jeśli usługa docelowa to WinRM,
 w miejscu docelowym uruchom następujące polecenie w celu przeanalizowania i skonfigurowania usługi WinRM: "winrm quick
config". </f:Message></f:WSManFault>
At line:1 char:1
+ Test-WSMan
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [Test-WSMan], InvalidOperationException
+ FullyQualifiedErrorId : WsManError,Microsoft.WSMan.Management.TestWSManCommand
PS C:\Windows\system32>
```

to znaczy, że usługa nie jest aktywna na wskazanej maszynie i należy ją uruchomić. W tym celu można posłużyć się prostym poleceniem

winrm quickconfig

Polecenie spowoduje uruchomienie szybkiej, automatycznej konfiguracji usługi WinRM. Przykładowy przebieg konfiguracji:

```

PS C:\Windows\system32> winrm quickconfig
Usługa WinRM nie jest skonfigurowana w celu odbierania żądań na tym komputerze.
Konieczne jest wprowadzenie następujących zmian:

Uruchom usługę WinRM.
Ustaw dla usługi WinRM typ opóźnionego automatycznego uruchamiania.
Czy wprowadzić te zmiany [y/n]? y
Usługa WinRM została zaktualizowana w celu odbierania żądań.

Typ usługi WinRM został zmieniony pomyślnie.
Uruchomiono usługę WinRM.
Usługa WinRM nie zezwala na zdalny dostęp do tego komputera w celu zarządzania.
Konieczne jest wprowadzenie następujących zmian:

Aby odbierać żądania do usługi WS-Man kierowane na dowolny adres IP na tym komputerze, utwórz odbiornik usługi WinRM na
HTTP://*.
Włącz wyjątek zapory dla usługi WinRM.
Czy wprowadzić te zmiany [y/n]? y
Usługa WinRM została zaktualizowana na potrzeby zdalnego zarządzania.

Aby odbierać żądania do usługi WS-Man kierowane na dowolny adres IP na tym komputerze, utworzono odbiornik usługi WinRM
na HTTP://*.
Wyjątek zapory dla usługi WinRM został włączony.
PS C:\Windows\system32>

```

Mając już skonfigurowaną usługę możemy spróbować się połączyć do naszego serwera z jakiegokolwiek komputera w sieci dysponującego konsolą PS. Aby rozpocząć połączenie wpisuje się polecenie:

Enter-PSSession -ComputerName <komputer>

np.

Enter-PSSession -ComputerName Serwer1

    bądź adres IP

Enter-PSSession -ComputerName 10.100.100.1

Oczywiście na 99% na naszej aktualnej konfiguracji komputer odmówi jakiegokolwiek połączenia z serwerem twierdząc, że nie znajduje się on na liście zaufanych hostów:

Można oczywiście zaprzętać sobie głowę i szukać rozwiązań jak uruchomić protokół HTTPS (polecenie to winrm quickconfig -transport:HTTPS) albo dodawać ręcznie komputery do listy zaufanych .

Get-Item wsman:\localhost\Client\TrustedHosts

wyświetli aktualnie dodane komputery do listy zaufanych. Poleceniem

Set-Item wsman:\localhost\Client\TrustedHosts -value \*

dodamy potencjalnie każdy wywoływany przez nas adres do listy zaufanych

```
PS C:\Windows\system32> Get-Item WSMAN:\localhost\Client\TrustedHosts

WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Client
Type      Name                               SourceOfValue      Value
----      -
System.String TrustedHosts                       -----
*

PS C:\Windows\system32> Set-Item WSMAN:\localhost\Client\TrustedHosts -Value *_
```

Co do protokołu HTTPS to prawdopodobnie otrzymamy taki oto komunikat:

```
PS C:\Windows\system32> winrm quickconfig -transport:HTTPS
Usługa WinRM jest już uruchomiona na tym komputerze.
WSManFault
Message
ProviderFault
WSManFault
Message = Nie można utworzyć odbiornika usługi WinRM nasłuchującego w protokole HTTPS, ponieważ ten kompu
ter nie ma odpowiedniego certyfikatu. Aby można było używać certyfikatu w protokole SSL, musi on mieć nazwę pospolitą (
CN) odpowiadającą nazwie hosta, musi być odpowiedni do uwierzytelniania serwera, musi być ważny i nie może być odwołany
ani mieć podpisu własnego.

Numer błędu: -2144108267 0x80338115
Nie można utworzyć odbiornika usługi WinRM nasłuchującego w protokole HTTPS, ponieważ ten komputer nie ma odpowiedniego
certyfikatu. Aby można było używać certyfikatu w protokole SSL, musi on mieć nazwę pospolitą (CN) odpowiadającą nazwie h
osta, musi być odpowiedni do uwierzytelniania serwera, musi być ważny i nie może być odwołany ani mieć podpisu własnego.

PS C:\Windows\system32>
```

co w zasadzie zapowiada się na trochę dłuższą zabawę (trzeba utworzyć certyfikat, podpisać go na serwerze po czym należy dodać go do certyfikatów w systemie gościa).

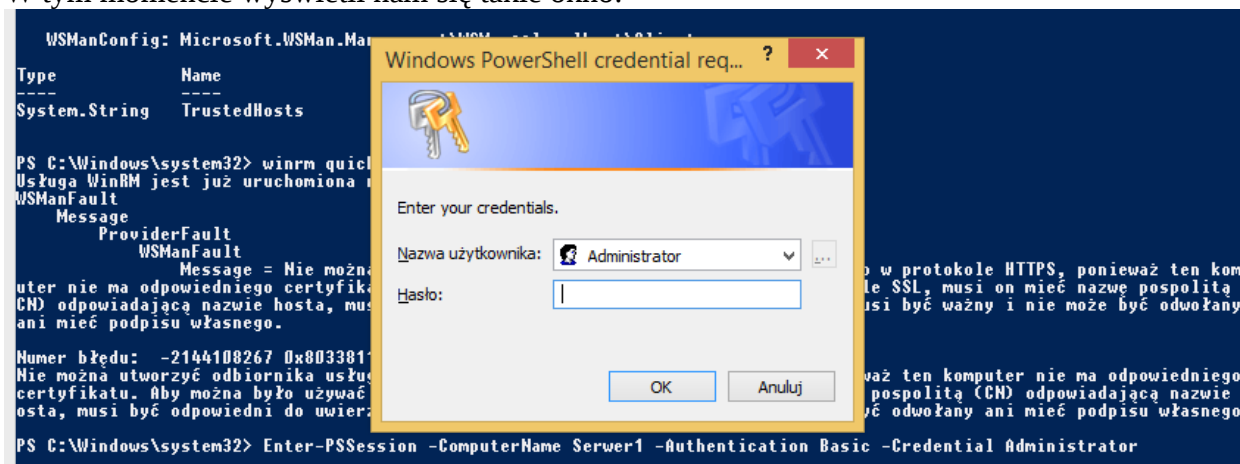
Na szczęście my wiemy, że nikt spoza sieci łączyć się do serwera nie będzie (jedynie np. poprzez IPSec/VPN). Dlatego możemy sobie pozwolić na „uproszczenie” tego logowania. W celu zalogowania się wystarczy użyć polecenia:

Enter-PSSession -ComputerName <komputer> -Authentication Negotiate -Credential <uzytkownik>

np.

Enter-PSSession -ComputerName 10.100.100.1 -Authentication Negotiate -Credential Administrator

W tym momencie wyświetli nam się takie okno:



w którym wystarczy podać swoje hasło. Od tego momentu przed znakiem zachęty będzie wyświetlana nazwa komputera zdalnego. Wykonanie polecenia w tej konsoli będzie równoznaczne z wykonaniem go na komputerze docelowym. Przykład wykonania polecenia ipconfig na komputerze klienckim (górne okno) oraz na komputerze zdalnym (dolne okno):

The image shows two screenshots of Windows PowerShell windows. The top window is titled 'Windows PowerShell' and shows the output of the 'ipconfig.exe' command. It displays configuration for 'Ethernet adapter Ethernet 2' and 'Tunnel adapter isatap. {1B40B3E0-20F5-4651-B0DD-9CC36385A916}:'.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Admin> ipconfig.exe

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3528:562d:f46b:817b%6
    IPv4 Address. . . . . : 10.100.100.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.100.100.1

Tunnel adapter isatap. {1B40B3E0-20F5-4651-B0DD-9CC36385A916}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
PS C:\Users\Admin>
```

The bottom window is titled 'Administrator: Windows PowerShell' and shows the output of the 'ipconfig.exe' command from an administrator perspective. It displays configuration for 'Ethernet adapter Ethernet 2:', 'Ethernet adapter Ethernet:', 'Tunnel adapter isatap.home:', 'Tunnel adapter isatap. {6D73B983-1417-42CC-8AE6-9CFDD9AB2993}:', and 'Tunnel adapter Teredo Tunneling Pseudo-Interface:'.

```
[Serwer1]: PS C:\Users\Administrator\Documents> ipconfig.exe

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::35ef:4fc4:267e:1f03%13
    IPv4 Address. . . . . : 10.100.100.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : home
    Link-local IPv6 Address . . . . . : fe80::e0c4:2b21:5ce0:a5dc%12
    IPv4 Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.2

Tunnel adapter isatap.home:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : home

Tunnel adapter isatap. {6D73B983-1417-42CC-8AE6-9CFDD9AB2993}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
[Serwer1]: PS C:\Users\Administrator\Documents>
```

Aby zakończyć połączenie zdalne należy wywołać polecenie:

Exit-PSSession

Proszę pamiętać, że tego typu połączenie zestawiane jest przez protokół HTTP/HTTPS (usługa IIS) i nie jest jako takie podobne do innych znanych połączeń zdalnych. Każde polecenie jest przesyłane/odbierane poprzez protokół SOAP. Z tego też powodu, gdy chcemy z niego korzystać poprzez sieć rozległą MUSIMY skonfigurować protokół HTTPS – dane w SOAP są przekazywane prostym, otwartym tekstem przez co bez najmniejszego kłopotu mogłyby być podsłuchane poprzez takie programy jak SNORT czy WireShark. Ponadto korzystając z połączenia zdalnego WinRM nie zadziałają nam niektóre „stare” polecenia konsoli poleceń, takie jak chociażby dir czy cd (o type, copy con nie wspominając). Jeżeli faktycznie chcemy uzyskać listę zawartych w aktualnym katalogu plików należy użyć polecenia

Get-ChildItem

W celu przemieszczenia się po katalogach:

Set-Location <sciezka>

Uruchomienie polecenia to oczywiście wpisanie jego nazwy (proszę pamiętać – nie uruchomią się

ŻADNE aplikacje graficzne). Jeżeli natomiast chcemy utworzyć nowy katalog to jak najbardziej zadziała polecenie mkdir. Można też użyć natywnego polecenia PowerShell:

```
New-Item <opcjonalna_sciezka_docelona> <nazwa_katalogu> -type directory
```

np.

```
New-Item C:\katalog -type directory
```

lub

```
New-Item katalog -type directory
```

w drugim przypadku katalog zostanie utworzony w bieżącej lokalizacji.

Podobnie sprawa się ma z tworzeniem plików:

```
New-Item <opcjonalna_sciezka_docelona> <nazwa_pliku> -type file
```

np.

```
New-Item C:\katalog plik.txt -type file
```

Gdy chcemy dodać treść do nowo tworzonych pliku:

```
New-Item C:\katalog plik.txt -type file -value „Treść nowego pliku!”
```

Dodawanie nowej treści do istniejącej już zawartości:

```
Add-Content <nazwa_pliku> „<nowa treść>”
```

Dodanie nastąpi w nowej linii.

Zamazanie poprzedniej treści i dodanie nowej (na początku pliku):

```
Set-Content <nazwa_pliku> „Treść zastępująca poprzednią”
```

Usunięcie pliku/katalogu :

```
Remove-Item <sciezka> <plik/katalog>
```

można również skorzystać z polecenia rm.

Informacja o aktualnie uruchomionym systemie Windows:

```
(Get-WmiObject -Class Win32_OperatingSystem).Caption
```

lub bardziej szczegółowo:

```
Get-WmiObject -Class Win32_OperatingSystem
```

Więcej o usłudze WinRM/WinRS:

<http://wss.geekclub.pl/baza-wiedzy/zdalne-zarzadzanie-za-pomoca-powershella.1397>

<http://msdn.microsoft.com/en-us/library/dd163506.aspx>

<http://clintboessen.blogspot.com/2010/01/what-is-winrm.html>

[http://msdn.microsoft.com/en-us/library/aa384372\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa384372(v=vs.85).aspx)

<http://blogs.technet.com/b/askperf/archive/2010/09/24/an-introduction-to-winrm-basics.aspx>

Polecenie New-PSSession i jego właściwości:

<http://technet.microsoft.com/en-us/library/hh849717.aspx>

Więcej o PowerShell:

[http://www.computerperformance.co.uk/powershell/powershell\\_remote.htm](http://www.computerperformance.co.uk/powershell/powershell_remote.htm)

<http://technet.microsoft.com/en-us/library/ee176914.aspx>

<http://searchwindowserver.techtarget.com/feature/Editing-content-with-Windows-PowerShell>

<http://stackoverflow.com/questions/7330187/how-to-find-windows-version-from-powershell-command-line>

## PODSUMOWANIE

Dzięki przedstawionym metodom administrator może zarządzać dowolnym komputerem w sieci przy pomocy wyżej przedstawionych narzędzi. Z drugiej strony serwer przeważnie stoi w serwerowni (bądź specjalnym, odizolowanym pomieszczeniu) i w celach konserwacji nie chodzi się najczęściej do tego pomieszczenia lecz przeprowadza poszczególne operacje zdalnie. W związku z tym komunikacja tego typu może być dwustronna lub, co jest częściej spotykane, administrator łączy się poprzez usługę zdalną do serwera i z niego dopiero zarządza poszczególnymi stacjami dostępnymi w sieci. Dzięki temu stacje nie muszą być wystawione „na zewnątrz”, a serwer pełni rolę bramy. Oczywiście temat ten jest bardziej rozległy gdyż serwer może być skonfigurowany jako brama, a administrator może mieć dostęp do poszczególnych komputerów pośrednio przez niego lecz nie wymaga się od niego by logował się bezpośrednio na serwer.

Opisane wyżej zadania/polecenia zostały wykonane przy wyłączonej zaporze sieciowej po stronie klienta (Windows 8).

Połączenie pulpitu zdalnego pozwalające na łączenie się do komputera dostępne jest jedynie dla wersji Professional lub wyższych. To samo tyczy się użytkowania narzędzi zdalnych. Oczywiście problem ten można ominąć poprzez stosowanie alternatywnych narzędzi zdalnych (serwer VNC, np. TightVNC) oraz protokół WinRM.

## ZADANIA:

1. Jak zostało wspomniane, komputer kliencki posiadał wyłączoną zaporę sieciową w celu administracji nim przez narzędzia zdalne (konsola MMC). Proszę odnaleźć port, na którym te narzędzia próbują komunikować się z komputerem docelowym, włączyć/dodać odpowiednią regułę i uruchomić zaporę sieciową (bezpieczeństwo!)
2. Na komputerze klienckim należy dodać nowy folder i udostępnić go w sieci. Operacja ma zostać wykonana po stronie serwera.
3. Jak zostało to wspomniane w tekście, narzędzie MMC pozwala na otwarcie kilku okien konsoli. Proszę przetestować jak działa ta funkcja. Czy można dodawać do nich różne narzędzia?
4. Proszę odnaleźć co oznacza opcja „Zezwalaj na zmianę wybranego komputera przy uruchamianiu z wiersza polecenia.”
5. Należy z serwera spróbować zdalnie zarządzać klienckim komputerem. W jaki sposób trzeba zalogować się na komputer podłączony do domeny. Jak dodać na czyjś pulpit plik tekstowy z listą rzeczy, które ma zrobić po zalogowaniu się?
6. Należy sprawdzić czy komputer klienta z uruchomioną usługą logowania zdalnego (RDP) pozwala na korzystanie dwóm jednocześnie zalogowanym użytkownikom. Sprawdzenie należy powtórzyć dla serwera.
7. Sprawdzić czy można zalogować się fizycznie i zdalnie na konto tego samego użytkownika.
8. Sprawdzić czy logowanie się poprzez usługę WinRM nie powoduje zakłóceń w pracy użytkownika zalogowanego do maszyny klienckiej.