Microsoft

Windows Server 2008

Poradnik administratora

Windows Server 2008

Windows Server® 2008

Poradnik administratora

Windows Server 2008

Materiał powstał przy współudziale wykładowców
autoryzowanych ośrodków szkoleniowych Microsoft:

- ABC Data
- Altkom Akademia
- Combidata
- Comp Safe Support

Spis Treści

1. Instalacja i konfiguracja systemu

Microsoft Windows Server 2008 w porównaniu z poprzednimi wersjami sytemu posiada zoptymalizowany i bardzo prosty proces instalacji. Uczestnictwo użytkownika zostało ograniczone do minimum. Instalator systemu wymaga podania tylko najistotniejszych informacji, takich jak miejsce instancji czy edycja systemu, która ma zostać zainstalowana. Pozostałe elementy związane z konfiguracją zostały przeniesione do narzędzia Initial Configuration Tasks Wizard, które jest automatycznie uruchamiane po zakończeniu instalacji i pierwszym zalogowaniu do systemu. Ten ulepszony instalator skraca znacznie czas oraz wysiłek poświęcony na przygotowanie serwera do pracy.

W tabeli poniżej został porównany proces instalacji i wstępnej konfiguracji systemu Windows Server 2008 z systemem Windows Server 2003

Windows Server 2003	Windows Server 2008
Windows Server 2003 Setup Security updates Manage Your Server Configure Your Server Wizard Windows Components Computer Management Security Configuration Wizard	Operating System Setup Initial Configuration Tasks Server Manager

Edycje systemu Microsoft Windows 2008

Podobnie jak wcześniejsze wersje systemu, Microsoft Windows Server 2008 występuje w kilku edycjach, które mają zaspokoić potrzeby różnych klientów. Poniżej zostało przedstawione zestawienie edycji.

Edycja	Opis
Windows Server 2008 Standard Editionx	Edycja systemu Windows Server 2008 zapewnia podstawową funkcjonalność serwera w większości jego ról i zastosowań. Dotyczy to obu opcji instalacji: wersji pełnej i wersji Server Core.
Windows Server 2008 Enterprise Edition	Jest to edycja oparta na Windows Server 2008 Standard Edition, zapewniająca jednak większą skalowalność i dostępność, a także wzbogacona o technologie przeznaczone dla dużych przedsiębiorstw, takie jak klastry i Active Directory Federation Services.

Windows Server 2008 Datacenter Edition	Edycja oferuje takie same funkcje jak Windows Server 2008 Enterprise Edition, a ponadto obsługuje dodatkową pamięć i procesory oraz zapewnia nieograniczone prawa używania obrazu wirtualnego.
Windows Web Server 2008	Edycja ta jest przeznaczona w szczególności do zastosowania jako serwer sieci Web i aplikacji. Inne role serwera i są niedostępne w tej wersji.
Windows Server 2008 dla systemów opartych na procesorze Itanium	Jest to wersja przeznaczona dla komputerów z 64-bitowym procesorem Intel Itanium. Pełni funkcje serwera sieci Web i aplikacji. Inne role i funkcje serwera mogą być niedostępne.

Microsoft Windows Server 2008 pracuje zarówno na 32-bitowej jak i 64-bitowej platformie sprzętowej.

Poniżej zostały przedstawione role serwera, które mogą być instalowane na poszczególnych edycjach Windows Server 2008

Server Role	**Enterprise**	**Datacenter**	**Standard**	**Itanium**	**Web**
Web Services (IIS)	☐	☐	☐	☐	☐
Application Server	☐	☐	☐	☐	
Print Services	☐	☐	☐		
Hyper-V[1]	☐	☐	☐		
Active Directory Domain Services	☐	☐	☐		
Active Directory Lightweight Directory Services	☐	☐	☐		
Active Directory Rights Management Services	☐	☐	☐		
DHCP Server	☐	☐	☐		
DNS Server	☐	☐	☐		
Fax Server	☐	☐	☐		
UDDI Services	☐	☐	☐		
Windows Deployment Services	☐	☐	☐		
Active Directory Certificate Services	☐	☐	☐ [2]		
File Services	☐	☐	☐ [3]		
Network Policy and Access Services	☐	☐	☐ [4]		
Terminal Services	☐	☐	☐ [5]		
Active Directory Federation Services	☐	☐			

Dla klientów, którzy nie potrzebują wirtualizacji firma Microsoft przygotowała edycje Windows Server 2008 Standard, Enterprise oraz Datacenter bez technologi Windows Server 2008 Hyper-V Technology.

Ograniczenie tylko do tworzenia urzędów certyfikatów (Certificate Authorities) bez innych funkcji ADFS (NDES, Online Responder Service).

Ograniczenie do jednego wolno stojącego roota DFS.

Ograniczenie do 250 połączeń RRAS, 50 połączeń IAS i 2 IAS Server Groups.

Ograniczenie do 250 połączeń Terminal Services Gateway.

Scenariusze aktualizacji

Niniejszy rozdział opisuje czystą instalację systemu Windows 2008 nie zajmując się możliwością aktualizacji z wcześniejszych wersji systemu, niemniej jednak w tabeli poniżej zostały podane możliwe uaktualnienia, aby ułatwić potencjalnym nabywcom decyzję, co do zakupu produktu.

Posiadana wersja	Do jakiej wersji można wykonać aktualizację
Windows Server 2003 R2 Standard Edition Windows Server 2003 Standard Edition z Service Pack 1 (SP1) Windows Server 2003 Standard Edition z Service Pack 2 (SP2) Windows Server 2008 Standard RC0	Pełna instalacja systemu Windows Server 2008 Standard Pełna instalacja systemu Windows Server 2008 Enterprise
Windows Server 2003 R2 Enterprise Edition Windows Server 2003 Enterprise Edition z Service Pack 1 (SP1) Windows Server 2003 Enterprise Edition z Service Pack 2 (SP2) Windows Server 2008 Enterprise RC0	Pełna instalacja systemu Windows Server 2008 Enterprise
Windows Server 2003 R2 Datacenter Edition Windows Server 2003 Datacenter Edition z Service Pack 1 (SP1) Windows Server 2003 Datacenter Edition z Service Pack 2 (SP2) Windows Server 2008 Datacenter RC0	Pełna instalacja systemu Windows Server 2008 Datacenter

Aktualizacja wersji 32-bitowej na 64-bitową i odwrotnie nie jest wspierana.

Nie możliwości aktualizacji poprzednich wersji systemu do instalacji Server Core. Nie ma również możliwości aktualizacji pełnej instalacji Windows Server 2008 do instalacji Server Core.

Podobnie jest zresztą z instancją Server Core nie może być ona uaktualniana do pełnej wersji Windows Server 2008.

Wymagania instalacyjne

Poniżej zostały podane wymagania, które musi spełniać sprzęt, aby była możliwa instancja i praca z Windows Server 2008

Procesor:
Minimum: 1 GHz (dla x86) lub 1.4 GHz (dla x64) dla pełnej wersji systemu
Rekomendowane: 2 GHz lub szybszy
Optymalne: 3 GHz lub szybszy

Pamięć:
Minimum: 512 MB zarówno dla wersji pełnej jak i Server Core
Rekomendowane: 1 GB lub więcej dla wersji pełnej
Optymalne: 2 GB lub więcej dla wersji pełnej systemu i 1GB lub więcej dla Server core
Maksimum (dla 32-bit systemów): 4 GB dla Windows Server 2008 Standard, 64 GB dla Windows Server 2008 Enterprise lub Windows Server 2008 Datacenter
Maksimum (dla 64-bit systemów): 32 GB dla Windows Server 2008 Standard, 2 TB dla Windows Server 2008 Enterprise, Windows Server 2008 Datacenter, lub Windows Server 2008 for Itanium-Based Systems

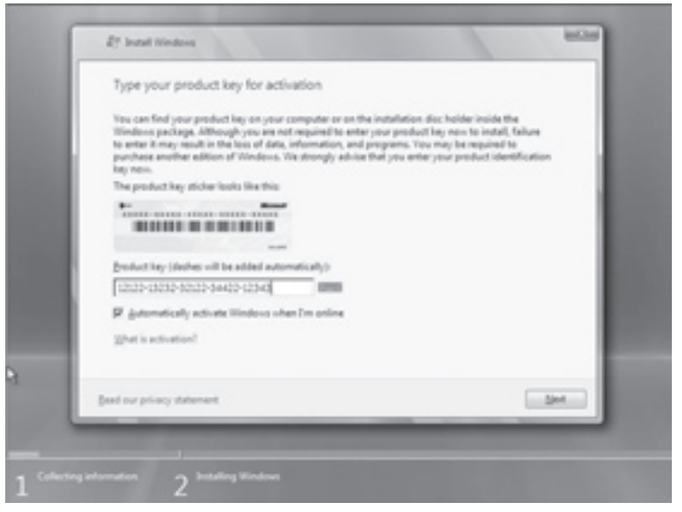
Dysk:
Minimum: 8 GB dla wersji pełnej jak i Server Core
Rekomendowane: 40 GB dla wersji pełnej systemu, 8 GB dla Server Core
Optymalne: 80 GB dla pełnej wersji systemu, 40 GB dla Server Core

Komputery posiadające więcej niż 16 GB RAM potrzebują więcej miejsca na dysku na pliki stronicowania, hibernację, czy zrzut pamięci.

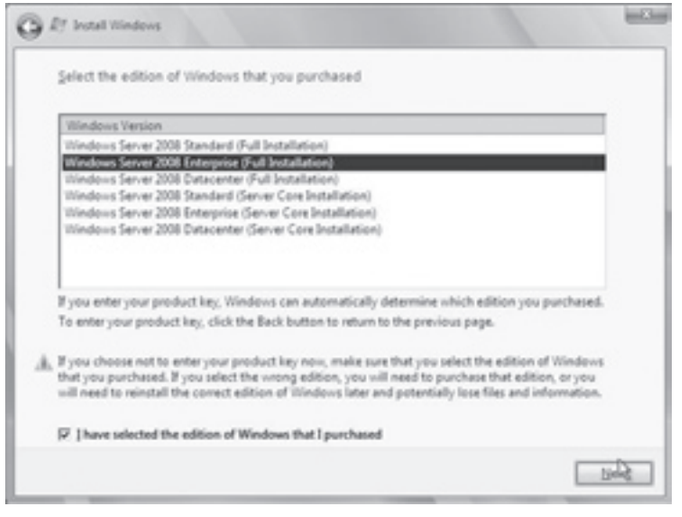
Proces instalacji i wstępnej konfiguracji pełnej wersji Windows Server 2008

Proces instalacji Windows Server 2008 został bardzo uproszczony i jest identyczny z instalacją Windows Vista. Po włożeniu płyty instalacyjnej do napędu, pojawia się pierwsze okno instalatora, w którym można wybrać ustawienia języka, czasu i układu klawiatury.

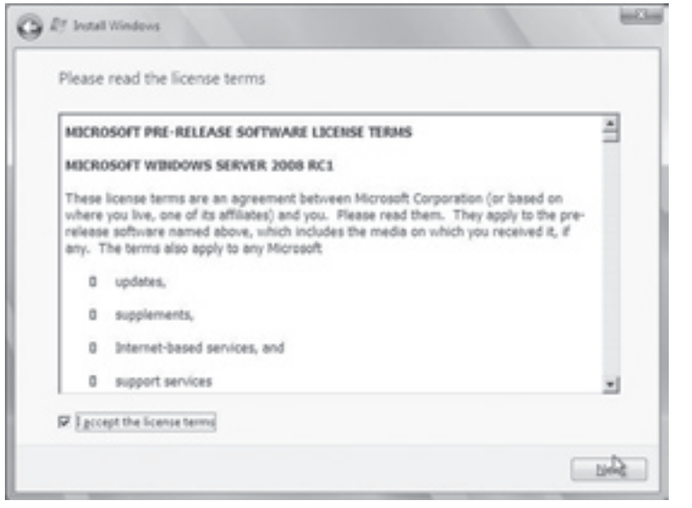
Instalator systemu Windows 2008 będzie potrzebował jeszcze kilku podstawowych informacji, podanych w początkowe fazie procesu. Między innymi jest to klucz produktu. W tym momencie można również zaznaczyć aktywację systemu, jeśli komputer ma możliwość połączenia z Internetem. Nowością jest możliwość zainstalowania bez podawania klucza produktu w czasie instalacji.



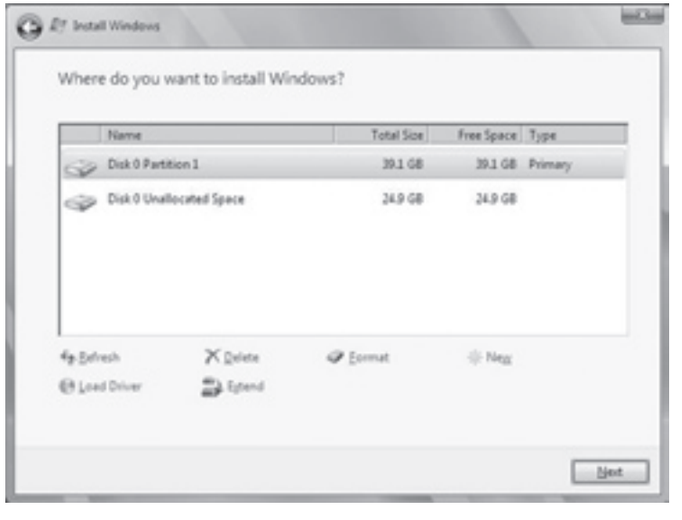
Poniższy ekran wygląda różnie w zależności od tego czy został wprowadzony klucz produktu czy nie. Jeśli klucz produktu został podany jest wybierana odpowiednia edycja systemu do instalacji, w przeciwnym razie można wybrać edycję systemu do instalacji.



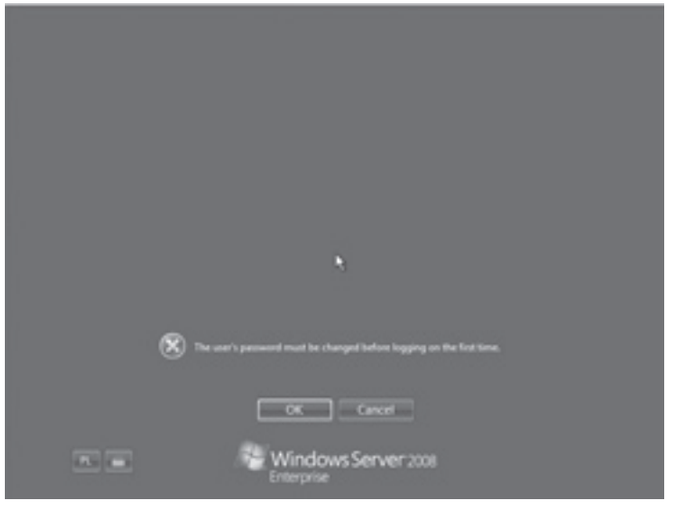
Kolejny krok instalatora to umowa licencyjna, którą należy zaakceptować.



Ostatnie informacje wymagane przez instalator to konfiguracja partycji, na której system zostanie zainstalowany. Oprócz możliwości stworzenia nowej partycji, skasowania, sformatowania lub rozszerzenia można również podać sterowniki potrzebne do prawidłowej instalacji. Nowością jest możliwość dodania sterowników z dowolnego napędu: CD, DVD, lub USB.



Po podaniu wymaganych informacji system już instaluje się dalej automatycznie. Instalator systemu Windows Server 2008 wykona automatycznie wszystkie wymagane restarty, a następnie nastąpi pierwsze uruchomienie systemu. Domyślnie hasło administratora pozostaje puste, trzeba je ustawić w czasie pierwszego uruchomienia systemu.



Proces instalacji Windows Server 2008 przebiega szybko i sprawnie a osoba instalująca nie musi stale kontrolować instalacji i wprowadzać informacji wymaganych przez instalator systemu. Ponieważ ilość informacji wprowadzanych w czasie pracy instalatora została ograniczona do minimum pewne parametry przyjmują domyślne wartości początkowe. Poniższa tabela pokazuje niektóre ustawienia domyślne instalacji Windows Server 2008.

Ustawienie	**Domyślna konfiguracja**
Hasło administratora	Domyślnie hasło konta administratora jest puste.
Nazwa komputera	Podczas instalacji nadawana jest losowa nazwa komputera.
Członkostwo w domenie	Domyślnie komputer nie jest wpięty do domeny; znajduję się grupie roboczej o nazwie WORKGROUP.
Usługa Windows Update	Usługa Windows Update jest domyślnie wyłączona.
Połączenia sieciowe	Adresy IP pobierane są z serwera DHCP.
Zapora systemu Windows	Zapora systemu Windows jest domyślnie włączona.
Zainstalowane role	Domyślnie nie są zainstalowane żadne role ani funkcje.

Po uruchomieniu systemu, zmianie hasła administratora i pierwszym zalogowaniu automatycznie pojawi się okno Initial Configuration Tasks. Narzędzie Initial Configuration Tasks jest wykorzystywane w celu szybkiego skonfigurowania ustawień serwera przede wszystkim domyślnej konfiguracji poinstalacyjnej. Pozwala ono ustawić strefę czasową, przypisać stały adres IP, zmienić nazwę komputera i jego członkostwo w domenie, oraz ustawienie pobierania poprawek systemowych i konfigurację zapory sieciowej. W fazie wstępnej konfiguracji mogą również zostać przypisane role i funkcje do serwera.

Nie tylko proces instalacji systemu został bardzo uproszczony. Prostsze jest również konfigurowanie systemu do wykonywania określonych zadań w sieci. Konfiguracja serwera została sprowadzona do przypisywania mu konkretnych ról i funkcji. Rola serwera opisuje główne zadanie, do którego serwer jest przeznaczony. Jednemu serwerowi można przydzielić wiele ról:

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Lightweight Directory Services
- Active Directory Federation Services
- Active Directory Rights Management Services
- DNS Server
- DHCP Server
- Fax Server
- File Server
- Terminal Services
- Network Access Services
- Print server
- Windows Deployment
- Services
- Windows Media Services
- UDDI Services
- Web Server (IIS)
- Windows SharePoint Services

Funkcja nie oznaczają zwykle głównych zadań serwera, tylko pomocnicze lub dodatkowe elementy wspierające pracę i funkcjonalność serwera:

- Background Intelligent Transfer Service (BITS) Server Extensions
- Windows BitLocker Drive Encryption
- Multipath I/O
- Storage Manager for Storage Area Networks (SANs)
- Windows Activation Service (WAS)
- Wireless Networking
- LPR Port Monitor
- Removable Storage Manager
- Remote Assistance
- Simple TCP/IP Services
- Telnet Client
- Telnet Server
- TFTP Client
- Windows Internet Name Service (WINS)
- Windows Server Backup
- Failover Clustering

Zwykle przypisywanie i ról i funkcji serwera związane jest z procesem zarządzania serwerem i wykonywane przy pomocy Server Manager opisanego w dalszej części niniejszej książki.

Proces instalacji i wstępnej konfiguracji wersji Core

Opcja instalatora Windows Server 2008 Server Core Instalation pozwala na zainstalowanie systemu z podstawową minimalną funkcjonalnością potrzebną do uruchamiania wybranych ról i funkcji serwera bez środowiska graficznego, redukuje to czynności związane z konserwacją i zarządzaniem środowiskiem, jak również przestrzeń narażoną na atak.

Poza ograniczeniem liczby serwisów i dostępności rozbudowanych narzędzi graficznych do zarządzania systemem, wersja Server Core ma również ograniczone możliwości konfiguracji ról i funkcji serwera. W tabeli poniżej zostały zestawione role, które mogą być konfigurowane na instalacji Server Core dla różnych edycji systemu.

Server Role	Enterprise	Datacenter	Standard	Web	Itanium
Web Services (IIS)	□	□	□	□	
Print Services	□	□	□		
Hyper-V[1]	□	□	□		
Active Directory Domain Services	□	□	□		

Active Directory Lightweight Directory Services	□	□	□		
DHCP Server	□	□	□		
DNS Server	□	□	□		
File Services	□	□	□[2]		

Dla klientów, którzy nie potrzebują wirtualizacji firma Microsoft przygotowała edycje Windows Server 2008 Standard, Enterprise oraz Datacenter bez technologi Windows Server 2008 Hyper-V Technology.

Ograniczenie do jednego wolnostojącego roota DFS

Podczas instalacji kopiowane są tylko te binaria, które są niezbędne do poprawnego funkcjonowania ról i usług dostępnych w wersji Server Core. Proces instalacji systemu nie różni się niczym od instalacji pełnej wersji. Różnicę można zobaczyć dopiero po pierwszym zalogowaniu, zamiast interfejsu graficznego pojawi się wiersz poleceń.

Podobnie jak w przypadku pełnej wersji Server Core zostanie zainstalowany z domyślnymi ustawieniami. Na początek, więc trzeba wykonać wstępną konfigurację:

- Ustawić hasło administratora, domyślnie hasło jest puste
- Ustawić adres IP, jeśli ma być stały domyślnie jest on pobierany z serwera DHCP
- Zmienić nazwę serwera
- Dodać serwer do istniejącej domeny, jeśli ma pracować w środowisku domenowym
- Aktywować system
- Skonfigurować zaporę sieciową
- Większość tych czynności trzeba wykonać z wiersza poleceń, tabela poniżej zestawia polecenia używane w tym celu.

	Wiersz poleceń	**Interfejs graficzny**
Ustawienie hasła administratora	Net user administrator *	Podczas logowania na konto administratora wcisnąć klawisze CTL+ALT+DEL i wybrać Change Password...
Konfiguracja stałe adresu IP	netsh interface ipv4 set address name="<ID>" source=static address=<StaticIP> mask=<SubnetMask> gateway=<DefaultGateway>	Nie ma
Konfiguracja adresu serwera DNS	netsh interface ipv4 add dnsserver name="<ID>" address=<DNSIP>index=1	Nie ma
Konfiguracja Windows Firewall	Należy konfigurować zdalnie z innego komputera Netsh advfirewall Set machine <ServerName>	Można wykorzystać konsolę Windows Firewall z Windows Vista lub Windows 2008 do zdalnego ustawienia zapory.
Zmiana nazwy serwera	Netdom renamecomputer %computername% / NewName:<NewComputerName>	Nie ma
Aktywacja	slmgr.vbs -ato	Nie ma
Dodanie serwera do domeny	netdom join %computername% /domain:<DomainName> / userd:<UserName> /passwordD:*	Nie ma

Aktywacja systemu Volume Activation 2.0

Wszystkie instalacje systemu Windows Vista oraz Windows Server 2008 muszą zostać aktywowane w ciągu 30 dni od chwili instalacji. Technologia Volume Activation 2.0 została zaprojektowana

aby pomóc specjalistom IT aktywować edycje systemu Windows licencjonowane zbiorowo. Wykorzystanie technologii aktywacji zbiorowej może przyspieszyć i uprościć wdrażanie, zapewnić skuteczne środki przeciwko piractwu, jak również dać wiele korzyści związanych z zarządzaniem i bezpieczeństwem.

Edycje licencjonowane zbiorowo domyślnie nie wymagają wprowadzania klucza produktu w trakcie instalacji.

Administratorzy systemu mogą zliczać aktywacje przy użyciu standardowego oprogramowania zarządzania systemem, na przykład Microsoft Operations Manager (MOM) oraz mieć dostęp do bardzo szczegółowych informacji na temat instalowanych licencji, stanu licencji i bieżącego terminu aktywacji lub terminu wygasania.

Technologia Volume Activation 2.0 zapewnia klientom dostęp do dwóch typów kluczy oraz trzech metod aktywacji:

- Klucz Multiple Activation Key (MAK)
- Niezależna aktywacja klucza MAK
- Aktywacja proxy klucza MAK
- Klucz Key Management Service (KMS)
- Aktywacja usługi KMS

W zależności od potrzeb przedsiębiorstwa i jego infrastruktury sieciowej, klienci mogą wybrać dowolną metodę aktywacji.

Aby uprościć aktywację zbiorową różnych wersji klienckich i serwerowych, firma Microsoft wprowadziła pojęcie grup edycji produktów licencjonowanych zbiorowo (Volume Edition Product Groups). Klucze usługi KMS oraz MAK można zastosować do grup edycji produktów, zamiast do każdej edycji osobno. Upraszcza to znacznie zarządzanie kluczami dzięki redukcji liczby możliwych kluczy. Tabela poniżej zawiera istniejące grupy produktów oraz edycje systemu Windows licencjonowane zbiorowo, należące do każdej z grup.

Grupa produktów licencjonowanych zbiorowo	**Edycje systemu Windows**	**Klucz MAK**	**Klucz KMS**
Vista VL	Windows Vista Business Windows Vista Enterprise	MAK	KMS
Server Group A	Windows Server 2008 Web Server Windows Server 2008 Compute Cluster Windows Server 2008 Storage Server*	MAK_A	KMS_A
Server Group B	Windows Server 2008 Standard Windows Server 2008 Enterprise Windows Server 2008 Storage Server Enterprise	MAK_B	KMS_B
Server Group C	Windows Server 2008 Datacenter Windows Server 2008 Itanium	MAK_C	KMS_C

Grupy produktów zorganizowane są według hierarchii celów aktywacji. Każda kolejna grupa produktów aktywuje wszystkie wcześniejsze grupy produktów. Innymi słowy, host usługi KMS z zainstalowanym kluczem KMS_B będzie mógł aktywować nie tylko urządzenia klienckie usługi KMS z grupy serwera B, ale również urządzenia klienckie korzystające z systemu Vista oraz grupy serwera A.

Klucz usługi KMS	**Grupy produktów**
KMS	Vista VL
KMS_A	Vista VL Server Group A
KMS_B	Vista VL Server Group A Server Group B
KMS_C	Vista VL Server Group A Server Group B Server Group C

Aktywacja klucza MAK wykorzystuje technologię podobną do używanej w subskrypcjach MSDN Universal i Microsoft Action Pack. Każdy klucz produktu może aktywować określoną liczbę komputerów. Aktywacja klucza MAK wymagana jest tylko raz, chyba, że nastąpią znaczące zmiany w sprzęcie.

Istnieją dwa sposoby aktywacji komputerów przy użyciu klucza MAK:

- Niezależna aktywacja klucza MAK: Wymaga, aby każdy komputer docelowy łączył się i aktywował niezależnie od firmy Microsoft.
- Aktywacja proxy klucza MAK: Pozwala na scentralizowane żądanie aktywacji dla wielu komputerów dzięki pojedynczemu połączeniu z firmą Microsoft. Aktywacja Proxy klucza MAK dostępna jest w narzędziu Volume Activation Management Tool (VAMT).

Usługa Key Management Service (KMS) pozwala przedsiębiorstwom przeprowadzać procesy lokalnych aktywacji komputerów w zarządzanych środowiskach bez potrzeby łączenia się z firmą

Microsoft. Klucz usługi KMS wykorzystywany jest do uruchomienia usługi KMS na komputerze głównym sterowanym przez administratora. Hostem usługi może być system Windows Vista, Windows 2008 i Windows 2003.

Usługa KMS zlicza liczbę żądań aktywacji, jakie otrzymuje, i odpowiada na nie. Komputery klienckie muszą łączyć się z hostem usługi KMS przynajmniej raz na 180 dni, aby odnawiać aktywację. Komputery, które nie zostały aktywowane, próbują łączyć się z hostem, co dwie godziny (wartość tę można skonfigurować). Po aktywacji, komputery próbują odnowić (lokalnie) swoją aktywację, co siedem dni (wartość tę także można skonfigurować), i jeśli proces się powiedzie, 180-dniowy termin aktywacji zostanie odnowiony.

Komputery lokalizują host usługi KMS przy użyciu jednej z następujących metod:

- Wykrywanie automatyczne: Komputer DNS, aby automatycznie zlokalizować host usługi KMS.
- Połączenie bezpośrednie: Administrator systemu określa lokalizację hosta usługi KMS oraz port komunikacyjny

Więcej na temat aktywacji systemów można znaleźć na:

www.microsoft.com/technet/volumeactivation.

www.microsoft.com/poland/technet/bazawiedzy/centrumrozwiazan/default.mspx
go.microsoft.com/fwlink/?LinkID=75674

Boot Configuration Data

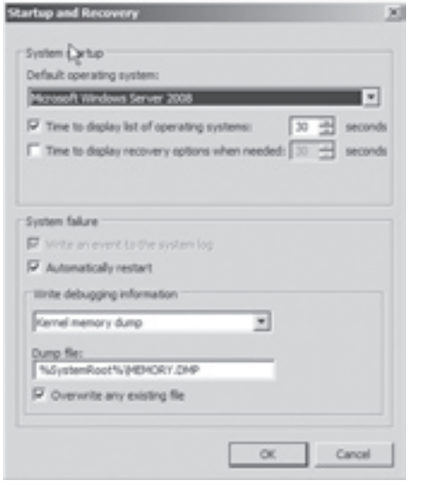
Boot Configuration Data jest magazynem, w którym system Windows Vista oraz Windows Server 2008 przechowują pliki oraz ustawienia aplikacji dotyczące rozruchu, zastąpił on plik Boot.ini znany z poprzednich wersji systemu. BCDEdit.exe jest edytorem z linii poleceń systemu, dzięki któremu można zarządzać magazynem danych konfiguracji rozruchu.

Microsoft wprowadził takie rozwiązanie w związku z wprowadzeniem EFI (Extensible Firmware Interface), systemem opracowywanym przez firmę Intel, który ma zastąpić znany wszystkim BIOS. BCD znajduje się w:

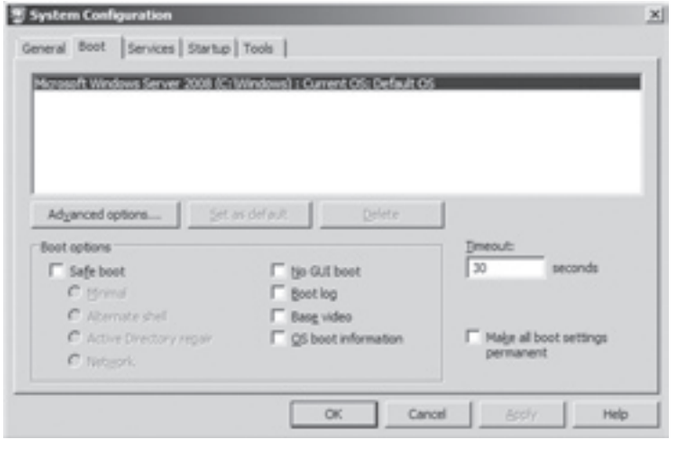
- W folderze Boot, który umieszczony jest na partycji aktywnej, jeśli komputer wyposażony jest w BIOS.
- Na specjalnej partycji EFI, gdy komputer wyposażony jest w to rozwiązanie.

BCD może być edytowane na kilka sposobów:

Okno Startup and Recovery

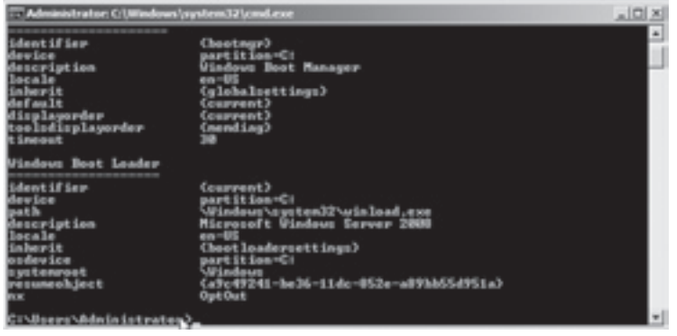


MSConfig.exe



WMI pozwala na tworzenie skryptów, którymi można edytować BCD.

BCDEdit służy do modyfikacji BCD z poziomu wiersza polecenia.



Poprzez BCDEdit. Można wykonywać następujące czynności:

- Modyfikować, dodawać oraz usuwać wpisy z BCD
- Importować oraz eksportować wpisy BCD
- Zarządzać menedżerem rozruchu
- Tworzyć nowe magazyny BCD dla innych instalacji
- Kontrolować usługi zarządzania awaryjnego (EMS) dla aplikacji i systemu
- Zmieniać opcje wpisów
- Przeglądać listy wszystkich aktywnych wpisów
- Stosować zmiany globalne we wszystkich magazynach BCD
- Konfigurować debugowanie w systemie

Więcej informacji na temat BCD można znaleźć na

www.microsoft.com/poland/technet/bazawiedzy/centrumrozwiazan/cr143.mspx

Windows Deployment Services – sieciowa dystrybucja systemów operacyjnych nowej generacji

Microsoft Windows Deployment Services (WDS) to unowocześniona i przeprojektowana wersja usługi Remote Installation Services (RIS). WDS jest częścią składową systemu operacyjnego Windows Server 2008. Występuje również jako dodatek do systemu Windows Server 2003.
Umożliwia automatyczną dystrybucję systemów operacyjnych z rodziny Vista / Server 2008, przy jednoczesnym zachowaniu kompatybilności ze starszymi wersjami systemów operacyjnych.

Daje możliwość w pełni zautomatyzowanej instalacji zróżnicowanych obrazów systemów operacyjnych poprzez sieć, na komputerach zgodnych ze standardem PXE, bez konieczności fizycznej obecności przy każdym z docelowych komputerów oraz bez użycia jakichkolwiek nośników instalacyjnych .

Trochę historii

Windows Deployment Services nie jest pierwszym rozwiązaniem firmy Microsoft, ułatwiającym i automatyzującym proces instalacji systemów operacyjnych. Początkowe wersje systemów operacyjnych (np.Windows NT4) korzystały z licznych plików konfiguracyjnych, co umożliwiało częściowe usprawnienie procesu instalacji.

Od momentu wypuszczenia na rynek produktów z serii Windows 2000, pojawiły się nowe możliwości, związane z usługą Remote Installation Services. Jednak i ona posiadała pewne ograniczenia. Głównym z nich był sposób przechowywania obrazów systemów operacyjnych – w postaci dużej ilości plików.

Kolejnym krokiem w kierunku nowoczesnej dystrybucji systemów operacyjnych była usługa Automated Deployment Services. Opierała się ona na sektorowej odmianie obrazów. Dedykowana była jednak do dystrybucji systemów serwerowych.

Wraz z usługą SMS Operating System Deployment, pojawił się zupełnie nowy standard – pierwsza wersja formatu Windows Image format (WIM).

Właśnie na tym formacie zapisu obrazów opiera się usługa WDS zaimplementowana w Serwerze 2008, pozwalając na połączenie wszystkich zalet poprzednich rozwiązań, eliminując zarazem ich wady. W przeciwieństwie do swoich poprzedników rozwiązanie to wspiera najnowsze wersje systemów operacyjnych.

Format WIM

WIM to nic innego jak kolejny format zapisu obrazów systemów operacyjnych. Bazuje on na pojedynczych plikach. W odróżnieniu do innych rozwiązań, posiada on jednak wiele ciekawych cech.

Po pierwsze nie jest on związany z platformą sprzętową komputerów będących odbiorcami dystrybuowanych systemów operacyjnych. Oznacza to bezproblemową pracę w dowolnie zróżnicowanym środowisku.

Kolejna kwestia to brak w obrazie zapisu informacji o strukturze dysków twardych na których instalowany jest docelowy system. Oszczędność ta wpływa korzystnie na rozmiar obrazów.

W ramach zmniejszania objętości plików dystrybucyjnych, format ten zapewnia kompresję, oraz daje możliwość przechowywania wielu obrazów systemowych w jednym pliku. Możliwe jest również zróżnicowanie w obrębie jednego pliku obrazów na rozruchowe i instalacyjne.

Implementacja tego formatu, będącego kluczowym składnikiem usługi WDS, jest usprawnioną wersją standardu opracowanego na potrzeby usługi SMS Operating System Deployment.

Daje to praktycznie nieograniczone możliwości dystrybucji systemów operacyjnych w nawet najbardziej zróżnicowanym środowisku.

WDS – charakterystyka usługi

Poza wykorzystaniem nowego formatu zapisu obrazów, usługa WDS posiada wiele możliwości niedostępnych u jej poprzedników.

Podstawową z nich jest dystrybucja systemów operacyjnych z rodziny Microsoft Vista, oraz Server 2008. W przeciwieństwie do usługi RIS, WDS posiada również własną konsolę MMC, dającą możliwość zarządzania wszystkimi jej funkcjami.

Kolejną nowością jest natywne wsparcie dla systemu Windows PE, umożliwiającego rozpoczęcie procesu instalacji, oraz wiele innych zadań opisanych poniżej.

Poprawiono również wydajność serwera PXE, odpowiadającego za zdalne uruchamianie instalacji systemów operacyjnych na komputerach posiadających zgodne z tym standardem karty sieciowe.

Usługę WDS, ze względu na obszary jej administracji można podzielić na trzy kategorie:

Komponenty zarządzające. Komponentem zarządzającym WDS jest specjalnie przygotowana konsola MMC. Są to narzędzia używane do administrowania serwerem WDS, obrazami systemów operacyjnych i kontami komputerów.

Komponenty serwerowe. Obejmują one przede wszystkim środowisko Pre-Boot eXecution Environment (PXE) oraz protokół Trivial File Transfer Protocol (TFTP), pozwalające prze transferować pliki do komputerów, w których ma być zainstalowany system operacyjny i uruchomić je w celu instalacji systemu. Udostępniony folder i repozytorium z obrazami instalacyjnymi i plikami niezbędnymi dla uruchomienia zdalnego komputera przez sieć, to również komponenty serwerowe usług WDS.

Komponenty klienckie. Obejmują graficzny interfejs użytkownika (GUI) w środowisku Microsoft Windows Preinstallation Environment (Windows PE), który daje możliwość skomunikowania się z komponentami serwerowymi oraz wybrania i zainstalowania odpowiedniego obrazu systemu operacyjnego.

Komponenty zarządzające:

- Konsola zarządzania usługami WDS

WDS gwarantuje znacznie wyższy poziom funkcjonalności narzędzi administracyjnych niż usługa RIS. Dedykowana konsola MMC daje możliwość dodawania i usuwania serwerów, konfigurowania opcji (takich, jak reguły nazewnictwa komputerów, opcje DHCP, opcje odpowiedzi PXE, itp.), dodawania i usuwania obrazów instalacyjnych i rozruchowych.

Daje również pełną kontrolę nad dodawanymi grupami obrazów i samymi obrazami.

- Wiersz poleceń

Alternatywą dla konsoli MMC jest narzędzie WDSUTIL, dające dostęp do takiego samego poziomu funkcji administracyjnych, z poziomu linii komend.

Jest to doskonałe rozwiązanie dla zaawansowanych administratorów, dające możliwość automatyzacji i skryptowania wszystkich dostępnych zadań administracyjnych usługi WDS.

Komponenty serwerowe

- Serwer TFTP

Rozwiązanie to opiera się na protokole FTP – jest jego mocno uproszczoną wersją. W protokole tym dane przesyłane są w blokach o stałej długości 512 bajtów – każdy z nich musi być potwierdzony przez pakiet potwierdzający. W środowisku WDS, odpowiada on za transport obrazu rozruchowego Windows PE na komputery klienckie wyposażone w kartu zgodne z PXE. Służy również do przesyłania obrazów systemów operacyjnych.

- Serwer PXE

Dostawca usługi PXE – zawiera w sobie zintegrowaną logikę do komunikacji z rdzeniem usługi WDS. Do przechowywania informacji wykorzystuje usługę katalogową Active Directory, łącząc fizyczny komputer z obiektem w Active Directory, jakim jest konto komputera wraz z przypisanym mu identyfikatorem GUID. Dla zapewnienia kompatybilności z usługą RIS zawiera komponenty emulujące RIS na WDS. Ze względu na przeznaczenie można go podzielić na trzy obszary pracy:

Komponenty klienckie

Środowisko Windows Preinstallation Environment (PE) 2.0 to nic innego jak środowisko znane z procesu instalacji systemów operacyjnych Windows Vista, oraz Server 2008 znacznie ułatwiające instalowanie spersonalizowanych wersji tych systemów. W trakcie instalowania systemu Windows

Vista, w ramach środowiska Windows PE, uruchamia się graficzne narzędzia zbierające informacje o konfiguracji. Ponadto środowisko Windows PE można dostosować i poszerzyć tak, aby spełniało indywidualnie określone potrzeby.

Środowisko to wykorzystywane jest w procesie instalacji systemów operacyjnych, w szczególności w trybie nienadzorowanym lub do przeprowadzania czynności serwisowych, gdy domyślny system operacyjny serwera lub stacji roboczej uległ jakiemuś uszkodzeniu. Ze względu na fakt wykorzystania jądra systemów Windows, nie istnieje już konieczność korzystania ze specjalnie przygotowanych sterowników do sprzętu pracujących w trybie 16-bitowym – wykorzystuje się tu domyślne sterowniki systemu Windows.

Firma Microsoft zaprojektowała Windows PE tak, aby mógł on zastąpić MS-DOS w roli środowiska pre-instalacyjnego.

Windows PE wykrywa najnowsze rozwiązania sprzętowe oraz potrafi komunikować się za pomocą protokołu Internet Protocol (IP). Środowisko Windows PE zajmuje mniej niż 100 MB przestrzeni dyskowej i może być uruchamiane w całości z pamięci RAM, co pozwala na odczytywanie w napędzie DVD płyty z innym oprogramowaniem, np. ze sterownikami. Dzięki temu Windows PE może być uruchamiany także w komputerach, których twardy dysk nie został jeszcze sformatowany oraz komputerach nie posiadających żadnego systemu operacyjnego. Jednakże Windows PE nie jest pełnym systemem operacyjnym takim, jak Windows Vista. Dostępne są wersje dla platformy x86, x64 oraz Itanium.

Instalacja i aktualizacja do usługi WDS

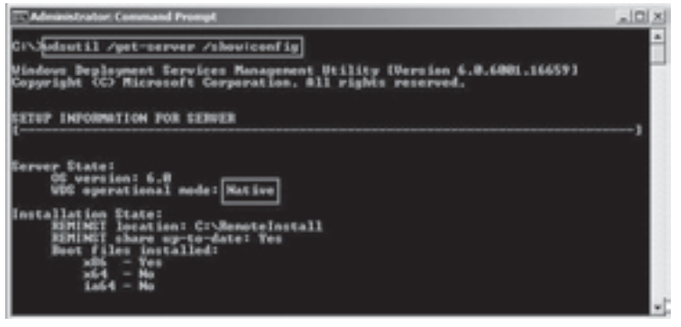
Niezależnie od tego, czy wybrana zostanie nowa instalacja, czy też proces uaktualniania systemu Windows Server 2003, muszą być spełnione następujące warunki:

Element systemu	Wymagana konfiguracja
Usługa Active Directory	Serwer usługi WDS, musi być członkiem domeny Active Directory. Tryb pracy domeny nie ma wpływu na funkcjonowanie usługi.
Serwer DHCP	Sieć objęta działaniem usługi WDS musi posiadać serwer DHCP, którego konfiguracja umożliwi klientom PXE otrzymywanie konfiguracji IP pozwalającej na komunikację z serwerem WDS.
Serwer DNS	Sieć objęta działaniem usługi WDS musi posiadać serwer DNS.
Partycja NTFS	Serwer WDS wymaga partycji zgodnej z systemem plików NTFS, do przechowywania obrazów systemów operacyjnych.
Uprawnienia	Uprawnienia niezbędne do instalacji i konfiguracji serwera WDS, to członkostwo w grupie lokalnych administratorów na serwerze WDS.

Aktualizacja usługi WDS

Istnieje możliwość aktualizacji systemu operacyjnego Microsoft Windows Server 2003 z zainstalowaną usługą WDS do systemu Server 2008. Możliwość wykonania tej operacji zależy od trybu pracy usługi WDS na serwerze 2003. Aby sprawdzić bieżący tryb pracy usługi należy wykonać z linii komend polecenie:

WDSUTIL /get-server /show:config



Jedyny tryb pracy, który umożliwia aktualizację usługi do platformy Server 2008, to tryb Native. Jeżeli system pracuje w trybie Legacy, lub Mixed, należy przełączyć go do trybu Native. Tryby Legacy i Mixed, aktywne są w sytuacji, kiedy na serwerze skonfigurowana jest usługa RIS.

Jeżeli system pracuje w trybie Legacy

W celu zmiany trybu pracy z Legacy na Mixed należy:

- Aktualizować usługę RIS do usługi WDS.
- Zainicjalizować serwer WDS za pomocą konsoli MMC usługi WDS, lub komendą:

WDSUTIL /Initialize-Server /RemInst:D:\RemoteInstall

Gdzie:
"D:\RemoteInstall" oznacza ścieżkę do folderu REMINST wykorzystywanego przez usługę RIS.

Po wykonaniu tych operacji usługa WDS przechodzi do pracy w trybie Mixed (koegzystencji z systemem RIS)

Jeżeli system pracuje w trybie Mixed

W celu zmiany trybu pracy z Mixed na Native należy:

- Prze konwertować istniejące obrazy systemów operacyjnych wykorzystywane przez serwer RIS na standard WIM. Można tego dokonać na kilka sposobów.

- Za pomocą konsoli MMC:
- Zaznaczając wybrany obraz legacy w konsoli WDS, można wybrać funkcję Convert To WIM

Z linii komend:

WDSUTIL /Convert-RIPREPImage /FilePath:<ścieżka1> /DestinationImage /FilePath:<ścieżka2>

Gdzie:
<ścieżka1> to ścieżka do pliku riprep.sif
<ścieżka2> to ścieżka do nowego obrazu w formacie WIM

Następnie należy uruchomić komendę:

WDSUTIL /Set-Server /ForceNative

Jeżeli usługa pracuje już w trybie Native standardowa aktualizacja systemu operacyjnego do systemu Server 2008, spowoduje przeniesienie wszystkich jej ustawień do nowej platformy.

Nowa instalacja

Instalacja usługi WDS w systemie Microsoft Windows Server 2008, możliwa jest zarówno przy wykorzystaniu narzędzia **Initial Configuration Tasks,** jak i z poziomu **Server Managera.**

Usługa ta jest jedną z ról systemowych, tak więc niezależnie od wybranego narzędzia, należy skorzystać z funkcji **Add roles.**

W menu dodawania nowej roli, należy wybrać Windows Deployment Services a następnie w kolejnym menu wybrać komponenty usługi:

Transport Server - Instalacja podstawowych usług sieciowych usługi WDS. Komponent ten pozwala na utworzenie serwera korzystającego z transmisji typu multicast do dystrybuowania obrazów systemów operacyjnych.

Deployment Server - Instalacja pełnej funkcjonalności usługi WDS.

Konfiguracja usługi WDS i dystrybucja systemów operacyjnych

Konfiguracja usługi WDS może odbywać się na dwa sposoby. Za pomocą konsoli MMC, oraz korzystając z polecenia WDSUTIL dostępnego z linii komend. W związku z tym kolejne procedury konfiguracyjne będą uwzględniały obydwie możliwości.

Poszczególne zadania konfiguracyjne warto podzielić na kroki.

Wstępna konfiguracja

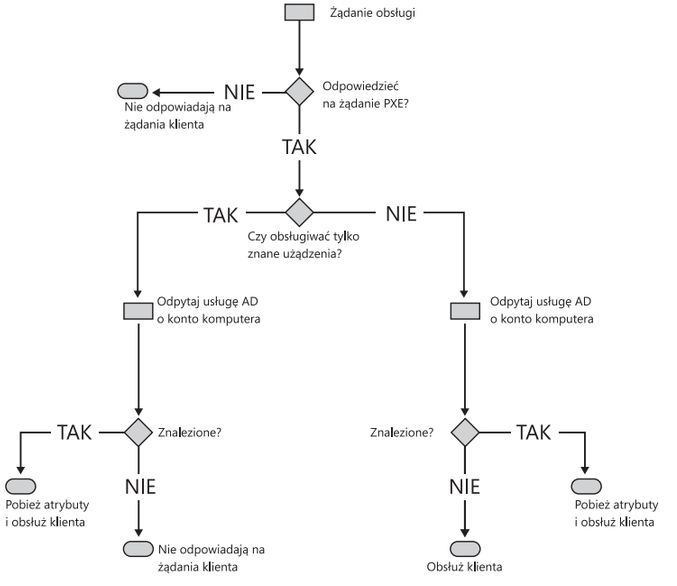
Pierwszym krokiem po instalacyjnym jest inicjalizacja usługi WDS. Obejmuje ona utworzenie udostępnionego folderu, w którym przechowywane będą dystrybuowane obrazy systemów operacyjnych, oraz wybór sposobu odpowiadania na żądania klientów. Folder ten powinien znajdować się na partycji z systemem plików NTFS.

Metoda odpowiadania na żądania klientów daje następujące możliwości wyboru:

- **Respond only to known client computers** - serwer odpowiada na zapytania wyłącznie klientom znanym (*ang. prestaged*), tj. posiadającym w domenie przeinstalowane konto komputera wraz z przypisanym do niego identyfikatorem GUID.
- **Respond to All (known and unknown) client computers** – powoduje wybranie trybu zezwalającego na obsługę wszystkich urządzeń, chyba że zostania zaznaczona opcja
- **For unknown client, notify administrator and respond after approval** – co spowoduje konieczność zatwierdzania każdego nowego żądania klienckiego przez administratora.

Wykorzystanie tej opcji umożliwia odpowiadanie również tym klientom, którzy nie mają wstępnie zdefiniowanego konta komputera w domenie. Takie konto, po zatwierdzeniu żądania przez administratora, będzie automatycznie tworzone.

Poniższy diagram obrazuje zachowanie się systemu w zależności od wybranego rozwiązania.



Za pomocą konsoli MMC należy:

- Uruchomić **Windows Deployment Services**
- Kliknąć prawym przyciskiem myszy konfigurowany serwer i wybrać funkcję **Configure Server**
- Uruchomiony w ten sposób kreator umożliwi określenie ścieżki do katalogu w którym przechowywane będą obrazy systemów operacyjnych, oraz sposobu odpowiadania na żądania klientów

Chcąc osiągnąć ten sam cel za pomocą narzędzia WDSUTIL należy wykonać polecenia:

WDSUTIL /initialize-server /reminst:"<litera_dysku>\<nazwa_folderu>"
WDSUTIL /Set-Server /AnswerClients:all

Gdzie:
<litera_dysku> - dysk na którym znajdować się będą obrazy systemów operacyjnych
<nazwa_folderu> - folder w którym znajdować się będą obrazy systemów operacyjnych

Jeżeli serwer WDS pełni również rolę serwera DHCP należy również wykonać polecenie:

WDSUTIL /Set-Server /UseDHCPPorts:no /DHCPoption60:yes

W większości przypadków, dystrybucja systemów operacyjnych powiązana jest z tworzeniem kont dla nowych urządzeń w usłudze Active Directory. Na tym etapie konfiguracji można więc określić metodologię tworzenia tych nazw, oraz docelową lokalizację kont (jednostka organizacyjna lub folder). Najprostszym sposobem konfiguracji jest skorzystanie z konsoli administracyjnej WDS. We właściwościach w zakładce znaleźć można następujące warianty konwencji nazewniczej:

- **%First** – nazwa identyczna z imieniem użytkownika tworzącego konta w Active Directory
- **%Last** - nazwa identyczna z nazwiskiem
- **%Username** – nazwa identyczna z nazwą użytkownika (login)
- **%MAC** - adres MAC komputera
- **%n#** - przyrostowa liczna n-cyfrowa (%2# daje numery za zakresu 1,2,3,...99)
- **%0n#** - jak wyżej, ale z nieznaczącymi zerami (so %02# daje numery 01,02,03,...99)

W miejscu tym możliwe jest również określenie ścieżki w usłudze katalogowej w której zostaną utworzone konta komputerów.

Konfiguracja metod rozruchu klientów PXE

Ta część zadań konfiguracyjnych odnosi się do sposobów początkowej obsługi żądań stacji klienckich związanych z menu rozruchowym. Pozwoli to na zróżnicowaną obsługę klientów w zależności od ich architektury systemowej.

Na początek warto przyswoić sobie trzy brzmiące podobnie pojęcia, które będą niezbędne do prawidłowej konfiguracji usługi.

Boot menu
Początkowe menu pojawiające się w trakcie rozruch sieciowego po stronie klienta PXE.

Boot images
Obrazy systemu Windows PE wykorzystywane w procesie wstępnej re konfiguracji stacji roboczej, przed właściwym procesem instalacyjnym, lub w procesie naprawczym.

Install images
Obrazy zawierające pliki instalacyjne systemów operacyjnych
Domyślna konfiguracja usługi WDS zawiera menu rozruchowe zarówno dla architektury x64 jak i x86.

Skutkiem tego klienci posiadający systemy klasy x86 będą mieli możliwość uruchomiania tylko i wyłącznie 32-bitowej wersji rozruchu , natomiast stacje 64-bitowe z racji możliwości uruchamiania aplikacji x86 będą mieli dostęp do dwóch rodzajów menu.
Zmianę sposobu obsługiwania stacji można wykonać za pomocą polecenia

WDSUTIL /Set-Server /Defaultx86x64ImageType:{x86|x64|both}.

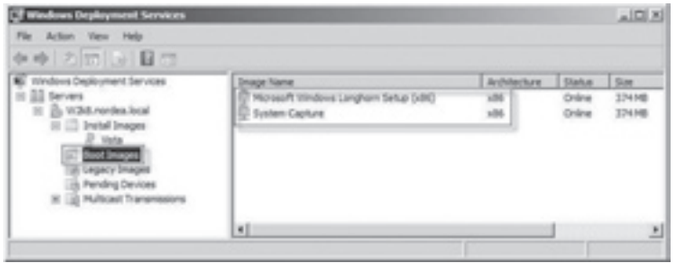
Jeżeli zaistnieje potrzeba dokonania zmian w treści początkowego menu, należy skorzystać z narzędzia **bcdedit.**

Konfigurując menu rozruchowe pamiętać należy również o pewnych jego ograniczeniach:

- Menu nie może zawierać więcej niż 13 pozycji
- Nazwy obrazów WIM nie mogą zawierać spacji

Celem początkowego menu rozruchowego jest uruchomienie środowiska systemu Windows PE. System ten znajduje się na nośniku instalacyjnym serwera 2008, oraz Vista pod nazwą boot.wim.

Choć w obydwu tych systemach wygląda on niemal identycznie, do zastosowania z usługą WDS należy korzystać tylko i wyłącznie z wersji dostarczanej z serwerem 2008, co umożliwi kompatybilność z usługami takimi jak multicasting.



Obraz systemu Windows PE nie jest standardowo powiązany z usługą WDS.

Chcąc dokonać tego za pomocą konsoli MMC należy:

- W konsoli usługi WDS rozwinąć listę wybranego serwera WDS.
- Kliknąć menu **Boot Images** I wybrać polecenie **Add Boot Image**.
- W kreatorze wskazać na plik boot.wim znajdujący się na nośniku instalacyjnym Windows Server 2008

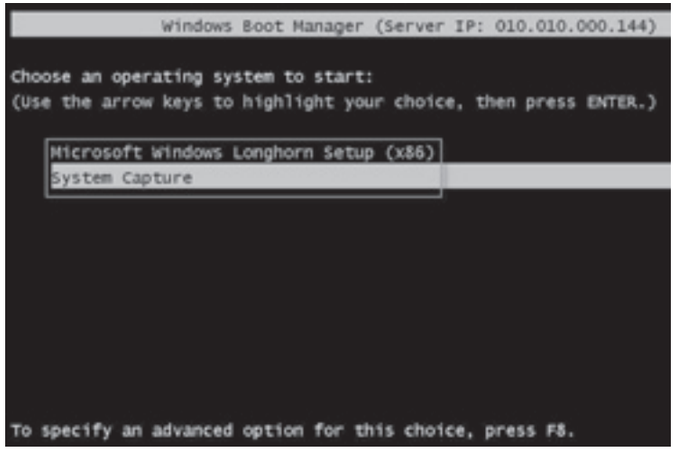
Natomiast z linii komend wystarczy polecenie:

WDSUTIL /Add-Image /ImageFile:<bootimage> /ImageType:boot

Gdzie:
<Bootimage> to ścieżka do pliku boot.wim znajdującego się na nośniku instalacyjnym **Windows Server 2008**

Można w ten sposób utworzyć wiele obrazów rozruchowych, których celem może być np.:

- Uruchomienie procesu instalacji systemu operacyjnego
- Prze formatowanie dysków twardych do korzystania ze standardu BitLocker Drive Encryption
- Uruchomienie narzędzi Windows Recovery Environment (Windows RE)



Poza standardowym zastosowaniem na uwagę zasługują również dwie dodatkowe funkcjonalności obrazów rozruchowych - Capture image, oraz Discover image.

Capture image – jest to obraz rozruchowy, którego celem jest przechwycenie w pełni skonfigurowanego systemu operacyjnego urządzenia, które zostało uruchomione z tego obrazu. Odnosi się to do komputerów, skonfigurowanych administracyjnie jako szablony (wzorce) konfiguracyjne i dostosowanych za pomocą programu sysprep do masowej dystrybucji. Przechwycony system zostaje zapisany w formacie WIM i przesłany do serwera WDS, w celu dalszej dystrybucji.

Discover image – ta dość specyficzna funkcjonalność pozwala na stworzenie obrazu rozruchowego dla komputerów nie kompatybilnych ze standardem PXE. Obraz taki gwarantuje możliwości analogiczne do swojego sieciowego odpowiednika, jest jednak uruchamiany z nośnika (USB, CD, DVD). Zawarty w nim system Windows PE, potrafi skomunikować się z serwerem WDS, niezależnie od tego, czy dany klient posiada zgodny z PXE interfejs sieciowy.

Obydwie te funkcjonalności, mogą być uzyskane z dodanego wcześniej obrazu rozruchowego Windows PE. Tak jak i w poprzednich wypadkach, zamiana standardowego obrazu na Capture lub Discovery możliwa jest zarówno z poziomu konsoli MMC, jak i z linii komend.

Za pomocą konsoli MMC należy:

Chcąc stworzyć **Capture image**

- W konsoli WDS wybrać odpowiedni serwer.
- W folderze BOOT Images kliknąć prawym przyciskiem myszki obraz rozruchowy
- Wykonać funkcję Create Capture BOOT Image

Chcąc stworzyć **Discover image**

- W konsoli WDS wybrać odpowiedni serwer.
- W folderze BOOT Images kliknąć prawym przyciskiem myszki obraz rozruchowy
- Wykonać funkcję Create Discover BOOT Image

Z linii komend cel można osiągnąć wpisując:

Chcąc stworzyć **Capture image**

WDSUTIL /New-CaptureImage /Image: <obraz_rozruchowy> /Architecture:x86 /Filepath:<captureimage>

Gdzie:
<obraz_rozruchowy> – to nazwa istniejącego obrazu rozruchowego
<captureimage> – ścieżka w której zostanie utworzony obraz typu capture

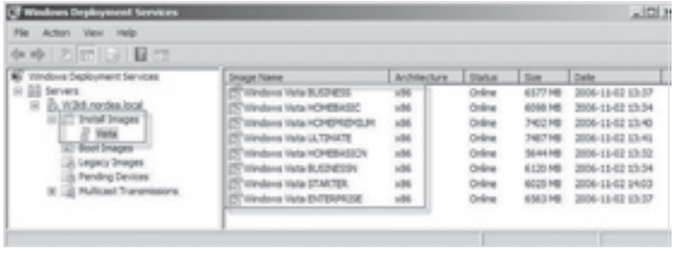
Chcąc stworzyć **Discover image**

WDSUTIL /New-DiscoverImage /Image:<obraz_rozruchowy> /Architecture:x86 /Filepath:<discoverimage>

Gdzie:
<obraz_rozruchowy> - to nazwa istniejącego obrazu rozruchowego
<discoverimage> - ścieżka w której zostanie utworzony obraz typu discover

Tworzenie i dystrybucja obrazów systemów operacyjnych

Przygotowywanie obrazów
Przygotowywanie obrazów instalacyjnych systemów operacyjnych może odbywać się na dwa sposoby. Pierwszym z nich jest wykorzystanie gotowych obrazów w formacie WIM zawartych na nośnikach instalacyjnych systemów Vista i Server 2008. Opublikowanie ich w usłudze WDS jest niezwykle proste.



Za pomocą konsoli MMC należy:

- W konsoli WDS wybrać odpowiedni serwer.
- Kliknąć prawym przyciskiem myszki na folder Install Images
- Wybrać funkcję Add Install Image
- W kreatorze wskazać obraz systemu operacyjnego w formacie WIM

Ta sama operacja z wiersza poleceń wygląda następująco:

WDSUTIL /add-image /ImageFile:<obraz_instalacyjny> /ImageType:install /ImageGroup:<nazwa_grupy>

Gdzie:
<obraz_instalacyjny> – pełna ścieżka do pliku w formacie WIM zawierającego obraz systemu operacyjnego
<nazwa_grupy> – nazwa grupy obrazów systemów operacyjnych

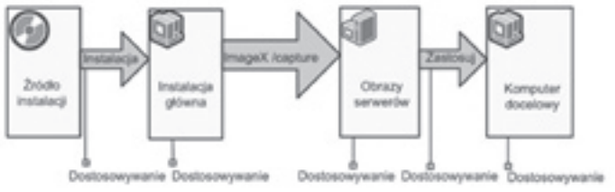
Jeżeli plik WIM zawiera wiele obrazów systemowych a konieczne jest dodanie tylko jednego z nich, należy skorzystać z dodatkowego przełącznika do komendy wdsutil **/SingleImage:<nazwa_obrazu**

Druga opcja to tworzenie obrazów w pełni dostosowanych systemów operacyjnych. Mogą one zawierać dowolną konfigurację oraz zainstalowany zestaw aplikacji wykorzystywanych w przedsiębiorstwie. Ten rodzaj przygotowywania dystrybucji opiera się na wykorzystaniu komputera „wzorca", będącego szablonem instalacyjnym dla pozostałych urządzeń w sieci.

Proces ten podzielić można na kilka faz:

- Instalacja główna na komputerze wzorcowym
- Modyfikacja instalacji domyślnej/dodanie aplikacji i sterowników dodatkowych

- Przechwycenia obrazu systemu
- Umieszczenie obrazów przechwyconych w punkcie dystrybucji
- Wdrożenie na komputerze/ach docelowych



Instalacja główna na komputerze wzorcowym
Polega na zainstalowaniu wybranego systemu operacyjnego z dowolnego nośnika na wydzielonym komputerze.

Modyfikacja instalacji domyślnej/dodanie aplikacji i sterowników dodatkowych
Ten etap to dopasowywanie środowiska systemowego. Polega na konfiguracji „Wzorca" tak aby reprezentował standard środowiska systemu operacyjnego, przeznaczonego dla danej organizacji. Konfiguracja ta jest zupełnie dowolna i powinna bazować jedynie na polityce organizacji dotyczącej infrastruktury IT.

Przechwycenia obrazu systemu
Zanim obraz systemu operacyjnego zostanie przechwycony za pomocą obrazu rozruchowego typu Capture Image, musi być on dostosowany do dystrybucji za pomocą narzędzia sysprep. W zależności od tego, czy jest to system klasy XP, czy Vista należy po zmodyfikowaniu domyślnej instalacji wykonać następujące polecenie:

W systemie Vista
sysprep /oobe /generalize /reboot

W systemie XP
sysprep -mini -reseal

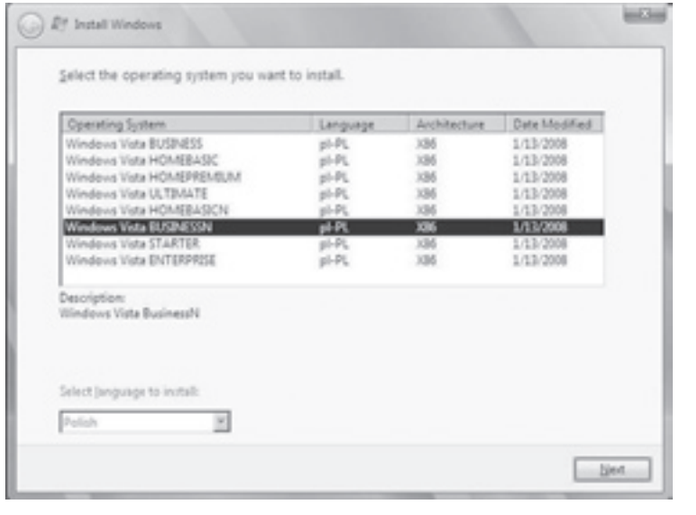
Po zakończeniu operacji komputer wolno uruchomić jedynie poprzez rozruch sieciowy, wybierając obraz typu Capture Image, który przechwyci dostosowany system operacyjny i przeniesie go w postaci pliku WIM na serwer WDS.

Umieszczenie obrazów przechwyconych w punkcie dystrybucji
Obraz przygotowany za pomocą funkcji Capture Image dodawany jest do usługi WDS tak samo jak zwykłe obrazy WIM znajdujące się na nośnikach instalacyjnych.

Wdrożenie na komputerze/ach docelowych
Choć standardowo celem przygotowania obrazów jest ich dystrybucja za pomocą środowiska WDS, nie ma przeciwwskazań do instalowania ich za pomocą dowolnych nośników (DVD, USB, itp.)

Przygotowane obrazy wzorcowe można w późniejszym czasie off-line'owo modyfikować bez konieczności ponownego wykonywania fazy wstępnej – przygotowywania komputera wzorcowego.

Instalacja obrazów systemów operacyjnych
Proces zainicjowania standardowej instalacji przygotowanych wcześniej obrazów, odbywa się z poziomu systemu Windows PE. Jeżeli nie są wykorzystywane pliki odpowiedzi automatyzujące proces instalacji, użytkownik uruchamiający system rozruchowy po uwierzytelnieniu się zobaczy listę systemów operacyjnych możliwych do zainstalowania na danym komputerze.



Jeżeli jednak instalacja systemu ma przebiec pomyślnie muszą być spełnione określone warunki. Dla systemu Microsoft Windows Vista wygląda to następująco:

Wymagania dotyczące partycji systemu, Windows Vista.
Aby system Windows Vista funkcjonował poprawnie, aktywna partycja musi zawierać około 700 MB wolnego miejsca podczas instalacji systemu Windows.

Wymagania środowiska odzyskiwania systemu Windows dotyczące partycji.
Środowisko odzyskiwania systemu Windows musi być zainstalowane na innej partycji, niż partycja systemu Windows Vista. Partycja ta powinna mieć następujące właściwości:

- Musi być sformatowana, jako system plików NTFS.
- Co najmniej 700 MB musi być zarezerwowane dla środowiska odzyskiwania systemu, Windows przy instalowaniu go, jako rozszerzonego obrazu.

Szyfrowanie dysków funkcją BitLocker – wymagania dotyczące partycji.

Szyfrowanie dysków funkcją BitLocker wymaga aktywnej partycji innej, niż partycja sytemu Windows Vista. Aktywna partycja musi mieć następujące właściwości: nie może być szyfrowana ani używana do przechowywania plików użytkownika.

Automatyzacja procesu instalacji – tryb nienadzorowany

Podobnie, jak we wcześniejszych wersjach systemu Windows, procedurę instalacyjną Windows Vista można zautomatyzować, stosując pliki odpowiedzi. W przypadku systemu Windows Vista pliki odpowiedzi Unattend.xml mają format Extensible Markup Language (XML), a nie format tekstowy. Plik Unattend.xml jest bardziej złożony niż wcześniejsze wersje plików odpowiedzi i dla ograniczenia prawdopodobieństwa wystąpienia błędów zaleca się przygotowywanie i edytowanie go w narzędziu Windows System Image Manager (Windows SIM), będącym składnikiem pakietu WAIK.

Usługa WDS pozwala skojarzyć osobny plik odpowiedzi z każdym dodanym do niej obrazem instalacyjnym. Można również wykorzystać globalny plik odpowiedzi dla każdej obsługiwanej platformy, tj. x86, x84 i IA64. Taki globalny plik odpowiedzi zawiera dane uwierzytelniające, pozwalające automatycznie zalogować się do serwera WDS. Plik ten specyfikuje też obraz załadowywany do docelowych komputerów klasy x86 oraz zawiera liczne inne ustawienia występujące w typowym pliku odpowiedzi, takie jak sposób konfiguracji partycji, członkostwo domeny czy strefę czasową. Łącznie zawiera kilkadziesiąt różnych ustawień systemowych, których szczegółowy opis znajduje się w dokumentacji pakietu WAIK.

Przykładowy plik unattend.xml ma następującą postać:

```
<?xml version="1.0" ?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
 <settings pass="windowsPE">
  <component name="Microsoft-Windows-Setup" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" processorArchitecture="x86">
   <WindowsDeploymentServices>
   <Login>
    <WillShowUI>OnError</WillShowUI>
    <Credentials>
     <Username>username</Username>
     <Domain>wds-dom</Domain>
     <Password>my_password</Password>
    </Credentials>
   </Login>
   <ImageSelection>
    <WillShowUI>OnError</WillShowUI>
    <InstallImage>
     <ImageName>Windows Vista with Office</ImageName>
     <ImageGroup>ImageGroup1</ImageGroup>
     <Filename>Install.wim</Filename>
    </InstallImage>
     <InstallTo>
     <DiskID>0</DiskID>
     <PartitionID>1</PartitionID>
    </InstallTo>
   </ImageSelection>
   </WindowsDeploymentServices>
   <DiskConfiguration>
   <WillShowUI>OnError</WillShowUI>
    <Disk>
     <DiskID>0</DiskID>
     <WillWipeDisk>false</WillWipeDisk>
     <ModifyPartitions>
      <ModifyPartition>
      <Order>1</Order>
      <PartitionID>1</PartitionID>
      <Letter>C</Letter>
      <Label>TestOS</Label>
      <Format>NTFS</Format>
      <Active>true</Active>
      <Extend>false</Extend>
      </ModifyPartition>
     </ModifyPartitions>
    </Disk>
   </DiskConfiguration>
  </component>
  <component name="Microsoft-Windows-International-Core-WinPE" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" processorArchitecture="x86">
   <SetupUILanguage>
   <WillShowUI>OnError</WillShowUI>
   <UILanguage>en-US</UILanguage>
   </SetupUILanguage>
   <UILanguage>en-US</UILanguage>
  </component>
 </settings>
</unattend>
```

Posiadany plik unattend.xml, można powiązać z usługą WDS na trzech poziomach.

Architektury – wszystkie komputery o danej architekturze sprzętowej (x86, x64 lub ia64), będą korzystały z wspólnych ustawień instalacji niepilnowanej.

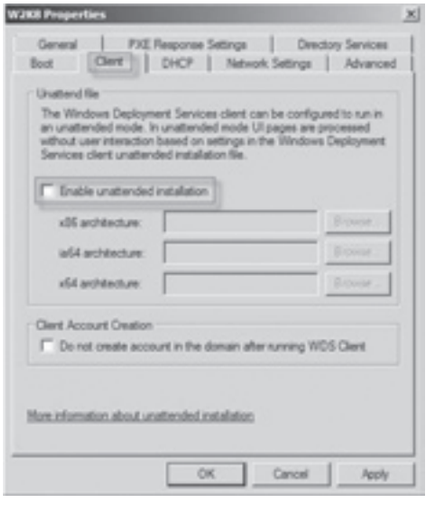
Konfigurując tą funkcjonalność za pomocą konsoli MMC należy:

Skopiować plik Unattend.xml do folderu RemoteInstall\WDSClientUnattend na serwerze WDS.

- W konsoli usługi WDS kliknąć prawym przyciskiem myszy wybrany serwer i poleceniem Properties wejść w jego właściwości

W oknie właściwości serwera w zakładce **Client** wybrać opcję **Enable unattended installation**

- Wskazać pliki unattend.xml dla poszczególnych architektur



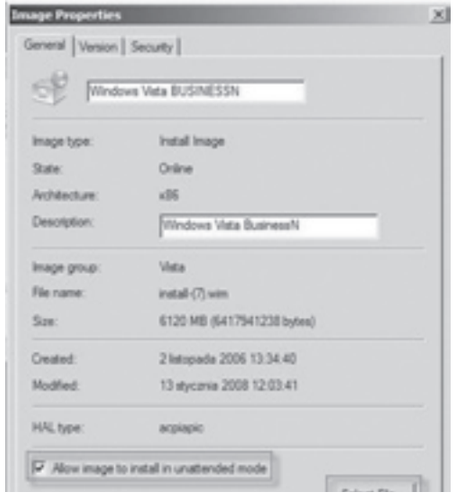
Natomiast korzystając z wiersza poleceń należy wprowadzić polecenie:

WDSUTIL /set-server /wdsunattend /policy:enabled /file:<ścieżka_do_pliku> / architecture:<arch>

Gdzie:
<ścieżka_do_pliku> – ścieżka do pliku unattend.xml
<arch> – rodzaj architektury (x86, x64, lub ia64)

Obrazu instalacyjnego – każde urządzenie korzystające z danego obrazu będzie stosowało ustawienia zawarte w pliku instalacji niepilnowanej.
W konsoli MMC należy:

- W konsoli MMC usługi Windows Deployment Services rozwinąć grupę obrazów instalacyjnych danego serwera WDS.
- Prawym przyciskiem myszy kliknąć wybrany obraz i wybrać Properites
- Zaznaczyć opcję Allow image to install in unattend mode.
- Wybrać Select File.
- Wprowadzić nazwę i ścieżkę pliku unattend.xml



Ta sama operacja ma następującą postać w linii poleceń:

WDSUTIL /Set-Image /Image:<nazwa_obrazu> **/ImageType:install / ImageGroup:**<nazwa_grupy_obrazów> **/UnattendFile:<**ścieżka_do_pliku**>**

Gdzie:
<nazwa_obrazu> – to nazwa obrazu z którym powiązany będzie plik unattend
<nazwa_grupy_obrazów> – to nazwa grupy obrazów w której znajduje się obraz przeznaczony do skojarzenia z plikiem unattend
<ścieżka_do_pliku> – ścieżka do pliku unattend.xml

Indywidualnego komputera – jeżeli zaistnieje taka potrzeba można indywidualnie skojarzyć dany plik odpowiedzi z konkretnym urządzeniem. Komputer ten rozpoznany będzie na podstawie unikalnego identyfikatora GUID, lub adresu MAC jego karty sieciowej. Realizuje się to za pomocą komendy:

WDSUTIL /set-device /device:<computername> /ID:<GUID lub adres MAC> / WdsClientUnattend:<ścieżka_do_pliku>

Gdzie:
<GUID lub adres MAC> – to identyfikator danego urządzenia
<ścieżka_do_pliku> – to ścieżka do pliku unattend

Dystrybucja obrazów systemowych za pomocą technologii Multicast
W sytuacji kiedy istnieje potrzeba jednoczesnej dystrybucji systemów operacyjnych do dużej liczby urządzeń, można skorzystać z transmisji typu Multicast, będącej jedną z nowości zawartych w usłudze WDS. Ten sposób komunikowania się z klientami usługi WDS możliwy jest tylko w sieciach wspierających Multicasting i tylko przy wykorzystaniu obrazu rozruchowego pobranego z nośnika systemu Windows Server 2008.

Rozwiązanie to pozwala na pozbycie się ograniczeń związanych z przepustowością sieci – przy standardowym sposobie dystrybucji obrazów wykorzystując sieć Gigabit Ethernet maksymalna liczba jednoczesnych instalacji nie przekroczy ze względów wydajnościowych 75-ciu urządzeń.

Usługa WDS daje możliwość skorzystania z dystrybucji multicastowej na dwóch poziomach funkcjonalności:

Auto-Cast
W tym trybie usługa multicast rozpoczyna natychmiastową obsługę klientów

Scheduled-Cast
Ten rodzaj transmisji daje możliwość określenia momentu rozpoczęcia rozgłaszania obrazów systemów operacyjnych, oraz ustalenia limitu maksymalnej liczby odbiorców usługi. W tym trybie tylko stacje zgłaszające potrzebę instalacji systemu przed rozpoczęciem transmisji zostaną obsłużone.

Konfiguracja transmisji multicast odbywać się może zarówno za pomocą konsoli MMC, jak i linii komend.
W pierwszym wypadku należy w konsoli WDS:

- Rozwinąć menu serwera WDS.
- W folderze Install Images wybrać obraz instalacyjny, który ma być dystrybuowany technologią multicast, a następnie kliknąć na niego prawym przyciskiem myszki.
- Wybrać z menu polecenie Create Multicast Transmission
- Za pomocą kreatora określić rodzaj transmisji

Za pomocą polecenia WDSUTIL chcąc:

- **stworzyć transmisję Auto-Cast**, należy wykonać polecenie :

WDSUTIL /New-MulticastTransmission /Image:<nazwa_obrazu> / FriendlyName:<nazwa> /ImageType:Install /ImageGroup:<Image group name> / TransmissionType:AutoCast

- **stworzyć transmisję Scheduled-Cast**, należy wykonać polecenie:

WDSUTIL /New-MulticastTransmission /Image:<nazwa_obrazu> / FriendlyName:<nazwa> /ImageType:Install /ImageGroup:<Image group name> / TransmissionType:ScheduledCast [/Time:<yyyy/mm/dd:hh:mm>][/Clients:<liczba_ klientów>]

Gdzie:
<nazwa_obrazu> – to nazwa obrazu przeznaczonego do dystrybucji metodą multicast
<nazwa> – nazwa wyświetlana, identyfikująca daną transmisję
<nazwa_grupy_obrazów> – to nazwa grupy obrazów w której znajduje się obraz przeznaczony do dystrybucji metodą multicast
<liczba_klientów> – maksymalna liczba obsługiwanych klientów

W każdej chwili możliwe jest bieżące monitorowanie postępu instalacji obrazów systemowych dystrybuowanych usługą multicast.

W konsoli MMC usługi WDS bieżąca aktywność widoczna jest w folderze Multicast Transmissions Natomiast z poziomu linii poleceń służy do tego komenda,

WDSUTIL /Get-MulticastTransmission /Image:<nazwa_obrazu> /ImageType:Install / ImageGroup:<nazwa_grupy_obrazów> /show:clients

Dodatkowo dostępne są również funkcje pozwalające na wstrzymanie i wznowienie transmisji w dowolnym momencie:

- **uruchomienie transmisji**

WDSUTIL /Start-MulticastTransmission /Image:<nazwa_obrazu> /ImageType:Install / ImageGroup:<nazwa_grupy_obrazów>

- **usunięcie transmisji**

WDSUTIL /Remove-MulticastTransmission /Image:<nazwa_obrazu> / ImageType:Install /ImageGroup:<nazwa_grupy_obrazów> /Force

- **deaktywacja transmisji:**

WDSUTIL /Remove-MulticastTransmission /Image:<nazwa_obrazu> / ImageType:Install /ImageGroup:<nazwa_grupy_obrazów>

- **właściwości transmisji**

WDSUTIL /Get-MulticastTransmission /Image:<nazwa_obrazu> /ImageType:Install / ImageGroup:<nazwa_grupy_obrazów>

Gdzie:
<nazwa_obrazu> – to nazwa obrazu dystrybuowanego metodą multicast
<nazwa_grupy_obrazów> – to nazwa grupy obrazów w której znajduje się obraz dystrybuowany metodą multicast

Optymalizacja transmisji multicast
Transmisja multicast dostępna w usłudze WDS, potrafi dostosowywać parametry swojej pracy do jakości posiadanego transportu sieciowego. Posiada zróżnicowane profile działania dla konfiguracji sieci 10 Mb, 100 Mb i 1 Gb.

Nie zawsze jednak standardowe ustawienia będą optymalne dla transmisji w danym środowisku sieciowym. W wypadku konieczności dopasowania parametrów transmisji, można skorzystać z profilu typu custom, umożliwiającego dowolną konfigurację transportu multicast.

Uruchomienie profile custom następuje po wykonaniu następującej komendy:

WDSUTIL /set-server / transport /profile:custom.

Natomiast parametry należy edytować za pomocą rejestru w kluczu znajdującym się na serwerze WDS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WDSServer\Providers\ WDSMC\Profiles\Custom

Najważniejsze z parametrów to:

TpMaxBandwidth
Wartość ta określa maksymalne procentowe wykorzystanie przepustowości interfejsów sieciowych zainstalowanych na serwerze WDS. Ustawienie to funkcjonuje prawidłowo, nawet jeżeli interfejsy te pracują z różną prędkością.

ApBlockSize
Ta wartość określa rozmiar bloków na które dzielona jest przesyłana informacja. Rozmiar ten definiowany jest w bajtach. Rekomendowane ustawienia to 4096 bajtów. Zwiększenie tej wartości powoduje przyspieszenie transferu, jakkolwiek zwiększa się ryzyko utraty przesyłanego pakietu.

TpMulticastTTL
Wartość TTL oznacza liczbę maksymalnych przeskoków (hops) po których pakiet zostanie odrzucony. Przeskoki odnoszą się do komunikacji poprzez urządzenia sieciowe. Ograniczanie tej wartości ma sens w przypadku potrzeby zawężenia dystrybucji do określonego obszaru sieci.

Należy pamiętać, że zmiana określonego parametru wymaga restartu usługi WDS.

ABC CENTRUM EDUKACYJNE DATA

2. Usługa wirtualizacji systemów operacyjnych

Wstęp

Dzisiejsze systemy informatyczne przedsiębiorstw to skomplikowane systemy składające się z dużej ilości serwerów, systemów operacyjnych i aplikacji i każdy z tych elementów musi być dostępny w odpowiednim czasie dla użytkowników i ich stacji roboczych. To powoduje, że dla działów IT zarządzanie i utrzymywanie krytycznych dla biznesu technologii to jedno z najważniejszych wyzwań. Jednym z rozwiązań tego problemu jest technologia wirtualizacji, która umożliwia konsolidację infrastruktury serwerowej do środowiska maszyn wirtualnych, działających na jednym serwerze rzeczywistym. Zastosowanie wirtualizacji umożliwia administratorom zminimalizować ilość serwerów rzeczywistych w sieci z zachowaniem separacji ról przy równoczesnym zmniejszeniu kosztów związanych z utrzymaniem systemów informatycznych. Wymienione korzyści wirtualizacji pozycjonują ją, jako jedną z najbardziej interesujących technologii dla przedsiębiorstw w następnych latach.

Korzyści z wirtualizacji

Windows Server® 2008 zawiera technologię wirtualizacji Hyper-V, która posiada wiele możliwości, które spowodują, że działy IT oraz przedsiębiorstwa mogą odczuć wiele korzyści z jej zastosowania, bez dodatkowych zakupów i wdrożeń oprogramowania firm trzecich.

Korzyści z wirtualizacji:

Konsolidacja serwerów – dzięki możliwości uruchomienia podstawowych serwerów np. DNS, DHCP, Active Directory, Exchange na pojedynczym serwerze możemy oczekiwać oszczędności z zmniejszonego zapotrzebowania na sprzęt przy wzrastającym zapotrzebowaniu na ilość serwerów dostępnych przez sieć przedsiębiorstwa.

Separacja ról serwerów – ta możliwość wpływa znacząco na dostępność podstawowych serwerów jak i powoduje, że infrastruktura jest bardziej odporna na błędy. Posiadając serwery np. DNS, DHCP, Active Directory na poszczególnych serwerach wirtualnych możemy oczekiwać sprawniejszego zarządzania i rozwiązywania problemów.

Testowanie oprogramowania – dzięki wirtualizacji oprogramowanie może być przetestowane w sposób nie możliwy lub trudny do uzyskania w sieci produkcyjnej. Technologia pozwala na łagodne przejście na nowsze technologie bez ryzyka, że technologie te są nieprzetestowane w warunkach produkcyjnych.

Zwiększenie dostępności serwerów przy awariach – w momencie uszkodzenia fizycznego serwera możliwość uruchomienia wirtualnych maszyn z podstawowymi dla przedsiębiorstwa aplikacjami i usługami, na właściwie dowolnym serwerze powoduje ze infrastruktura firmowa jest bardziej odporna na błędy.

Zmniejszenie kosztów infrastruktury – koszty serwerów fizycznych można zmniejszyć nawet 5 krotnie a jeśli wziąć pod uwagę coraz większe skomplikowanie infrastruktury przedsiębiorstwa, korzyści są jeszcze większe.

Skalowalność rozwiązań – dzięki wirtualizacji możemy stopniowo przyspieszać naszą infrastrukturę w zależności od posiadanych możliwości finansowych przedsiębiorstwa i rozwijać ją zgodnie z zwiększającymi się wymaganiami funkcjonalnymi.

Usługi wirtualizacji Windows Server 2008

Technologia wirtualizacji jest obecna w produktach Microsoft od lat. Już dziś wiele firm wykorzystuje tą technologię w środowisku produkcyjnym. Produkty takie jak Microsoft Virtual Server 2005 oferują rozwiązania, które spopularyzowały tą technologię. Firmy wykorzystują wirtualizacje między innymi do konsolidacji serwerów, w tej dziedzinie zwrot inwestycji z wdrożenia jest największy, dlatego tak ważne było stworzenie środowiska, którego możliwości są ściśle powiązane z wydajnością i a z drugiej strony łatwością wdrożenia i zarządzania. Jednym z podstawowych właściwości, jaka oczekiwał rynek to wydajność, jaką daje wirtualizacja w połączeniu ze sprzętową platformą 64-bitową. Rozwiązania 64-bitów dają możliwości, które powodują, że dla większości zastosowań i użytkowników nie ma różnicy w wydajności w dostępie do usług i danych poprzez sieć. Z punktu widzenia administratora natomiast wirtualizacja daje korzyści, które trudno przecenić, np. możliwość przenoszenie serwerów na inną platformę sprzętową, trwa kilka minut, dokładnie tyle ile przegranie plików .vhd. To wszystko powoduję, że wirtualizacja jest kluczową cechą, Windows 2008. To właśnie ta technologia będzie kluczową dla rynku, IT w następnych latach

Elastyczne możliwości wirtualizacji

Technologia wirtualizacji Windows 2008 jest częścią szerszej strategii dostępu stacji roboczych do centrów danych, która to pozwala odczuć korzyści z wirtualizacji na każdym poziome infrastruktury przedsiębiorstwa. Co więcej model ten łatwo również zaadaptować dla dużych rozwiązań central firm aż po korzyści z wirtualizacji w oddziałach zdalnych czy mniejszych firmach.

W dzisiejszych czasach gdzie świat IT staje się coraz bardziej skomplikowany, nasze zapotrzebowanie na wyspecjalizowane serwery rośnie coraz mocnej. Nasze serwerownie są często przeładowane nowoczesnym hardwarem, wykorzystującym najnowsze technologie, które wydajność dzisiejszych serwerów i zasoby którymi zarządzają, przewyższają możliwości dzisiejszego software. Ten moment jest doskonałym punktem do zastosowania np. konsolidacji serwerów w naszych sieciach.

Kluczowe funkcje wirtualizacji systemu Windows Server

Nowa i ulepszona architektura. Nowa 64-bitowa architektura hypervisor z zastosowaniem technologii mikrojądra umożliwia rozszerzenie obsługi urządzeń oraz zwiększenie wydajności i skuteczności zabezpieczeń przy użyciu wirtualizacji Windows.

Obsługa wielu systemów operacyjnych. Rozszerzona obsługa równocześnie uruchamianych systemów operacyjnych różnego typu, z systemami 32-bitowymi i 64-bitowymi włącznie, na różnych platformach serwerów, takich jak Windows, Linux i inne.

Obsługa symetrycznego przetwarzania wieloprocesorowego. Obsługa nawet 4 procesorów w środowisku maszyny wirtualnej umożliwia pełne wykorzystanie możliwości aplikacji wielowątkowych na maszynie wirtualnej.

Obsługa pamięci. Uwzględniając obsługę dużych przydziałów pamięci dla maszyny wirtualnej, umożliwiającą wirtualizację dla większości poziomów obciążenia, można uznać wirtualizację systemu Windows Server za optymalną platformę dla dużych przedsiębiorstw oraz małych i średnich firm.

Ulepszony dostęp do magazynu. Dostęp do dysków z przekazywaniem oraz rozszerzona obsługa sieci magazynowania (SAN) i dostępu do dysków wewnętrznych to czynniki zapewniające większą elastyczność wirtualizacji systemu Windows Server w zakresie optymalnej konfiguracji i wykorzystania środowisk magazynowania.

Równoważenie obciążenia sieciowego. Wirtualizacja systemu Windows Server oferuje nowe funkcje przełącznika wirtualnego. Maszyny wirtualne można więc łatwo konfigurować do uruchamiania z równoważeniem obciążenia sieciowego systemu Windows w celu równoważenia obciążenia maszyn wirtualnych na różnych serwerach.

Nowa architektura udostępniania sprzętu. Nowa architektura wirtualnego dostawcy/ klienta usług (VSP/VSC) wirtualizacji systemu Windows Server zapewnia sprawniejszy dostęp do podstawowych zasobów, takich jak dysk, sieć, karta wideo itp., oraz lepsze wykorzystanie tych zasobów.

Szybka migracja. Wirtualizacja systemu Windows Server umożliwia szybką migrację uruchomionej maszyny wirtualnej na inny fizyczny system hosta przy minimalnym przestoju – za pomocą znanych, zapewniających wysoki poziom dostępności funkcji systemu Windows Server i narzędzi do zarządzania pakietu System Center.

Kopia stanu maszyny wirtualnej. Wirtualizacja systemu Windows Server umożliwia wykonywanie kopii stanu uruchomionej maszyny wirtualnej, ułatwiających przywrócenie poprzedniego stanu i usprawnienie całego rozwiązania w zakresie wykonywania kopii zapasowych i odzyskiwania.

Skalowalność. Korzystając z obsługi wielu procesorów i rdzeni na poziomie hosta oraz ulepszonego dostępu do pamięci w ramach maszyn wirtualnych, można skalować środowisko wirtualizacji „pionowo" w celu obsługi dużej liczby maszyn wirtualnych na danym hoście i kontynuować skalowanie na wielu hostach przy użyciu funkcji szybkiej migracji.

Możliwości rozbudowy. Korzystając ze zgodnych ze standardami interfejsów WMI i API wirtualizacji systemu Windows Server, niezależni dostawcy i deweloperzy oprogramowania mogą szybko opracowywać niestandardowe narzędzia i ulepszenia platformy wirtualizacji.

Wirtualizacja Windows Serwer 2008 jako składowa strategii Microsoft's Datacenter-to-desktop Virtualization

W śród wielu rozwiązań wirtualizacyjnych dostępnych na rynku, oferta firmy Microsoft cechuje się kompleksowym rozwiązaniem umożliwiającym maksymalne wykorzystanie korzyści wynikających z zastosowania technologii wirtualizacji w przedsiębiorstwie. Wirtualizacja Serwerowa dostępna w Windows Server 2008 jest integralną częścią promowanej przez firmę strategii o nazwie "The Microsoft datacenter-to-desktop virtualization". Poniżej zwięźle omówione zostaną różne komponenty stanowiące rodzinę technologii wirtualizacji objętych strategią Microsoft. Wyjaśnione zostanie w jaki sposób technologie te wraz z wirtualizacją Windows Server 2008 powagą rozwiązać szereg problemów pojawiających się w różnych obszarach funkcjonowania system teleinformatycznego przedsiębiorstwa. Strategia wirtualizacji Microsoft składa się
z pięciu kluczowych komponentów:

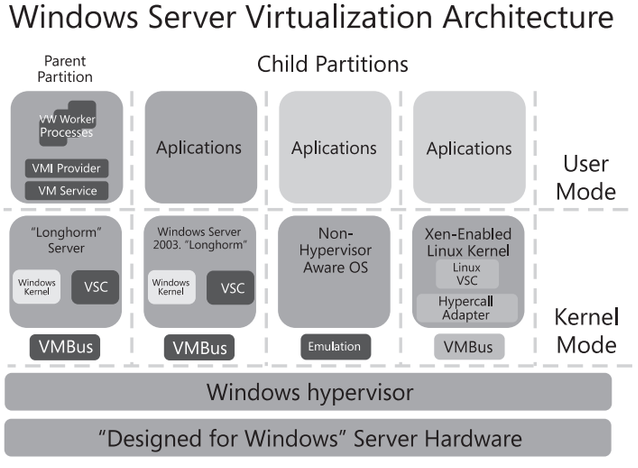
- **Wirtualizacja serwerowa (Server virtualization)**, umożliwia konsolidację wielu ról serwerów infrastrukturalnych przedsiębiorstwa do środowiska wirtualnego, w którym serwery te wykorzystywać będą zasoby fizyczne tego samego komputera
- **Wirtualizacja prezentacji (Presentation virtualization),** umożliwia użytkownikom zdalnym dostęp do wirtualnych instancji ich komputerów biurowych lub aplikacji serwerowych
- **Wirtualizacja pulpitu (Desktop virtualization),** umożliwia na stacja roboczych tworzenie środowiska testowego opartego o wiele systemów operacyjnych (ten rodzaj wirtualizacji najczęściej realizowany jest w oparciu o Microsoft Virtual PC 2007)
- **Wirtualizacja aplikacji (Application virtualization)**, jest to bardzo interesujące rozwiązanie dla przedsiębiorstw, umożliwiające zminimalizowanie występowania konfliktów aplikacji działających na tym samym komputerze. Rozwiązanie to umożliwia również dystrybucję aplikacji w przedsiębiorstwie bez konieczności jej instalowania na komputerze docelowym co znacznie poprawia stabilność stacji roboczych (produkt ten pod nazwą SoftGrid jest integralną częścią pakietu Microsoft Desktop Optimalization Package 2007)
- **Zintegrowane zarządzanie**, wszystkimi wirtualnymi komponentami przedsiębiorstwa w ramach ujednoliconego narzędzia do administrowania, monitorowania i kontroli zasobów zarówno maszyn wirtualnych jak i fizycznych.

Tabela 1 Produkty Microsoft w zastosowaniu w wirtualizacji

Produkty Microsoft	Typ wirtualizacji
Windows Server 2008	Sprzętowa wirtualizacja serwerowa
Virtual Server 2005 R2	Programowa wirtualizacja serwerowa
Terminal Services	Wirtualizacja prezentacji
SoftGrid Application Virtualization	Wirtualizacja aplikacji
Virtual PC 2007	Wirtualizacja pulpitu stacji klienckich
Windows Vista Enterprise Centralized Desktop (VECD)	Wirtualizacja pulpitu

Wirtualizacja serwerowa (Server Virtualization)

Firma Microsoft oferuje dwie technologie wirtualizacyjne dla platform serwerowych: Windows Server virtualization (WSv) na platformie Windows Server 2008 oraz obecny już od dłuższego czasu Virtual Server 2005 R2.



Wirtualizacja serwerowa realizowana w założeniu na 64-bitowych systemach operacyjnych diametralnie zwiększyła wydajność i możliwości zarządzania środowiskiem 32-bitowych maszyn wirtualnych, rozszerzyła ilość dostępnej pamięci wirtualnej dla komputerów "gości" oraz wprowadziła obsługę wielu procesorów. Wirtualizacja stała się obecnie głównym narzędziem umożliwiającym uzyskanie pełnej izolacji środowiska wirtualnego z zachowaniem korzyści wynikających z konsolidacji ról serwerowych.

Tabela 2 Porównanie możliwość Hyper-V i Virtual Servera

	Wirtualizacja Windows Server 2008 (Hyper-V)	**Virtual Server 2005 R2 SP2**
32-bit host		□
64-bit host	□	□
Wsparcie dla wielu procesorów w systemie gościa	□	
Rozszerzone narzędzia do zarządzania	□	
Hypervisor typu 1 (Wirtualizacja serwerowa hardwarowa)	□	
Wirtualizacja serwerowa softwarowa		□

Wirtualizacja prezentacji (Presentation Virtualization)

Wirtualizacja prezentacji jest technologią umożliwiającą uruchamianie aplikacji na zdalnym serwerze i prezentowanie wyników jej działania lokalnie u klienta. Technologia wirtualizacji prezentacji oraz Microsoft Terminal Services, umożliwiają użytkownikom zdalnym dostęp do środowiska pracy z sieci zewnętrznych przy zachowaniu pełnej funkcjonalności aplikacji, dostępu do zasobów oraz interfejsu aplikacji niezależnie od platformy systemowej lub zainstalowanych komponentów. Korzyści tej technologii widoczne są również dla administratorów systemowych, gdyż umożliwia im ona dostęp do narzędzi administracyjnych ze zdalnych lokalizacji lub też współdzielić je z administratorem pracującym lokalnie.

Wirtualizacja prezentacji dostarcza użytkownikom mechanizmów do centralizacji i zabezpieczania danych, redukuje koszty wdrażania i zarządzania aplikacjami, obniża koszty testowania kompatybilności aplikacji z systemem operacyjnym i potencjalnie zwiększa ogólną wydajność całego środowiska.

Wirtualizacja stacji roboczych (Desktop Virtualization)

Wirtualizacja stacji roboczych jest sytuacją kiedy technologia wirtualizacji wykorzystywana jest w środowisku stacji roboczej klienta. Istnieje wiele sytuacji, w których wirtualizacja stacji roboczych jest funkcjonalnie zbliżona do wirtualizacji serwerowej znanej z Virtual Server 2005 R2. Zbieżności te widać głównie w sytuacjach związanych z rozwiązywaniem problemów niekompatybilności aplikacji, kiedy to użytkownik musi wykorzystywać w pracy aplikację która jest niekompatybilna z jego systemem operacyjnym. W takiej sytuacji wykorzystuje się jedną z wymienionych technologii do stworzenia środowiska wirtualnego opartego o wymagany dla aplikacji system operacyjny i udostępnienie go użytkownikowi lokalnie lub poprzez sieć komputerową.

Wirtualizacja stacji roboczej jest również bardzo często wykorzystywana do budowania środowisk testowych umożliwiających analizę zachowania aplikacji w różnych systemach operacyjny oraz różną konfiguracją.

Pomimo zbieżności w funkcjonowaniu tych dwóch metod wirtualizacji należy pamiętać, że przeznaczeniem technologii Virtual Server 2005 jest konsolidacja ról serwerowych i tworzenie środowiska infrastrukturalnego, natomiast zastosowanie wirtualizacji stacji roboczych jest w głównej mierze rozwiązywanie problemów z kompatybilnością oraz budowa środowiska testowego.

Wirtualizacja aplikacji (Application Virtualization)

Wirtualizacja aplikacji pomaga w izolowaniu środowiska uruchomieniowego aplikacji od procesu instalacji w systemie operacyjnym, poprzez tworzenie specyficznej kopii środowiska (kopia rejestrów, systemu plików itp.) dla potrzeb działania aplikacji. Zastosowanie tej technologii minimalizuje koszty kładzione na testowanie zgodności aplikacji. Wykorzystując Microsoft SoftGrid, w środowisku lokalnym i sieciowym użytkownicy mogą zminimalizować czas instalacji aplikacji i wyeliminować potencjalne konflikty pomiędzy aplikacjami dając każdej z nich wirtualne środowisko dostępne wyłącznie dla nich. Dzięki oparciu aplikacji wirtualnych o abstrakcyjną warstwę dostępu do elementów systemu, mechanizm ten minimalizuje czas oraz koszty wdrażania i aktualizacji aplikacji.

Kompleksowe zarządzanie środowiskiem wirtualnym

Technologie wirtualizacji dostarczają szerokiej gamy korzyści, jednak wraz z konsolidacją komputerów do środowiska wirtualnego, staje się ono bardziej abstrakcyjne. Zwiększanie poziomu abstrakcyjności środowiska może powodować problemy administracyjne związane z zarządzaniem, monitorowaniem i analizą środowiska.

Administracja środowiskiem wirtualnym stawia przed administratorami takie same wymagania jak środowiskiem rzeczywistym, wykorzystując do tego celu te same narzędzia. Problem dostępności narzędzi do zarządzania środowiskiem zwirtualizowanym jest dość poważny i pomimo dużej ilości różnego rodzaju narzędzi dostępnych na rynku, brak jest skonsolidowanego, ujednorodnionego narzędzia administracyjnego. Z tego też powodu firma Microsoft podczas projektu nowej linii produktów położyła bardzo duży nacisk na ich stworzenie. Wraz z pojawieniem się platformy Hyper-V Windows Server 2008 oraz System Center Virtualization Manager zostały udostępnione narzędzia tak zaprojektowane, aby dostarczyć środowisku przedsiębiorstw sprawnych i wydajnych mechanizmów do zarządzania, monitorowania środowiska wirtualnego.

Posiadanie dużej ilości różnych interfejsów administracyjnych do zarządzanie środowiskiem wirtualnym powoduje problemy z monitorowaniem i diagnozą środowiska. Główną korzyścią z zastosowania System Center Virtualization Manager jest dostarczenie zintegrowanych narzędzi administracyjnych dla wszystkich składowych infrastruktury IT (w tym też infrastruktury zwirtualizowanej).

Poziom integracji narzędzi administracyjnych dostarczany przez rodzinę System Center oraz standaryzacja środowiska IT jest głównym czynnikiem minimalizacji kosztów wdrażania zarządzania i rozwiązywania problemów w przedsiębiorstwie. Stosowanie tego typu narzędzi umożliwia usprawnienie procesu szkolenia administratorów i zarządzania dynamicznie rozwijającym się środowiskiem wirtualnym. Pamiętać należy, że głównym zadaniem rozwiązań opartych o System Center jest stworzenie dynamicznie adoptowalnego środowiska IT do pojawiających się w infrastrukturze sytuacji krytycznych.

Dalsze informacje dotyczące rozwiązań wirtualizacji na platformie Windows Server oraz omówienie głównych korzyści i cech funkcjonalnych znaleźć można pod adresem www. microsoft.com/virtualization.

Identyfikacja kluczowych potrzeb biznesowych

Poniżej omówione zostaną informacje na temat w jaki sposób wirtualizacja Windows Server 2008 umożliwia wsparcie dla kluczowych potrzeb biznesowych związanych z funkcjonowaniem infrastruktury IT. Przedstawione zostaną następujące scenariusze:

- Konsolidacja serwerów
- Utrzymanie ciągłości procesu biznesowego i mechanizmy odporności na awarie
- Testowanie i rozwój
- Zarządzanie oddziałami zdalnymi

Konsolidacja serwerów

Jednym z kluczowych powodów wdrożenia rozwiązań wirtualizacji w przedsiębiorstwie jest konsolidacja ról serwerowych. Dynamiczne zmiany warunków rynkowych, chęć utrzymywania przewagi w sektorze branżowym, lub konkurencyjność oferty wywiera na firmy coraz większy nacisk związany z minimalizacją kosztów. Świadome przedsiębiorstwa szybko zauważyły, że jednym z narzędzi umożliwiających obniżenie kosztów operacyjnych systemów teleinformatycznych jest uproszczenie administracji, przy równoczesnym zachowaniu elastyczności, skalowalności i bezpieczeństwa. Zachowanie tych atrybutów jest fundamentalnym założeniem konsolidacji serwerów.

Redukcja kosztów

Dzięki konsolidacji serwerów zmniejsza się ilość potrzebnych jednostek komputerowych, co powoduje główny spadek kosztów infrastruktury. Jednakże na ogólną redukcję kosztów infrastruktury wpływać będą również oszczędności wynikające ze zmniejszonego zapotrzebowania na energię elektryczną, obciążenia klimatyzatorów oraz zmniejszenie kosztów związanych z przestojami infrastruktury w sytuacjach awaryjnych. Konsolidacja zmniejsza również obszar potencjalnego ataku teleinformatycznego i umożliwia skupić większą uwagę administratorów na mniejszej ilości urządzeń serwerowych.

Umieszczenie środowiska maszyn wirtualnych na wysoko dostępnych rozwiązaniach sprzętowych w przedsiębiorstwie podnosi niezawodność, sprawność i dostępność infrastruktury przy równoczesnym zmniejszeniu kosztów infrastruktury.

Optymalizacja infrastruktury

Utylizacja sprzętu rozwiązań serwerowych w przedsiębiorstwa sięga obecnie 5%-15% ich możliwości. Tak niska utylizacja zasobów wprowadza trudności w określenie wartości bazowych i maksymalnych dla codziennej pracy serwera. Uniemożliwia to w racjonalny sposób określić rzeczywiste zapotrzebowanie system na zasoby sprzętowe. Wiele firm podejmuje decyzję o utylizacji zasobów na podstawie określenia głównych komponentów mających wpływ na realizowane przez serwer role. Decyzja o zalokowaniu zasobów serwera podejmowana jest na podstawie pomiaru obciążenia dla procesora CPU, dostępu do dysku, zajętości RAM i obciążenia interfejsu sieciowego. Prowadzona w ten sposób analiza pokazuje, że serwery posiadają zasoby, które może wykorzystać technologia wirtualizacji. Dzięki takiemu podejściu możliwe jest maksymalne wykorzystanie zasobów sprzętowych w przedsiębiorstwie z równoczesną realizacją oczekiwań działów IT w stosunku do rozwoju infrastruktury.

Pomiar wydajności środowiska serwerowego może być realizowany w oparciu o narzędzia systemowe tj. Monitor Wydajności lub przez dedykowane do tego celu narzędzia infrastrukturalne takie jak System Center Operations Manager.

Elastyczność

Nowa architektura wirtualizacji Windows Server 2008 dostarcza elastycznych mechanizmów zarządzania skonsolidowanym środowiskiem serwerowym. Przez udostępnienie maszynom wirtualnym rozszerzonych zasobów sprzętowych takich jak wielordzeniowe procesory, usprawniony dostęp do dysku twardego czy też rozszerzenie przestrzeni adresowych pamięci RAM, wirtualizacja serwerowa Windows Server 2008 znacznie zwiększyła wydajność i skalowalność platform wirtualizacji. W połączeniu z pozostałymi możliwościami Windows Serwer 2008, mechanizmy wirtualizacji umożliwiają obecnie optymalizację obciążenia systemów zarówno 32 jak i 64-bitowych na jednym systemie rzeczywistym. Nowe mechanizmy wirtualizacji takie jak Hyper-V umożliwiają zmniejszenie odciążenia maszyn 32-bitowych przez wykorzystanie cech środowiska 64-bitowego.

Ciągłość działania procesów biznesowych i oporność na awarie

Wdrażanie mechanizmów zapewnienia ciągłości działania jest konieczne, aby zminimalizować czas przerw funkcjonowania infrastruktury sieciowej przedsiębiorstwa, zarówno tych

planowanych, jaki tych nieplanowanych,. Proces ten obejmuje czas, który jest przeznaczony zarówno na podstawowe czynności administracyjne, takie jak zarządzanie i wykonywanie kopii zapasowych. Wirtualizacja w Windows Server 2008 jest doskonałym rozwiązaniem dla zapewnienia ciągłości działania, sprawia, że czas pracy serwera bez awarii, a co za tym idzie, czas dostarczania określonych usług biznesowych, został znacznie wydłużony. Odtwarzanie systemu po awariach jest kluczowym elementem w procesie ciągłości działania. Katastrofy naturalne, złośliwy kod, błędy, czy problemy w konfiguracji sprzętowej i programowej, w wielu przypadkach są w stanie zakłócić działanie usług i aplikacji do czasu, w którym administrator nie naprawi zaistniałego problemu lub odtworzy kopii zapasowej. Ważnym elementem procesu utrzymania ciągłości działania są szybkie i wiarygodne czynności, dzięki którym zminimalizuje się skutek utraty danych oraz dzięki którym możliwe jest zdalne administrowanie środowiskiem. Wirtualizacja Windows Server wspiera takie rozwiązania jak Shadow Copy Services (VSS), czyli funkcjonalność kopii zapasowych, która umożliwia odtwarzanie wirtualnych maszyn bez przerwy w działaniu. We współpracy z System Center Data Protection Manager lub innymi podobnymi technologiami kopii zapasowych partnerów Microsoft, możliwe jest przechowywanie danych w bezpieczny sposób, także w oddziałach zdalnych. W sytuacji, kiedy nastąpi awaria serwera, który nie może zostać odtworzony, administratorzy mogą w szybki sposób odtworzyć z kopii zapasowej maszynę wirtualną, zarówno w siedzibie głównej, jak i w oddziale zdalnym, dzięki temu czas przestoju jest niewielki. Co więcej, obecnie wirtualne maszyny przechowywane są w formacie VHD, dzięki temu można w bezpieczny sposób odtworzyć maszynę wirtualną w oddziale zdalnym na każdym komputerze, na którym została uruchomiona platforma Windows Server.

Monitorowanie w System Center Operations Manager, połączone z możliwościami wirtualizacji w Windows Server, umożliwia administratorom w oddziałach zdalnych dowiedzieć się, jaki jest stan serwerów w czasie rzeczywistym. Wykorzystywane są także czynności związane z administracją systemem operacyjnym, często przy wykorzystaniu skryptów administratorskich, które pozwalają na uruchomienie zadań przeciwdziałających awarii, czy zadań odtwarzania. Monitorowanie systemów jest przydatne przy planowaniu ryzyka, np. poprzez sprawdzenie, jakie minimalne możliwości musi posiadać serwer, aby nadal pozostawał użyteczny lub minimalne wymagania potrzebne do skontaktowania się z serwerem, który przejmie zarządzanie, podczas gdy obecny serwer nie jest w stanie świadczyć żadnych usług.

Jedną z ważniejszych funkcjonalności wirtualizacji Windows Server jest Quick Migration. Opcja ta została specjalnie utworzona do zwiększenia efektywności procesu ciągłości działania. W połączeniu z usługą klastrowania w Windows Server 2008, wspieraną w edycjach Enterprise i Datacenter, Quick Migration umożliwia zarządzanie usługami wysokiej dostępności dla maszyn wirtualnych (gdy jeden z serwerów ulegnie awarii, jego pracę przejmuje inny węzeł, z minimalną przerwą w działaniu w dostępie użytkowników. Opcja ta jest także przydatna, aby poprawić dostępność podczas zaplanowanego zarządzania systemem i umożliwia administratorom przeniesienie maszyn wirtualnych na inne systemy operacyjne przed dokonaniem aktualizacji sprzętowej, czy programowej na serwerze bazowym. Cechy te, jak i wiele, wiele więcej sprawiają, że wirtualizacja Windows Server staje się efektywną platformą wirtualizacji, ulepszającą proces zachowania ciągłości działania i ochrony przed awarią dla wszystkich dostępnych maszyn wirtualnych w przedsiębiorstwie, zachowując także możliwości serwera bazowego oraz pozostałych jednostek środowiska informatycznego organizacji.

Testowanie i rozwój

Testowanie i rozwój są bardzo często uważane za jedne z ważniejszych cech biznesowych przeważających na korzyść wirtualizacji. Wykorzystanie maszyn wirtualnych oraz narzędzi wspomagających ich rozwój okazuje się przydatne do testów w wirtualnym środowisku, odpowiadającym środowisku rzeczywistemu, a także zasymulowania sytuacji, które mogą zdarzyć się w przyszłości. Przykładowo, zespół programistów jest w stanie sprawdzić nowe wersje aplikacji na wielu platformach przy wielu konfiguracjach sprzętowych. Dział informatyczny może wykorzystywać wirtualne maszyny do weryfikacji działania rozwiązań wdrożonych na serwerach oraz na komputerach użytkowników. Wirtualizacja Windows Server zwiększa możliwości sprawdzania poprawności działania sprzętu, ograniczając przy tym koszty oraz, w znacznym stopniu, poprawiając zarządzanie polityką testowania oraz zwiększając obszar możliwych do przeprowadzenia testów.

Wsparcie dla innych systemów operacyjnych

Wirtualizacja Windows Server wspomaga 64-bitowe systemy operacyjne, także firm trzecich, włączając w to niektóre dystrybucje Xen+Linux, pozwalając dzięki temu na sprawdzenie jak funkcjonują aplikacje innego typu. Wirtualizacja Windows Server pozwala także na uruchomienie większości podstawowych systemów operacyjnych na maszynach 32-bitowych. Wirtualizacja Windows Server pozwala także na jednoczesną pracę 64-bitowych i 32-bitowych środowisk wirtualnych, przy wykorzystaniu których można budować wiele scenariuszy wdrożeń, wykorzystując do tego narzędzia stosowane w środowisku produkcyjnym.

Repozytoria maszyn wirtualnych

System Center Virtual Machine Manager przechowuje i zarządza maszynami wirtualnymi, które znajdują się w repozytorium. Jest to bardzo cenna funkcjonalność ze względu na testowanie i rozwój. Repozytorium może zawierać wirtualne maszyny lub szablony wirtualnych maszyn bazujące na każdym systemie operacyjnym wykorzystywanym w organizacji, umożliwiając zespołowi programistów sprawdzenie poprawności działania nowych produktów, zaraz po tym jak się pojawią, a co za tym idzie, umożliwiając także zaobserwowanie, jaki wpływ będzie miała dana aplikacja na środowisko produkcyjne, zanim w rzeczywistości aplikacja ta zostanie wdrożona.

W wielu środowiskach maszyny wirtualne są tworzone i zarządzane przez administratorów serwerów, podlegających wirtualizacji i przez nich są administrowane i dystrybuowane. Sytuacja ta tworzy niepotrzebne opóźnienia w dostarczaniu maszyn wirtualnych do zespołów testujących. Z portalem System Center Virtual Machine Self-service, zespół testujący może utworzyć lub usuwać maszyny wirtualne w zależności od potrzeb, bez włączania w to administratorów. Rolą administratorów jest kontrola przydziału zasobów dla każdego zespołu testującego, a także kontrola typów maszyn wirtualnych, które można uruchamiać,

bądź tworzyć w sieci. Wirtualizacja Windows Server stanowi platformę dla tych możliwości w oparciu o Active Directory i Group Policy. Szczegółowa kontrola zasobów w wirtualizacji Windows Server pomaga także izolować sprawdzane środowiska poprzez wykorzystanie cech takich tak VLAN.

Kopie stanu maszyn wirtualnych w procedurze testowania i wdrażania środowiska

Kopie stanu jako punkty kontrolne są bardzo cennym narzędziem w procesie odzyskiwania, testowania i rozwoju środowiska wirtualnego przedsiębiorstwa.

Procedury testowania i rozwoju zwykle wymagają od zespołu testującego czasu na instalację, reinstalację i odinstalowanie. Dzięki punktom kontrolnym w wirtualizacji Windows Server, możliwe staje się przywrócenie pierwotnego stanu maszyny wirtualnej, która została zmodyfikowana np. tej na której została zainstalowana określona aplikacja, aby zaoszczędzić czas na przywrócenie maszyny do stanu sprzed instalacji. Opcja ta sprawia, że sprawdzanie wielu konfiguracji danej aplikacji przebiega dużo szybciej, a wykorzystanie zasobów sprzętowych jest ograniczone do minimum.

Zarządzanie oddziałami zdalnymi

Infrastruktura przedsiębiorstwa oparta o oddziały zdalne stawia przed administratorami wiele wyzwań tj. wdrażanie serwerów, utrzymanie ciągłości procesów biznesowych, zdalne zarządzanie zasobami oraz uniknięcie w oddziałach zdalny użytkowników z uprawnieniami administracyjnymi.

Wirtualizacja Windows Serwer 2008 dostarcza administratorom szereg narzędzi umożliwiających zdalna administrację środowiskiem eliminując potrzebę posiadania użytkownika z uprawnieniami administracyjnym w oddziale zdalnym. Wszystkie czynności związane z utrzymaniem I konserwacją infrastruktury tj. kopie zapasowe mogą zostać całkowicie zautomatyzowane. Nowe mechanizmy zarządzania środowiskiem i auto naprawy potrafią rozwiązywać część problemów z konfiguracja maszyn wirtualnych bez udziału administratora.

Dzięki wykorzystywaniu wirtualizacji Windows Server 2008 oddziałom zdalnym przedsiębiorstw zostały udostępniane technologie dotychczas zarezerwowane dla centrów danych, tj. odporność na awarie i utrzymanie ciągłości działania, testowanie zmian konfiguracji środowiska oraz możliwość tworzenia rozwiązań wysoko dostępnych bez znacznych nakładów finansowych.

Konsolidacja serwerów w oddziałach zdalnych

Korzyści wynikające z zastosowania konsolidacji najbardziej widoczne są dla infrastruktury opartej o oddziały zdalne. Organizacja, która wykorzystuje obecnie oddziały zdalne posiada z reguły kilka serwerów które pełnią określone role takie jak serwery pocztowe, serwery plikowe, serwery fax'ów i wydruku, itp. Zbudowanie takiej infrastruktury w oddziałach zdalnych wprowadza wiele problemów administracyjnych oraz podraża ogólne koszty utrzymania infrastruktury IT przedsiębiorstwa. Dzięki konsolidacji serwerów do środowiska wirtualnego administracja staje się wydajna i bezpieczniejsza, a koszty utrzymania niższe.

Zastosowanie wirtualizacji wprowadza redukcję kosztów na poziomie planowania rozwoju infrastruktury, zakupie urządzeń, zarządzaniu i wykorzystaniu zasobów działu IT. Dzięki omówionym wcześniej narzędziom do zarządzania środowiskiem wirtualnym zdalnie możliwe jest ograniczenie ilości użytkowników z uprawnieniami administracyjnymi w oddziałach zdalnych. Wirtualna infrastruktura oddziału zdalnego wprowadza również korzyści, które już omówione zostały wcześniej w tym podręczniku.

Utrzymanie ciągłości procesu biznesowego w oddziałach zdalnych

Utrzymanie ciągłości działania procesów biznesowych w oddziałach zdalnych ma takie same wymagania jak dla organizacji skupionej w pojedynczej lokalizacji. Oczywiście w czasie projektowania takiej infrastruktury należy położyć większy nacisk na bezpieczeństwo dostępu do danych wytwarzanych, magazynowanych i przesyłanych w kanałach komunikacyjnych pomiędzy oddziałem zdalnym a centralą. Wykorzystanie wirtualizacji w infrastrukturze oddziału zdalnego umożliwi wyposażenie jej w wysokodostępne środowisko wspierające procesy biznesowe przedsiębiorstwa. Wykorzystując wirtualizację serwerową Windows 2008 utrzymanie ciągłości działania i procesu biznesowego może być realizowane przy wykorzystaniu technologii klastrowych oraz wysoko dostępnych mechanizmów wykonywania kopii i odtwarzania środowiska po awarii. W sytuacji awaryjnej w oddziale zdalnym administratorzy w centrali mogą w swoim środowisku testowym rozwiązać problem wykorzystując odpowiednio przygotowane środowisko wirtualne a następnie przesłać je do oddziału zdalnego i wdrożyć przy wykorzystaniu narzędzi zdalnej administracji.

Testowanie i wdrażanie infrastruktury oddziału zdalnego

Organizacje wykorzystujące wirtualizację dla optymalizacji infrastruktury oddziału zdalnego, z reguły budują soje laboratoria testowe w centrali, gdzie przeprowadzane są wszelkie testy związane z optymalna konfiguracją środowiska oddziału. Idea wykorzystania tego modelu została przedstawiona już w poprzedniej sekcji. Planując taki model organizacyjny należy uwzględnić sposób dystrybucji skonfigurowanego środowiska wirtualnego do oddziału zdalnego (np. wykorzystując nośniki DVD lub szybkie łącza WAN).

Zwiększenie sprawności w oddziałach zdalnych

Firma Microsoft projektują nową rodzinę serwerów Windows 2008 położyła bardzo duży nacisk na optymalizację infrastruktury opartej o oddziały zdalne. Jednym z głównych wyzwań stawianych przed infrastrukturą opartą o oddziały zdalne jest niewystarczająca przepustowość łączy WAN co często utrudnia prowadzanie czynności administracyjnych. Dostarczane wraz z środowiskiem Hyper-V i System Center Virtual Machine Manager narzędzia mają za zadanie usprawnić administrację na łączach o niskiej przepustowości. Wykorzystując w infrastrukturze przedsiębiorstwa SCVM administratorzy mogą w tym samym czasie zarządzać centralnie przesyłaniem, wdrażaniem i administracją środowiska wirtualnego w oddziałach zdalnych.

Wymagania sprzętowe i wsparcie

Windows Server wymaga:

- procesora x64,
- sprzętowej obsługi wirtualizacji i
- sprzętowej ochrony wykonywania danych.

Poniżej zestawienie elementów które są ważne dla poprawności instalacji i uruchomienia środowiska Hyper-V.

PROCESOR
Virtualizacja Hyper-V wymaga 64-bitowych procesorów z technologiami wspomagania wirtualizacji AMD-V i Intel VT. W przypadku procesorów AMD możliwe jest uruchomienie wirtualizacji na procesorach z socjet AM2 lub Athlon/Opteron Revision F.

Intel
Xeon: Procesory XEON które posiadają architekturę Core 2 DUO maja wsparcie dla wirtualizacji. Procesory te posiadają cztero cyfrowe oznaczenia np. x3220, x5355, x5320 i x 7120. Jednakże odpowiedz nie jest prosta co do innych modeli, najlepszym rozwiązaniem jest sprawdzić to na stronach porównawczych Intela http://compare.intel.com/pcc/default.aspx?familyID=5&culture=pl-PL

CORE 2 DUO: Wszystkie procesory CORE 2 DUO posiadają wsparcie Intel VT, jedynym wyjątkiem jest procesor T5500 (1.66 GHz). Jeśli nie ma wparcia dla Intel VT na komputerach z CORE 2 DUO należy sprawdzić czy posiadamy najnowszy BIOS

CORE DUO: Procesory z CORE DUO są 32 bitowe co oznacza że niemożliwe jest wsparcie dla Hyper-V. Na tej platformie sprzętowej jedynym rozwiązaniem jest wirtualizacja softwarowa czyli Microsoft Virtual Server 2005 SP1 lub Virtual PC 2007.

CORE SOLO: Procesory z CORE SOLO są 32 bitowe co oznacza że niemożliwe jest zainstalowanie systemu Windows 2008 64 bitowego a tylko ten system posiada wsparcia dla Hyper-V. Na tej platformie sprzętowej jedynym rozwiązaniem jest wirtualizacja softwarowa czyli Microsoft Virtual Server 2005 SP1 lub Virtual PC 2007.

PENTIUM D.: Ostatnie modele tej linii procesorów posiadają wsparcie dla wirtualizacji Intel VT. Jednakże odpowiedz nie jest prosta co do innych modeli, najlepszym rozwiązaniem jest sprawdzić to na stronach porównawczych Intela http://compare.intel.com/pcc/default.aspx?familyID=1&culture=pl-PL

AMD
SOCKET AM2: Wszystkie procesory tej linii posiadają wsparcie dla hardwarowej wirtualizacji AMD-V

Athlon/Opteron Rev. F: lub późniejsze posiadają wsparcie dla hardwarowej wirtualizacji AMD-V

BIOS
Poniżej opcje BIOS muszą być włączone w zależności od platformy hardwarowej:

- Platforma AMD: NX (No Execute)
- Platforma Intel: XD (eXecute Disable))
- Wsparcie dla wirtualizacji hardwarowej
  - Intel Hardware: w większości opcja to VT w BIOS-ie
  - AMD Hardware: nie ma najczęściej żadnej opcji w BIOS-ie,

Dla poprawnego działania zaleca się update do najnowszej wersji BIOS-u dostępnej dlażdanego komputera.

PAMIĘĆ
Do zastosowań wirtualizacji powinniśmy posiadać 2 GB RAM

DYSKI
Wielkość i szybkość dysku zależy od zamierzeń co do wykorzystania systemu operacyjnego wewnątrz komputera wirtualnego i ilości komputerów wirtualnych. Można przyjąć wartość 2GB dla Windows 2003 i 8 GB dla Windows 2008. Jednakże wartość uniwersalną którą należy przyjąć dla wdrożeń to 50 GB wolnej przestrzeni.

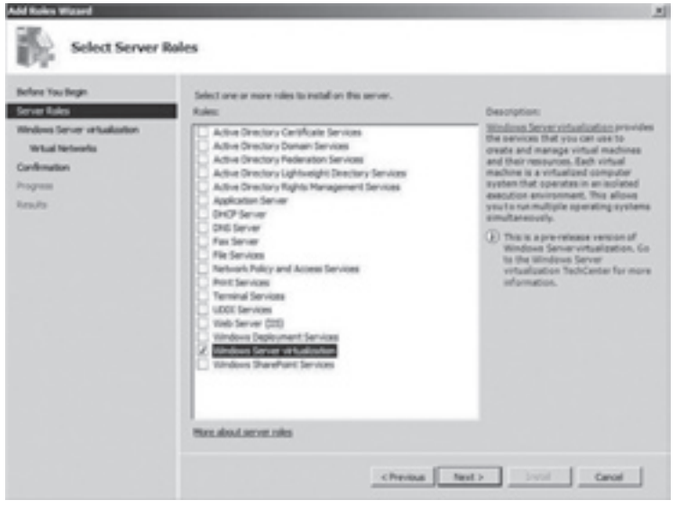
Instalacja

W systemie Windows 2008 większość usług instaluje, konfiguruje, zarządza się z jednego miejsca **Server manager.** Ta zasada również funkcjonuje dla instalacji, zarządzania usługami wirtualizacyjnymi. Dzięki. Hyper-V jest rolą serwera Windows 2008 która możemy doinstalować w pełnej instalacji Windows 2008 64- bit. Aby włączyć Hyper-V należy:

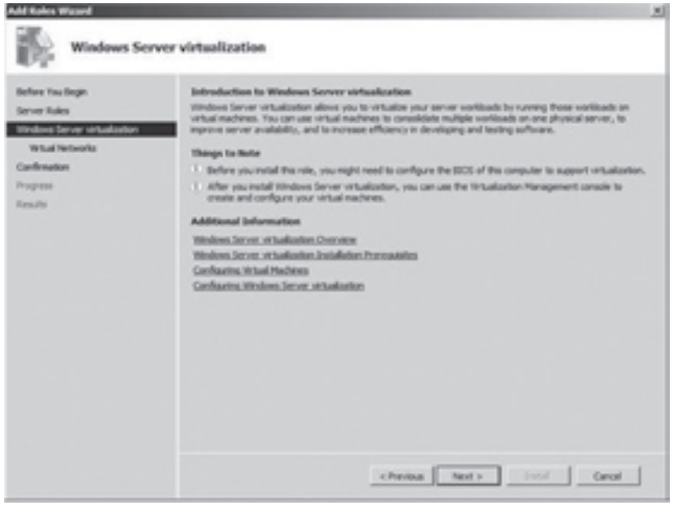
1. Przed instalacją należy się upewnić, że jest włączona sprzętowa obsługa wirtualizacji. Jeżeli wprowadzono zmiany w konfiguracji systemu BIOS w celu włączenia funkcji sprzętowych, to przed kontynuowaniem procedury należy wykonać pełną procedurę wyłączania i ponownego włączania zasilania.

2. Uruchom Menedżera serwera. Aby to zrobić, kliknij przycisk **Start**, wskaż polecenie **Administrative Tools**, a następnie kliknij polecenie **Server Manager**. Aby dodać role do serwera, należy się zalogować przy użyciu konta z uprawnieniami administracyjnymi.

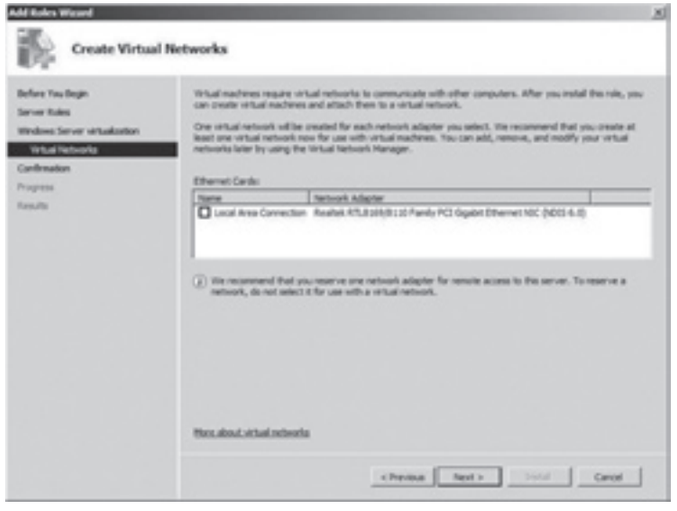
3. W **Server Manager** dodaj rolę wirtualizacji systemu Windows Server. Aby to zrobić, kliknij przycisk **Add Roles** w obszarze **Roles Summary**, a następnie wybierz opcję **Windows Server Virtualization** w kreatorze dodawania ról.



4. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby zakończyć działanie **Add Roles Wizard.**

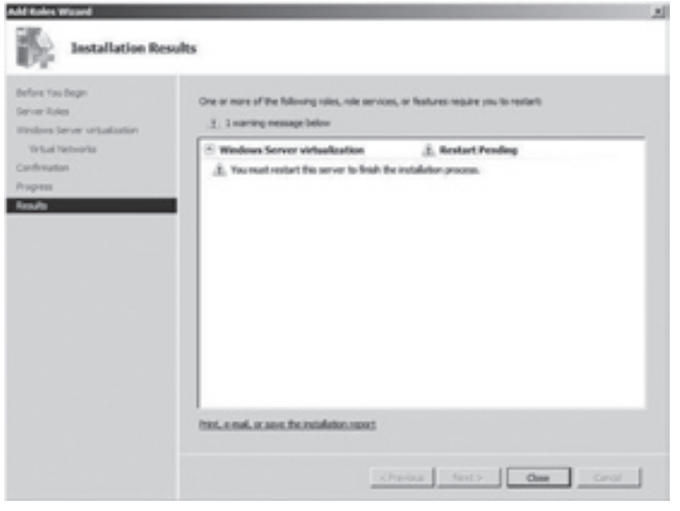


Uwaga: Opcjonalnie można zezwolić maszynom wirtualnym na dostęp do zasobów sieciowych. Co najmniej jedna karta sieciowa musi być wybrana w celu powiązania z wirtualnym przełącznikiem sieci. Jeżeli w komputerze jest zainstalowana jedna karta sieciowa, zostanie wyświetlone ostrzeżenie. Zalecane jest udostępnienie co najmniej dwóch kart sieciowych.



5. Po zakończeniu działania Kreatora dodawania ról należy ponownie uruchomić komputer, aby umożliwić włączenie roli wirtualizacji systemu Windows Server.

6. Zalecane jest wyłączenie innych ról systemu Windows Server 2008 w systemie hosta, jeżeli rola wirtualizacji systemu Windows Server jest włączona w systemie.



Ważne: po ponownym uruchomieniu należy się zalogować przy użyciu konta używanego do instalacji roli wirtualizacji systemu Windows Server zgodnie z powyższą procedurą.

Uwaga: Aby potwierdzić instalację roli wirtualizacji systemu Windows Server, należy przejść do przystawki Menedżer serwera programu MMC, rozwinąć węzeł Rolę i zaznaczyć pozycję Wirtualizacja systemu Windows Server. Należy się upewnić, że dwie usługi, „vhdsvc" i „vmms", są uruchomione.

Instalacja Hyper-V w systemie Windows 2008 CORE

W CORE czyli wersji instalacyjnej Windows 2008 pozbawionej środowiska graficznego możemy uruchomić instalacje z linii komend.

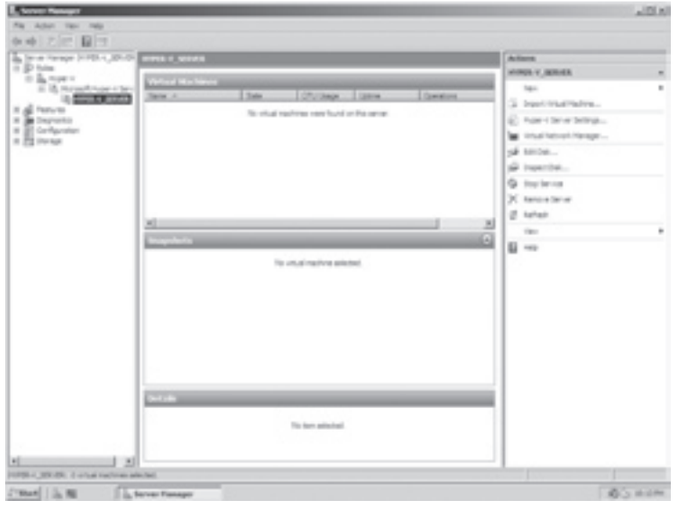
1. Wpisz "Start /w ocsetup Microsoft-Hyper-V" aby włączyć rolę Hyper-V.

2. Po zakończeniu instalacji, zrestartuj komputer

Zarządzanie wirtualizacją systemu Windows Server za pośrednictwem programu MMC

Zainstalowaną rolą wirtualizacji systemu Windows Server można zarządzać za pośrednictwem programu MMC, podobnie jak innymi rolami w systemie Windows Server 2008.

1. Należy wybrać pozycję Virtualization Management systemu Windows z folderu Administrative Tools w menu Start,.



Korzystając z tej konsoli, można zarządzać lokalnym systemem lub łączyć się z innymi serwerami i zarządzać nimi.

Korzystając z konsoli zarządzania wirtualizacją, można łatwo tworzyć nowe maszyny wirtualne, modyfikować ustawienia dla komputera-hosta i maszyny wirtualnej, zatrzymywać i uruchamiać maszyny wirtualne, wykonywać migawki itp. przy użyciu znanych kreatorów zgodnych z interfejsem systemu Windows.

Instalacja systemu Gościa na Hyper-V

Usługa wirtualizacji w Windows 2008 (Hyper-V) jest doskonałym sposobem na konsolidacje serwerów. Jeśli już usługa została skonfigurowana i działa, przyszła kolej na instalacje systemu operacyjnego systemu gościa. System operacyjny gościa naszym przykładzie Windows 2008 jednakże może być:

1. Należy wybrać pozycję **Virtualization Management** z folderu **Administrative Tools** w menu **Start**,.

2. Kliknij na **New**, który znajduje się na prawym panelu i wybierz **Virtual Machine**

3. Uruchomi się **virtual machine wizard,** w kolejnych krokach wybierz:

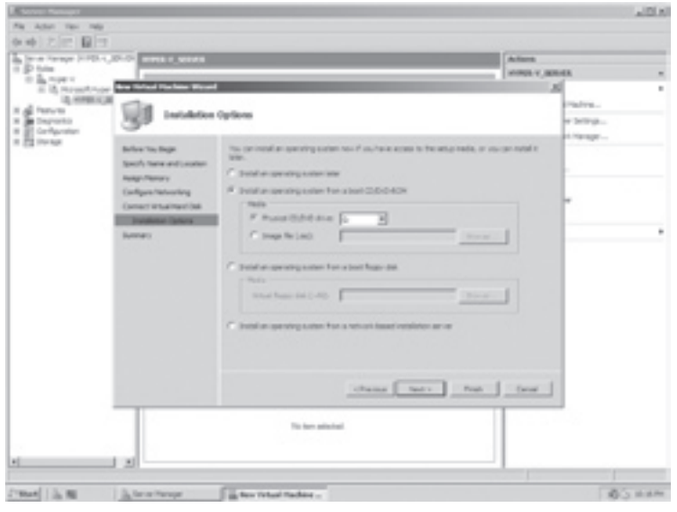
    a. Nazwę i lokalizację dla nowego komputera wirtualnego

    b. Pamięci RAM przydzielonej dla nowej maszyny – Windows 2008 wymaga do poprawnego działania 512 MB – dla sprawnego działania jeśli to możliwe wybierz 1GB.

    c. Wielkość i lokalizacje dla pliku VHD – pliku który staje się wirtualnym dyskiem tworzonej maszyny wirtualnej, domyślna wartość 127 GB jest zupełnie wystarczająca.

    d. Jeśli chcesz aby po utworzeniu maszyny wirtualnej automatycznie rozpoczął się proces instalacji systemu operacyjnego wskaż nośnik Windows 2008. Może być to nośnik fizyczny, w takim wypadku wskaż napęd a jeśli posiadasz obraz płyty DVD wskaż odpowiedni plik ISO

4. W podsumowaniu S



COMBIDATA
GRUPA PROKOM

3. Usługi terminalowe

Wprowadzenie

Zarówno firmy, jak i pracownicy są w ciągłym ruchu. Pracownicy potrzebują dostępu do kluczowych danych i aplikacji biznesowych niezależnie od miejsca, w którym się aktualnie znajdują – w samochodzie, w domu, w terenie, jak również w biurze. Firmy, które zapewniają scentralizowany dostęp do aplikacji za pomocą systemu Windows Server 2008, mogą zmniejszyć wydatki, zwiększyć produktywność i dostarczyć pracownikom narzędzi potrzebnych do osiągania sukcesów w pracy.

Zapewnienie zdalnego dostępu do aplikacji przy jednoczesnym zachowaniu bezpieczeństwa jest wyzwaniem dla specjalistów IT, a także stanowi główny cel ulepszeń scentralizowanego dostępu do aplikacji zawartego w Microsoft Windows Server 2008.

System Windows Server 2008 dodaje ulepszenia oraz innowacje do Usług Terminalowych, które ułatwiają integrację zdalnych aplikacji na komputerach klientów, zapewniają łatwy dostęp do tych samych programów za pomocą przeglądarki internetowej, jak również dostarczają środków umożliwiających dostęp do odległych terminali i aplikacji, poprzez zapory firewall, bez potrzeby otwierania dodatkowych portów.

Dzięki Windows Server 2008 organizacje są w stanie zapewnić swoim użytkownikom, zarówno tym pracującym zdalnie, jak i tym pracującym w sieci, dostęp do aplikacji zebranych i zabezpieczonych w centrum danych, przy jednoczesnym zapewnieniu spójności danych i wydajności, niezależnie od lokalizacji użytkownika.

Poniższy rozdział przedstawi zarys technologii Usług Terminalowych w Windows Server 2008, umożliwiających organizacjom:

- Zapewnienie scentralizowanego dostępu do kluczowych aplikacji biznesowych za pośrednictwem Internetu.
- Zmniejszenie ryzyka utraty danych z komputerów przenośnych poprzez wykorzystanie bezpiecznego dostępu zdalnego do centralnej bazy aplikacji i danych.
- Obniżenie kosztów zarządzania dzięki rezygnacji z serwerów aplikacyjnych w innych lokalizacjach.
- Zapewnienie bezpiecznego dostępu do Usług Terminalowych bez konieczności udostępniania pełnego dostępu do sieci poprzez Wirtualne Sieci Prywatne (VPN).

Do nowych komponentów Usług Terminalowych należą:

- Terminal Services RemoteApp. TS RemoteApp – pozwala użytkownikom na uruchomienie programów dostępu zdalnego w systemie Windows na ich pulpicie, tuż obok lokalnych aplikacji, przy użyciu nowego klienta Remote Desktop Connection w wersji 6.0 lub wyższej.
- Terminal Services Gateway. TS Gateway – poszerza zasięg Usług Terminalowych poza firmową zaporę firewall poprzez zapewnienie bezpiecznego dostępu do Usług Terminalowych oraz udostępnionych pulpitów, bez potrzeby korzystania z dodatkowej infrastruktury VPN.
- Terminal Services Web Access. TS Web Access – oferuje rozwiązanie upraszczające proces publikowania aplikacji zdalnych dla administratora, przy jednoczesnym ułatwieniu użytkownikom wyszukiwania i uruchamiania zdalnych aplikacji.
- Single Sign-on. SSO – usprawnia pracę użytkownika zdalnego dzięki wyeliminowaniu konieczności wielokrotnego uwierzytelniania.
- Terminal Services Easy Print. TS Easy Print – jest sterownikiem drukarki w Usługach Terminalowych, który usprawnia administrację w celu umożliwienia drukowania obsługiwanym klientom.
- Ulepszenia Licencyjne. Istnieje wiele ulepszeń w licencjonowaniu Usług Terminalowych, które ułatwiają zarządzanie i śledzenie licencji.

Podstawowa funkcjonalność Usług Terminalowych

Wstęp

Usługi Terminalowe w systemie Windows Server 2008 dostarczają technologii umożliwiającej użytkownikom dostęp do programów działających pod kontrolą systemu Windows, które zostały zainstalowane na serwerze terminali, lub dostęp do pulpitu systemu Windows z niemal każdego urządzenia klienckiego (np. komputera PC, laptopa, palmtopa itd.). Użytkownicy mogą łączyć się z serwerem terminali, aby korzystać z programów lub zasobów sieci dostępnych na tym serwerze.

Usługi Terminalowe pozwalają na efektywne rozmieszczenie i wykorzystanie oprogramowania w środowisku korporacyjnym. Programy mogą być instalowane w jednej, centralnej lokalizacji. Ponieważ instaluje się programy na serwerze terminali, a nie na komputerze klienta, łatwiej je później aktualizować i kontrolować.

Kiedy użytkownik korzysta z programu na serwerze terminali, wykonanie programu ma miejsce na serwerze. Jedynie akcje klawiatury, myszy i obrazy ekranu są transmitowane przez sieć. Każdy z użytkowników widzi jedynie swoją indywidualną sesję. Sesja jest zarządzana indywidualnie przez system operacyjny serwera i jest niezależna od sesji pozostałych użytkowników.

Korzyści z zastosowania Usług Terminalowych

Korzyści wynikające z użytkowania Usług Terminalowych w systemie Windows Server 2008 są różnorodne. Zaliczamy do nich:

- Szybkie wdrażanie aplikacji, które są często aktualizowane, rzadko używane lub trudne w obsłudze.
- Scentralizowany dostęp do pojedynczych aplikacji bez potrzeby korzystania z pełnego Pulpitu Zdalnego. Aplikacje uruchamiane zdalnie są zintegrowane z lokalnym pulpitem użytkownika – wyglądają i zachowują się jak lokalne aplikacje.
- Uproszczenie dostępu do aplikacji dla użytkowników, partnerów lub klientów.
- Kompleksowy model konfiguracji zabezpieczeń, który daje możliwość kontroli dostępu do zasobów w sieci korporacyjnej.
- Organizacje mogą zapewnić pracownikom dostęp do scentralizowanych aplikacji, pulpitów i źródeł z Internetu poprzez użycie HTTPS, bez konieczności konfiguracji pełnego dostępu przez Wirtualne Sieci Prywatne (VPN) lub otwierania niepożądanych portów na zaporach firewall.
- Możliwość prostego i bezpiecznego połączenia zdalnego użytkowników z serwerami terminali i zdalnymi pulpitami poprzez zapory firewall i translację adresów sieciowych (NAT).
- Optymalizacja przepustowości łącza sieciowego, która jest wymagana przy dostępie do aplikacji zdalnych.
- Lepsze działanie programu dla pracowników w biurach wydziałowych, którzy potrzebują dostępu do centralnych magazynów danych.

Kto będzie zainteresowany nowymi możliwościami Usług Terminalowych w systemie Windows Server 2008?

- Analitycy i planiści IT, szukający rozwiązań zapewniających zdalny dostęp pracownikom firmy.
- Planiści przedsięwzięć IT, architekci i projektanci pracujący dla organizacji.
- Architekci zabezpieczeń, którzy odpowiadają za wdrażanie sprawdzonych rozwiązań , spełniających kryteria Trustworthy Computing (więcej informacji na stronie http://www.microsoft.com/poland/security/twc/projekt.mspx).

- Profesjonaliści IT odpowiedzialni za serwery terminali lub zdalny dostęp do stacji roboczych.
- Profesjonaliści IT, którzy poszukują wydajnych i obniżających koszty metod instalowania aplikacji dla użytkowników.

Usługi Terminalowe w systemie Windows Server 2008 oferują funkcjonalność, która umożliwia scentralizowany dostęp do aplikacji na potrzeby różnych scenariuszy korporacyjnych.

Trzy rozszerzenia istniejących cech funkcjonalnych Usług Terminalowych systemu Windows Server 2008 mają szczególnie istotne znaczenie dla scentralizowanego dostępu do aplikacji:

- Brama Usług Terminalowych (TS Gateway) - umożliwia autoryzowanym zdalnym użytkownikom dostęp do usług terminalowych i zdalnego pulpitu wewnętrznej sieci korporacyjnej z dowolnego miejsca i urządzenia ze skonfigurowanym klientem Remote Desktop Connection 6.0. TS Gateway eliminuje potrzebę konfigurowania połączeń Wirtualnej Sieci Prywatnej (VPN), umożliwiając zdalnym użytkownikom bezpośrednie i bezpieczne połączenie do wewnętrznej sieci korporacyjnej z sieci zewnętrznej, takiej jak na przykład Internet. Jednocześnie zapewnia pełną kontrolę nad tymi połączeniami przy dostępie do poszczególnych zasobów sieci korporacyjnej.
- TS RemoteApp - funkcje TS RemoteApp są dostępne zdalnie poprzez usługi terminalowe i zachowują się tak, jakby były uruchomione na lokalnym komputerze docelowego użytkownika.
- TS Web Access - powoduje, że funkcje TS RemoteApp są dostępne dla użytkowników z przeglądarki internetowej. Za pomocą rozszerzenia TS Web Access użytkownik może odwiedzić witrynę sieci Web (zarówno z Internetu, jak i z intranetu), aby uzyskać listę dostępnych programów.

Instalacja Usług Terminalowych, konfiguracja i zarządzanie

Podstawową metodą zarządzania Usługami Terminalowymi jest Server Manager Console. To narzędzie umożliwia implementację ról niezbędnych do wsparcia Usług Terminalowych i zarządzanie właściwościami każdej roli; na przykład zarządzanie funkcją Remote Program. Role niezbędne do implementacji Usług Terminalowych na pojedynczej maszynie to:

- Usługi Terminalowe,
- Serwer plików,
- Usługi dostępu do sieci,
- Serwer Web (IIS).

Nowe cechy środowiska pracy użytkownika

Środowisko pracy użytkowników zdalnych łączących się z serwerem Usług Terminalowych Windows Server 2008 jest znacznie udoskonalone w porównaniu z wersjami poprzednimi, dzięki rozszerzeniu istniejących i dodaniu nowych funkcji:

- Wsparcie dla licznych typów wyświetlaczy i różnych rozdzielczości,
- Możliwość rozszerzenia obrazu pulpitu na kilka monitorów,
- Wsparcie dla funkcji systemu Windows Vista (Windows Media Player, motywy pulpitu, zarządzanie zdjęciami),
- Wygładzanie czcionek,
- Wsparcie dla Windows Server 2008 Audio Mixer,
- Możliwość ustawienia 32-bitowej mapy kolorów,
- Wsparcie dla kompresji połączeń RDP,
- TS Easy Print.

mechanizmy bezpieczeństwa

Znaczna poprawa bezpieczeństwa została uzyskana poprzez wykorzystanie nowych funkcji systemu Windows Server 2008, w tym:

- Uwierzytelnianie dostępu klientów do sieci,
- Pojedyncze logowanie Single Sign-in dla klientów podłączonych do domeny,
- Integracja z Credential Manager and Credential Security Support Provider (CredSSP),
- Możliwość blokowania klienta pre-RDPG,
- Izolacja sesji i bezpośrednio połączonych urządzeń,
- Udoskonalone ustawienia zabezpieczeń TS Gateway, między innymi wsparcie dla Network Access Protection (NAP), wskazówki dla przekierowywania urządzeń i monitorowanie połączeń.

Nowe mechanizmy kontroli dostępu i skalowalności

Usługi Terminalowe Windows Server 2008 zawierają wiele nowych i udoskonalonych funkcji związanych z zarządzaniem i skalowalnością, między innymi:

- Narzędzie do zarządzania rolami serwera,
- Priorytetyzacja przesyłania danych ekranowych,
- Nowe metody kompresji,
- Lepsza skalowalność bufora wydruku,
- Polepszone liczniki wydajności,

- Pełne wsparcie dla IPv6,
- Śledzenie licencji w trybie Per User,
- Pojedynczy klient Win32 i ActiveX, zintegrowany z systemem i Windows Update,
- Wsparcie dla architektury i aplikacji 64-bit,
- Wbudowana usługa UPH Clean Service.

Usługa UPH Clean Service, wydana poprzednio jako dodatek do Windows Server 2003, teraz została wbudowana zarówno do systemu Windows Server 2008, jak i do Windows Vista. UPHClean jest usługą zaprojektowaną po to, by usuwać problemy związane z nierozładowującymi się profilami użytkowników. Symptomy tych problemów to długotrwałe wylogowywanie się, nieuzgodnione profile mobilne lub przekroczony limit rozmiaru rejestru. To kluczowe dla usługi terminalowej narzędzie nie wymaga już oddzielnej instalacji, co oznacza, że jakiekolwiek aktualizacje usługi będą przeprowadzane przez Windows Updates Services, ułatwiając tym samym zarządzanie.

Wsparcie dla architektury 64-bitowej

Jednym z głównych problemów Usług Terminalowych uruchomionych na platformie Windows 32-bit jest ograniczona przestrzeń dostępna dla wirtualnej przestrzeni adresowej jądra systemu. 32-bitowy system operacyjny rezerwuje 2 GB wirtualnej przestrzeni adresowej dla struktur danych jądra. Ta wirtualna przestrzeń adresowa jest współdzielona przez wszystkie procesy uruchomione w systemie. Kiedy przestrzeń adresowa jest wyczerpana, żadne nowe procesy (lub jakiekolwiek inne obiekty systemowe) nie mogą być tworzone. To oznacza, że nowi użytkownicy nie będą w stanie się zalogować, a już zalogowani będą mieli znaczne ograniczenia wydajności.

64-bitowa architektura dostarcza znacznie większą wirtualną przestrzeń adresową dla struktur danych jądra systemu (8 terabajtów [8 TB]). Z tego punktu widzenia 64-bitowa architektura będzie normalnie zapewniać więcej połączeń użytkowników.

Jest wskazane, aby zawsze uruchamiać Usługi Terminalowe Windows Server 2008 na 64-bitowej architekturze, w celu uzyskania lepszej skalowalności i znacząco większej wirtualnej przestrzeni adresowej.

Usługi Terminalowe systemu Windows Server 2008 uruchomione w 64-bitowym środowisku oferują następującą funkcjonalność:

- Uruchamiają 32-bitowe oprogramowanie bez potrzeby jego rekompilowania.
- Obsługują 64-bitowe sterowniki i oprogramowanie skompilowane dla zestawu instrukcji x64.
- Uruchamiają 32-bitowe aplikacje, zdolne do pracy w większej przestrzeni adresowej (large memory aware) i wymagające większej wydajności w przestrzeni adresowej 4GB.
- Uruchamiają 64-bitowe aplikacje w wirtualnej przestrzeni adresowej 8 TB.
- Ułatwiają migrację do 64-bitowej infrastruktury.

Instalacja i konfiguracja

Rola serwera Usług Terminalowych, znana wcześniej jako komponent serwera Usług Terminalowych w Windows Server 2003, umożliwia systemowi Windows Server 2008 udostępnianie pojedynczych aplikacji zgodnych z systemem Windows lub pełnego pulpitu systemu Windows. Usługi Terminalowe są rolą serwera składającą się z kilku podkomponentów, które można oznaczyć jako „usługi ról".

W systemie Windows Server 2008 na Usługi Terminalowe składają się następujące usługi ról:

- *Serwer Terminali.* Rola Serwera Terminali umożliwia udostępnianie programów zgodnych z systemem Windows lub całego pulpitu Windows.
- *TS Licensing*. Terminal Services Licensing (TS Licensing) zarządza licencjami dostępowymi klienta Usług Terminalowych (TS CALs), które są wymagane do połączenia z serwerem terminalowym.
- *TS Session Broker*. Terminal Services Session Broker pozwala użytkownikowi na ponowne połączenie z serwerem, który zawiera bieżącą sesję, w przypadku korzystania z technik równoważenia obciążenia i farmy serwerów. TS Session Broker równoważy obciążenia, nawet jeśli inne mechanizmy równoważenia obciążenia nie są stosowane. Pozwala także wygaszać sesje terminalowe na sewerach terminali, które mają być poddane przeglądowi okresowemu.

Jeśli użytkownik przerwie sesję (niezależnie od tego, czy miał taki zamiar, czy też wynika to z awarii sieci), aplikacje będą nadal działały. Kiedy ponownie się połączy, TS Session Broker roześle zapytanie, aby ustalić, czy ma on działającą sesję, a jeśli tak, to na którym serwerze w farmie. Jeżeli odbywa się sesja, TS Session Broker przekierowuje klienta do serwera terminali, na którym ta sesja się znajduje. Funkcjonalność ta chroni użytkownika przed rozpoczęciem nowej sesji, jeśli istnieje już rozpoczęta, lecz przerwana sesja.

- *Brama Usług Terminalowych (TS Gateway).* Brama Usług Terminalowych pomaga zapewnić bezpieczne połączenie zdalne z serwerami terminali i zdalnymi pulpitami w sieci korporacyjnej z każdego miejsca w Internecie.
- *TS Web Access.* Dostęp Internetowy dla Usług Terminalowych (TS Web Access) pozwala użytkownikom na dostęp do zdalnych programów za pośrednictwem protokołów internetowych.

Po zainstalowaniu usług na serwerze terminali, aby zakończyć konfigurację Usług Terminalowych, administratorzy muszą podjąć następujące kroki:

- Zainstalować aplikacje na serwerze.
- Skonfigurować ustawienia zdalnego połączenia (określając użytkowników i grupy, które potrzebują połączenia z serwerem terminali).
- Rozważyć umieszczenie indywidualnych programów na oddzielnych serwerach terminali w następujących przypadkach:
  - Jeśli program posiada problemy z kompatybilnością, które mogą wpłynąć na inne programy.
  - Jeśli parametry aplikacji lub liczba użytkowników korzystających z aplikacji wymaga pełnej wydajności serwera.
- Skonfigurować klientów do korzystania z Usług Terminalowych.

Uwierzytelnianie

Windows Server 2008 wspiera Network Level Authentication, Server Authentication oraz Single Sign-on, kiedy łączymy się z serwerem terminali z serwera Windows Server 2008 , klienta Windows Vista lub z Windows XP Service Pack 2 z aktualizacją RDC 6.0.

- *Network Level Authentication* jest nową metodą uwierzytelniania, która pozwala na zakończenie uwierzytelniania użytkownika, zanim zostanie ustanowione pełne połączenie z Pulpitem Zdalnym i zanim pojawi się ekran logowania.
  Korzyści z Network Level Authentication to:
  - Wymaga mniej zasobów zdalnego komputera, ponieważ zdalny komputer wykorzystuje tylko ograniczone zasoby serwera terminali przed uwierzytelnieniem użytkownika. We wcześniejszych wersjach komputer zdalny od razu nawiązywał pełne połączenie Pulpitu Zdalnego.
  - Pomaga uzyskać większe bezpieczeństwo poprzez redukowanie ryzyka ataku blokującego usługę (Denial of Service).
  - Używa identyfikacji zdalnego komputera, co pomaga ochronić użytkowników przed połączeniem ze zdalnymi komputerami podającymi nieprawdziwą tożsamość.
- *Server Authentication* sprawdza, czy łączymy się z właściwym zdalnym komputerem lub serwerem. To zabezpieczenie pomaga uchronić użytkownika przed połączeniem z komputerem lub serwerem innym od tego, z którym miał zamiar się połączyć. Zapobiega tym samym przypadkowemu ujawnieniu poufnych informacji. Domyślnie uwierzytelnienie serwera jest włączone dla wszystkich połączeń.

- *Single Sign-on* jest metodą uwierzytelniania, która pozwala użytkownikowi z kontem w domenie zalogować się raz, przy użyciu hasła lub karty procesorowej, a następnie uzyskać dostęp do zdalnych serwerów bez potrzeby ponownego wprowadzenia uwierzytelnień.

  Kluczowe scenariusze dla metody Single Sign-on to:
  - Wdrażanie aplikacji Linii Biznesowej (LOB),
  - Scentralizowane wdrażanie aplikacji.

Aby utrzymać niższe koszty, wiele organizacji woli instalować swoje aplikacje Linii Biznesowej (LOB) na serwerze terminali i udostępniać je poprzez TS RemoteApp lub Pulpit Zdalny. Single Sign-on pozwala użytkownikom na wygodniejsze użytkowanie, eliminując potrzebę każdorazowego wprowadzania uwierzytelnień przy rozpoczynaniu zdalnej sesji.

Aby zaimplementować funkcjonalność Single Sign-on w Usługach Terminalowych, należy się upewnić, czy spełniamy następujące wymagania:

- Z Single Sign-on można korzystać jedynie w przypadku zdalnych połączeń z komputerów działających pod kontrolą systemu Windows Vista, z serwerem terminali działającym pod kontrolą systemu Windows Server 2008, lub w przypadku zdalnych połączeń pomiędzy dwoma serwerami działającymi pod kontrolą systemu Windows Server 2008.
- Konta użytkowników, z których korzystamy, muszą mieć odpowiednie uprawnienia do logowania, zarówno na serwerze terminali, jaki i na stacji roboczej Windows Vista.
- Zarówno komputer klienta, jak i serwer terminali muszą należeć do domeny.

Przekierowanie urządzeń

Windows Server 2008 wspiera przekierowanie urządzenia dla połączeń z serwerem terminali nawiązywanych z serwera Windows Server 2008, stacji roboczej z systemem Windows Vista lub Windows XP Service Pack 2 z aktualizacją RDC 6.0.

Przekierowanie urządzeń typu Plug and Play

W systemie Windows Server 2008 przekierowywanie zostało ulepszone i rozszerzone. Aktualnie można, w połączeniu terminalowym, przekierować przenośne urządzenia zgodne z platformą Windows Portable Devices, szczególnie odtwarzacze działajace w oparciu o Media Transfer Protocol (MTP) i kamery cyfrowe działające w oparciu o Picture Transfer Protocol (PTP).

Można kontrolować przekierowanie urządzeń typu Plug and Play, wykorzystując jedno z następujących ustawień zasad grup:

- Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Device and Resource Redirection\Do not allow supported Plug and Play device redirection policy setting,
- Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions policy settings.

Można także kontrolować przekierowanie urządzeń typu Plug and Play za pomocą zakładki **Client Settings** w narzędziu **Terminal Server Configuration tool** (tsconfig.msc).

Przekierowanie urządzenia typu Plug and Play nie jest wspierane przez kaskadowe łączenia serwerów terminali. Na przykład, jeśli urządzenie typu Plug and Play jest podłączone do lokalnego komputera klienckiego, to można przekierować i użyć tego urządzenia, jeśli łączymy się z serwerem terminali (na przykład Server1). Jeśli w trakcie zdalnej sesji na serwerze Server1 łączymy się z innym serwerem terminalowym (na przykład Server2), to nie będziemy mogli przekierować i używać urządzenia typu Plug and Play podczas zdalnej sesji na serwerze Server2.

Windows Embedded for Point of Service Device Redirection

W systemie Windows Server 2008 można przekierować urządzenia działające pod kontrolą Windows Embedded for Point of Service, korzystające z Microsoft POS dla .NET 1.1.

Przekierowanie urządzenia działającego pod kontrolą Windows Embedded for Point of Service jest wspierane, jeśli serwer terminali działa na wersji Windows Server 2008 przeznaczonej dla architektury x86. Aby uzyskać więcej informacji, sprawdź hasło Windows Embedded for Point of Service na stronie Microsoftu (http://go.microsoft.com/fwlink/?LinkId=67182). Można pobrać Microsoft POS for .NET 1.1 z Microsoft Download Center na stronie (http://go.microsoft.com/fwlink/?linkid=66169).

Aby uaktywnić przekierowanie dla urządzeń działających pod kontrolą systemu Windows Embedded for Point of Service, należy wykonać następujące czynności:

- Zainstalować Microsoft POS for .NET 1.1 na własnym serwerze terminali.
- Skonfigurować plik Remote Desktop Protocol (.rdp).

Urządzenia działające pod kontrolą systemu Windows Embedded for Point of Service domyślnie nie są wymienione w zakładce Local Resources w Remote Desktop Connection. Dlatego, aby umożliwić przekierowanie urządzeń Windows Embedded for Point of Service, należy edytować plik Remote Desktop Protocol (.rdp), którego używamy do połączenia z serwerem terminali. Aby zasięgnąć informacji o ustawieniach pliku .rdp, należy sprawdzić ustawienia Remote Desktop Protocol w Windows Server 2003 i w Windows XP (http://gp.microsoft.com/fwlink/?linkid=66168).

- Po zaimplementowaniu Microsoft® POS for .NET 1.1 na serwerze terminali i przekierowaniu urządzenia działającego pod kontrolą systemu Windows Embedded for Point of Service w pliku .rdp należy podłączyć urządzenie Windows Embedded for Point of Service, a następnie połączyć się z komputerem zdalnym, używając zmodyfikowanego pliku .rdp. Po połączeniu z komputerem zdalnym urządzenie, które zostało przekierowane, powinno być automatycznie instalowane na komputerze zdalnym. Informacja o instalacji urządzenia typu Plug and Play pojawi się na pasku zadań komputera zdalnego.

Kiedy przekierowane urządzenie działające pod kontrolą systemu Windows Embedded Point of Services jest zainstalowane na komputerze zdalnym, każda aplikacja korzystająca z tego urządzenia, działająca na serwerze terminali, ma dostęp do urządzenia Windows Embedded Point of Services, tak jakby urządzenie to było dostępne lokalnie. Istnieje próbna aplikacja w POS dla .NET 1.1 SDK, którą można wykorzystać do przetestowania dostępu do funkcjonalności wbudowanego urządzenia POS. Aplikacja próbna to ccltestapp.exe i można ją znaleźć w folderze \SDK\Samples\Sample Application, znajdującym się w katalogu, w którym była instalowana aplikacja POS dla .NET 1.1.

- Przekierowanie urządzenia działającego pod kontrolę systemu Windows Embedded for Point of Services można kontrolować, używając jednego z następujących ustawień zasad grupy:
  - Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Device and Resource Redirection\Do not allow supported Plug and Play device redirection policy setting,
  - Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions policy settings.

Przekierowanie urządzenia działającego pod kontrolą systemu Windows Embedded for Point of Service można także kontrolować za pomocą zakładki **Client Settings** w narzędziu **Terminal Server Configuration tool** (tsconfig.msc).

Nowe możliwości środowiska

Usługi Terminalowe Windows Server 2008 zawierają nowe cechy funkcjonalności, które w znaczny sposób wzbogacają środowisko pracy użytkownika zdalnie podłączonego do serwera Usług Terminalowych Windows Server 2008.

Wysoka rozdzielczość/indywidualna konfiguracja ekranu

Rozdzielczość ekranu Usług Terminalowych była ograniczona przez standardy obowiązujące w systemie Windows Server 2003 (format ekranu 4:3, maksymalna rozdzielczość 1600x1280). To ograniczenie związane było z limitami pamięci wirtualnej.

Usługi Terminalowe systemu Windows Server 2008 umożliwiają indywidualne dostosowanie ekranu do większej rozdzielczości oraz wybranie alternatywnych formatów ekranu, takich jak 16:9 lub 16:10. Na przykład nowsze monitory z rozdzielczością 1680x1050 lub 1920x1200 są obecnie wspierane. Maksymalną wspieraną rozdzielczością jest 4096x2048.

Indywidualne ustawienia rozdzielczości ekranu można ustawić w pliku .rdp, modyfikując wartości desktopwidth:i:<value> oraz desktopheight:i:<value>, gdzie <value> jest zadaną liczbą pikseli w poziomie lub pionie (odpowiednio), np. 1680 lub 1050. Ustawienie rozdzielczości może być także skonfigurowane w wierszu polecenia: mstsc.exe /w:<width> /h:<height>, gdzie width jest zadaną liczbą pikseli w poziomie, a height w pionie.

Rozszerzenie obrazu pulpitu

Rozszerzanie obrazu pulpitu (monitor spanning) umożliwia wyświetlenie zdalnej sesji na wielu monitorach.

Monitory użyte do takiego rozszerzenia obrazu pulpitu muszą spełniać następujące wymagania:

- Muszą pracować w tej samej rozdzielczości (nie można na przykład ustawić rozdzielczości jednego monitora na 1024x768, zaś drugiego na 800x600).
- Muszą być zestawione w poziomie. Nie ma obecnie możliwości rozszerzania obrazu w pionie.
- Łączna rozdzielczość monitorów nie może przekroczyć 4096x2048.

Rozszerzanie obrazu pulpitu można włączyć w pliku .rdp, modyfikując wartość Span:i:<value>, gdzie <value> może przyjmować ustawienie 0 –rozszerzanie wyłączone, 1- rozszerzanie włączone. Rozszerzanie obrazu pulpitu może też być włączone z wiersza poleceń: mstsc.exe /span.

Funkcja Desktop Experience

Oprogramowanie Remote Desktop Connection 6.0 powiela zdalny pulpit serwera terminali na lokalny komputer klienta. Jeśli komputer lokalny działa pod kontrolą systemu operacyjnego Windows Vista, a serwer terminali pod kontrolą sytemu Windows Server 2008, to dla uzyskania pełnej funkcjonalności środowiska pracy użytkownika z systemu Vista, na serwerze terminali należy zainstalować funkcję Desktop Experience. Włączenie tej funkcji umożliwi pojawienie się na Pulpicie Zdalnym własności systemu Windows Vista, takich jak odtwarzacz multimedialny Windows Media® Player 11, kompozycje pulpitu i zarządzanie zdjęciami.

Nowa jakość koloru 32-bity

System Windows Server 2008 wspiera obecnie 32-bitową jakość koloru. Ze względu na wdrożoną technologię kompresji połączenia Pulpitu Zdalnego, użycie 32-bitowej jakości koloru jest zalecane, gdyż kompresja zapewnia lepszą wydajność sesji użytkownikowi końcowemu.

Wygładzanie czcionek na ekranie

Windows Server 2008 obsługuje technologię ClearType®, która wyświetla czcionki na ekranie tak, że wydają się one bardziej gładkie i wyraźne. Różnicę w stosunku do wcześniejszej wersji widać zwłaszcza na ekranach monitorów LCD.

Serwer Usług Terminalowych Windows Server 2008 może być tak skonfigurowany, że klienci uzyskujący z nim połączenie przy użyciu Pulpitu Zdalnego w wersji 6.0 będą mogli korzystać z funkcji wygładzania czcionek (ClearType).

Wygładzanie czcionek jest możliwe, jeśli na komputerach klienckich jest zainstalowany któryś z poniższych systemów operacyjnych:

- Windows Vista,
- Windows Server® 2003 Service Pack 1,
- Windows® XP Service Pack 2.

Domyślnie funkcja ClearType w systemie Windows Server 2008 jest włączona.

Stosowanie wygładzania czcionek w trakcie połączenia zdalnego pulpitu może zwiększyć obciążenie łącza pomiędzy komputerem klienta i serwerem Usług Terminalowych Windows Server 2008.

Priorytetyzacja danych

Priorytetyzacja danych (Display Data Prioritization) kontroluje ruch w wirtualnym kanale sesji zdalnego pulpitu tak, że dane wyświetlane na ekranie, wprowadzone z klawiatury lub za pomocą myszki, mają wyższy priorytet niż inny ruch w wirtualnym kanale sesji, taki jak drukowanie czy transfer plików. Tego rodzaju uprzywilejowanie jest zaprojektowane w celu zapewnienia niezakłóconej pracy w zdalnym środowisku, nawet w przypadku wystąpienia zadań silnie obciążających połączenie, takich jak duże zadania drukowania.

Domyślnie stosunek liczbowy podziału pasma sieciowego wynosi 70: 30. Dane wejściowe i ekranu mają przydzielonych 70 procent pasma, natomiast pozostały ruch, taki jak schowek, transfer plików lub zadania drukowania, ma przydzielonych 30 procent pasma.

Ustawienia priorytetyzacji danych można dostosować do własnych potrzeb, zmieniając ustawienia podkluczy w kluczu rejestru HKLM\SYSTEM\CurrentControlSet\Services\TermDD:

- FlowControlDisable. Można wyłączyć priorytetyzację danych, jeśli wartość FlowControlDisable zostanie ustawiona na 1. Jeśli priorytetyzacja danych jest włączona, wszystkie żądania są obsługiwane na zasadzie „pierwszy wchodzi, pierwszy wychodzi" (FIFO). Domyślnym ustawieniem dla FlowControlDisable jest 0.

- FlowControlDisplayBandwidth. Klucz ten określa pasmo sieci przydzielone na ekran (i dane wejściowe). Domyślną wartością tego klucza jest 70, maksymalną dozwoloną wartością jest 255.
- FlowControlChannelBandwidth. Klucz ten określa pasmo sieci przydzielone pozostałemu ruchowi (schowek, transfery plików, zadania drukowania).
- FlowControlChargePostCompression. Wartość tego klucza decyduje o tym, czy alokacja pasma sieciowego jest obliczana na podstawie bajtów przed, czy po kompresji. Domyślna wartość 0 oznacza, że pod uwagę będą brane bajty przed kompresją.

Stosunek liczbowy podziału pasma sieciowego obliczany dla priorytetyzacji danych opiera się przede wszystkim na wartościach kluczy FlowControlDisplayBandwidth i FlowControlChannelBandwidth. Jeśli na przykład wartość FlowControlDisplayBandwidth jest ustawiona na 150, a FlowControlChannelBandwidth na 50, to stosunek liczbowy wynosi 150:50, czyli danym ekranu i danym wejściowym będzie przydzielonych 75 procent pasma sieciowego.

TS Easy Print

Poprzez nową funkcję Windows Server 2008 o nazwie TS Easy Print zarówno drukarki lokalne, jak i sieciowe są wspierane na serwerze Usług Terminalowych bez potrzeby instalacji ich sterowników. Umożliwia to użytkownikom bezproblemowe drukowanie z sesji Pulpitu Zdalnego lub z funkcji TS RemoteApp na lokalnej lub sieciowej drukarce zainstalowanej na komputerze klienta. W momencie, kiedy użytkownicy chcą drukować z sesji Pulpitu Zdalnego lub z funkcji TS RemoteApp, mogą zobaczyć okno dialogowe z właściwościami drukarki i otrzymać dostęp do jej wszystkich ustawień.

W celu zredukowania kosztów i poprawienia skalowalności możliwe jest skorzystanie z Zasad Grupy w celu ograniczenia ilości przekierowanych drukarek do jednej domyślnej drukarki.

Zarządzanie zasobami Usług Terminalowych

Funkcja Windows System Resorce Manager (WSRM) jest wbudowana w system operacyjny Windows Server 2008. Jest to opcjonalna funkcja, która może być zainstalowana w systemie za pomocą przystawki Server Manager.

Przed instalacją funkcji Windows System Resorce Manager musi być zainstalowana funkcja Windows Internal Database. Jeśli nie jest ona jeszcze zainstalowana, kreator instalacji WSRM udostępnia możliwość jednoczesnego zainstalowania jej.

Funkcja WSRM umożliwia administratorom kontrolowanie zasobów procesora i pamięci oraz tego, w jaki sposób są one alokowane do aplikacji, usług i procesów komputera. Zarządzanie zasobami tym sposobem znacznie poprawia wydajność systemu i redukuje możliwość wzajemnego odbierania sobie przez aplikacje, usługi i procesy zasobów procesora, pamięci. Zarządzanie zasobami zapewnia także stabilniejsze środowisko użytkownikom aplikacji i usług uruchomionych na komputerze.

Scenariusze wdrożenia/wykorzystania

Scentralizowany dostęp do aplikacji

Scentralizowany dostęp do aplikacji jest osiągany dzięki Usługom Terminalowym systemu Windows Server 2008, ponieważ:

- Zapewnia dostęp do aplikacji biznesowych poprzez Internet lub intranet z niemal każdego urządzenia.
- Zapewnia użytkownikom dostęp do centralnie zarządzanych pulpitów Windows.
- Zapewnia łatwe i bezpieczne zdalne połączenia z serwerami terminali i Pulpitami Zdalnymi także przez zapory firewall i translację adresów sieciowych (NATs).

Zwiększenie bezpieczeństwa

Bezpieczeństwo zostało zwiększone dzięki użyciu Usług Terminalowych systemu Windows Server 2008, ponieważ:

- Usługi te usuwają ryzyko utraty danych z laptopów dzięki użyciu bezpiecznego, zdalnego dostępu do aplikacji i centralnego przechowywania danych.
- Zapewniają bezproblemowy, scentralizowany i poufny dostęp do pojedynczych aplikacji bez konieczności korzystania z całego Pulpitu Zdalnego.
- Kontrolują dostęp do specyficznych zasobów w sieci korporacyjnej bez udzielenia pełnego dostępu do zasobów sieci korporacyjnej.
- Zapewniają bezpieczny dostęp do scentralizowanych aplikacji, pulpitów i zasobów organizacji z Internetu, dzięki użyciu HTTPS bez potrzeby konfiguracji dostępu poprzez Wirtualne Sieci Prywatne (VPN) lub otwierania dodatkowych portów w zaporze firewall.

Scentralizowane zarządzanie aplikacją

Scentralizowane zarządzanie aplikacjami zostało ulepszone w przypadku Usług Terminalowych systemu Windows Server 2008, ponieważ:

- Szybko rozlokowują programy działające w systemie Windows, na terminalach w całym przedsiębiorstwie. Usługi Terminalowe bywają szczególnie przydatne, kiedy programy są często uaktualniane, rzadko używane lub trudne w zarządzaniu.
- Umożliwiają zdalny dostęp do wykorzystywanych aplikacji, sprawiających problemy przy pracy poprzez sieć WAN.

Redukowanie obciążenia łącza sieciowego

Usługi Terminalowe mogą znacznie zmniejszyć potrzebną przepustowość łącza sieciowego, wymaganą przy dostępie do zdalnych aplikacji.

Polepszenie produktywności użytkownika
Produktywność użytkownika wzrasta przy wykorzystaniu Usług Terminalowych Windows Server 2008, gdyż:

- Użytkownicy mogą korzystać z programów, które są aktywne na serwerze terminali, łącząc się z nimi z takich urządzeń, jak komputery, kioski internetowe, urządzenia mobilne i systemy operacyjne inne niż Microsoft Windows.
- Usługi Terminalowe rozmieszczają aplikacje, które bezproblemowo integrują się z lokalnym pulpitem użytkownika, zmniejszając niepewność dotyczącą miejsca przechowywania danych.

Zmniejszenie złożoności/uproszczenie
Usługi Terminalowe zapewniają pracownikom, partnerom handlowym i klientom uproszczony dostęp do aplikacji.

Optymalizacja biura wydziałowego
Usługi Terminalowe mogą zapewnić lepszą wydajność programów używanych przez pracowników w biurach wydziałowych, którzy potrzebują dostępu do centralnych magazynów danych. Programy intensywnie przetwarzające dane czasami nie posiadają protokołów klienta/serwera, które są zoptymalizowane dla połączeń o niskiej prędkości. Programy tego typu często działają lepiej poprzez połączenie Usług Terminalowych niż poprzez sieć WAN.

Zalecenia

Aby w pełni wykorzystać możliwości systemu Windows Server 2008 w zakresie zdalnego dostępu, należy:

- Uaktualnić istniejące serwery terminali do Usług Terminalowych Windows Server 2008.
- Skonfigurować systemy klienckie, aby korzystały z klienta Remote Desktop Connecrion 6.0.
- Zaimplementować Desktop Experience i Display Data Prioritization na serwerach terminali Windows Server 2008, aby wykorzystać pełną funkcjonalność systemu Windows Vista.
- Korzystać z usługi Single Sign-on Usług Terminalowych, aby scentralizować administrację procesem uwierzytelniania i wspomóc pracę użytkownika.
- Korzystać z Bramy Usług Terminalowych w celu ustanowienia bezpiecznego, szyfrowanego połączenia pomiędzy zdalnymi użytkownikami w Internecie oraz zdalnymi komputerami uruchamiającymi aplikacje, bez możliwości dostępu do reszty sieci korporacyjnej.

- Korzystać z funkcji RemoteApp Usług Terminalowych, aby umożliwić uwierzytelnionym zdalnym użytkownikom połączenie z wybranymi programami uruchamianymi na serwerach terminali i Pulpitach Zdalnych (zdalnych komputerach}, a nie z całym pulpitem.
- Zaimplementować funkcję TS Web Access, aby udostępnić programy z sieci lokalnej poprzez przeglądarkę WWW.
- Zaimplementować Usługi Terminalowe na sprzęcie x64 nawet wtedy, jeśli nie jesteśmy jeszcze gotowi do korzystania z 64-bitowych aplikacji.
- Korzystać z funkcji WSRM, aby kontrolować zasoby na serwerze terminalowym.

Podsumowanie

Usługi Terminalowe dają możliwość korzystania z technologii, które umożliwiają dostęp do zainstalowanych na serwerze programów uruchamianych w systemie Windows lub do pełnego pulpitu Windows, zmniejszając wysiłki administracyjne i koszty związane z zapewnieniem zdalnego dostępu do zasobów. Użytkownicy w łatwy sposób mogą połączyć się z serwerem terminali, aby uruchamiać programy, zapisywać pliki i korzystać z zasobów sieciowych na tym serwerze.

Brama Usług Terminalowych

Wstęp

Brama Usług Terminalowych (TS Gateway) jest nową rolą Usług Terminalowych, która umożliwia autoryzowanym użytkownikom zdalnym łączenie się z serwerami terminalowymi oraz Pulpitami Zdalnymi (zdalnymi komputerami) w sieci korporacyjnej z dowolnego urządzenia mającego dostęp do internetu. Brama Usług Terminalowych korzysta z RDP poprzez protokół HTTPS do utworzenia bezpiecznego, szyfrowanego połączenia między zdalnymi użytkownikami a zdalnymi komputerami, na których uruchomione są aplikacje biznesowe.

Jeśli firma udostępnia aplikacje oparte na Usługach Terminalowych użytkownikom spoza sieci korporacyjnej, Brama Usług Terminalowych może ułatwić administrowanie Usługami Terminalowymi oraz zmniejszyć ryzyko związane z dostępem zdalnym. W tej sekcji omawiane będą następujące zagadnienia:

- Korzyści płynące z zastosowania Bramy Usług Terminalowych.
- Zarządzanie Bramą Usług Terminalowych.
- Warunki korzystania z Bramy Usług Terminalowych.

Zalety Bramy Usług Terminalowych

Zastosowanie serwera Bramy Usług Terminalowych wiąże się z wieloma korzyściami. Brama Usług Terminalowych:

- Zapewnia kompleksowy model zabezpieczeń pozwalający na kontrolę dostępu do określonych zasobów sieci.
- Przyczynia się do redukcji kosztów zarządzania dzięki eliminacji konieczności korzystania z serwerów aplikacyjnych w biurach wydziałowych..
- Ułatwia scalenie istniejących serwerów terminali, poprzez migracje na architektrurę x64.
- Może być zintegrowana z serwerem Network Policy Server (NPS), co umożliwi centralne wdrażanie konfiguracji bramy, a także zredukowanie całkowitego kosztu utrzymania (TCO) ponoszonego przez firmę.
- Umożliwia monitorowanie statusu, jakości oraz zdarzeń występujących w trakcie połączeń zdalnych.
- Pozwala użytkownikom na zdalne korzystanie z serwerów terminali oraz funkcji Pulpitu Zdalnego nawet, jeśli komunikacja przechodzi przez zapory firewall i translację adresów (NAT).

Zabezpieczenia stosowane w poprzednich wersjach systemów operacyjnych Windows, uniemożliwiały użytkownikom dostęp z zewnątrz do sieci firmowych przez zapory firewall i translację adresów (NAT), gdyż port 3389 wykorzystywany w połączeniach RDP (Remote Desktop Protocol) ze względu na bezpieczeństwo, był standardowo blokowany. W Windows Server 2008, TS Gateway transmituje ruch RDP do portu 443, wykorzystując tunel TLS (HTTP Transport Layer Security). Oznacza to, że cały ruch przekazywany przez Internet między klientem a serwerem jest szyfrowany.

- Pozwala na łączenie z Internetu z sieciami wewnętrznymi firm bez konieczności zestawiania Wirtualnej Sieci Prywatnej (VPN).

  Usługi Terminalowe w Windows Server 2008 pozwalają na bezpieczne, płynne połączenie z siecią korporacyjną bez konieczności wcześniejszego wdrażania VPN, dzięki skorzystaniu z RDP tunelowanego za pomocą protokołu HTTPS. Korzystają przy tym z tej samej infrastruktury co Microsoft Outlook, jeśli program ten jest skonfigurowany do łączenia się przez RPC po HTTPS. Możesz odgrodzić serwer Windows Server 2008 wieloma zaporami firewall, bez konieczności otwierania innych portów niż port 443.

  Należy stosować Bramę Usług Terminalowych w miejsce Wirtualnych Sieci Prywatnych (VPN) w następujących przypadkach:

  – Gdy nie są wymagane lokalne kopie danych.

  – Kiedy istnieje potrzeba szybkiego połączenia.

  – Gdy przepustowość pasma lub rozmiary danych aplikacji czynią korzystanie z Wirtualnych Sieci Prywatnych (VPN) mało wydajnym.

Zarządzanie Bramą Usług Terminalowych

Przystawka TS Gateway Management zapewnia zintegrowane narzędzie do zarządzania Bramą Usług Terminalowych , co:

- Pozwala na konfigurowanie wymogów, jakie muszą być spełnione przez zdalnych użytkowników, żądających zdalnego dostępu do zasobów sieci. Przykładowo, można zdefiniować:

  – Grupy użytkowników, którzy będą posiadać prawo zdalnego korzystania z zasobów sieci firmowej.

  – Określone zasoby, z którymi użytkownicy ci będą się mogli połączyć zdalnie.

  – Czy użytkownicy zdalni muszą być członkami domeny.

  – Wymóg, aby zdalnie mogły się łączyć wyłącznie komputery będące członkami określonych grup Windows.

- Umożliwia monitorowanie zdarzeń Bramy Usług Terminalowych. Można określić zdarzenia, np. takie jak nieudane próby połączenia z serwerem Bramy Usług Terminalowych, które należy monitorować; w chwili ich wystąpienia można prześledzić podobne zdarzenia używając przystawki Podglądu Zdarzeń.
- Umożliwia przeglądanie informacji o aktywnych połączeniach użytkowników, ustawianie maksymalnego limitu połączeń, oraz dokonywanie innych operacji służących kontroli dostępu do zasobów sieci poprzez serwer Bramy Usług Terminalowych.

Żaden zdalny komputer nie jest bezpośrednio dostępny z Internetu, a wszystkie dane pozostają w sieci korporacyjnej.

Wymagania Bramy Usług Terminalowych

Aby Brama Usług Terminalowych funkcjonowała poprawnie, muszą zostać spełnione następujące wymagania:

- *System operacyjny*. Serwer musi pracować pod kontrolą systemu operacyjnego Windows Server 2008.

- *Uwierzytelnienia*. Brama może być konfigurowana wyłącznie przez członków grupy Administratorzy danego komputera.

- *Network Policy Server (NPS)*. NPS to implementacja firmy Microsoft serwera RADIUS, tj. Remote Authentication Dial-In User Service, wcześniej znanego pod nazwą Internet Authentication Service (IAS). Serwer NPS umożliwi centralne magazynowanie zasad działania bramy, centralne zarządzanie zasadami oraz centralną ich walidację.

Jeśli przed zainstalowaniem bramy serwer NPS nie był w danej organizacji wykorzystywany, to zostanie on automatycznie zainstalowany w trybie lokalnym na tej samej maszynie, co brama.

- *Certyfikat Serwera*. Standardowo komunikacja między bramą TS Gateway a klientami w Internecie opiera się na szyfrowaniu TLS 1.0 (Transport Layer Security), które wymaga, aby serwer TS Gateway posiadał certyfikat.

  – Certyfikat można uzyskać wewnątrz firmy, jeśli posiada ona uprawnienia Urzędu Certyfikacji (CA), skonfigurowane do wydawania certyfikatów X.509 zgodnych z SSL, które spełniają wymogi Bramy Usług Terminalowych. Jednakże taki certyfikat musi być także podpisany przez główny Urząd Certyfikacji (CA), biorącym udział w programie Microsoft Root Certificate Program Members, co zagwarantuje pracownikom możliwość łączenia się z komputerów domowych, bądź zewnętrznych terminali.

  – Jeśli firma nie posiada własnego Urzędu Certyfikacji (CA) ustawionego zgodnie z certyfikatami X.509 zgodnymi z SSL, może nabyć certyfikat od sprzedawcy spoza firmy Microsoft, który uczestniczy w programie Microsoft Root Certificate Program Members.

Więcej informacji znajduje się na stronie http://go.microsoft.com/fwlink/?LinkID=59547; niektórzy z tych dostawców mogą oferować certyfikaty bezpłatnie, lub w wersji testowej.

Innym sposobem jest stworzenie oraz zaimportowanie na próbę samodzielnie podpisanego certyfikatu dla Twojego serwera Bramy Usług Terminalowych. Takie certyfikaty mogą być używane jedynie do celów próbnych na pojedynczych komputerach. Są one mniej bezpieczne od certyfikatów wydawanych przez Urząd Certyfikacji Przedsiębiorstwa lub zaufanych sprzedawców spoza firmy Microsoft, uczestniczących w programie Microsoft Root Certificate Program Members, gdyż nie gwarantują one tożsamości organizacji, która go wydała.

Konfiguracja Bramy Usług Terminalowych

Aby skonfigurować Bramę Usług Terminalowych, należy wykonać następujące czynności:

- *Zainstalować rolę TS Gateway* .

Aby Brama Usług Terminalowych prawidłowo funkcjonowała, muszą być zainstalowane również następujące role: Web Server (IIS), Network Accesss Services, RPC over HTTP Proxy i Windows Activation Service.

- *Skonfigurować ustawienia IIS dla TS Gateway Server*. W menadżerze serwera pod Configuration Task, po kliknięciu polecenia: Konfiguruj ustawienia IIS dla TS Gateway, ustawienia zostaną automatycznie zmodyfikowane zgodnie z potrzebą.

- *Uzyskać/skonfigurować certyfikat dla TS Gateway server*. Certyfikat musi spełnić następujące wymagania:

  – Nazwa w Subject line certyfikatu serwera (nazwa certyfikatu lub CN) musi odpowiadać nazwie, która jest skonfigurowana na TS Gateway Server.

  – Celem certyfikatu jest uwierzytelnienie serwera.

  – Certyfikat ma klucz prywatny.

- *Utworzyć* Zasady uwierzytelniania połączenia *(CAP) dla TS Gateway Server*. Zasady uwierzytelniania połączenia (CAPs) kontrolują, czy użytkownik może przekroczyć granicę bramki, aby uzyskać dostęp do sieci korporacyjnej. Pozwalają na określenie użytkowników, grup użytkowników (i opcjonalnie grup komputerów), które mają dostęp do serwera Bramy Usług Terminalowych. CAP-y tworzy się w celu:

  – Uproszczenia zarządzania i wzmocnienia zabezpieczeń poprzez zapewnienie wyższego poziomu kontroli dostępu do zdalnych komputerów w sieci korporacji.

  – Włączenia wymogu spełnienia specyficznych warunków dostępu do serwera Bramy Usług Terminalowych przez użytkowników, grupy użytkowników i grupy komputerów Możesz okreslić specyficzne warunki w każdym CAP-ie. Na przykład możesz zażądać, by użytkownik użył karty procesorowej w celu połączenia przez Bramę Usług Terminalowych.

  – Udzielania użytkownikom dostępu do serwera Bramy Usług Terminalowych tylko wtedy, gdy spełniają lub przekraczają warunki wymienione w CAP-ie, który dotyczy ich grupy.

CAP-y zezwalają użytkownikom jedynie na dostęp do serwera Bramy Usług Terminalowych, a nie do konkretnych zdalnych komputerów w sieci. Po zdefiniowaniu CAP-ów musisz utworzyć grupę zasobów i zasadę przydziału zasobów (RAP), aby zezwolić na dostęp z serwera Bramy Usług Terminalowych do konkretnego zdalnego komputera w sieci. Zamiast tworzyć grupę zasobów ręcznie, można użyć grupy, bezpieczeństwa zdefiniowanej w Active Directory.

- *Tworzenie grupy zasobów i zasady przydziału zasobów dla serwera Bramy Usług Terminalowych.* RAP-y są tworzone w celu:

  – Zdefiniowania grup zdalnych komputerów, do których użytkownicy mogą mieć dostęp. Pozwalają na zarządzanie dostępem użytkownika do grup zasobów.

  – Udzielania dostępu do konkretnych komputerów zdalnych w sieci tylko w wypadku, kiedy zostaną spełnione lub przekroczone określone warunki.

  – Zagwarantowania, że właściwi użytkownicy mają dostęp do właściwych komputerów zdalnych w sieci.

Grupy zasobów reprezentują listę komputerów lub grupę komputerów. RAP-y pozwalają na określenie, do jakich komputerów użytkownicy mogą mieć dostęp w sieci z internetu przez serwer Bramy Usług Terminalowych. Po utworzeniu jednej lub większej liczby grup zasobów możesz utworzyć RAP przez skojarzenie jednej lub kilku grup zasobów z jedną lub kilkoma grupami użytkowników, którzy mają dostęp do zdalnych komputerów w tej grupie zasobów. Użytkownicy łączący się z Bramką usług Terminalowych [TS Gateway] uzyskują dostęp do zdalnych komputerów w sieci korporacyjnej, jeżeli spełniają warunki przynajmniej jednego CAP-u i jednego RAP-u.

Klient bramy musi wykorzystywać jedną z następujących wersji Windows:

- Windows Vista
- Windows Server 2008
- Windows XP z SP2 i RDC 6.0 (lub wyższym)
- Windows Server 2003 z SP1 i RDC 6.0 (lub wyższym)

Procedura: Konfiguracja Bramy Usług Terminalowych

Aby skonfigurować Bramę Usług Terminalowych:

1. Z menu **Start** wybierz pozycję **All Programs/Administrative Tools** i kliknij pozycję **Server Manager.** W oknie **Server Manager** rozwiń listę **Roles** i wybierz pozycję **Terminal Services**. Sprawdź, czy wszystkie usługi są uruchomione.

2. Rozwiń listę **Roles/Web Server (IIS)** i wybierz pozycję **Internet Information Services (IIS) Manager**. Następnie w panelu **Connections** wybierz pozycję **Default Web Site**. W panelu **Action** wybierz pozycję **Advanced Setting** i sprawdź, czy parametr **Start Automatically** jest ustawiony na wartość **True**, a astępnie zaakceptuj zmienione ustawienia i zamknij przystawkę **Server Manager**.

Importowanie i mapowanie certyfikatu z Urzędu Certyfikacji dla Bramy Usług Terminalowych

3. Zaimportujesz teraz certyfikat z Urzędu Certyfikacji dla Bramy Usług Terminalowych. W tym celu uruchom konsolę **TS Gateway Manager** z okna eksplorera. Wybierz odpowiedni serwer, a następnie wyświetl jego właściwości za pomocą panelu **Action**. Wybierz zakładkę **SSL Certificate,** a następnie kliknij przycisk **Create Certificate...**. W oknie **Create Self-Signed Certificate** w wpisz ścieżkę dostępu do Twojego certyfikatu i potwierdź klikając przycisk **OK**.


4. Dodaj przystawkę **Certificates** do konsoli **MMC (Microsoft Management Konsole).** W przystawce **Certificates** wybierz pozycję **Computer Account** i kliknij przycisk **Next.** W oknie **Select Computer** zaznacz pozycję **Local Computer,** a następnie kliknij przycisk **Finish**. W oknie **Add or Remove Snap-ins** kliknij przycisk **OK**. W konsoli1 rozwiń drzewo **Console Root/Certificates (Local Computer)/Trusted Root Certification Authorities** i zaznacz pozycję **Certificates.** W menu **Action** wybierz pozycję **All Tasks**, a następnie **Import...**. Po uruchomieniu kreatora importu certyfikatu w drugim kroku w polu **File Name:** wpisz lokalizację pliku z certyfikatem ***.cer**. W oknie **Certificate Store** upewnij się, że wszystkie pola wyboru są zaznaczone, a następnie wybierz przycisk **Next**. W ostatnim kroku kreatora importu certyfikatu zapoznaj się z podsumowaniem i kliknij przycisk **Finish**.


Tworzenie Zasad Uwierzytelniania Połączenia (CAP) dla Bramy Usług Terminalowych

5. Aby utworzyć Zasady Uwierzytelniania Połączenia dla Bramy Usług Terminalowych, w programie **TS Gateway Manager** rozwiń drzewo **nazwa_serwera (Local)/ Policies**, a następnie wybierz pozycję **Connection Authorization Policies**. W panelu kliknij pozycję **Create New Policy,** a następnie kliknij pozycję **Wizard**. W oknie **Authorization Policies** upewnij się, że jest zaznaczona opcja **Create only a TS CAP** i kliknij przycisk **Next**. Następnie sprawdź, czy zaznaczona jest metoda autentykacji **password** i wprowadź grupę użytkowników poprzez kliknięcie przycisku **Add Group**. Po uzupełnieniu wartości zakończ pracę z kreatorem.


Tworzenie Grupy Zasobów

6. Z poziomu programu **TS Gateway Manager** utworzysz teraz Grupę Zasobów. W tym celu rozwiń drzewo **nazwa serwera (Local)/Policies** i zaznacz pozycję **Resource Authorization Policies**. Z panelu **Actions** wybierz **pozycję Manage Local Computer Groups**. W **oknie Manage Local Computer Groups** kliknij przycisk **Create group**. W oknie **New TS Gateway** na zakładce **General** wypełnij odpowiednie pola. Przejdź do zakładki **Network resources**. Podaj nazwę stacji roboczej, a następnie kliknij przycisk **Next**. Powtórz tę samą czynność dla pozostałych stacji i serwera.


Tworzenie zasad dostępu do zasobów w Bramie Usług Terminalowych

7. Aby utworzyć zasady dostępu do zasobów w Bramie Usług Terminalowych, w **TS Gateway Manager** rozwiń drzewo **nazwa serwera (Local)/Policies** i zaznacz pozycję **Resource Authorization Policies**. Z panelu **Actions** wybierz pozycję **Create New Policy** i wybierz pozycję **Wizard**. Po uruchomieniu kreatora upewnij się, że jest zaznaczona opcja **Create only a TS RAP** i kliknij przycisk **Next**. Aby dokończyć konfigurowanie kreatora, uzupełnij wartości, a na koniec zakończ pracę z kreatorem.

Monitorowanie Połączeń

8. Połączenia możesz monitorować w **TS Gateway Manager**. W tym celu rozwiń drzewo **nazwa_serwera (Local)/Monitoring.** Za pomocą tego okna można analizować połączenia i zarządzać nimi.

Zalecenia

- Należy korzystać z Bramy Usług Terminalowych zamiast VPN, gdy lokalne kopie danych nie są wymagane, gdy potrzebny jest szybszy czas połączenia, a także gdy przepustowość połączenia lub rozmiary danych przesyłanych przez aplikację sprawiają, iż połączenie za pomocą VPN nie jest optymalne.
- Należy wykorzystać dedykowany serwer jako Bramę Usług Terminalowych; chociaż Brama Usług Terminalowych może współegzystować z serwerem Outlook RPC/HTTP, nie jest to zalecane poza sytuacjami związanymi z bardzo niskim obciążeniem.
- Należy skonfigurować zasady dostępu do połączeń, grupy zasobów i zasady dostępu do zasobów.
- Należy korzystać z zarządzania Bramą Usług Terminalowych, aby monitorować status, żywotność i zdarzenia na zdalnych połączeniach.
- Nie należy korzystać z samopodpisanego (self-signed) certyfikatu SSL w środowisku produkcyjnym; lepiej korzystaj z certyfikatu wydanego przez zaufany Urząd Certyfikacji, takiego jak certyfikatu możliwego do uzyskania z Verisign, aby uniknąć potrzeby dystrybuowania certyfikatów do klientów.
- Należy korzystać z zapory działającej w warstwie aplikacji (application-layer firewall), takiej jak ISA Server, aby filtrować przepływ danych RPC i wzmocnić bezpieczeństwo.
- Nie należy polegać na funkcji Bramy Usług Terminalowych blokującej urządzenia; to raczej parametr konfiguracyjny (podpowiedź dla klienta) niż parametr bezpieczeństwa.

Podsumowanie

Brama Usług Terminalowych umożliwia uwierzytelnionym zdalnym użytkownikom połączenie z serwerami terminali i Pulpitami Zdalnymi (zdalnymi komputerami) w sieci korporacyjnej z dowolnego połączonego z Internetem urządzenia, na którym zainstalowana jest aplikacja Remote Desktop Connection (RDC) 6.0. Brama Usług Terminalowych eliminuje potrzebę konfiguracji połączeń Wirtualnej Sieci Prywatnej (VPN), umożliwiając zdalnym użytkownikom połączenie z siecią firmową przez Internet, jednocześnie zapewniając bezpieczny model konfiguracji połączenia, który umożliwia kontrolę dostępu do specyficznych zasobów.

Usługa TS RemoteApp

Wstęp

Usługa TS RemoteApp umożliwia organizacjom zapewnienie dostępu do standardowych programów Windows właściwie z każdej lokalizacji przez Internet lub intranet użytkownikom każdego komputera opartego na systemie Windows Vista lub użytkownikom komputerów opartych na systemie Windows XP z zainstalowanym nowym klientem Remote Desktop Connection 6.0. RemoteApp jest wbudowana w Usługi Terminalowe w Windows Server 2008.

W przeszłości, Usługi Terminalowe dostarczały jedynie mechanizmu połączenia użytkowników do całych Pulpitów Zdalnych. Potrzebny był nowy mechanizm by zintegrować korzyści płynące z wykorzystania centralnie wdrażanych i zarządzanych aplikacji z korzyściami lokalnych aplikacji klienta. Usługi Terminalowe Windows Server 2008 zapewniają taki mechanizm poprzez TS RemoteApp w celu dostarczenia aplikacji za pośrednictwem ścisłej integracji pomiędzy serwerem terminali oraz klientem Windows.

Czym są programy TS RemoteApp?
Programy TS RemoteApp to aplikacje, do których dostęp przebiega zdalnie poprzez Usługi Terminalowe, a działają, tak jakby zostały uruchomione były na lokalnym komputerze użytkownika końcowego. Użytkownicy mogą uruchamiać programy RemoteApp jednocześnie ze swoimi programami lokalnymi.

Jakich korzyści dostarcza użytkowanie TS RemoteApp?
TS RemoteApp umożliwia organizacjom zapewnienie dostępu do standardowych programów Windows właściwie z każdej lokalizacji przez Internet lub sieć lokalną użytkownikom każdego komputera opartego na systemie Windows Vista lub użytkownikom komputerów opartych na systemie Windows XP, z zainstalowanym nowym klientem Remote Desktop Connection 6.0. TS RemoteApp przyczynia się do zwiększenia doświadczenia użytkownika, otwiera nowe drogi do zastosowania programów oraz ogranicza zasób pracy administracyjnej koniecznej dla wsparcia tych programów w wielu przypadkach:

- W biurach wydziałowych, w których lokalne wsparcie IT może być ograniczone, w celu centralizacji zarządzania aplikacjami oraz ulepszenia działania programów zdalnych w przypadku ograniczonej przepustowości łącza.
- Kiedy użytkownicy muszą zdalnie łączyć się z aplikacjami.
- Kiedy istnieje potrzeba zastosowania aplikacji Lini Biznesowej (LOB), w szczególności niestandardowych aplikacji LOB na komputerach korzystających z różnych konfiguracji i wersji Microsoft Windows.
- W środowiskach stosujących „gorące biurka" lub „hotelowy" obszar roboczy, w którym użytkownicy nie mają przydzielonych komputerów.
- Gdy wymagane jest użytkowanie wielu wersji aplikacji, szczególnie jeśli lokalna instalacja wielu wersji powodowałaby konflikty.
- Gdy chodzi o zapewnianie rozwiązań dla przemieszczających się użytkowników, którzy muszą pracować na różnych komputerach, które mogą nie mieć zainstalowanych wymaganych programów lokalnie.
- Gdy organizacje szukają sposobów na ulepszenie swoich stacji roboczych typu „rich-client", na przykład w sytuacji biura wydziałowego, kiedy wybrane aplikacje umieszczane są w lokalizacji, gdzie mogą być łatwo zarządzane, lecz jednocześnie pracownikom pozostawiane są stacje robocze typu „rich-client", ponieważ zawierają aplikacje, które muszą być uruchamiane lokalnie.

Czy trzeba zmienić jakikolwiek istniejący kod, by pracować z TS RemoteApp?
Aby oprogramowanie działało zdalnie z TS RemoteApp, serwer terminali, będący hostem dla oprogramowania, musi działać pod kontrolą systemu Windows Server 2008. Każdy program mogący działać w zakresie Usług Terminalowych lub w sesji Pulpitu Zdalnego powinien być zdolny do działania jako program TS RemoteApp.

Niektóre z podstawowych zmian dotyczących systemu operacyjnego Windows Server 2008 mogą mieć wpływ na wcześniejsze wersje oprogramowania, które działają poprawnie pod wcześniejszymi wersjami systemu operacyjnego Windows. Jeśli wystąpią trudności podczas uruchomienia programu pod TS RemoteApp należy sprawdzić czy działa on poprawnie na lokalnej konsoli serwera działającego pod systemem Windows Server 2008.

Praktyka
Użytkownicy mogą uruchamiać programy zdalnie z serwera terminali i odnosić wrażenie, że są one uruchomione na komputerze lokalnym użytkownika końcowego.

Co działa inaczej?
Gdy klient łączy się z serwerem Windows 2008, na którym uruchomiony jest Terminal Services TS RemoteApp następuje wiele zmian:

- Zdalny program zintegrowany jest z pulpitem klienta, więc zamiast ukazywać się użytkownikowi na Pulpicie Zdalnym serwera terminali, zostaje, uruchomiony we własnym rozszerzalnym oknie z własnym udziałem na pasku zadań.
- Jeśli program ten używa ikony obszaru powiadamiania ikona ta pojawia się w obszarze powiadamiania klienta.
- Wyskakujące okienka typu Popup zostają przekierowane na lokalny pulpit.
- Lokalne napędy oraz drukarki mogą zostać przekierowane tak, by pojawiały się w zdalnym programie..

Wielu użytkowników może nie zauważyć, że program zdalny różni się od programu lokalnego.

Konfiguracja Serwera RemoteApp Usług Terminalowych
Administrator musi podjąć następujące kroki, by skonfigurować Serwer TS RemoteApp:

- Włączyć Dostęp Zdalny.
- Dodać przystawkę TS Remote App.
- Skonfigurować TS Remote App:
  - Zainstalować aplikacje na serwerze z zainstalowaną i uruchomioną rolą Terminal Server.
  - Uruchomić Kreator RemoteApp, aby dodać program do listy dozwolonych programów (Allow) i udostępnić go zdalnie użytkownikom.

By wykonać tę procedurę, trzeba być członkiem grupy Administratorzy na serwerze terminali.

- Utworzyć Pakiet RDP lub Pakiet MSI.

Można utworzyć pakiet RDP dla dowolnego programu z listy dozwolonych programów (Allow).

Można utworzyć wiele pakietów RDP z różnymi ustawieniami dla tego samego programu, jeśli potrzeba. Dodatkowy utworzony plik .rdp otrzyma numer w nawiasie dołaczony do nazwy pliku, np. Remote WordPd(1).rdp.

Można utworzyć pakiet MSI dla dowolnego programu z listy dozwolonych programów (Allow).

Jeśli zostanie utworzony pakiet MSI za pomocą programu, który jest udostępniony użytkownikom poprzez TS Web Access, rozszerzenie pliku pakietu MSI przyjmie postać .rap.msi. Jeśli pakiet zostanie utworzony za pomocą programu, który nie jest udostępniony użytkownikom poprzez TS Web Access, rozszerzenie pliku pakietu MSI przyjmie postać .rdp.msi. W obu przypadkach pakiet MSI zawiera plik .rdp, który zostanie zainstalowany na lokalnym komputerze końcowego użytkownika.

- Rozdystrybuować programy TSRemoteApp do użytkowników.

Można dystrybuować plik .msi do lokalnego komputera użytkownika końcowego, korzystając ze scentralizowanego procesu dystrybucji, takiego jak Microsoft System Management Server lub zasady grup Active Directory.

- Zarządzać listą dozwolonych programów (Allow).
  - Zmienić lub usunąć program RemoteApp.
  - Włączyć lub wyłączyć listę dozwolonych programów (Allow).
  - Wyeksportować lub zaimportować listę dozwolonych programów (Allow).

W jaki sposób użytkownicy mogą uzyskać dostęp do programów RemoteApp?

Użytkownicy systemu Windows Server 2008 mogą uruchomić programy RemoteApp na kilka sposobów:

- Podwójnie klikając plik .rdp, który został utworzony i rozdystrybuowany przez administratora. (Można dystrybuować plik .msi, aby utworzyć skróty do plików .rdp na pulpitach użytkowników lub w menu Start).
- Podwójnie klikając plik, którego rozszerzenie jest powiązane z programem TS RemoteApp. Może tego dokonać administrator, korzystając z pliku .msi.
- Posłużyć się odnośnikiem do programu na stronie Web, korzystając z usługi Terminal Services Web Access.

Pliki .rdp i .msi zawierają ustawienia niezbędne do uruchomienia TS RemoteApp. Po otwarciu programu udostępnionego przez funkcję TSRemoteApp na lokalnym komputerze, użytkownik może korzystać z programu uruchomionego na serwerze terminali tak jakby był uruchomiony lokalnie.

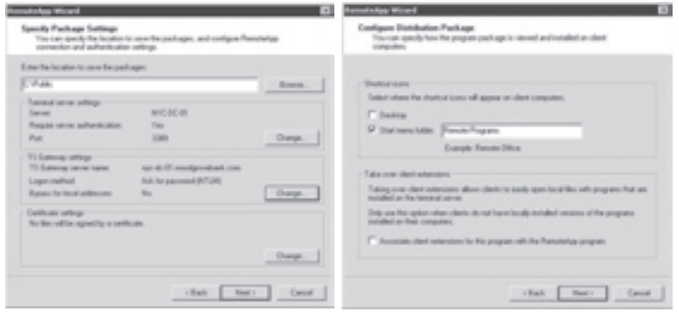
Procedura: Wdrożenie TS RemoteApp

Dodawanie programu do listy Allow list

1. Aby dodać program do listy Allow, powinieneś zalogować się na konto Administratora do kontrolera domeny. Z menu **Start** przejdź do pozycji **All Programs/Administrative Tools/Terminal Services/TS RemoteApp Manager**, a następnie z menu **Action** wybierz pozycję **Add RemoteApps**. Na pierwszej stronie kreatora **RemoteApp** kliknij przycisk **Add**, aby przejść do okna **Choose RemoteApp to add to the allow list.** Kliknij przycisk **Browse**, podaj ścieżkę dostępu do programu i wybierz przycisk **Open**. W oknie podsumowującym kreatora wybierz przycisk **Finish**. W podobny sposób możesz dodać program, który znajduje się już na liście dostępnych (wcześniej zdefiniowanych) programów.
2. W konsoli **RemoteApp** w panelu **Contents** zaznacz wcześniej dodaną aplikację i z panelu **Actions** wybierz **Properties**. W oknie dialogowym **Remote Program Properties** możesz zmienić nazwę wyświetlanego programu. Na zakończenie zatwierdź wprowadzone zmiany.

Tworzenie pliku MSI w celu zainstalowania aplikacji

3. Teraz utworzysz plik **MSI** do późniejszej jej dystrybucji. W tym celu w oknie **RemoteApp Manager**, w panelu **Contents**, zaznacz aplikację z której ma zostać stwożony plik **MSI.** W panelu **Actions** uruchom kreator, klikając pozycję **Create Windows Installer Package**. W **drugim kroku kreatora Specify Packages Settings określ lokalizację docelową zapisywanego pliku. W części TS Gateway Settings kliknij przycisk Change, a w oknie Configure TS Gateway Settings** zaznacz opcję **Use these TS Gateway Server settings**:. Wprowadź odpowiednie ustawienia, a następnie zatwierdź zmienione ustawienia. W **RemoteApp Wizard**, na stronie **Configure Distribution Package** zaakceptuj domyślne ustawienia, a w ostatnim oknie kreatora zapoznaj się z podsumowaniem i kliknij przycisk **Finish**.



Wykorzystanie dostępu do zdalnych aplikacji

4. Aby podłączyć się do zdalnej aplikacji, musisz zalogować się na stacji klienckiej na konto Administratora. W menu **Start** wybierz pozycję **Search** i podaj ścieżkę do programu na zdalnym serwerze. W Windows Explorer dwukrotnie kliknij pozycję z plikiem ***.RDP**, a w oknie dialogowym **Windows Security** wprowadź nazwę logowania użytkownika i jego hasło. Następnie zaznacz opcję **Remember my credentials** i zatwierdź wprowadzone zmiany, a w oknie dialogowym **RemoteApp** zaznacz opcję **Don't prompt me again for connections to this computer**. Po kliknięciu przycisku **Yes** zamkniesz zdalny program **On The Server**.

5. W Windows Explorer dwukrotnie kliknij plik z aplikacją ***.rap.msi**, aby zainstalować zdalną aplikację. Kiedy aplikacja zostanie pomyślnie zainstalowana, z menu **Start/All Programs** wybierz pozycję **RemoteApp – nazwa programu**, co spowoduje uruchomienie tej aplikacji.

Scenariusze wdrożenia/wykorzystania

Rozlokowanie aplikacji Linii Biznesu (LOB)
W przypadku fuzji, firmy łączące się będą chciały w sposób niezakłócony korzystać z aplikacji Lini Biznesu (LOB) na różnych konfiguracjach sprzętowych, pod różnymi wersjami systemu Windows. Zamiast ponoszenia kosztów rozlokowania wszystkich aplikacji LOB do wszystkich komputerów w firmie, aplikacje LOB mogą zostać zainstalowane na serwerze terminali i udostępnione poprzez funkcje TSRemoteApp.

„Gorące biurka"
W firmie stosującej elastyczną politykę stanowisk pracy użytkownicy mogą pracować na różnych komputerach.
W pewnych przypadkach komputer, na którym pracuje użytkownik, niekoniecznie musi mieć programy zainstalowane lokalnie. Kiedy używane są funkcje TS RemoteApp, programy mogą być zainstalowane na serwerze terminali i udostępnione użytkownikom tak, jakby były zainstalowane lokalnie.

Zarządzanie wersjami
Dzięki TS RemoteApp nie trzeba rozlokowywać i utrzymywać różnych wersji tego samego programu dla poszczególnych komputerów. Jeśli pracownicy muszą korzystać z różnych wersji programu, wersje te mogą być zainstalowane na jednym lub większej liczbie serwerów terminali i udostępnione za pośrednictwem funkcji TS RemoteApp.

Biura Wydziałów
Firmy często mają oddziały w różnych lokalizacjach, w kórych możliwość pomocy IT może być ograniczona. TS RemoteApp pozwala im na scentralizowanie zarządzania aplikacjami i poprawę wydajności zdalnych programów w scenariuszach z ograniczoną przepustowośccią łącza. Ten sposób wdrożenia może zredukować jego złożoność i ograniczyć ilość wymaganych zasobów administracyjnych.

Zalecenia

Aby osiągnąć największe korzyści z funkcji TSRemoteApp w Windows Server 2008, należy:

- Umieścić podobne aplikacje, takie jak Microsoft Office, na tym samym serwerze terminali.
- Rozważyć umieszczenie poszczególnych aplikacji na oddzielnych serwerach terminali w następujących sytuacjach:
  - Gdy aplikacja ma problemy z kompatybilnością.
  - Parametry aplikacji lub liczba korzystających z aplikacji użytkowników wymagają pełnej wydajności serwera.

  - W przypadku utworzenia farmy serwerów i balansowania obciążenia dla pojedynczych aplikacji, które przekraczają możliwości wydajnościowe jednego serwera.

- Utworzyć farmę serwerów i zastosować balansowanie obciążenia dla pojedynczych aplikacji, które przekraczają możliwości wydajnościowe jednego serwera.
- Rozważyć umieszczenie serwera TSRemoteApp za ISA Server, a nie tylko za sprzętową zaporą (firewall).
- Korzystać z certyfikatu SSL podpisanego przez zaufany Urząd Certyfikujący.

Podsumowanie

TS RemoteApp systemu Windows Server 2008 umożliwia organizacjom zapewnienie dostępu do standardowych programów Windows teoretycznie z każdego miejsca użytkownikom i użytkownikom każdego komputera działającego w systemie Windows Vista lub o Windows XP, z zainstalowanym klientem Remote Desktop Connection 6.0, poprzez Internet lub intranet. Dostęp do programów RemoteApp jest możliwy zdalnie poprzez Usługi Terminalowe. Programy te zachowują się tak, jakby były uruchomione na komputerze lokalnym końcowego użytkownika.

Usługa TS Web Access

Wstęp

Terminal Services Web Access służy uruchamianiu aplikacji hostowanych na serwerze TS RemoteApp z poziomu strony internetowej. Programy te stają się dostępne dla użytkowników korzystających z przeglądarki internetowej. Za pomocą funkcji TS Web Access, użytkownik może odwiedzić stronę Web – łącząc się zarówno z Internetu, jak i intranetu – aby uzyskać listę dostępnych programów TS RemoteApp. Kiedy użytkownik uruchamia funkcję TS RemoteApp, rozpoczęta zostaje sesja na serwerze terminali, który hostuje ten program.

TS Web Access zawiera domyślną stronę Web, którą można wykorzystać w celu rozlokowania TS RemoteApp w sieci. Strona Web składa się z ramki i konfigurowalnych webpartów. Alternatywnie, możesz włączyć webparty do serwisu Microsoft Windows SharePoint Services.

> TS Web Access zapewnia tylko mechanizm dostępu do aplikacji; nie zapewnia mechanizmu transportowego.

Korzyści

- Uwierzytelnieni użytkownicy mogą szybko uzyskać dostęp do programów z dowolnej lokalizacji, łącząc się z prostą stronąWWW.
- Administratorzy mogą szybko i łatwo dodawać i usuwać programy z listy udostępnionych bez konieczności dystrybuowania, instalacji i deinstalacji aplikacji na lokalnej maszynie.
- TS Web Access dostarcza prostego, gotowego rozwiązania, jednocześnie zapewniając infrastrukturę, którą można wykorzystać w bardziej skomplikowanych scenariuszach.

Wymagania serwera i konfiguracja

Trzeba zainstalować usługę TS Web Access na serwerze, z którym użytkownicy mają się łączyć poprzez sieć, aby uzyskać dostęp do funkcji TS RemoteApp. Podczas instalacji TS Web Access, instalowany jest także program Microsoft Internet Information Services (IIS) 7.0 jako wymagany komponent.

Po zainstalowaniu funkcji TS Web Access można określić źródło danych służące do wypełnienia listy programów TS RemoteApp, które pojawiają się w webpartach. Ponieważ serwer Web może wypełnić listę na podstawie zewnętrznego źródła danych, serwer Web nie musi być serwerem terminali.

Aby użytkownicy mieli dostęp do strony WWW z Internetu, można wykorzystać Bramę Usług Terminalowych, aby zabezpieczyć zdalne połączenia.

Wymagania klienta i konfiguracja

Aby możliwe było połączenie z TS Web Access, na komputerze klienckim musi być zainstalowany jeden z poniższych systemów operacyjnych:

- Windows Vista.
- Microsoft Windows XP z Service Pack 2 lub późniejszym.
- Windows Server 2008.
- Microsoft Windows Server 2003 z Service Pack 1 lub późniejszym.

Komputer kliencki musi być skonfigurowany w następujący sposób:

- Na komputerze klienckim musi być uruchomiony klient Remote Desktop Connection w wersji 6.0 lub późniejszej.
- Musi być włączona usługa Terminal Services ActiveX Client.
- Serwer TS Web Access musi być dodany do strefy Zaufanych Witryn lub Strefy Lokalnego Intranetu w przeglądarce Internet Explorer.

Praktyka

Wypełnianie webpartów TS RemoteApp

TS Web Access może wypełnić webparty TS RemoteApp, korzystając z jednego z poniższych źródeł danych:

- *Active Directory*. Jeśli usługa Active Directory jest określona jako źródło danych, lista programów zdalnych, która pojawia się w webpartach jest unikalna dla każdego użytkownika. Tylko pakiety .msi (z rozszerzeniem rap.msi), które są publikowane dla tego określonego użytkownika z wykorzystaniem Zasad Grup pojawiają się na liście.

- *Pojedynczy serwer terminali*. Jeśli pojedynczy serwer terminali jest określony jako źródło danych, lista dostępnych zdalnych programów, która pojawia się w webpartach, nie jest unikalna dla użytkownika. Zamiast tego, wszystkie zdalne programy, które zostały skonfigurowane jako dostępne przez WWW, znajdują się na liście Allow List na tym serwerze i pojawiają się na stronie internetowej.

Wykorzystanie usługi Active Directory jako źródła danych

Domyślnie, TS Web Access wypełnia listę programów TS RemoteApp z Active Directory. Kiedy Active Directory jest określone jako źródło danych, webpart TS Web Access jest wypełniana przez pakiety TS Remote App .msi, które są publikowane dla użytkownika poprzez Zasady Grup. Zalety tego rozwiązania są następujące:

- TS Web Access wyświetli tylko te pakiety, które są unikalne dla obecnego użytkownika.

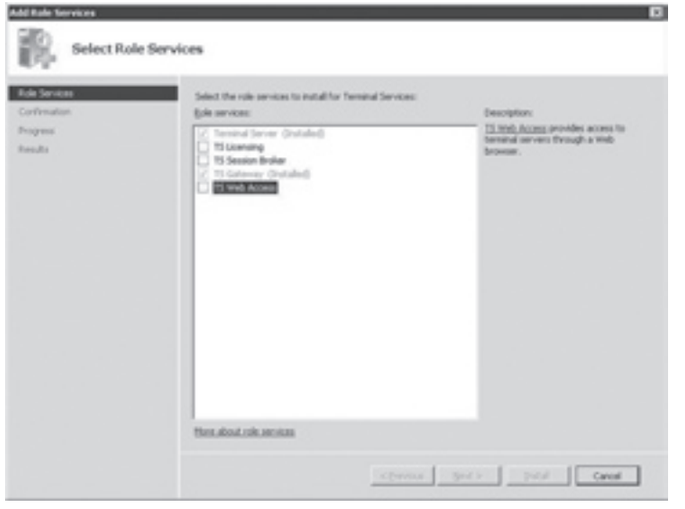
- Pakiety RemoteApp .msi, które kierują do innych serwerów terminali mogą zostać wszystkie skonsolidowane do postaci pojedynczej listy w webparcie TS Web Access.

Wykorzytanie pojedynczego serwera terminali jako źródła danych

Domyślnie, TS Web Access wypełnia listę programów TS RemoteApp z Active Directory. Jednakże, można skonfigurować webpart TS Web Access, aby wypełniał listę programów TS RemoteApp z pojedynczego serwera terminali. Kiedy pojedynczy serwer jest określony jako źródło danych, webpart jest wypełniany wszystkimi programami Ts RemoteApp, które zostały skonfigurowane w celu uzyskania dostępu do sieci na liście Allow List na serwerze, a lista wyświetlanych programów nie jest dostosowywana dla użytkownika.

Procedura: Instalacja i konfiguracja Usług Terminalowych dostępnych przez www

1. Aby zainstalować i skonfigurować dostęp do Usług terminalowych przez **www**, zaloguj się do swojego serwera jako **Administrator.** Z menu **Start** przejdź do pozycji **All Programs/Administrative Tools/Server Manager** i rozwiń drzewo **Roles/Terminal Services.** Zaznacz opcję **Terminal Services** i w panelu **Contents** wybierz pozycję **Add Roles Services.** Zostanie uruchomione okno dialogowe **Select Role Services**, w którym zaznacz opcję **TS Web Access**, a następnie wybierz przycisk **Add Required Role Services**. W drugim kroku uruchomionego kreatora zaznacz opcję **Web Server (IIS)** i kliknij przycisk **Next**. Kolejne okna kreatora pozostaw z ustawieniami domyślnymi, a w ostatnim oknie **Confirm Installation Selections** przeanalizuj podsumowanie i kliknij przycisk **Install**. Proces instalacji nie powinien zająć dłużej niż 3 do 5 minut.



2. Po zainstalowaniu i skonfigurowaniu Usług Terminalowych za pośrednictwem www aby uruchomić aplikację na stacji roboczej, będziesz musiał przejść kilka kroków. Zaloguj się na stacji roboczej, uruchom **Internet Explorer** i podaj adres swojego serwera, na którym zainstalowane są usługi www do obsługi **Usług Terminalowych** np.: **http://nazwa serwera/ts**. W oknie dialogowym **Connect to ...** podaj nazwę użytkownika i hasło. Na stronie www wybierz aplikację, a w oknie dialogowym **Windows Security** wpisz nazwę użytkownika i hasło. Po zatwierdzeniu wprowadzonych danych aplikacja zostanie uruchomiona.

Scenariusze wdrożenia/wykorzystania

Scentralizowany dostęp do aplikacji

Użytkownicy mogą uzyskać dostęp do aplikacji z dowolnej lokalizacji, łącząc się za pomocą przeglądarki internetowej z prostą stroną internetową.

Rozlokowanie nowych wersji
Wiele organizacji wolałoby udostępniać użytkownikom nowe wersje aplikacji (np. Office 2007). Jednakże, mogą pojawić się czynniki związane z zarządzaniem, sprzętem lub kosztami, które zabraniają rozlokowania aplikacji do lokalnych stanowisk. TS Web Access pomaga rozwiązać ten problem, umożliwiając użytkownikom wypróbowanie nowych cech aplikacji, zw ykorzystaniem istniejącej wersji produktu.

Zalecenia

Aby osiągnąć największe korzyści z rozlokowania TS Web Access, trzeba rozważyć następujące działania:

- W rozlokowaniu opartym na pojedynczym serwerze korzystać z domyślnych ustawień TS Web Access.
- W scenariuszu zakładającym wykorzystanie wielu serwerów:
  - Należy korzystać z Active Directory, gdy klienci mają doświadczenie z dystrybucją plików MSI poprzez Active Directory.
  - Jeśli klient nie posiada na miejscu mechanizmu rozlokowania MSI, należy skorzystać z innej metody, np. SMS, zaawansowane rozwiązanie bazujące na skryptach ASP, lub produktu innych firm.

Podsumowanie

TS Web Access pracujący w środowisku Windows Server 2008 udostępnia użytkownikom programy TS RemoteApp, z poziomu przeglądarki internetowej. Za pomocą TS Web Access użytkownik może odwiedzić stronę Web (z Internetu lub intranetu), aby uzyskać dostęp do listy dostępnych programów TS RemoteApp.

Zakończenie

Usługi Terminalowe w Windows Server 2008 są najpotężniejszą platformą aplikacyjną, jaka kiedykolwiek została wypuszczona na rynek przez firmę Microsoft. Usługi te oferują imponujący zakres możliwości, które radykalnie poprawiają jakość pracy administratorów i użytkowników z aplikacjami rozlokowanymi i zarządzanymi przy użyciu Usług Terminalowych.

Windows Server 2008 wspiera Usługi Terminalowe, dostarczając platformę o podwyższonym stopniu bezpieczeństwa, a zarazem łatwą w użytkowaniu, co zapewnia zdalny dostęp „z każdego miejsca" do aplikacji i zasobów zarządzanych centralnie.

Nowe cechy Usług Terminalowych umożliwiają dostęp do nich znacznie większej liczbie klientów. Dzięki nim możliwe jest także zastosowanie wielu nowych rozwiązań. Nowe scenariusze, takie jak rozlokowanie Biura Wydziałowego, zostały zoptymalizowane dla rozwiązań o niskim stopniu złożoności, aby jak najwięcej klientów mogło czerpać korzyści z możliwości oferowanych przez Usługi Terminalowe.

Nowe Opcje Usług Terminalowych w połączeniu z innymi możliwościami programu Windows Server 2008 dostarczają rozwiązań dla następujących scenariuszy:

- Zdalny Dostęp do Aplikacji.
- Zabezpieczenie Aplikacji i Danych (Zgodność Regulacyjna).
- Integracja Fuzji lub Outsourcing.
- Dyspozycyjni Użytkownicy Biura.

Zdalny Dostęp do Aplikacji umieszcza aplikację blisko potrzebnych danych i udostępnia je poprzez TS RemoteApp, TS Gateway i/lub TS Web Access, poprawiając reakcję aplikacji zarówno w odniesieniu do użytkowników zdalnych, jak i dostępnych w biurach wydziałowych. Funkcja TS Easy Print pozwala tym użytkownikom na pełne korzystanie ze wszelkich udogodnień, jakie oferuje praca w biurze.

Zabezpieczenie Aplikacji i Danych (Zgodność Regulacyjna) chroni aplikację i jej dane w lokalizacji centralnej, zmniejszając ryzyko przypadkowej utraty danych, spowodowanej na przykład utratą laptopa. Centralizacja aplikacji i danych minimalizuje ryzyko wydostania się ich poza sieć korporacyjną. Dzięki wykorzystaniu funkcji TS Gateway i TS RemoteApp, administratorzy nie muszą przekazywać już użytkownikom, partnerom ani klientom pełnego dostępu do sieci firmowej bądź komputerów, a nawet mogą go w razie potrzeby ograniczyć do pojedynczej aplikacji.

W przypadku fuzji przedsiębiorstw łączone firmy będą musiały korzystać ze spójnych aplikacji Linii Biznesowej [LOB] na różnych wersjach i konfiguracjach systemu Windows. Może to dotyczyć także stosowania outsourcingu dla organizacji partnerskich, które wymagają dostępu tylko do specyficznych aplikacji LOB, a nie do całej sieci korporacyjnej. Zamiast ponosić koszty rozmieszczenia wszystkich aplikacji LOB na wszystkich komputerach w przyłączonej firmie lub u outsourcera, pracownicy działu IT mogą zainstalować aplikacje LOB na serwerze usług terminalowych i udostępnić je za pomocą funkcji TS RemoteApp. Jest to szczególnie przydatne w sytuacji, gdy aplikację trudno wysłać lub nią zarządzać, gdy nie można jej rozpowszechnić za pomocą Microsoft Systems Management Server (SMS) lub gdy istnieją inne problemy związane z jej zarządzaniem.

W przedsiębiorstwie, w którym pracownicy nie mają przypisanych stanowisk pracy, użytkownicy mogą pracować każdego dnia na innym komputerze w biurze. W niektórych przypadkach komputer, z którego korzysta użytkownik, może nie mieć zainstalowanych potrzebnych mu programów. Dzięki Usługom Terminalowym specjaliści IT mogą zainstalować te programy na serwerze usług terminalowych i udostępnić je użytkownikom tak, jakby instalowali je lokalnie.

4. Bezpieczna administracja zdalnymi lokalizacjami

Wstęp

Bezpieczne zarządzanie danymi, usługami znajdującymi się w zdalnych lokalizacjach może być wyzwaniem dla nawet najbardziej doświadczonych pracowników IT. Windows Serwer 2008 wyposażony jest w liczne funkcjonalności, które pozwalają na utrzymanie zarządzalnej infrastruktury sieci komputerowych w lokalizacjach firmy nieposiadających zabezpieczeń, jakie istnieją w głównej siedzibie firmy.

Ważnym elementem w komunikacji pomiędzy filiami firmy, jest wydajność. Nowa architektura stosu protokołu TCP/IP i liczne ulepszenia w funkcjach sieciowych powinny zadowolić nawet najbardziej wymagających użytkowników sieci.

W tym rozdziale zostaną omówione cztery funkcjonalności Windows Server 2008. Dwie pierwsze mają kluczowe znaczenie dla bezpieczeństwa aktywnych katalogów i tym samym danych przechowywanych na serwerach pracujących w filiach naszej firmy.

- Kontroler domeny tylko do odczytu RODC (***Read Only Domain Controller***)
- BitLocker – szyfracja dysków

Dwie kolejne, dotyczą zagadnień związanych wydajnością i bezpieczeństwem transmisji danych w sieciach LAN/WAN opartych o stos TCP/IP nowej generacji (***New Generation TCP/IP stack***), który jest integralną częścią systemu Windows Serwer 2008.

- NetIO (***Network Input/Output?)***
- Blok komunikatów serwerów (SMB) 2.0

Kontroler domeny tylko do odczytu RODC (Read Only Domain Controller)

Wstęp

Kontroler domeny tylko do odczytu (RODC) to nowy typ kontrolera domeny dostępny tylko na platformie Windows Serwer 2008. RODC został stworzony przedewszystkim dla niewielkich lokalizacji naszych firm, które posiadają niewystarczające zabezpieczenia dostępu fizycznego

do serwerów, brak pewnego, stałego łącza do siedziby głównej i personel IT o niewielkiej wiedzy technicznej. Kontroler tylko-do-odczytu przetrzymuje pełną kopie bazy AD DS (wyjątkiem są tutaj hasła użytkowników i komputerów), ale tylko w trybie do odczytu. Zadaniem RODC jest przede wszystkim wsparcie procesów uwierzytelnienia i autoryzacji w obrębie danej lokalizacji. Administrator domeny wskazuje konta użytkowników i konta komputerów, których hasła mają być replikowane do RODC. Jeżeli RODC pełni również role serwera DNS i Wykazu Globalnego (Global Catalog) nie ma potrzeby kontaktu z innym kontrolerem, aby proces uwierzytelnienia użytkownika zakończył się sukcesem. Aplikacje lokalne, które żądają dostępu do odczytu do katalogu, uzyskują go. Aplikacje protokołu LDAP, które żądają dostępu do zapisu, otrzymują odpowiedź odsyłającą protokół LDAP, która kieruje je do zapisywalnego kontrolera domen, znajdującego się zwykle się w siedzibie głównej organizacji.

Active Directory tylko do odczytu

Kontroler domeny RODC przechowuje wszystkie te informacje o obiektach i atrybutach, które znajdują się na standardowym kontrolerze AD (oprócz haseł do kont). RODC nie pozwala jednak na wprowadzenie jakichkolwiek modyfikacji w replikach partycji, które posiada. Reasumując administracja aktywnymi katalogami lub próba wprowadzenia zmian, które mogłyby stanowić zagrożenie dla bazy AD jest po prostu nie możliwe w oparciu tylko i wyłącznie o komunikacje z RODC.

Replikacja jednokierunkowa

Ponieważ żadne zmiany w bazie AD nie mogą być realizowane na kontrolerze RODC, replikacja pomiędzy kontrolerem tylko-do-odczytu a pozostałym kontrolerami jest replikacją jednokierunkową. Tworzenie nowych obiektów, usuwanie i modyfikacja istniejących, jest realizowane w oparciu o kontroler, który posiada replikę partycji danych w trybie odczyt-zapis. Zmiany są replikowane do RODC. Ruch związany z replikacją AD jest dzięki temu znacznie mniejszy niż pomiędzy standardowymi kontrolerami, co powoduje znaczne zmniejszenie wykorzystywanej przepustowości łączy WAN.

System nazw domen (DNS) tylko do odczytu

System nazw domen (Domain Name System) funkcjonujący na kontrolerze RODC, może posiadać wszystkie partycje aplikacyjne przechowujące strefy DNS zintegrowane z AD, w szczególności ForestDnsZone i DomainDnsZone. Podobnie jak repliki partycji Aktywnych Katalogów, strefy te będą strefami tylko-do-odczytu. Reasumując, serwer DNS na kontrolerze RODC może obsłużyć żądanie rozwiązania nazwy, przez dowolny komputer kliencki, ale nie jest wstanie dokonać aktualizacji już istniejących rekordów w przetrzymywanych strefach. Replikacja tych stref pomiędzy standardowym kontrolerem a kontrolerem RODC jest jednokierunkowa.

Buforowanie Poświadczeń

Buforowanie poświadczeń należy rozumieć jako możliwość przechowywania niewielkich informacji dotyczących haseł kont użytkowników i komputerów, które umożliwią proces uwierzytelnienia. Domyślnie kontroler RODC nie przechowuje żadnych haseł obiektów AD, wyjątkiem jest konto kontrolera RODC i specjalne konto użytkownika Kerberos Ticket-Granting-Ticket (krbtgt_x), które jest tworzone w Aktywnych Katalogach dla każdego kontrolera RODC i służy do zabezpieczenia procesu uwierzytelnienia użytkowników i komputerów. Administrator domeny musi jawnie wskazać konta użytkowników i komputerów, których hasła mają być przechowywane na kontrolerze RODC.

Kontroler RODC stanowi centrum uwierzytelnień dla danej lokalizacji. (Oczywiście tej, w której kontroler domeny tylko-do-odczytu się znajduje). Użytkownik identyfikuje kontroler dzięki serwisowi DNS i wysyła żądanie wystawienia biletu TGT do kontrolera RODC. Jeżeli jest to pierwsze uwierzytelnienie użytkownika, kontroler RODC komunikuje się z najbliższym standardowym kontrolerem przetrzymującym replikę partycji danych w trybie odczyt-zapis i żąda kopi poświadczeń uwierzytelnienia użytkownika. Kontroler sztandarowy rozpoznaje kontroler RODC i weryfikuje politykę replikacji haseł dla danego RODC. Jeżeli poświadczenia danego użytkownika mogą być przechowywane przez RODC, od tej pory kontroler będzie je buforował (tym samym będzie miał możliwość wystawiania biletów TGT podpisywanych kontem krbtg RODC) aż do ich zmiany i kontakt ze standardowym kontrolerem nie będzie potrzebny.(Przy pierwszym uwierzytelnieniu bilet TGT zostanie wystawiony przez standardowy kontroler i podpisany kontem domenowym Krbtg) Oczywiście dla tych użytkowników i komputerów, których hasła nie są buforowane na RODC proces uwierzytelnienia zakończy się sukcesem, jeżeli standardowy kontroler posiadający replikę partycji danych odczyt-zapis będzie dostępny.
Domyślnie polityka replikacji haseł dla kontrolera RODC opiera się o członkostwo w dwóch grupach.

- **Allowed RODC Password Replication Group** – poświadczenia członków tej grupy mogą być replikowane do RODC. Grupa domyślnie pusta.
- **Denied RODC Password Replication Group** - poświadczenia członków tej grupy nie mogą być replikowane do RODC. Grupa domyślnie zawiera: Enterprise Domain Controllers, Enterprise Read-Only Domain Controllers, Group Policy Creator Owners, Domain Admins, Cert Publishers, Enterprise Admins, Schema, Admins, i domenowe konto krbtgt.

Wymagania wstępne

Instalacja kontrolera tylko-do-odczytu zakończy się sukcesem, jeżeli zostaną spełnione poniższe warunki.

- Upewnij się, że rola **PDC Emulator** jest położona na kontrolerze domeny opartym o Windows Serwer 2008 (tym samym przynajmniej jeden kontroler domeny musi być oparty o Windows Serwer 2008)
- Upewnij się, że minimalnym trybem funkcjonowania lasu Aktywnych Katalogów jest **Windows Serwer 2003**
- Rozszerz schemat AD dla prowidłowej replikacji stref DNS zintegrowanych z AD. (Uwaga operacja ta nie jest konieczna, jeżeli nie posiadasz kontrolerów domen starszych niż Windows serwer 2008 lub nie używasz stref DNS zintegrowanych z AD)

- Uwierzytelnij się na kontrolerze domeny z uprawnieniami Enterprise Administrator (operacje najlepiej wykonać z kontrolera pełniącego role Schema Master)

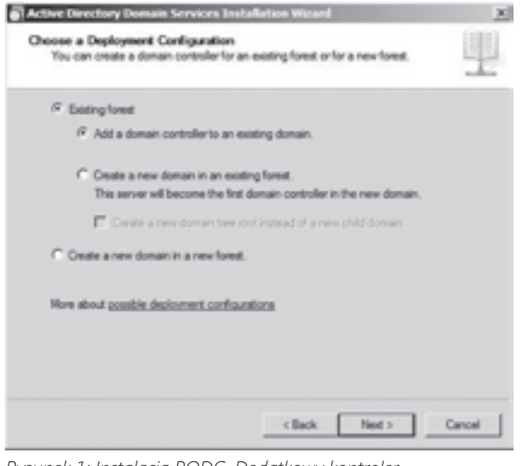
  a. Skopiuj zawartość katalogu \sources\adprep z płyty instalacyjnej Windows Serwer 2008 na dysk kontrolera domeny

  b. Nawigując do powyższego katalogu z linii poleceń wykonaj komendę adprep.exe /RODCprep

- Stały adres IP i prawidłowy adres serwera DNS obsługujący domene AD DS

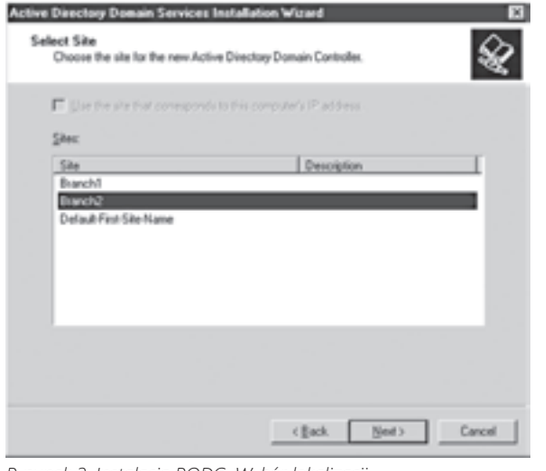
Instalacja RODC na pełnej platformie Windows Serwer 2008

1. Zaloguj się na serwerze jako członek grupy Domain Admins.
2. W menu **Start** naciśnij **Run** i wpisz **Dcpromo** i potwierdź klawiszem ENTER (Kreator instalacji Aktywnych Katalogów powinien zostać uruchomiony)
3. W pierwszym kroku kreatora wybierz **Use advanced mode installation** i potwierdź przyciskiem **Next.**
4. W oknie **Operating System Compatibility** potwierdź przyciskiem Next
5. W oknie **Choose a Deployment Configuration** wybierz **Existing forest** i potwierdź przyciskiem **Next**.



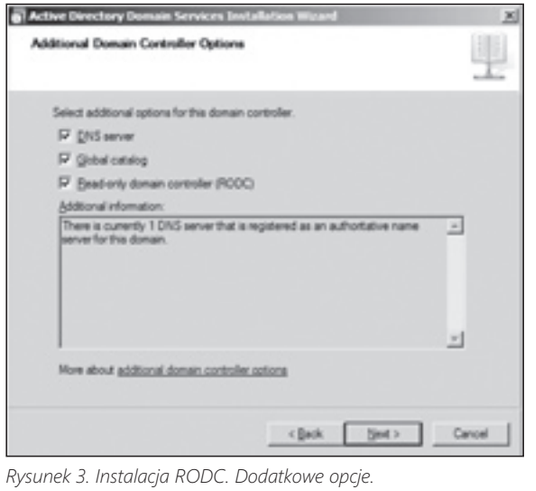
Rysunek 1: Instalacja RODC. Dodatkowy kontroler.

6. W oknie **Network Credentials** potwierdzamy nazwe domeny, w której będzie instalowany RODC i konto użytkownika w kontekście, którego przeprowadzamy instalację. Ponieważ serwer jest członkiem domeny i aktualnie zalogowany użytkownik posiada uprawnienia Domain Admins, potwierdzamy przyciskiem **Next**. (Jeżeli serwer nie jest członkiem domeny nazwe domeny i konto użytkownika domenowego trzeba wprowadzić ręcznie)
7. W oknie **Select Domain** wskazujemy obiekt domeny i potwierdzamy przyciskiem **Next**
8. W oknie **Select Site** wybieramy właściwą lokalizacje, potwierdzamy przyciskiem **Next**



Rysunek 2. Instalacja RODC. Wybór lokalizacji.

9. W oknie **Additional Domain Controller Options** zaznacz **Read-only domain Controller (RODC)** (opcje **DNS server** i **Global catalog** zaznaczone są domyślnie)



Rysunek 3. Instalacja RODC. Dodatkowe opcje.

10. W oknie **Specify the Password Replication Policy** możemy zdefiniować politykę replikacji haseł dla kontrolera RODC. Wskazujemy grupy użytkowników, których hasła mają być replikowane (tryb **Allow**) i grupy użytkowników, których hasła nie mogą być replikowane (tryb **Deny**). Politykę replikacji haseł można zdefiniować i modyfikować w dowolnym momencie po instalacji kontrolera RODC.
11. W oknie **Delegation od RDOC Instalation and Administration** wskazujemy obiekt grupy lub konto użytkownika, który będzie miał prawa administracyjne do kontrolera RDOC (wskazany kontekst bezpieczeństwa zostanie użyty do dokończenia instalacji)
12. W oknie **Install from Media** kreator daje nam możliwość instalacji kontrolera na podstawie wykonanej kopii zapasowej już istniejącego dowolnego kontrolera domeny. (kopie bazy AD można wykonać z dowolnego kontrolera w oparciu o konsole NTDSUTIL, polecenie **ifm**). Przyciskiem **Next** potwierdzamy domyślną opcje **Replicate data over network from an existing domain controller.**
13. W oknie **Source Domain Controller** wskazujemy kontroler domeny, z którego ma nastąpić ściągniecie replik AD DS, lub pozostawiamy wybór kreatorowi. Potwierdzamy przyciskiem **Next.**
14. Wybierz domyślną lokalizacje plików bazy Aktywnych Katalogów, logów i katalogu SYSVOL, potwierdź klawiszem **Next**
15. Wpisz i potwierdź hasło dla trybu **Directory Services Restore Mode**, potwierdź klawiszem **Next**
16. W oknie **Summary** potwierdź klawiszem **Next**
17. Potwierdź restart systemu

Instalacja RODC na Windows Serwer 2008 Server Core

Instalacja RODC na platformie Server Core jest realizowana w trybie instalacji niepilnowanej przy wykorzystaniu pliku odpowiedzi i wywołaniu kreatora Dcpromo w trybie „cichym" **Dcpromo /unattended:ŚcieżkaDoPlikuOdpowiedzi**

1. Zainstaluj Windows Serwer 2008 w trybie Serwer Core
2. Przygotuj plik odpowiedzi do instalacji niepilnowanej.
   (Przykład pliku odpowiedzi poniżej)

```
[DCInstall]

InstallDNS=Yes

ConfirmGc=No

CriticalReplicationOnly=No

DisableCancelForDnsInstall=No

PasswordReplicationAllowed=Nazwy grup, których członkowie będą posiadali możliwość przechowywania haseł na RDOC (konwencja LDAP)

PasswordReplicationDenied= Nazwy grup, których członkowie nie będą posiadali możliwość przechowywania haseł na RDOC (konwencja LDAP)

Password=hasło użytkownika posiadającego uprawnienia Domain Admins

RebootOnCompletion=No

ReplicaDomainDNSName=pełna nazwa domeny w konwencji DNS

ReplicaOrNewDomain=ReadOnlyReplica

ReplicationSourceDC=nazwa kontrolera domeny Windows Server 2008 w tej samej domenie

SafeModeAdminPassword= hasło dla trybu Directory Services Restore Mode

SiteName=nazwa lokalizacji, w której będzie funkcjonował RDOC

UserDomain=nazwa domeny

UserName=nazwa konta posiadającego uprawnienia Domain Admins
```

*Sekcje PasswordReplicationAllowe i PasswordReplicationDenied są opcjonalne.

3. Zaloguj się na konsole serwera z uprawnieniami Domain Admins
4. Wywołaj z linii poleceń **Dcpromo /unattended:ŚcieżkaDoPlikuOdpowiedzi**

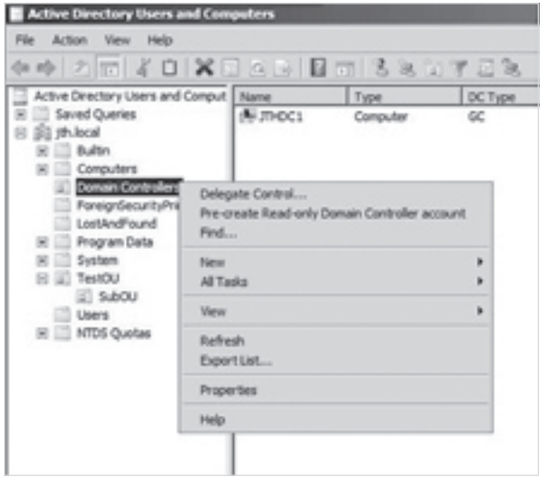
Instalacja RODC w trybie delegacji uprawnień

Instalacja RODC w trybie delegacji składa się z dwóch etapów. Pierwszy polega na stworzeniu i konfiguracji konta dla nowego kontrolera RODC w AD DS i wymaga uprawnień Domain Admins. Drugi etap to stowarzyszenie fizycznego komputera, na którym instalujemy RODC z uprzednio stworzonym kontem w AD DS. Proces ten wykonywany jest z kontekstu bezpieczeństwa grupy wskazanej podczas realizacji pierwszego etapu i nie koniecznie posiadającej uprawnienia administracyjne w obrębie domeny. Serwer, na którym instalujemy kontroler RODC nie może być członkiem domeny AD, dla której będzie pełnił role kontrolera. Ten typ instalacji zalecany jest w sytuacji, kiedy nie chcemy, aby osoby instalujące RODC w fili firmy posiadały uprawnienia administracyjne w obrębie domeny.

Stworzenie konta dla nowego kontrolera RODC w AD DS

1. Uwierzytelnij się na konsoli istniejącego kontrolera z uprawnieniami Domain Admins
2. Uruchom konsole **Active Directory Users and Computers**

3. Rozwiń obiekt domeny i zaznacz Domain Controllers OU. W meni podręcznym (prawy klik myszki) wybierz opcje **Pre-create Read-only Domain Controller account.** Kreator instalacji AD DS powinien zostać uruchomiony.



Rysunek 4: Tworzenie konta kontrolera RODC

4. W pierwszym kroku kreatora wybierz **Use advanced mode installation** i potwierdź przyciskiem **Next.**

5. W oknie **Network Credentials** potwierdzamy nazwę domeny i konto użytkownika które zostanie użyte do stworzenia konta RODC. Potwierdzamy przyciskiem **Next**

Rysunek 5. Kontekst bezpieczeństwa instalacji RODC

6. W oknie **Specify the Computer Name** wprowadzamy nazwę komputera na którym ma funkcjonować RODC

7. W oknie **Select a Site** wskazujemy lokalizacje dla RODC

8. W oknie **Additional Domain Controller Options** opcje **DNS server** i **Global catalog** zaznaczone są domyślnie. Opcja **Read only domain Controller (RODC)** jest zaznaczona domyślnie również i nie można jej odznaczyć.

9. W oknie **Specify the Password Replication Policy** możemy zdefiniować politykę replikacji haseł dla kontrolera RODC. Wskazujemy grupy użytkowników, których hasła mają być replikowane (tryb **Allow**) i grupy użytkowników, których hasła nie mogą być replikowane (tryb **Deny**). Politykę replikacji haseł można zdefiniować i modyfikować w dowolnym momencie po instalacji kontrolera RODC.

10. W oknie **Delegation of RODC Installation and Administration** wskazujemy obiekt grupy lub konto użytkownika który będzie miał prawa administracyjne do kontrolera RDOC. (Wskazany kontekst bezpieczeństwa zostanie użyty do dokończenia instalacji) Jezeli konto nie zostanie wskazane tylko członkowie grup Domain Admins lub Enterprise Admins będą mogli dokończyć instalację.

Rysunek 6. Delegacja uprawnień administracyjnych dla RODC

11. W oknie **Summary**, potwierdź ustawienia przyciskiem **Next**

12. W oknie **Completing the Active Directory Domain Services Installation Wizard** zakończ operację przyciskiem **Finish**

Instalacja i stowarzyszenie RODC z kontem w AD DS

1. Zaloguj się na serwer jako lokalny administrator
2. Z linii poleć wprowadź **dcpromo /UseExistingAccount:Attach.** Kreator instalacji AD DS powinien zostać uruchomiony.
3. W pierwszym kroku kreatora wybierz **Use advanced mode installation** i potwierdź przyciskiem **Next.**
4. W oknie **Network Credentials** wprowadzamynazwe domeny w której będzie instalowany RODC i konto użytkownika w kontekście, którego przeprowadzamy instalację. (Konto to może być ustalone w trakcie Etapu I i nie musi mieć uprawnień administracyjnych w obrębie domeny) Potwierdzamy przyciskiem **Next**.
5. W oknie **Select Domain Controller Account** potwierdzamy konto kontrolera RODC znalezione w AD i zgodne z nazwą serwera RODC.
6. W oknie **Install from Mednia** kreator daje nam możliwość instalacji kontrolera na podstawie wykonanej kopii zapasowej już istniejącego dowolnego kontrolera domeny. (Kopie bazy AD można wykonać z dowolnego kontrolera w oparciu o konsole NTDSUTIL, polecenie **ifm**). Przyciskiem **Next** potwierdzamy domyślną opcje **Replicate data over network from an existing domain controller.**
7. W oknie **Source Domain Controller** wskazujemy kontroler domeny, z którego ma nastąpić ściągniecie replik AD DS, lub pozostawiamy wybór kreatorowi. Potwierdzamy przyciskiem **Next.**
8. W oknie **Location for Database, Log Files, and SYSVOL** wybierz domyślną lokalizacje plików bazy Aktywnych Katalogów, logów i katalogu SYSVOL, potwierdź klawiszem **Next**
9. Wpisz i potwierdź hasło dla trybu **Directory Services Restore Mode**, potwierdź klawiszem **Next**
10. W oknie **Summary** potwierdź klawiszem **Next**
11. Potwierdź restart systemu

Delegowanie uprawnień lokalnego Administratora RODC

Domyślnie uprawnienia administratora na kontrolerze RODC posiadają członkowie grup Domain Admins, Enterprise Admins i grupa (lub konto użytkownika), które zostało wskazane w trakcie instalacji RODC (sekcja **Delegation of RODC Installation and Administration** instalatora DCPROMO). Nadanie uprawnień lokalnego administratora dla dodatkowych operatorów kontrolera RODC można zrealizować przy użyciu konsoli DSMGMT.

1. Zaloguj się na konsole serwera RODC na użytkownika z uprawnieniami administracyjnymi.
2. Uruchom z linii poleceń aplikacje DSMGMT.EXE (każdą poniższą operacje potwierdź klawiszem ENTER)

   Local Roles

   Add *NazwaDomeny\NazwaUzytkownika* Administrators

   Quit

   Quit

Konfiguracja polityki replikacji haseł dla kontrolera RODC

Jeżeli konfiguracja polityki replikacji haseł dla kontrolera RODC nie została zdefiniowana w trakcje instalacji kontrolera można ją skonfigurować dowolnym momencie po instalacji. Do konfiguracji polityki potrzebne są uprawnienia Domain Admins. Polityka replikacji haseł jednoznacznie definiuje, dla jakich użytkowników domeny, hasła będą replikowane do kontrolera RODC. Domyślnie jedynie hasła członków grupy **Allowe RODC Password Replication Group** będą replikowane do RODC (domyślnie grupa ta jest grupą pustą) Sterowanie członkostwem tej grupy daje możliwość określenia zbiorowości użytkowników, dla których proces uwierzytelnienia będzie się opierał wyłącznie o komunikacje z serwerem RODC. Wskazanie dodatkowych grup użytkowników i komputerów, których hasła mają być replikowane do RODC wymaga konfiguracji polityki replikacji haseł dla RODC.

1. Uruchom konsole **Active Directory Users and Computers** z uprawnieniami Domain Admins
2. Zaznacz konto kontrolera RODC (domyślnie Domain Controllers OU) i wywołaj właściwości obiektu.(Prawy klik myszki, opcja **Properties)**
3. Uaktywnij zakładkę **Password Replication Policy**
4. Przyciskiem **Add** wskaż obiekty grupy (w trybie **Allow**). Hasła członków tej grupy będą replikowane do RODC.
5. Przyciskiem **Add** wskaż obiekty grupy (w trybie **Deny**). Hasła członków tej grupy nie będą replikowane do RODC.

Uwaga! Wskazując użytkowników, których hasła mają być replikowane do RODC należy pamiętać o kontach komputerów na których ci użytkownicy pracują. Hasła kont komputerów także powinny być replikowane do RODC, w przeciwnym wypadku komputer operujący w domenie nie będzie w stanie potwierdzić swojej tożsamości tylko w oparciu o dostęp do kontrolera RODC.

Rysunek 7. Konfiguracja polityki replikacji haseł dla RODC

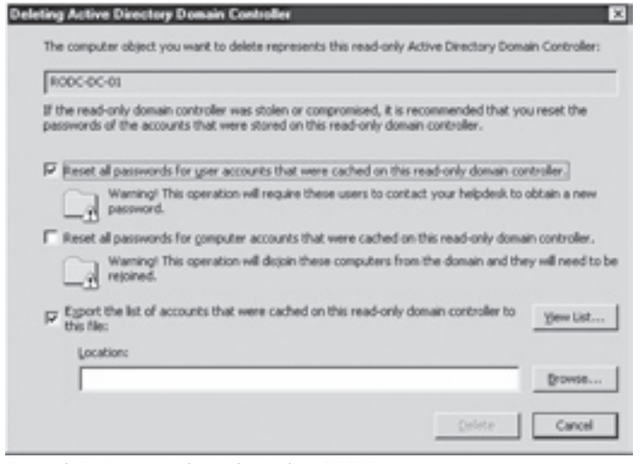
Domyślnie hasła użytkowników będą replikowane do RODC przy pierwszym uwierzytelnieniu użytkownika. W zakładce **Password Replication Policy** po włączeniu przycisku **Advanced** możesz wskazać konta użytkowników, których hasła mają być natychmiast przereplikowane do RODC (przycisk **Prepopulated Passwords...**) lub otrzymać informację dotyczącą kont użytkowników , którzy zostali już uwierzytelnieni przez kontroler RODC (**Accounts that have been authenticated to this Read-only Domain Controller**) i dla których RODC posiada hasła. (**Accounts whose password are stored on this Read-only Domain Controller**)

Reset haseł przechowywanych na kontrolerze RODC.

Poniższa procedura powinna być wykonana w sytuacji kiedy kontroler RODC został skradziony lub zgubiony.

Skasowanie konta kontrolera tylko-do-odczytu i reset haseł użytkowników i komputerów, które były przechowywane na RODC spowoduje że wszelkie próby „wyciągnięcia" haseł z takiego kontrolera będą bezcelowe.

1. Uruchom konsole **Active Directory Users and Computers** z uprawnieniami Domain Admins
2. Zaznacz konto kontrolera RODC (domyślnie Domain Controlersl OU) i rozpocznij procedurę usunięcia konta RODC.(prawy klik myszki, opcja **Delete)**
3. W oknie **Deleting Active Directory Domain Controllers** upewnij się że opcja **Reset all password for users that were cached on this read-only domain controller** jest zaznaczona. Hasła użytkowników, które były replikowane do RODC zostaną zresetowane. Użytkownik będzie zmuszony zmienić hasło. Zaznaczenie opcji **Reset all password for computer accounts that were cached on this read-only domain controller** spowoduje reset haseł kont komputerów i wymusi powtórne dołączenie ich do domeny.



Rysunek 8. Kasowanie konta kontrolera RODC

4. Potwierdź operacje przyciskiem **Delete**

BitLocker Drive Encryption (BDE) – szyfracja dysków

Do czego i dla kogo?

Bitlocker Drive Encryption (BDE) to funkcjonalność implementowana w systemach Windows Serwer 2008 i Windows Vista, (w wersjach Ultimate i Enterprise) która ma za zadanie chronić dane przechowywane na twardych dyskach. Funkcja ta jest szczególnie atrakcyjna dla pracowników firmy wykorzystujących komputery przenośne i dla serwerów znajdujących się w filiach firm gdzie zabezpieczenie pomieszczenia serwerowni może być niedostateczne.

Utrata ważnych danych, ujawnienie ich, nieprawidłowe wykorzystanie przez osoby trzecie może być katastrofalne w skutkach dla wielu firm. Szyfracja partycji dyskowych, którą realizuje BitLocker daje gwarancje poufności i bezpieczeństwa danych znajdujących się na chronionych dyskach nawet wtedy kiedy trafią one w niepowołane ręce.

BitLocker podnosi poziom ochrony danych dzięki połączeniu dwóch głównych funkcji składowych: szyfrowaniu woluminu systemowego oraz sprawdzaniu integralności przez

komponenty uruchamiania systemu. Cały wolumin systemowy jest szyfrowany, łącznie z plikami wymiany i hibernacji. BitLocker chroni przed kradzieżą danych oraz problemami ze zgubionymi, skradzionymi i wyrzuconymi komputerami. BitLocker pomaga również organizacjom w spełnianiu wymagań rządowych, takich jak np. amerykańskie ustawy Sarbanes-Oxley i HIPAA, które wymagają bardzo wysokich standardów zabezpieczeń i ochrony danych.

Szyfracja danych

Potrzebne są przynajmniej dwie partycje. Jedna o zalecanej wielkości 1,5G tzw partycja rozruchowa, która pozostanie niezaszyfrowana i na której będzie przechowywany klucz symetryczny VEK (Volume Encryption Key) służący do szyfracji i deszyfracji danych na partycji systemowej. BitLocker oferuje nam możliwość użycia klucza 128 lub 256 bitowego zgodnego z algorytmem AES (Advanced Encryption Standard). Należy zdawać sobie sprawę, że partycja rozruchowa pozostanie w stanie niezaszyfrowanym, więc umieszczanie tam jakichkolwiek ważnych danych jest niewskazane. Druga partycja, to partycja systemowa, która będzie szyfrowana za pomocą klucza VLK (oczywiście istnieje możliwość szyfracji dowolnej ilości partycji) Jeżeli decydujemy się na implementacje BitLockera przed instalacją systemu operacyjnego, możliwość stworzenia odpowiednich partycji oferuje nam instalator systemu. Jeżeli jednak posiadamy już zainstalowany system z partycją z danymi, która zajmuje cały dysk jesteśmy zmuszeni ją zmniejszyć tak aby wygospodarować przynajmniej 1,5G wolnej przestrzeni dla partycji rozruchowej. Do zmniejszania partycji (również takiej , która zawiera już dane) służy polecenie SHRINK systemowego programu DISKPART. W trybie już działającego BitLockera, klucz VLK posłuży do zaszyfrowania każdego sektora na partycji systemowej zawierającego dane. Proces ten jest zupełnie nie zauważalny dla użytkownika jak i uruchamianych aplikacji. Sterownik FVE odpowiedzialny za szyfrację sektorów dyskowych jest umieszczony bardzo nisko w systemie operacyjnym i od danych dzieli go tylko Volume Manager i sterowniki dyskowe. FVE dostaje dane, gdy tylko zostaną one odczytane i od razu je deszyfruje. Każdy inny element systemu, aplikacje operują już wyłącznie na danych rozszyfrowanych. Zapis jest realizowany bardzo podobnie, FVE szyfruje dane tuż przed zapisem na dysk. Dane, które nie są aktualnie używane pozostają w stanie zaszyfrowanym. W trakcje inicjalizacji BitLockera sterownik FVE ma trochę więcej pracy. Oprócz obsługi żądań odczytu i zapisu w trybie rzeczywistym (i tym samym szyfracji danych) FVE szyfruje sektor po sektorze aż wszystkie dane niebędące aktualnie używane zostaną zaszyfrowane. Szybkość tego procesu w dużej mierze jest zależny od mocy procesora, wielkości dysku i może trwać wiele godzin.

Ochrona klucza VEK

Klucz VEK, który służy do szyfracji partycji dyskowych jest przechowywany na partycji rozruchowej (niezaszyfrowanej). Klucz VEK może być zaszyfrowany i tym samym chroniony w oparciu o jeden z dwóch mechanizmów.

Pierwszy i zalecany, opiera się o wykorzystanie modułu sprzętowego TPM w wersji 1.2 (Trusted Platform Module). Moduł TPM został opracowany przez organizację Trusted Computing Group (http://www.trustedcomputinggroup.org) i jest w tej chwili powszechnie implementowany przez producentów sprzętu komputerowego. Założeniem twórców TPMa było umieszczenie sprzętowego modułu kryptograficznego na płycie głównej komputera, który będzie wykonywał operacje kryptograficzne i dostarczał powszechnie używanych algorytmów (między innymi RSA, SHA-1, HMAC i AES) jednocześnie gwarantując ich bezpieczeństwo. TPM jest również wstanie wyliczyć sumę kontrolną z aktualnie wykonywanego kodu przez procesor w postaci tzw. ciągów SRK (Storage Root Key)
Ta funkcjonalność jest wykorzystywana przez BitLockera, który żąda od TPMa (w momencie uruchamiania komputera) sumy kontrolnej policzonej z kodu sekwencji startowej. Tak wyliczony SRK przez moduł TPM pozwala na wygenerowania klucza VMK (Volume Master Key), który posłuży do deszyfracji klucza VLK. TPM nie przetrzymuje ciągu SRK, wylicza go każdorazowo przy starcie komputera. Oznacza to że jeżeli kod startowy ulegnie zmianie (np: dysk zostanie przełożony do innego komputera, zmiana moduł TPM, utrata integralności, zmiany plików startowych, zmiany w Master Boot Records lub sektorach startowych) wyliczony SRK nie będzie mógł być użyty do prawidłowej deszyfracji klucza VEK i tym samym prawidłowego startu systemu operacyjnego. Należy zwrócić uwagę, że proces ten może być całkowicie transparentny dla użytkownika uruchamiającego komputer o ile oczywiście TPM pracuje w „znanym otoczeniu". Dodatkową ochroną tego mechanizmu może być wymuszenie podania PINu składającego się od 4 do 20 cyfr, który posłuży do prawidłowego wyliczenia i użycia SRK (opcja TPM with PIN) lub dostarczenie odpowiedniego klucza startowego (startup key) na nośniku USB (opcja TPM with USB)

Druga metoda pozwala na użycie BitLockera bez modułu TPM. Klucz startowy (startup key) musi być umieszczony na napędzie USB i każdorazowo przy starcie systemu będzie stamtąd pobierany aby BitLocker mógł prawidłowo dokonać deszyfracji VLK i tym samym deszyfrować dane na partycji systemowej.

Sytuacje awaryjne

Pozostaje pytanie, co się stanie jeżeli administrator wgra nową wersje BIOSu, lub zmieni pliki startowe instalując łatki systemowe bądź w jakikolwiek (oczywiście słuszny) dokona modyfikacji sekwencji startowej tak, że wyliczony SRK nie będzie dawał możliwości prawidłowej deszyfracji klucza VLK ? Twórcy BitLockera przewidzieli taką sytuację. Administrator ma możliwość posłużenia się 48 cyfrowym kluczem (recovery password), który jest wpisywany z klawiatury komputera, jeżeli system nie jest w stanie odszyfrować klucza VLK. W praktyce oznacza to, że klucz VLK może być szyfrowany wielokrotnie różnymi mechanizmami i wiele jego chronionych kopii może istnieć na partycji startowej. Inną metodą jest wygenerowanie tzw. „recoyery key" w trakcie inicjalizacji BitLockera i w sytuacji awaryjnej dostarczenie go systemowi na napędzie USB.(klucze te mogą być również przetrzymywane w aktywnych katalogach, lub w postaci plików) Jeżeli administrator przewiduje operację, która zmieni kod sekwencji startowej może wygenerować tzw. „clear key", który w stanie jawnym jest składowany na partycji startowej na czas realizowanej operacji (np: wgranie nowej wersji BIOS, instalacja *service pack*). Oczywiście w tym czasie sprawdzanie poprawności, integralności sekwencji startowej jest czasowo wyłączona.

Szyfracja dodatkowych dysków

Obecnie interfejs graficzny BitLockera nie daje możliwości szyfracji dysków innych niż systemowy. Szyfracja partycji innych niż partycja systemowa (w tym również partycji systemowej) jest możliwe poprzez uruchomienie skryptu **manage-bde.wsf** z odpowiednimi parametrami linii poleceń (plik ten znajduje się w folderze *system32* katalogu systemowego). Klucze VEK szyfrujące dodatkowe partycje mogą być przechowywane w rejestrze systemu operacyjnego (opcja zalecana, partycje dodatkowe są automatycznie deszyfrowane po deszyfracji partycji systemowej) lub zabezpieczone i złożone na nośniku USB.

Najistotniejszym parametrem linii poleceń skryptu jest parametr *–h*, który dostarczy nam informacje pomocy na temat pozostałych parametrów. Oto niektóre z nich:

- „**status**" – wyświetla bieżące informacje na temat dysków. W informacjach tych znajdują się dane na temat rozmiaru partycji, postępu szyfrowania, stosowanego algorytmu oraz dane o sposobie zaszyfrowania VEK.
- „**on**" – włącza szyfrowanie dla wybranego dysku. Opcja ta pozwala na wybranie algorytmu szyfrowania i wybranie metody, którą wyliczany jest VEK.
- „**off**" – rozszyfrowuje wskazany dysk
- „**pause**" i „**resume**" – wstrzymywanie i wznawianie procesu szyfrowania dysku
- „**lock**" i „**unlock**" – włącza i wyłącza dostęp do dysku w systemie. Domyślnie, po restarcie wszystkie niesystemowe dyski są w stanie „lock" i trzeba podając klucz je włączyć, żeby móc z nich skorzystać
- „**autounlock**" – umożliwia zapisanie klucza w rejestrze, przez co dysk ma automatycznie wykonywaną operację „unlock" przy każdym starcie systemu. Jest to w praktyce bardzo użyteczna funkcjonalność
- „**protectors**" – zarządza kluczami pozwalającymi rozszyfrować VEK. Dzięki tej opcji możliwe jest dodanie dowolnej ilości kluczy liczbowych i plikowych dla każdego zabezpieczanego dysku.

W praktyce użycie skryptu **manage-bde.wsf** jest o wiele bardziej efektywna niż użycie interfejsu graficznego BDE.

Konfiguracja BDE poprzez GPO (Group Policy Object)

Zestaw polityk konfiguracjących BitLockera znajduje się w każdym obiekcie GPO definiowanym w obrębie Aktywnych Katalogów. Lokalne GPO również posiadają definicje polityk wspierających BDE. W obu przypadkach należy otworzyć kontekst:

Computer Configuration\Administrative Templates\Windows Componets\BitLocker Drive Encryptions

Znajdziemy tam siedem polityk, które pomogą skonfigurować BDE zgodnie z przyjętymi założeniami.

1. **Turn on BitLocker Backup to Active Directory Services** - politka umożliwia archiwizację hasła odzyskiwania (recovery password) i kluczy do AD
2. **Control Panel Setup: Configure recover folder** – wskazanie domyślnej lokalizacji przechowywania hasła odzyskiwania. Przy uruchomieniu kreatora szyfracji i wyborze opcji **Save the password in a folder** wskazana siceżka dostępu, pojawi się automatycznie.
3. **Control Panel Setup: Configure recover Options –** konfiguracja metod odzyskiwania. Do wyboru możliwość użycia hasła odzyskiwania i (lub) klucza odzyskiwania (na nośniku USB)
4. **Control Panel Setup: Enabled advanced startup options** – możliwość definicji opcji zaawansowanych w kreatorze Bitlockera. Domyślnie kreator proponuje jedynie sprawdzanie sekwencji startowej w oparciu o moduł TPM. Plityka pozwala na możliwość dodatkowego wyboru pomiędzy powyższą opcja a opcjami *TPM with PIN*, *TPM with USB*.
5. **Configure encryption method –** Domyślnym algorytmem szyfrowania danych jest AES 128bit. Polityka daje możliwość włączenia trybu AES 256bit (dodatkowo możliwość włączenia lub wyłączenia dyfuzora)
6. **Prevent memory overwrite on restart –** zapobieganie czyszczenia pamięci RAM z danych poufnych umieszczonych tam prze BiltLockera w trakcie restartu.
7. **Configure platform validation profile –** polityka definiuje element startowe, które są sprawdzane przez TPM w trakcie rozruchu komputera.

Wymagania sprzętowe

- komputer spełniający minimalne wymagania dla Windows Serwer 2008 (Windows Vista Enterprise lub Ultimate)
- mikrochip TPM, wersja 1.2, włączony (dla opcji z TPM),
- BIOS spełniający standardy organizacji Trusted Computing Group (TCG) (dla opcji z TPM),
- dwie partycje NTFS na dysku, jedna na wolumen systemowy, a druga na wolumen startowy. Partycja systemowa musi mieć co najmniej 1,5 GB i być partycją aktywną,
- ustawienia BIOSu wskazujące na dysk twardy, jako pierwsze urządzenie startowe, nie na napędy USB czy CD.

Uwaga: Przy każdym teście z napędem flash USB, BIOS musi wspierać odczyt flash USB przy starcie systemu.

Partycjonowanie dysku bez systemu operacyjnego pod kątem funkcji BitLocker

Podczas tej procedury należy uruchomić komputer z DVD Windows serwew 2008, a następnie wprowadzić serię komend, aby wykonać następujące czynności:

- utworzyć nową partycję o rozmiarze 1,5 GB,
- oznaczyć tę partycję jako aktywną,
- utworzyć drugą partycję podstawową, wykorzystując pozostałe miejsce na dysku,
- sformatować obie nowe partycje, aby mogły być wykorzystane jako wolumeny Windows,
- zainstalować Windows Serwer 2008 na większym wolumenie (dysk C).

Aby spartycjonować dysk bez systemu operacyjnego dla BitLocker:

1. Uruchom komputer z płyty DVD z systemem Windows Serwer 2008.
2. Na początkowym ekranie **Install Windows**, wybierz **Installation language**, **Time and currency format** oraz **Keyboard layout** (język instalacji, format czasu i waluty, układ klawiatury), a następnie kliknij **Next**.
3. Na kolejnym ekranie **Install Windows**, kliknij opcję **System Recovery Options** (opcje odzyskiwania systemu) umiejscowione w lewym dolnym rogu ekranu.
4. W oknie dialogowym **System Recovery Options**, wybierz swój układ klawiatury, a następnie kliknij Next.
5. W kolejnym oknie dialogowym **System Recovery Options** upewnij się, że nie został wybrany żaden system operacyjny. Aby to zrobić, kliknij w pustym obszarze listy Operating Systems, poniżej wszystkich wymienionych pozycji. Następnie kliknij **Next**.
6. W kolejnym oknie dialogowym **System Recovery Options,** kliknij na **Command Prompt**.
7. Użyj funkcji Diskpart do stworzenia partycji na wolumen startowy. W wierszu poleceń wpisz **diskpart**, a następnie wciśnij ENTER.
8. Wpisz select *disk 0*.
9. Wpisz clean, aby wymazać istniejącą tablicę partycji.
10. Wpisz *create partition primary size=1500* , aby utworzyć partycję, która będzie partycją rozruchową.

11. Wpisz *assign letter=D* aby nadać tej partycji oznaczenie D.
12. Wpisz *active*, aby ustawić nową partycję jako aktywną.
13. Wpisz *create partition primary*, aby utworzyć inną partycję systemową. Będziesz instalował Windows na tej większej partycji.
14. Wpisz *assign letter=C* aby nadać tej partycji oznaczenie C.
15. Wpisz *list volume*, aby zobaczyć listę wszystkich wolumenów na dysku.
16. Wpisz *exit*, aby opuścić aplikację diskpart.
17. Wpisz *format c: /y/q/fs:NTFS*, aby prawidłowo sformatować wolumen C.
18. Wpisz *format s: /y/q/fs:NTFS*, aby prawidłowo sformatować wolumen D.
19. Wpisz exit, aby opuścić wiersz poleceń.
20. W oknie **System Recovery Options**, użyj ikony zamykania okna w górnym prawym rogu (lub naciśnij ALT+F4), aby zamknąć okno i powrócić do głównego ekranu instalacyjnego.
21. Kliknij na **Install now** i kontynuuj proces instalacji systemu Windows Server 2008.

Włączanie funkcji BitLocker Drive Encryption (BDE)

- Przed włączeniem BitLockera należy go doinstalować (Bitlocker instalowany jest jako funkcjonalność z konsoli Server Manager).
- Przed wykonaniem poniższej operacji można również dokonać jednorazowej inicjalizacji modułu TPM poprzez konsole TPM.msc.(oczywiście jeżeli płyta główna naszego komputera jest wyposażona w moduł TPM). (http://technet2.microsoft.com/WindowsVista/en/library/29201194-5e2b-46d0-9c77-d17c25c56af31033.mspx?mfr=true)
- Procedura zakłada wykorzystanie opcji zaawansowanych włączanych w polityce **Control Panel Setup: Enabled advanced startup options**
- Dla BDE bez modułu TPM, pomiń punkty 4 i 5.
- Dla BDE z modułem TPM, pomiń punkty 6 i 7.

1. Kliknij przycisk **Start**, następnie opcję **Control Panel** i opcję **BitLocker Drive Encryption.**
2. Na stronie **BitLocker Drive Encryption,** kliknij opcję **Turn On BitLocker** na wolumenie systemowym.

Jeśli TPM nie jest uruchomiony, zobaczysz kreator Initialize TPM Security Hardware. Postępuj zgodnie ze wskazówkami, aby uruchomić TPM, a następnie zrestartuj komputer. (możesz dokonać inicjalizacji modułu TPM wcześniej poprzez konsole TPM.msc)

3. W oknie potwierdzającym użycie BDE wybieramy opcję **Continue with Bitlocker Drive encryption.**

4. (Tylko z TPM) Jeżeli używamy modułu TPM, kolejne okno kreatora daje nam wybór metody weryfikacji sekwencji startowej.

Opcja ta pojawia się tylko dla komputerów wyposażonych w moduł TPM. Dostępne są trzy tryby startowe:

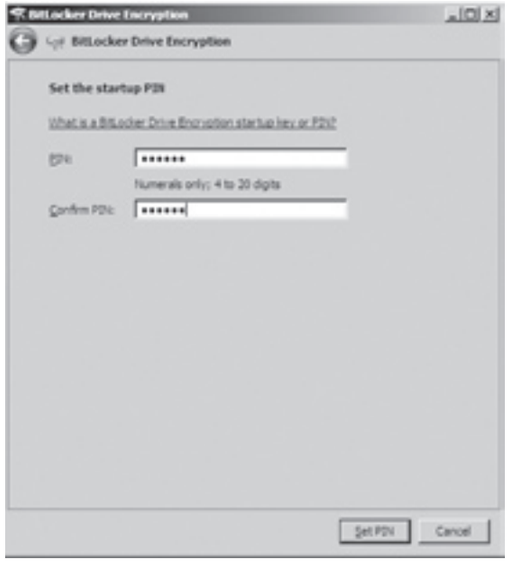
- **Use BitLocker without additional keys** (opcja *only TPM)*
- **Require PIN at every startup** (opcja *TPM with PIN)*
- **Require startup USB at every startup** (opcja *TPM with USB)*

Dalsza procedura zakłada, że operator wybrał najpopularniejszą i najbezpieczniejszą opcję ochrony serwerów w filiach firm – opcje *TPM with PIN*.

Uwaga: Jeżeli w danej lokalizacji nie istnieje żadna jednostka IT należy się zastanowić na wyborem opcji *only TPM*

Rysunek 9. Konfiguracja BDE. Opcje startowe.

5. (Tylko z TPM) W kolejnym kroku kreatora należy wprowadzić PIN. (sekwencja od 4 do 20 cyfr) Zdefiniowany PIN będzie musiał być wprowadzany przy każdym starcie systemu.



Rysunek 10. Konfiguracja BDE. Definiowanie PINu.

6. (Bez TPM) W oknie **Set BitLocker Startup Preferences** zanacz opcje **Require Startup USB Key at every startup.** Jest to jedyna opcja dostępna dla komputerów nieposiadających modułu TPM. Klucz startowy musi być dostarczany na napędzie USB przy każdym restarcie systemu.

7. (Bez TPM) W oknie **Save your Startup Key** zanacz lokalizację napędu USB i naciśnij przycisk Soave

8. Na stronie **Save the recovery Password** (zapisz hasło odzyskiwania) zobaczysz następujące opcje:

   - **Save the password on a USB Drive**. Zapisuje hasło na napędzie flash USB.
   - **Save the password In a folder.** Zapisuje hasło na dysku sieciowym lub w innej lokacji.
   - **Sprint the password**. Drukuje hasło.

Rysunek 11. Konfiguracja BDE. Hasło odzyskiwania.

Użyj co najmniej jednej z tych opcji, aby zachować hasło odzyskiwania. Dla każdej opcji zaznacz ją i postępuj zgodnie z instrukcją kreatora, aby wybrać miejsce przechowywania hasła odzyskiwania lub jego sposób wydruku.

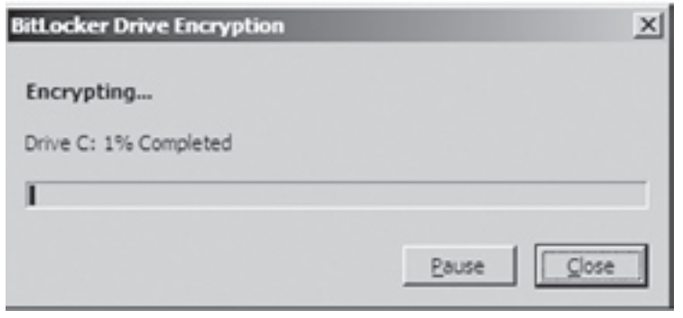
9. Kiedy skończysz zapisywanie hasła odzyskiwania, kliknij **Next**?

Ważne: Hasło odzyskiwania (recover password) będzie wymagane w wypadku, gdy trzeba będzie przenieść zaszyfrowany dysk do innego komputera lub wprowadzić zmiany w informacjach startowych. To hasło jest tak ważne, że zaleca się wykonanie jego dodatkowych kopii przechowywanych w bezpiecznym miejscu, żeby zapewnić sobie dostęp do swoich danych. Hasło odzyskiwania będzie potrzebne do odszyfrowania zaszyfrowanych danych na wolumenie, jeśli BitLocker zablokuje komputer.

10. W oknie **Encrypt the selected disk volume**, upewnij się, że jest zaznaczone pole wyboru **Run BitLocker System Check,** a następnie kliknij przycisk **Continue**.

11. Potwierdź, że chcesz uruchomić ponownie komputer, klikając na **Restart Now**. Komputer uruchamia się ponownie i BitLocker sprawdza, czy komputer jest z nim kompatybilny i gotowy do szyfrowania. Jeśli nie, zobaczysz komunikat błędu, informujący o problemie.

12. Kiedy dysk będzie gotowy do szyfrowania, pojawi się pasek stanu Encryption in Progress. Możesz śledzić postęp szyfrowania dysku przez przeciągnięcie kursora myszki na ikonę BitLocker Drive Encryption na pasku narzędzi na dole ekranu.



Rysunek 12. Konfiguracja BDE. Proces szyfracji.

Przeprowadzenie tej procedury oznacza, że wolumen startowy został zaszyfrowany i utworzono dla niego unikalne hasło odzyskiwania. Kolejne logowania będą przebiegały bez widocznych różnic. Jeśli TPM się zmieni lub będzie niedostępny, zmienią się kluczowe pliki systemu, lub jeśli ktoś będzie próbował uruchomić komputer z innego nośnika aby ominąć system operacyjny, komputer przełączy się w tryb odzyskiwania aż do podania hasła odzyskiwania.

Porcedura odzyskiwania dostępu do danych przy użyciu Bitlocker Drive Encryption (BDE)

Jeżeli kod startowy uległ zmianie, napęd wykorzystywanego nośnika USB z kluczem startowym uległ uszkodzeniu lub PIN został zapomniany, należy użyć poniższej procedury do poprawnego startu systemu operacyjnego.

1. Włącz komputer

2. Jeżeli sekwencja startowa nie będzie poprawna, start komputera zostanie zablokowany i pojawi się okno **BitLocker Drive Encryption Recovery Console.** Włóż nośnik USB zawierający hasło odzyskiwania (recover password) i naciśnij klawisz ESC. Komputer zrestartuje się automatycznie.

3. Jeżeli nie posiadasz nośnika USB z hasłem odzyskiwania nacisnij ENTER.

4. Wprowadź hasło odzyskiwania z klawiatury (48 cyfr) i naciśnij ENTER (jeżeli nie znasz hasła odzyskiwania naciśnij ENTER dwukrotnie i wyłącz komputer)

Jeżeli zapisałeś hasło odzyskiwania w pliku na innym typie nośnika niż USB lub na katalogu udostępnionym, poszukaj pliku który nazywa się tak samo jak ciąg numeryczny **Password ID** wyświetlany na konsoli zablokowanego komputera.
Otwórz plik, zczytaj hasło odzyskiwania i wprowadź w konsoli **BitLocker Drive Encryption Recovery Console.**

Wyłączanie funkcji Bitlocker Drive Encryption (BDE)

1. Kliknij przycisk **Start,** następnie opcję **Control Panel** i opcję **BitLocker Drive Encryption.**
2. Na stronie **BitLocker Drive Encryption,** kliknij opcję **Turn Off BitLocker** na wolumenie systemowym.
3. W oknie **What level of decryption do you want** wybierz, **Disable BitLocker Drive Encryption** lub **Decrypt the volume.**

Windows Serwer 2008 – NetIO

Wstęp

Jedną z podstawowych zmian odróżniających nowy system Windows Serwer 2008 od jego poprzedników jest implementacja nowego stosu TCP/IP. (***Next Generation TCP/IP***) Liczne ulepszenia, nowe funkcjonalności, obsługa protokołu IPv6, nowa wersja protokułu SMB (SMB 2.0) powodują zwiększenie szybkości i stabilności transmisji danych.

- TCP/IP nowa generacja
- Protokół IPv6
- Kontrola jakości połączeń (QoS)
- Zapora systemu Windows serwer 2008

TCP/IP nowa generacja

Systemy Windows Serwer 2008 i Windows Vista posiadają nową architekturę stosu protokołu TCP/IP. Stos nowej generacja TCP/IP (***Next Generation TCP/IP***) oferuje funkcjonalności i wydajność transmisji danych, która nie była osiągalna w poprzednich systemach Windows. Całkowicie przeprojektowana funkcjonalność dotyczy zarówno wersji protokołu IPv4, jak i IPv6. Nowe rozwiązania spełniają jakościowe wymagania nawet bardzo zróżnicowanych środowisk i technologii sieciowych.

Wprowadzono następujące zmiany i ulepszenia w protokole TCP/IP :

Automatyczne dostrajanie okna odbiorczego *(Receive Window Auto-Tuning)*
Rozmiar okna odbiorczego TCP to porcja danych, TCP jaką odbiorca pozwala wysyłać nadawcy bez potrzeby potwierdzenia ich odbioru. W celu optymalizacji tego rozmiaru zależnie od bieżących warunków panujących w łączu, stos TCP/IP nowej generacji wykorzystuje funkcję *Receive Window Auto-Tuning* (automatyczne dostrajanie okna odbiorczego). Funkcja ta optymalizuje rozmiar okna odbiorczego osobno dla każdego nawiązanego połączenia, mierząc iloczyn: pasmo-opóźnienie (***bandwidth-delay product, BDP)*** oraz współczynnik ***retrieval rate*** komunikującej się aplikacji, który jest negocjowany w trakcie inicjalizacji połączenia. Wykorzystanie pasma sieci podczas transferów danych rośnie wraz ze wzrostem przepływności między komunikującymi się aplikacjami. Gdyby wszystkie aplikacje były zoptymalizowane z punktu widzenia odbioru danych przesyłanych protokołem TCP, to ogólne wykorzystanie sieci mogłoby się znacznie zwiększyć.

Funkcja Compound TCP
O ile automatyczne dostrajanie okna odbiorczego optymalizuje przepustowość po stronie odbiorcy, to funkcja Compound TCP (CTCP) stosu TCP/IP następnej generacji optymalizuje przepustowość po stronie nadawcy. Współpracując, obie funkcje mogą doprowadzić do znacznie lepszego wykorzystania łącza.

Dla połączeń TCP, które wykorzystują duże okna odbiorcze i gdzie parameter BDP jest stosunkowo duży, funkcja Compund TCP umożliwia agresywnie zwiększenie ilości danych wysyłanych w porcji danych.

W testach wykonanych wewnętrznie w firmie Microsoft okazało się, że czas zapisu dużego pliku kopii zapasowej przez łącze o paśmie 1 Gb/s i czasie RTT (round-trip) 50 ms spadł prawie o połowę..

Zwiększona przepustowość transmisji danych
Stos TCP/IP następnej wykorzystuje następujące algorytmy mające na celu zoptymalizowania przepustowości w środowiskach o wysokich stratach. O to najważniejsze z nich:

- RFC 2582: Modyfikacja NewReno algorytmu Fast Recovery.
- Nowy algorytm NewReno zapewnia większą przepustowość dzięki zmienionemu sposobowi, na jaki nadawca może zwiększyć tempo nadawania w sytuacji, gdy w oknie danych tracone są liczne segmenty i nadawca otrzymuje tylko częściowe potwierdzenia (potwierdzenie tylko danych pomyślnie otrzymanych).
- RFC 2883: Poszerzenie opcji Selective Acknowledgement (SACK) dla TCP.
- Zdefiniowana w RFC 2018 opcja SACK pozwala odbiorcy potwierdzić maksymalnie 4 niesąsiadujące bloki nadesłanych danych. W zaleceniu RFC 2883 zdefiniowano dodatkowe użycie pól opcji SACK TCP dla potwierdzania ponownie otrzymanych pakietów. Pozwala to odbiorcy segmentu TCP z opcją SACK określić, kiedy niepotrzebnie wysłał ponownie jakiś segment i stosownie do tego dopasować swe przyszłe zachowanie, aby uniknąć dublowania. Im mniej niepotrzebnych ponownych transmisji, tym lepsza przepustowość sieci.
- RFC 3517: Algorytm Loss Recovery dla TCP oparty o Conservative Selective Acknowledgment (SACK).

- Implementacja stosu TCP/IP w systemie Windows Server 2003 oraz w Windows® XP wykorzystuje informacje SACK tylko do określenia tych segmentów TCP, które nie dotarły do miejsca przeznaczenia. W zaleceniu RFC 3517 zdefiniowano metodę wykorzystywania tych informacji także do odzyskiwania utraconych pakietów w momencie, gdy pojawiło się potwierdzenie duplikatu, zastępującego algorytm szybkiego odzyskiwania wtedy, kiedy w danym połączeniu uaktywniona jest funkcja SACK. Stos TCP/IP następnej generacji przechowuje informacje SACK dla każdego połączenia z osobna i monitoruje nadchodzące potwierdzenia pakietów oraz potwierdzenia duplikatów, aby móc szybciej odtworzyć dane w sytuacji, gdy do miejsca przeznaczenia nie dotarło wiele pakietów.

- RFC 4138: Algorytm Forward RTO-Recovery (F-RTO): wykrywanie w połączeniach TCP przekroczeń czasu zbędnych ponownych transmisji (Spurious Retransmission Timeouts) i protokół Stream Control Transmission (SCTP).

- Zbędne ponowne transmisje segmentów TCP mogą zdarzyć się wtedy, gdy wystąpi nagły chwilowy wzrost czasu RTT. Algorytm F-RTO zapobiega zbędnej ponownej transmisji segmentów TCP. Nawet w środowiskach, w których wystąpi nagły chwilowy wzrost RTT (np. kiedy jakiś bezprzewodowy klient przemieści się z jednego punktu dostępu do innego punktu dostępu), algorytm F-RTO zapobiegnie niepotrzebnej, ponownej transmisji segmentów i spowoduje szybszy powrót do normalnego tempa nadawania

Wykrywanie niedostępności sąsiadów w ruchu IPv4

Neighbor Unreachability Detection to funkcja protokołu IPv6: węzły sieci ciągle sprawdzają, czy sąsiednie węzły są dostępne, przez co można szybciej wykrywać błędy i omijać je w sytuacji, gdy któryś z węzłów nagle stanie się niedostępny. Stos TCP/IP następnej generacji wspiera tę funkcję także dla ruchu IPv4 poprzez śledzenie stanu sąsiadów IPv4 i zapamiętywanie go w pamięci podręcznej routingu IPv4. Funkcja weryfikuje, czy sąsiedni węzeł jest dostępny, wymieniając z nim komunikaty ***ARP*** (Address Resolution Protocol) ***Request*** i ***ARP Reply*** albo posiłkuje się w tym celu protokołami wyższych warstw, np. TCP.

Wykrywanie nieaktywnych bram

W stos TCP/IP systemów Windows Server 2003 i Windows XP wbudowano funkcję wykrywania i omijania nieaktywnych bram (fail-over), ale nie posiadają one właściwości fail-back, tj. funkcji okresowego weryfikowania, czy nieaktywna brama nie zaczęła ponownie działać. Stos TCP/IP następnej generacji oferuje taką kontrolę: okresowo podejmuje próby wysłania pakietów TCP przez bramę, która została uprzednio zakwalifikowana, jako niedostępna. Jeśli któraś z takich prób zakończy się pomyślnie, stos z powrotem przełączy ruch TCP na tę bramę, jako bramę standardową. Funkcja fail-back może zaowocować większą przepustowością, jeśli ruch wróci do podstawowej bramy w danej podsieci.

Wykrywanie routerów PMTU działających jako „Black hole" (czarne dziury)

Wykrywanie jednostek PMTU (Path Maximum Transmission Unit) według definicji w dokumencie RFC 1191 polega na odbiorze komunikatów ***Destination Unreachable-Fragmentation Needed*** oraz ***Don't Fragment (DF) Set*** protokołu ICMP (Internet Control Message Protocol)

z routerów zawierających MTU następnego ogniwa. Jednakże w niektórych przypadkach routery pośredniczące ignorują te pakiety, które nie mogą być fragmentowane. Takie routery są znane, jako czarne dziury. Ponadto routery pośredniczące mogą gubić komunikaty ICMP ze względu na reguły skonfigurowane na zaporach firewall. W wyniku ignorowania dużych segmentów oraz gubienia komunikatów ICMP połączenia TCP mogą być przerywane wskutek przekroczenia czasu.

Funkcja wykrywania routerów PMTU, działających jak czarne dziury, wskazuje ponowne transmisje dużych segmentów TCP i automatycznie dopasowuje PMTU danego połączenia zamiast polegać na odbiorze komunikatów ***Destination Unreachable-Fragmentation Needed*** oraz ***Don't Fragment (DF) Set*** protokołu ICMP.Stos TCP/IP w systemach Windows Server 2003 i Windows XP miał standardowo wyłączoną tę funkcję, ponieważ zwiększała ona maksymalną liczbę retransmisji wykonywanych w danym segmencie sieci. Natomiast w stosie następnej generacji jest ona standardowo włączona, aby zapobiec przedwczesnemu zrywaniu połączeń TCP.

Separacja tablicy routingu (Routing compartments)

Aby zapobiec niepożądanemu przekazywaniu ruchu pomiędzy interfejsami wirtualnych sieci prywatnych (VPN), stos TCP/IP następnej generacji obsługuje separację tablicy routingu (routing compartments). Podział tablicy routingu to połączenie zestawu interfejsów VPN z sesją logowania, która operuje swymi własnymi tabelami routingu IP. Ten sam komputer może mieć wiele wzajemnie izolowanych podziałów tablicy routingu, jednak każdy interfejs może należeć tylko do jednego przedziału.

Gdy użytkownik systemu Windows XP zainicjuje połączenie VPN przez Internet z jakąś siecią prywatną, jego komputer będzie łączył się zarówno z Internetem, jak i z intranetem, manipulując pozycjami w tabeli routingu IPv4. W niektórych sytuacjach może zaistnieć możliwość przekazywania ruchu z Internetu przez zestawiony kanał VPN do prywatnego intranetu. Natomiast w przypadku klientów VPN obsługujących podział tablicy routingu, stos TCP/IP następnej generacji odizoluje łączność z Internetem od łączności z prywatnym intranetem stosując osobne tabele routingu IP.

Network Diagnostics Framework

Network Diagnostics Framework to bogata platforma, mająca za zadanie wspierać użytkowników w diagnozowaniu problemów sieciowych i przywracaniu działania sieci.

W przypadku diagnozowania problemów w połączeniach TCP/IP platforma zadaje użytkownikowi serię pytań eliminujących poszczególne możliwe przyczyny, aż przyczyna problemu zostanie zdiagnozowana albo wszystkie możliwości zostaną wyczerpane.
Platforma ***Network Diagnostics Framework*** może diagnozować następujące kwestie, odnoszące się do komunikacji TCP/IP:

- niepoprawny adres IP

- niedostępna standardowa brama (router)

- niepoprawna standardowa brama
- niepowodzenie przy określaniu nazwy *NetBIOS over TCP/IP (NetBT*)
- niepoprawne ustawienia DNS
- zajęty port lokalny
- nie pracuje klient DHCP
- brak odległego odbiorcy
- odłączone media
- zablokowany port lokalny
- za mało wolnej pamięci

Obsługa statystyk ESTATS

Stos TCP/IP następnej generacji obsługuje przedłożoną przez Internet Engineering Task Force propozycję „TCP Extended Statistics MIB", w której zdefiniowano poszerzone dane statystyczne obrazujące pracę TCP. Analizując statystyki ESTATS, dotyczące połączenia można określić, co jest wąskim gardłem w tym połączeniu: aplikacja wysyłająca, aplikacja odbierająca, czy też łącza. Zapisywanie statystyk ESTATS jest domyślnie wyłączone, funkcję można włączyć dla wykonania konkretnego połączenia. W oparciu o statystyki ESTATS niezależni dostawcy oprogramowania (ISV) mogą tworzyć narzędzia do diagnostyki i analizy przepustowości sieci.

Windows Filtering Platform

Windows Filtering Platform (WFP) to nowa platforma stosu TCP/IP następnej generacji udostępniająca niezależnym dostawcom oprogramowania (ISV) interfejsy programistyczne API tak, że mogą oni uczestniczyć w podejmowaniu decyzji dotyczących filtrowania pakietów na kilku poziomach stosu protokołów TCP/IP oraz w kilku miejscach systemu operacyjnego. W platformie zintegrowano obsługę takich cech zapór firewall następnej generacji jak łączność uwierzytelniana czy dynamiczne konfigurowanie zapór uzależnione od wykorzystania przez aplikacje interfejsu Windows Sockets API (zasady uzależnione od konkretnych aplikacji). Używając platformy, dostawcy oprogramowania mogą tworzyć zapory, oprogramowanie antywirusowe, diagnostyczne, inne aplikacje i usługi. Zapora Windows Firewall oraz protokół IPsec w systemach Windows Server 2008 i Windows Vista korzystają z WFP API.

Funkcja Explicit Congestion Notification.

Gdy okaże się, że jakiś segment TCP został utracony, protokół TCP przyjmuje, że został on utracony wskutek tłoku na routerze i przystępuje do kontroli zatłoczenia, w wyniku, czego tempo nadawania danych może radykalnie spaść. Jeśli w obu komunikujących się aplikacjach TCP i w routerach uaktywni się funkcja ECN (Explicit Congestion Notification), zatłoczone routery będą stosownie oznaczać pakiety przed przekazaniem ich dalej. Aplikacja TCP, otrzymująca tak oznakowane pakiety żąda obniżenia tempa transmisji po to, aby rozładować tłok i zapobiec utracie segmentów. Możliwość wykrycia natłoku, zanim zdarzy się utrata pakietu, zwiększa ogólną przepustowość pomiędzy komunikującymi się aplikacjami TCP. Funkcja ECN jest domyślnie wyłączona.

Protokoł IPv6

Wraz ze stosem TCP/IP następnej generacji wprowadzono następujące modyfikacje protokołu IPv6

Domyślnie włączona obsługa protokołu IPv6

W systemach Windows Server 2008 i Windows Vista obsługa protokołu IPv6 jest domyślnie włączona.. Protokołu IPv6 nie można odinstalować, można go jedynie wyłączyć. Konfiguracja Ipv6 jest dokonywana poprzez interfejs graficzny (kontekst **Network Connections**) lub polecenie **netsh**.

Podwójny stos IP

Stos TCP/IP następnej generacji obsługuje architekturę z dwoma warstwami IP, w której implementacja IPv4 dzieli z implementacją IPv6 wspólną warstwę transportową (obejmującą TCP i UDP) oraz warstwę definiującą ramki. Obie implementacje IPv4 i IPv6 są w stosie TCP/IP następnej generacji standardowo włączone i nie trzeba instalować żadnego osobnego komponentu, aby uzyskać dostęp do obsługi IPv6.

Modernizacja adresacji Teredo

Technika Teredo umożliwia pracę poprzez translatory adresów sieciowych (NAT) aplikacjom IPv6, wymagającym dopuszczenia nie zamawianego ruchu przychodzącego i globalnego adresowania, np. aplikacjom klasy peer-to-peer. Gdyby takie aplikacje posługiwały się protokołem IPv4, wymagałyby ręcznego skonfigurowania translatora NAT bądź nawet w ogóle nie mogłyby pracować bez modyfikacji protokołu sieciowego.
Obecnie technika Teredo ma zastosowanie w przypadku, kiedy klient Teredo znajduje się za translatorem adresów sieciowych NAT lub większą ich liczbą. NAT mapuje w ruchu wychodzącym ten sam wewnętrzny (prywatny) adres sieciowy i numer portu na różne zewnętrzne (publiczne) adresy oraz porty, zależnie od zewnętrznego adresu docelowego. Takie nowe zachowanie pozwala Teredo połączyć przez Internet większą grupę hostów.

Zintegrowana obsługa protokołu IPsec

W systemach Windows Server 2008 i Windows Vista w aspekcie IPsec ruch IPv6 jest obsługiwany tak samo, jak ruch IPv4, łącznie z obsługą *Internet Key Exchange (IKE)* i szyfrowaniem transmisji danych. Zapora Windows Firewall z *Advanced Security oraz IP Security Policies* obsługuje teraz konfigurowanie zasad IPsec dla ruchu IPv6 podobnie, jak dla ruchu IPv4. Integracja protokłu IPSec ze stosem IPv6, ulepszenia wprowadzone w formach uwierzytelnienia umożliwia łątwą implementacje bezpiecznej sieci i izolacje wybranych zasobów.

Protokół Multicast Listener Discovery v2

Protokół *Multicast Listener Discovery*, , v2 (MLDv2)wyspecyfikowany w RFC 3810, obsługuje ruch grupowy (wieloemisyjny) zależnie od nadawcy. Protokół MLDv2 jest ekwiwalentem *Internet Group Management Protocol*, v3 (IGMPv3) dla IPv4.

Link-Local Multicast Name Resolution

Technika *Link-Local Multicast Name Resolution (LLMNR)* pozwala hostom IPv6 i IPv4 pracującym w tej samej podsieci, określić wzajemnie swe nazwy bez użycia serwera DNS.

IPv6 przez PPP
Wbudowany klient zdalnego dostępu obecnie obsługuje zdefiniowany w RFC 2472 protokół IPV6CP (IPv6 Control Protocol), służący do konfigurowania węzłów IPv6 w łączach PPP (Point-to-Point Protocol). Natywny ruch IPv6 może być, więc teraz przesyłany połączeniami PPP. Obsługa IPV6CP pozwala na przykład połączyć się z dostawcą Internetu operującym adresacją IPv6 przez łącze wydzwaniane lub przez łącze PPPoE (PPP over Ethernet), które można wykorzystać do szerokopasmowego dostępu do Internetu

Losowe identyfikatory kart sieciowych
Aby zapobiec wykrywaniu adresów IPv6 w oparciu o identyfikatory opublikowane przez producentów kart sieciowych, systemy Windows Server 2008 i Windows Vista domyślnie generują losowe identyfikatory interfejsów sieciowych w przypadku samo-konfigurujących się na stałe adresów IPv6, włączając w to adresy publiczne i link-local.

Obsługa DHCPv6
W systemy Windows Server 2008 i Windows Vista wbudowano klienta DHCP (Dynamic Host Configuration Protocol) z możliwościami DHCPv6, który może auto-konfigurować adresy we współpracy z serwerem DHCPv6.

Pełne wsparcie DNS dla sieci IPv6
Serwisy DNS funkcjonujące na platformach Windows server 2008 w pełni wspierają rozwiązywanie nazw długich dla protokołu IPv6 jak i dla IPv4. W nowej wersji DNS umożliwiono również obsługę rozwiązywania nazw krótkich dzięki strefom nowego typu tzw. *GlobalNames zone*

Kontrola jakości połączeń (Quality of service)

Mechanizm Qos (kontrola jakości połączeń) był implementowany już w systemach Windows serwer 2008 i Windows XP dzięki wykorzystaniu interfejsu programowego API Generic QoS (GqoS). Aplikacje mogły wykorzystywać tę funkcjonalność poprzez ustalanie priorytetów dostarczanch pakietów. W systemach Windows Server 2008 i Windows Vista pojawiły się nowe możliwości zarządzania ruchem w sieciach korporacyjnych i domowych.

Zasady dotyczące jakości obsługi sieciowej w systemach Windows Server 2008 i Windows Vista pozwalają administratorom ustalać priorytety oraz zarządzać tempem nadawania ruchu wychodzącego z sieci. Zasady te mogą być uzależnione od :

- nazw konkretnych aplikacji generujących ruch sieciowy
- adresów IPv4 lub IPv6 aplikacji źródłowej albo docelowej
- portów TCP lub UDP używanych przez aplikację źródłową albo docelową.

Zasady te ustawia się w ramach zasad grupowych użytkownika lub komputera za pomocą edytora **Group Policy Object Editor,** po czym łączy z odpowiednimi kontenerami usług Aktywnych Katalogów (domeny, lokalizacji, jednostki organizacyjne) za pomocą konsoli **Group Policy Management Console**. Mechanizm pozwala na wprowadzenie różnych polityk dla różnych aplikacji w obrębie całej lub tylko części korporacji.

Zarządzając wykorzystaniem pasma sieci, administrator może skonfigurować zasady QoS, limitujące tempo nadawania ruchu wychodzącego z sieci. Taki limit spowoduje ograniczenie zagregowanej ilości danych wychodzących z sieci do wyspecyfikowanego poziomu. Aby ustalić priorytet dostarczania, pakiety danych mogą być oznaczane odpowiednio skonfigurowaną wartością DSCP (*Differentiated Services Code Point*). Routery pracujące w infrastrukturze sieciowej będą segregować pakiety według ich wartości DSCP do różnych kolejek, a zatem różnicować priorytet ich dostawy. Oznaczenia DSCP i technika limitowania tempa nadawania mogą być użyte łącznie dla skuteczniejszego zarządzania ruchem. Ponieważ obie te techniki dotyczą warstwy sieci, aplikacje nie muszą być w żadnym stopniu przystosowywane.

Rysunek 13. Tworzenie nowej polityki kontroli jakości połączeń (QoS)

Zapora systemu Windows Serwer 2008

Zapora systemu Windows Serwer 2008 ma za zadanie w pełni kontrolować ruch przychodzący i wychodzący dla danego serwera. Możliwość dokładnej filtracji komunikacji sieciowej kierowanej do serwera zapobiega uzyskaniu nieautoryzowanego dostępu do aplikacji i usług sieciowych. Nadzorowanie ruchu wychodzącego zmniejsza ryzko ewentualnego infekowania pozostałych systemów sieciowych, wirusami, robakami (o ile nasz serwer został nimi zarażony) lub wykonywania połączeń, które nie powinny mieć miejsca.

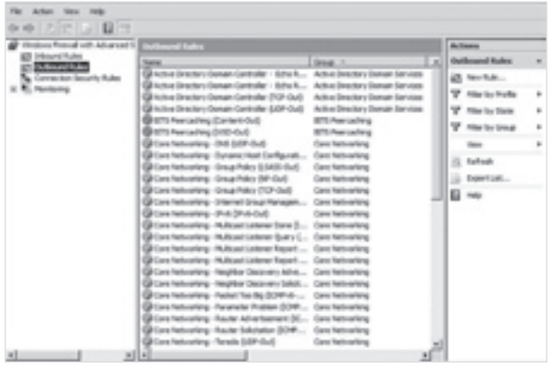
Co nowego ?
Funkcjonalność *firewall* istniała już w poprzednich systemach Windows. Zapora systemu Windows serwer 2008 zawiera znacznie większą ilość funkcji i rozszerzeń.

- Możliwość automatycznego blokowania niechcianego ruchu wysyłanego przez serwer. Zapora posiada definicję reguł pozwalającą na komunikacje wybranych popularnych usług takich jak: DNS, DHCP, udostępnianie plików i drukarek, ruch związany z AD. Pozostałe transmisje mogą być blokowane.

- Nowa konsola do zarządzania. Przystawka *Windows Firewall with Advanced Security* pozwala na prostą i czytelną definicje reguł kontrolujących ruch wychodzących

(*Out-bound Rules*), reguł ruchu przychodzącego (*Inbound Rules*) oraz monitorowania ruchu (kontekst *Monitoring*)

- Integracja zapory z protokołem IPSec. Protokuł IPsec umożliwia ochrone transmisji danych pomiędzy komputerami przy wykorzystaniu różnych metod szyfracji i uwierzytelnienia. Kontekst *Connection Security Rules* pozwala na tworzenie reguł przy wykorzystaniu protokołu IPSec, mających na celu izolowanie i ochrone komunikacji między systemami domenowymi od pojawiających się w sieci obcych komputerów. (Możliwa jest definicja izolacji również w obrębie danej domeny)
- Pełne wsparcie dla protokołu IPv6



Rysunek 14. Zapora systemu Windows serwer 2008

Blok komunikatów serwerów (SMB) 2.0

Wstęp

Blok komunikatów serwera (Serwer Message Block) protokół znany również pod nazwą CIFS (Common Internet Name Standard) jest domyślnym protokołem pozwalającym na dostęp do sytemu plików i drukarek na komputerach opartych o systemy Windows. Windows zawiera klienta SMB (składnik Klient systemu Microsoft Windows) i serwer SMB (składnik Udostępnianie plików i drukarek systemu Microsoft Windows). Protokół SMB 1.0 – technologia dla wersji systemu Windows poprzedzających system Windows Server 2008 i Windows Vista – został zaprojektowany 15 lat temu dla pierwszych sieciowych systemów operacyjnych Windows, takich jak Microsoft LAN Manager i Windows for Workgroups. Ograniczenia pierwszego projektu są widoczne w protokole SMB 1.0. Funkcja SMB w systemie Windows Server 2008 obsługuje wersję SMB 1.0 oraz wersję SMB 2.0 – nową wersję bloku komunikatów serwera, zaprojektowaną od nowa dla potrzeb obecnych złożonych środowisk sieciowych i serwerów nowej generacji.

Cechy protokołu SMB 2.0

Protokół SMB 2.0 zapewnia szereg udoskonaleń komunikacji, takich jak większa wydajność komunikacji z plikami udostępnianymi przez łącza cechujące się dużymi opóźnieniami oraz wyższe bezpieczeństwo dzięki zastosowaniu techniki wzajemnego uwierzytelnienia i podpisywania komunikatów.

Niektóre cechy protokołu SMB 2.0:

- Wykorzystanie standardowego portu 445/TCP
- Obsługa wysyłania wielu poleceń SMB w tym samym pakiecie. Zmniejsza to liczbę pakietów przesyłanych między klientem i serwerem SMB, która to cecha była wadą wersji SMB 1.0.
- Zwiększenie restrykcyjnych stałych w protokole, które mają umożliwiać skalowalność. Na przykład zwiększono liczbę dojść do równocześnie otwartych plików na serwerze i liczbę udziałów plików dozwolonych na serwerze.
- Obsługa o wiele większych rozmiarów buforów w porównaniu z wersją SMB 1.0.
- Obsługa trwałych dojść, umożliwiająca przetrwanie krótkich przerw w dostępności sieci.
- Obsługa łączy symbolicznych.

Systemy Windows Serwer 2003 i Windows Vista wspierają użycie zarówno SMB 1.0 i SMB 2.0. Wersja protokołu używana pomiędzy klientem i serwerem jest ustalana w fazie negocjacji SMB. Poniższa tabela pokazuje użytą wersja protokołu SMB w zależności od wersji sytemu operacyjnego klienta i serwera.

Klient	Serwer	Używana wersja SMB
Windows Serwer 2008 lub Windows Vista	Windows Serwer 2008 lub Windows Vista	SMB 2.0
Windows Serwer 2008 lub Windows Vista	Windows XP, Windows Serwer 2003 lub Windows 2000	SMB 1.0
Windows XP, Windows Serwer 2003 lub Windows 2000	Windows Serwer 2008 lub Windows Vista	SMB 1.0
Windows XP, Windows Serwer 2003 lub Windows 2000	Windows XP, Windows Serwer 2003 lub Windows 2000	SMB 1.0

Tabela 1: Wersje używanego protokołu SMB pomiędzy różnymi systemami operacyjnymi.

5. Zarządzanie tożsamością i dostępem

Zarządzanie tożsamością i dostępem w Windows Server 2008

Zanim przejdziemy do dokładniejszego omówienia, jakie zmiany nastąpiły w technologii AD RMS najpierw przyjrzymy się miejscu, jakie ona zajmuje w całościowej koncepcji zarządzania tożsamością opracowanej przez Microsoft. Jest to o tyle istotne, iż bez tego wiele zmian wprowadzonych w Windows Server 2008 może wydawać się poprawkami kosmetycznymi, które nie mają ze sobą niczego wspólnego.

Czym jest tożsamość i dostęp?

Czy zarządzanie tożsamością i dostępem do informacji jest istotnym zagadnieniem dla przedsiębiorstwa. Zastanówmy się, co ma miejsce w momencie kiedy użytkownik próbuje uzyskać dostęp do poufnego dokumentu przechowywanego na jednym z serwerów. Zakładamy, iż chcemy chronić informacje zawarte w tym dokumencie. Nasza infrastruktura zarządzająca tożsamością i dostępem powinna w takim przypadku:

1. Określić kim jest użytkownik, który próbuje dostać się do dokumentu.
2. Przydzielić użytkownikowi odpowiedni poziom dostępu do tego dokumentu.
3. Chronić poufne dane zawarte w tym dokumencie.
4. Przechowywać informacji o czynnościach wykonywanych przez użytkownika korzystającego z dokumentu.

Najprostszym rozwiązaniem byłoby ograniczenie dostępu na poziomie konkretnych uprawnień do pliku. Natomiast dodatkowa ochrona jest potrzebna aby zabronić określonym użytkownikom możliwości kopiowania z dokumentu, który mogą otworzyć. Należy także pamiętać o odpowiednim audytowaniu dostępu do dokumentu.

Wyzwanie związane z przygotowanie I wdrożeniem takiej infrastruktury staje się jeszcze większe w chwili, kiedy ma ona obsługiwać nie tylko naszych etatowych pracowników, ale także na przykład klientów czy firmy partnerskie. Dodatkowym wyzwaniem jest rozszerzenie granic działalności przedsiębiorstwa i otwarcie na kolejne kanały komunikacji jak, poczta elektroniczna, komunikatory czy usługi webowe oraz urządzenia mobilne zezwalające na przenoszenie danych. Microsoft nieustannie pracuje na spójnym rozwiązaniem pozwalającym na wdrożenie takiego mechanizmu. Poniżej krótko zostanie omówiona ewolucja jaka nastąpiła w technologii zarządzania tożsamością i dostępem.

Tożsamość i dostęp w Windows Server 2003

W stosunku do Windows 2000 Server zostały dokonane ulepszenia we wzajemnej współpracy usług Active Directory (AD) oraz Certificate Services. Dodano także nową funkcjonalność o nazwie Authorization Manager, która zezwalała na uwierzytelnianie użytkowników w oparciu o rolę jaką mają pełnić w konkretnej aplikacji biznesowej. Mimo, iż Active Directory samo w sobie pozwalało na kontrolę dostępu, była to jednak kontrola jedynie na poziomie obiektu realizowana za pomocą ACL. Authorization Manager zezwalał na role-based access control (RBAC), co pozwalało na przypisywanie jednemu użytkownikowi różnych uprawnień w oparciu o rolę jaką mógł pełnić. Authorization Manager pozwalał aplikacji na zarządzanie oraz weryfikację żądań użytkownika związanych z wykonaniem określonych czynności z użyciem aplikacji. Dostępna była także odpowiednia konsolka MMC, która pozwalała administratorowi aplikacji na zarządzanie różnymi rolami użytkowników I ich uprawnieniami.

Inna usługą, którą Microsoft przygotował dla Windows Server 2003 jest Windows Rights Management Service (RMS), technologia ochrony informacji, która pozwala, przy współpracy z obsługującymi ją aplikacjami, na zabezpieczenie wartościowych danych cyfrowych przed nieautoryzowanym użyciem bez względu na sposób i miejsce ich przechowywania. Efektywne korzystanie z RMS jest możliwie dzięki scentralizowanemu zarządzaniu szablonami określającymi sposoby użycia dokumentu. Szablony te, współpracując z odpowiednimi aplikacjami klienckimi są stosowane bezpośrednio do istotnych biznesowo informacji na przykład wiadomości e-mail. Wdrożenie RMS wymaga usługi katalogowej Active Directory, PKI oraz IIS. Wszystkie te komponenty są częścią składową Windows Server 2003. Dodatkowo potrzebna są aplikacje współpracujące z RMS, jak Microsoft Office 2003 i Internet Explorer oraz Microsoft SQL Server w celu zapewnienia odpowiedniej bazy danych dla usługi.

Jako dodatek do wspomnianych powyżej komponentów służących do zarządzania tożsamością i dostępem, opublikowany został Microsoft Identity Integration Server (MIIS) 2003, który umożliwia scentralizowane przechowywanie informacji związanych z tożsamością w przedsiębiorstwie posiadającym wiele usług katalogowych. Pozwala także na ujednoliconą prezentację wszystkich znanych informacji dotyczących tożsamości użytkownika, aplikacji oraz zasobów sieciowych. MIIS 2003 jest zaprojektowany jako narzędzie służące do zarządzania cyklem życia tożsamości, polisami dostępu oraz polisami zarządzającymi prawami. Narzędzie dostępne jest w dwóch wersjach, jako MIIS 2003 Enterprise Edition oraz Identity Integration Feature Pack dla Windows Server Active Directory, który udostępnia te same funkcje co MIIS 2003 EE, ale jedynie pomiędzy usługami katalogowymi AD, Active Directory Application Mode (ADAM) oraz Exchange 2000 i późniejszym.

Tożsamość i dostęp w Windows Server 2003 R2

W wersji Windows Server 2003 R2 Microsoft dodał dwie kolejne usługi pozwalające na bardziej kompleksowe wsparcie zarządzania tożsamością. Jedną z nich jest Active Directory Application Mode a drugą Active Directory Federation Services. W skrócie ADAM to samodzielna wersja AD zaprojektowana do współpracy z aplikacjami wykorzystującymi usługę katalogową. ADAM nie wymaga do pracy istnienia lasu czy domeny AD, więc może być wykorzystywany w grupach roboczych na serwerach, które nie muszą pełnić funkcji kontrolera domeny. Dodatkowo ADAM przechowuje i replikuje tylko dane związane z aplikacjami, które z nim współpracują, nie zawiera żadnych informacji o zasobach sieciowych takich jak użytkownicy, grupy czy komputery. Istotna cechą ADAM jest to, iż nie jest usługą systemową w związku z tym istnieje możliwość uruchomienia wielu jego instancji na jednym komputerze. Każda z takich instancji może obsługiwać inną aplikację, mieć własny magazyn danych oraz przypisane osobne porty LDAP i SSL a także dzienniki zdarzeń. ADAM stanowi opcjonalny komponent Windows Server 2003 R2, ale dostępna jest także wersja do pobrania, która może zostać zainstalowana na Windows Server 2003 bądź Windows XP.

Active Directory Federation Services (ADFS) jest kolejnym opcjonalnym komponentem Windows Server 2003 R2, który udostępnia funkcjonalność single sgn-on (SSO) dla użytkowników zasobów webowych. Możliwe jest to dzięki bezpiecznej wymianie informacji o cyfrowej tożsamości oraz powiązanych z nią praw. ADFS jest ściśle powiązana z AD i może współpracować zarówno z usługą katalogową jak i ADAM. Korzystając z ADFS przedsiębiorstwo może rozszerzyć istniejącą infrastrukturę AD na Internet w celu umożliwienia dostępu do zasobów oferowanych za pośrednictwem Internetu przez zaufanych partnerów. Zaufanymi partnerami mogą być zarówno firmy zewnętrzne jak i oddziały wewnątrz przedsiębiorstwa.

Tożsamość i dostęp w Windows Server 2008

Spoglądając na ewolucję technologii zarządzania tożsamością i dostępem dysponujemy w chwili obecnej następującymi rozwiązaniami zaimplementowanymi w Windows Server 2003 R2:

- usługa katalogowa Active Directory oraz Certificate Services – dwa podstawowe komponenty, które mogą być wdrożone osobno bądź wspólnie
- Authorization Manager, ADAM oraz ADFS – oddzielne komponenty, które wymagają usługi katalogowej AD (Authorization Manager wymaga dodatkowo Certificate Services)
- MIIS 2003 dostępny zarówno jako osobny produkt, bądź darmowy Feature Pack
- RMS dostępny jako osobny component

W Windows Server 2008 Microsoft postanowił dokonać konsolidacji tych rozwiązań w jeden, zintegrowany mechanizm zarządzania tożsamością i dostępem zbudowany w oparciu o AD. W związku z tym dostępne są cztery kluczowe komponenty zarządzania tożsamością i dostępem:

- Active Directory Domain Services (AD DS) oraz Active Directory Lightweight Directory Services (AD LDS), które udostępniają usługę katalogową zarówno w środowisku domenowym jak I w grupie roboczej
- Active Directory Certificate Services (AD CS), która umożliwia weryfikację tożsamości przy pomocy PKI
- Active Directory Rights Management Services (AD RMS), który chroni informacje zawarte w dokumentach, poczcie elektronicznej itp.

- Active Directory Federation Services (AD FS), Tora eliminuje konieczność tworzenia i zarządzania wieloma tożsamościami.

Należy także zwrócić uwagę na zmianę nazw niektórych usług:

- usługa katalogowa Active Directory nazywa się teraz AD DS.
- Active Directory Application Mode to teraz AD LDS
- Certificate Services nazwano AD CS
- Windows Rights Management Services przemianowano na AD RMS

W oparciu o powyższe rozważania widać, że technologia RMS stała się w końcu integralną częścią zarządzania tożsamością i dostępem użytkownika realizowanym w oparciu o Active Directory.

Active Directory Rights Management Services

Jak już zostało wspomniane wcześniej AD RMS jest następcą opcjonalnego komponentu Windows Server 2003, który nazywał się Windows RMS i był przeznaczony do ochrony kluczowych informacji przechowywanych w dokumentach, poczcie elektronicznej czy stronach internetowych przed nieautoryzowanym przeglądaniem, modyfikacją czy użyciem. AD RMS został zaprojektowany do współpracy z odpowiednimi aplikacjami obsługującymi ten mechanizm takimi jak Microsoft Office 2007 System i Internet Explorer 2007. Udostępnia także API, które pozwala programistom na przygotowanie własnych aplikacji czy rozszerzeń obsługujących RMS.

AD RMS pracuje w układzie klient-server, w którym serwer AD RMS jest odpowiedzialny za weryfikację tożsamości oraz wystawienie odpowiedniego certyfikatu. Kiedy tylko użytkownik taki certyfikat otrzyma może starać się o dostęp do chronionej treści. Informacje chronione są przez „publishing license", która tworzona jest dla danych i zawiera informacje o tym, w jaki sposób dane mogą być używane i przez kogo. W chwili dystrybucji treści, informacje o przysługujących prawach są także dystrybuowane i dotyczą zarówno użytków wewnątrz organizacji jak i poza nią.

Użytkownicy, który otrzymają chroniony dokument muszą uzyskać odpowiedni certyfikat od serwera AD RMS zanim uzyskają dostęp do chronionych informacji. W chwili, kiedy użytkownik próbuje przejrzeć chronione informacje aplikacja zgodna z technologią RMS wysyła żądanie do serwera AD RMS w celu uzyskania odpowiedniego zezwolenia. Usługa AD RMS wystawia wtedy unikatową licencję pozwalającą na dostęp do dokumentu z określonymi prawami w oparciu o warunki zdefiniowane w „publishing license". AD RMS weryfikuje tożsamość użytkownika wżoparciu o AD DS.

Usługa AD RMS została rozszerzona o kilka udoskonaleń: instaluje się ją jako rolę serwera zżwykorzystaniem Server Managera, dostępna jest konsola MMC zamiast interfejsu webowego obecnego w poprzedniej wersji, usługa integruje się z AD FS oraz umożliwia bardziej efektywne zarządzanie uprawnieniami do administracji serwerami AD RMS. Użycie konsoli administracyjnej zamiast interfejsu webowego pozwala na stworzenie w pełni spójnego środowiska wykorzystywanego w całym Windows Server 2008, które zostało zaprojektowane jako prostsze wżobsłudze i nawigacji. Dodatkowo zaimplementowanie ról administracyjnych dla serwera AD RMS powoduje, że konsola AD RMS wyświetla tylko te elementy, do których użytkownik ma dostęp. Na przykład użytkownik, który należy do grupy pełniącej rolę AD RMS Template Administrators jest ograniczony tylko do zadań związanych z zarządzaniem szablonami AD RMS, wszystkie pozostałe zadania będą w konsoli niedostępne.

Role administracyjne AD RMS

W celu lepszego zarządzania delegowaniem uprawnień do środowiska AD RMS zostały opracowane nowe role administracyjne. Te role są lokalnymi grupami typu security, które są tworzone w trakcie instalacji usługi AD RMS. Każda z tych grup ma inny poziom dostępu do AD RMS. Nowe role to AD RMS Service Group, AD RMS Enterprise Administrators, AD RMS Template Administrators, and AD RMS Auditors.

AD RMS Service Group jest kontem usługi AD RMS. Kiedy dodawana jest rola AD RMS konto podane w czasie procesu instalacji jest automatycznie dodawane do tej grupy.

Rola AD RMS Enterprise Administrators zezwala członkom tej grupy na zarządzanie wszystkimi ustawieniami i polisam AD RMS. W trakcie instalacji usługi AD RMS do grupy tej dodawane jest konto użytkownika, który tą usługę instaluje a także grupa lokalnych administratorów. Członkostwo w tej grupie powinno być ograniczone tylko do kont użytkowników wymagających pełnej kontroli administracyjnej nad usługą AD RMS.

Rola AD RMS Templates Administrators zezwala członkom tej grupy na zarządzanie "rights policy templates" w szczególności na wyświetlenie szablonów polis, tworzenie nowych szablonów, modyfikowanie istniejących oraz eksport szablonów.

Rola AD RMS Auditors zezwala na zarządzanie logami i raportami. Rola ta ma przypisaną tylko możliwość odczytu, która ograniczona jest jedynie do informacji o ustawieniach logów oraz zezwala na uruchomienie przygotowanych wcześniej raportów.

Wymagania dla usługi AD RMS

AD RMS pracuje na komputerze z systemem operacyjnym Windows Server 2008. W momencie instalacji roli AD RMS instalowane są wszystkie wymagane usługi, m. in. Internet Information Services (IIS). Do poprawnej pracy wymagana jest także baza danych taka jak Microsoft SQL Server, która może być uruchomiona zarówno na tym samym komputerze jak i na zdalnym serwerze oraz las bądź domena AD DS. Jeśli w trakcie procesu instalacji nie określimy zdalnej

bazy danych dla AD RMS Configuration and Logging kreator instalacji roli AD RMS automatycznie zainstaluje i skonfiguruje Windows Internal Database do pracy z usługą AD RMS. Dodatkowo potrzebne jest konto, bez żadnych uprawnień w systemie, na którym będzie pracować usługa AD RMS.

Poniższa tabela zawiera informacje o minimalnych jak i zalecanych wymaganiach sprzętowych pozwalających na zainstalowanie roli AD RMS na komputerze pracującym pod kontrolą Windows Server 2008.

Wymagania	**Zalecenia**
One Pentium 4 3 GHz processor or higher	Two Pentium 4 3 GHz processors or higher
512 MB of RAM	1024 MB of RAM
40 GB of free hard disk space	80 GB of free hard disk space

Następna tabela opisuje wymagania dotyczące konfiguracji oprogramowania, które pozwolą na uruchomienie roli AD RMS. Niektóre z tych wymagań zostaną włączone i skonfigurowane na etapie instalacji roli serwera AD RMS.

Oprogramowanie	**Wymagania**
System operacyjny	Windows Server 2008 pomijając Windows Web Server 2008
System plików	NTFS zalecany
Messaging	Message Queuing
Usługi WWW	Internet Information Services (IIS). ASP.NET must be enabled.
Active Directory lub Active Directory Domain Services	AD RMS musi być zainstalowana w domenie Active Directory, w której kontrolery domeny pracują z uruchomionym Windows Server 2000 z Service Pack 3 (SP3), Windows Server 2003, bądź Windows Server 2008. Wszyscy użytkownicy, którzy korzystają z AD RMS w celu uzyskania licencji muszą mieć przypisany adres e-mail w Active Directory.
Serwer bazodanowy	AD RMS wymaga serwera bazodanowego takiego jak Microsoft SQL Server 2005

W celu przygotowania chronionej zawartości wymagany jest Microsoft Office 2007 Enterprise, Professional Plus bądź Ultimate. W celu zapewnienia dodatkowego bezpieczeństwa AD RMS może zostać zintegrowany z innymi technologiami, jak smart card.
Klient AD RMS jest wbudowany w Windows Vista. Pozostałe systemy operacyjne wymagają pobrania i zainstalowania pakietu RMS client with Sernice Pack 2 (SP2).

Zalecenia przed-instalacyjne

Oprócz określonych wymagań dla usługi AD RMS warto zastosować się do poniższych zaleceń:

- serwer bazodanowy obsługujący bazę AD RMS powinien być zainstalowany na osobnym komputerze
- dostęp do serwera AD RMS powinien odbywać się z wykorzystaniem protokołu SSL, certyfikat powinien być wystawiony przez zaufany główny urząd certyfikujący
- zdefiniować aliasy (CNAME) zarówno dla serwera AD RMS jak i dla komputera obsługującego bazę danych, w przypadku awarii serwera AD RMS pozwoli to na szybkie zaktualizowanie aliasa bez konieczności ponownej publikacji wszystkich chronionych plików
- w przypadku wykorzystania nazwanej instancji konfiguracyjnej bazy danych AD RMS należy się upewnić czy na serwerze bazodanowym jest uruchomiona usługa SQL Server Browser, w przeciwnym wypadku próba instalacji roli AD RMS zakończy się niepowodzeniem.

Dodatkowo należy wziąć pod uwagę następujące wskazówki:

- Windows Internal Database współpracujący z AD RMS zalecany jest tylko do wykorzystania w środowisku testowym, ponieważ Windows Internal Database nie wspiera zdalnych połączeń, więc nie będzie możliwości dodania kolejnego serwera
- na etapie instalacji localhost nie jest wspierany jako adres URL wskazujący na serwer AD RMS
- w trakcie określania konta, na którym będzie funkcjonować usługa AD RMS należy się upewnić, że smart card nie jest włożony do komputera, ponieważ w takiej sytuacji wyświetlony zostanie komunikat o błędzie stwierdzający, że konto użytkownika instalującego AD RMS nie ma możliwości odpytania AD DS
- w przypadku dołączania kolejnego serwera do istniejącego już klastra AD RMS certyfikat SSL dla nowego serwera musi znajdować się na komputerze przed rozpoczęciem procesu instalacji.

Zalecenia dla aktualizacji RMS do AD RMS

Przed wykonaniem uaktualnienia z dowolnej wersji RMS do AD RMS należy wykonać następujące czynności:

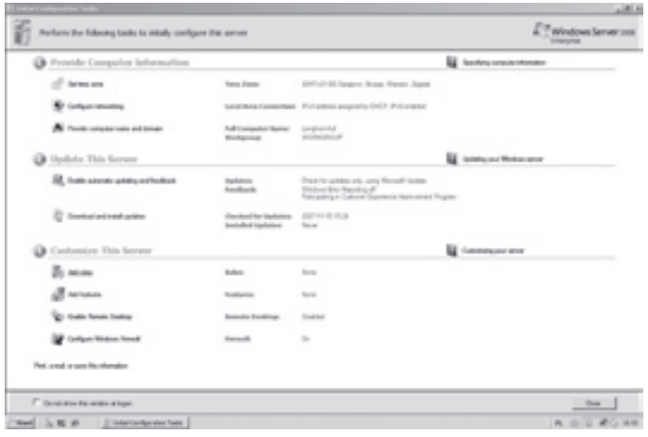
- kopię zapasową bazy danych RMS oraz złożyć ją w bezpiecznej lokalizacji
- w przypadku korzystania z MSDE do obsługi bazy danych AD RMS należy najpierw dokonać aktualizacji środowiska do Microsoft SQL Server, w przeciwnym wypadku aktualizacja nie jest wspierana

- oczyścić kolejkę RMS Message Queuing w celu upewnienia się, że wszystkie wiadomości zostały zapisane w baize danych RMS.

Instalacja AD RMS

Po zainstalowaniu systemu operacyjnego na serwerze można skorzystać z Initial Configuration Tasks bądź Server Manager w celu zainstalowania odpowiednich ról. Aby zainstalować AD RMS z listy zadań należy wybrać **Add roles**, a następnie kliknąć check box **Active Directory Rights Management Services**.

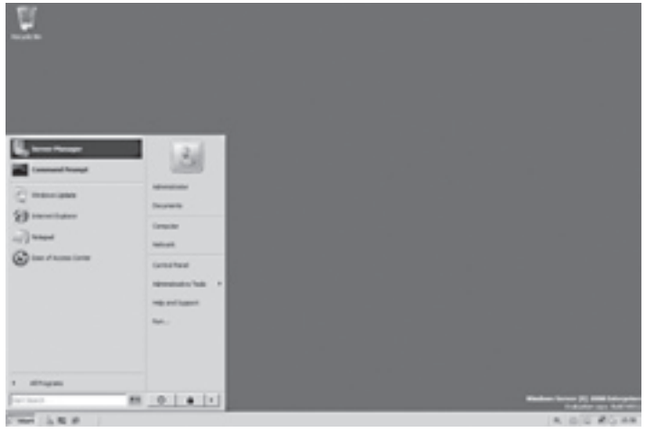
1. Instalacja roli za pomocą Initial Configuration Tasks:



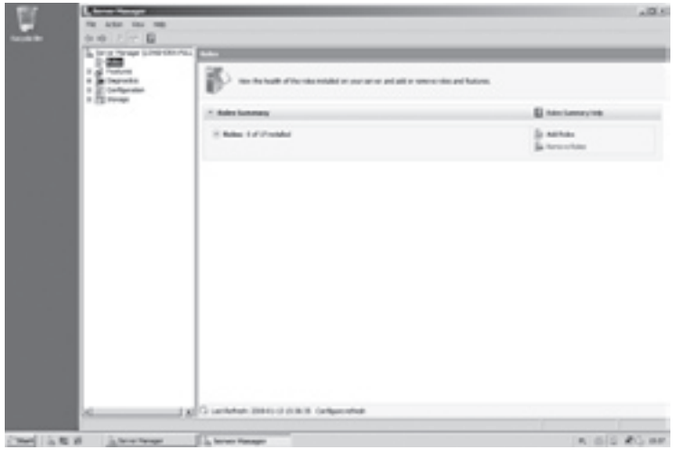
Klikamy **Add Role**

Wybieramy rolę **AD RMS**

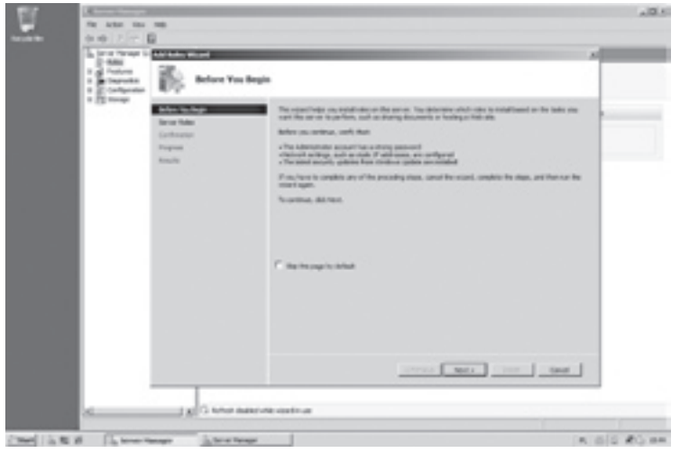
2. Instalacja roli za pomocą Server Manager



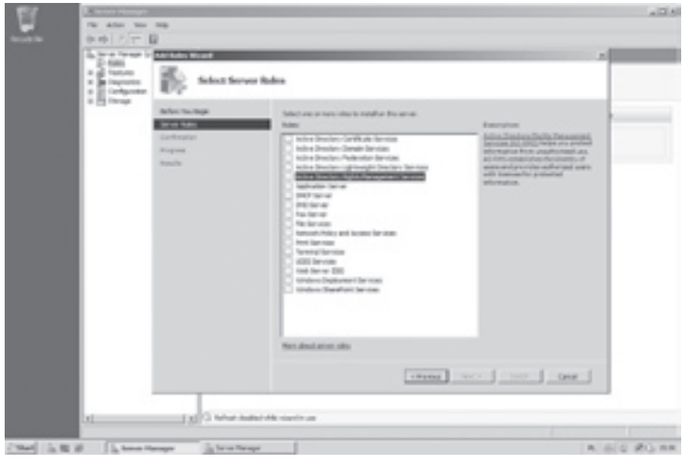
Klikamy **Roles**



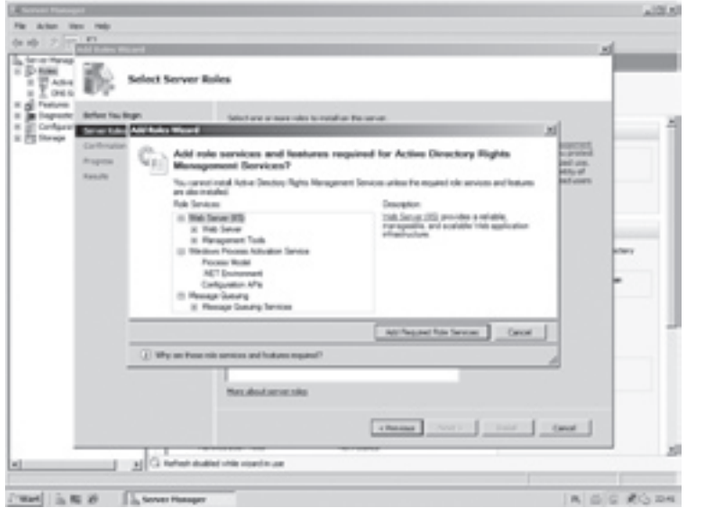
Wybieramy **Add Roles**



Wybieramy rolę **AD RMS**



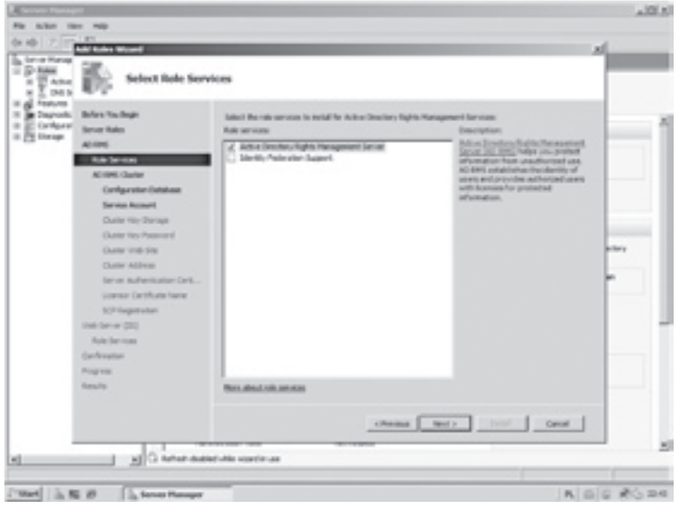
Pojawia się strona **Role Services** informująca o rolach i funkcjonalnościach, od których zależy AD RMS. Należy się upewnić, że wyświetlone są **Web Server (IIS)**, **Windows Process Activation Service (WPAS)** oraz **Message Queuing**. Klikamy **Add Required Role Services** a następnie **Next**.



Na stronie **Select Server Role** upewnij się, że są wybrane **Active Directory Rights Management Server** oraz **Web Server (IIS)** a następnie naciśnij **Next**.

Przeczytaj wprowadzenie od AD RMS i wybierz **Next**.

Na stronie **Select Role Services** sprawdź czy zaznaczona jest opcja **Active Directory Rights Management Server** i naciśnij **Next**.



Wybierz opcję **Create a new AD RMS cluster** a później kliknij **Next**.

W przypadku braku zewnetrznego serwera bazodanowego możemy wybrać opcję **Use Windows Internal Database on his server**, pamiętając o ograniczeniach tego rozwiązania. Klikamy **Next**.

Wybieramy **Specify** i określamy konto użytkownika, na którym będzie uruchamiana usługa AD RMS, klikamy **OK** a następnie **Next**.

Upewniamy się, że wybrana jest opcja **Use AD RMS centrally managed key storage** i klikamy **Next**.

Wprowadź mocne hasło w polach **Password** oraz **Confirm password** i wybierz **Next**.

Wybierz stronę webową, na której zainstaluje się AD RMS i kliknij **Next**. Instalator użyje domyślnych ustawień, jedyną dostępną stroną jest **Default Web Site**.

W przypadku braku certyfikatu dla serwera WWW wybierz opcję **Use an unencrypted connection (http://)**. W polu **Fully-Qualified Domain Name** wpisz adres serwera i kliknij **Validate**. Jeśli weryfikacja zakończy się sukcesem przycisk **Next** stanie się aktywny i będzie można go kliknąć.

W polu **Friendly name** wpisz nazwę, która łatwo pozwoli na identyfikację klastra i wybierz **Next**.

Upewnij się, że wybrana jest opcja **Register the AD RMS service connection point now** a następnie kliknij **Next**.

Przeczytaj instrukcje na stronie **Web Server (IIS)** i kliknij **Next**. Pozostaw zaznaczone ustawienia domyślne i wybierz **Next** a następnie **Install** w celu zainstalowania AD RMS.

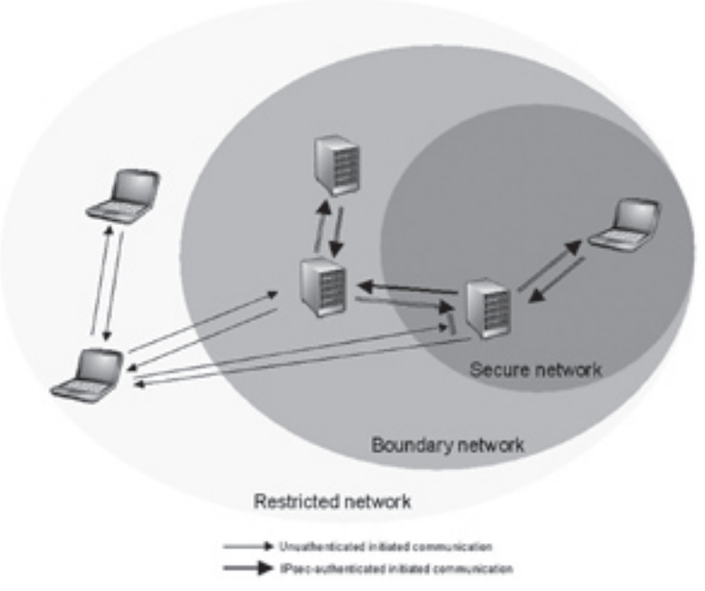
Po zakończeniu procesu instalacji kliknij **Close**.

W celu umożliwienia zarządzania usługą AD RMS należy wylogować i ponownie zalogować użytkownika, którego konto posłużyło do instalacji. Spowoduje to aktualizację informacji o członkostwie w grupach. Jest to istotne o tyle, że w trakcie procesu instalacji konto stało się członkiem grupy **AD RMS Enterprise Administrators.**

Network Access Protection

Czym jest NAP

Celem wielu godzin pracy administratorów jest uaktualnianie systemu operacyjnego i zainstalowanego dodatkowego oprogramowania wymaganego w korporacji. Przykładem takiego oprogramowania jest program antywirusowy, który powinien być aktualny – to znaczy mieć zainstalowane najnowsze definicje szczepionek. Do podobnej grupy należy też konfiguracja oprogramowania, nie chcemy aby użytkownik mógł w nią ingerować. Na przykład samodzielne wyłączenie firewalla nie jest pożądaną przez nas czynnością. W domenie chcielibyśmy mieć wszystkie komputery podłączone i skonfigurowane według pewnych zasad. Tak aby tylko komputery spełniające pewne zasady mogły kontaktować się z serwerami, oraz aby komputery które nie są skonfigurowane tak jak my chcemy nie były dopuszczone do sieci z zasobami. Network Access Protection (**NAP**) to technologia która pomaga administratorom osiągnąć ten cel. Za pomocą **NPS** czyli Network Policy Server definiujemy zasady które muszą być spełnione przez NAP klienta aby mógł się dostać do bezpiecznej sieci. W ten sposób komputer który nie podoła wymaganiom stawianym przez system nie dostanie certyfikatu zdrowia czyli nie będzie mógł się dostać do zabezpieczonej przez IPsec bezpiecznej części firmy. Będzie za to mógł dostać się do serwerów z których będzie mógł zaaplikować sobie niezbędne łaty. Schematycznie przedstawia to rysunek poniżej:



NAP po stronie klienta wymaga komponentu NAP Client który jest już wbudowany w Microsoft Vista, Windows Server 2008 oraz dostępny będzie w SP3 do Windows XP. Jeśli chcemy używać Windows XP z SP2 to możemy doinstalować klienta pobranego ze strony www.microsoft.com.

Kiedy stosować

NAPa można wykorzystać w kilku przypadkach. Pierwszy to z usługa **DHCP**. Klient który jest niezgodny z polityką dostaje adres IP, maskę – zawsze tą samą 255.255.255.255 oraz zamiast domyślnej bramy jest wpis 0.0.0.0. Dodatkowo są dodawane statyczne wpisy które zapewniają dostęp do serwerów z których można pobrać uaktualnienia tak aby dostosować komputer do wymaganej polityki. Statyczne wpisy są dodawane za pomocą opcji Clessless Static Routes. W takim wypadku jeżeli użytkownik chciałby skorzystać z serwera, do którego nie ma dostępu, zostanie wygenerowany błąd. W chwili gdy jego stan się zmieni zgodnie z wymaganiami polisy, automatycznie zostanie wygenerowany dla niego certyfikat zdrowia i będzie miał dostęp do bezpiecznej sieci.

Następnym przypadkiem w której możemy korzystać z NAP są połączenia VPN. Serwer blokuje ruch do zasobów zabezpieczonych w wypadkach gdy stacja robocza nie ma odpowiedniego certyfikatu, w przeciwnym przypadku pozwala się z nim komunikować. Ta technologia działa tylko dla klientów łączących się za pomocą połączenia VPN.

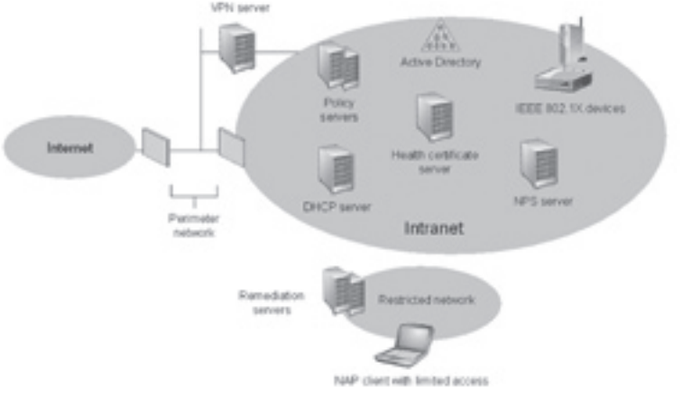
Kolejną możliwością zastosowania NAP-a są urządzenia łączące się za pomocą standardu IEEE 802.1X. Kiedy niezgodny klient próbuje łączyć się do punktu dostępowego (AP) dostaje się do VLAN-u z restrykcjami. Po uaktualnieniu się lub gdy się połączy klient spełniający wymagane polityki jest kierowany do chronionego obszaru sieci.

Największą zaletą technologii NAP jest współpraca z IPSec. To właśnie taki połączenie pozwala nam na pełne odseparowanie od siebie poszczególnych sieci. Komputer, który uzyskał certyfikat zdrowia może należeć do sieci bezpiecznej – tam cały ruch odbywa się z wykorzystaniem szyfrowania. Dobrze jest to pokazane na ilustracji powyżej. Do tej sieci mogą należeć tylko i wyłącznie komputery z ważnym certyfikatem zdrowia. Jeżeli takiego nie ma, zostaje zakwalifikowany do sieci mniej bezpiecznej, ograniczonej w której może podnieść swój „stan zdrowia". Następną oddzielną siecią dla wszystkich którzy nie mogą się wylegitymować swoim stanem zdrowia – czyli na przykład: komputery, które nie maja zainstalowanego klienta NAP lub komputery gości, dostają się do sieci z ograniczeniami. Ta sieć nie ma dostępu do żadnych serwerów.

Komponenty infrastruktury

Infrastruktura NAP korzysta z następujących komponentów:

- *NAP Client* – komputer kliencki który używa Network Access Protocol do zabezpieczenie komunikacji korzystając z połączeń 802.1X, DHCP, IPSsc oraz VPN.
- *NAP Server* – komputer z systemem operacyjnym Windows Server 2008 który używa Network Policy Server (NPS). NPS jest używany do sprawdzenia stanu zdrowia klienta NAP. Jest on także odpowiedzialny za sprawdzenie dlaczego dany klient nie ma dostępu do bezpiecznej sieci i jakie komponenty muszą być poprawione aby miał dostęp do sieci
- *NPS Server* – Network Policy Server jest następcą Internet Autentication Service (IAS). Uruchamia się na Windows Server 2008 i służy do sprawdzania klienta NAP oraz przyporządkowania do odpowiedniej sieci. Na tym serwerze występuje System Health Validator (SHV) który odczytuje polisy, zbiera wyniki od klienta, porównuje ze sobą oraz decyduje w jakiej sieci ma się znaleźć dany klient



- *Policy Servers* – Komputer który przechowuje aktualny stan systemu dla NPS
- *Active Directory Directory Service* – Ustawienie polis grupowych dla komunikacji wykorzystującej IPsec oraz przetrzymuje wszystkie informacje niezbędne do uwierzytelnienia klientów VPN oraz 802.1X
- *Restricted Network* – Oddzielony kawałek sieci w którym znajdują się serwery do podniesienia swojego stanu zdrowia (Remediation Servers). Na tych serwerach powinny znajdować się uaktualnienia do systemu operacyjnego oraz innych programów – na przykład najnowsze szczepionki do programu antywirusowego używanego w korporacji
- *Remediation Server* – Serwer który przechowuje uaktualnienia. Dostępny z sieci Restricted, zawiera wszystko co niezbędne komputerowi aby stać się klientem w pełni zgodnym z obowiązującą polityką firmy.
- *Health Certificate Server* – Komponent odpowiedzialny za wystawianie certyfikatów X.509 klientom którzy przeszli poprawnie proces weryfikacji.
- *System Health Agent* – Komponent który występuje po stronie klienta. Jest odpowiedzialny za sprawdzenie stanu systemu i ewentualnego porównania go z serwerami Remediation. Wysyła także Statement of Health (SoH) do odpowiedniego SHV

- *System Health Validator* – Porównuje Statement of Health wysłany przez agenta i odpowiednią konfiguracją polityk. Jeżeli klient spełnia wymagania jest tworzona wiadomość Statement of Health Response(SoHR) i zostaje wysłana do Quarantine serwera. Jeżeli za to nie spełnia wymagań jest wysyłana odpowiedź z odpowiednimi instrukcjami co należy zaktualizować. Ten komponent działa na serwerze NPS

- *Statement of Health* – Odpowiedz ze stanem zdrowia wysyłana przez System Health Agenta do Sysyem Health Validator.

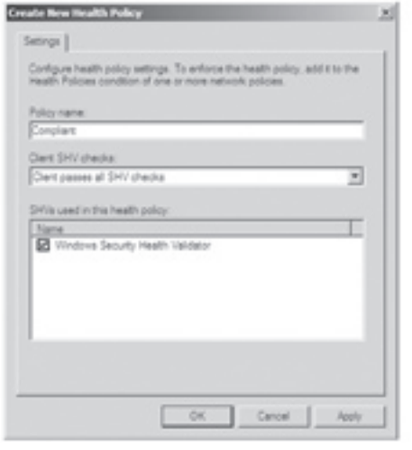
Jak skonfigurować NAP z usługą DHCP

Weźmy teraz pod lupę NAP-a z usługą DHCP. Jak to działa i czym jest.
Usługa DHCP ma za zadanie przydzielić klientowi numer IP taki aby umożliwić jemu komunikacje z innymi komputerami i serwerami w sieci. Dodatkowo z numerem IP są przepisywane opcje DHCP.

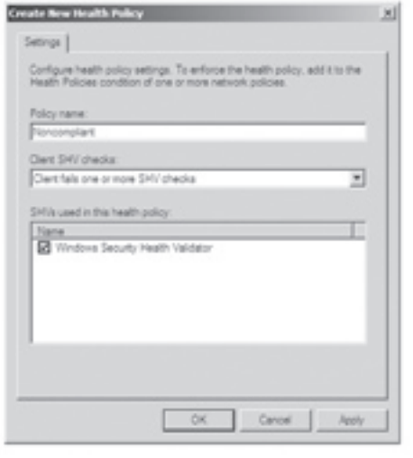
Jak to skonfigurować ?

Na serwerze Windows 2008 trzeba najpierw dodać role Network Policy Server oraz DHCP, następnie skonfigurować DHCP. Dalszą czynnością jest skonfigurowanie serwera aby działał jako Health Policy Server. Do tego będzie potrzebne dodanie SHV w którym ustalamy co ma być sprawdzane na jakim systemie

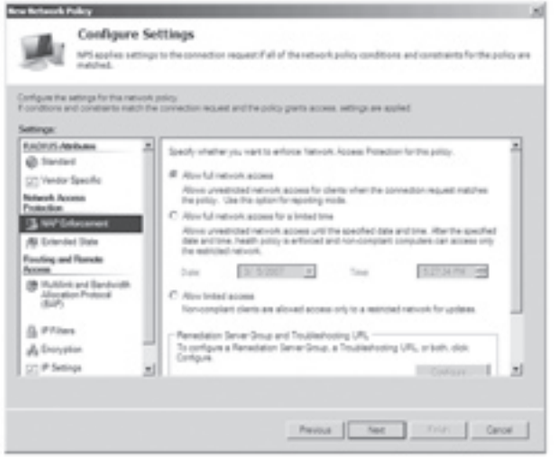
Tu jak widać możemy wybrać kilka punktów do sprawdzenia. Następnie zatwierdzamy naszą konfiguracje i przechodzimy do serwerów korygujących (remediation) Tu ustalamy numery IP i nazwy serwerów oraz przechodzimy dalej do Health Polices i wybieramy, że klientowi który spełni wszystkie wymagania zostanie przypisana polisa „compliant".



Pozostałym klientom zostanie przypisana polisa „noncompliant"

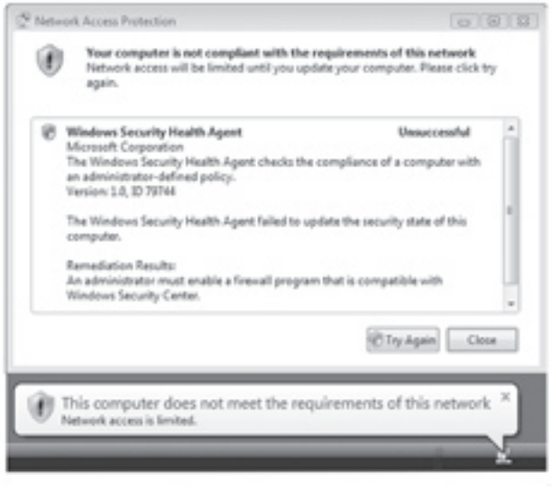


Następnie należy ustawić polise sieciową dla komputerów „compliant" i „noncompliant" wskazując im do jakiej sieci mają należeć. Warto wspomnieć o tym, że mamy wybór pomiędzy Allow Full Network Access czyli pełnym dostępem do sieci, oraz Allow Full Network Access for a limited time – co pozwala nam zezwolić na dostęp czasowy. Tutaj także konfigurujemy serwery Remediation oraz zaznaczając enable auto-remediation of client computer wskazujemy aby po dopasowaniu się do wymagań polis komputer automatycznie dostał się do sieci z pełnym dostępem



Od strony konfiguracji to prawie wszystko, zostało tylko odpowiednie ustawienie usługi DHCP. Miejsce w którym to robimy to zakładka Network Access Protection która pojawia się w konsoli DHCP przy konfigurowaniu protokołu IPv4. Warto zaznaczyć, że konfiguracja NAP-a może zostać zrobiona tylko i wyłącznie dla protokołu IPv4.

Ostatnią czynnością którą należy zrobić jest skonfigurowanie klienta tak aby korzystał z serwera DHCP oraz zainstalowanie na nim NAP klienta, jeżeli jest taka konieczność. Efektem działania dla klienta który ma na przykład wyłączony firewall powinien być następujący ekran



Klient taki także nie będzie miał pełnego dostępu do sieci - jego dostęp będzie ale ograniczony.

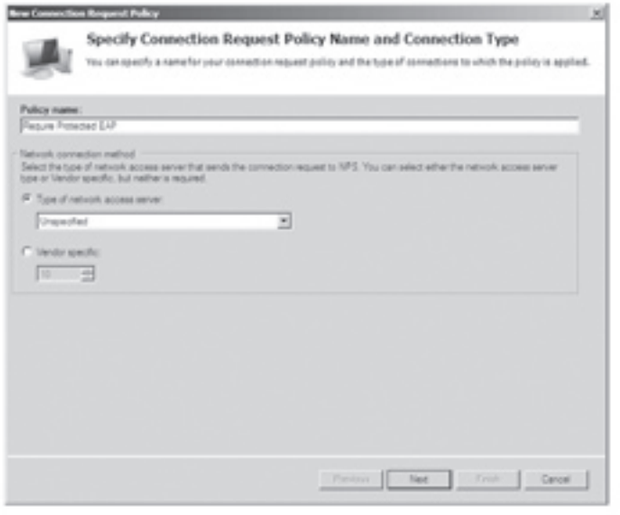
Warto też zauważyć, że osoba może sama zmienić IP na komputerze na poprawne. To zadziała, ale trzeba pamiętać, że normalna osoba w firmie nie powinna mieć uprawnień do wykonania takiej czynności. A ta usługa nie zabezpiecza przed takimi osobami (zabezpiecza przed tym NAP z IPSec)

Jak skonfigurować NAP z uwierzytelnieniem 802.1X

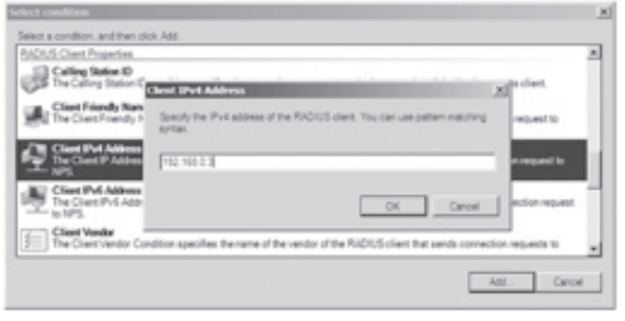
W tym rozwiązaniu możemy dokonać uwierzytelnienia stacji na urządzeniu sieciowym zgodnym z IEEE 802.1X. Weryfikacja wygląda następująco: urządzenie sieciowe przesyła stan zdrowia klienta do serwera NPS gdzie następuje sprawdzenie do której sieci zakwalifikować klienta. Jeżeli z klientem jest wszystko dobrze zostanie przypisany do sieci pełnej – czyli odpowiedniego VLAN-u bez restrykcji, w innym przypadku zostanie dopisany do kawałka sieci z restrykcjami. Klient nie ma możliwości na przepięcie się sam z jednego segmentu do drugiego.

Do konfiguracji takiego rozwiązania niezbędne jest urządzenie które ma zaimplementowany standard 802.1X. Załóżmy, że mamy switch na którym tworzymy wirtualne sieci z nazwami „compliant_vlan" i „noncompliant_vlan". Na urządzeniu powinien być wyłączony routing pomiędzy tymi sieciami. Do dobrze działającego rozwiązania powinniśmy korzystać z certyfikatów. Serwer certyfikatów możemy postawić lokalny. Tak samo jak w poprzednim rozwiązaniu będzie trzeba na serwerze Windows 2008 zainstalować role Network Policy Server, dalej powinniśmy zainstalować certyfikat dla serwera i skonfigurować go jako Health Policy Server. Następny krok to konfiguracja obsługi RADIUS clienta

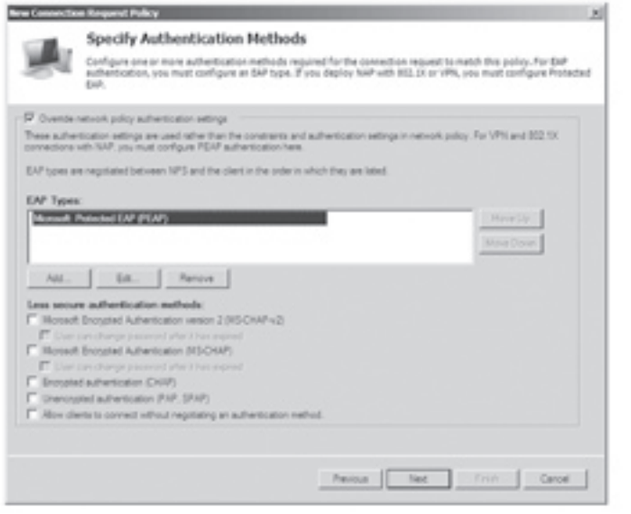
Kolejną czynnością jest utworzenie polisy.



I przypisujemy klienta



Jak widać klienta opisać możemy za pomocą kilku właściwości. Dalej zostało nam określenie metody uwierzytelniania.



Na koniec jeszcze zobaczymy ekran podsumowujący wszystko i trzeba się zabrać za konfigurację SHV. Robi się to podobnie jak w poprzedniej metodzie. Wybieramy co jest wymagane do sprawdzania (firewall czy jest włączony, antywirus czy zainstalowany i uaktualniony, zabezpieczenie spyware, automatyczne update...) Następnie Health Policies tak samo jak w poprzednim temacie. W efekcie końcowym powinniśmy zobaczyć okno pokazane poniżej.

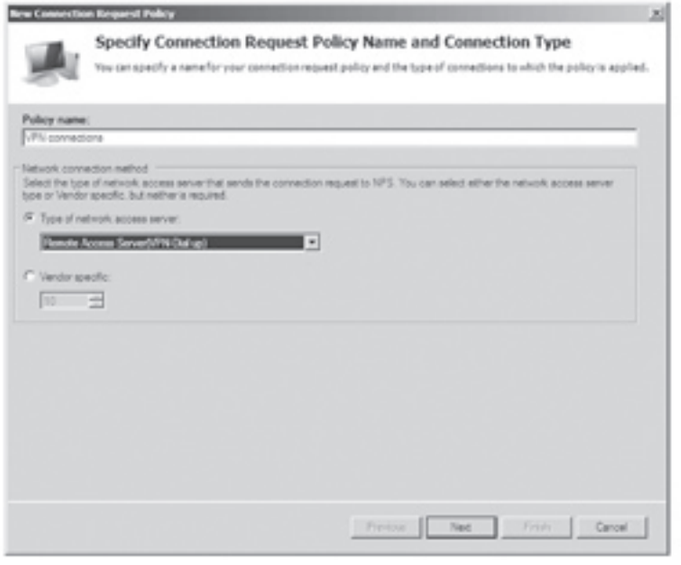
Ostatnim krokiem jest konfiguracja klienta. W NAP kliencie można skonfigurować metodę autentykacji oraz określić czy ma korzystać z certyfikatów.

Po połączeniu się z klientem odpowiadającym warunkom pracy u nas, w sieci powinniśmy zobaczyć informację, ze mamy pełny dostęp do sieci. W przeciwnym przypadku otrzymujemy informacje o ograniczonym połączeniu.

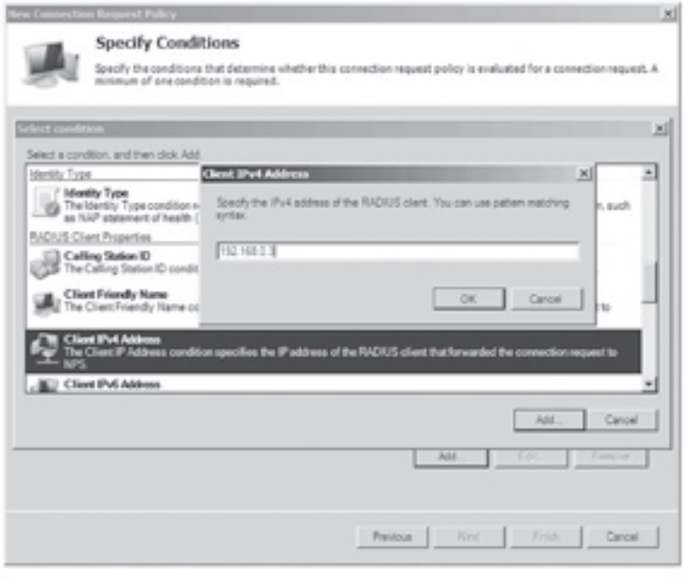
Jak skonfigurować połączenia VPN wykorzystując NAP

Połączenia VPN są dość często używanymi a mechanizm jest podobny do znanego z ISA Server. Zasadniczą różnicą pomiędzy tymi rozwiązaniami jest sposób przesyłania wyników do serwera. Wcześniejsze rozwiązanie bazowało na skryptach które były uruchamiane, sprawdzały i raportowały do serwera, teraz prace skryptów przejął klient NAP.

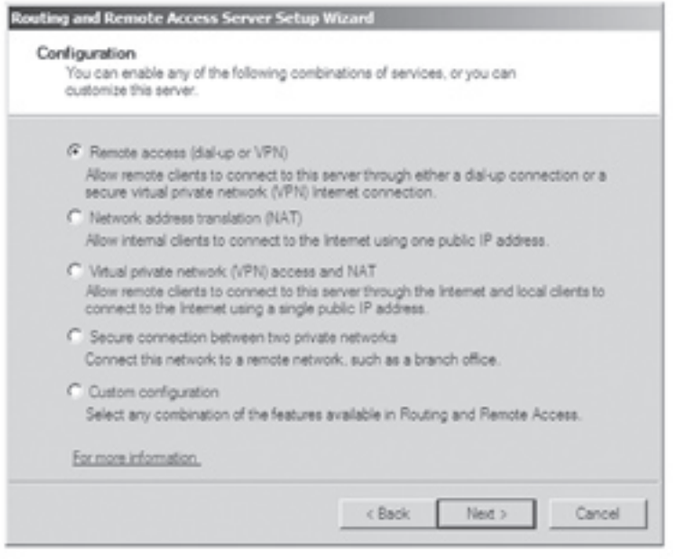
Do konfiguracji będzie nam potrzebny serwer certyfikatów, który możemy zainstalować na jakimś serwerze w domenie. Podobnie jak w poprzednich scenariuszach dodajemy rolę Network Policy Server oraz konfigurujemy System Health Validator, dalej dodajemy tak jak w pierwszym rozwiązaniu polisy i ustalamy, które są dla komputerów spełniających wymagania a które dla niespełniających ich. Dalej potrzebujemy Network Policy i Connection Request Policy aby określić przynależność klienta do danej sieci. Tworząc je wpisujemy nazwę i wybieramy serwer dostępowy



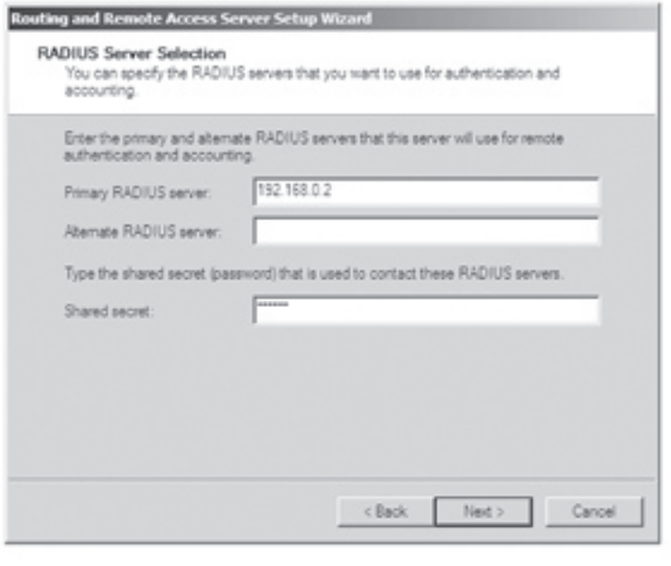
Oraz ustalamy numer IP serwera RADIUS



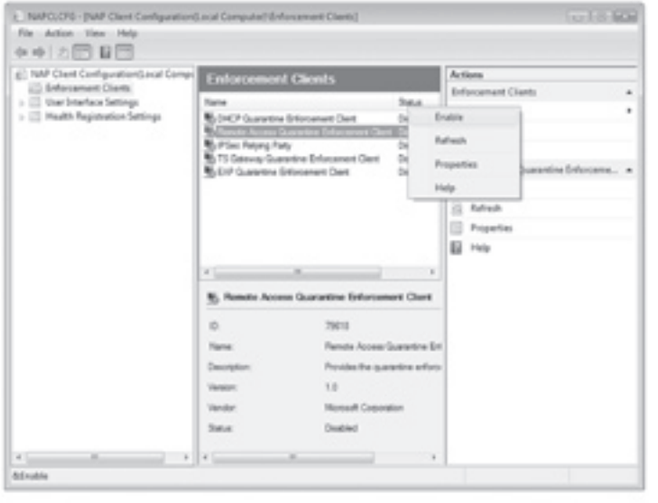
Mając już te ustawienie wybieramy jeszcze mechanizm autentykacji i to wszystko na tym serwerze. Na serwerze VPN instalujemy oraz konfigurujemy RRAS-a



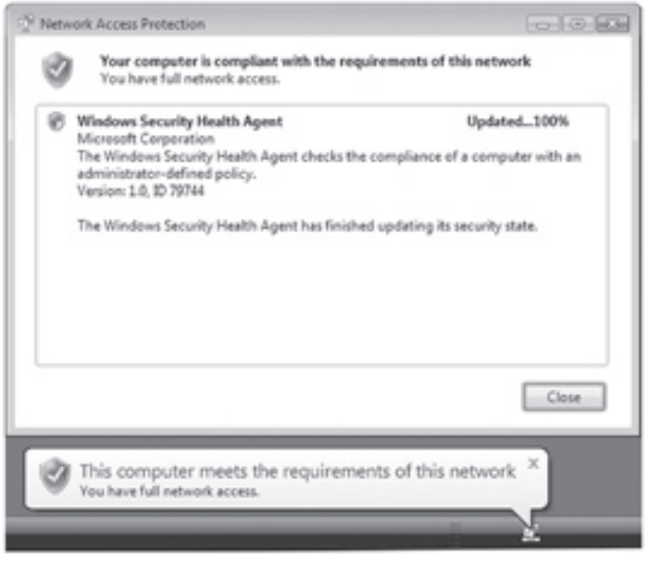
Podczas konfiguracji wypełniamy informacje o serwerze RADIUS



I to tyle po stronie serwerów. Przenosimy się na klienta. Jego oczywiście dodajemy do domeny, instalujemy NAP klienta (jeśli nie ma wbudowanego), oraz konfigurujemy go. Konfiguracja sprowadza się do włączenia jednego komponentu – Remote Access Quarantine Enforcement Client tak ja na ekranie poniżej



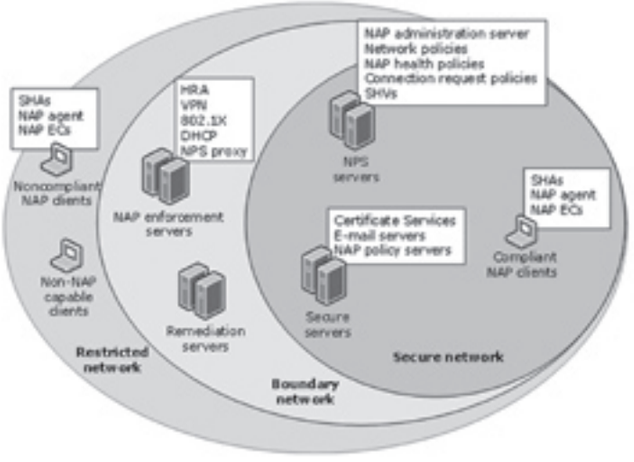
Oraz to co przy każdej konfiguracji VPN czyli tworzenie nowego połączenia. Po pozytywnym połączeniu się powinniśmy zobaczyć informację



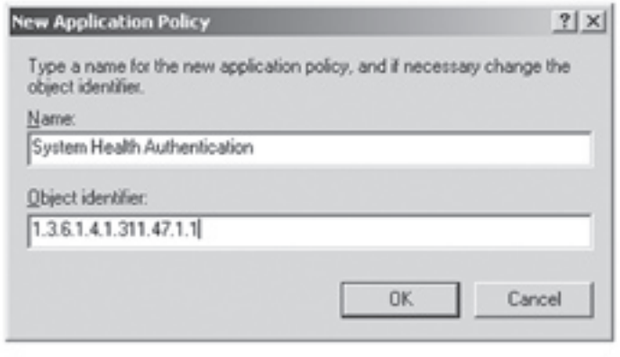
Jak skonfigurować NAP w połączeniu z IPsec

Najważniejsza część NAP. Ten komponent wykorzystuje mechanizm nazwany izolacją domeny. Jak izolację połączymy z certyfikatami zdrowia wyjdzie nam potężne dobrze działające i bezpieczne środowisko do pracy. Komputer który będzie chciał dostać się do domeny będzie potrzebował certyfikatu IPsec a tym będzie certyfikat zdrowa, dostanie go jak będzie wyglądał na odpowiednio skonfigurowany i z najnowszymi aktualizacjami. To rozwiązanie może być używane bez izolacji domeny – jednak nie jest to już tak bezpieczne rozwiązanie. To znaczy komunikacja może być szyfrowana, ale nie musi być szyfrowana.

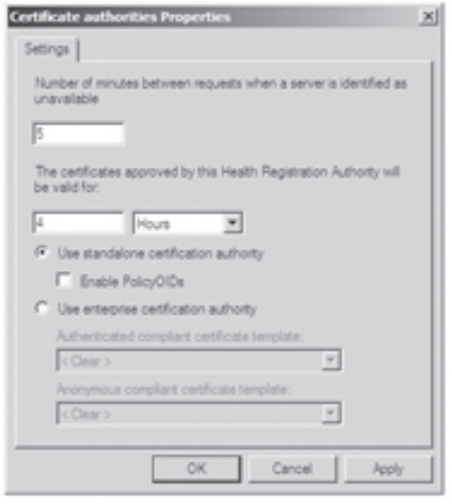
Schemat takiego rozwiązanie widzimy na poniższym diagramie.



A konfiguracje wygląda następująco: przyjmijmy, ze mamy serwer AD z DNS, Windows 2008 i stacje klienckie. Na serwerze z Active Directory instalujemy serwer certyfikacji na którym tworzymy szablon do naszych certyfikatów. Ważne aby w polu Object identifier wpisać wartość 1.3.6.1.4.1.311.47.1.1



Dalej dobrze jest ustawić autoenrollment w systemowych polisach. Na serwerze Windows 2008 instalujemy role Health Registration Authority oraz konfigurujemy aby korzystała z certyfikatów wystawionych przez nasz CA. Później powinniśmy zainstalować na naszym serwerze z NAP podrzędne CA do wystawiania certyfikatów. Taki certyfikat powinien być wystawiony na dość krótki czas



Dalej postępujemy zgodnie ze standardowymi procedurami czyli tworzymy Security Health Validatora, który określa co ma być sprawdzane na kliencie

I w zasadzie to wszystko. Przynajmniej od strony serwera NAP. Na stacji trzeba zainstalować klienta NAP oraz zobaczyć czy działa autoenrollment certyfikatów.

ABC CENTRUM EDUKACYJNE DATA

6. Platforma webowa ILS 7.0

Wstęp

Na wstępie warto wspomnieć o poprzednich wersjach serwera. Zacznijmy od IIS 5.0 dostępnego na platformie Windows 2000. Rozwiązanie to charakteryzowało sie tym, że produkt po zainstalowaniu zawierał wszystkie mozliwe usługi i komponenty: SMTP, NNTP, WWW. Serwer www posiadał wszystkie dostępne uwczesnie moduły i rozwiązania: IP Printing, obslugę CGI, strony pomocy, rozszerzenia front page, webową stronę administracyjną itd. Powodowało to sporo zagrożeń związanych z bezpieczeństwem systemu operacyjnego. Stawiało to również przed administratorem nowe wyzwania i wymagało od niego nie małej wiedzy z zakresu bezpieczeństwa w celu właściwego zabezpieczenia serwera webowego. Przydatnymi narzędziami do tego celu były między innymi takie programy jak IISLockdown, URLScan.

Kolejna wersja Internet Information Serwera- IIS 6.0 została napisana całkowicie od nowa. Wiązało sie to między innymi ze zmianą polityki w Microsofcie gdzie bezpieczeństwo w myśl hasła „Secure by design, secure by default" stało się sprawa kluczową. IIS 6.0 nie jest instalowany domyślnie, natomiast po zainstalowaniu oferuje minimalną funkcjonalność- obsługa stron statycznych. Domyślnie wyłączona jest obsługa wszystkich rozszerzeń z wyjątkiem Static HTML. Kolejna kluczowa zmiana to pojawienie się pul aplikacyjnych. Wpłynęło to na stabilność i wydajność serwera webowego. Podniósł się poziom bezpieczeństwa poprzez zastosowanie konta lokalnego network_service w trybie, którego działałają pule aplikacyjne. Rozwiązania takie jak Recycling, health ping dalej są stosowane w kolejnej wersji produktu.

W Wersji 7.0 podstawową zmianą jest modularność rozwiązania. Mamy dostępnych ponad 40 modułów. Każdy moduł stanowi pewną atomową jednostke jak np. AnonymousAuthenticationModule, które mozemy łączyć w pewne zestawy. Instalacja domyślna powoduje dodanie tylko paru wymaganych, określanych nazwą Core Modules. Możemy również definiować i dodawać swoje moduły dzięki czemu jest to rozwiazanie w pełni rozszerzalne. Warto wspomnieć, że w przypadku Windows 2003 po dodadniu Serwera IIS 6.0 instalowal on sie w sposób „okrojony" komponenty domyślnie instalowane były wyłączone, ale kod znajdował się w systemie. Mogło to stanowic pewne zagrożenie. Jezeli chodzi o IIS 7.0 nie wybranie modułu na etapie dodawania roli blokuje jego fizyczna instalacje i kopiowanie na dysk.

Poniżej znajduje się lista nowych rozwiązań zaimplementowanych w tej wersji produktu.

Platforma webowa ILS 7.0 charakteryzuje się następującą funkcjonalnością:

Architektura modularna, rozszerzalność – Możliwośc dodawania pojedyńczych modułów zarządzanych niezależnie (instalacja, usunięcie) Redukuje to ilość kodu zainstalowanego na serwerze co finalnie ogranicza mozliwości ataku oraz podnosi wydajność. Redukuje też działania

administracyjne związane z zarządzaniem i aktualizowaniem produktu. Można łatwo rozszerzać funkcjonalność poprzez tworzenie i dodawanie swoich modułów

Rozszerzony interfejs uzytkownika – Zmiana sposobu prezentacji obiektów z zakładek na ikony. Zarządzanie za pomocą aplikacji wywoływanych z linni polecen: APPCMD, Powershell. Konsola IIS 7.0 Manager umożliwia delegowanie kontroli i dostęp tylko do konkretnych obiektów, pozwala to finalnie przypisywać administratorom różnego szczebla uprawnienia do operacji, które powinni wykonywać

Schemat i konfiguracja IIS przechowywana w czytelnym pliku XML – Jest możliwość przenoszenia plików XML jak i trzymania ich w jednym centralnym punkcie. Ułatwia to administracje serwerami webowymi zwłaszcza w przypadku firm hostingowych

Zwiększone bezpieczeństwo – W IIS 7.0. Możemy konfigurować autentykacje opartą na formularzach webowych do dowolnej zawartości np: HTML, ASP, PHP. Istotną zmianą wartą podkreślenia jest możliwość definiowania kont lokalnych w IIS. Dzięki czemu nie ma potrzeby autentykować użytowników w oparciu o konta domenowe lub konta lokalne serwera. Możemy zarządzać dostępem do obiektów z jednego miejsca przypisując prawa uzytkownikom domenowym, lokalnym systemowym i IISa.

Wbudowane narzędzia do analizy oraz śledzenia zdarzeń – IIS 7.0 zawiera moduły ułatwiające diagnostykę problemów i zdarzeń. Wysoki poziom szczegółowoćci komunikatów pozwala programistom szybko wyizolować i naprawić błąd. Zdarzenia możemy sledzić podając typ błędu, wywołanie rozszerzenia pliku, czy przekazania na serwer webowy określonego polecenia itp.

Bezproblemowa i wydajna obsługa aplikacji webowych zawierających dowolną zawartość – Obsługiwane są statyczne strony, PHP, ASP, ASP.NET i inne z mozliwością „mieszania" technologi . Związane jest to z nowym zestawem publicznych API używanych zamiast standardowych ISAPI.

Nowy Serwer FTP dostępny poza dystrybuacją IIS 7.0 – Najnowszą wersję serwera FTP można pobrać ze strony www.iis.net. Serwer FTP zamieszczony w wersji instalacyjnej systemu Windows 2008 jest produktem zgodnym z IIS 6.0

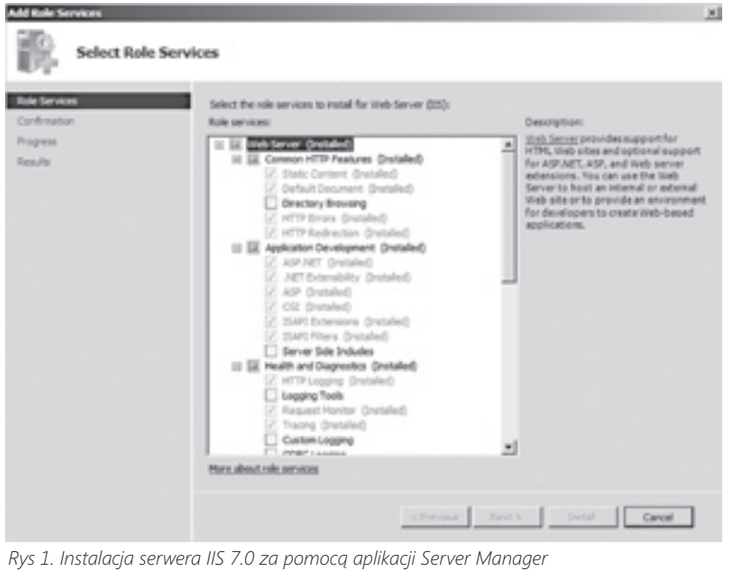
Instalacja Serwera IIS 7.0

Podobnie jak w przypadku wersjji poprzedniej systemu operacyjnego. Serwer IIS 7.0 jest dostępny wraz z platformą Windows 2008 natomiast nie jest automatycznie instalowany. System Operacyjny wraz z komponentami jest domyślnie skonfigurowany w sposób maksymalnie bezpieczny. Oznacza to, ze po zainstalowaniu otrzymujemy podstawowa funkcjonalność i sami w pełni świadomie ją rozszerzamy.

Podstawowa różnica w do wersji 6.0 jest widoczna już na etapie instalacji. Jest to modularność IIS. Serwer IIS 6.0 był monolityczny- albo wszystkie podstawowe komponenty albo zaden. W tej wersji jest dostępnych okolo 40 gotowych modułów do wyboru. Mozna też rozszerzać funkcjonalność serwera dodając swoje komponenty. Dla przykładu- po zainstalowaniu IIS 6.0 otrzymywaliśmy platforme webowa z wszystkimi metodami autentykacji takimi jak: Anonymous, Basic, Windows Intagrated. Oczywiście od Administratora zależało włączenie odpowiedniej metody. Istotne jest jednak to, że kod do wszystkich modułów był instalowany i znajdował sie w systemie operacyjnym. W IIS wersja 7.0 Każdy moduł jest dodawany oddzielnie.
Proces instalacji odbywa się poprzez sekcje Roles w aplikacji Server Manager.

Instalacja Serwera IIS 7.0 za pomocą aplikacju Server Manager

1. W celu zainstalowania serwer IIS 7.0 uruchom aplikacje **Server Manager**.
2. Przejdź do sekcji **Roles** i kliknij **Add Role Services** a nastepnie wybierz odpowiednie moduły.
3. Po zweryfikowaniu wybranych modułów kliknij Next i po zakończeniu instalacji Finish



Rys 1. Instalacja serwera IIS 7.0 za pomocą aplikacji Server Manager

Instalacja za pomocą narzędzi linii poleceń

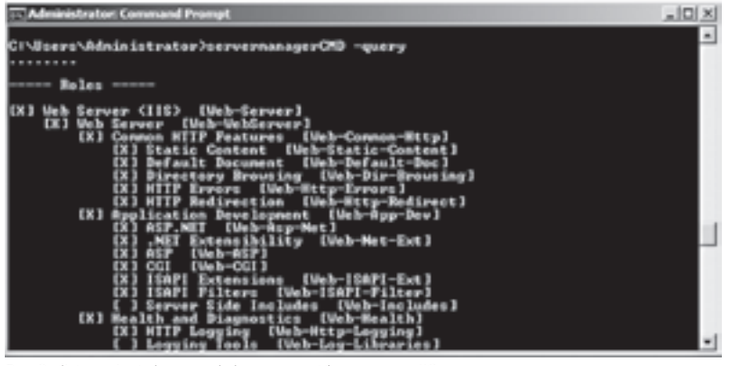
Kolejna metoda instalacji (przydatna zwłaszcza na platformie bez trybu graficznego –Core) to instalacja za pomocą aplikacji systemowych- **ServerManagerCmd** i **PKGMGR**. W celu zainstalowania IIS 7.0 z linii poleceń wykonaj poniższą operację.

Ponizszy przykład pozwala na instalacje IIS 7.0 z domyślnymi komponentami:

ServerManagerCMD -I Web-Server

Poniższy przykład pozwala na instalacje tylko wybranych komponentów:

ServerManagerCMD -install Web-Http-Redirect Web-ASP-Net Web-Net-Ext Web-ASP Web-CGI Web-ISAPI-Ext Web-ISAPI-Filter Web-Http-Tracing Web-Basic-Auth Web-URL-Auth Web-Dyn-Compression Web-Scripting-Tools Web-Mgmt-Service



Rys 2- lista zainstalowanych komponentów serwera IIS

Kolejna aplikacja wywoływana z linii poleceń to PKGMGR. Proces instalacyjny wykonywany za pomocą pkgmgr pozwala również na uszczegółowienie komponentów instalacyjnych:

Start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-ASP;IIS-ISAPIExtensions;IIS-ApplicationDevelopment;IIS-CGI;IIS-HealthAndDiagnostics;IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-Security;IIS-RequestFiltering

Instalacja niepilnowana

Instalacja IISa w sposób niepilnowany może zostac wykonana za pomoca wyżej opisancyh aplikacji PKGMGR i ServerManagerCMD, gdzie parametry instalacyjne zostaną przekazane przez plik XML np.

start /w pkgmgr /n:C:\unattend.xml

Weryfikacja poprowności instalacji

Po zainstalowaniu serwera IIS należy zweryfikować poprawność instalacji. Najłatwej wykonać tą operację poprzez sprawdzenie statusu IIS w konsoli administracyjnej, przejrzenie zainstalowanych

ról, sprawdzenie sekcji „Role Status", weryfikacje folderu c:\inetpub jak i usług IIS 7.0. Przejrzenie logu aplikacyjnego i systemowego

Administracja serwerem IIS 7.0

Konsola IIS Manager

Zaczniemy od omówienia konsoli administracyjnej Inernet Information Services Manager.
Dla osoby znającej poprzednią wersje IISa pierwszą widoczną różnicą bedzie zmiana dotychczasowych zakładek konfiguracyjnych na ikony. Interfejs konsoli jest zgodny z interfejsem konsoli MMC 3.0. Składa się z trzech elementów: lewa- widok drzewa, srodkowa właściwości obiektu, prawa akcje do wykonania. IIS Manager umozliwia przeglądanie statusu serwera w czasie rzeczywistym, konfiguracje komponentów, zbierania informacji o zdarzeniach, konfigurowanie współdzielenia konfiguracji, delegowania uprawnień do wybranych elementów.

Rys 3- Konsola administracyjna IISa 7.0

Aplikacje wywoływane z linii poleceń

Operacje administracyjne moga byc wykonywane za pomocą wyżej wymienionej konsoli graficznej, lub za pomocą aplikacji wywoływanych z linii poleceń. Aplikacje wywoływane z linii poleceń są szczególnie przydatne w przypadku instalacji serwera IIS 7.0 na platformie Core. Wykonując zadania administracyjne możemy wspierać się potężnymi narzędziami takimi jak **appcmd** i **powershell**.

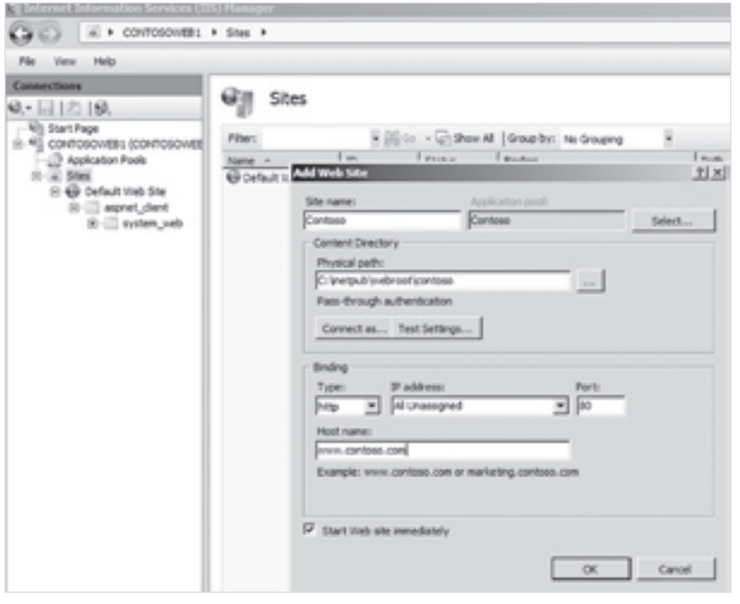
Poniżej znajduje się przyklad zastosowania aplikacji APPCMD w celu utworzenia web site:*AppCmd add site /name:"test1 Website" /bindings:http/*:80:www.test1.com /physicalPath:"c:\inetpub\test2"*

Poniżej znajduje się przyklad zastosowania aplikacji APPCMD w celu utworzenie puli aplikacyjnej: *appcmd add apppool /name:Test1AppPool*

Podstawowe operacje administracyjne

Utworzenie Web Site
Jedną z podstawowych początkowych operacji po zainstalowaniu IIS jest utworzenie web situ. Wykonamy to w tym przykładzie za pomocą konsoli administracyjnej.

1. W celu utworzenia Web Situ kliknij prawym przyciskiem myszy na kontenerze Sites.
2. Pod prawym przyciskiem wybierz opcję Add Web Site. Następnie wypełnij następujące pola: Site Name, physical path, Bindings i Host name. Przykład zajduje się na poniższym rysunku.



Rys. 4 Tworzenie Web Site

Tworzenie pul aplikacyjnych

Warto zwrócić uwagę na to, że tworząc web site tworzymy od razu pulę aplikacyjną dla danego situ. W przypadku IIS 6.0 administrator musiał sam utworzyć pulę aplikacyjną i przenieśc do niej aplikacje webową. Opcjonalnie pozostawić Web site w domyślnej puli aplikacyjnej. W IIS 7.0 domyslnie każdy web site działa w oddzielnej puli aplikacyjnej.

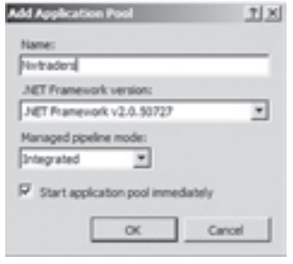
Pula aplikacyjna definiuje nam właściwości procesu danej aplikacji (worker process) określa takie właściwości jak Identity- tryb konta, w którym działa worker proces, parametry odzyskiwania (Recyckling) Ogólnie rzecz biorąc dzięki temu, że automatycznie każda aplikacja webowa działa w oddzielnej puli aplikacyjnej mamy wiekszą stabilność serwera jak i możliwość elastycznej konfiguracji każdego web situ. Pule aplikacyjne oddzielają aplikacje webowe przed możliwą interakcją między sobą. Zawieszenia aplikacji webowej nie będzie miało wpływu na pozostałe web site. Konfiguracja Recyclingu umozliwia ustawienia np. odbudowania procesu w3wp.exe (worker proces) o wskazanych godzinach. Dodadkowe ustawienia odbudowywania procesu w3wp.exe znajdują się w Recycling Conditions. Serwer IIS 7.0 umożliwia tworzenie dwóch typów pul aplikacyjnych Classic i Integrated. Domyślnym typem jest Integrated Mode.

Classic mode – jest trybem zgodnosci z IIS 6.0. Dotyczy to mechanizmów Recyclingu, sprawdzania stanu procesu (health monitoring) Funkcjonalność pozostała niezmieniona w porównaniu do wersji IIS 6.0. Tryb Classic powoduje zainstalowanie i użycie tego samego modułu ISAPI oraz ASPNET_ISAPI.dll co w IIS 6.0. Kiedy worker proces puli aplikacyjnej otrzyma ządanie (request) najpierw jest on przetwarzany przez IISa, np. jest wykonywana autentykacja uzytkownika, następnie żądanie jest przekazywane do biblioteki ASPNET_ISAPI.dll, finalnie żądanie wraca do IISa w celu wysłania odpowiedzi. Takie rozdzielenie powoduje wykonywanie podwójne niektórych kroków jak autentykacja i autoryzacja (na poziomie IISa i ASP.NET) dodatkowo uniemozliwia stosowanie np. formularzy autentykacyjnych w innych technologiach z wyjątkiem ASP.NET. Czy warto uzywać trybu Classic? Ciężko jednoznacznie powiedzieć. Zależy to od typu aplikacji i finalnie może sie okazać, ze nie które aplikacje w trybie classic będą działac lepiej niż w integrated.

Integrated mode – nowy tryb, ktory jest trybem domyślnym dla każdej nowej puli aplikacyjnej. Umozliwia przetwarzanie kodu w sposób strumieniowy dla wszystkich ządań niezależnie od technologii np. mozemy zastosować .NET Forms authentication dla dowolnej zawartości. Kiedy aplikacja używa trybu Integrated korzysta z zalet architektury IIS i ASP.NET. Kiedy worker proces puli aplikacyjnej otrzyma żądanie (request) przekazywany jest on przez uporządkowaną listę modułów gdzie kazdy moduł wykonuje sobie przypisane zadanie i wysyła odpowiedź. Funkcjonuje to od nazwą “unified Pipeline”. Za przetwarzanie żądan w trybie integrated odpowiada Webengine.dll. Jest to natywny moduł zaimplementowany w IIS, ktorego definicja znajduje sie pliku ApplicationHost.Config w sekcji <Global Modules>. Podsumowując pozwala to programistom na mieszanie kodu (modułów) tworzonego w wielu technologiach i jest onżfinalnie przetwarzany jako jeden strumień niż oddzielnie przez odpowiednie ISAPI.

1. W celu utworzenia puli aplikacyjnej przejdź w sekcji **connections** do obiektu **Application Pools.**

2. Kliknij prawym przyciskiem i wybierz **Add Aplication Pool**. Wybierz tryb zgodności i kliknij **OK**



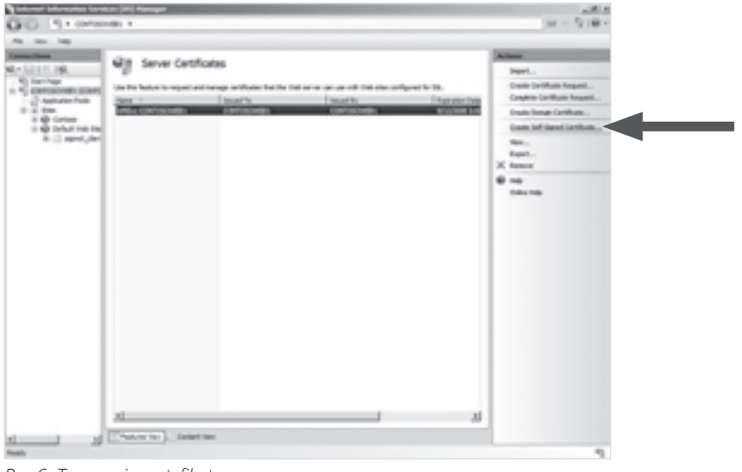
Rys 5. Tworzenie puli aplikacyjnej

Wygenerowanie Certyfikatu

Kolejna częsta operacja administracyjna jest wygenerowanie certyfikatu i przypisanie certyfikatu do situ webowego. Warto wspomnieć o tym, że IIS 7.0 ma zawartą w sobie aplikacje znaną z Resource Kita do wczesniejszych wersji serwera IIS- SelfSSL. Umozliwia ona generowanie certyfikatu dla samego siebie bez odwołania do CA. Poniżej znajduje się rysunek przedstawiający sekcje Server Certyficates. Warto zwrócic uwagę na sekcję Actions i opcję „Create SelfSignedCertyficates".

1. W celu wygenerowanie certyfikatu Kliknij na serwerze webowym znajdującym sie na liście **connection.**

2. Kliknij w polu środkowym na ikonie **Server Certyficates** a następnie w sekcji **Actions** na opcję **Create SelfSigned Certyficate.**



Rys 6. Tworzenie certyfikatu

Przypisanie wygenerowanego certyfikatu do Web Situ.

1. W tym celu przejdź do sekcji **Sites**. Wybierz odpowiedni Web site.

2. Kliknij w polu **Actions** na opcję **Bindings**.

3. Następnie kliknij przycisk **Add**. W okienku **Add site Bindings** z listy type wybierz **https**. Po wybraniu https należy wskazać certyfikat który chcemy przypisać do tego web situ.

4. Włącz stosowanie szyfrowanego połączenia. Wykonujemy to na poziomie web situ za pomoca opcji **SSL Settings**.

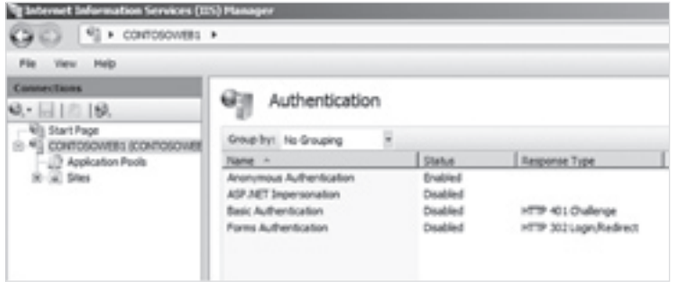
Rys.7 Włączenie SSL na poziomie web situ

Rys. 8 Przypisywanie certyfikatu do Web Situ

Konfiguracja metod Autentykacji

W celu skonfigurowanie wybranego typu autentykacji należy tą operację najpierw wykonac na poziomie serwera, gdzie globalnie określamy, które mechanizmy logowania można edytować (Patrz delegowanie uprawnień w części bezpieczeństwo). Domyślna konfiguracja jest taka, że ustawień dot. autentykacji na poziomie serwera nie mozna nadpisać na poziomie Situ. Wobec tego na poziomie Web Situ mamy możliwość włączenia tylko tych mechanizmów, które zostały włączone wczesniej na poziomie serwera.

Poniższy rysunek prezentuje zawartość modułu autentykacyjnego na poziomie serwera. Proszę zwrócić uwage, że nie ma tam popularnej metody logowania Windows Integrated. Wynika to po prostu z tego, że ten moduł nie został dodany w trakcie instalacji.

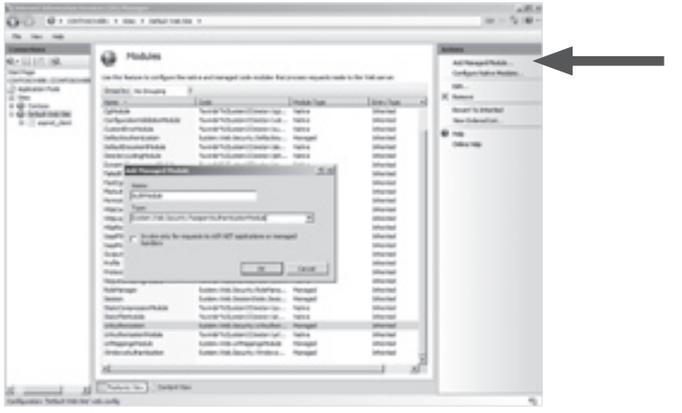


Rys 9. Konfiguracja Autentykacji na poziomie serwera

Dodawanie modułu

Jak już było wielokrotnie wspominane IIS 7.0 charakteryzuje się budową modularną. Umozliwia to dodawanie tylko tego kodu, który jest niezbędny w celu osiągnięcia oczekiwanej przez nas funkcjonalności. Ponizszy zrzut ekranu prezentuje w jaki sposób możemy zarządzac modułami.

1. W celu dodania nowego modułu wybierz odpowiedni web site z listy **connections**.
2. W sekcji środkowej kliknij na obiekcie **Modules**.
3. Z sekcji z prawej strony wybierz **Add Managed Module**.
4. Wybierz moduł, który chcesz dodać. Moduły możmy rownież definiować w ApplicationHost.Config w sekcji <Modules>. Proces dodania modułu został zaprezentowany na poniższym zrzucie ekranu.

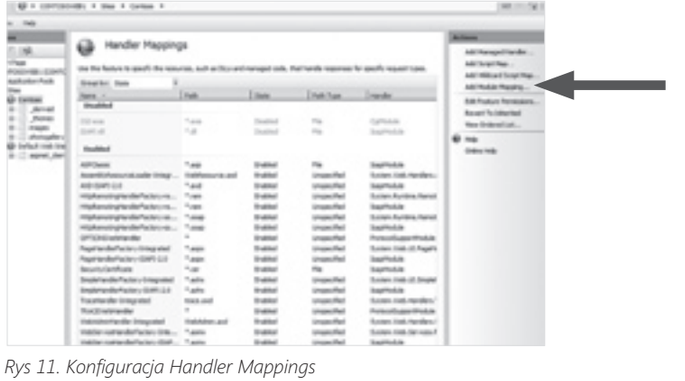


Rys 10. Dodawanie modułu

Dodanie nowego handlera (Handler Mappings)

Konfiguracja Handler Mappings jest kolejnym krokiem po dodaniu własnego modułu. Handler Mappings stanowi powiązanie pomiędzy modułem zaisntalowanym w IIS a typem stronym obsługiwanym przez ten moduł. Proszę zwrócić uwagę, że dostępne są standardowe handlery do obsługi stron: asp, aspx, soap, cer, asmx i innych.

1. W celu zdefiniowania nowego handlera kliknij w sekcji **connections** na wybranym web sicie.
2. Przejdź do sekcji srodkowej i kliknij na ikonie **Handler Mappings**, następnie z menu actions wybierz **Add Module Mappings**.
3. Podaj określone rozszerzenia plików obsługiwane przez dodawany handler, wybierz moduł z listy.
4. Podaj nazwe **handlera** i kliknij na przycisku **OK.**



Rys 11. Konfiguracja Handler Mappings

Konfiguracja Serwera IIS 7.0

Serwer webowy nie zawiera już metabase znanej z poprzednich wersji serwera IIS. Wobec tego narzędzie MetaBaseEdit jest już bezużyteczne. Konfiguracja znajduje się odpowiednio w plikach **ApplicationHost.Config** – ustawienia serwera i **Web.Config** – ustawienia web situ. MetaBase w poprzednich wersjach IISa była ściśle powiązana z okreslonym serwerem, wobec tego komplikowało to proces przenoszenia konfiguracji na inny serwer. Z applicationhost.config jest inaczej, jest on całkowicie przenośny. Zaletą tego rozwiązania jest właśnie mozliwośc kopiowania konfiguracji pomiedzy serweramy za pomocą Xcopy jak i skonfigurowanie jednego centralnego punktu przechowywania pliku konfiguracyjnego do którego równolegle, może odwoływac się wiele serwerów. Jest to niewątpliwie przydatne w przypadku administrowania farmą serwerów. Stwarza to nowe możliwości dla firm hostingowych ponieważ konfiguracja wielu serwerów może być składowana w jednym miejscu.

Przechowywanie całej konfiguracji w XML umożliwia też w zależności od potrzeb biznesowych definiowanie odpowiednich sposobów administracji. Mamy możliwość nadawania uprawnień do wykonywania tylko określonych operacji, co było niemozliwie w poprzedniej wersji. Mozemy np. dać uprawnienia do zarządzania modułami autentykacyjnymi. Uzytkownik z takimi prawami będzie w stanie tylko konfigurować mechanizmy autentykacyjne na poziomie danego web situ. Wobec tego możemy wprowadzic nastepujący podzial metod administracji:

Zcentralizowana - mozliwosc edycji pliku konfiguracyjnego na poziomie serwera applicationhost.config- administracja całym serwerem IIS

Delegowana- nadanie uprawnien do wybranych sekcji w applicationhost.config i mozliwosc edytowania ich w pliku web.config przez administratora portalu

Jednym ze sposobów konfiguracji serwera jest użycie PowerShella, który w sposób pośredni wykonuje edycje pliku ApplicationHost.config. PowerShell jest mocno wspierany w IIS 7.0. Serwer webowy zawiera również rozszrzenie WMI, które umozliwia dostęp do informacji na temat serwera również za pomocą VBScript, Jscript. Ze względu na modularność IIS 7.0 w celu uzyskania wymienionej funkcjonalności należy doinstalować komponent IIS Management Scripts and Tools.

Konfiguracja serwera IIS za pomocą ApplicationHost.config

ApplicationHost.config znajduje sie w lokalizacji %windir%\system32\inetsrv\config. Zawiera ustawienia globalne dla całego serwera IIS. Zablokowanie określonych opcji powoduje calkowite zablokowanie dla wszystkich web sitów, czyli brak możliwości właczenia w pliku web.config na niższym poziomie. Nalezy zauważyć, że mozliwość nadpisywania w pliku web.config zależy od „allow" lub „deny" na koncu wiersza danej sekcji w pliku applicationhost.config. Poniżej zawarty fragment pliku ApplicationHost zawiera ustawienia dot. autentykacji. Warto zwrócić uwagę na overrideModeDefault="Deny" blokuje to modyfikacje na poziomie web situ.

```
<sectionGroup name="security">
  <section name="basicAuthentication" overrideModeDefault="Deny" />
  <section name="digestAuthentication" overrideModeDefault="Deny" />
<section name="windowsAuthentication" overrideModeDefault="Deny"/>
</sectionGroup name="security">
```

Kolejna sekcja, której sie przyjrzymy to fragment modułów globalnych. Zawiera ona domyslnie zainstalowane moduły, które są napisane w kodzie natywnym C\C++

```
<globalModules>
    <add name="DynamicCompressionModule" image="%windir%\System32\inetsrv\compdyn.dll" />
    <add name="StaticCompressionModule" image="%windir%\System32\inetsrv\compstat.dll" />
    <add name="DefaultDocumentModule" image="%windir%\System32\inetsrv\defdoc.dll" />
</globalModules>
```

Sekcja <Sites> w pliku applicationhost.config zawiera konfiguracje poszczególnych sitów

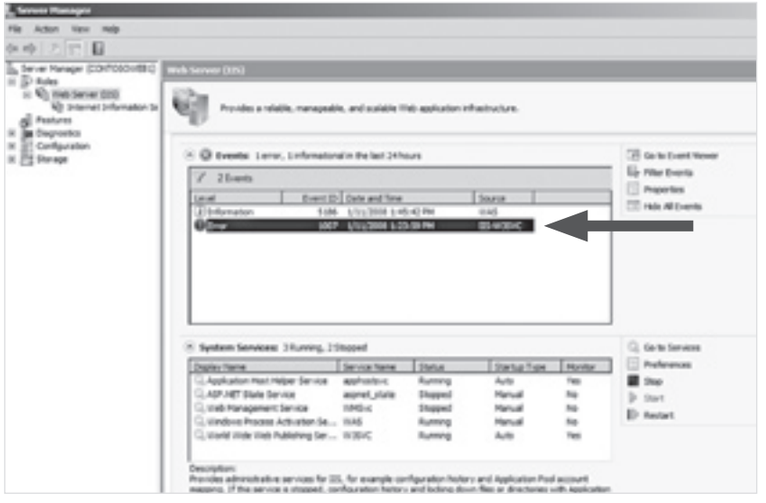
```
<sites>
    <site name="Default Web Site" id="1">
      <application path="/">
        <virtualDirectory path="/" physicalPath="%SystemDrive%\inetpub\wwwroot" />
      </application>
      <bindings>
        <binding protocol="http" bindingInformation="*:80:" />
      </bindings>
    </site>
```

Monitorowanie i obsługa błędów

Jedną z kluczowych zmian w IIS 7.0 jest rozudowany system monitorowania i diagnostyki. Programiści jak i administratorzy są w stanie szczegółowo analizować działanie każdej strony. Komunikaty o błędach w przypadku problemów są równiez zdecydowanie bardziej rozbudowane niz w wersjach poprzednich. Jednym z częstych problemow w IIS 6.0 i IIS 5.0 było analizowanie aplikacji webowych pod kątem występowania błędów. Pomiędzy wysłaniem żądania z przeglądarki a przetworzeniem i wysłaniem odpowiedzi następuję wiele operacji a proces nie był transparenty. Analiza każdego kroku była bardzo utrudniona. Niskopoziomowe monitorowanie wymagało specjalnych narzędzi dostępnych jako dodatki w pakiecie Resource Kit i w Service packu 1 do IIS 6.0.

Weryfikacja poprawnego działania w IIS 7.0 może być ukierunkowana na konkretną aplikacje i stronę. Można raportować zdarzenia związane z procesami roboczymi IISa (worker proces). Można przeglądać status wykonania w czasie rzeczywistym lub zbierać dane do logu w momencie spełnienia określonych warunkow, np. każdy błąd 500, lub żądania których przetworzenie trwało więcej jak 5 sekund. Dodatkowo programiści mogą rozszerzać liste zdarzeń zapisywanych w logu

Podstawowe raportowanie o zdarzeniach jest dostępne w server managerze na poziomie sekcji Rules. Klikając na prezentowanym Evencie typu Error mozna wywołac szczegóły tego zdarzenia. Sekcja Roles umożliwia również zweryfikowanie działania usług.



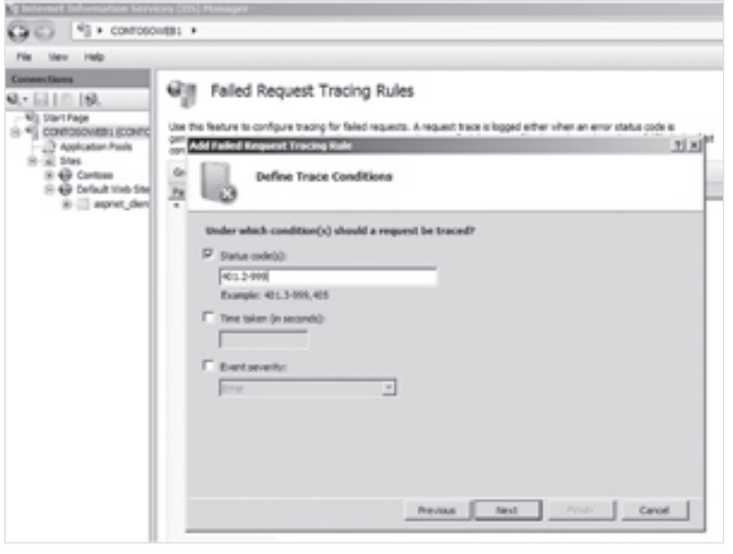
Rys 12. Bląd prezentowany w sekcji Roles w server Managerze

Monitoring FREB/MFRT (Making Failed Request Tracing)

FREB jest jednym z najciekawszych narzędzi w IIS 7.0. Umożliwia szczegółową analizę błędów jak i niskopoziomową analizę działania wybranych aplikacji webowych. Pozwala wyłapać wystąpienie konkretnego błędu, oraz szczegółowo zapisac informacje na temat wystapienia tego zdarzenia w logu. W celu konfiguracje FREB należy włączyć okreslony moduł Failed Request Tracing Rules. Wynik monitorowania zostanie zapisany do lokalizacji podanej w ścieżce.

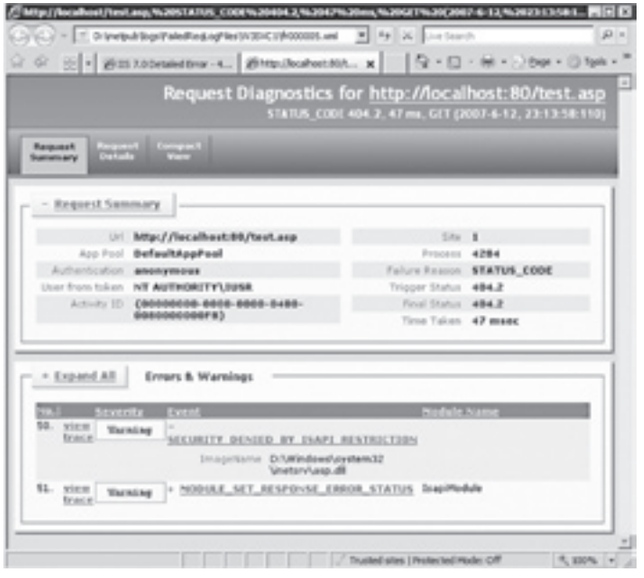
Włączenie monitorowania FREB

1. W celu włączenia monitorowanie FREB kliknij na serwerze webowym w sekcji **connections.**
2. Następnie kliknij w sekcji centralnej kliknij na **Failed Request Tracing Rules.**
3. Podaj jakiego typu zdarzenia chcesz logowac do pliku.
4. Podaj na jakiego typu stronach: ASP, ASP.NET itd (Po zapisaniu reguly monitorowania w momencie wygenerowania zdefiniowanego błedu szczegółowe informacje zostana zapisane do logu tekstowego w formacie XML)



Rys. 13 Konfiguracja FREB

Poniżej na zrzucie ekranu widać wynik logowania informacji na temat błędu zdefiniowanego w kroku poprzednim. Strona zawiera dwie sekcje: Request summary prezentującą podstawowe informacje na temat wystapienia zdarzenia i sekcje Errors & Warnings zawierającą szczegółowy opis problemu



Rys 14. Wynik działania FREB

Runtime Status and Control API (RSCA)

W IIS 7.0 pojawiło się narzedzie umożliwiające szczegółową analizę działania serwera webowego w czasie rzeczywistym. RSCA umozliwia bardzo szczegółowe monitorowanie sitów, pul aplikacyjnych, aplikacji .NET Framework. Zebrane informacje mogą być bardzo przydatne dla administratorów i programistow w celu optymalizacji działania serwera IIS 7.0. RCSA pobiera informacje na temat działania obiektu poprzez WMI i API (Microsoft.Web.Administration)
Do wyswietlania tych informacji może posłużyć aplikacja AppCMD

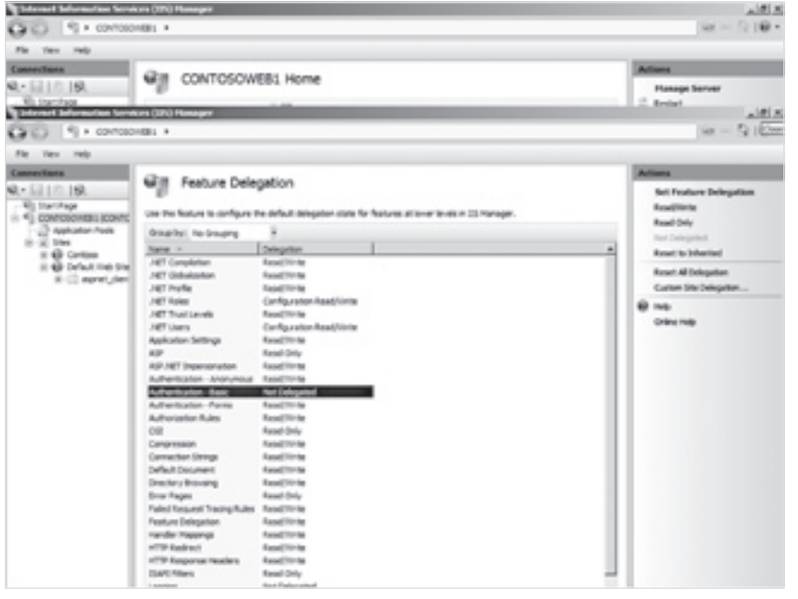
Bezpieczeństwo

Poruszając zagadnienia zw. z bezpieczeństwem serwera IIS 7.0 ponownie trzeba wspomnieć o tym, że nie jest on instalowany domyslnie wraz z systemem operacyjnym a po instalacji otrzymujemy tylko podstawową funkcjonalność – statyczny HTML. Dodatkowo na etapie instalacji mamy mozliwość doboru modułów do instalacji.

Zaczniemy od zmiany modelu administracyjnego. W IIS 6.0 w celu wykonywania wszystkich operacji administracyjnych na serwerze webowym były wymagane uprawnienia lokalnego administratora. W IIS 7.0 pojawiła sie możliwosc delegowania uprawnien do wykonywania określonych operacji.

Delegowanie kontroli

W celu delegowania kontroli należy ustawić wartosc „Allow" dla poszczególnych modułów na poziomie serwera w pliku applicationhost.config do odpowiednich sekcji. Nastepnie nadać prawa na poziomie web situ. Możemy to wykonać w sposób bezpośredni edytując plik applicationhost.config ustawiając wartości „Allow" lub „Deny" na poziomie globalnym. Jednym ze sposobów na odblokowanie "Unlock" sekcji na poziomie serwera, to ustawienie wartości dla klucza **OverrideModeDefault** na **Allow** (fragment pliku applicationhost.config- patrz powyżej) Następnie sekcje „Unlocked"mogą być delegowane i ustawiane w pliku web.config.
Plik Web.config, może byc kopiowany pomiędzy serwerami dzięki czemu automatycznie dana osoba uzyska dostęp do wskazanej sekcji na każdym serwerze. Drugą metodą jest ustawienia opcji Read/Write na wybranym module w sekcji **Feature Delegation** na poziomie Web Serwera za pomocą konsoli administracyjnej IIS Manager. Opcja **Read Only** pozwala na przegladanie ustawień, **Not Delagated** blokuje wyświetlanie danej opcji. Widok Feature Dlegation jest prezentowany poniżej



Rys 15. Ustawianie delegacji za pomocą IIS Managera

Podsumowując Delegacja pozwala uzytkownikom nie posiadajacym uprawnień administacyjnych na serwerze, na zarządzanie pewnym wycinkiem konfiguracji. Dzięki czemu finalnie możemy zdefiniować uzytkowników pełniących następujące funkcje administracyjne:

Administrator Serwera Webowego- Web Administrator ma pełne uprawnienia i możliości konfiguracyjne. Administrator serwera musi należec do lokalnej grupy administratorow systemowych.

Web Site Administrator- Administrator situ ma mozliwości konfiguracyjne na poziomie Web situ. Musi mieć mozliwość zalogowania do serwera Webowego co oznacza, że musi posiadać konto na poziomie domeny, lokalnego komputera lub na poziomie serwera Webowego (nowe rozwiązanie)

Web Application administrator. Administrator Aplikacji webowej może konfigurować ustawienia aplikacji na poziomie web situ. W tym celu podobnie jak administrator web situ musi miec konto i delegowane uprawnienia do odpowiedniej sekcji.

Lokalne konta w IIS 7.0

Jedną z kluczowych nowości w serwerze IIS 7.0 jest mozliwosc zakladania kont na poziomie serwera Webowego. Konta zakładamy na poziomie serwera a później delegujemy dostęp na poziomie web situ. Ponizej znajduje się formularz tworzenia konta lokalnego w IIS 7.0

Tworzenie kont lokalnych

1. W celu utworzenia konta w IISie kliknij w sekcji lewej (connections) na serwerze webowym.
2. W sekcji środkowej (Feature View) kliknij na ikonie **IIS Manager Users**.
3. Z prawej strony z sekcji Actions kliknij na **Add User.** Wypełnij poniższe pola.

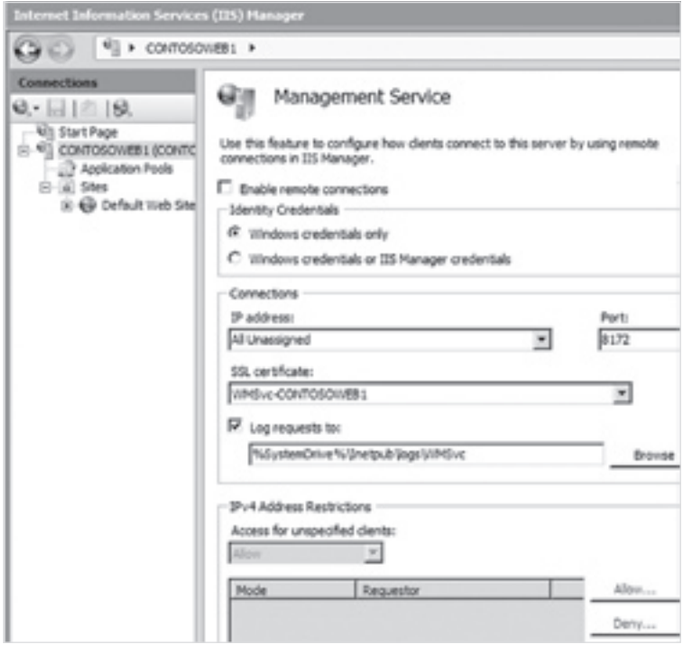
Rys 16. Tworzenie konta lokalnego

Zdalna administracja

IIS 7.0 umożliwia zdalną administracje z poziomu konsoli IIS Managera . Konsola kontaktuje się z wybranym serwerem po HTTPS (domyslnie na porcie 8172) co ułatwia cały proces konfiguracyjny. Nie ma dotychczasowej komunikacji DCOM pomiędzy stacja zarzadzającą a serwerem IIS, która była trudna do skonfigurowania na firewallu. Nowe rozwiązanie o nazwie **Management Service** umozliwia zdalne podłączenie do serwera IIS 7.0 za pomocą konsoli IIS 7.0 Manager. Połączenie obsługiwane jest przez specjalny serwis **WMSVC**. Połączenie jest szyfrowane, następuje weryfikacja poświadczeń, oraz praw do obiektów (Feature Delegation).

Włączenie zdalnej administracji

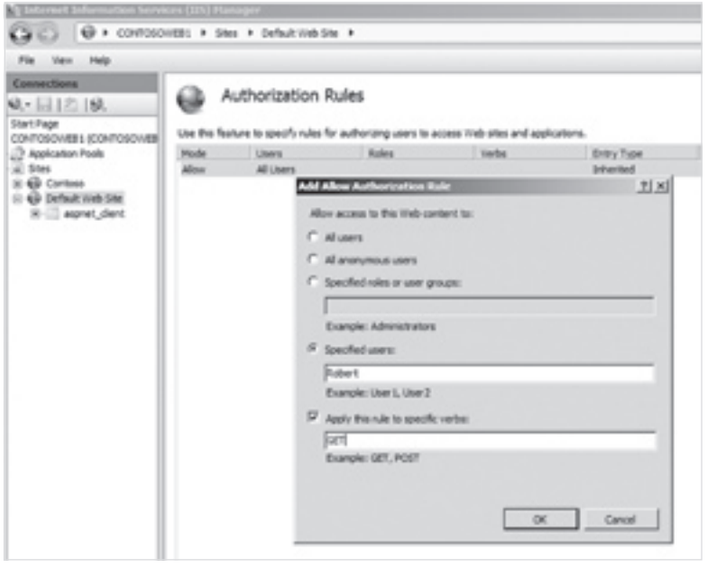
1. W celu włączenia zdalnej administracji za pomocą IIS Managera kliknij na serwerze webowym w sekcji **connections**, przejdź do srodkowej cześci (Feature View)
2. kliknij na ikonie **Management Service** Ustaw **Enable**, parametry dostępu – tylko konta windows lub konta Windows i lokalne IIS Serwera.
3. W polu **IP Adress Restriction** podaj opcjonalnie z jakich adresów IP będzie dostęp do serwera Webowego.



Rys 17. Zdalna administracja

Autoryzacja

W IIS 7.0 pojawiła sie nowa metoda autoryzacji pozwalająca na nadanie uprawnień dostępowych dla konkretnego komputera, grupy komputerów, domen itd. do sitów, aplikacji, folderów i plików na serwerze. Dla przykładu, mozemy mieć wewnętrzna strone webową, która zawiera treści dostepne dla pracowników danej firmy. Jeśli dodamy zawartośc, do której dostęp ma być ograniczony tylko do pracowników działu HR możemy dodać regułę autoryzacyjną weryfikującą przynależność do grupy HR. Ten model jest dosyc podobny do modelu ASP.NET z tą jednak różnicą, że wynik przetwarzania reguł nie zależy od ich kolejnosci, reguły deny jednak jak zawsze są przetwarzane jako pierwsze



Rys 18. Autoryzacja

Podsumowanie

Dzięki modularnośći została podniesiona wydajność i bezpieczenstwo aplikacji webowych. Plik konfiguracyjny xml umożliwia delegacje uprawnien, przenosność i zcentralizowaną administracje. Polepszony monitoring serwera, szczegółowe logowanie zdarzeń: FREB, RSCA pozwalają administratorom na zbieranie bardziej dokładnych danych na temat działania serwera IIS 7.0. Obsługa wielu technologi programistycznych .NET. PHP ułatwia proces tworzenia aplikacji webowych.

Comp Safe Support

7. Zarządzanie usługami systemu

Wstęp

Windows 2008 dostarcza nowych narzędzi do instalacji i zarządzania systemem, które oferują wydajniejszym administrację systemem i usługami. Na szczególną uwagę zasługuje nowo wprowadzona konsola Server Manager, jest to narzędzie, które z jednego miejsca daje administratorowi możliwość kontroli nad wszystkimi rolami serwera, a przede wszystkim stanowi centrum informacji i monitoringu stanu serwera i wszystkich obsługiwanych ról.

Nie jest to tylko narzędzie integrujące wiele konsol operacyjnych systemu Windows Server 2003, daje również możliwość sięgania do zaawansowanej konfiguracji z jednego centralnego miejsca.

Cechy konsoli, role oraz funkcje serwera

Konsola Server Manager to rozbudowana konsola MMC (Microsoft Management Console), która daje możliwość wykonywania wszystkich operacji związanych z administracją serwerem. Administrator może instalować i usuwać poszczególne role oraz usługi serwera oraz dokonywać rekonfiguracji już istniejących.

Server Manager pozwala ona przeglądać praktycznie wszystkie informacje dotyczące działania serwera i korzystać z dostępnych narzędzi służących do zarządzania tym działaniem. Efektywność pracy administratora zostaje zwiększona przez możliwość wykonywania z jednego centralnego miejsca następujących czynności:

- przeglądanie i modyfikacja konfiguracji zainstalowanych ról oraz funkcje serwera
- wykonywanie czynności administracyjnych związanych z bieżącym utrzymaniem serwera (na przykład: zatrzymywanie, uruchamianie usług, zarządzanie zasobami lokalnymi)
- wykonywanie czynności administracyjnych związanych z bieżącą obsługą ról i funkcji
- badanie stanu serwera, wykrywanie i identyfikowanie krytycznych zdarzeń, analiza i naprawa zaistniałych problemów

Przegląd konsoli Server Manager

Główne okno tego narzędzia administracyjnego:

- przedstawia zgrupowane informacje na temat zainstalowanych ról oraz funkcji

- daje dostęp do opcji diagnostycznych takich jak dziennik zdarzeń, menedżer urządzeń i monitor wydajności
- pozwala na konfigurację harmonogramu zadań, zapory systemowej, usług oraz kont lokalnych użytkowników i grup
- udostępnia narzędzia służące do zarządzania archiwizacją i odtwarzaniem systemu

Rys.1 Konsola Server Manager

Oprócz konsoli graficznej administrator ma możliwość automatyzacji wdrażania i zarządzania rolami poprzez aplikację ServerManagerCmd.exe. Podstawową funkcjonalnością tego narzędzia wiersza poleceń jest możliwość instalacji i usuwania ról i funkcji serwera zgodnie z parametrami zawartymi w przygotowanym pliku odpowiedzi (XML answer file).

Przykład użycia ServerManagerCmd.exe

Polecenie	Opis
ServerManagerCmd.exe –query	Zwraca informacje o zainstalowanych rolach i funkcjach
ServerManagerCmd.exe -install Web-Server -resultPath installResult.xml	Instaluje Serwer Internetowy (IIS) oraz przekazuje informacje wynikowe do wskazanego pliku
ServerManagerCmd.exe -inputPath install.xml –whatIf	Instalacja ról lub funkcji ze wskazanego pliku odpowiedzi wraz z wyświetlaniem informacji o postępie wykonywanych kroków
-restart	Dołączenie tego parametru do wywoływanego polecenia powoduje automatyczne ponowne uruchomienie serwera, jeśli będzie ono potrzebne po wykonanych operacjach

Role serwera Windows Server 2008

Konsola Server Manager dostarcza zbiór narzędzi i kreatorów ułatwiających dodawanie, usuwanie ról Sewera zarówno pojedynczych jak i wielu na raz w jednej sesji redukując tym samym czas poświęcony przez administratora na konfigurację serwera. Role definiują główne cele, do których może zostać przeznaczony serwer. W systemie Windows Serwer 2008 odnajdziemy następujące role:

Nazwa roli	Opis
Usługi certyfikacyjne AD (Active Directory Certificate Services)	Pozwalają na tworzenie i zarządzanie cyfrowymi certyfikatami przeznaczonymi dla użytkownika, komputera lub organizacji, jako części infrastruktury kluczy publicznych.
Usługi AD DS (Active Directory Domain Services)	Przechowują informacje o obiektach znajdujących się w zarządzanej sieci. Serwery pełniące funkcję kontrolerów domeny dają możliwość zarządzania procesami uwierzytelnienia i autoryzacji użytkownika podczas dostępu do zasobów sieciowych
Usługi AD FS (Active Directory Federation Services)	Dostarczają prosty mechanizm zarządzania tożsamościami i implementacji rozwiązania jednokrotnej rejestracji (single sign-on SSO) do zasobów Web.
Usługi AD LDS (Active Directory Lightweight Directory Services)	Dają możliwość magazynowania danych dla aplikacji wykorzystujących DS., nie wymaga jednocześnie posiadania kontrolerów domenowych w infrastrukturze sieciowej.
Usługi AD RMS (Active Directory Rights Management Services)	Dają możliwość zarządzania dostępem do poufnych informacji z poziomu aplikacji przystosowanych do współpracy z tymi usługami.

Serwer Aplikacyjny	Daje możliwość centralnej administracji aplikacjami biznesowymi działającymi w oparciu o na przykład.NET Framework 3.0.
Serwer DHCP	Centralne przydzielanie i zarządzanie adresami IP oraz konfiguracją protokołu TCP/IP.
Serwer DNS	Translacja nazw DNS na adresy IP. Wymagany przez usługi Active Directory Domain Services.
Serwer faksowania	Wysyłanie, odbieranie faksów. Zarządzanie zadaniami, raportami i konfiguracją urządzeń faksujących
Serwer plików	Daje możliwość zarządzania pamięcią masową, replikacją plików, szybkim wyszukiwaniem danych
Usługi kontroli dostępu przez sieć (Network Policy and Access Services)	Wspierają usługi routingu w sieciach LAN i WAN, pozwalają na tworzenie i wymuszanie zasad bezpiecznego dostępu do zasobów dla klientów zdalnego dostępu oraz VPN
Serwer wydruków	Pozwala na zarządzanie i określanie dostępu do drukarek sieciowych i ich sterowników
Serwer usług terminalowych	Dostarcza technologii pozwalających na zdalny dostęp do pulpitu serwera oraz aplikacji
Usługi UDDI (Universal Description, Discovery and Integration)	Pozwalają na zarządzanie udostępnionymi informacjami zarówno na potrzeby intranetu jak i partnerów biznesowych w oparciu o usługi Web
Serwer internetowy (IIS)	Pozwala na tworzenie niezawodnej, skalowalnej i w pełni zarządzanej infrastruktury aplikacji internetowych
Usługi WDS (Windows Deployment Services)	Instalacja systemów operacyjnych Windows na komputerach posiadających dostęp do sieci w sposób prosty, szybki i bezpieczny

Funkcje serwera Windows Server 2008

W przeciwieństwie do ról, funkcje serwera nie stanowią głównych zastosowań serwera, a są elementami wspierającymi realizację podstawowych zadań. Dzięki nim administratorzy mają możliwość wzbogacić funkcjonalność podstawowych ról serwerowych. Używając konsoli Server Manager można zarządzać następującymi funkcjami:

Nazwa funkcji	**Opis**
.NET Framework 3.0	Daje wsparcie dla nowych technologii pozwalających tworzyć aplikacje oferujące wydajny interfejs użytkownika, chroniących tożsamość i dane spersonalizowane, wspierające bezpieczną komunikację oraz procesy biznesowe
BitLocker Drive Encryption	Ochrona danych (szyfrowanie) na poziomie całego woluminu wspomagana sprzętowo
Background Intelligent Transfer Service (BITS) Server Extensions	Pozwala klientom na pobieranie i wysyłanie plików do serwera BITS. Rozszerzenie nie jest wymagane by klienci mogli pobierać dane.
Connection Manager Administration Kit	Tworzy profile połączeń zawierające uprzednio zdefiniowane ustawienia, które mogą zostać zastosowane na komputerach klienckich
Desktop Experience	Rozszerzenie o funkcje systemu Windows Vista, takie jak odtwarzacz Windows Media Player, motywy pulpitu, zarządzanie zdjęciami
Failover Clustering	Funkcja zwiększająca dostępność i niezawodność ról serwera oraz aplikacji takich jak serwer SQL, bazuje na współdzielonej przestrzeni dyskowej
Group Policy Management	Rozszerzenie oferujące efektywniejsze zarządzanie obiektami GPO w środowisku domenowym
Internet Printing Client	Pozwala klientom na wykorzystanie protokołu HTTP do podłączenia się do drukarek opublikowanych na serwerze wydruku Web
Internet Storage Naming Server (iSNS)	Przetwarzania rejestracji i wyrejestrowywania zgłoszeń oraz zapytań do urządzeń iSCSI
Line Printer Remote (LPR) Port Monitor	Pozwala na dostęp do drukarek obsługiwanych przez systemy UNIX
Message Queuing (MSMQ)	Pozwala na komunikowanie się aplikacji uruchomionych w systemach heterogenicznych, które również mogą czasowo znajdować się w trybie offline. MSMQ jest gwarantem dostarczenia wiadomości, prawidłowego ich routingu, bezpieczeństwa oraz uwzględniania nadanych priorytetów

Multipath I/O	Pozwala na wykorzystanie różnych dróg dostępu do pamięci masowych
Network Load Balancing	Rozpraszanie zapytań klienckich do grupy serwerów obsługujących odpytywaną aplikacje. Daje równoważenie obciążenia serwerów oraz zwiększa dostępność aplikacji
Peer Name Resolution Protocol	Pozwala aplikacjom na rejestrowanie i rozwiązywanie nazw komputerów komunikujących się z wykorzystaniem danej aplikacji
Quality Windows Audio Video Experience (qWave)	Platforma do strumieniowego przesyłania danych audio/wideo dla aplikacji w sieciach IP. Rozszerzenie gwarantujące zdefiniowaną wydajność w oparciu o quality-of-service (QOS)
Remote Assistance	Funkcja wspierająca diagnozę i rozwiązywanie problemów pojawiających się na komputerach zdalnych
Remote Differential Compression	Funkcja oferująca możliwość różnicowego transferu danych między obiektami w sieci w celu zmniejszenia wykorzystania sieci
Remote Server Administration Tools	Daje możliwość zdalnego zarządzania rolami i funkcjami na innych serwerach Windows Server 2008. Funkcja nie instaluje źródeł wybranych komponentów a jedynie narzędzia administracyjne
Removable Storage Manager	Katalogowanie, zarządzanie nośnikami wymiennymi oraz automatyzacja zarządzania napędami.
RPC over HTTP Proxy	Przesyłanie ruchu RPC generowanego przez aplikacje klienckie z wykorzystaniem protokołu HTTP. Alternatywa dla kanałów VPN
Simple TCP/IP Services	Usługi Simple TCP/IP
Simple Mail Transfer Protocol (SMTP) Server	Transfer poczty elektronicznej
SNMP Services	Zawiera usługi SNMP oraz dostawcę SNMP WMI
Storage Manager for Storage Area Networks (SANs)	Konfiguracja i obsługa sieci SAN zgodnych z VDS (Virtual Disk Services)

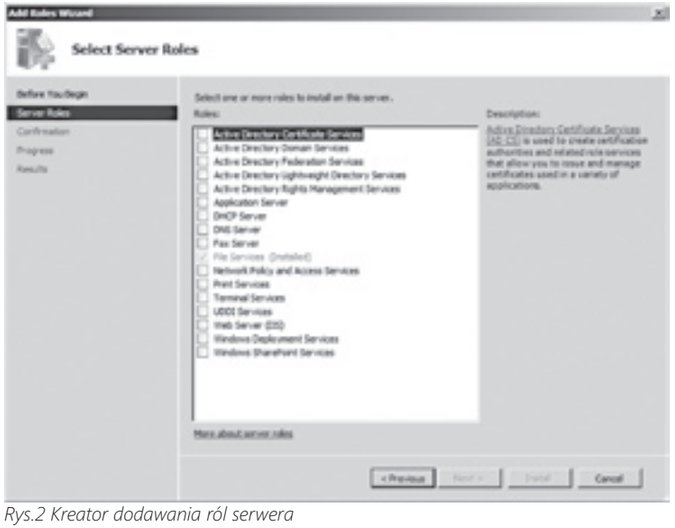
Subsystem for UNIX-based Applications (SUA)	Pozwala na uruchamianie aplikacji i pracę z wierszem poleceń systemu UNIX
Telnet Client	Pozwala na połączenie się i uruchamianie aplikacji na serwerze Telnet
Telnet Server	Zdalni klienci Telnet (w tym klienci UNIX) mogą administrować z poziomu wiersza poleceń oraz uruchamiać aplikacje na serwerze
Trivial File Transfer Protocol (TFTP) Client	Pozwala na transfer plików do i z serwera TFTP
Windows Internal Database	Używająca SQL Server 2005 Embedded Edition relacyjna baza danych, która przechowuje tylko informacje na temat ról i funkcji serwera.
Windows PowerShell	Powłoka wiersza poleceń i języka skryptowego wspierająca i zwiększająca produktywność profesjonalistów IT
Windows Process Activation Service (WPAS)	Daje wsparcie dla interfejsu programistycznego środowiska.NET
Windows Server Backup	Archiwizacja zasobów plikowych, systemu operacyjnego. Możliwość przywrócenia stanu z okresowo wykonywanych migawek
Windows Internet Name Service (WINS) Server	Translacja nazw NetBIOS w sieciach IP
Wireless Networking	Konfiguracja łączności i profili WLAN

Zarządzanie rolami i funkcjami z konsoli Server Manager

Kreator dodawania nowej roli serwera **Add Roles Wizard** (Rys.2) pozwala na dodawanie w tym samym momencie wielu ról.

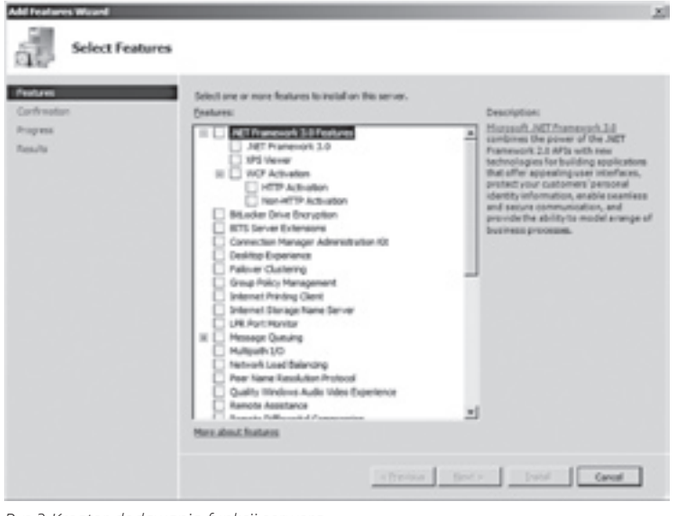
Większość ról jest instalowanych z domyślną konfiguracją, jedynie w przypadku niektórych, na przykład usługi AD FS (Active Directory Federation Services), czy też usługi certyfikacyjne AD (Active Directory Certificate Services) dostępne są kolejne kroki konfigurujące rolę lub pozwalające wybrać usługi, z których składają się komponenty danej roli.

Kreator na bieżąco analizuje również zależności i jeżeli wybrana rola wymaga funkcji serwera, które nie są jeszcze zainstalowane, wyświetlany jest odpowiedni monit dający możliwość ich instalacji.



Rys.2 Kreator dodawania ról serwera

Dodawanie nowych funkcji odbywa się z wykorzystaniem kreatora **Add Features Wizard** (Rys.3). Podobnie jak w przypadku ról, administrator ma możliwość w jednej sesji instalacji wszystkich wymaganych funkcji.



Rys.3 Kreator dodawania funkcji serwera

Również tutaj następuje bieżąca weryfikacja zależności, która wskazuje, jakie role/funkcja są wymagane po wybraniu funkcji serwera.

Usuwanie ról oraz funkcji serwera z konsoli Server Manager odbywa się z wykorzystaniem kreatorów **Remove Roles Wizard** oraz **Remove Roles Wizard**, które podobnie jak opisane wyżej pozwalają na zarządzanie wieloma rolami lub funkcjami w jednej sesji.

Po instalacji odpowiednich ról serwera, konsola Server Manager daje administratorowi doskonałe narzędzie pozwalające po wskazaniu odpowiedniego komponentu z jednego miejsca dostęp do: zdarzeń związanych z danym elementem, sekcja **Events**

- statusu zainstalowanych i powiązanych z rolą usług systemowych, sekcje **System Services** oraz **Role Services**
- możliwości instalacji **Add Role Services** lub usunięcia **Remove Role Services** poszczególnych usług powiązanych z daną rolą
- informacji o rekomendowanej konfiguracji wybranej roli oraz zadaniach i najlepszych praktykach z nią związanych, sekcja **Resources and Suport**

W przypadku niektórych ról z tego miejsca jest również dostęp do przystawek MMC pozwalających na zarządzanie i konfigurację danej roli, a także wszelkich komponentów z nią powiązanych.

Server Core – wstęp

Czym jest Server Core? Z pewnością nie jest to kolejna wersja systemu Windows Server 2008. Można powiedzieć, że jest to nowa opcja instalacyjna tego systemu. Dzięki niej mamy możliwość uruchomienia systemu operacyjnego zawierającego minimalne środowisko pozwalające na uruchomienie podstawowych (nie wszystkich) ról. Spośród wszystkich ról dostępnych w pełnej instalacji Windows Server 2008, Server Core oferuje wsparcie dla:

- Active Directory Domain Services
- Active Directory Lightweight Directory Services
- DHCP Server
- DNS Server
- File Services
- Print Services
- Windows Media Services

- Web Server (IIS)
- Typer-V (Virtualization)

Dodatkowo, administrator będzie ma możliwość skorzystania z następującej funkcji:

- Failover Clustering
- Network Load Balancing
- Subsystem for UNIX-based Applications (SUA)
- Windows Server Backup
- Multipath I/O
- Removable Storage Manager
- BitLocker Drive Encryption
- SNMP Services
- Windows Internet Name Service (WINS) Server
- Telnet client

Jaki jest cel i korzyści z posiadania takiego systemu? Podstawowe zalety to:

- Większa stabilność i dostępność systemu. Ograniczenie ilości ról jakie dostępne są w Server Core, zmniejsza ryzyko związane z nieprawidłową konfiguracją poszczególnych elementów, dzięki czemu bezpośrednio wpływa na stabilność systemu
- Mniejsze koszty i czas administracyjny związany z utrzymaniem serwera w porównaniu do pełnej instalacji Windows Server 2008
- Zwiększona odporność na ataki ze względu na mniejszą ilość dostępnych usług, które mogą stanowić potencjalne źródło ataku oraz brak możliwości uruchamiania aplikacji działających w interfejsie graficznym
- Zmniejszenie wymagań sprzętowych, mniejsza ilość danych instalowanych wraz z systemem operacyjnym

Przy podejmowaniu decyzji o wdrożeniu instalacji typu Server Core, należy wsiąść pod uwagę fakt, że nie może on stanowić podstawy dla warstwy aplikacyjnej. Jedyne aplikacje dostępne lokalnie i możliwe do uruchomienia w instalacji typu Server Coreto powłoka systemowa (CMD) oraz niektóre narzędzia administracyjne.

Pada więc pytanie, czy i jak można zarządzać instalacją Server Core?

Odpowiedzią jest możliwość użycia:

- Zdalnych narzędzi administracyjnych – ich zastosowanie nie wymaga dokładania żadnych dodatkowych komponentów po stronie instalacji Server Core, a jedynie komunikacji do zdalnego systemu przy użyciu odpowiednich protokołów sieciowych, np. RPC
- Lokalnych narzędzi administracyjnych – nie oferują żadnego interfejsu użytkownika w środowisku Server Core.

Instalacja i konfiguracja Server Core

Instalacja

Proces instalacji systemu Server Core przebiega podobnie do instalacji samego serwera Windows Server 2008, z tą różnicą że musi to być zawsze nowa instalacja.

Nie jest dopuszczalna aktualizacja z poprzednich oraz bieżącej wersji systemów operacyjnych do wersji Server Core. Również wersja Server Core nie może być aktualizowana do systemu Windows Server 2008.

Proces instalacji wersji Server Core przebiega podobnie do instalacji całego systemu Microsoft Windows Server 2008, jedynie na początku kreatora należy wskazać opcję instalacji **Server Core Installation** (rysunek poniżej). W dalszej części kreatora instalacji również administrator ma możliwość skonfigurowania wykorzystywanych przestrzeni dyskowych

Rys.4 Wybór instalacji Server Core

Lokalna konfiguracja Server Core

Ponieważ po procesie instalacji administrator nie ma do dyspozycji interfejsu graficznego, proces konfiguracji musi zostać przeprowadzony przy użyciu narzędzi dostępnych w wierszu poleceń. Pamiętać należy również o tym, że niektóre komendy konfiguracyjne uwzględniają wielkość liter. Restrykcje z brakiem interfejsu graficznego nie objęły jednakże wszystkich aplikacji, nadal możemy w trybie graficznym mieć dostęp do:

- Notepad.exe
- Timedate.cpl – graficzna regulacja czasu i stref czasowych
- Intl.cpl – graficzne zarządzanie ustawieniami językowymi i stroną kodową
- Taskmgr.exe

Poniżej zostały przedstawione podstawowe czynności administracyjne, które należy wykonać po instalacji systemu.

Ustawienie hasła administratora

1. W wierszu poleceń wprowadź,

   net user administrator *

2. Potwierdź przez klawisz **Enter.**

3. Następnie wprowadź nowe hasło dla konta administratora i ponownie potwierdź klawiszem **Enter.**

Przypisywanie stałego adresu IP oraz domyślnej bramy

Jeśli Server Core powinien posiadać skonfigurowany stały adres IP (po instalacji protokół TCP/IP korzysta z serwera DHCP), należy wykonać czynności wskazane poniżej.

1. W wierszu poleceń wprowadź

   netsh interface IPv4 show interface

2. Potwierdź przez klawisz **Enter**.

   Zostanie wówczas wyświetlona lista interfejsów sieciowych dostępnych w konfigurowanym systemie. Do dalszych czynności potrzebna jest wartość parametru **Idx** lub **Name** dla interfejsu, który chcemy skonfigurować. Jednakże prostszym w praktycznym wykorzystaniu będzie **Idx**, dlatego konfiguracja przedstawiona w dalszej części wykorzystuje właśnie ten parametr.

3. Po zapamiętaniu wartości **Idx** przechodzimy do konfiguracji IP. W wierszu poleceń wpisz.

   netsh interface IPv4 set address name = Idx source= static address = 192.168.1.101 mask = 255.255.255.0 gateway=192.168.1.1 gwmetric=1

   (gdzie Idx przy parametrze *name* jest wartością zapamiętaną w poprzednim kroku, a wprowadzony przykładowy statyczny adres IP to 192.168.1.101 z 24-bitową maską, dodatkowo została wskazana domyślna brama o adresie 192.168.1.1)

Weryfikację ustawień można przeprowadzić używając polecenia *ipconfig*.

Konfiguracja właściwości protokołu TCP/IP

Dodatkową konfiguracją protokołu TCP/IP, która może być wymagana na maszynie z Server Core jest wskazanie adresów IP serwera DNS, WINS. W takim przypadku można nadal posłużyć się przywoływanym już narzędziem *netsh*.

1. W wierszu poleceń wpisz.

   netsh interface IPv4 set dnsserver name = Idx source = static address = 192.168.1.100 register = primary

2. Potwierdzenie przez klawisz **Enter**.

   (w powyższym przykładzie został ustawiony adres IP serwera DNS na wartość 192.168.1.100 oraz włączona rejestracja nazwy host w oparciu tylko o podstawowy sufiks, podobnie jak wcześniej parametr **Idx** jest identyfikatorem konfigurowanego interfejsu sieciowego)

Inne czynności administracyjne

Opis czynności	Przykład
Zmiana nazwy serwera	NETDOM RENAMECOMPUTER *StaraNazwa* / NewName:*NowaNazwa* /UserO:Administrator /PasswordO:* W przykładzie zostaje zmieniona nazwa z wykorzystaniem konta lokalnego użytkownika Administrator
Dodanie do domeny	NETDOM JOIN *NazwaKopmutera* /Domain:*NazwaDomeny* / UserD:*UżytkownikDomenowy* /PasswordD:*
Aktywacja systemu operacyjnego	slmgr -ato
Włączenie automatycznej aktualizacji	Cscript %windir%\system32\scregedit.wsf /AU 4 (użycie parametru /AU 1 wyłącza automatyczną aktualizację)

Włączenie zdalnych połączeń terminalowych	Cscript %windir%\system32\scregedit.wsf /AR 0 (użycie parametru /AR 1 wyłącza dostęp terminalowy)
Dołożenie sterowników do systemu operacyjnego	Pnputil –i –a [lokalizacja oraz nazwa pliku INF]
Zarządzanie usługami	Polecenia NET START lub NET STOP Można też wykorzystać WMIC i kontekst aliasu SERVICE

Instalacja i usuwanie ról serwerowych

Ponieważ instalacja typu Server Core nie dostarcza interfejsu graficznego do zarządzania serwerem, również proces lokalnej instalacji oraz usuwania nowych ról lub funkcji wymaga użycia wiersza poleceń. Poniżej zostały przedstawione przykładowe polecenia zarządzające rolami. Należy pamiętać o uwzględnieniu dużych i małych znaków w nazwach instalowanych komponentów.

DNS

Jeśli chcesz zainstalować usługę DNS w wierszu poleceń wpisz:

Start /w ocsetup DNS-Server-Core-Role

Jeśli chcesz usunąć rolę DNS Server w wierszu poleceń wpisz:

Start /w ocsetup DNS-Server-Core-Role /uninstall

Zarządzanie usługą DNS możne przeprowadzić z konsoli lokalnej wykorzystując aplikację *dnscmd*.

Przykład konfiguracji stref DNS:

dnscmd /zoneadd test.local /dsprimary
dnscmd test.local /zoneadd secondtest. test.local /secondary 192.168.1.2
dnscmd /recordadd gateway A 192.168.1.1

DHCP

Jeśli chcesz dodać serwer DHCP w wierszu poleceń wpisz:

Start /w ocsetup DHCPServerCore

Polecenie

Start /w ocsetup DHCPServerCore /uninstall

usuwa rolę DHCP Server

Zarządzanie konfiguracją serwera DHCP może być również przeprowadzone z poziomu konsoli Server Core z wykorzystaniem polecenia netsh i kontekstu *dhcp*. Nie należy w tym miejscu zapomnieć o potrzebie autoryzacji serwera DHCP jeśli znajduje się on w środowisku domenowym.

Przykład konfiguracji zakresów DHCP:

netsh dhcp server 192.168.1.101 add scope 192.168.1 255.255.255.0 ZakresLokalny OpisZakresu

netsh dhcp server 192.168.1.101 add iprange 192.168.1.110 192.168.1.120

netsh dhcp server 192.168.1.101 scope 192.168.1.0 set state 1

Instalacja pozostałych ról

Serwer plików. Jest instalowany domyślnie, można jedynie wzbogacić jego funkcjonalność o następujące komponenty:

- File Replication Service:

  start /w ocsetup FRS-Infrastructure

- Distributed File System:

  start /w ocsetup DFSN-Server

- Distributed File System Replication:

  start /w ocsetup DFSR-Infrastructure-ServerEdition

- Network File System:

  start /w ocsetup ServerForNFS-Base

Media Services. Instalacja roli z wiersza poleceń poprzez wywołanie:

start /w ocsetup MediaServer

Po instalacji konfigurację należy przeprowadzić zdalnie z poziomu konsoli MMC

Serwer wydruków. Instalacja poprzez wiersz poleceń:

Start /w ocsetup Printing-ServerCoreRole

Active Directory Lightweight Directory Services.:

Start /w ocsetup DirectoryServices-ADAM-ServerCore

Serwer internetowy (IIS). Instalacja z domyślną konfiguracją, w wierszu poleceń wprowadzamy:

Start /w pkgmgr /iu:IIS-WebServerRole;WAS-WindowsActivationService;WAS-ProcessModel

Instalacja pozostałej funkcjonalności usług IIS wymaga wskazania pakietów poniżej znajduje się lista wszystkich opcji:

start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-HttpRedirect;IIS-ApplicationDevelopment;IIS-ASP;IIS-CGI;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-ServerSideIncludes;IIS-HealthAndDiagnostics;IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-HttpTracing;IIS-CustomLogging;IIS-ODBCLogging;IIS-Security;IIS-BasicAuthentication;IIS-WindowsAuthentication;IIS-DigestAuthentication;IIS-ClientCertificateMappingAuthentication;IIS-IISCertificateMappingAuthentication;IIS-URLAuthorization;IIS-RequestFiltering;IIS-IPSecurity;IIS-Performance;IIS-HttpCompressionStatic;IIS-HttpCompressionDynamic;IIS-WebServerManagementTools;IIS-ManagementScriptingTools;IIS-IIS6ManagementCompatibility;IIS-Metabase;IIS-WMICompatibility;IIS-LegacyScripts;IIS-FTPPublishingService;IIS-FTPServer;WAS-WindowsActivationService;WAS-ProcessModel

Active Directory Domain Services. Do instalacji tych usług wykorzystać należy polecenie dcpromo. Ponieważ aplikacja ta nie może zostać uruchomiona z jej interfejsem graficznym, należy wcześniej przygotować odpowiedni plik odpowiedzi, a następnie w wierszu poleceń wykonać:

Dcpromo /unattend:PlikOdpowiedzi

Do poprawnego działania usług Active Directory Domain Services będzie potrzebne ponowne uruchomieni serwera. Zarządzać bazą domenową można również z konsoli lokalnej systemu Server Core z wykorzystaniem aplikacji
Dsadd – dodaje obiekty do bazy
Dsget – daje możliwość wyświetlenia właściwości wskazanego obiektu
Dsmod – modyfikacja parametrów obiektu
Dsmove – przeniesienie obiektu do innej lokalizacji
Dsquery – wyszukuje obiekty spełniające wskazane kryteria
Dsrm – służy do usuwania obiektów z bazy
Ldifde lub Csvde – eksport/import danych
Oczywiście dostępna jest również aplikacja ntdsutil.exe

Instalacja funkcji serwera

Podobnie jak w przypadku ról wykorzystujemy aplikację *ocsetup*. Poniżej zostały przedstawione parametry, których należy użyć w wierszu poleceń w celu zainstalowania wybranej funkcji:

Funkcjonalność	**Nazwa funkcji wprowadzana przy wywołaniu ocsetup**
Backup	WindowServerBackup
BitLocker Drive Encryption	BitLocker
Failover Cluster	FailoverCluster-Core
Multipath IO	Microsoft-Windows-Multipathio
Network Load Balancing	NetworkLoadBalancingHeadlessServer
Removable Storage Management	Microsoft-Windows-RemovableStorageManagementCore
Simple Network Management Protocol (SNMP)	SNMP-SC
Subsystem for UNIX-based applications	SUACore
Telnet Klient	TelnetClient
Windows Internet Naming Service (WINS)	WINS-SC

Zdalna administracja systemem Server Core

Ponieważ instalacja typu Server Core wymaga wstępnej konfiguracji z wykorzystaniem wiersza poleceń i nie daje możliwości wykorzystania standardowych narzędzi graficznych, dużym ułatwieniem w administracji takim systemem jest możliwość zdalnej administracji.
W tym celu możemy posłużyć się następującymi rozwiązaniami:

Zdalny dostęp przez Usługi Terminalowe. Oczywiście zdalna konsola nie pozwoli nam na używanie aplikacji graficznych, administracja systemem będzie nadal polegała na wykorzystaniu wiersza poleceń. By można było terminalowo łączyć się z systemem Server Core należy w pierwszej kolejności zezwolić na połączenia zdalne w wierszu poleceń wpisz:

Cscript %windir%\system32\scregedit.wsf /AR 0

Dobrym rozwiązaniem jest również publikacja poprzez usługi terminalowe aplikacji **cmd.exe** poprzez Terminal Services Remote Programs.

Wykorzystanie Windows Remote Shell. Podobnie jak w poprzednim przypadku mamy dostęp tylko do aplikacji działających w wierszu poleceń.

1. Włączenie Remote Shell wymaga z konsoli Server Core wykonania polecenia:

   Winrm quickconfig

2. Następnie z maszyny zdalnej możemy wykonać czynności administracyjne z użyciem następującej składni:

   Winrs –r:ZdalnyServer [polecenie, które chcemy wykonać na zdalnym serwerze]

Wykorzystanie zdalnej administracji w oparciu o konsolę MMC. System z którego chcemy zarządzać Server Core musi posiadać zarejestrowane odpowiednie przystawki do konsoli MMC, które dadzą możliwość zdalnej administracji poszczególnymi rolami, funkcjami czy właściwościami serwera. Można się w tym celu posłużyć dostępną funkcją **Remote Server Administration Tools** i z niej wybrać wszystkie niezbędne konsole administracyjne. W przypadku gdybyśmy chcieli zdalnie zarządzać podsystemem dyskowym, należy wcześniej na systemie Server Core uruchomić usługę vds (Virtual Disk), można to wykonać z wiersza poleceń na przykład przez

Net start vds

Należy w tym przypadku pamiętać o tym, że nie wszystkie czynności można wykonać poprzez zdalną administrację przystawkami konsoli MMC. Przykładem może tu być włączenie/wyłączenie automatycznej aktualizacji lub usług zdalnego dostępu.

Zarządzanie poprzez aplikacje wiersza poleceń dające możliwość zdalnej konfiguracji systemów. Ostatnim ze sposobów na zdalną administrację systemem Server Core jest wykorzystanie aplikacji wiersza poleceń, które oferują poprzez parametryzację możliwość zarządzania systemami zdalnymi. Przykładem może tu być aplikacja *netdom*.

Windows PowerShell – wstęp

Windows PowerShell jest nową powłoką systemu operacyjnego, która daje możliwość obsługi wiersza poleceń i nowego języków skryptów. Ma za zadanie wspomóc pracę administracyjną poprzez automatyzację obsługi systemu operacyjnego. Udostępnia zestaw narzędzi oferujących spójną składnie i pozwalających efektywniej, szybciej i wydajniej zarządzać takimi danymi jak rejestr, Windows Management Instrumentation (WMI), usługami np. Active Directory.

Niewątpliwą zaletą powłoki PowerShell jest możliwość obsługi istniejących skryptów VBScript (*.vbs), batch file (*.bat) czy też perl. Dzięki temu w organizacji nie ma potrzeby wykonywania migracji istniejących rozwiązań skryptowych, a w oparciu o nową powłokę i jej funkcjonalność wykorzystywanie istniejących rozwiązań i rozwijanie o nową funkcjonalność.

Czym jest PowerShell Cmdlet?

Administratorzy wykorzystując PowerShell w dalszym ciągu mają możliwość używania standardowych aplikacji i poleceń interpretera CMD.exe. Jednakże nowa powłoka oferuje wbudowany zbiór poleceń zwanych cmdlet („command-let"). Ich przeznaczeniem jest ułatwienie pracy administracyjnej, poprzez wykorzystywanie programów wbudowanych w powłokę pozwalających na wykonywanie skomplikowanych zadań. Dzięki nim administrator ma możliwość pracy z powłoką bez znajomości języka skryptowego PowerShell. Polecenia te w większości bazują na standardowej konwencji nazewniczej *czasownik-rzeczownik* gdzie czasownik określa czynność jaka ma zostać wykonana na obiekcie wskazanym przez rzeczownik, na przykład:

Get-Help, polecenie get pozwala na wyświetlenie informacji o obiekcie wskazanym po prawej stronie myślnika, w przykładzie wyświetlenie pomocy,

Start-Service polecenie start pozwala na uruchomienie obiektu występującego po prawej stronie myślnika, w tym przykładzie uruchomienie usługi.

Użycie PowerShell w administracji

Podstawowymi założeniami Windows PowerShell są dostarczenie lepszych, łatwiejszych w użyciu narzędzi administracyjnych pozwalających na pełną kontrolę systemów w trybie interaktywnym lub też przy wykorzystaniu skryptów. Administracja z wykorzystaniem powłoki PowerShell pozwala na

- Zarządzanie procesami lokalnymi. Poprzez dwa polecenia Get-Process i Stop-Process administrator ma możliwość wykonywania skomplikowanych czynności związanych z monitorowaniem i zarządzaniem uruchamianymi procesami.
- Zarządzanie usługami lokalnymi. Polecenia cmdlet przeznaczone do administracji usługami to: Get-Service, Resume-Service, Start-Service, Stop-Service, Restart-Service, Suspend-Service, Set-Service, New-Service
- Zbieranie informacji o konfiguracji maszyny. Cmdlet Get-WmiObject jest bardzo ważnym poleceniem, które umożliwia efektywne zarządzanie systemem. Wszystkie krytyczne podsystemy i komponenty posiadają swoją reprezentację w repozytorium WMI. Dodatkowo WMI gromadzi informacje dotyczące tych obiektów a powłoka PowerShell pozwala pracować z tymi obiektami, przeglądać przechowywane wartości pojedynczych lub wielu obiektów w tym samym czasie, co pozwala na uproszczenie wielu zaawansowanych czynności administracyjnych
- Pracę z Software Installation. Ponieważ nie wszystkie aplikacje wykorzystują w procesie instalacji usługę Windows Installer, Windows PowerShell może być elementem wspierającym zautomatyzowaną instalację oprogramowania w przypadkach kiedy prawidłowe przeprowadzenie procesu instalacji wymaga manipulowania zasobami typu pliki, foldery czy klucze rejestrowe

- Zmianę stanu systemu. Cmdlet Get-WmiObject pozwala na zmianę stanu systemu poprzez klasę Win32_OperatingSystem reprezentującą system operacyjny. Użycie metody Win32Shutdown z odpowiednim parametrem daje możliwość

Wartość parametru	Opis działania
0	Wylogowanie
4	Wymuszone wylogowanie
1	Zamknięcie systemu (Shutdown)
5	Wymuszone zamknięcie systemu (Shutdown)
2	Ponowne uruchomienie systemu
6	Wymuszone ponowne uruchomienie systemu
8	Zamknięcie systemu (Power Off)
12	Wymuszone zamknięcie systemu (Power Off)

```
PS C:\> (Get-WmiObject Win32_OperatingSystem).Win32Shutdown(0)
```

Administrator ma również możliwość zarządzania systemami zdalnymi, na przykład poprzez wykonanie następującego polecenia

```
PS C:\ > (Get-WmiObject Win32_OperatingSystem –ComputerName SERWER1).
Win32Shutdown(0)

__GENUS                 : 2
__CLASS                 : __PARAMETERS
__SUPERCLASS            :
__DYNASTY               : __PARAMETERS
__RELPATH               :
__PROPERTY_COUNT        : 1
__DERIVATION            : {}
__SERVER                :
__NAMESPACE             :
__PATH                  :
ReturnValue             : 0
```


- Wykonywanie czynności związanych z konfiguracją sieci. Podobnie jak w przypadku zmiany stanu systemu, dzięki repozytorium WMI, powłoka PowerShell umożliwia konfigurację interfejsów sieciowych, Klasą, która jest wykorzystywana w tym przypadku jest Win32_NetworkAdapterConfiguration.
  Pracę z katalogami i plikami. Podstawowa codzienna praca wymaga również wykonywania operacji na systemie plików, PowerShell udostępnia odpowiednie polecenia umożliwiające taką pracę. Przykładem mogą tu być cmdlet Set-Location, który jest odpowiednikiem polecenia CD, czy też Get-ChildItem, odpowiednik polecenia DIR. Oprócz tego administrator może wykorzystać w codziennej pracy następujące polecenia

Polecenie	Opis
New-Item	tworzy nowe elementy
Remove-Item	usuwa istniejące elementy
Copy-Item	kopiuje elementy
Move-Item	przenosi elementy
Rename-Item	zmienia nazwę elementów
Invoke-Item	uruchamia program lub otwiera plik przy pomocy skojarzonego program

- Pracę z rejestrem. Powłoka PowerShell pozwala na operacje w rejestrze z wykorzystaniem poleceń używanych w pracy z systemem plików. Dzięki temu praca z zawartością rejestru jest zbliżona do pracy z systemem plików.

Instalacja Windows PowerShell

W systemie operacyjnym Microsoft Windows Server 2008 powłoka PowerShell jest dostępna jako jedna z funkcji. Windows PowerShell może zostać również zainstalowany na starszych systemach operacyjnych, na przykład Windows XP z SP2, Windows Server 2003 z SP1 czy też Windows Vista, pod warunkiem, że na tych systemach również znajdzie się Microsoft .NET Framework 2.0, który jest wymagany do poprawnego działania powłoki.

Po instalacji, powłokę możemy uruchomić wykorzystując skrót dostępny w menu **Start | Programs | Windows PowerShell** lub poprzez uruchomienie z menu **Run** polecenia *PowerShell*.

Użycie poleceń interpretera CMD

Podobnie jak w standardowym interpreterze CMD mamy możliwość poruszania się po strukturze dysku oraz uruchamiania jego poleceń.

1. Uruchom PowerShell.
2. Po uruchomieniu powłoki zostanie wyświetlony znak zachęty, który domyślnie znajduje się w katalogu Users zalogowanego użytkownika.

   PS C:\Users\Administrator>

3. Zmień katalog wprowadzając polecenie

   PS C:\Users\Administrator> cd c:

4. Wyświetl zawartość katalogu

   PS C:\> dir

5. Wpisz polecenie ipconfig/all wysyłając wynik do pliku tekstowego

   PS C:\> ipconfig /all > wynik.txt

6. Przejrzyj wynik używając Notatnika

   PS C:\> notepad wynik.txt

Jednakże PowerShell oferuje możliwość uruchamiania poleceń wieloskładnikowych w jednym wierszu. Poszczególne polecenia są rozdzielane średnikiem. Kroki opisane powyżej mogą zostać wobec tego wywołane w następujący sposób.

1. Uruchom PowerShell
2. Wykonaj polecenie wieloskładnikowe

   PS C:\Users\Administrator> ipconfig /all > wynik.txt; notepad wynik.txt

3. Wykonaj polecenie wieloskładnikowe, które do istniejącego pliku zawierającego wynik polecenia ipconfig/all dołącz do wyniuk działania polecenia router print, wykorzystaj do tego znak przekserowania i dołączenia (>>).

   PS C:\Users\Administrator> ipconfig /all >nowy_wynik.txt; route print >> nowy_wynik.txt; notepad nowy_wynik.txt

Zarządzanie usługami

W przypadku administracji usługami serwera powłoka PowerShell oferuje zestaw cmdlet, które pozwalają przeglądać istniejące usługi oraz zarządzać ich właściwościami.

Na początku wyświetl listę dostępnych poleceń związanych z usługami systemowymi (obiekt service).

1. Uruchom PowerShell
2. Wykonaj polecenie

   PS C:\> Get-Command *-service

CommandType	Name	Definition
-----------	----	----------
Cmdlet	Get-Service	Get-Service [[-Name] <String..
Cmdlet	New-Service	New-Service [-Name] <String>..
Cmdlet	Restart-Service	Restart-Service [-Name] <Str..
Cmdlet	Resume-Service	Resume-Service [-Name] <Stri..
Cmdlet	Set-Service	Set-Service [-Name] <String>..
Cmdlet	Start-Service	Start-Service [-Name] <Strin..
Cmdlet	Stop-Service	Stop-Service [-Name] <String..
Cmdlet	Suspend-Service	Suspend-Service [-Name] <Str..

   Wykonanie powyższego polecenia pokazało wszystkie operacje jakie mogą zostać wykonane na usługach.

3. Jeżeli potrzebujesz pomocy dotyczącej jakiegoś polecenia możesz użyć następującej składni.

   PS C:\> get-help get-service

   Alternatywą może być użycie polecenia

   PS C:\> get-service -?

   NAME

   Get-Service

   SYNOPSIS

   Gets the services on the local computer.

   SYNTAX

   Get-Service [[-name] <string[]>] [-include <string[]>] [-exclude <string[]>] [<CommonParameters>]

4. Do wyświetlenia listy dostępnych usług wybierz polecenie.

```
PS C:\> get-service

Status     Name               DisplayName
------     ----               -----------
Running    AeLookupSvc        Application Experience
Stopped    ALG                Application Layer Gateway Service
Stopped    Appinfo            Application Information
Stopped    AppMgmt            Application Management
Running    AudioEndpointBu...  Windows Audio Endpoint Builder
Running    AudioSrv           Windows Audio
Running    BFE                Base Filtering Engine
Running    BITS               Background Intelligent Transfer Ser...
Stopped    Browser            Computer Browser
Stopped    CertPropSvc        Certificate Propagation...
```

Powyższe polecenie zwróciło listę usług oraz pewne ich właściwości. Jeżeli ilość zwracanych informacji jest zbyt mała potrzebujesz informacji o tym jakie inne właściwości są przypisane do danego obiektu.

5. Użyj komendy get-member do zwrócenia informacji o metodach i właściwościach dostępnych dla usług systemowych.

```
PS C:\> get-service | Get-Member

   TypeName: System.ServiceProcess.ServiceController

Name                MemberType     Definition
----                ----------     ----------
Name                AliasProperty  Name = ServiceName
add_Disposed        Method         System.Void add_Disposed(EventHandle...
Close               Method         System.Void Close()
Continue            Method         System.Void Continue()
CreateObjRef        Method         System.Runtime.Remoting.ObjRef Creat...
Dispose             Method         System.Void Dispose()
Equals              Method         System.Boolean Equals(Object obj)
ExecuteCommand      Method         System.Void ExecuteCommand(Int32 com...
GetHashCode         Method         System.Int32 GetHashCode()
GetLifetimeService  Method         System.Object GetLifetimeService()
GetType             Method         System.Type GetType()
```

Powyższy przykład używa znaku przekazującego strumienie danych (|) pozwalającego na łączenie wielu komend poprzez przekazanie danych z komendy poprzedniej do następnej.

6. Jeśli chcesz zawęzić listę otrzymywanych informacji tylko do właściwości związanych z usługami wykonaj polecenie.

```
PS C:\> get-service | Get-Member -MemberType property

   TypeName: System.ServiceProcess.ServiceController

Name                  MemberType  Definition
----                  ----------  ----------
CanPauseAndContinue   Property    System.Boolean CanPauseAndContinue
                                  {get;}
CanShutdown           Property    System.Boolean CanShutdown {get;}
CanStop               Property    System.Boolean CanStop {get;}
Container             Property    System.ComponentModel.IContainer...
DependentServices     Property    System.ServiceProcess.ServiceControl...
DisplayName           Property    System.String DisplayName {get;set;}
MachineName           Property    System.String MachineName {get;set;}
ServiceHandle         Property    System.Runtime.InteropServices.Safe...
ServiceName           Property    System.String ServiceName {get;set;}
..
```

Dodatkowo w zwracanym wyniku dostajemy informację o tym czy dana właściwość może być czytana i modyfikowana {get;set;} w polu Definition

7. Jeżeli chcesz zmienić sposób prezentacji wyników wykonaj następujące polecenie.

PS C:\> Get-Service | Sort-Object Status, ServiceName | Format-List ServiceName, Status, ServicesDependedOn

ServiceName : ALG

Status : Stopped

ServicesDependedOn : {}

ServiceName : Appinfo

Status : Stopped

ServicesDependedOn : {RpcSs, ProfSvc}

ServiceName : AppMgmt

Status : Stopped

ServicesDependedOn : {}

...

ServiceName : AeLookupSvc

Status : Running

ServicesDependedOn : {}

ServiceName : BFE

Status : Running

ServicesDependedOn : {RpcSs}

Przykład używa cmdlet Sort-Object do wskazania porządku sortowania zwracanych wyników (w przykładzie pierwszą grupę sortowania stanowi właściwość Status, drugą ServiceName, dodatkowo prezentacja danych została ułożona w formacie listy i zwracane są pola ServiceName, Status oraz ServicesDependedOn w wymienionej kolejności

Powłoka PowerShell daje również możliwość ustawiania parametrów usług, takich jak sposób uruchomienia. Także zatrzymanie, uruchomienie, wstrzymanie oraz wznowienie działania usług możesz wykonać z poziomu powłoki poprzez polecenia cmdlet

1. Uruchom PowerShell
2. Zmień sposób uruchomienia usługi Windows Audio Endpoint Builder wykonując następujące polecenie.

   PS C:\> $usluga = get-service -displayname „Windows Audio End*"

   PS C:\> $usluga.Name

   PS C:\> Set-Service –name $usluga.Name –description "Nowy opis uslugi" –StartupType Automatic

   W powyższym przykładzie użyto zmiennej, do której została przypisana modyfikowana usluga, następnie korzystając z właściwości (Name) zmieniono opis i spsoć uruchamiania danej uslugi.

3. Korzystając z przypisania uslugi do zmiennej możemy również używać dostępnych metod danego obiektu. W przypadku usług są to na przykład Stop(), Start(), Pause(), Continue().

   PS C:\> $service.Start()

   Jeśli w konsoli nie zostanie zwrócony błąd, polecenie zostało wykonane poprawnie. W przypadku na przykład próby ponownego uruchomienia już działającej usługi dostaniemy błąd.

   Exception calling „Stop" with „0" argument(s): „Cannot stop AudioEndpointBuilder '.'."

   At line:1 char:13

   + $usluga.Stop(<<<<)

4. Należy w tym miejscu zaznaczyć, ze nie każda usluga daje możliwość wstrzymania działania (Pause/Continue). Jeśli chcesz zobaczyć właściwość wskazującą czy usluga daje taka możliwość, wykonaj następujące polecenie.

   PS C:\> $usluga.CanPauseAndContinue

   False

Zarządzanie procesami

Powłoka PowerShell daje również możliwość zarządzania lokalnymi procesami. Masz dostęp do takich poleceń cmdlet jak **Get-Process** oraz **Stop-Process**. Polecenia te mogą posłużyć również do monitorowania stanu i aktywności procesów w lokalnym systemie.

1. Uruchom PowerShell
2. Uruchom nowy proces Notepad.exe wprowadzając następujące polecenie.

   PS C:\> notepad

3. Wyświetl uruchomione procesy

   PS C:\> Get-Process

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
82	6	3584	6760	65	0.42	3068	cmd
...							
171	15	4172	8600	81	0.08	2540	msdtc
49	5	2056	5204	63	0.38	2256	notepad

4. Opis zwracanych informacji znajdziesz w pomocy szczegółowej dla polecenia Get-Process, wykonując poniższe polecenie.

   Get-Help Get-Process –Full > c:\process.txt

5. Wyświetl stan procesu Notepad.exe poprzez polecenie.

   PS C:\> Get-Process -name notep*

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
49	5	2056	5204	63	0.38	2256	notepad

6. Jeśli chcesz zobaczyć procesy, które wykorzystują więcej niż 50MB RAM, wykonaj polecenie

   PS C:\> get-process | where-object {$_.WorkingSet -gt 50000000}

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
628	41	175228	135312	692	68.00	956	mmc
511	24	76224	76032	580	22.75	2104	powershell

W przykładzie została dodatkowo wykorzystana komenda where-object, która pozwala na filtrowanie obiektów i wykonywanie na nich dostępnych operacji. Założony filtr sprawdza czy właściwość WorkingSet jest większa od 50 000 000 bajtów. Został tu również użyty operator porównawczy, poniżej znajduje się zestawienie dostępnych operatorów.

Operator	Opis
eq	Równy
ne	Różny
gt -ge	większy, większy lub równy
lt –le	mniejszy, mniejszy lub równy

7. Jeśli chcesz zatrzymać wybrany proces, możesz do tego użyć następującej składni.

   PS C:\> Stop-Process –id 49

8. Jeśli chcesz zatrzymać wszystkie procesy realizowane przez na przykład program Notepad użyj następującej składni.

   PS C:\> Stop-Process –name notepad

9. Jeśli chcesz zatrzymać procesy wykorzystujące na przykład więcej niż 50MB RAM wykonaj polecenia

   PS C:\> $procesy = get-process | where-object {$_.WorkingSet -gt 50000000}

   PS C:\> Stop-Porcess –InputObject $procesy

   W przykładzie została wykorzystana zmienna $procesy, która gromadzi listę procesów spełniających określone kryteria.

10. Jeśli chcesz zatrzymać procesy o konkretnych nazwach wykonaj następujące polecenia

    PS C:\> $lista = Get-Process -name notepad, iex*

    PS C:\> Stop-Process -InputObject $lista

    W przykładzie zostają zatrzymane wszystkie procesy notepad oraz te, których nazwy rozpoczynają się na „iex"

Kontrolowanie wykonywanych poleceń

Ponieważ powłoka PowerShell oferuje olbrzymie możliwości konfiguracji i zarządzania systemem, bardzo istotnym wydaje się możliwość kontrolowania procesu wykonywanych poleceń.
Do dyspozycji są dwa argumenty –whatIf, –confirm oraz suspend

-whatIf
Argument ten użyty w wykonywanym poleceniu powoduje zwrócenie informacji o tym jak zadziała wywołane polecenie przed jego rzeczywistym wykonywaniem.

-confirm
Argument ten powoduje, ze wybrane polecenie wymaga potwierdzenia przed wykonaniem

Suspend
Powoduje wstrzymanie działania polecenia, które zostało wywołane i oczekuje na potwierdzenie. Dzięki temu mamy możliwość wykonania innych poleceń, które na przykład są wymagane do poprawnego wykonania polecenia wstrzymanego, a których zapomnieliśmy wykonać wcześniej.

1. Uruchom PowerShell
2. Uruchom notepad

   PS C:\> notepad

3. Sprawdź czy proces notepad jest uruchomiony

   PS C:\> Get-Process -name notepad

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
49	5	2056	5204	63	0.38	3592	notepad

4. Wykonaj polecenie zatrzymujące proces notepad z argumentem -whatIf

   PS C:\> Stop-Process -name notepad -whatIf

   What if: Performing operation „Stop-Process" on Target „notepad (3592)".

5. Ponownie sprawdź czy proces notepad jest uruchomiony. Proces działa dalej mimo wywołania cmdlet Stop-Process w poprzednim punkcie.
6. Uruchom kolejny proces notepad

   PS C:\> notepad

7. Sprawdź listę procesów notepad

   PS C:\> Get-Process -name notepad

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
49	5	2056	5204	62	0.20	2496	notepad
54	5	2272	5712	63	0.38	3592	notepad

8. Wykonaj polecenie zatrzymujące proces notepad z argumentem –confirm

   PS C:\> Stop-Process -name notepad –confirm

9. Pojawi się wówczas następująca informacja

   Confirm

   Are you sure you want to perform this action?

   Performing operation „Stop-Process" on Target „notepad (2496)".

   [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is „Y"):

10. Wpisz "y" i naciśnij ENTER, proces zostanie zatrzymany i ponownie pojawi się komunikat

    Confirm

    Are you sure you want to perform this action?

    Performing operation „Stop-Process" on Target „notepad (3592)".

    [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is „Y")

11. Tym razem wpisz „s" i naciśnij ponownie ENTER. Polecenie zostanie wstrzymane, a w znaku zachęty pojawi się potrojona strzałka.

    PS C:\>>>

12. Uruchom kolejny proces notepad i wyświetl listę działających procesów notepad.

PS C:\>>> notepad

PS C:\>>> get-process -name notepad

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
51	5	1648	4308	62	0.03	1792	notepad
54	5	2272	5712	63	0.38	3592	notepad

W ten sposób zawiesiłeś działanie polecenia Stop-Process i masz możliwość wykonywania dodatkowych niezbędnych czynności w trakcie działania tego polecenia

13. Wpisz exit i naciśnij ENTER by wrócić do głównego polecenia. Ponownie zobaczysz komunikat główny potwierdzenia zatrzymania procesu notepad.

PS C:\>>> exit

Confirm

Are you sure you want to perform this action?

Performing operation „Stop-Process" on Target „notepad (3592)".

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is „Y"):

14. Wpisz "y" i naciśnij ENTER. Następnie wyświetl listę procesów notepad.

PS C:\> get-process -name notepad

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
51	5	1648	4308	62	0.03	1792	notepad

Zwróć uwagę, ze proces, który został uruchomiony podczas wstrzymanego polecenia Stop-Process działa nadal.

COMBIDATA
GRUPA PROKOM

8. Wysoka dostępność

Wprowadzenie

Zachowanie ciągłości procesów biznesowych wymaga stosowania rozwiązań oferujących wysoką dostępność aplikacji i usług, na przykład klastra niezawodnościowego. Niestety, dotychczas było to rozwiązanie skomplikowane, wymagające wysokich nakładów przy wdrażaniu i wyspecjalizowanej kadry do obsługi. Ponadto nie istniała możliwość łatwego tworzenia klastrów rozproszonych geograficznie.

Udoskonalenia wprowadzone w wersji klastra niezawodnościowego dla systemu operacyjnego Windows Server 2008 z powodzeniem eliminują większość problemów związanych z wcześniejszymi wersjami. Jednocześnie znacznie upraszczają procedury związane z instalacją i zarządzaniem klastrem.

Poniższy rozdział przedstawia zmiany wprowadzone do klastra niezawodnościowego w systemie Windows Server 2008 oraz cechy, dzięki którym powinno to być rozwiązanie nadające się do zainstalowania także w małych i średnich przedsiębiorstwach, wymagających zapewnienia ciągłości procesów biznesowych.

Taki stan rzeczy został osiągnięty między innymi dzięki:

- Usprawnieniom procesu instalacji klastra i migracji danych.
- Usprawnieniom w zarządzaniu klastrami.
- Usprawnieniom w zarządzaniu i konfiguracji pamięci masowych.
- Usprawnieniom dotyczącym bezpieczeństwa danych.
- Usprawnieniom w obsłudze sieci.

Klastry niezawodnościowe

Wstęp

Funkcja klastra niezawodnościowego w Windows Server 2008 została ulepszona pod kątem łatwości użytkowania, stabilności i bezpieczeństwa.

Klaster jest to grupa wielu komputerów działających jak jeden system w celu zwiększenia redundancji i dostępności. Komputery będące częścią klastra nazywane są węzłami (nodes).

Korzystanie z klastrów niezawodnościowego pozwala organizacjom używać wysoce dostępnych rozwiązań w celu dotrzymania zobowiązań wynikających z gwarancji jakości świadczonych usług (SLA) dla serwera i ciągłości działania aplikacji.

Aplikacjami, które najlepiej nadają się do skonfigurowania w klastrze niezawodnościowym są te, które używają scentralizowanych zbiorów danych. Aplikacje, takie jak SQL Server, Exchange Server i usługi, takie jak DHCP, plik i drukowanie oraz WINS korzystają ze scentralizowanych zbiorów danych i dlatego nadają się idealnie do konfigurowania do pracy w klastrze niezawodnościowym. Skonfigurowanie tych aplikacji i usług w klastrze pozwala zapewnić ich wysoką dostępność dla użytkowników.

Małe i średnie firmy często unikają tworzenia klastrów niezawodnościowych , ponieważ jest to uważane za trudną i wymagającą technologię. Wypuszczenie na rynek Windows Server 2008 ułatwi wdrażanie klastrów niezawodnościowych przedsiębiorstwom różnych rozmiarów.

Korzyści ze stosowania klastrów niezawodnościowych

Korzystanie z klastrów niezawodnościowych zapewnia kilka korzyści dotyczących serwera oraz rozmieszczeń aplikacji, włączając:

- Redukcję okresu przestoju w wypadku awarii serwera.
- Redukcję okresu przestoju w wypadku awarii systemu operacyjnego.
- Redukcję okresu przestoju podczas planowanych konserwacji serwera.

Firmy, które muszą spełniać warunki wynikające z gwarancji jakości świadczonych usług lub prowadzić aplikacje kluczowe dla codziennych interesów korzystają z klastrów, aby osiągnąć wymaganą sprawność serwera. Wartość tej sprawności jest często opisywana liczbą dziewiątek. Nie są rzadkością firmy dążące do pięciu dziewiątek sprawności (99,999%), co oznacza mniej niż 10 minut przestoju serwera w ciągu roku.

Aplikacje i usługi w klastrze mogą być przedmiotem trzech różnych działań:

- *Przeniesienie.* Operator zainicjował przeniesienie pojedynczej instancji grupy zasobów do innego węzła w klastrze. Może tego dokonać albo w przystawce Failover cluster Management wybierając akcję "Move this service or application to another node" lub poprzez użycie narzędzia wiersza poleceń **cluster.exe** z wykorzystaniem przełącznika **/move** dla grupy zasobów.
- *Przełączenie awaryjne.* Przeniesienie grupy zasobów do innego węzła w klastrze w wypadku awarii zasobu (lub wielu zasobów) w grupie.
- *Przełączenie poawaryjne*. Jeśli przełączenie awaryjne nastąpiło dla grupy zasobów i ta grupa została przeniesiona do innego komputera w klastrze, gdyż awarii uległ komputer, na którym była pierwotnie udostępniana, wówczas zasoby zostaną na ten komputer z powrotem przeniesione, gdy tylko z powodzeniem udało się nawiązać połączenie z klastrem, a zasady przełączenia poawaryjnego zostaną zaimplementowane. Domyślną zasadą przełączenia poawaryjnego jest zapobieganie przełączeniu poawaryjnemu.

Zmiany w klastrach niezawodnościowych w systemie Windows Server 2008

Rola klastra niezawodnościowego w Windows Server 2008 oferuje wiele znaczących ulepszeń pomagających w tworzeniu wysoce dostępnych rozwiązań z zakresu klastrów serwerów i zarządzania nimi. Nowe cechy przyczyniają się do uproszczenia procesu wdrażania i zarządzania klastrami, co redukuje całościowy koszt posiadania (TCO) klastrów. Zmniejszenie TCO sprawia, że klastry niezawodnościowe stanowią atrakcyjne rozwiązanie dla przedsiębiorstw różnej wielkości.

Nowe cechy i ulepszenia dotyczące klastrów w systemie opercyjnym Windows Server 2008 uwzględniają:

- Instalację i migrację.
- Zarządzanie klastrami i funkcjonowanie.
- Zwiększanie dostępności.
- Pracę z pamięciami masowymi.
- Pracę z sieciami i konfigurację zabezpieczeń sieci.

Do nowych cech i ulepszeń w systemie operacyjnym Windows Server 2008 zaliczamy:

- Lepszą weryfikację klastra poprzez narzędzie Kreatora Werfikowania Konfiguracji Klastra.
- Uproszczenie procedur instalacyjnych i zarządzania opartego na zadaniach dzięki przystawce Cluster Administrator.
- Zwiększone wsparcie węzła klastra przez 64 bitową edycję systemu operacyjnego Windows Server 2008
- Nową architekturę kworum (Witness disk).
- Ulepszone funkcjonalności adresowania IP (IPv6, DHCP).
- Eliminację wymogu konfiguracji wirtualnej sieci (VLAN) dla rutowalnej komunikacji klastra.
- Eliminację zależności od protokołu NetBIOS.
- Wsparcie dla pamięci masowych komunikujących się poprzez światłowód, iSCSI lub SAN.

Komponenty klastrów niezawodnościowych
Udana implementacja klastra jest zależna od spełnienia koniecznych wymagań dotyczących sprzętu, oprogramowania i konfiguracji. Oto wymagania:

- Windows Server 2008 – wersja Enterprise lub Datacenter
- Przynajmniej dwie karty sieciowe dla każdego węzła w klastrze
- Wspólna pamięć masowa dla węzłów w klastrze
- Sprzęt certyfikowany jako "Designed for Windows Server 2008"

Weryfikowanie zawartości węzła klastra

Tworzenie klastrów zawsze było uważane za trudne do poprawnego wdrożenia. Traktowane było jako wyspecjalizowana i wysoce techniczna funkcja, która może zostać wdrożona, a następnie zarządzana wyłącznie przez doświadczonego specjalistę IT. Funkcja klastra w Windows Server 2008 rozpoczyna nową erę, upraszczając proces tworzenia klastrów i usuwając wiele technicznych trudności, które uniemożliwiały szersze stosowanie klastrów jako popularnego rozwiązania chroniącego dane. Windows Server 2008 wprowadza wiele nowości:

- Uproszczony process instalacji nowych klastrów.
- Nowe narzędzie ułatwiające migrację istniejących klastrów.
- Nowa konsola administracyjna upraszczająca zarządzanie i konfigurację.
- Zwiększona dostępność poprzez wsparcie większej liczby węzłów na klaster.
- Udoskonalona konfiguracja pamięci masowych i zadań zarządzania.
- Udoskonalone funkcje sieciowe.
- Udoskonalone mechanizmy bezpieczeństwa.

Udoskonalenia w procesie instalacji klastra

Aspekty związane z tworzeniem klastrów w poprzednich wersjach systemu Windows często powodowały zamieszanie wśród wielu osób i skutkowały tym, że albo niewłaściwie konfigurowały one klaster albo po prostu poddawały się, rezygnując z tworzenia klastrów.

Klienci firmy Microsoft raportowali, iż tworzenieie klastrów nie było wystarczająco intuicyjne lub było zbyt trudne do poprawnego wdrożenia. W celu przezwyciężenia problemów związanych z poprzednimi wersjami, Microsoft wprowadził udoskonalenia do procesu instalacyjnego, które pomagają wyeliminować problemy z konfiguracją. Nowe narzędzie dostępne w Windows Server 2008 dokonuje pełnego sprawdzenia konfiguracji klastra , uwzględniając testy węzłów, testy sieci i testy pamięci masowych. Nowy kreator instalacji upraszcza tworzenie klastra, zaś nowe funkcje skryptów umożliwiają automatyzację instalacji i konfiguracji klastra.

Udoskonalenia w zarządzaniu i funkcjonowaniu klastrów

Wszystkie udoskonalenia procesu instalacyjnego ułatwiają instalowanie klastra i redukują możliwość wystąpienia błędu lub zestawienia nieprawidłowej konfiguracji. Zmiany dokonane w funkcjonalności klastra nie kończą się jednak na tym. Windows Server 2008 zawiera także usprawnienia w zarządzaniu i funkcjonowaniu klastra.

Klastrowe narzędzia administracyjne
Nowa, łatwa w obsłudze konsola zarządzania zapewnia oparte na zadaniach zarządzanie poszczególnymi węzłami w klastrze, nowymi węzłami dodanymi do klastra, a także tworzenie klastra dla aplikacji lub usług.

Nowa przystawka do konsoli MMC umożliwia zarządzanie wieloma klastrami z poziomu jednej konsoli, a także pozwala na dynamiczne i szybkie dodawanie zasobów do pracujących klastrów. Zaaawansowane zarządzanie klastrem poprzez narzędzia lini poleceń jest dostępne w systemie operacyjnym Windows Server 2008 z wykorzystaniem polecenia cluster.exe.

Śledzenie zdarzeń dla Windows (ETW) jest bardziej wydajnym i szybszym narzędziem, które zastąpiło poprzednią metodę debugowania do pliku cluster.log. ETW może dostarczać pełnej informacji o systemie lub zostać wykorzystane do mierzenia konkretnych wskaźników w konkretnych środowiskach.

Tworzenie kopii zapasowych i odtwarzanie danych pracują teraz w kontekście nowego modułu zapisującego usługi kopiowania woluminów w tle (VSS) .

Przeglądanie klastrów ujawnia tylko ścieżki i udziały, które są przypisane do klastra. Zasoby, które nie wchodzą w skład konfiguracji klastra i są zasobami lokalnymi węzłów, nie są wyswietlane.

Udoskonalenia konfiguracji i zarządzania pamięciami masowymi

Wsparcie dla pamięci masowych z interfejsem światłowodowym FC, iSCSI ewentualnie szeregowo podłączonym SCSI (SAS), w połączeniu z udoskonaleniem współpracy pomiędzy klastrem i pamięcią masową, pozwalają na zwiększenie wydajności klastra. Wprowadzono następujące udoskonalenia:

- Możliwość dodawania dysków w trakcie pracy aplikacji bez ryzyka zaburzenia jej funkcjonowania.
- Wsparcie dla dysków z tablicą partycji GUID, pozwalające na tworzenie woluminów większych niż 2 TB.
- Minimalne zakłócenia klastra w trakcie zadań sprawdzania pracy dysku.

Dodawanie dysków w trakcie pracy aplikacji klastra

Klastry w systemie Windows Server 2008 są bardziej dynamiczne niż w poprzednich wydaniach. Dodatkowe dyski mogą być udostępnione klastrowi podczas pracy aplikacji. Zależności zasobów mogą być modyfikowane bez przenoszenia zasobów do trybu offline, co oznacza, że użytkownik może udostępnić dodatkowy dysk bez konieczności dostępu do aplikacji.

Lepsza wydajność pamięci masowych i stabilność działania

Kiedy klaster komunikuje się z siecią pamięci masowych (SAN) lub przyłączaną bezpośrednio pamięcią masową (DAS), korzysta on z nowego algorytmu ustawicznego arbitrażu. Poprzednie wersje klastra korzystały z SCSI bus resets, co mogło zakłócać funkcjonowanie SAN. Dyski w systemu Windows Server 2008 nigdy nie są pozostawiane w stanie niechronionym, dzięki czemu zostaje zmniejszone ryzyko awarii woluminu.

> Konfiguracja klastra z wykorzystaniem Virtual Server 2005 ze współdzieloną szyną SCSI nie jest już wspierana. Klastry korzystające ze współdzielonej szyny SCSI wymagają użycia interfejsu SAS, który nie jest obsługiwany przez Virtual Server 2005.

Wsparcie dla większych partycji

Wykorzystanie dysków z tablicą partycji GUID (GPT) umożliwia administratorom nie tylko korzystanie z woluminów większych niż 2 TB, ale także wykorzystanie wbudowanej redundancji. Dyski GPT, w przeciwieństwie do dysków master boot sector (MBR), obsługują większą liczbę woluminów, umożliwiając utworzenie do 128 partycji na jednym dysku, ale przyrost wielkości woluminów może doprowadzić do wydłużenia czasu trwania zadań serwisowych. Chociaż narzędzie CHKDSK było udoskonalane z każdym kolejnym wydaniem systemu Windows, nadal bezpieczniej jest przewidzieć więcej czasu na przeprowadzenie analizy dla większych woluminów.

Łatwiejsze wykonywanie zadań serwisowych dla dysków

Udoskonalona funkcja "Maintenance mode" pozwala użytkownikom na uruchamianie narzędzi służących do łatwiejszego sprawdzania, naprawy, tworzenia kopii zapasowej i przywracania danych z mniejszymi zakłóceniami dla pracy klastra.

Zmiany w sterowniku dysku klastra wprowadzają udoskonalenia do ochrony dysku i funkcjonowania arbitrażu. Działania związane z ochroną dysku (umożliwiające dostęp do dysku i i zabraniające go) teraz są przekazywane do sterownika PartMgr.sys, co usprawnia integrację z zarządzaniem dysku przez system operacyjny i redukuje prawdopodobieństwo awarii dysku. Przeniesienie odpowiedzialności za ochronę dysku na system operacyjny umożliwia wszystkim węzłom funkcjonowanie podczas instalacji funkcji klastrowania, w przeciwieństwie do poprzednich systemów operacyjnych, które wymagały kompleksowego i systematycznego procesu instalacji, z tylko jednym węzłem uruchomionym w danej chwili.

Funkcja arbitrażu dyskowego została przeorganizowana, aby mogła korzystać ze stałych rezerwacji eliminujących prawdopodobieństwo funkcjonowania dysku w stanie niechronionym. Włączenie stałych rezerwacji oznacza także, że resetowania szyny nie są już konieczne. Ta zmiana eliminuje nadmierne zakłócenia SAN.

Udoskonalenia w bezpieczeństwie

Usługa klastrowania w systemie Windows Server 2008 pracuje w kontekście bezpieczeństwa konta LocalSystem. Korzystanie z konta LocalSystem wzmacnia bezpieczeństwo, eliminując potrzebę korzystania z dodatkowego konta użytkownika. Korzystanie z konta Local System zapobiega także konfliktom obiektów zasad grupy, które mogłyby skutkować awarią usługi z powodu blokady lub wygaśnięcia kont.

Uwierzytelnianie protokołem Kerberos i wzmocnione szyfrowanie

Mechanizmy uwierzytelniania zostały zmienione, tak aby stosować wyłącznie protokół Kerberos do uwierzytelniania. Protokół Kerberos jest wykorzystywany przez domeny Windows 2000 i w późniejsze.

Uwierzytelnianie wyłącznie protokołem Kerberos w usługach klastrowych Windows Server 2008 zapewnia model wzajemnej identyfikacji , który oferuje wzmocnione szyfrowanie i lepszą wydajność.

Ulepszony audyt

Nowe funkcje związanie z audytem w systemie Windows Server 2008 pozwalają na szczegółowe śledzenie dostępu do klastra awaryjnej jego zasobów, a także na integrację z Security Log in Event i innymi aplikacjami do monitorowania aplikacji, jak Microsoft Operations Manager (MOM). Dzięki audytowi klastra Windows Server 2008 można śledzić, kto korzystał z klastra i kiedy.

Udoskonalenia w komunikacji sieciowej

Wsparcie dla IPv6 w produkcji i prywatnych sieciach

Klastry niezawodnościowe w systemie Windows Server 2008 mają pełne wsparcie dla IPv6 do komunikacji węzeł-węzeł poprzez sieć lokalną, jak również do komunikacji klient-do-klastra w produkcyjnej konfiguracji sieci.

Udoskonalona komunikacja węzeł-węzeł

Komunikacja węzeł-węzeł w sieci prywatnej może teraz być rutowana między podsieciami bez potrzeby korzystania z wirtualnych sieci LAN (VLAN) w celu rozlokowania geograficznie rozproszonych klastrów.Węzły klastra nadając i odbierając sygnały testowe (heartbeats), aby potwierdzić obecność innych węzłów, teraz korzystają z bardziej niezawodnego protokołu Transmission Control Protocol (TCP), zamiast protokołu User Datagram Protocol (UDP). Chcoiaż nadal wykorzystywany jest port 3343, sygnał testowy nie jest emisją UDP, ale transmisją TCP typu „unicast", która korzysta z mechanizmu „Żądanie-Odpowiedź". Zawiera bardziej zaawansowane cechy jak bezpieczeństwo i sekwencyjne numerowanie. Domyślne zachowanie zostało poprawione z uwzględnieniem tego, jak wiele odpowiedzi może pozostać ominiętych zanim uznamy węzeł za nieosiągalny i polecenie „Przegrupuj" jest wykonywane, aby utworzyć zaktualizowany widok członkostwa klastra. Istnieje prawdopodobieństwo, że wersja produkcyjna systemu Windows Server 2008 pozwoli na ręczną konfigurację tego procesu.

Nowy sterownik NDIS zwany "Microsoft Failover Cluster Virtual Adapter" (neft.sys) zastępuje poprzedni sterownik sieci klastra (slusnet.sys). Podczas gdy poprzedni sterownik sieci klastra był

wyświetlany jako "Non-PNP Driver", nowy odporny na błędy adapter pojawia się jako adapter sieci, gdy włączy się opcję pokazywania ukrytych urządzeń w Menedżerze Urządzeń.

Celem nowego sterownika NDIS jest utrzymywanie połączenia TCP/IP pomiędzy dwoma lub większą liczbą systemów pomimo awarii dowolnego pojedynczego urządzenia w wykorzystywanej trasie komunikacji, tak długo jak alternatywna fizyczna trasa komunikacji istnieje. Innymi słowy, awaria urządzenia sieciowego nie powinna powodować przerwania komunikacji. Komunikacja powinna trwać tak długo, jak alternatywna fizyczna trasa istnieje.

Dostępne statusy dla interfejsów sieciowych i sieci zmieniły się, co przedstawiono poniżej.

Interfejsy sieciowe

- *Up*. Może komunikować się ze wszystkimi innymi interfejsami w sieci LAN, które nie mają statusu Failed lub Unavailable. To jest normalny stan funkcjonowania
- *Failed*. Informuje, że inne interfejsy w sieci LAN mogą komunikować się między sobą lub z zewnętrznymi komputerami, podczas gdy lokalny interfejs nie może.
- *Unreachable*. Nie może komunikować się z co najmniej jednym interfejsem, którego status nie jest oznaczony jako „Failed" ani „Unavailable".

Sieci

- *Up*. Wszystkie interfejsy sieciowe zdefiniowane w tej sieci klastra, które nie mają statusu „Failed" lub „Unavailable", mogą się komunikować. Jest to normalny stan funkcjonowania.
- *Down*. Wszystkie interfejsy sieciowe zdefiniowane w tej sieci klastra przestały się komunikować. Wszystkie podłączone interfejsy sieciowe na węzłach o statusie „Up" mają status „Failed" lub „Unreachable". W związku z tym, wszystkie adresy zasobów TCP/IP, które są zdefiniowane w tej samej podsieci, oraz wszystkie zależności, są niedostępne w sieci LAN.
- *Partitioned*. Jeden lub więcej interfejsów sieciowych znajduje się w stanie „Unreachable", ale co najmniej dwa interfejsy nadal mogą komunikować się ze sobą lub za pomocą zewnętrznego hosta.

Rozwiązywanie nazw DNS

Klastry zbudowane w poprzednich wersjach systemu Windows były zależne od systemu rozwiązywaniu nazw NetBIOS. Klastry zbudowane w systemie Windows Server 2008 nie są już zależne od NetBIOS, co eliminuje potrzebę wdrażania serwera WINS.

Dodatkowe usprawnienia sieci polegają na możliwości dopasowania zależności. Na przykład, można dopasować zależności pomiędzy nazwą sieci a powiązanymi adresami IP, aby upewnić się, że nazwa sieci pozostanie dostępna, jeśli jeden, nie oba, spośród adresów IP, jest dostępny.

Adresowanie DHCP

W klastrze niezawodnościowym Windows Server 2008 klaster może uzyskać adresy IP dynamicznie z serwerów DHCP lub mogą one zostać skonfigurowane statycznie. Jeśli węzły klastra są skonfigurowane do uzyskiwania adresów IP z serwera DHCP, wówczas domyślnym zachowaniem będzie uzyskanie adresu IP automatycznie dla wszystkich adresów IP klastra. Podobnie, jeśli węzły klastra mają statycznie przydzielone adresy IP, adresy IP klastra będą musiały być ręcznie skonfigurowane z wykorzystaniem statycznych adresów IP. Przydział adresu IP do zasobu klastra naśladuje przydział adresów IP do węzłów klastra.

Organizacje z dużą liczbą węzłów klastów oraz aplikacji i usług działających na klastrach będą preferować otrzymywanie adresów z serwera DHCP. Zarówno adresy IP dla zasobów klastra jak i dla sygnału testowego klastra mogą być dostarczane przez DHCP.

Praktyka

Traktowany często jako technicznie zaawansowany sposób wdrażania aplikacji i serwera, klaster niezawodnościowy został uproszczony, aby możliwe było jego szersze stosowanie w sieciach korporacyjnych. Niniejszy rozdział podkreśla nowe możliwości, jakie daje klaster w systemie Windows Server 2008, a w szczególności funkcje i narzędzia zaprojektowane w celu uproszczenia obsługi, zwiększenia stabilności działania i podniesienia poziomu bezpieczeństwa. Rozwój technologiczny klastra niezawodnościowego był projektowany z myślą o wyposażeniu specjalistów IT w narzędzia umożliwiające wdrażanie wysoko dostępnych rozwiązań serwerowych. Redukowanie stopnia technologicznej specjalizacji wymaganej do wdrażania klastrów czyni tę funkcję dobrym rozwiązaniem biznesowym zarówno dla dużych, jak i dla małych środowisk biznesowych.

Usługa klastra składa się z zestawu modułowych komponentów, które są zależne od siebie i pracują wspólnie, by zapewnić funkcjonalność klastra w systemie Windows Server 2008.

Komponent	Funkcjonalność
Messaging	Zawiera różne komponenty, które odpowiadają za komunikację pomiędzy węzłami klastra. Zaliczamy do nich: GEM (Good Enough Multicast), Causal Multicast i MRR (Multicast-Request-Reply).
Object Manager [OM]	Prosty system zarządzania obiektami dla kolekcji obiektów przechowywanych w pamięci operacyjnej.
Host Manager	Kontroluje procesy formowania i dołączania węzłów, generuje powiadomienia o awarii węzłów.
Membership Manager [MM]	Obsługuje dynamiczne zmiany członkostwa klastra.
Global Update Manager [GUM]	Zarządza ulotnymi i trwałymi zmiennymi stanu globalnego całego klastra.

Resource Control Manager [RCM]	Kontroluje konfigurację i stan zasobów oraz drzewa zależności zasobów. Jest odpowiedzialny za monitorowanie aktywnych zasobów w celu sprawdzenia, czy są one nadal online. Tworzy i utrzymuje procesy Resource Host Subsystem (RHS).
Topology Manager [TM]	Zarządza wszystkimi komponentami sieciowymi. Network Manager [NM] zarządza sieciami klastra. Natomiast Interface Manager [IM] zarządza interfejsami sieciowymi i ich właściwościami.
Database Manager [DM]	Implementuje bazę danych konfiguracji klastra. Zajmuje się aktualizowaniem lokalnych replik i/lub replik „witness disk", lub obu rodzajów replik.
Quorum Manager [QUORUM]	Zarządza działaniami powiązanymi z kworum. Szacuje, czy kworum zostało osiągnięte na podstawie skonfigurowanego „modelu" kworum. Ocenia, czy obecny „widok" członkostwa klastra osiągnął „kworum".
Security Manager [SM]	Zarządza wszystkimi kontekstami bezpieczeństwa dla „netft" i warstw komunikacyjnych trybu użytkownika. Działa z Host Managerem w kontekście każdego procesu przyłączania. Obsługuje także podpisywanie i szyfrowanie całej komunikacji w klastrze.
Core [CORE]	Integruje wszystkie komponenty klastra i utrzymuje podstawową informację o klastrze.

Wymagania klastra niezawodnościowego

Wdrożenie sprawnego klastra niezawodnościowego zależne jest od spełnienia wszystkich wymogów programowych, sprzętowych i konfiguracyjnych. Do wymogów tych zaliczamy:

- *Zainstalowany system Windows Server 2008 Enterprise Edition lub Datacenter Edition*.
- *Przynajmniej dwie karty sieciowe*. Węzły w klastrze muszą zawierać dwie karty sieciowe do wspomagania łączności między systemami klienckimi w sieci produkcyjnej oraz do komunikacji z pozostałymi węzłami klastra w trybie sygnału testowego. Sieć używana przez klientów do łączności z klastrem musi być skonfigurowana z adresem IP wspólnym dla wszystkich węzłów w tym klastrze. Ponieważ zazwyczaj dwie karty sieciowe nie mogą mieć wspólnego adresu IP, oprogramowanie klastra pozwala na zduplikowanie adresu IP poprzez konfigurację wspólnego wirtualnego adresu MAC dla węzłów w tym klastrze. Węzły korzystają z sieci prywatnej dla potwierdzenia obecności innych węzłów w klastrze. Sygnał testowy wysyłany jest co sekundę, aby informować pozostałe węzły o swej obecności. W przypadku, kiedy sygnał z węzła posiadającego zasób klastra nie zostanie wysłany wcześniej skonfigurowaną liczbę razy, włącza się tryb pracy awaryjnej klastra, następuje przeniesienie grup zasobów z uszkodzonego węzła na inny sprawny węzeł klastra, co zapewnia ich dostępność. **Karty sieciowe stosowane w komunikacji w ramach sieci produkcyjnej i sieci prywatnej nie mogą jednocześnie służyć do komunikacji z sieciową pamięcią masową iSCSI.**
- *Współdzielona pamięć masowa*. Klastry niezawodnościowe opierają się na architekturze współdzielonej pamięci masowej, dostępnej z poziomu dowolnego węzła w klastrze. Dlatego też wszystkie węzły w klastrze muszą mieć dostęp do współdzielonej pamięci masowej, która gromadzi dane potrzebne każdemu węzłowi na wypadek przejęcia przez dany węzeł funkcji węzła głównego. Pamięcią masową dla węzłów klastra może być sieć pamięci masowych (SAN) z przełącznikiem światłowodowym (FC), urządzenie iSCSI SAN, ewentualnie połączenie szeregowe SCSI (SAS). W przeszłości rozwiązania oparte na światłowodach przewyższały wydajnością technologie iSCSi, choć są od nich znacznie droższe. Zwiększone prędkości i mniejsze koszty sieci opartej na iSCSI przyczyniają się jednak do wzrostu popularności rozwiązań opartych na protokole IP. Kontrolery pamięci masowej używane w połączeniu szeregowym SCSI (SAS) lub przy światłowodach powinny być identyczne na wszystkich węzłach. Kontrolery powinny także korzystać z tej samej wersji oprogramowania producenta. Przy korzystaniu z iSCSI każdy węzeł klastra musi mieć albo kartę sieciową, albo kartę host bus, dedykowaną do pamięci masowej klastra. Używanie karty sieciowej wymaga przeznaczenia tej karty wyłącznie do obsługi technologii iSCSI i niewykorzystywania jej do komunikacji z siecią prywatną lub produkcyjną. Karty sieciowe obsługujące sieć prywatną i produkcyjną nie mogą być wykorzystywane do połączeń z pamięcią masową. Karty sieciowe stosowane do obsługi pamięci masowych powinny być kartami gigabitowymi. Zwielokrotnione karty sieciowe nie są wspierane w komunikacji z pamięciami masowymi iSCSI.

Migracja klastrów

Migracja klastrów była dotąd sporym wyzwaniem. Firmom pracującym z klastrami serwera Windows Server 2003 nowe narzędzie – Kreator Weryfikowania Konfiguracji Klastra (ClusPrep) – daje możliwość łatwego przejścia do klastra w systemie operacyjnym Windows Server 2008, dzięki użyciu graficznego kreatora migracji konfiguracji klastra.

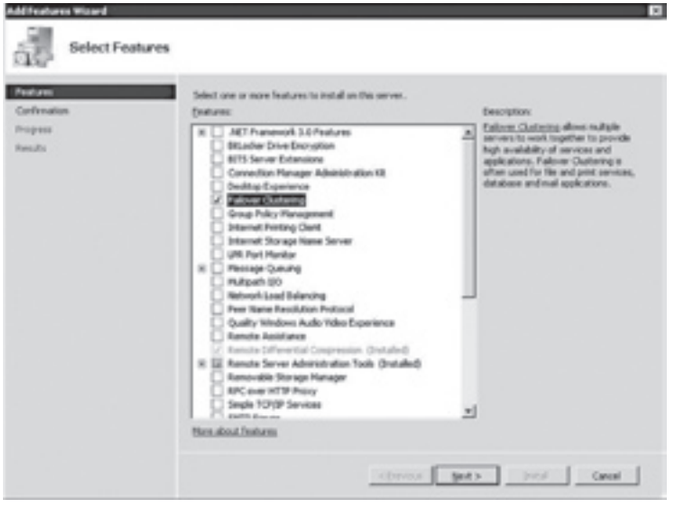
Narzędzie ClusPrep wykryje ustawienia istniejącego klastra działajacego na serwerze Windows Server 2003 i zastosuje je do nowego klastra, pracującego na serwerze Windows Server 2008.

Procedura: Instalacja funkcji klastra niezawodnościowego

Aby zainstalować klaster, możesz skorzystać z kreatora Add Features, który umożliwia dodawanie wielu funkcji serwera jednocześnie. W tym celu:

1. Przygotuj dwa komputery z zainstalowanym systemem Microsoft Windows 2008 Server w wersji Enterprise lub DataCenter zwanych **Węzeł1** i **Węzeł2**, które są niezbędne do instalacji funkcji klastra niezawodnościowego.

2. Uruchom kreator wybierając z menu **Start/Administrative Tools**, a następnie z grupy Server Manager wybierz opcję **Features**. W panelu **Features Summary** wybierz pozycję **Add Features**, co spowoduje uruchomienie kreatora **Add Features Wizard**. W kolejnych krokach zaznacz opcję **Failover Clustering** i na zakończenie kliknij przycisk **Install**. Operację tę wykonaj na komputerach **Węzeł1** i **Węzeł2**.



Kreator Weryfikowania Konfiguracji Klastra (ClusPrep)

Jak poznać, czy instalacja się powiodła? Skąd wiadomo, że konfiguracja sprzętu jest prawidłowa? Czy ustawienia sieciowe są poprawnie skonfigurowane?

W celu uniknięcia niepowodzenia podczas instalacji klastra, firma Microsoft dołączyła do serwera Windows 2008 Kreator Weryfikowania Konfiguracji Klastra (ClusPrep). Narzędzie to pozwala na przeprowadzenie testów węzłów klastra, sieci oraz urządzeń magazynujących, w celu sprawdzenia zdolności przeprowadzenia instalacji klastra na serwerze.

- ClusPrep pozwala na samodzielną weryfikację klastra przed umieszczeniem go w środowisku produkcyjnym.
- ClusPrep, korzystając z rekomendacji firmy Microsoft, identyfikuje właściwe ustawienia konfiguracyjne dla danego klastra.

Test węzłów przeprowadzany przez Kreator Weryfikowania Konfiguracji Klastra sprawdza, czy wybrane serwery spełniają wymogi klastra niezawodnościowego, np. czy pracują na tych samych wersjach systemu Windows i czy posiadają te same aktualizacje.

Test sieci przeprowadzany przez Kreator Weryfikowania Konfiguracji Klastra sprawdza, czy planowana sieć łącząca klaster spełnia konkretne wymogi, takie jak posiadanie przynajmniej dwóch odrębnych podsieci dla redundancji sieci.

Test pamięci masowej stwierdza, czy każdy węzeł wspomaga wymagane komendy SCSI i czy każdy węzeł poradzi sobie z czynnościami klastra.

Weryfikowanie konfiguracji węzłów klastrów

Weryfikowanie konfiguracji węzła klastra

W celu sprawdzenia poprawności konfiguracji serwera, przed rozpoczęciem procedury instalacji klastra Microsoft wzbogacił Windows Server 2008 o Kreator Weryfikowania Konfiguracji Klastra (ClusPrep).

Aplikacja ClusPrep sprawdza wersję systemu operacyjnego każdego węzła w klastrze, włącznie z poprawkami hot fix i dodatkami service pack. Wszelkie rozbieżności są zgłoszane w analizie końcowej. ClusPrep weryfikuje podzespoły sprzętowe, takie jak architektura procesora, karty sieciowe, pamięć, karty HBA (host bus adapters), a także obecność niepodpisanych sterowników. Dla zapewnienia właściwego zarządzania pamięcią masową między węzłami, testowane są też rezerwacje SCSI każdego węzła.

Narzędzie ClusPrep generuje raport, a także pomaga zidentyfikować niespójności, mogące uniemożliwić udaną konfigurację klastra niezawodnościowego.

Weryfikowanie węzła klastra

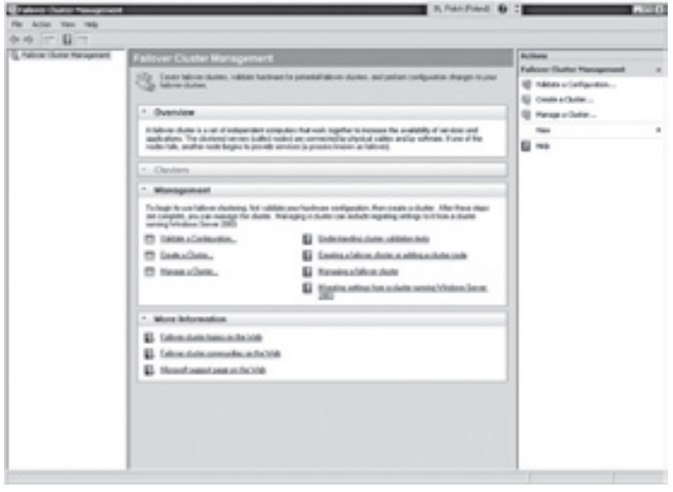
Po zweryfikowaniu konfiguracji potencjalnego klastra narzędzie ClusPrep weryfikuje konfigurację klastra niezawodnościowego dla ponownego sprawdzenia prawdopodobieństwa jego zadziałania. Walidacja węzła klastra dotyczy:

- Łączności między węzłami.
- Kompatybilności rezerwacji SCSI pomiędzy węzłami.
- Obecności i konfiguracji wielu kart sieciowych o różnych adresach IP.
- Dostępności wspólnej pamięci masowej.
- Wejść i wyjść sieciowych i dyskowych.

Raport Podsumowujący Konfigurację Klastra: Na koniec działania Kreatora Weryfikowania Konfiguracji Klastra jest generowany pełen raport. Zawiera on zidentyfikowane przez narzędzie ClusPrep parametry konfiguracji i opis ewentualnych problemów. Raport jest dostępny w folderze c:\Program Files\Microsoft\ClusPrep\Reports\SummaryReport.xml.

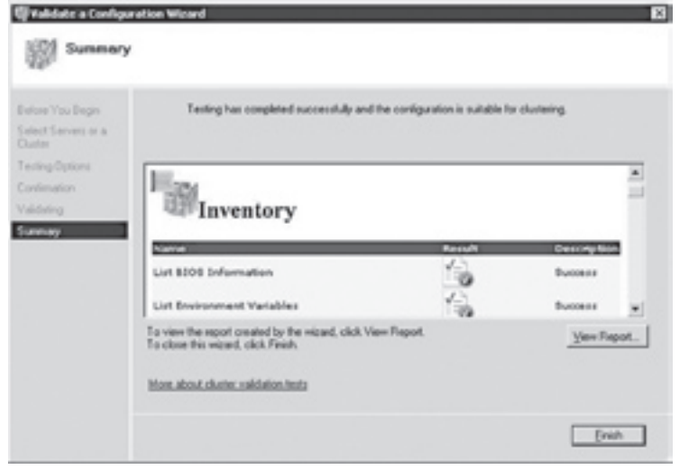
Procedura: Kreator weryfikacji konfiguracji klastra

1. Po zainstalowaniu klastra należy zweryfikować konfigurację węzłów. W tym celu powinieneś skorzystać z konsoli **Failover Clustering Management,** którą uruchomisz z menu **Start/Administrative Tools**.



2. Z panelu **Actions** w konsoli **Failover Clustering Management** wybierz pozycję **Validate a Configuration**. W drugim kroku uruchomionego kreatora **Validate a Configuration Wizard** wprowadź nazwy serwerów, które pełnią rolę węzłów.

3. W kolejnych krokach kreatora pozostaw domyślne opcje. W ciągu kilku minut zostanie wygenerowany raport, który należy przeanalizować i ewentualne błędy naprawić.



Administrator klastra

Konsola Cluster Administrator Management jest nowym interfejsem Microsoft Management Console 3.0, który nie tylko ułatwia tworzenie klastrów niezawodnościowych, ale też minimalizuje ryzyko ich złej konfiguracji. Na przykład uproszczony kreator uwzględnia kwestie potrzebne do zbudowania klastra wymieniającego się plikami, takie jak:

- Jakie pliki mają mieć wysoki stopień dostępności?
- Jakiej nazwy będą używać użytkownicy przy łączeniu się?
- Z jakiego adresu IP powinny korzystać zasoby?
- Których zasobów magazynowych chcemy używać?
- Który folder chcemy udostępnić?

Procedura: Konfigurowanie klastra

Po zainstalowaniu klastra i zweryfikowaniu konfiguracji węzłów należy utworzyć klaster z wcześniej przygotowanych serwerów (węzłów).

Z Panelu **Actions** w konsoli **Failover Clustering Management** wybierz pozycję **Create a Cluster**. W drugim kroku uruchomionego kreatora **Create Cluster Wizard** wprowadź nazwę serwerów, które pełnią rolę węzłów. W kolejnym kroku wpisz nazwę klastra i adres IP, pod którym będzie on widoczny w sieci. W ostatnim kroku po kliknięciu przycisku **Next** zostanie rozpoczęta procedura konfiguracji klastra.

Maksymalizowanie dostępności

Wiele nowych zmian strukturalnych, wprowadzonych we właściwościach klastra niezawodnościowych w serwerze Windows 2008 będzie miało ogromny wpływ na rozmieszczenie serwerów w sieciach firmowych. Nowy model kworum oraz konfigurowalna wartość sygnału testowego pozwalają na przesyłanie sygnału testowego przez sieć otwartą. Koncepcja dysku kworum z poprzednich wersji klastra niezawodnościowego została zastąpiona nowym modelem, nazwanym Witness Disk.

W celu przezwyciężenia pojedynczego punktu awarii w kworum poprzednich wersji klastrów, klastry systemu Windows Server 2008 korzystają z procesu głosowania dla podtrzymania aktywności klastra, kiedy kworum nie może zostać ustanowione.

Nowy model powstał z połączenia dwóch poprzednich modeli - kworum większościowego oraz kworum współdzielonego. Oprócz nowego modelu wykorzystującego Witness Disk, także oba poprzednie można konfigurować w klastrach niezawodnościowych systemu Windows Server 2008. Nowy model jest preferowany w wypadku wystąpienia:

- Małych i dużych węzłów klastra.
- Klastrów bez wspólnej pamięci masowej.
- Klastrów znajdujących się w różnych lokalizacjach.

Na przykład w klastrze o dwóch węzłach z Witness Disk zawarte są trzy głosy. Aby klaster był aktywny, musi utrzymać dwa z trzech głosów. Dodatkowe modele głosowania pozwalają uczestniczyć w procesie głosowania tylko węzłom (podobnie jak w przypadku starszego modelu kworum wielowęzłowego), albo tylko pamięci masowej SAN (podobnie jak w starszej konfiguracji klastra, gdzie kworum miało głos decydujący). Nowy model eliminuje pojedynczy punkt awarii, ponieważ pozwala, by klaster przetrwał utratę dysku kworum.

Poprzednie wersje klastrów wspomagały do ośmiu węzłów. Natomiast Windows Server 2008, działając w edycji 64-bitowej, wspiera obecnie aż do szesnastu węzłów w klastrze.

Klastry niezawodnościowe rozproszone geograficznie

Geograficznie rozproszone klastry często wchodzą w skład planu odzyskiwania kryzysowego oraz ciągłości biznesowej firmy. Klaster geograficzny zawiera dwa geograficznie rozproszone węzły, przystosowane do współpracy między sobą w celu dostarczenia usługi bądź aplikacji. Każdy węzeł przechowuje dane w lokalnej sieci pamięci masowych (SAN), której struktura wykonuje w tle kopie tych danych. W przypadku awarii jednego węzła, dla zachowania ciągłości dostępu, prawo własności zasobów przechodzi na węzeł zapasowy. Dzięki zastosowaniu klastra rozproszonego geograficznie, firmy mogą utworzyć lokacje zapasowe, zapewniając tym samym ciągłość pracy w przypadku wyłączenia z funkcjonowania lokacji głównej.

W poprzednich wersjach systemu Windows klastry rozproszone geograficznie wymagały użycia wirtualnej sieci LAN (VLAN) dla pokonania geograficznych ograniczeń topologii sieci, a także z powodu nierutowalnej komunikacji między węzłami klastra. System Windows Server 2008 upraszcza tworzenie klastrów geograficznych poprzez usunięcie ograniczenia łączności z węzłem klastra w pojedynczej podsieci. Innowacje te wspomagają firmy w projektowaniu i wdrażaniu rozwiązań kryzysowych, co pozwala na zredukowanie czasu przestoju.

Zalecenia

Postępowanie zgodne z najlepszymi praktykami firmy Microsoft pomaga przeprowadzić udane wdrożenie klastra zapasowego. Oto sugerowane sposoby postępowania:

- Sprawdzenie, czy sprzęt w węzłach klastra jest kompatybilny z systemem Windows Server 2008.
- Minimalizacja ilości usług instalowanych na węzłach klastra.
- Zapewnienie fizycznego bezpieczeństwa węzłów klastra.
- Wprowadzenie spójnych mechanizmów zabezpieczeń w celu śledzenia i zapobiegania nieprawidłowym i niepożądanym połączeniom z węzłami klastra.
- Zapewnienie bezpieczeństwa usług sieciowych, których wymagają klastry niezawodnościowe (Active Directory, DNS, DHCP).
- Testowanie i instalowanie najnowszych poprawek i service packów na węzłach klastra.
- Zarządzanie węzłami klastra tylko z zaufanych komputerów.

Podsumowanie

Wraz z rozwojem klastrów w systemie Windows Server 2008 Microsoft znacząco usprawnił proces instalacji i zarządzania klastrami niezawodnościowymi. Nowe i poprawione funkcjonalności zapewniają w sumie uproszczenie procesu, który pozwala zarówno małym, jak i dużym przedsiębiorstwom na obniżenie całkowitych kosztów utrzymania (TCO) i zwiększenie niezawodności rozlokowania aplikacji.

Zakończenie

Funkcja klastra niezawodnościowego w systemie Windows Server 2008 znacząco ułatwia konfigurację i zarządzanie rozwiązaniami zapewniającymi wysoką wydajność. Możliwość szybkiej weryfikacji zgodności sprzętu i oprogramowania z wymaganiami klastra, przyjazny użytkownikowi kreator instalacji i efektywnie działająca konsola zarządzania są znaczącymi zmianami.

Powinny one pozwolić małym i średnim przedsiębiorstwom na stosowanie rozwiązań zapewniających wysoką dostępność. Było to dotychczas poza ich zasięgiem z uwagi na wymóg posiadania wysokowykwalifikowanej kadry IT, która mogłaby zapewnić poprawną instalację klastrów i zarządzanie nimi.

Także duże organizacje skorzystają z nowości oferowanych przez klaster niezawodnościowy w systemie Windows Server 2008. Szczególnie atrakcyjne wydają się tu ułatwienia dotyczące komunikacji poprzez sieci zewnętrzne przy tworzeniu zapasowych lokacji dla klastrów. Natomiast rezygnacja z zależności od systemu rozpoznawania nazw NetBIOS oznacza możliwość uproszczenia infrastruktury rozpoznawania nazw.

Podsumowując, rola klastra niezawodnościowego może okazać się właściwym rozwiązaniem, jeśli organizacja wymaga:

- odpornego na awarie dostępu do aplikacji,
- ochrony zasobów sprzętowych i aplikacji,
- niezakłóconego dostępu do danych o kluczowym znaczeniu dla przedsiębiorstwa.

ABC Data Centrum Edukacyjne powstało w czerwcu 2003 roku. Celem naszego Centrum jest prowadzenie szeroko rozumianej działalności szkoleniowej w zakresie zaawansowanych technologii informatycznych.

Dzięki bogatej ofercie ułatwiamy Państwu zdobycie specjalistycznej wiedzy, a także zweryfikowanie posiadanych umiejętności. Proponujemy szkolenia autoryzowane, autorskie oraz konsultacje z zakresu różnorodnych dziedzin informatyki. Kursy prowadzone w naszych ośrodkach mogą mieć charakter otwarty lub zamknięty. Otworzyliśmy na terenie kraju już sześć oddziałów naszego Centrum Edukacyjnego i nie ustajemy w staraniach, by zaspokoić wszelkie Państwa oczekiwania.

Systematycznie poszerzamy ofertę i staramy się dotrzeć do wszystkich zainteresowanych rozwojem swoich kompetencji. Nasi Klienci mają możliwość dołączenia do szerokiego grona uczestników Programu Lojalnościowego .gif(t). Każdy Uczestnik Programu Lojalnościowego jest nagradzany za nabywanie usług objętych Programem poprzez przyznanie punktów, które mogą być następnie wymieniane na cenne nagrody . Zapraszamy serdecznie do skorzystania z naszej oferty!

Adres
Zielna 39
Warszawa, 00-108

Osoba kontaktowa
Aneta Czajkowska-Turek
Tel.: (48 22) 31 32 333
Fax: (48 22) 31 32 334
aneta.czajkowska@abcdata.pl
www.edukacja.abcdata.pl

Altkom powstał w 1988 roku. Obecnie zatrudnia 342 pracowników w siedmiu ośrodkach na terenie całego kraju: w Warszawie, Krakowie, Katowicach, Poznaniu, Wrocławiu, Gdyni oraz Łodzi. Zakres działalności firmy obejmuje trzy obszary: Usługi edukacyjne: Altkom Akademia posiada w stałej ofercie ponad 400 autorskich i autoryzowanych szkoleń związanych z różnymi technologiami. Zatrudnia 120 wykwalifikowanych instruktorów. Dysponuje 56 własnymi, w pełni wyposażonymi salami szkoleniowymi. Z usług Altkomu skorzystało już ponad 140 tysięcy osób. Posiada największą na rynku liczbę certyfikatów i autoryzacji wszystkich liczących się dostawców technologii, w tym Microsoft. Obecny potencjał Altkom umożliwia realizację największych, jak również najbardziej złożonych projektów i przedsięwzięć. Usługi projektowo-programistyczne: Altkom tworzy oprogramowanie na zamówienie. Rozwiązania, które oferuje wspomagają zarządzanie, sprzedaż, łańcuchy dostaw oraz relacje z klientami. Realizuje je w technologiach intranetowych, internetowych i ekstranetowych. Wykorzystuje przy tym nowoczesne systemy baz danych i architekturę trójwarstwową. Usługi integracyjne: Altkom prowadzi prace integratorskie, których celem jest stworzenie i utrzymanie optymalnego środowiska informatycznego w firmie klienta. Specjalizuje się w rozwiązaniach systemowych w zakresie: • integracji struktur informatycznych, oprogramowania i sprzętu • projektowania i wdrażania struktur bezpieczeństwa IT • projektowania usług katalogowych, integracji katalogów oraz integracji usług katalogowych z aplikacjami i systemami operacyjnymi.

Adres
Chłodna 51
Warszawa, 00-867

Kontakt
Tel.: 0 801 258 566
www.altkom.pl

COMBIDATA zajmuje się szkoleniami w ich najbardziej rozwiniętej formie, tj. od analizy procesów biznesowych i określenia potrzeb kompetencyjnych, do dostarczania wiedzy, umiejętności i zachowań w różnych technologiach edukacyjnych (np. różne formy e-learningu). Na szkolenia składa się wiele różnych elementów, tj. np. infrastrukturalne, trenerskie, projektowe, podręcznikowe, itd. Znaczną część wymaganych elementów w procesie projektowania i realizacji szkoleń COMBIDATA posiada. Niektórych z nich poszukuje na rynku, ażeby jak najlepiej spełnić wymagania klienta. z tego punktu widzenia wydaje się, że COMBIDATA jest **INTEGRATOREM USŁUG SZKOLENIOWYCH**.

Od 2000 roku COMBIDATA posiada certyfikat ISO 9001:2000 (pierwotnie ISO 9001:1994) obejmujący projektowanie, organizowanie i prowadzenie szkoleń, a w tym szkoleń elektronicznych do samokształcenia. Certyfikat dotyczący szkoleń COMBIDATA otrzymała jako pierwsza firma w Polsce.

Główna siedziba firmy znajduje się w Sopocie, firma posiada pięć biur regionalnych i 30 centrów szkoleniowych na terenie całego kraju.

COMBIDATA Poland prowadzi jedyny w Polsce ORACLE Approved Education Center, uzyskała status Microsoft Certified Gold Partner for Learning Solutions, a także CISCO Sponsored Organization i Authorised Thomson Prometric Testing Centre.

COMBIDATA Poland została uznana przez firmę Microsoft za największy autoryzowany ośrodek szkoleniowy w Polsce w roku 2007, uzyskując i miejsce za największą liczbę przeprowadzonych szkoleń autoryzowanych w zakresie technologii Microsoft.

Adres
Emilii Plater 12
Sopot, 81-777

Osoba kontaktowa
Monika Koszewska
Tel.: (58) 550 95 35
Fax: (58) 550 95 51
monika.koszewska@combidata.pl
www.eduportal.pl

Comp Safe Support SA jest jedną z największych firm na polskim rynku informatycznym, świadczącą kompleksową obsługę w zakresie IT. W ofercie firmy znajdują się: Szkolenia Informatyczne, Usługi Wdrożeniowe, Konsultacje, Specjalne Systemy Bezpieczeństwa, Bezpieczeństwo IT i Ochrona Informacji, Systemy PKI i Autoryzacji, Outsourcing IT, Usługi Serwisowe, Usługi Sieciowe. **Comp Safe Support SA** współpracuje z **Microsoft** od 14 lat.

Spółka jest certyfikowanym partnerem firmy Microsoft - Microsoft Gold Certified Partner posiadającym kompetencję Learning Solutions w zakresie usług szkoleniowych, kompetencję Information Worker Solutions w obszarze wdrożeń nowoczesnych rozwiązań IT Microsoft Office System, kompetencję Advanced Infrastructure Solutions w zakresie projektowania i wdrażania zaawansowanych technologii informatycznych oraz kompetencję Licensing Solutions w zakresie audytu i zarządzania oprogramowaniem. Centrum Edukacyjne Comp Safe Support SA jest autoryzowanym ośrodkiem testowym firm Prometric i Pearson VUE w zakresie przeprowadzania egzaminów na inżynierów systemowych oraz CertiPort w zakresie prowadzenia testów dla użytkowników pakietu Microsoft Office. Od 2006 r. Comp Safe Support SA oferuje szkolenia informatyczne dofinansowane ze środków Europejskiego Funduszu Społecznego (EFS) Unii Europejskiej. W ofercie znajduje się szeroka gama szkoleń autoryzowanych z produktów firmy Microsoft, przeznaczonych dla użytkowników, administratorów sieci i systemów, programistów oraz szefów projektów informatycznych.

Adres
Jutrzenki 116
Warszawa, 02-230

Osoba kontaktowa
Mirosław Trzpil
Tel.: (022) 465 04 00
Fax: (022) 520 26 53
miroslaw.trzpil@comp-css.pl
www.comp-css.pl

Microsoft TechNet

Centrum wiedzy technicznej dla specjalistów IT:

- baza wiedzy
- wersje testowe oprogramowania
- wirtualne laboratoria
- konferencje i seminaria
- szkolenia i certyfikacje
- webcasty
- blogi
- społeczności

www.microsoft.pl/technet