SPOŁECZNA WYŻSZA SZKOŁA PRZEDSIĘBIORCZOŚCI I ZARZĄDZANIA W ŁODZI

KIERUNEK STUDIÓW: **INFORMATYKA**

Jakub Sułkowski
Numer albumu: 49599

WDROŻENIE ACTIVE DIRECTORY Z POLISAMI BEZPIECZEŃSTWA DLA PRZEDSIĘBIORSTWA „JASKULEK”

Praca inżynierska napisana
w Wydziale Stosunków Międzynarodowych
i Informatyki
pod kierunkiem dr inż. Piotra Goetzena

Łódź 2011

Spis treści:

Rozdział 1

WSTĘP

Systemami firmy Microsoft i usługami zaimplementowanymi w tych systemach interesowałem się już od dawna. Zagadnienia związane z Active Directory to bardzo szerokie spektrum i długo zastanawiałem się jak należałoby to opisać. W toku różnorakich przemyśleń powstała ta właśnie praca.

Żyjemy w czasach, gdy rozmaite instytucje na całym świecie coraz intensywniej wykorzystują technologie informatyczne. Zapotrzebowanie na nowe usługi IT zwiększa się z każdym rokiem. Wiele firm informatycznych stara się sprostać coraz większym wymaganiom stawianym najczęściej przez ich kluczowych klientów. Na rynku istnieje kilka usług zapewniających wspomaganie zarządzania przedsiębiorstwem. Jedną z nich jest Samba oferowana przez systemy Linux. Rozwiązanie to nie jest jednak popularne, mimo tego, że jest całkowicie darmowe.

Inną technologia jest eDirectory oferowana przez firmę Novell. Można spotkać jeszcze przedsiębiorstwa, które z powodzeniem ją wykorzystują. Novell swoje eDirectory wprowadził od wersji 6.0, początkowo jako dodatek płatny (konieczne było wykupienie dodatkowej licencji). Obecnie w wersji 6.5, (jest jeszcze dystrybuowana) czyli ostatniej wersji serwera oferowanej przez tę firmę, eDirectory dołączano bezpłatnie wraz z usługami: DHCP, DNS, PRINTSERVER, czy wbudowaną bazą danych PERVASIVE SQL.

IBM również ma swoją technologię usług katalogowych, nazwaną IBM Tivoli Directory Server.

Według mnie najciekawszą technologią istniejącą obecnie na rynku IT jest usługa Active Directory i usługi z nią powiązane, oferowana przez firmę Microsoft. Od momentu wprowadzenia, AD cieszy się coraz większa popularnością, a wykorzystują ją zarówno małe jak i wielkie przedsiębiorstwa niezależnie od branży.

Rozdział 2
CEL I ZAKRES PRACY

Celem niniejszej pracy jest projekt i implementacja usługi Active Directory opartej na systemie Microsoft Windows 2008 R2 dla przedsiębiorstwa „Jaskulek”. Zostanie ona podzielona na część teoretyczną i praktyczną. Zakres pracy będzie obejmował kompletną instalację i konfigurację wyżej wymienionego systemu. W części teoretycznej znajdą się podstawowe informacje o systemie serwerowym firmy Microsoft i jego rolach. Część praktyczna natomiast to kompletny projekt wdrożenia tegoż systemu dla konkretnie sprecyzowanych potrzeb firmy „Jaskulek”.

Rozdział 3

HISTORIA O SYSTEMACH WINDOWS SERWER [4, 6]

W 1994 roku firma z Redmond wydała pierwszą wersję systemu serwerowego o nazwie Windows NT 3.5 Server. Po siedemnastu latach i sześciu wersjach systemu określanych mianem serwerowych, Microsoft zaprezentował Windows Server 2008 R2. Wydany on został 22 lipca 2009 roku, ale oficjalna premiera odbyła się dopiero 22 października 2009 roku.

Do rodziny systemu Windows Server 2008 R2 można zaliczyć następujące wersje systemu:

- Windows Server 2008 R2 Foudation
- Windows Server 2008 R2 Standard Edition
- Windows Server 2008 R2 Enterprise Edition
- Windows Server 2008 R2 Datacenter Edition
- Windows Server 2008 R2 Web Server
- Windows Server 2008 R2 dla systemów Itanium

Poszczególne wersje systemu Windows Serwer różnią się między sobą pod wieloma względami. Zasadnicze różnice ukazuje poniższe zestawienie tabelaryczne, które zostało opracowane na podstawie zestawienia Williama R. Stanek:

Tabela nr 1 Istotne różnice pomiędzy poszczególnymi wydaniami Windows Server

Wersja Funkcja	Standard	Enterprise	Datacenter	Web Serwer	Foudation	Itanium
Server WINS	Tak	Tak	Tak	Nie	Nie	Tak
Windows PowerShell	Tak	Tak	Tak	Tak	Tak	Tak
Licencjonowanie Grupowe	Tak	Tak	Tak	Tak	Tak	Nie
Obrazy Wirtualizacyjne	Host + 1VM	Host +4VM	Bez ograniczeń	Tylko jeden system gościa	Bez ograniczeń	n/d
Autonomiczne Korzenie systemu DFS	1	Bez ograniczeń	Bez ograniczeń	n/d	n/d	1
Maksymalna liczba gniazd Procesorów	4	8	64	4	64	1
Opcja instalacji Server Core	Tak	Tak	Tak	Tak	Nie	Nie
RAM	32GB	2TB	2TB	32GB	2TB	8GB
Hyper-V	Tak	Tak	Tak	Nie	Nie	Nie
Wymiana procesorów na gorąco	Nie	Nie	Tak	Nie	Tak	Nie
Wymiana pamięci na gorąco	Nie	Nie	Tak	Nie	Tak	Nie
Dodawanie procesorów na gorąco	Nie	Nie	Tak	Nie	Tak	Nie
Dodawanie pamięci na gorąco	Nie	Nie	Tak	Nie	Tak	Nie
Odporna na uszkodzenia synchronizacja pamięci	Nie	Nie	Tak	Nie	Tak	Nie
Active Directory Rights Management Services	Tak	Tak	Tak	Nie	Nie	Tak

Źródło: **Stanek William R.**, *Vademecum Administratora Windows Server 2008 R2*,wyd.2, Microsoft Press, Warszawa 2010, str.4-5

Microsoft wprowadził dużo zmian w systemie Windows Server 2008 R2. Porównując go z poprzednimi wersjami systemów serwerowych można zauważyć, że Windows Server 2008 R2 jest dostępny już tylko w wersji 64-bitowej. Jego poprzednicy dostępni byli (Windows 2000 Server, Windows 2003 Server, Windows 2003 R2 Server, Windows 2008 Server) w wersjach 32- i 64-bitowych. Dodatkową nowością, która została wprowadzona w Windows Server 2008 jest możliwość instalacji systemu w dwóch typach. Po instalacji danego typu zmiana na drugi nie jest już możliwa.

Wersja „Core” - opcja minimalnej instalacji zapewnia wsparcie dla określonych ról i funkcji systemu. Interfejs użytkownika w tym typie instalacji zawiera minimalną ilość

funkcji użytkowych. Natomiast dużym plusem typu instalacji „Core" jest bezpieczeństwo, ponieważ wersja tak, jak wspomniałem powyżej, posiada na tyle mało funkcji, że liczba potencjalnych ataków na taki serwer (mała ilość luk w systemie) jest znikoma. Wersja „Core" to aż dziewięć ról i zarazem jedenaście funkcji opcjonalnych:

- Role
  - Active Directory Domain Services,
  - Active Directory Lightweight Directory Services,
  - Active Directory Certificate Services,
  - DHCP Server,
  - DNS Server,
  - File Services,
  - Print Server,
  - Streaming Media Services,
  - IIS 7.5,
  - Hyper-V
- Funkcje
  - Klaster pracy awaryjnej,
  - Równoważenie obciążenia sieciowego,
  - Podsystem aplikacji systemu UNIX,
  - Kopia zapasowa,
  - Wielościeżkowe We/Wy,
  - Menadżer magazynu wymiennego,
  - Szyfrowanie dysków funkcja BitLocker,
  - Usługi SNMP,
  - Server WINS,
  - Klient Telnet,
  - Quality of Service,

Do dodatkowych zmian wprowadzonych w typie Core w Windows Server 2008 R2 należą:

- Zdalne zarządzanie przy użyciu Server Manager
- Narzędzie Windows Server Migration
- Windows PowerShell

Wersja „Full” - to opcja instalacji pełnej, w której administrator ma możliwość zainstalowania wszystkich ról i funkcji systemu.

Podczas instalacji Windows Server 2008 R2, system jest instalowany z minimalnymi ustawieniami. Dopiero administrator decyduje jakie role i funkcje mają być zainstalowane. Ponieważ żadne dodatkowe usługi nie są instalowane, zmniejsza się liczba potencjalnych dziur systemowych oraz daje to większe bezpieczeństwo.

System Windows Server 2008 R2 udostępnia nam następujące role:

Tabela nr 2 Podstawowe role i związane z nim usługi roli systemu Windows Server 2008 R2

Rola	Opis
Active Directory Certificate Services (AD CS)	AD CS udostępnia funkcje niezbędne do wystawania i odwoływania certyfikatów cyfrowych dla użytkowników komputerów klienckich i serwerów. AD CS zawiera następujące usługi Certification Authority Web Enrollment, online Responder, Network Device Enrollment Service, Certificate Enrollment Web Service oraz Certificate Enrollment Policy Web Service.
Active Directory Domain Services (AD DS)	AD DS. udostępnia funkcje wymagane do przechowywania informacji o użytkownikach grupach komputerach i innych obiektach w sieci oraz pozwala na korzystanie z tych informacji użytkownikom i komputera.
Active Directory Federation Services (AD FS)	AD FS uzupełnia funkcje uwierzytelnienia i kontroli dostępu oferowane przez AD DS, rozszerzając je na sieć World Wide Web. Zawiera następujące usługi roli i usługi pomocnicze Federation Service, Federation Service Proxy, AD FS Web Agent, Claims-aware Agent oraz Windows Token-based Agent.
Active Directory Lightweight Directory Services (AD LDS)	AD LDS udostępnia magazyn danych dla aplikacji z włączoną obsługą katalogu, który nie wymaga pełnej wersji AD DS i nie musi być instalowany na kontrolerze domeny.
Active Directory Rights Management Services (AD RMS)	AD RMS zapewnia kontrolowany dostęp do chronionych wiadomości e-mail, dokumentów i innych plików. Zawiera następujące usługi roli: Active Directory Rights Managment Server oraz Identity Federation Support.
Application Server	Rola serwera aplikacji pozwala serwerowi na utrzymywanie rozproszonych aplikacji zbudowanych przy użyciu ASP.NET, Enterprise Services lub .NET Framework 3.0 zawiera kilkanaście usług roli.
DHCP Server	DHCP zapewnia scentralizowane sterowanie adresowaniem IP.
DNS Server	DNS jest systemem rozpoznawania nazw, przekształcających nazwy komputerów na adresy IP i odwrotnie Serwery DNS są podstawą rozpoznawania nazw w domenach Active Directory.
Fax Server	Rola zapewnia scentralizowane wysyłanie i odbieranie faksów dla całego przedsiębiorstwa. Server tej roli może działać jako bramka faksowania i pozwala na zarządzanie zasobami faksu.
File Services	Rola usług plików zapewnia podstawowe usługi zarządzania i udostępniania plików w sieci. Liczne role serwerów wymagają pewnego typu usług plików. Rola zawiera następujące usługi roli oraz usługi podrzędne: File Server, Distributed File System, DFS Namespace, DFS Replication, File Server Resource Manager, Services for Network File System (NFS), Windows Search Service, Windows Server 2003 File Services, File Replication Service (FRS), Indexing Services oraz BranchCache for Network Files.

Hyper-V	Udostępnia usługi pozwalające utworzyć i zarządzać maszynami wirtualnymi emulującymi fizyczne komputery. Maszyny wirtualne mają odrębne środowisko systemu operacyjnego od środowiska hosta.
Network Policy and Access Services (NPAS)	NPAS udostępnia podstawowe usługi zarządzania routingiem i dostępem zdalnym do zasobów w sieci. Zawiera następujące usługi roli: Network Policy Server, Routing and Remote Access Services RRAS, Remote Access Service, Routing, Health Registration Authority oraz Host Credential Authorization Protocol (HCAP).
Print and Document Services	Rola zapewnia usługi drukowania w sieci i zarządzania drukarkami sieciowymi, skanerami sieciowymi i odpowiadającymi im sterownikami. Obejmuje następujące usługi roli: Print Server, LDP Service, Internet Printing oraz Distributed Scan Server.
Remote Desktop Services	Zapewnia usługi terminalowe, umożliwiające uruchomienie aplikacji Windows zainstalowanych na serwerze zdalnym. Gdy użytkownicy uruchamiają programy na serwerze terminali, całość przetwarzania odbywa się na serwerze. Zaś przez sieć transmitowane są tylko dane obrazujące ich działanie. Rola zawiera następujące usługi roli: Remote Desktop Session Host, Remote Desktop Virtualization Host, Remote Desktop Licensing, Remote Desktop Connection Broker, Remote Desktop Gateway oraz Remote Desktop Web Access.
Universal Description Discovery Integration (UDDI) Services	UDDI dostarcza możliwości udostępniania informacji o usługach Web tak wewnątrz organizacji, jak między organizacjami. Zawiera następujące usługi roli: UDDI Services DataBase oraz UDDI Services Web Application.
Web Server (IIS)	Server sieci Web (IIS) służy do utrzymywania witryn Web oraz aplikacji opartych na sieci Web. Witryny Web mogą zawierać zarówno statyczną, jak i dynamiczną zawartość. Aplikacje Web można budować przy użyciu ASP.NET lub .NET Framework 3.5.1 Po wdrożeniu serwera Web można zarządzać jego konfiguracją przy użyciu modułów ISS 7.5 oraz narzędzi administracyjnych. Zawiera kilkadziesiąt usług roli.
Windows Deployment Services (WDS)	WDS udostępnia usługi pozwalające na wdrażanie systemów Windows w skali całego przedsiębiorstwa z jednego punktu. Zawiera następujące usługi Deployment Server oraz Transport Server.
Windows Server Update Services	Udostępnia usługi Microsoft Update, pozwalając na stworzenie własnego punktu dystrybucji poprawek dla stacji klienckich w sieci.

Źródło: **William R. Stanek,** *Vademecum administratora Windows Server 2008 R2*, wyd. 2, APN Promise 2010, str.31-33

Rozdział 4
OPIS USŁUGI ACTIVE DIRECTORY [1, 2]

Active Directory jest technologią stworzoną przez Microsoft. Technologia ma już ponad dziesięć lat. Premiera tej technologii miała miejsce wraz z pojawieniem się systemu Windows Server 2000. Active Directory zastąpiła poprzednią usługę Microsoft jaką była domena znana z czasów Windows NT. Active Directory usunęło największe wady poprzedniej usługi. Można w niej przechować ponad milion obiektów. Poprawiono także hierarchiczność przechowywania informacji oraz rozszerzalność schematu zawierającego definicje obiektów. Active Directory do swojego poprawnego działania wykorzystuje zmodyfikowane wersje istniejących protokołów i usług. Należą do nich:

- Lightweight Directory Access Protocol LDAP
- Uwierzytelnienie oparte na Kerboros
- DNS

Wraz z pojawieniem się systemu Windows Server 2008 R2 Microsoft zmienił nazwę usługi Active Directory na Active Directory Domain Services. AD DS jest hierarchiczną bazą danych. Można ją podzielić na dwie części-fizyczną i logiczną, co dokładnie opiszę w poniższych podrozdziałach.

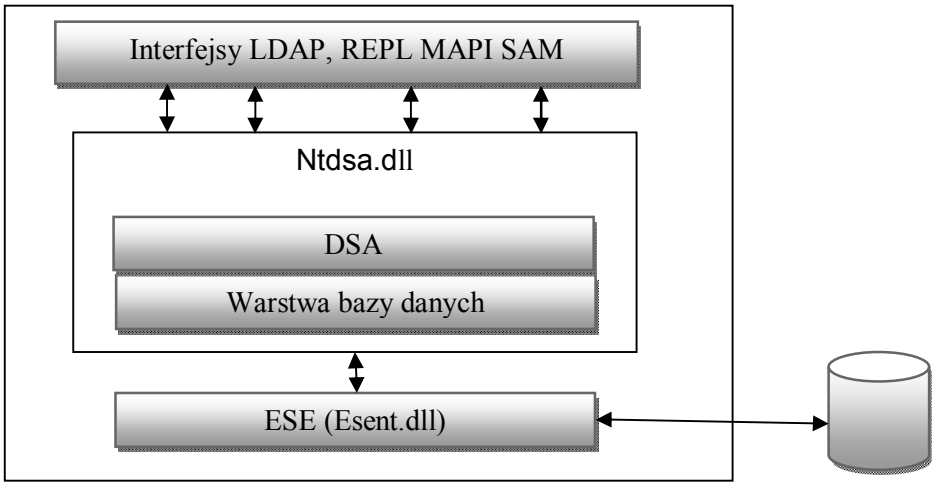
4.1. Struktura fizyczna

Struktura fizyczna to baza danych, która jest pojedynczym plikiem. Plik bazy danych jest przechowywany na każdym kontrolerze domeny. Znajduje się on w pliku Ntds.dit, a dzienniki transakcji na kontrolerze domeny. Te domyślnie pliki przechowywane są w folderze NTDS na dysku logicznym, gdzie znajduje się kontroler domeny. Pliki te przechowują wszystkie informacje o katalogu domeny. Również w tym pliku przechowywane są wszystkie informacje, które są współużytkowane przez inne kontrolery domeny w przedsiębiorstwie. Dodatkowo serwery wykazu globalnego zawierają w tych plikach swoje dane wykazu globalnego.

4.1.1. Magazyn danych katalogu

Magazyn danych katalogu instalowany jest na wszystkich kontrolerach w lesie. Składa się on ze składników, które przedstawia poniższy rysunek. Tabela nr 3 zawiera opis interfejsów oraz składniki magazynu danych.

Rysunek nr 1 Składniki magazynu danych



Źródło**: Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str. 22

Katalog ten zawiera wszystkie informacje o obiektach (użytkownicy, komputery, jednostki organizacyjne, domeny, grupy, zasady zabezpieczeń). Katalog ten jest przechowywany na wszystkich kontrolerach domeny. Dostęp do niego posiadają aplikacje sieciowe lub usługi. Komputery klienckie, inne kontrolery domeny i administratorzy nie mogą komunikować się bezpośrednio z bazą danych. Dlatego magazyn danych obsługuje interfejsy, które zostały wymienione w tabeli nr 3. Według teorii w strukturze AD może istnieć jeden bądź więcej kontrolerów domeny. Każdy z takich kontrolerów przechowuje kopię folderu dla całej domeny. Zmiany wprowadzone w tym katalogu na jednym kontrolerze są natychmiast replikowane do innych kontrolerów w danej domenie. Replikowane są:

- **Dane domeny**
- **Dane konfiguracyjne**
- **Dane schematu**
- **Dane aplikacji**

Tabela nr 3 Składniki magazynu danych

Składnik	Opis
Interfejsy	LDAP (Lightweight Directory Access Protocol) Protokół LDAP v3 jest najczęściej używanym interfejsem przez klientów katalogu do zlokalizowania informacji w magazynie katalogu. Protokół LDAP v3 jest zgodny z poprzednią wersja LDAP v2. Klienci mogą korzystać z portu 389 (standardowy port LDAP), portu 636 (protokół LADP zabezpieczony przez SSL), portu 3269 (dla wyszukiwania wykazu globalnego) oraz portu 3269 (globalny wykaz LADP zabezpieczony przez SSL) do uzyskania dostępu do interfejsu LDAP. Klienci mogą również użyć portu 389 protokołu UDP zarówno dla LDAP jak dla Netlogon (interfejs ten jest używany do zlokalizowanie kontrolerów domen).
	MAPI (Messaging API) interfejs ten jest używany przez klientów do przekazywania wiadomości, takich jak program Outlook, do uzyskania dostępu do danych programu Microsoft Exchange Server 2000 przechowywanych w magazynie danych. Program Microsoft Exchange Server 2000 i jego późniejsze wersje korzysta z magazynu danych usług AD DS do przechowywania wszystkich informacji o odbiorcy, a interfejs MAPI umożliwia klientom pocztowym uzyskanie dostępu do globalnej list adresów GAL(Global Address List). Interfejs używa komunikacji RPC.
	SAM Security (Accounts Manager) program SAM jest interfejsem opracowanym przez MS służącym połączeniom do DSA w imieniu klientów korzystających z systemu Windows NT 4.0 lub wcześniejszych systemów. Te systemy klienckie używają interfejsów API sieci systemu Windows NT 4.0 do połączenia się z DS przez interfejs SAM Komunikacja interfejsu SAM również korzysta z komunikacji RPC.
	REPL (interfejs zarządzania replikacją i kontrolerem domeny) interfejs zarządzania REPL jest używany przez narzędzia zarządzania usług AD DS podczas replikacji pomiędzy kontrolerami domen. Interfejs ten udostępnia funkcje wyszukiwania danych o kontrolerach domen, konwersji nazw obiektów sieci występujących w różnych formach i funkcje obsługi głównych nazw usługi SPN(Service Pricipal Name) i agentów DSA. Interfejs ten jest dostępny poprzez wywołania RPC(Remote Procedure Call) i protokołów SMTP (jedynie dla replikacji opartych na SMTP).
Directory Service Agent (DSA)(Ntdsa.dll)	Agent usługi katalogowej DSA (uruchamiany jako biblioteka Ntdsai.dll na każdym kontrolerze domeny) udostępnia interfejsy dostępu do magazynu danych. Ponadto agent DSA wymusza semantykę katalogu, utrzymuje schemat, gwarantuje tożsamość obiektu i wymusza typy danych dla atrybutów. Kiedy klienci lub inne kontrolery domen potrzebują uzyskać dostęp do magazynu danych, korzystają z jednego z obsługiwanych interfejsów do połączenia z agentem DSA, a następnie wyszukują, odczytują i zapisują informacje w obiektach i atrybutach usług AD DS
Warstwa bazy danych	Warstwa bazy danych znajduje się w pliku Ntdsai.dll i udostępnia wewnętrzny interfejs pomiędzy DSA a bazą danych katalogu. Agent DSA nie może bezpośrednio łączyć sie z bazą danych; aplikacje przechodzą przez warstwę bazy danych. Warstwa bazy danych możliwa również przeglądanie obiektów bazy danych katalogu, przez co dane stają się dostępne dla DSA jako zestaw hierarchicznych kontenerów. Warstwa bazy danych jest także odpowiedzialna za tworzenie, uzyskiwanie i usuwanie poszczególnych rekordów(obiektów), atrybutów wewnątrz rekordów i wartości wewnątrz atrybutów.
ESE (Esent.dll)	Mechanizm ESE(Extensible Storage Engine) jest składnikiem systemu Windows używanym przez usługi AD DS, jak również przez kilka innych składników systemu Windows jako interfejs do bazy danych. Składnik ESE jest odpowiedzialny za indeksowanie danych w pliku bazy danych i za transfer danych do/z bazy danych. Składnik ten utrzymuje także wiersze i kolumny, z których składa się baza danych, i jego zadaniem jest umożliwienie aplikacjom przechowywanie i uzyskiwanie danych. Składnik ESE implementuje również proces transakcji przekazywania zmian w bazie danych.
Pliki bazy danych	Magazyn danych przechowuje informacje o katalogu w pojedynczym pliku bazy danych. Ponadto magazyn danych korzysta także z plików dziennika transakcji, w których zapisuje tymczasowo zadysponowane i niezadysponowane zmiany przed przekazaniem ich do bazy danych.

Zródło: **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str. 23-24

4.1.2. Wykaz globalny

Wykazem globalnym jest partycja przechowująca informacje o wszystkich obiektach w lesie. Taka struktura znajduje się tylko na tych kontrolerach domeny, na których została zaznaczona odpowiednia opcja, tzn. dany kontroler ma być serwerem wykazu globalnego. Dużym jego plusem jest szybsze wyszukiwanie obiektów w domenie bądź miedzy domenami. Administratorzy mogą sami zadecydować, które atrybuty będą replikowane do wykazu globalnego. Dodatkowo serwer takiego wykazu wykorzystywany jest do logowania.

4.1.3. Wzorce operacji

Usługa Active Directory Domain Service jest systemem replikacji z wieloma wzorcami operacji. W replikowanych bazach danych niektóre informacje muszą być zmieniane tylko przez jedną replikację. Kontrolery domeny, które wykonują określone role są nazywane wzorcami operacji. Kontrolery domeny, które pełnią rolę wzorca, wykonują określone zadania, w celu zapewnienia niezawodności i spójności. Służą także do wyeliminowania wpisów w bazie danych AD DS, tych, które powodują niestabilną pracę konflikty. W usługach AD DS można wyróżnić pięć wzorców operacji:

- *Wzorzec schematu*
- *Wzorzec nazw domen*
- *Wzorzec RID*
- *Wzorzec PDC*
- *Wzorzec infrastruktury*

Dodatkowo ten podział dzieli się na jeszcze bardziej szczegółowy. Wzorzec schematu oraz wzorzec nazw domen są rolami, które mogą występować tylko w lesie. Oznacza to, że każdy z nich może być tylko jeden w lesie. Pozostałe trzy wzorce odnoszą się do każdej domeny.

4.1.3.1. Role wzorców, które mogą być tylko w lesie

Wzorzec schematu – w lesie może istnieć tylko jeden kontroler domeny, który pełni rolę wzorca schematu i ma uprawnienia (zapis) do schematu katalogu. Pozostałe kontrolery domeny w lesie otrzymują repliki katalogu schematu tylko do odczytu. Aby zmodyfikować schemat katalogu użytkownik musi należeć do grupy „administratorzy schematu". Ewentualnie grupa, do której należy dany użytkownik musi być członkiem grupy „administratorzy schematu". Wspomniany użytkownik musi być zalogowany do kontrolera domeny pełniącego rolę wzorca schematu.

Wzorzec nazw domen - potrzebny jest do zarządzania i modyfikacji wszystkich partycji katalogu w hierarchii lasu. Kontroler domeny utrzymujący tę rolę musi być dostępny w:

- *Dodawaniu lub usuwaniu domen* - jak sama nazwa wskazuje, ta rola odpowiedzialna jest za dodawanie lub usuwanie domen w lesie. Ponadto odpowiedzialna jest za sprawdzanie nazw domen i dbanie o to, żeby domeny w lesie się nie powtarzały. Jeśli kontroler utrzymujący rolę wzorca nazw domen nie będzie dostępny, nie można dodać bądź usunąć żadnej domeny.
- *Dodawaniu lub usuwaniu partycji katalogu aplikacji* - partycje katalogu aplikacji są to specjalne partycje, które tworzone są na kontrolerach domen po to, by współdzielić magazyn dla aplikacji dynamicznych. Jeśli kontroler domeny pełniący tę rolę jest niedostępny w lesie, niemożliwe jest dodawanie i usuwanie partycji katalogu aplikacji.
- *Dodawaniu lub usuwaniu obiektów wzajemnych odwołań* - gdy tworzony jest nowy las na pierwszym kontrolerze domeny, tworzone są partycja katalogu domeny, jego konfiguracja oraz schemat. Dla wszystkich partycji katalogu w kontenerze „Partycje" tworzony jest obiekt wzajemnych odwołań (cross-reference object). Jeśli tworzona jest nowa domena lub partycje w katalogu aplikacji, to w kontenerze „Partycja" tworzone są także skojarzone odwołania. Gdy ten wzorzec nazw domeny jest niedostępny, nie można tworzyć i modyfikować wzajemnych odwołań.

- *Walidacji instrukcji zmiany nazwy domeny* - podczas zmiany nazwy domeny za pomocą polecenia Rendom.exe narzędzie to musi mieć dostęp do wzorca operacji nazw domen. W trakcie działania tego narzędzia skrypt języka XML zawierający instrukcje zmiany nazwy wprowadza zmiany w atrybucie MSDN-UpdateScript. Nowa nazwa DNS domeny, dla której zmiana nastąpiła jest tak samo zapisywana do atrybutu: MSDN-DnsRootAlias.[1]

4.1.3.2. Role wzorców które mogą być tylko w domenie

Wzorzec RID **-** wzorzec RID jest rolą używaną do zarządzania pulą identyfikatorów RID. Identyfikatory te tworzą nowe podmioty zabezpieczeń w całej domenie. Dla takich podmiotów wydawany jest SID, zawierający identyfikator domeny oraz względny identyfikator RID. Jest on unikalny dla każdego podmiotu zabezpieczeń. Podmioty takie mogą być tworzone na każdym kontrolerze domeny zawierającym kopię katalogu z możliwością jej zapisu. Wzorzec RID uniemożliwi wydanie tego samego identyfikatora RID przez dwa kontrolery. Wzorzec RID wydaje każdemu kontrolerowi tak zwany blok identyfikatorów, które potocznie nazywane są pulą. Jeśli zajdzie taka sytuacja, że na kontrolerze domeny pula zmniejszy się, kontroler domeny wygeneruje zadanie uzyskania kolejnej puli. Gdy nastąpi taka sytuacja, ze wzorzec RID jest nieosiągalny, proces tworzenia nowych podmiotów zabezpieczeń może zakończyć się niepowodzeniem. W celu wyeliminowania tej sytuacji wzorzec RID zaprojektowano tak, aby taka sytuacja nie miała miejsca. Gdy kontroler domeny zauważy ze wyczerpuje mu się pula RID, zgłoszenie generowanie jest o wiele wcześniej.

Wzorzec infrastruktury – ma za zadanie aktualizować odniesienia między domenami (np. grupa-użytkownik). Rola zapewnia, że zmiany w nazwach obiektów znajdą swoje odbicie w informacjach o członkach grup dla grup znajdujących się w innych domenach.

[1] **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str. 32.

Wzorzec utrzymuje pełną aktualną listę tych odniesień a następnie replikuje te informacje do innych kontrolerów domeny.

Emulator PDC – dla systemów operacyjnych starszych niż Windows 2000 niezbędny będzie emulator PDC. Taki emulator daje możliwość komunikowania się z kontrolerem w celu zmiany haseł, ponadto umożliwia replikowanie tychże haseł.

4.1.4. Kontroler domeny tylko do odczytu

Jest to kontroler domeny przeznaczony tylko do odczytu stanowiący innowację, która pojawiła się wraz z premierą systemu Windows Serwer 2008. Utrzymuje ona bazę danych usług, AD DS zawierającą parametr Read Only.

4.2. Struktura logiczna

Struktura logiczna usługi AD DS jest zbudowana z partycji, domen, drzewa domen, lasów, lokacji oraz jednostek organizacyjnych.

4.2.1. Partycje

Baza danych AD DS przechowywana jest w jednym pliku bazy danych.[2] Każda partycja logiczna (zawiera bazę danych katalogu) przechowuje inny typ informacji. Żeby zobaczyć partycje usługi AD DS trzeba skorzystać z narzędzia Ldp.exe, bądź ADSI Edit. Partycje można podzielić na:

- ***Partycję katalogu*** **domeny -** partycja ta posiada wszelkie wiadomości o domenie W skład tych informacji wchodzą użytkownicy, komputery, grupy, kontakty. Wszystko to, co można przeglądać za pomocą narzędzia Active Directory Users And

[2] **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str. 45.

Computers znajduje się w partycji katalogu domeny, która jest automatycznie kopiowana do każdego kontrolera w domenie.

- ***Partycję katalogu konfiguracji*** **–** która mieści w sobie dane o ustawieniach całego lasu. W niej przechowywane są dane o połączeniach replikacji, łączach lokacji i lokacjach. Inne aplikacje, takie jak Exchange Server 2007 również przechowują w tej partycji informacje. Partycja ta jest kopiowana w całym lesie. Na wszystkich kontrolerach domeny znajduje się kopia danej partycji z możliwością zapisu. Edycja partycji jest możliwa na dowolnym kontrolerze domeny. Oznacza to, że poszczególny kontroler domeny w lesie będzie dysponował tymi samymi danymi o ustawieniach w tej partycji.
- ***Partycję katalogu schematu*** - przechowuje schemat całego lasu, który jest zbiorem reguł określających poszczególne typy obiektów, które mogą być tworzone w AD DS. Dodatkowo partycja ta zawiera zasady opisujące każdy rodzaj obiektu w lesie. Partycja ta jest kopiowana do każdego kontrolera domeny w całym lesie. Kontroler domeny, który pełni rolę wzorca schematu przechowuje kopię, dzięki której można zapisać zmiany.
- ***Partycję wykazu globalnego*** - ten typ partycji ma inne znaczenie niż pozostałe. Pomimo, że mieści się ona w bazie danych, administratorzy nie mogą zmieniać zawartych w niej informacji, ponieważ służy ona tylko do odczytywania informacji.
- **Partycje katalogu aplikacji:** jest to partycja, która pozwala przechowywać dane dosyć specyficzne dla aplikacji użytkowych.

4.2.2. Domeny

Domena jest jednostką administracyjną, która definiuje granice zasad zabezpieczeń. W usługach AD DS domeny określają następujące granice:

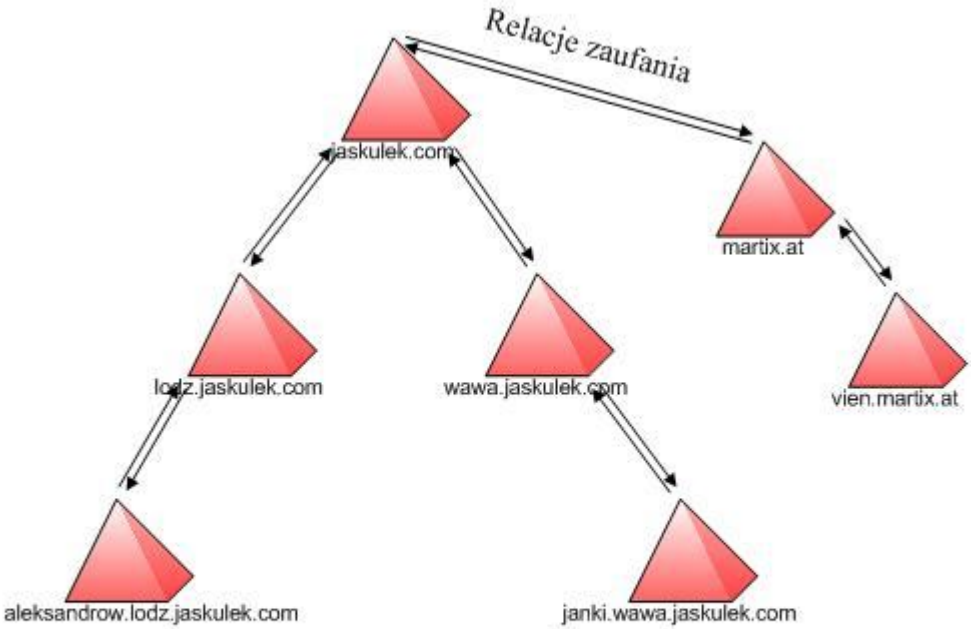
- Granice replikacji
- Granice zasad ubezpieczeń
- Granice dostępu do zasobów
- Granice zaufania

4.2.3. Las

Las to zespół jednej bądź większej ilości domen. Jest on granicą zabezpieczeń dla całego przedsiębiorstwa. Las AD DS może być określony przez składniki wszystkich kontrolerów domen lasu, do których należą:

- ***Wspólny schemat*** – jest identyczny dla wszystkich kontrolerów i przechowywany w odpowiedniej partycji.
- ***Wspólny wykaz globalny -*** wykaz globalny (patrz rozdział 4.1.2.) zawiera dane o poszczególnych obiektach jakie występują w lesie.
- ***Wspólna partycja katalogu konfiguracji -*** każdy kontroler domeny ma identyczny kontroler konfiguracji. Partycja ta zawiera informacje o wszelakich ustawieniach lasu, kontrolerów domen oraz samych domen. Do wyżej wspomnianych informacji można zaliczyć: listę wszystkich lasów, domen i drzew oraz dane o umiejscowieniu wykazów globalnych a także kontrolerów domen. Dodatkowo partycja ta używana jest przez inne aplikacje np. Exchange Server.
- ***Wspólny w całym lesie zestaw wzorców operacji i administratorów -*** wzorce nazw schematu i domen mogą działać tylko na poziomie lasu. W każdym lesie może być tylko jeden wzorzec schematu i nazw. W domenie głównej lasu automatycznie tworzone są dwie grupy zabezpieczeń: grupa administratorzy schematu i administratorzy przedsiębiorstwa. Pierwsza z nich może zmieniać istniejący schemat, druga zaś ma uprawnienia do realizacji działań na poziomie lasu.
- ***Współużytkowana konfiguracja konfiguracji relacji zaufania -*** kiedy tworzy się domeny lasu zostają one automatycznie skonfigurowane, by mogły sobie wzajemnie ufać. Poniższy rysunek przedstawia przykładowy las dla przedsiębiorstwa „Jaskulek”. Ukazuje on las z wieloma domenami.

Rysunek nr 2 Przykładowy las ukazujący relacje zaufania



Źródło: Opracowanie własne na podstawie **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit*, Microsoft Press, Warszawa 2008

Relacje zaufania: jeśli nie zostaną one skonfigurowane, granicą dostępu do zasobów w firmie będzie tylko domena. Dzięki odpowiednim uprawnieniom dowolnych podmiotów zabezpieczeń, istnieje możliwość przeglądania udostępnionych zasobów w tej samej domenie. Aby uzyskać dostęp do zasobów w innej domenie musimy również wykorzystać relacje zaufania. Takie relacje, to połączenie uwierzytelnienia pomiędzy dwiema domenami. Jeśli miedzy nimi została ustawiona relacja zaufania, mechanizm uwierzytelniania każdej domeny ufa mechanizmowymi uwierzytelniania wszystkim innym zaufanym domenom. Poniżej wyminie kilka typów relacji zaufania.

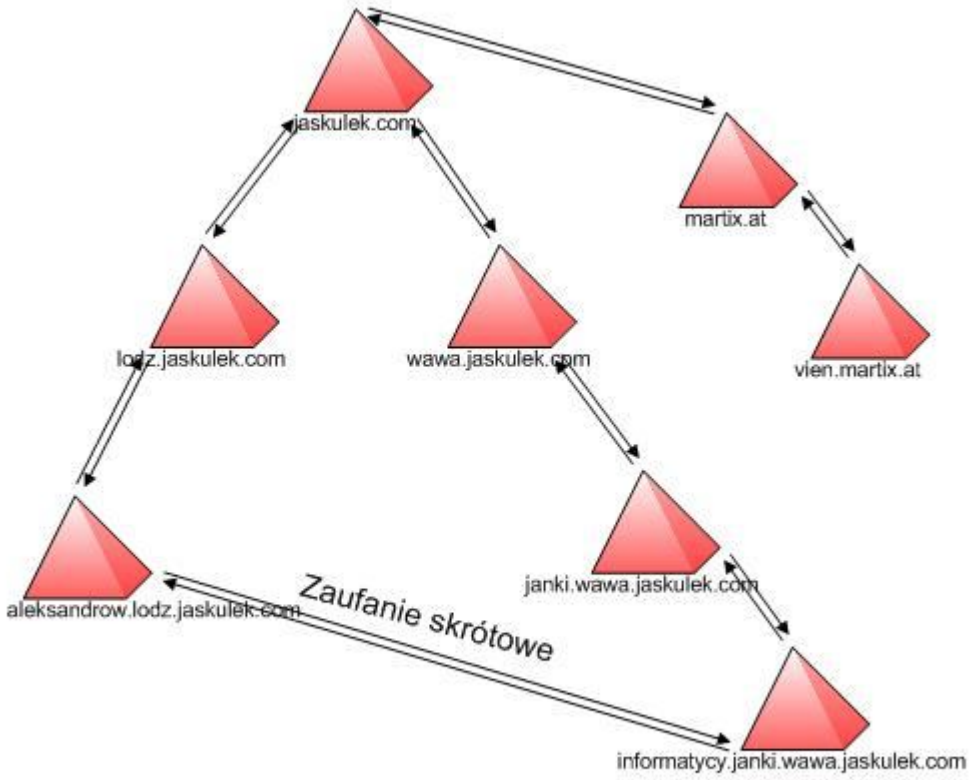
Przechodnie dwukierunkowe relacje zaufania: kiedy do lasu dodawana jest nowa domena, automatycznie tworzone są przechodnie dwukierunkowe relacje zaufania. Te relacje zaufania tworzone są miedzy domeną nadrzędną i podrzędną. Relacje te wykorzystywane są w sytuacji kiedy użytkownik w domenie „lodz.jaskulek.com" jest w stanie uzyskać dostęp do wszystkich zasobów w domenie „jaskulek.com". Dodatkowa rzeczą o której warto wspomnieć jest to, że: relacje zaufania pomiędzy domenami w jednym lesie są „przechodnie". Mianem

„przechodnie” określić można wszystkie domeny istniejące w lesie i ufające sobie wzajemnie. Przechodnie relacje zaufania stosowane są też do głównych zaufań drzewa. Polega to na tym, że domena „jaskulek.com” ufa domenie „matrix.at”.

Relacje zaufania skrótu **-** relacje tego typu nie są tworzone automatycznie jak w przypadku relacji zaufania, które zostały opisane powyżej. Jeśli mamy do czynienia z relacjami skrótu dochodzimy do wniosku, że te relacje będą konfigurowane i ustawiane osobiście przez administratora. Relacji zaufania używamy również wtedy, kiedy chcemy wywołać spójną relację pomiędzy dwoma domenami, które są domenami podrzędnymi.

Oto przykładowa relacja między wyżej wymienionymi domenami. Założyć można, że dowolna grupa w domenie „aleksandrów.lodz.jaskulek.com” bardzo często potrzebuje mieć dostęp do udostępnionych zasobów w domenie „informatycy.janki.warzawsza.jaskulek.com. Dzięki skrótowym relacją zaufania pomiędzy tymi dwoma domenami, w których została skonfigurowana taka relacja, użytkownicy nie muszą odnosić się do każdego kontrolera domeny, który znajduje się pomiędzy tymi dwiema domenami w danym drzewie. (jak to ma miejsce w przypadku relacji dwukierunkowych). Relacja dwukierunkowa nie byłaby w tym przypadku efektywna. Relacja skrótu zapewni bezpośredni dostęp do danych miedzy tymi dwoma domenami, dzięki temu dostęp do zasobów będzie szybszy.

Rysunek nr 3 Przykładowy las ukazujący relacje skrótowe



Projekt własny na podstawie **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008

Relacje zaufania lasów To dwukierunkowa i przechodnia relacja zaufania pomiędzy dwoma lasami. Kiedy zostanie ona skonfigurowana podmioty zabezpieczeń w lesie „A" mogą mieć dostęp do zasobów w domenie innego lasu. Dodatkowo każdy użytkownik ma możliwość logowania się w każdej istniejącej domenie obu lasów, miedzy którymi istnieje relacja zaufania lasów, używając do tego tej samej nazwy UPN.

Relacje zaufania lasów mają następujące ograniczenia:

- ***Relacje zaufania lasów nie są przechodnie*** – oznacza to, że konfigurując relacje zaufania miedzy lasami „jaskulek.com" a „kaja.at", dodatkowo skonfigurowana została relacja miedzy lasami „kaja.at' i „karolina.at". To relacja między lasami jaskulek.com a „karolina.at" nie zostanie automatycznie skonfigurowana.
- ***Relacje zaufania lasów pomiędzy sobą umożliwiania jedynie uwierzytelnienie*** **-** oznacza to że pomiędzy lasami gdzie została skonfigurowana ta relacja. nie

są replikowane żadne pliki konfiguracyjne. Każdy z lasów będzie miał swój wykaz globalny, własny schemat.

- ***Zewnętrzne relacje zaufania:*** relacja ta wykorzystywana jest do połączenia domen które znajdują się w rożnych lasach. Relacje te mogą również posłużyć do połączenia struktury AD DS. z domeną systemów starszych typów.
- ***Relacje zaufania obszaru***: konfigurowane są pomiędzy instancją Windows Server 2008 a obszarem protokołu Kerberos w wersji 5, różnym od tego zainstalowanego w systemie Windows

4.2.4. Lokacje

Lokację można tłumaczyć jako oddział przedsiębiorstwa. Najczęściej jest to fizyczne biuro bądź miasto. Źródła Microsoftu definiują lokacje jako obszar sieci, w której występuje kontroler domeny. Dodatkowo można dodać, że lokacja zawiera jedna lub kilka podsieci w sieci lokalnej. I lokacja połączona jest z resztą sieci poprzez wolne łącza WAN. Powodem dla którego warto myśleć nad tworzeniem lokacji jest możliwość administrowania ruchem miedzy oddziałem a centralą przedsiębiorstwa. Takie połączenia są bardzo drogie i powolne. W takim przypadku można myśleć o wprowadzeniu kontrolera domeny w oddziale. Należy zaznaczyć również, że lokacje umożliwiają administrowanie ruchem w sieci, natomiast wewnątrz sieci systemu Windows lokacje używają trzech metod do kontrolowania ruchu. Metody te to:

- Replikacja
- Uwierzytelnienie
- Usługi sieci rozpoznające lokacje

4.2.5. Jednostki organizacyjne

Jednostki organizacyjne - w skrócie (OU), skrót pochodzi od anglojęzycznej nazwy Organization Unit. Jest to kontener na obiekty w AD DS. Jednostka organizacyjna nie jest tylko kontenerem dla obiektów, ale jest również zakresem zarządzania obiektami. Struktura hierarchiczna pozwala tworzyć modyfikowalne jednostki organizacyjne. Do każdej OU można podłączyć obiekt zwany (GPO), W obiekcie (GPO) jest możliwość zastosowania dowolnych ustawień zabezpieczeń i konfiguracji, które będą stosowane przez komputery i użytkowników w (OU). Jednostki organizacyjne mogą zawierać w sobie kilka typów obiektów: *Komputery, kontakty, grupy, konta inetOrgPerson, drukarki, użytkowników, foldery udostępnione, jak również jednostki organizacyjne.*

4.2.6. Poziom funkcjonalności

Poziom funkcjonalności - funkcjonalność która, jest dostępna w lesie lub domenie. Określa, jakie funkcje będą dostępne dla danego lasu, bądź domeny. W rozdziale poświeconym projektowi zostaną przedstawione poszczególne dostępne poziomy funkcjonalności lasu i domeny.

4.2.7. Drzewa domen

Drzewa Domen - jest to przestrzeń nazw DNS dla domeny. Na przykład jeśli w firmie „Jaskulek" znajdowałyby się następujące domeny „jaskulek.com" i „lodz.jaskulek.com", to te dwie domeny byłyby ciągłym fragmentem przestrzeni nazw DNS.

4.3. Dodatkowe role

Poza usługa AD DS, w systemie Windows Server 2008 R2, istnieje możliwość zainstalowania dodatkowych ról, które są powiązane z usługą AD DS.

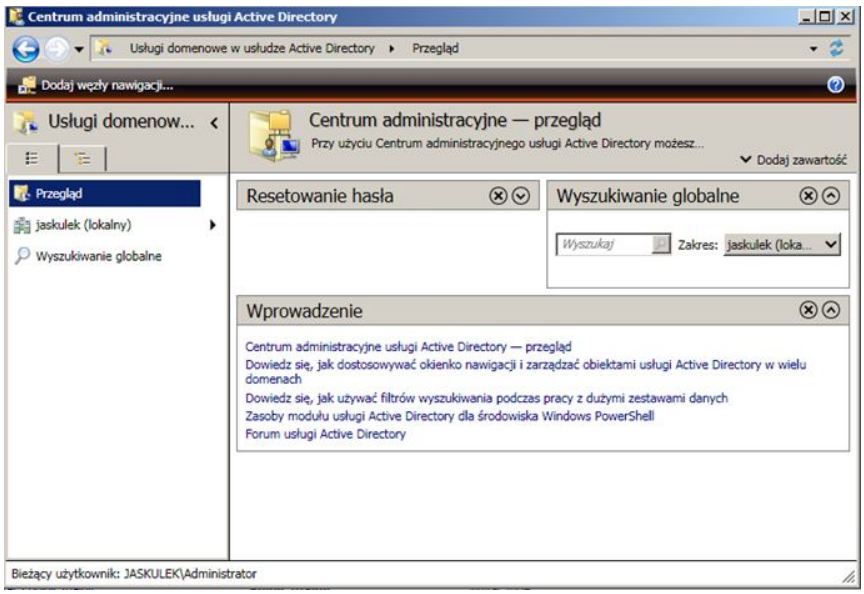
- AD CE Active Directory Certificate Services
- AD FS Active Directory Federation Services
- AD LDS Active Directory Lightweight Directory Services
- AD RMS Active Directory Rights Management Services

4.4. Narzędzia administracyjne[4]

W tym rozdziale zostaną omówione podstawowe narzędzia do administrowania AD DS. Można je podzielić na: graficzne, wiersza poleceń, polecenia cmd, skrypty PowerShell oraz programy pomocnicze. Narzędzia graficzne, które są najczęściej stosowane do administrowania usługą AD DS., to:

- *Centrum administracyjne usługi Active Directory:* jest to nowe narzędzie które firma Microsoft wprowadziła w systemie Windows Server 2008 R2. Narzędzie to daje możliwość zarządzania użytkownikami, komputerami, grupami, jednostkami organizacyjnymi. Narzędzie to poniekąd może przypominać narzędzie „Komputery i użytkownicy Active Directory". Dodatkowo narzędzie to pozwala na wykonywaniu globalnych wyszukiwań w domenie. Ciekawostką jest to ze istnieje możliwość skorzystania z tego narzędzia w systemie Windows 7.

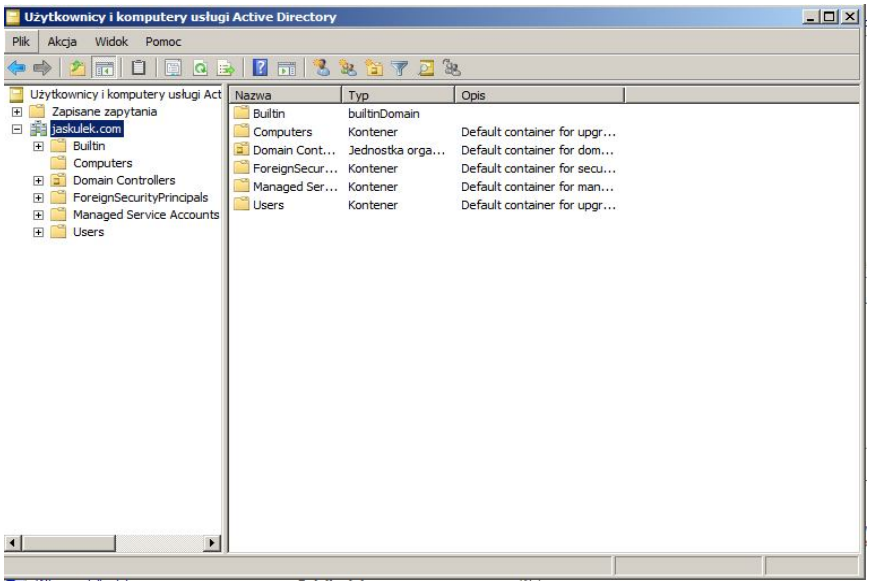
Rysunek nr 4 Centrum administracyjne usługi Active Directory



Źródło: *opracowanie własne*

- *Komputery i użytkownicy Active Directory.* Narzędzie to daje możliwość dodawania, usuwania, modyfikowania(użytkownikami, komputerami, grupami oraz jednostkami organizacyjnymi). Obrazek () przedstawia wygląd narzędzia.

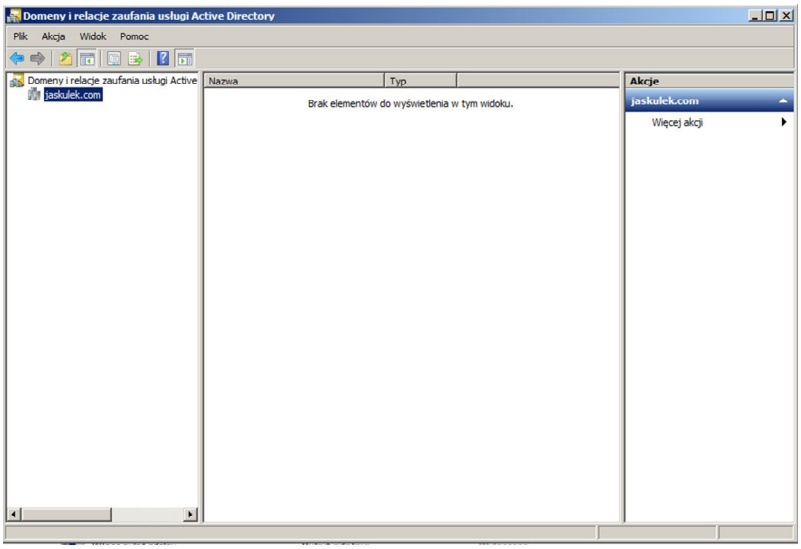
Rysunek nr 5 Komputery i użytkownicy Active Directory



Źródło: *opracowanie własne*

- *Domeny i relacje zaufania Active Directory* umożliwią pracę z domenami, drzewami oraz lasami.

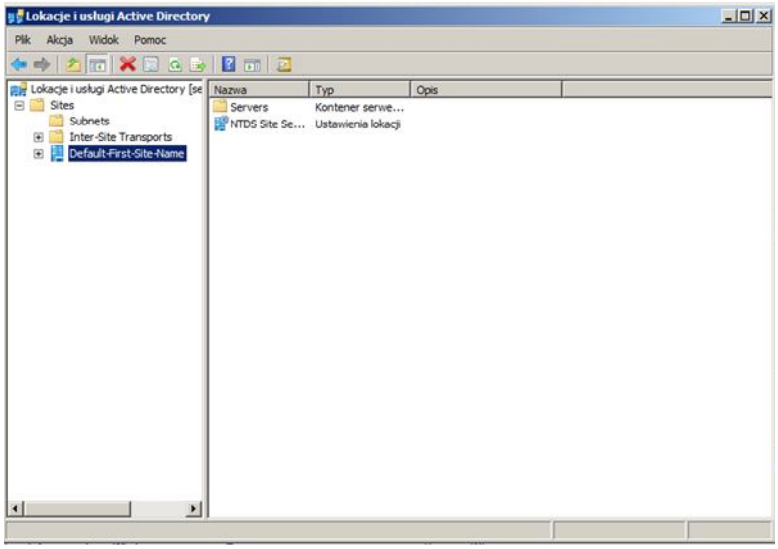
Rysunek nr 6 Domeny i relacje zaufania Active Directory



Źródło: *opracowanie własne*

- *Lokacje i usługi Active Directory* daję możliwość konfiguracji lokacji i podsieci.

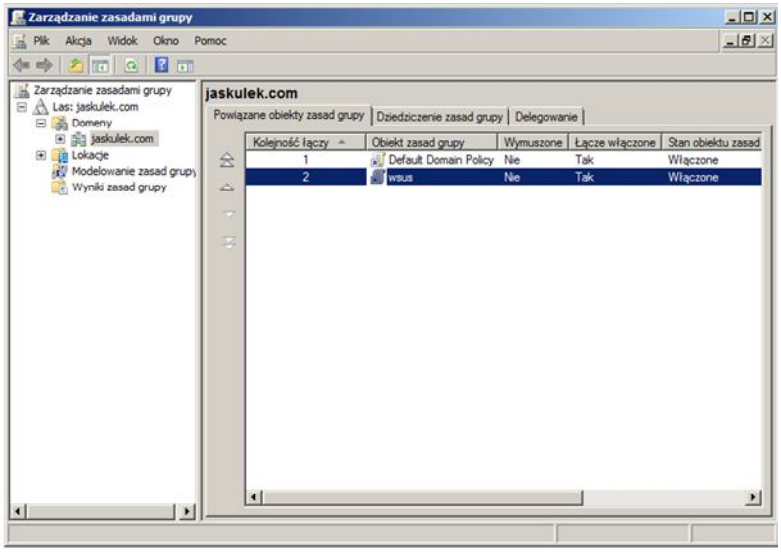
Rysunek nr 7 Lokacje i usługi Active Directory



Źródło: *opracowanie własne*

- *Konsola zarządzania zasad grupy:* to bardzo zaawansowane narzędzie, pozwalające na konfigurację metod stosowania zasad grup w przedsiębiorstwie.

Rysunek nr 8 Konsola zarządzania zasad grupy



Źródło: *opracowanie własne*

Rozdział 5
PROJEKT USŁUG

Rozdział piąty poświecę na projekt, zawierający usługi takie jak: AD DS, WDS, WSUS, DNS, DHCP. Dodatkowo opiszę proces projektowania usługi AD DS, zanim zostaną zainstalowane i skonfigurowane usługi AD DS.

Przed przystąpieniem do każdego projektu usług AD DS bardzo ważnym krokiem jest analiza aktualnego środowiska sieci i katalogu w przedsiębiorstwie. Taka analiza ułatwi późniejszy proces przebiegu projektu AD DS. Na taka analizę składają się następujące informacje:

Udokumentowanie sieci fizycznej

Udokumentowanie infrastruktury rozpoznawania nazw

Udokumentowanie infrastruktury Active Directory

Udokumentowanie dodatkowych składników infrastruktury

Udokumentowanie sieci fizycznej modeli i procesów administracyjnych[3]

W tej części opiszę szczegóły poszczególnych punktów oraz zbiorę informacje od Zarządu firmy „Jaskulek", które później pomogą mi w projekcie usługi jaką jest AD DS. Ponieważ w głównej siedzibie firmy „Jaskulek" aktualnie nie jest uruchomiona żadna usługa, etap ten częściowo będzie tylko teoretyczny. Przedstawię informacje jakie należałoby zgromadzić, gdyby w przedsiębiorstwie istniały zainstalowane usługi.

Analizę aktualnego środowiska powinno zacząć się od udokumentowania sieci fizycznej. Proces ten należy zacząć od zebrania informacji o wszystkich budynkach, oddziałach firmy. Przy dokumentowaniu oddziałów firmy należy również uwzględnić ilość pracowników w danym oddziale, czy sposób zabezpieczania takiego oddziału. Ważną rzeczą podczas dokumentowania informacji o oddziałach jest również informacja o typie połączeń oraz prędkości łącz miedzy oddziałem a centralą,

[3] **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str. 159.

Zbierając informacje na temat firmy „Jaskulek” stwierdziłem, że przedsiębiorstwo nie posiada żadnych oddziałów regionalnych. Centrala firmy mieści się tylko w jednym budynku. W tym wypadku nie będzie oczywiście dokumentacji informującej o oddziałach, czy rodzaju wykorzystywanych łącz telekomunikacyjnych.

Następnym krokiem związanym z analizą aktualnego środowiska jest udokumentowanie infrastruktury rozpoznawania nazw. System DNS jest bardzo ważną usługa dla usługi AD DS. AD DS wykorzystuje DNS do wyszukiwania innych kontrolerów domen oraz do lokalizowania kontrolerów domen przez komputery klienckie. Dlatego proces udokumentowania tej infrastruktury jest bardzo ważny. Ten rodzaj infrastruktury polega na sporządzeniu listy jakiej aktualnie używają systemy DNS i sprawdzeniu czy systemy te będą w stanie obsłużyć rekord (SRV). Następnym etapem jest ustalenie, kto zarządza serwerami, na których został zainstalowany system DNS, gdyż trzeba ustalić gdzie znajdują się serwery DNS odpowiedzialne za rozpoznawanie wewnętrznych nazw. Należy również ustalić, jaka jest bieżąca konfiguracja systemu DNS tzn: liczbę przestrzeni adresowych, sposób użycia wskazówek dotyczących serwerów głównych, usługi przesyłania dalej, usługi warunkowego przesyłania dalej, strefy skrótów i delegowania. Ostatnią rzeczą jaką należy ustalić, to czy usługa ta jest już zintegrowana z systemem DNS.

Posiłkując się listą ustaloną na początku tego rozdziału można zauważyć, że kolejnym etapem mojego projektu będzie dokumentacja infrastruktury usługi Active Directory. Dokumentując infrastrukturę Active Directory należy zebrać informacje o ilości lasów i ilości domen zainstalowanych w poszczególnym lesie. Dokumentując lasy należy zebrać informacje dotyczące wykorzystywania lasów oraz jakie celów tworzenia lasu. Jeśli w przedsiębiorstwie znajduje się wiele lasów trzeba określić, czy założenia, które zostały wcześniej sporządzone są aktualne. Opisując domeny należy zebrać informacje do czego dana domena jest wykorzystywana oraz zapoznać się z celami dla jakich została wcześniej utworzona. Ważne jest także to czy te cele są jeszcze aktualne. Jeśli zostały zebrane już informacje o lasach i domenach kolejnym etapem jest dokumentacja relacji zaufania. Należy zebrać wszystkie informacje o skonfigurowanych relacjach zaufania oraz powody dla których ktoś wcześniej je skonfigurował. Następnie określić, czy przyczyny, dla których relacje zostały wcześniej zaimplementowane są jeszcze aktualne. Kolejną rzeczą, którą należy ustalić, to poziom funkcjonalności lasów i domen. Po udokumentowaniu poziomu funkcjonalności, należy

zebrać informacje o lokacjach. W procesie dokumentacji lokacji zawiera się ilość lokacji, informacje o podsieciach, o kosztach łączy i harmonogramu replikacji. Ważną rzeczą wymagającą udokumentowania jest konfiguracja jednostek organizacyjnych, konfiguracja zasad grup oraz grup użytkowników. Na proces dokumentacji zasad grup składa się ich przeznaczenie, ustawienia obiektów, dziedziczenia oraz informacja dla jakiego podmiotu one są ustawione. Dokumentując grupy należy uaktualnić ich konfigurację.

Dokumentując dodatkowe składniki infrastruktury konieczne będzie zgromadzenie informacji o aktualnie wykorzystywanych programach w przedsiębiorstwie. Etap ten można podzielić na kilka części, z których najważniejszą jest informacja, czy w przedsiębiorstwie został zaimplementowany program Exchange Server. Jeśli tak, to trzeba udokumentować całą jego infrastrukturę. Niezbędna także będzie dokumentacja programów, które korzystają ze schematu Active Directory, sposób przywracania po awarii (dokumentacja o używanych technologiach zapasowych) i dokumentacja wszystkich aplikacji, które są wykorzystywane w przedsiębiorstwie.

Ostatnim etapem procesu dokumentacji aktualnego środowiska jest udokumentowanie modeli i procesów administracyjnych. Etap ten polega na pełnej dokumentacji struktury administracyjnej. Proces ten można podzielić na kilka mniejszych etapów. Pierwszym jest aktualny model administracyjny firmy. Tutaj należy stwierdzić, iż ważne jest określenie, czy administracja IT jest scentralizowana, czy poszczególne regiony maja swój własny dział IT. Drugi etap tyczy sie określenia modelu administracyjnego kont użytkowników. Należy określić, czy istnieje pojedyncza grupa dla wszystkich ról związanych z zarządzaniem kontami użytkowników bądź czy każdy dział przedsiębiorstwa ma jedną osobę, która jest za to odpowiedzialna. Nie można pominąć udokumentowania poszczególnych działów w przedsiębiorstwie. Nie będzie to szczegółowy opis stosunków miedzy poszczególnymi działami w firmie, natomiast przydatne mogą być podstawowe informacje. Będzie można je wykorzystać do planowania wdrożenia kilku lasów. Dokumentowanie tego podetapu polega na ustaleniu granic bezpieczeństwa miedzy oddziałami. Należy sprawdzić czy jakiś dział ma swoje własne granice bezpieczeństwa i chce je odizolować, a być może dla wszystkich działów istnieje tylko jedna granica bezpieczeństwa. Należy również uwzględnić jak wygląda komunikacja miedzy działami. [1]

5.1. Projekt AD DS

Projekt usługi AD DS. można podzielić na kilka etapów:

5.1.1. Projektowanie lasu

Projektowanie lasu - Pierwszą najważniejszą decyzją przy projektowaniu usługi AD DS jest określenie ilości lasów. Microsoft zaprojektował las usług AD DS tak, by, las stanowił niezależną jednostkę. Ilość lasów zależy od tego, co dla firmy „Jaskulek" jest najważniejsze. Wybranie jednego lasu w usłudze AD DS, usprawni współużytkowanie i łatwiejszy dostęp do danych wewnątrz firmy „Jaskulek". Wybranie kilku lasów umożliwi utrzymane pełnej izolowanej kontroli nad częścią firmy. Przed podjęciem ostatecznej decyzji ile będzie lasów w AD DS. wymienię powody, dla których można zastanawiać się nad instalacją kilku lasów.

Tabela nr 4 Powody dla których warto instalować kilka lasów
Niektóre przedsiębiorstwa instalują oddzielne lasy usług AD DS. w sieciach obwodowych (lub DMZ). Większość organizacji instaluje w sieci obwodowej serwery, które muszą być bezpośrednio dostępne z sieci Internet, aby zapewnić dodatkowy poziom bezpieczeństwa dla sieci wewnętrznej. Serwery te mogą być instalowane jak serwery autonomiczne, ale poprzez zainstalowanie oddzielnego lasu usług AD DS. w sieci obwodowej można korzystać z zalet funkcji zarządzania komputerami i użytkownikami udostępnianych przez usługi AD DS. i jednocześnie zachować izolacje od wewnętrznego lasu usług AD DS.
Niektóre przedsiębiorstwa nie maja silnych wymagań dotyczących współpracy z innymi przedsiębiorstwami . W niektórych przypadkach jednostki biznesowe działają prawie niezależnie od innych, przy niewielkich potrzebach dotyczących wymiany informacji innych niż poczta e-mail. Przedsiębiorstwa te nie tracą niczego poprzez zainstalowanie wielu lasów
W niektórych przedsiębiorstwach wymagana jest pełna separacja informacji w sieci. Ze względów bezpieczeństwa lub ze względów prawnych przedsiębiorstwo musi zapewnić, że niektóre informacje w sieci nie mogą być dostępne dla nikogo poza jednostką biznesową. Domyślnie informacje jednego lasu nie są widoczne w żadnym innym lesie.
W niektórych przedsiębiorstwach wymagane są niekompatybilne konfiguracje schematu. Jeśli w dwóch częściach organizacji wymagane jest stosowanie unikatowego schematu, ponieważ instalowane są aplikacje, które wykonują niezgodne modyfikacje schematu, trzeba utworzyć oddzielne lasy.
W niektórych przedsiębiorstwach nie do zaakceptowania są procedury scentralizowanej administracji. Jeśli jednostki biznesowe nie mogą zgodzić się na zasady kontroli zmian lasu lub schematu lub jeśli nie mogą zgodzić sie na scentralizowaną administrację, to będzie konieczne zainstalowanie oddzielnych lasów.
W niektórych przedsiębiorstwach zachodzi konieczność ograniczania zakresu relacji zaufania wewnątrz lasu wszystkie domeny współużytkują przechodnie relacje zaufania i nie istnieje żadna operacja, która może zmienić te konfigurację. Jeśli w danym środowisku wymagana jest konfiguracja relacji zaufania inna niż dwukierunkowe relacje przechodnie pomiędzy wszystkimi domenami, to trzeba zainstalować wiele lasów

Zródło: **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008

W przypadku instalowania wielu lasów należałoby zaprojektować modele projektu lasów oraz relacje zaufania lasów. Model projektu lasu składa się z trzech opcji do wyboru.

- Ograniczony model lasu
- Model lasu zasobów
- Model lasu z ograniczonym dostępem[4]

Do projektu relacji zaufania lasu zaliczałoby się zaprojektowanie kierunku relacji zaufania lasu, uwierzytelnienia selektywnego, filtrowania identyfikatora SID, routingu sufiksu nazwy UPN. Po wyborze ilości lasów następnym krokiem, który związany jest z tą częścią projektu jest wybranie poziomu funkcjonalności lasu.

[4] **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str. 173.

Tabela nr 5 Poziomy funkcjonalności lasu

Poziom	Funkcje	Obsługiwane kontrolery domeny
Windows Server 2000	Wszystkie domyślne funkcje usługi AD	Windows Server 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2003	Wszystkie domyślne funkcje usługi AD, plus nowe: • Relacje zaufania lasu • Zmiana nazwy domeny • Możliwość instalowania kontrolerów domeny tylko do odczytu(RODC), które działają w systemie Windows Server 2008 • Poprawione algorytmy i skalowalność usług KCC • Możliwość tworzenia instalacji dynamicznych klas pomocniczych nazywanych dynamicObject w partycji katalogu domeny • Możliwość konwersji instalacji obiektu inetOrgPerson do instalacji obiektu User i odwrotnie • Dezaktywacja i ponowne definiowanie atrybutów i klas schematu.	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2008	Wszystkie domyślne funkcje usługi AD na poziomie lasu systemu Windows Server 2003, żadnych nowych dodatkowych funkcji.	Windows Server 2008 Windows Server 2008 R2
Windows Server 2008 R2	Poziom funkcjonalności lasu systemu Windows Server 2008 R2 zapewnia wszystkie funkcje dostępne na poziomie funkcjonalności lasu systemu Windows Server 2008 oraz następującą dodatkową funkcję: • Kosz, który po włączeniu umożliwia przywracanie usuniętych obiektów w całości podczas działania usług domenowych w usłudze Active Directory.	Windows Server 2008 R2

Zródło: **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str. 193

Analizując informacje o przedsiębiorstwie „Jaskulek" zadecydowałem, że najlepszym rozwiązaniem dla tej firmy, będzie instalowanie jednego lasu. Ponieważ firma ta posiada charakterystykę scentralizowaną, w tym przypadku nie ma potrzeby instalowania wielu

lasów. Dodatkowo firmie zależy, żeby jej zasoby i współużytkowanie było stosunkowo łatwe w całym przedsiębiorstwie. Dlatego instalowanie jednego lasu w firmie „Jaskulek" jest idealnym rozwiązaniem. Kolejną rzeczą na jaką należy zwrócić uwagę jest wybór poziomu funkcjonalnego lasu. Jak już wcześniej przedstawiłem w tabeli 5, Windows Server 2008 R2 udostępnia kilka poziomów. W firmie „Jaskulek" nie znajduje się żaden kontroler domeny. Zadecydowałem, że najlepszym rozwiązaniem dla tej firmy będzie poziom funkcjonalności lasu na poziomie Windows Server 2008 R2.

5.1.2. Projektowanie domeny

Projektowanie domeny jest następnym etapem projektowania usługi AD DS. Domen można używać do podzielenia lasu na mniejsze składniki. Jeżeli chodzi o wybór ilości domen, nie jest to już tak proste jak w przypadku wyboru ilości lasów. Tabela poniżej przestawi porównanie słuszności instalacji jednej lub wielu domen..

Tabela nr 6 Wybór ilości domen

Wybór pojedynczej	Wybór wielu domen
Magazyn domen może bez problemu zawierać ponad milin obiektów, co oznacza, że liczba obiektów AD DS. bardzo rzadko jest powodem tworzenia wielu domen.	Należy ograniczyć ruch replikacji. Partycja katalogu domeny, która jest najważniejsza i najczęściej modyfikowana, jest replikowana do wszystkich kontrolerów domeny w danej domenie. Również do wszystkich kontrolerów danej domeny replikowany jest folder SYSVOL. W niektórych przypadkach może to generować zbyt duży ruch replikacji pomiędzy lokalizacjami firmy. To może stać się problemem, jeśli używana są wolne połączenia sieci pomiędzy lokalizacjami firmy lub jeśli w wielu lokalizacjach firmy jest duża liczna użytkowników. Jednym sposobem ograniczenia tego ruchu replikacji jest utworzenie dodatkowych domen.
Jeśli przedsiębiorstwo jest często reorganizowane lub jeśli użytkownicy przenoszą się pomiędzy jednostkami biznesowymi, to łatwo można ich przenosić pomiędzy jednostkami organizacyjnymi w domenie. Przenoszenie użytkowników pomiędzy domenami jest znacznie trudniejsze.	W niektórych lokalizacjach używany jest protokół SMTP. Wszystkie firmy w których używana jest łączność w oparciu o SMTP, musza być skonfigurowane jako oddzielne domeny. Partycje domeny nie mogą być replikowane poprzez łącza lokacji, które używają SMTP.
Łatwiejsze jest zarządzanie pojedynczymi domenami, ponieważ problemy związane są z jednym zestawem administratorów i jednym zestawem zasad na poziomie domeny. Ponadto zarządzany jest tylko jeden zestaw kontrolerów domen.	Wymagane są różne zasady haseł. jedynym sposobem używania różnych zasad hasła, różnych zasad blokady konta i biletów protokołu Kerberos jest instalowanie oddzielnych domen. Pomimo ze w pojedynczej domenie można skonfigurować dokładne zasady hasła w celu zmodyfikowania zasad hasła dla niektórych użytkowników to zarządzanie różnymi zasadami haseł dla kilku grup osób w tej samej domenie będzie wymagało dodatkowego nakładu pracy administracyjnej.
Najprostszym scenariuszem zarządzania zasadami grupy jest środowisko pojedynczej domeny. Niektóre składniki zasad grupy są przechowywane w folderze SYSVOL na każdym kontrolerze domeny w danej domenie. Jeśli istnieje tylko jedna domena , obiekty zasad grupy są automatycznie replikowane do wszystkich kontrolerów domen.	Dostęp musi być ograniczony. Jeśli zachodzi potrzeba ograniczenia dostępu do zasobów i uprawnień administracyjnych, trzeba zainstalować dodatkowe domeny. W przypadku niektórych firm mogą również istnieć regulacje ustawowe, dla których trzeba tworzyć oddzielne jednostki administracyjne.
Pojedyncza domena zapewnia najprostsze środowisko do zaprojektowania uwierzytelnienia i dostępu do zasobów. W przypadku pojedynczej domeny nie trzeba analizować relacji zaufania lub przypisywania dostępu do zasobów dla użytkowników w innych domenach. Wewnątrz jednej domeny praktycznie jest również stosowanie tylko jednej grupy, do której przypisywany jest dostęp do zasobów, a nie konfigurowanie zarówno kont jak i grup zasobów.	Dla różnych jednostek biznesowych wymagane są oddzielne przestrzenie nazw. podczas łączenia się organizacji, dla wszystkich jednostek biznesowych może być istotną kwestią utrzymanie unikalnej tożsamości. Poprzez zainstalowanie wielu domen w różnych drzewach dla każdej domeny można utrzymywać unikalne przestrzenie nazw.
W pojedynczej domenie, wszystkie kontrolery domeny mogą być serwerami wykazu globalnego, ponieważ nie są stosowane ograniczenia wzorca infrastruktury. Oznacza to ze nie trzeba planować rozmieszczenia wykazu globalnego.	Dla organizacji najlepszym sposobem przeprowadzenia migracji jest aktualizacja kilku aktualnie utrzymywanych domen.

Zródło: **Reimer S., Kezema C., Molar M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit*, Microsoft Press, Warszawa 2008, 183-184

Podczas instalowania wielu domen należy ustalić, czy instalować dedykowaną domenę główną (empty Root). Gdy przedsiębiorstwo zdecyduje się na taką instalację, wynikną z tego następujące korzyści:[1]

Tabela nr 7 Korzyści wynikające z instalacji dedykowanej domeny

Domena główna zawiera grupy administracyjne poziomy lasu - Administratorzy przedsiębiorstwa i Administratorzy schematu – i kontrolery domeny wzorca operacji poziomu lasu(wzorzec nazw domeny i wzorzec schematu). Używanie dedykowanej domeny głównej ułatwia również ograniczenie członkostwa grup administracyjnych poziomu lasu. Nawet jeśli ściśle ograniczona zostanie liczba administratorów w grupach Schema Admins i Enterprise Admins, wszyscy członkowie grupy Domain Admins w domenie głównej lasu mogą modyfikować listy tych grup.
Dedykowana domena Głowna może być prosto replikowana do innych lokacji. Domena Głowna lasu musi być zawsze dostępna podczas logowania użytkowników do domen innych niż ich domenach macierzyste lub podczas uzyskiwania dostępu do zasobów w innych domenach. Ponieważ nie zachodzi potrzeba częstego modyfikowania magazynu danych dedykowanej domeny głównej lasy, prawie w ogóle nie występuje ruch replikacji pomiędzy kontrolerami domeny główniej, dzięki czemu można rozmieszczać kontrolery domeny w kilku lokalizacjach firmy, zapewniając w ten sposób redundancję. Cecha ta ułatwia również przeniesienie domeny głównej do innej lokalizacji w sytuacjach awaryjnych.
Dedykowaną domeną główną jest łatwiej zarządzać niż domeną główną zawierająca wiele obiektów. Ponieważ baza danych katalogu będzie niewielka, łatwo tworzone są kopie zapasowe i prostsze jest przywracanie kontrolerów domeny głównej. Domena Głowna nie może być zastępowana: jeśli dom Głowna uległa uszkodzeniu i nie można jej przywrócić, trzeba odbudować cały las.
Dedykowana domena główna nigdy nie staje się przestarzała, w szczególności jeśli domenie przydzielono nazwy ogólne.

Zródło: **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008

Jeśli domena główna została już zaprojektowana, następnym krokiem byłoby określenie ilości domen dodatkowych i jakim sposobem będą one dopasowane w przestrzeni DNS.
Microsoft wyróżnia trzy modele tworzenia dodatkowych domen. Są to:

- Tworzenie domen w oparciu o lokalizacje geograficzna lub regionalnych domen
- Tworzenie domen w oparciu o jednostki biznesowe
- Tworzenie domen i kont zasobów[5]

Kolejnym etapem przy projekcie domeny będzie projekt drzewa domeny oraz relacji zaufania. Domeny w usłudze AD DS mogą być dodawane do lasu w postaci jednego drzewa bądź wielu drzew. Jeśli doda się wszystkie domeny do jednego drzewa, domeny te będą tworzyły ciągłą przestrzeń nazw. Inną możliwością jest instalowanie wielu drzew, wtedy każde drzewo będzie miało swoją własna przestrzeń nazw. Rozwiązanie polegające na stosowaniu kilku przestrzeni nazw miałoby miejsce wtedy, gdy w przedsiębiorstwie istniałoby kilka oddziałów o różnych profilach działalności. Następnym problemem jakim należy stawić czoła przy projektowaniu

[5] **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008,

domeny są relacje zaufania. Opis szczegółowy znajduje się w rozdziale 4.2.2 Jak już wcześniej wspomniałem domyślnie można wyróżnić dwa typy relacji zaufania: nadrzędne-podrzędne oraz drzewo - domena. W przypadku instalowania wielu domen, między którymi spodziewany jest duży ruch, warto skonfigurować relacje zaufania skrótowe. Relacje zaufania skrótowe zostały opisane wyżej w (rozdziale 4.2.2). Przedostatnią rzeczą przy projektowaniu domeny jest ustalenie jej właściciela. Można przyjąć, że właścicielem domeny będzie administrator tejże domeny. Administrator domeny będzie odpowiedzialny za następujące funkcje:

Tabela nr 8 Zadania Administratora

Tworzenia zasad zabezpieczeń na poziomie domeny
Projektowanie konfiguracji zasad grupy na poziomie domeny
Tworzenie w domenie struktury najwyższego poziomy jednostki organizacyjnej
Delegowanie praw wewnątrz domeny
Zarządzanie grupami administracyjnymi na poziomie domeny

Źródło: **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008

Ostatnią rzeczą, która zakończy proces projektu domeny jest wybranie poziomu funkcjonalności domeny. Tabelka nr 9 przedstawia możliwe do wyboru poziomy oraz funkcje jakie dane poziomy udostępniają.

Tabela nr 9 Poziomy funkcjonalności domeny

Poziom	Funkcje	Obsługiwane kontrolery domeny
Windows Server 2000	Wszystkie domyślne funkcje usługi Active Directory oraz następujące funkcje: • Grupy uniwersalne włączone dla grup dystrybucji i zabezpieczeń • Zagnieżdżanie grup • Konwersja grup • Historia SID	Windows Server 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2003	Funkcje dostępne na poziomie funkcjonalności domeny Windows Server 2003 obejmują wszystkie funkcje dostępne na poziomie funkcjonalności domeny Windows Server 2000 oraz następujące dodatkowe funkcje: • Zmiana nazwy domeny • Możliwość przekierowania kontenerów Użytkownicy i Komputery • Możliwość ustawienia atrybutu userPassword jako hasła obowiązującego obiektach inetOrgPerson i w obiektach użytkownika. • Uwierzytelnienie selektywne	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2
Windows Server 2008	Funkcje dostępne na poziomie funkcjonalności domeny Windows Server 2008 obejmują wszystkie funkcje dostępne na poziomie funkcjonalności domeny Windows Server 2003 oraz następujące dodatkowe funkcje: • obsługa replikacji systemu plików DFS w katalogu SYSVOL, co zapewnia bardziej niezawodną i szczegółową replikację zawartości katalogu. • Obsługa AES 128 i 256 • informacje o ostatnim logowaniu interakcyjnym wyświetlające datę ostatniego pomyślnego logowania interakcyjnego użytkownika, liczbę prób logowania zakończonych niepowodzeniem od ostatniego logowania i datę ostatniego logowania zakończonego niepowodzeniem • szczegółowe zasady haseł	Windows Server 2008 Windows Server 2008 R2
Windows Server 2008 R2	Funkcje dostępne na poziomie funkcjonalności domeny Windows Server 2008 R2 obejmują wszystkie funkcje dostępne na poziomie funkcjonalności domeny Windows Server 2008 oraz następującą dodatkową funkcję: • Ubezpieczenie uwierzytelniania, które umożliwia określenie metody logowania użytej przez użytkownika na podstawie jego tokenu Kerberos.	Windows Server 2008 R2

Zródło: **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit*, Microsoft Press, Warszawa 2008, str, 191-192

Po dokładnym zapoznaniu się ze strukturą przedsiębiorstwa „Jaskulek" zdecydowałem, że najlepszym rozwiązaniem dla tej firmy będzie zainstalowanie pojedynczej domeny. Firma ta nie posiada oddziałów geograficznych. Wszystkie kontrolery domeny jakie znajdą się w firmie będą znajdowały się w jej centrali.

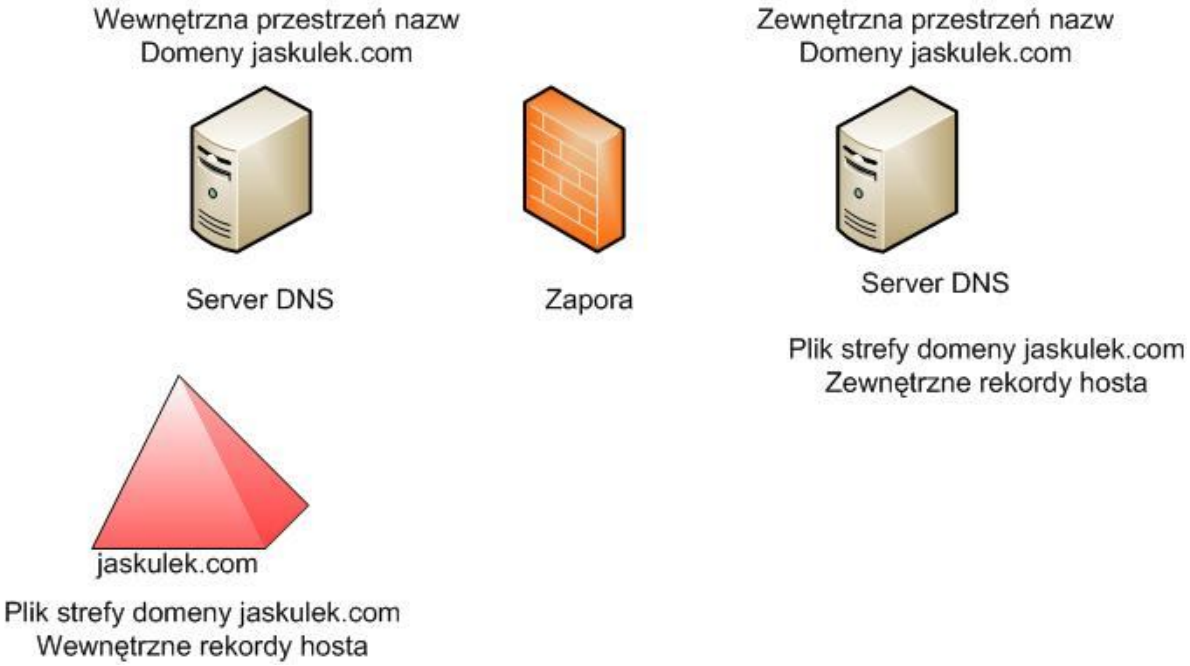
Przy wyborze poziomu funkcjonalności lasu na poziomie najwyższym kreator automatycznie ustawia poziom funkcjonalności domeny na tym samym poziomie i nie da się

go zmienić. Natomiast przy wyborze wcześniejszego poziomu istnieje możliwość wyboru bieżącego poziomu funkcjonalności lub nowszego. Nie ma możliwości wybrania wcześniejszego poziomu funkcjonalności domeny, niż ten poziom, na którym znajduje się las. Dlatego, jak już wspomniałem wcześniej, poziom domeny został automatycznie ustawiony na poziomie funkcjonalności Windows Server 2008 R2.

5.1.3. Projektowanie infrastruktury systemu DNS

Niezwykle istotną sprawą przy projektowaniu usługi AD DS jest projekt infrastruktury systemu DNS. Podczas projektowania infrastruktury DNS w usłudze AD DS skorzystać można z dwóch typów projektu tej infrastruktury. Mowa o strukturze podzielnego mózgu oraz całego mózgu. Poniżej przybliżę oba te pojęcia oraz wybrać odpowiednią strukturę dla firmy „Jaskulek". Struktura „podzielnego mózgu" polega na używaniu tych samych przestrzeni nazw wewnątrz jak i na zewnętrz przedsiębiorstwa.

Rysunek nr 9 Struktura podzielnego mózgu



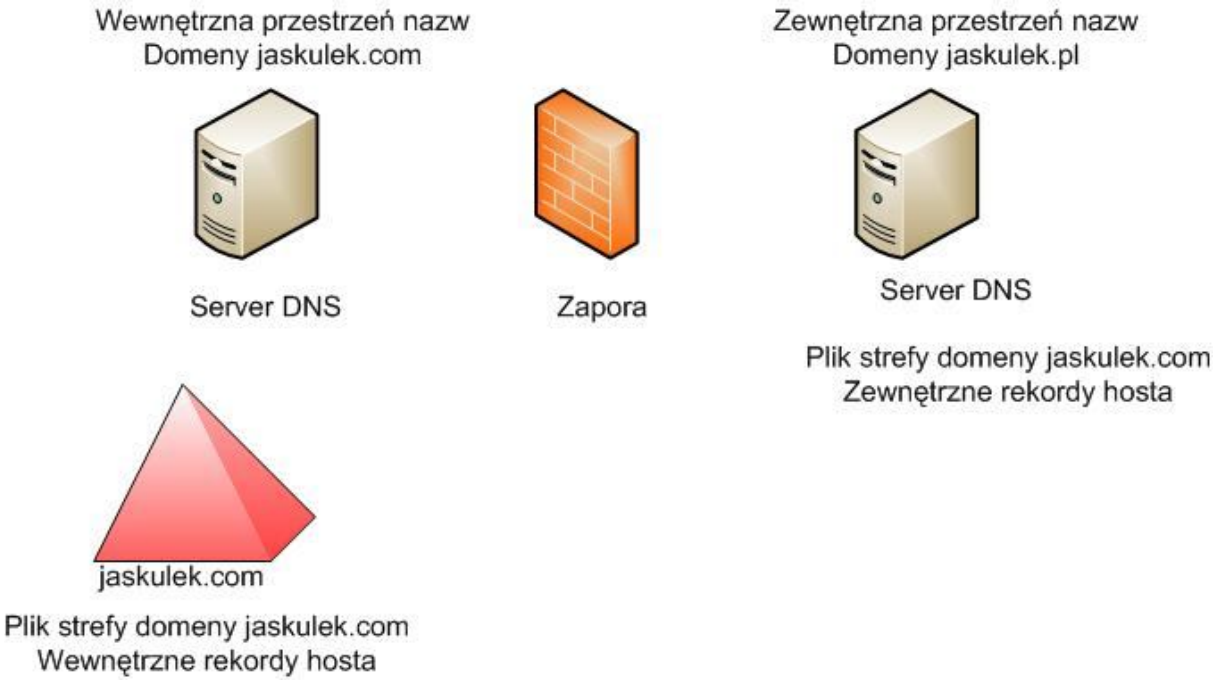
Źródło: Opracowanie własne na podstawie **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str, 195

W takim rozwiązaniu firma „Jaskulek" rejestruje jedną domenę „jaskulek.com" dla sieci Internet. Firma „Jaskulek" tak samo może korzystać z tej nazwy wewnątrz jak i na zewnątrz

swojego przedsiębiorstwa. Jedną z głównych zalet tego rozwiązania jest rejestrowanie tylko jednej domeny DNS.

Minusem takiego rozwiązania jest spory nakład pracy administratora w kwestii zabezpieczeń. Gdyby firma „Jaskulek" używała tej metody może skomplikować zarządzanie systemem DNS, gdyż administrator systemu DNS byłby zmuszony zarządzać dwoma różnymi strefami posiadającymi taką samą nazwę. Ponadto administrator utrzymywałby dwie takie same nazwy DNS dla dwóch osobnych celów po obu stronach zapory. Niewątpliwym minusem takiego rozwiązania będą również utrudnienia podczas konfigurowania systemów klienckich przedsiębiorstwa. Struktura „całego mózgu" polega na używaniu dwóch innych przestrzeni nazw wewnątrz jak i na zewnętrz przedsiębiorstwa.

Rysunek nr 10 Struktura całego mózgu



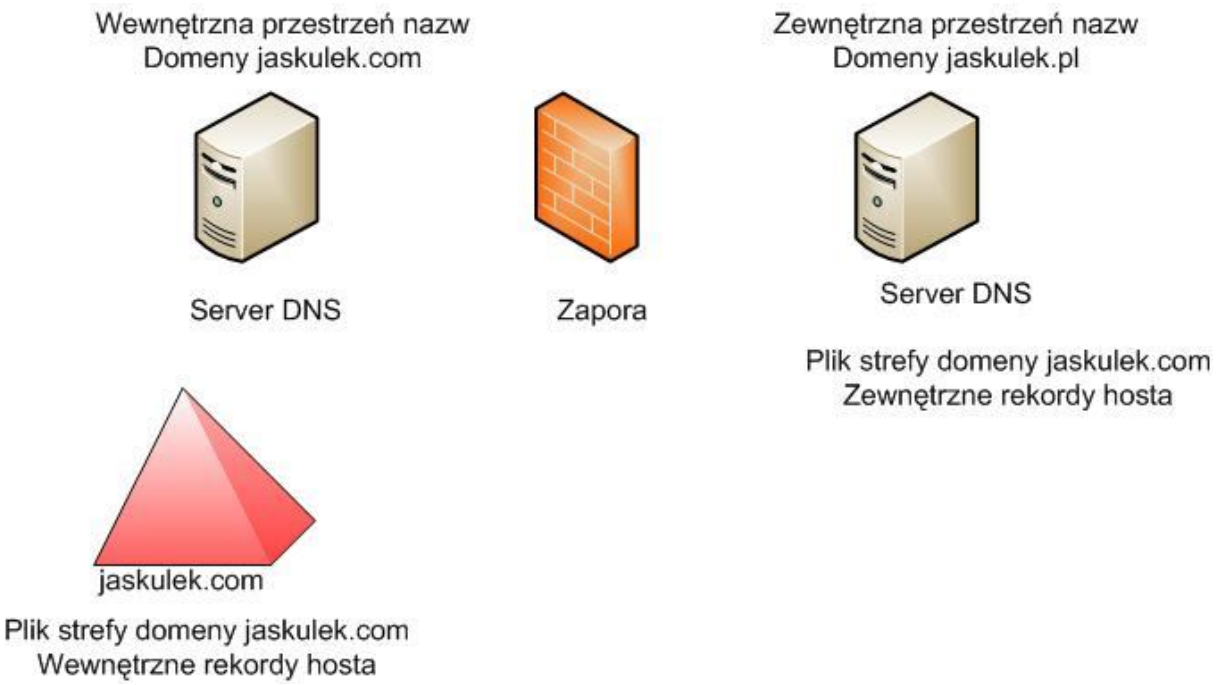
Źródło: Opracowanie własne na podstawie **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str, 196

W tej strukturze firma „Jaskulek" musi zarejestrować przynamniej jedną domenę zewnętrzną. Rejestrowanie domeny wewnętrznej nie jest obowiązkowe, ale jest zalecane, ponieważ inna firma może w każdej chwili wykupić używaną wewnętrzną domenę firmy „Jaskulek". Bardzo dużym plusem takiego rozwiązania jest bezpieczeństwo. Można w ten sposób chronić

wewnętrzną nazwę domenową przed opublikowaniem jej w Internecie. Konfiguracja DNS i zapór jest znacznie łatwiejsza. [1]

Przedsiębiorstwo „Jaskulek" bardzo dużo uwagi poświęca bezpieczeństwu. Dlatego też zadecydowałem się na projekt DNS o strukturze całego mózgu.
Kolejnym etapem jaki należy do projektu infrastruktury DNS jest sposób instalowania struktury DNS w przedsiębiorstwie, w jego aktualnym środowisku. Jak już wcześniej wspominałem firma „Jaskulek" aktualnie nie posiada środowiska DNS, tak więc zaprojektowanie DNS o strukturze całego mózgu nie będzie sprawiało tak wielu problemów, jak to jest w przypadku istniejących środowisk.
Usługa AD DS również może współpracować z innymi systemami operacyjnymi, na których zainstalowany jest DNS. W przypadku instalacji usługi DNS na systemie Windows, usługa DNS podczas instalacji usługi AD DS konfiguruje się automatycznie, natomiast, gdy instaluje się usługi AD DS. która opiera się o DNS innego systemu operacyjnego wszystkie ustawienia systemu DNS trzeba konfigurować samodzielnie. Dlatego zdecydowałem, że system DNS zainstaluję na systemie operacyjnym Windows Server 2008 R2 razem z usługami AD DS. Projekt infrastruktury DNS dla przedsiębiorstwa będzie wyglądał następująco:

Rysunek nr 11 Struktura całego mózgu



Źródło: Opracowanie własne na podstawie **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008, str, 196

Jak już wcześniej wspomniałem rola DNS instaluje się automatycznie wraz z rola AD DS. DNS umożliwia wyszukiwanie rekordów na dwa sposoby. Pierwszy sposób nazywa się wyszukiwaniem do przodu a drugi wyszukiwaniem wstecznym.

Strefa wyszukiwania do przodu (FLZ Forward Lookup Zone) polega na: zamianie/mapowaniu adresu domenowego na adres IP.

Strefa wyszukiwania wstecznego (RLZ Reverse Lookup Zone) polega na: zamianie/mapowaniu adresu IP na adres domenowy.

Podczas instalacji roli AD DS z automatyczną instalacją roli DNS, konfigurowana jest automatycznie strefa wyszukiwania do przodu. Ponieważ przedsiębiorstwo „Jaskulek" jest rozwijającą się firma, która zamierza korzystać z rożnych aplikacji, które mogą wykorzystywać „strefy wyszukiwania wstecznego" zamierzam również skonfigurować tę strefę.

Wewnętrzny serwer DNS będzie tak skonfigurowany, żeby przesyłał dalej zapytanie do zewnętrznego serwera DNS. Dodatkowo dla zwiększania bezpieczeństwa na serwerach

utrzymujących rolę DNS należy upewnić się, że usługa przesyłania dalej jest poprawnie ustawiona oraz została wyłączona opcja „użyj wskazówek dotyczących serwerów głównych" Stanowi bardzo dużą lukę w bezpieczeństwie, gdyż w sytuacji kiedy zewnętrzne serwery nie będą odpowiadać, serwery wewnętrzne będą komunikowały się z serwerami DNS w Internecie.

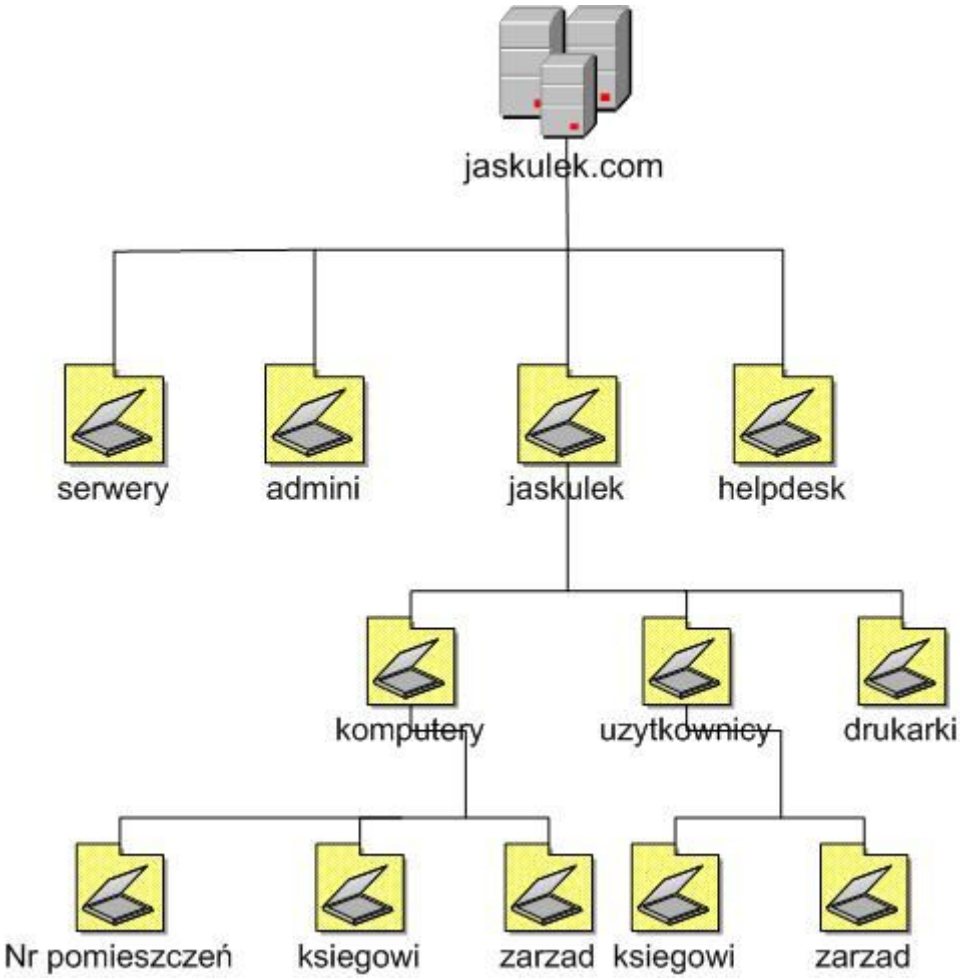
5.1.4. Projektowanie jednostek organizacyjnych

Jak wcześniej wspomniałem jednostka organizacyjna jest kontenerem. Jednostek organizacyjnych można także używać do stworzenia struktury w domenie. Projektując jednostki organizacyjne administrator ma duży poziom elastyczności w ich tworzeniu. Istnieje kilka opcji dla których można tworzyć jednostki organizacyjne. Pierwszą opcją jest możliwość tworzenia jednostek organizacyjnych, które odzwierciedlają schemat przedsiębiorstwa. W opcji drugiej istnieje możliwość projektowania OU w oparciu o zasady grupy. OU umożliwia ustawienie zasad grupy dla danej jednostki organizacyjnej. Dzięki takiemu rozwiązaniu możliwa będzie konfiguracja oraz ustawienia dla obiektów znajdujących się w poszczególnych jednostkach organizacyjnych. Trzecią opcją projektowania OU jest projekt oparty na delegowaniu administracji. Do jednostki organizacyjnej można oddelegować administratora z uprawnieniami konkretnymi dla właściwej jednostki organizacyjnej. [1]

Projektując strukturę jednostek organizacyjnych dla przedsiębiorstwa „Jaskulek", zastosuję te wszystkie metody. W pierwszej kolejności utworzę trzy jednostki najwyższego poziomu: *„admini", „helpdesk" „J\jaskulek"* oraz serwery. Jednostka organizacyjna *„admini"* będzie zawierała administratorów przedsiębiorstwa oraz ich stanowiska komputerowe, na tą chwilę nie przewiduję żeby ta jednostka organizacyjna zawierała dodatkowe jednostki organizacyjne. W jednostce organizacyjnej *„helpdesk",* będą znajdować się osoby, które będą wspomagać użytkowników w codziennej pracy. Jednostka organizacyjna „jaskulek", będzie jednostką najwyższego poziomu dla jednostek organizacyjnych „komputery", „użytkownicy", „drukarki". Ponadto jednostka organizacyjna „użytkownicy" będzie zawierała dwie jednostki organizacyjne „zarząd" i „księgowi". Natomiast jednostka organizacyjna „komputery" będzie zawierała wszystkie komputery, oraz utworzone w tej jednostce OU jednostki organizacyjne

dla komputerów zarządu i księgowych. Spowodowane to jest tym, że funkcje tych dwóch grup będą w dużym stopniu odbiegać od globalnej konfiguracji komputerów.

Rysunek nr 12 Projekt Struktury jednostek organizacyjnych



Źródło: *Opracowanie własne na podstawie*

5.1.5. Projektowanie zabezpieczeń oraz wstępnej konfiguracji

W tym miejscu omówione zostaną wybrane elementy bezpieczeństwa. Bardziej szczegółowe ustawienia zabezpieczeń będą opisane wraz z procesem instalacji AD DS. Biorąc pod uwagę wyjątkowo istotne dla firmy „Jaskulek" bezpieczeństwo zdecydowałem się na zainstalowanie zapasowego kontrolera domeny oraz zapasowego serwera DNS. Kontroler ten będzie replikował wszystkie dane z głównego kontrolera domeny. Zapewni to bardzo duże

bezpieczeństwo, gdyż w przypadku awarii głównego kontrolera domeny, kontroler zapasowy przejmie jego rolę. Pozwoli to użytkownikom na bezawaryjną pracę oraz zapobiegnie jakimkolwiek przestojom w pracy systemu przedsiębiorstwa, gdzie nawet niewielkie i krótkotrwałe awarie skutkują utratą przychodów. Dodatkowym aspektem bezpieczeństwa będą szczegółowe zasady haseł przypisane poszczególnym grupom. Firmie zależy, żeby dane użytkowników zapisywane były w jednym miejscu sieciowym. Operacje tego tupu będą przeprowadzane za pomocą skryptów logowania. Każdy użytkownik będzie posiadał swój własny dysk sieciowy o określonej pojemności. Dane użytkowników będą natomiast zapisywane na dysk logiczny o określonej pojemności. W celu łatwiejszego udostępniania danych wszyscy użytkownicy będą mieli dostęp do tego zasobu sieciowego, w którym zarząd będzie udostępniał pliki dla pracowników. Każda z istniejących grup będzie posiadała również swój własny zasób sieciowy, do którego będą miały dostęp osoby z pojedynczej grupy. Przewidywany jest również jeden mały zasób sieciowy w celu wymiany plików miedzy pracownikami. Zasób ten będzie wskazany ponieważ pracownicy firmy będą mieli ograniczony dostęp do portu USB. Zablokowana będzie możliwość zapisu. Uniemożliwi to kradzież informacji firmowych, oraz wprowadzenie złośliwego oprogramowania przez użytkownika za pomocą przenośnych nośników danych. Dużą luką w bezpieczeństwie usługi AD DS jest możliwość dodania komputera do domeny przez użytkownika. Ze względu na wymogi bezpieczeństwa IT w firmie „Jaskulek" opcja ta została zablokowana. Dalsze aspekty bezpieczeństwa będą projektowanie i wdrażane wraz z implementacją środowiska AD DS. W przedsiębiorstwie „Jaskulek" zdecydowano, by systemy operacyjne pobierały aktualizacje z jednego punktu.

Według wytycznych komputery z systemem Windows nie będą łączyły się z witryną Microsoft w celu pobrania aktualizacji. Ponadto administratorzy sami będą decydować, które z udostępnianych aktualizacji zostaną wdrożone w przedsiębiorstwie. Ze względu na taki stan rzeczy przewiduję instalację oprogramowania Windows Server Update Services(WSUS). Opis tego oprogramowania zostanie umieszczony w rozdziale 5.2.1.

Dział informatyków w przedsiębiorstwie „Jaskulek", chciałby mieć osobny pododdział, który będzie udzielał wsparcia dla użytkowników. W tym celu w projekcie jednostek organizacyjnych została utworzona jednostka organizacyjna „helpdesk". Zakres obowiązków

dla helpdesk-u będzie obejmował: dodawanie/usuwanie użytkowników komputerowo oraz resetowanie haseł.

5.2. Opis oraz projekt dodatkowych usług

5.2.1. DHCP

DHCP (Dynamic Host Configuration Protocol) jest to protokół komunikacyjny opublikowanym w 1993 roku. DHCP udostępnia komputerom dane konfiguracyjne. Poprzednikiem DHCP był protokół BOOTP. [7]

5.2.2. Windows Server Update Services

WSUS czyli Windows Server Update Services to oprogramowanie zaprojektowane przez Microsoft. Pierwsza wersja tego programu pojawiła się w marcu 2005 roku. Do prawidłowego działania usługa WSUS używa SQL Server i ról IIS. Należy w tym miejscu wspomnieć o elastyczności tejże usługi. Mam tutaj na myśli swobodę administratorów w instalowaniu udostępnianych aktualizacji, możliwość ich testowania przed ostatecznym zainstalowaniem (ewentualne administrator usunie konflikty wynikające z niezgodności z oprogramowaniem zainstalowaniem na stacjach roboczych). Program WSUS po instalacji zawiera dwie standardowe grupy komputerów: wszystkie komputery oraz komputery nieprzypisane. Gdy komputer łączy się z serwerem WSUS po raz pierwszy, dodawany jest do grupy „komputery nieprzypisane”. Istnieją dwie metody dodawania komputerów klienckich do serwera WSUS. Pierwszą metodą jest wykorzystanie zasad grup (GPO). Żeby jednak skorzystać z tej metody, musi już istnieć Active Directory. Drugą metodą dodawania komputerów do WSUS jest konfiguracja lokalnych zasad grup na komputerze klienckim. Dodawanie komputerów do grup również odbywa się w podobny sposób. Można ustalić poprzez GPO do jakiej grupy należy komputer. Ewentualnie administrator sam przypisze komputer do odpowiedniej grupy w konsoli Windows Server Update Services. Instalację oraz konfigurację WSUS opiszę w rozdziale dotyczącym implementacji. [3]

5.2.3 Windows Deployment Services

WDS (Windows Deployment Services) to technologia wdrażania systemów operacyjnych Windows za pośrednictwem sieci LAN. Usługa ta zastąpiła poprzednie rozwiązanie, jakim był RIS (Remote Instalation Service). WDS wprowadziło wsparcie dla Windows Imaging Format(WIM), RIS nie udostępniał tego rozwiązania. Dzięki WIM można instalować systemy operacyjne, takie jak Windows Vista, Windows 7, Windows Server 2008 i Windows Server 2008 R2. [5]

5.2.4. Distributed File System

DFS Distributed File System to rozproszony system plików. Pozwala on przedsiębiorstwu na zbudowanie jednego hierarchicznego obrazu udziałów plików. Aby użytkownik mógł skorzystać z udziału DFS należy podać alias ścieżki.
Usługa ta składa się z następujących elementów:

- Przestrzeń nazw – jest to wirtualna nazwa udostępnionych folderów w przedsiębiorstwie.
- Serwer przestrzeni nazw – zawiera wirtualne nazwy udostępnionych folderów.
- Katalog główny przestrzeni nazw – jest to punkt, który określa początek wirtualnej przestrzeni nazw.
- Folder – kontener, który zawiera skrót przekierowujący użytkowników do docelowego elementu.
- Element docelowy folderu – docelowy folder, w którym znajdują się dane.

DFS umożliwia tworzenie dwóch rodzajów przestrzeni nazw. Pierwszym rodzajem jest przestrzeń nazw oparta ma autonomicznej przestrzeni nazw. Metoda ta magazynuje dane o konfiguracji w Rejestrze docelowego członka replikacji. Minusem tej metody jest to, że nie wspiera ona replikacji plików. Drugą metodą tworzenia przestrzeni nazw jest metoda oparta na domenie. Polega ona na tym, że przestrzeń nazw publikowana jest przy pomocy Active Directory Domain Services. Plusem takiego rozwiązania jest to, że dzięki oparciu przestrzeni nazw o usługę Active Directory Domain Services możliwa jest replikacja plików. Istnieje tutaj również możliwość wykorzystania wbudowanych mechanizmów odporności na błędy.

Usługa DFS opiera się na dwóch technologiach. Pierwszą z nich jest DFS Namespaces - usługa umożliwiająca publikowanie udostępnionych folderów, rozmieszczonych w rożnych serwerach pod jedną wirtualną nazwą. Drugą techniką wykorzystywaną przez DFS, jest DFS Replication. Jest ona multimaster'owym typem replikacji pozwalającym na wspieranie planowania czasu nastąpienia (wykonania) replikacji. Ponadto DFS Replication wykorzystuje protokół Remote Differantial Compression (RDC), używany zazwyczaj do replikacji plików w sieciach, w których występują kłopoty z przepustowością.[3]

Rozdział 6
INSTALACJA SYSTEMU WINDOWS SERVER 2008 R2

Rozdział będzie opisywał proces instalacji oraz konfiguracji AD, DNS, WDS, WSUS, DHCP i implementacją GPO.

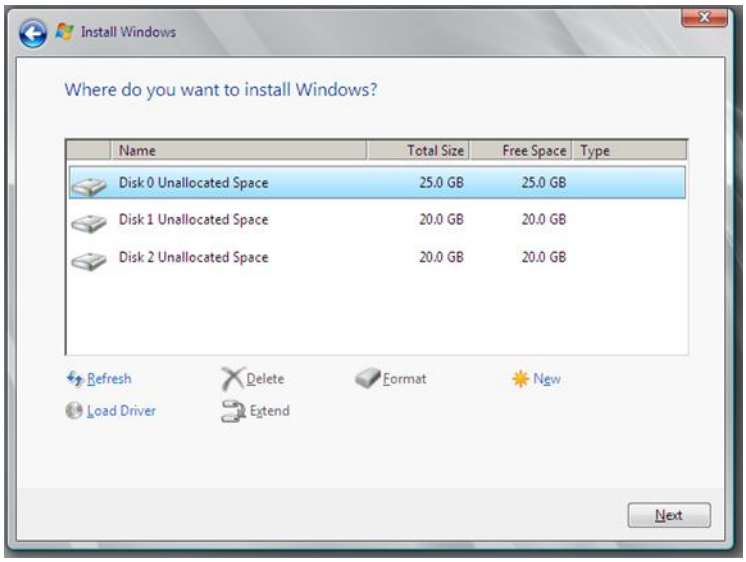
Zaczynając implementację projektu zaczynam od instalacji systemu operacyjnego Windows Server 2008 R2. Pierwszą opcją jaką mam do wyboru przy instalacji systemu jest wybór języka, oraz format czasu. Ponieważ przedsiębiorstwo jest polską firmą, ustawiam parametry na język polski.

Rysunek nr 13 Wybór języków przy instalacji systemu

Źródło: *opracowanie własne*

Kolejną opcją wyboru, którą muszę zatwierdzić jest wersja systemu operacyjnego. Dostępne wersje systemu operacyjnego opisałem w rozdziale 4. Wybieram wersję Windows Server 2008 R2 Enterprise w typie instalacji „Full". Typ „Full" umożliwi mi instalację dodatkowych ról serwera, które nie są dostępne wersji „Core", a których wymaga przedsiębiorstwo. Następną rzeczą jaką muszę ustalić, jest wybór dysku, na którym zostanie zainstalowany system operacyjny.

Rysunek nr 14 Dyski twarde



Źródło: *opracowanie własne*

W serwerze umiesiłem **trzy osobne dyski.** Na **dysku pierwszym** zainstaluję system operacyjny. **Drugi dysk** przeznaczę na dane użytkowników. **Dysk trzeci** posłuży do obsługi programów WSUS. Będą znajdować się na nim aktualizacje. System Windows Server 2008 R2 zainstaluję na Dysku 0. Gdy system operacyjny zostanie zainstalowany, następnym krokiem do poprawnego działania systemu jest jego konfiguracja. Dla zwiększania bezpieczeństwa zmienię nazwę konta „administrator" na „jaskulek". **Zamiana nazwy konta** administratora zapobiegnie wykrywaniu przez złośliwe oprogramowanie konta administratora i samoczynne instalowanie złośliwego oprogramowania. W celu zamiany nazwy wchodzę w zasady zabezpieczeń lokalnych, otwieram węzeł zasady lokalne następnie wybieram podwęzeł opcje zabezpieczeń i wybieram opcje „konto: zmienianie nazwy konta administratora" i zmieniam nazwę konta administratora na „jaskulek".

Teraz zajmę się aktualizacją systemu. W tym celu pobiorę ze strony Microsoftu najnowsze aktualizacje systemu oraz je zainstaluję.

Zaznaczam, że w przedsiębiorstwie będą znajdować się jeszcze **dwa serwery**. Instalacja tych systemów będzie przebiegała w podobny sposób, z tym że serwer1 będzie **pełnił rolę głównego kontrolera domeny oraz serwera WSUS**, **serwer2 będzie spełniał rolę zapasowego kontrolera domeny, serwera DHCP i WDS**. Serwer2 będzie również zawierał trzy dyski. **Pierwszy dysk** posłuży do instalacji systemu operacyjnego**, drugi** przeznaczę na

replikację danych użytkowników. **Dysk trzeci** posłuży mi za obrazy systemów dla serwera WDS.

Serwer 3 będzie zawierał jeden dysk, będzie miał zainstalowaną usługę DNS i zostanie wykorzystany jako zewnętrzny serwer DNS.

Przewidywana adresacja serwerów.

- Serwer1 10.1.0.1/8
- Serwer2 10.1.0.2/8
- Serwer3 10.1.0.3/8

6.1. Instalacja zewnętrznego Serwera Domain Name System

Po instalacji i konfiguracji serwer3 mogę przystąpić do instalacji zewnętrznego serwera DNS. Serwer ten **nie będzie dołączony do domeny**. W celu dodania roli serwera **DNS, uruchamiam kreator dodawania ról.**

Kreator ten uruchamiam po kliknięciu w oknie „**zadania konfiguracji początkowej**" dodaj rolę. **Wybieram opcję serwera DNS.** Po chwili system zainstaluje serwer DNS. Żeby skonfigurować serwer DNS wchodzę w konsolę znajdującą się w „**menu start" – „narzędzia administracyjne" – „DNS**". **Konfiguruję obie strefy**, które będą **strefami podstawowymi**. Firma „Jaskulek" **wykupiła dwie domeny,** więc strefa ta będzie nazywała się „jaskulek.pl".

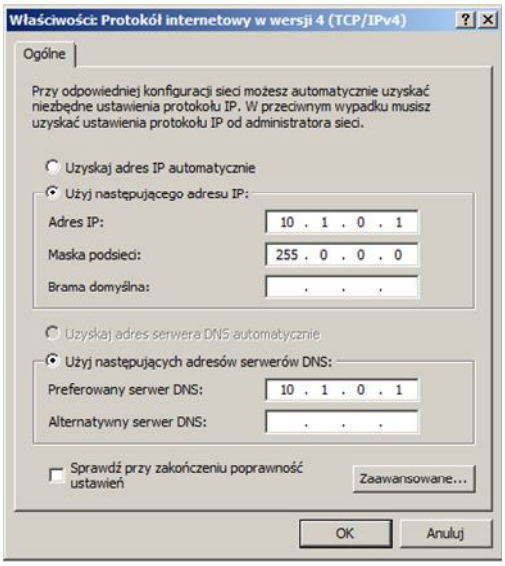
6.2. Implementacja Active Directory Domain Services i Domain Name Server

System

Jeśli zbiorę dane dotyczące projektu struktury AD mogę przystąpić do wdrażania usługi AD DS. Jak wspomniałem w **rozdziale 5** dotyczącym projektu, usługa AD DS będzie składała się z **jednego lasu oraz pojedynczej domeny**. Dla zwiększania bezpieczeństwa **na serwerze2 zainstaluję również kontroler domeny**. Będzie on pełnił rolę zapasowego kontrolera domeny. System Windows Server 2008 R2 udostępnia mi dwa rodzaje typów

instalacji roli: **graficzny i z użyciem wiersza poleceń**. Zanim przystąpię do instalowania roli, na serwerze muszę skonfigurować adresy IP serwera. Adresy IP jakie przyjmuje to:

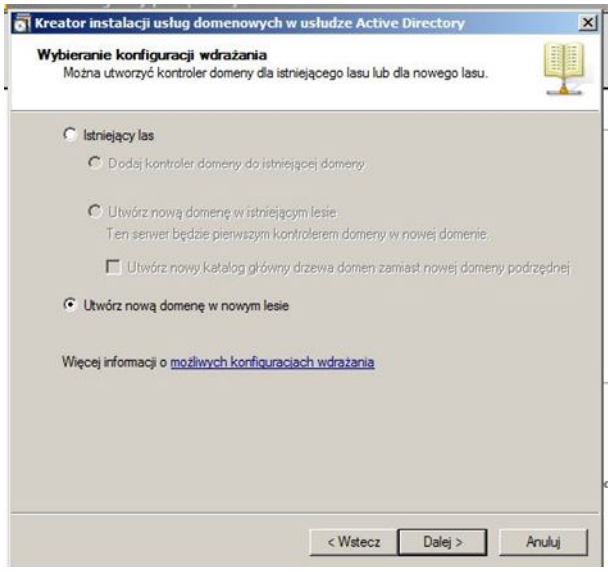
Rysunek nr 15 Konfiguracja adresów IP



Źródło: *opracowanie własne*

Skorzystam z pierwszej metody. W tym celu w konsoli „**Menedżer Serwera**" klikam prawym przyciskiem myszy węzeł „**Role**". Kiedy uruchomi **się kreator dodawania ról**, wybieram opcję usługi AD DS. Po tej operacji **nie można niestety skorzystać** z ustawień konfiguracyjnych roli AD DS. Zostaną natomiast zainstalowane pliki, które są potrzebne do **uruchomienia usługi. W celu konfiguracji roli AD DS**, muszę skorzystać z **kreatora instalacji usług domenowych w usłudze Active Directory**. Polecenie „**DCPROMO.EXE**" uruchamia wspomniany kreator. Polecenie to mogę uruchomić przy pomocy wiersza poleceń. Po uruchomieniu kreatora jestem proszony o potwierdzanie zgodności systemu operacyjnego, co uczynię. Następnie jestem proszony o określenie, czy dodaję kontroler domeny do istniejącej już domeny, czy tworzę nową domenę w istniejącym lesie, lub czy tworzę nowy las z nowa domeną.

Rysunek nr 16 Kreator instalacji usługi Active Directory



Źródło: opracowanie własne

Wybrałem drugą opcję, ponieważ jest to **pierwszy kontroler domeny** w przedsiębiorstwie. Kolejnym krokiem będzie ustalenie przeze mnie nazw **FQDN oraz NetBIOS**. Nazwa FQDN jest nazwą głównej domeny lasu. Firma „Jaskulek" do tego celu wykupiła własną nazwę **jaskulek.com**, nazwa NetBIOS jest generowana automatycznie. Kolejnym etapem konfiguracji roli AD jest wybór **poziomów funkcjonalności lasu i domeny**. Ustalam poziom funkcjonalności lasu na **Windows Server 2008 R2**, poziom funkcjonalności domeny zostanie automatycznie ustawiony **na taki sam poziom, co las.** Na następnej stronie kreatora (dodatkowe opcje kontenera domeny) mam możliwość wyboru następujących opcji.

Serwer DNS – ta opcja zaznaczona jest domyślnie, spowoduje ona automatyczną instalację i konfigurację serwera DNS.

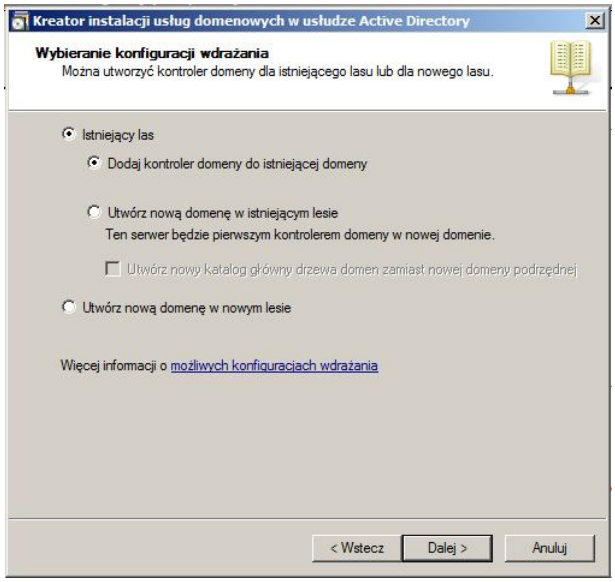
Wykaz globalny – ta opcja jest domyślnie zaznaczona, ponieważ gdy instalowany jest pierwszy kontroler domeny, musi on być serwerem wykazu globalnego.

RODC opcja ta odpowiada za typ kontrolera domeny tylko do odczytu.

W kolejnym etapie konfiguracji mogę zmienić domyślną lokalizację folderów roli AD DS. **Pozostawię te foldery w domyślnej lokalizacji.** Ponieważ instaluję jeszcze zapasowy kontroler domeny oraz serwer DNS **proces tez będzie zdublowany**. Przed czynnościami opisanymi powyżej, **muszę dodać serwer2 do domeny**, a następnie **powtórzyć powyższy proces**. Będzie on się jednak **różnił** w miejscu wyboru tworzenia nowego lasu, bądź dodania

kontrolera domeny do istniejącej domeny. W tym miejscu zaznaczę opcję **„istniejący las”** oraz **„dodaj kontroler do domeny”.** W następnym etapie kreator instalacji wymusi podanie nazwy **dla nowej domeny.** Z uwagi na to, że będzie to kontroler zapasowy, skorzystam z nazwy istniejącej już domeny czyli **jaskulek.com**.

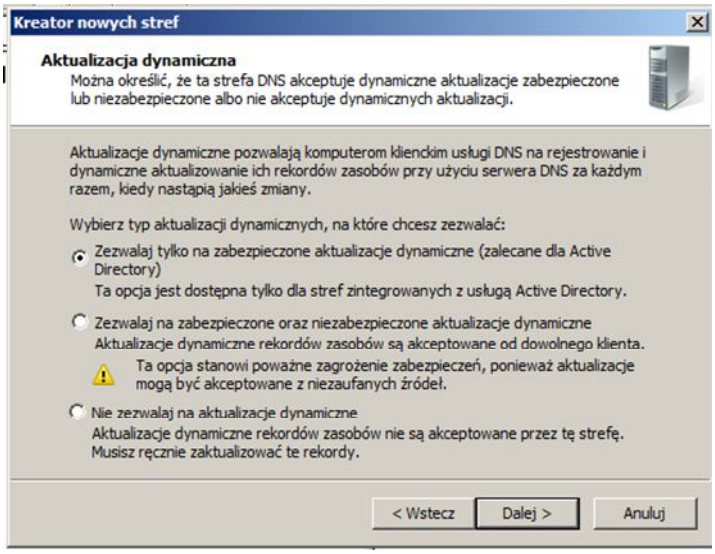
Rysunek 17 nr Kreator instalacji usługi Active Directory



Źródło: *opracowanie własne*

Po konfiguracji serwer2 będzie **pełnił rolę zapasowego kontrolera domeny**, jak również rolę **wykazu globalnego**. Kolejnym krokiem jaki zamierzam uczynić jest dodanie **strefy wyszukiwania wstecznego do wewnętrznych DNS**. W tym celu wchodzę w **konsole zarządzania serwerem DNS** i uruchamiam **kreatora nowych stref**. Kreatora uruchomiłem klikając prawym klawiszem myszy na węzeł „**strefy wyszukiwania wstecznego**”. Kreator przeprowadza mnie poprzez następujące opcje: pierwsza opcja daje do wyboru typ strefy – ja wybieram strefę podstawową. Kolejną rzeczą, którą ustalam jest zakres replikacji strefy. Nie korzystam z adresów IPv6, więc ustawiam strefę wyszukiwania wstecznego dla IPv4. Ostatnią rzeczą wymagającą konfiguracji przy pomocy kreatora jest wpisanie **identyfikatora sieci**. Przy wyborze „aktualizacji dynamicznych”, mając na uwadze względy bezpieczeństwa wybieram opcję pierwszą.

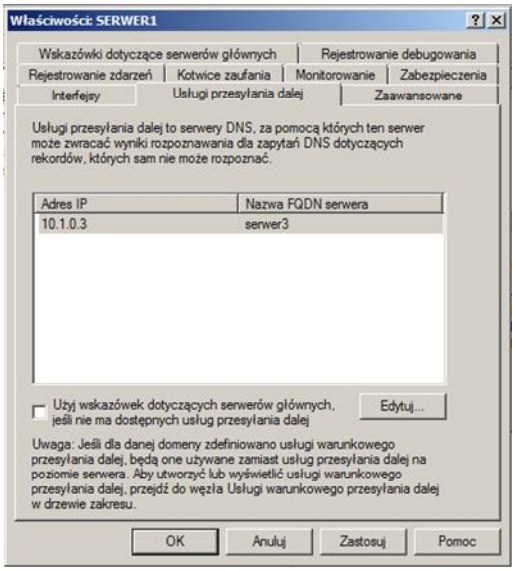
Rysunek nr 18 Kreator konfiguracji stref



Źródło: *opracowanie własne*

Proces opisany powyżej powtórzę na serwerze2. Jak wspomniałem w rozdziale dotyczącym projektowania zabezpieczeń w tym miejscu muszę skonfigurować wewnętrzne serwery DNS, żeby nie łączyły się z Internetem. W tym celu we właściwościach serwera DNS na serwerach 1 i 2, w zakładce „usługi przesyłania dalej" podaję adres zewnętrznego serwera DNS. Odznaczam także opcje „**użyj wskazówek dotyczących serwerów głównych, jeśli nie ma dostępnych usług przesyłania dalej**" (Rysunek nr 19). Jest to bardzo ważna opcja, która zwiększy bezpieczeństwo.

Rysunek nr 19 Właściwości konfiguracji DNS

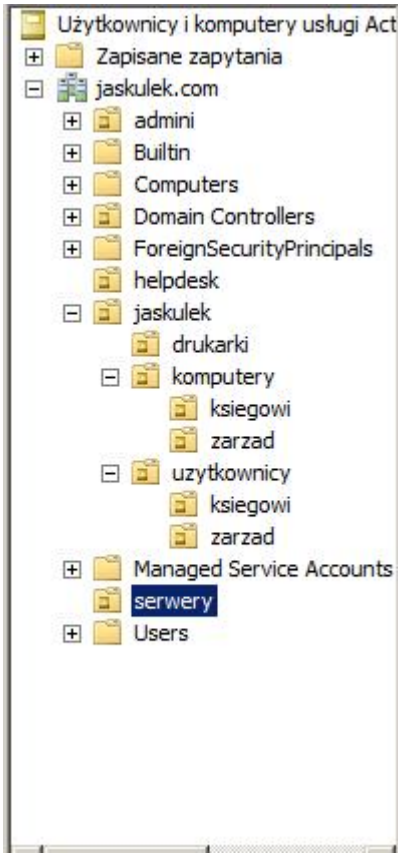


Źródło: *opracowanie własne*

6.2.1 Jednostki organizacyjne

Po konfiguracji usługi AD DS. i serwerów DNS mogę przystąpić do tworzenia **jednostek organizacyjnych**. System Windows Server 2008 R2 umożliwia mi to na kilka sposobów. Skorzystam z konsoli „**użytkownicy i komputery usługi Active Directory**”. W celu utworzenia jednostek organizacyjnych wchodzę w wymienioną konsolę i tworzę jednostki organizacyjne zgodnie ze schematem, który został przyjęty w projekcie.

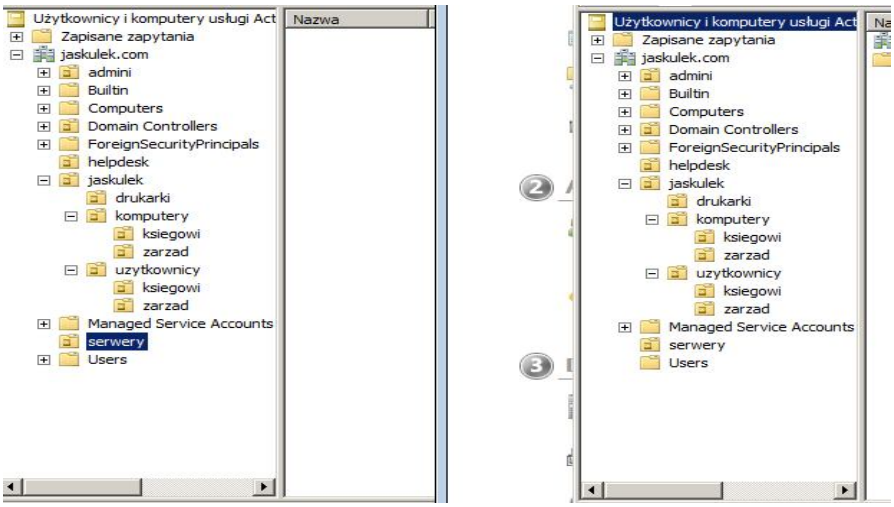
Rysunek nr 20 Tworzenie jednostek organizacyjnych



Źródło: *opracowanie własne*

Po utworzeniu jednostek organizacyjnych sprawdzam, czy zostały one **zreplikowane** do zapasowego kontrolera domeny.

Rysunek nr 21 Sprawdzanie jednostek organizacyjnych



Źródło: *opracowanie własne*

6.2.2. Tworzenie komputerów

Tak samo jak w przypadku użytkowników konta komputerów mogę dodawać poprzez interfejs graficzny albo za pomocą skryptów. Firma „Jaskulek" posiada określoną ilość stanowisk komputerowych. W każdym z pokoi dodam po jednym komputerze. Firma posiada pięćdziesiąt pomieszczeń. Konta komputerów dodam za pomocą następującego skryptu.

```
$dataSource=import-csv "c:\a.csv"
foreach($dataRecord in $datasource) {
#map variables to data source
$nazwakomputera = $dataRecord.AssetTag
$nrpokoju = $dataRecord.Type

#determine name
$kuba = $nazwakomputera
$druganazwa=$kuba + "$"
#determine OU

$strOUADsPath = "LDAP://OU=" + $nrpokoju + `
",OU=komputery,OU=jaskulek,DC=jaskulek,DC=com"

#create the computer object
$objOU=[ADSI]$strOUADsPath
$objComputer=$objOU.Create("computer","CN="+$kuba)
$objComputer.Put("sAMAccountName",$druganazwa)
$objComputer.Put("userAccountControl",4096)
$objComputer.SetInfo()
}
```

Źródło: opracowanie własne na podstawie[2]

Nazewnictwo komputerów będzie następujące: **numer pokoju, następnie numer gniazda i dodatkowo numer wtyczki** np. (1-1-1). Skrypt ten będzie pobierał z pliku listę komputerów i umieszczał je w odpowiedniej jednostce organizacyjnej.

6.2.3. Tworzenie grup

Po utworzeniu jednostek organizacyjnych przystępuję do tworzenia grup. Aby je utworzyć mogę skorzystać z **kilku możliwości.** Pierwszą możliwością jest standardowy proces tworzenia grup, natomiast drugim znanym mi sposobem który pozwalającym **szybko utworzyć wiele grup** jest zastosowanie **skryptów PowerShell.**

Dla potrzeb firmy „Jaskulek" utworzyłem następujące grupy

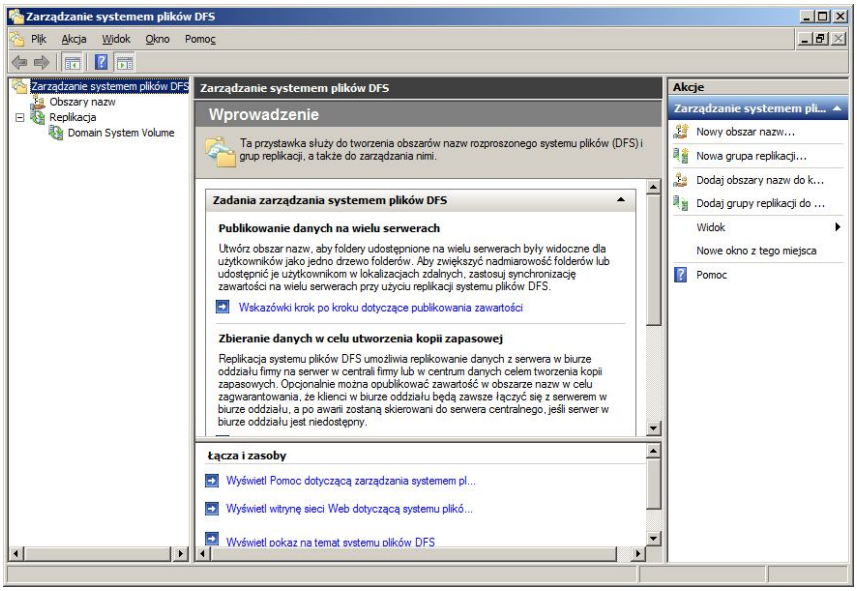
- ksiegowi
- zarzad
- pracownicy

- admini
- zwyklekontaadmini
- helpdesk
- zwyklekontahelpdesk

6.2.4. Konfiguracja Distributed File System

Rola DFS nie jest domyślnie instalowana. Aby ją dodać uruchamiam konsolę **menedżer serwera,** klikam na węzeł **usługi plików** i uruchamiam kreatora dodawania ról. Gdy rola zostanie zainstalowana mogę przystąpić do konfiguracji obrazu nazw i replikacji.
Jak wspomniałem w części projektu zabezpieczeń, każdy użytkownik będzie miał swój własny udział sieciowy. Dlatego pierwszym obszarem nazw jaki skonfiguruję, będzie obszar nazw dla prywatnych zasobów użytkowników. Następnie ustawię replikację tego zasobu. Ustawienie takie spowoduje ciągły dostęp do prywatnego zasobu użytkownika w razie przerwania pracy serwera.

Rysunek nr 22 Konsola DFS

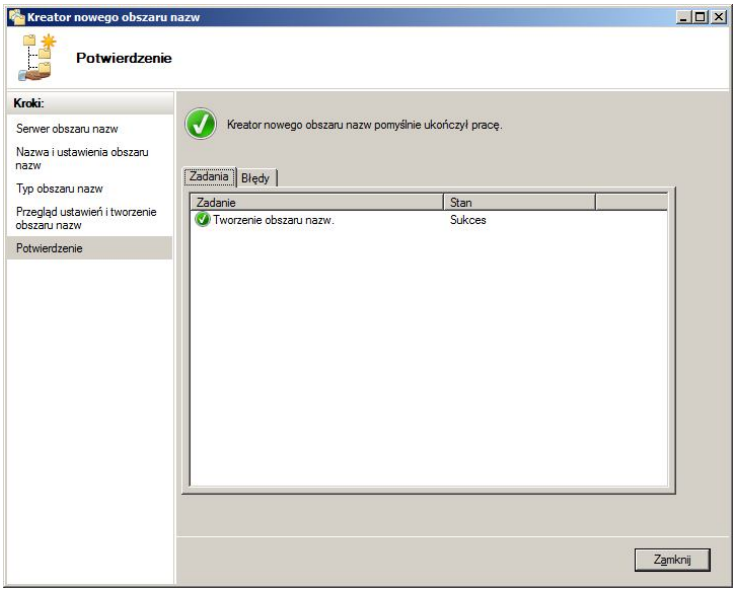


Źródło: *opracowanie własne*

Konsola zarządzanie systemem plików DFS umożliwia mi konfigurację obszarów nazw i replikacji. W celu stworzenia obszaru nazw dla prywatnych zasobów użytkowników utworzyłem na dysku lokalnym „E” serwera 1 i 2 udostępniony folder o nazwie

„dokumenty” z uprawnieniami **„share”.** Folder ten będzie zawierał **udostępnione prywatne foldery użytkowników**. Foldery te utworzę za pomocą skryptu, oraz nadam im uprawnienia wyłączności tylko dla danego użytkownika. Gdy mam już stworzone *„główne foldery”* mogę przystąpić do skonfigurowania obszaru nazw dla tego folderu. W tym celu klikam w konsoli **zarządzanie systemem plików DFS** prawym klawiszem myszy na węzeł **obszary nazw** i wybieram opcję **nowy obszar nazw**. Po chwili uruchamia się **kreator nowego obszaru nazw**. Pierwszą rzeczą jaką ustalam jest wybór pierwszego serwera, który będzie pełnił rolę serwera obszaru nazw. Kolejnym krokiem przy konfiguracji jest **nadanie nazwy obszaru**. Nazwą dla tego obszaru będzie nazwa ***„dane”.*** Po nadaniu nazwy obszaru, wybiorę przestrzeń nazw, na której dany obszar ma się opierać. Opcje te zostały opisane w rozdziale (5.2.4.). Ja wybiorę opcję opartą na domenie. Gdy dane zostaną poprawnie wprowadzone kreator powiadomi o ***poprawnym skonfigurowaniu nazwy strefy obrazu***. (rysunek 23)

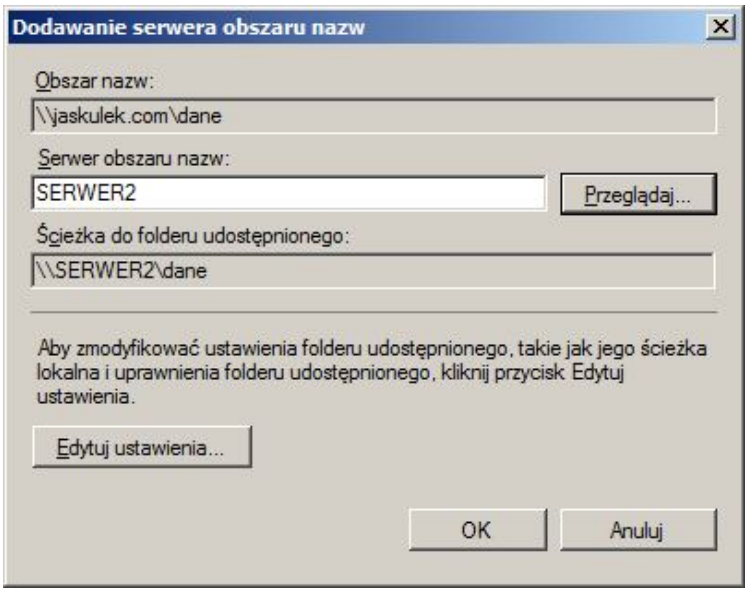
Rysunek nr 23 Kreator nowego obszaru nazw



Źródło: *opracowanie własne*

W obszarze nazw, dla zwiększenia bezpieczeństwa, dodam drugi serwer nazw Będzie nim serwer2. W celu dodania serwera2 jako obrazu serwera nazw, klikam prawym klawiszem myszy na **węzeł jaskulek.com\dane** i wybieram opcję **dodaj serwer obszaru nazw**.

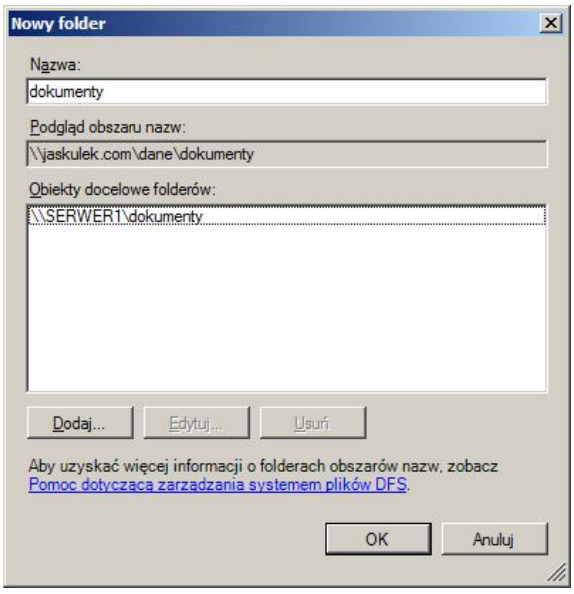
Rysunek nr 24 Dodawanie serwera obszaru nazw



Źródło: *opracowanie własne*

Aby ***folder dokumenty*** był dostępny pod nową nazwą obszaru muszę go dodać. W celu dodania folderu ***dokumenty*** klikam na węźle **jaskulek.com\dane** i wybieram opcję **dodaj folder.**

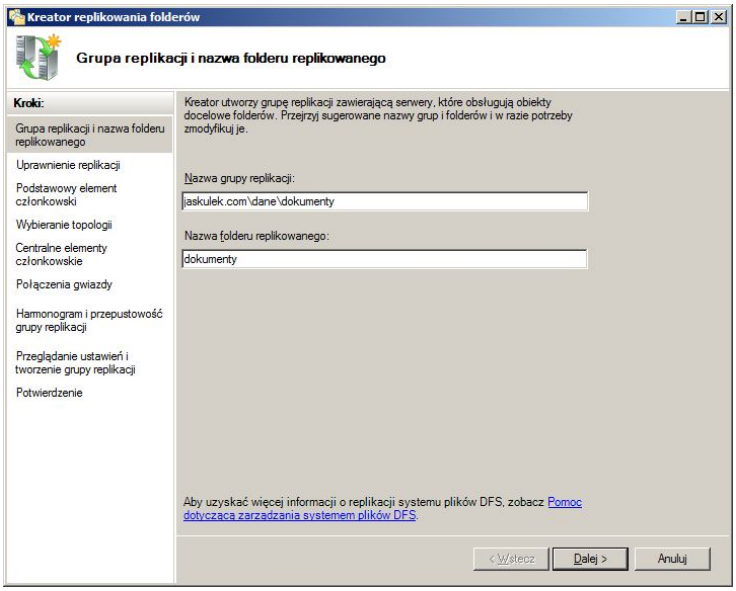
Rysunek nr 25 Dodawanie nowego folderu



Źródło: *opracowanie własne*

Tego rodzaju operację umożliwia wyżej wymienione okno. Należy podać w nim folder docelowy oraz jego nazwę. Folderem tym będzie folder ***„dokumenty”.*** Od tego momentu udziały te będą dostępne pod nazwą ***(\\jaskulek.com\dane\dokumenty\”nazwa”).*** Ostatnią rzeczą, jaka skonfiguruję dla tego obszaru nazw jest replikacja. Replikację konfiguruję za pomocą kreatora, który uruchamiam po kliknięciu prawym klawiszem myszy na węzeł **dokumenty** i wybieram opcję **replikuj folder**. Żeby folder mógł zostać replikowany, muszę ustalić **docelowe miejsce replikacji**. Wybieram folder udostępniony o nazwie **dokumenty** na serwerze2. Po wybraniu miejsca docelowego uruchamia się kreator tworzenia replikacji.

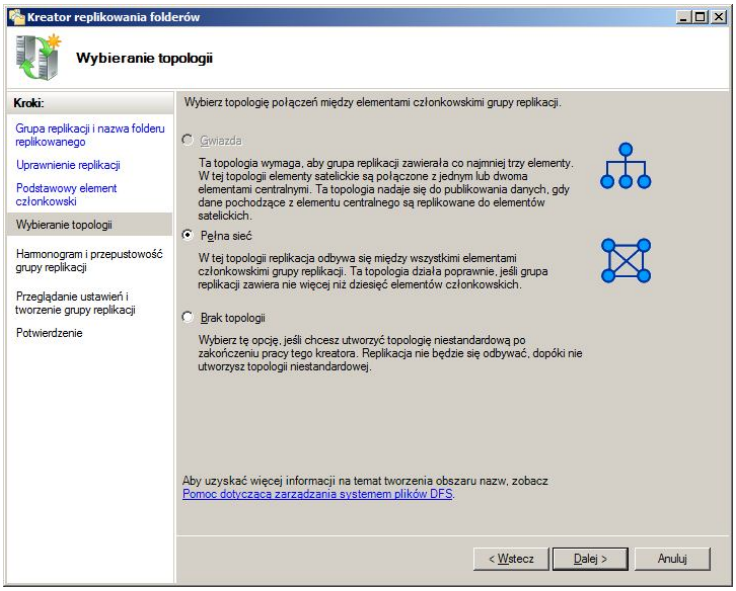
Rysunek nr 26 Kreator replikowania folderów część I



Źródło: *opracowanie własne*

Przy konfiguracji replikacji ustalam miedzy innymi podstawowy serwer członkowski. Ważną rzeczą, przy konfiguracji replikacji, jest wybranie topologii. Kreator umożliwia mi wybór kilku typów topologii.

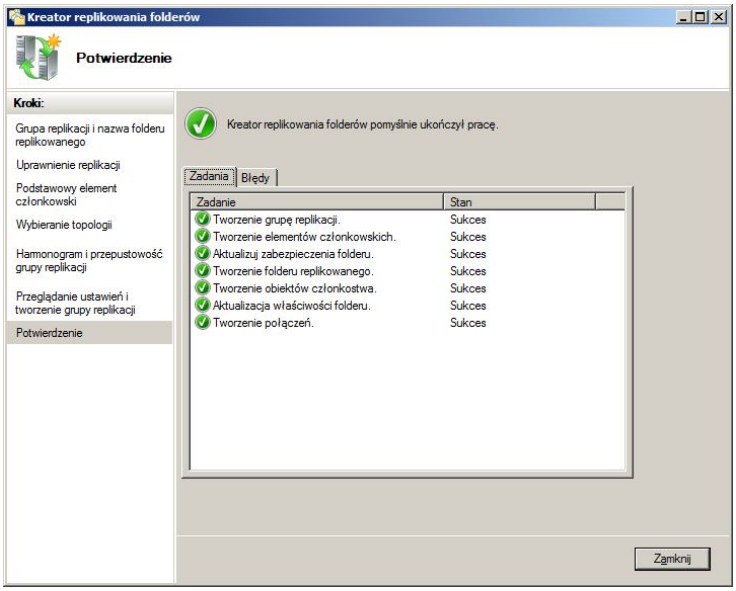
Rysunek nr 27 Kreator replikowania folderów część II



Źródło: *opracowanie własne*

Wybrałem ***pełną sieć***. Kolejnym ważnym etapem przy konfiguracji replikacji jest skonfigurowanie harmonogramu oraz przepustowości. Wybrałem pełną przepustowość. Po jej wybraniu kreator sprawdzi, czy wszystko zostało skonfigurowane poprawnie.

Rysunek nr 28 Kreator replikowania folderów część III



Źródło: *opracowanie własne*

W części poświęconej projektowi zabezpieczeń napisałem, że „każda z grup będzie miała swój własny zasób sieciowy". W tym celu utworzę katalogi na serwerach 1 i 2 oraz udostępnię je. Katalogi te **nazwę** tak samo, jak nazywają się **grupy**. Tworzę dla nich nowy obszar nazw **\\jaskulek.com\grupy\nazwagrupy**. Następnie dodam **udostępnione foldery** do obszaru nazw, i utworzę pełną replikacją dla tych folderów. Docelowe nazwy zasobów wyglądają następująco: **\\jaskulek.com\grupy\pracownicy, \\jaskulek.com\grupy\ksiegowi \\jaskulek.com\grupy\zarzad.**

Trzecim obszarem nazw będą zasoby przeznaczone na wnioski, oraz wspólne dane użytkowników. Docelowe nazwy zasobów wyglądają następująco: **\\jaskulek.com\pliki\wnioski, \\jaskulek.com\plik\wymianaplikow.**

Udostępniony folder **wnioski** będzie zawierał dla większości grup dane tylko do odczytu. Dla tego stworzę tak zwaną grupę cień Nazwę grupę **„uprawnieniadownioskow**" ułatwi mi to nadawanie uprawnień. Grupa „**uprawnieniadownioskow"**, zawiera grupy takie jak: ***księgowi, pracownicy, zwyklekontaadmini, zwyklekontahelpdesk***. Grupy „**uprawnieniadownioskow"** pozbawiłem uprawnień tworzenia i usuwania plików i folderów oraz przejmowania na własność i zmiany uprawnień. Pełną kontrolę ma grupa **zarząd,** ponieważ jest to zasób przeznaczony na informacje powiązane bezpośrednio z danymi osobowymi chronionymi ustawą RP. Natomiast zasób wymiana plików jest zasobem ogólnodostępnym. **Podsumowując, utworzyłem następujące zasoby.**

Tabela nr 10 Zasoby

Nazwa zasobu	Miejsce docelowe
\\jaskulek.com\dane\dokumenty\	Katalog użytkownika
\\jaskulek.com\grupy\	Ad mini
	Helpdesk
	Księgowi
	Pracownicy
	Zarząd
	Zwyklekontadmini
	Zwyklekontahelpdesk
\\jaskulek.com\it\	Sterowniki
\\jaskulek.com\pliki\	Wnioski
	Wymianaplikow

Źródło: *opracowanie własne*

6.2.5. Tworzenie użytkowników oraz konfiguracja użytkowników

Windows Server 2008 R2 pozwala na tworzenie użytkowników na kilka sposobów. Pierwszym sposobem jest tworzenie użytkowników za pomocą interfejsu graficznego. Przy dużej ilości użytkowników zajmowałoby to bardzo dużą ilość czasu. Drugim sposobem tworzenia użytkowników jest import listy użytkowników z pliku „nawa.csv" za pomocą skryptów PowerShell. W pracy będę stosował obie metody. W przedsiębiorstwie znajduje się jeden administrator i dla niego zostanie utworzone osobne konto administratora i konto do tzw. codziennego użytku. Na głównym koncie administratora, zostanie ustawione silne 10 – cio znakowe hasło, lecz konto to nie będzie wykorzystywane. Dział helpdesk posiada dwóch użytkowników. Dla nich, podobnie jak dla administratora, zostaną skonfigurowane konta codziennego użytku jak i konta administracyjne. Dział księgowości zawiera trzech użytkowników, podobnie jak zarząd. W przedsiębiorstwie pracuje określona liczba pracowników, ja natomiast dodam tylko pięćdziesięciu dziewięciu. Biorąc pod uwagę wcześniejsze założenia, każdy użytkownik będzie miał swój własny zasób sieciowy. Będzie

on znajdował się na serwerze 1, na dysku logicznym o nazwie „dane”. Każdy z użytkowników będzie dysponował przestrzenią dyskową wynoszącą 3GB. Użytkownicy będą mieli dostęp do wspólnego zasobu na dokumenty firmowe. Zasób ten będzie wynosił także 3GB. Każda z grup będzie też dysponowała zasobem sieciowym, ale tylko dana grupa danego zasobu będzie miała do takiego zasobu dostęp.

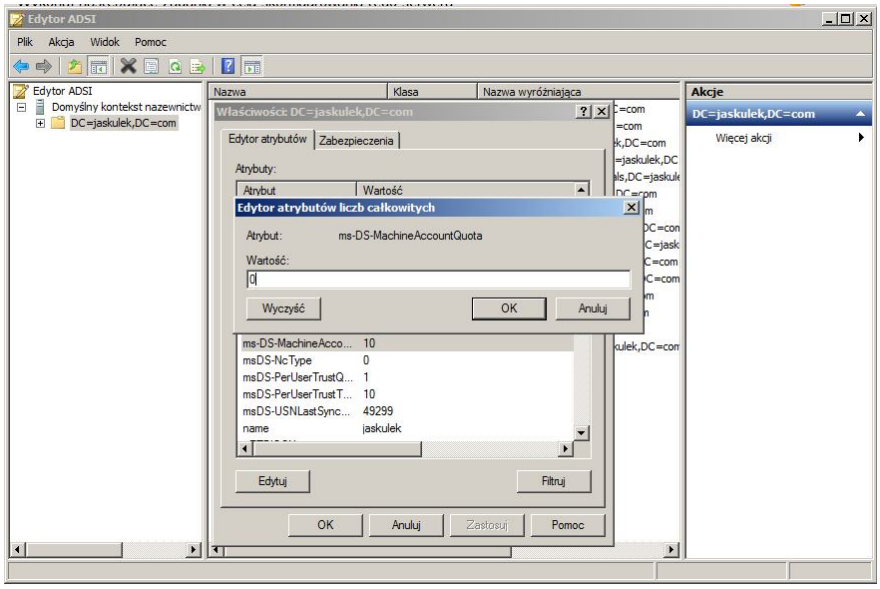
Za pomocą skryptu PowerShell dodałem użytkowników. Skrypt ten dodatkowo utworzył katalog użytkownika będący jego folderem macierzystym. Folder ten będzie dostępny jako zasób sieciowy „Z”. Skrypt nada również uprawnienia użytkownikowi do pełnej kontroli folderu właściciela, a ponadto skonfiguruje jego konto tak, aby ten po zalogowaniu zmienił swoje hasło.

```
$objOU=[ADSI]"LDAP://OU=uzytkownicy,OU=jaskulek,DC=jaskulek,DC=com"
$dataSource=import-csv "C:\nazwa.csv"
foreach($dataRecord in $datasource)
{
#pobieranieimieniainazwiska
$givenName=$dataRecord.imie
$sn=$dataRecord.nazwisko
#tworzeniezmiennych
$displayName=$givenName + " " + $sn
$sAMAccountName=$givenName + $sn
$userPrincipalName=$givenName + $sn + "@jaskulek.com"
$homeDrive="Z:"
$homeDirectory="\\jaskulek.com\dane\dokumenty\" + $sAMAccountName
$stanowisko="pracownik"
$miasto="lodz"
#tworzenieuzytkownikaiwypelnianiedanych
$objUser=$objOU.Create("user","CN="+$displayName)
$objUser.Put("sAMAccountName",$sAMAccountName)
$objUser.put("userPrincipalName",$userPrincipalName)
$objUser.Put("displayName",$displayName)
$objUser.Put("givenName",$givenName)
$objUser.Put("sn",$sn)
$objUser.Put("homeDrive",$homeDrive)
$objUser.Put("homeDirectory",$homeDirectory)
$objUser.Put("description",$stanowisko)
$objUser.Put("l",$miasto)
$objUser.SetInfo()
$objUser.SetPassword("P@ssw0rd")
$objUser.psbase.InvokeSet("AccountDisabled",$false)
$objUser.pwdLastSet = 0
$objUser.SetInfo()
#tworzenieorazudostepnianiakataloguoraznadwanieuprawnien
mkdir e:\dokumenty\$sAMAccountName
net share $sAMAccountName="e:\dokumenty\$sAMAccountName" "/grant:$sAMAccountName,FULL"
$polecenie = 'icacls' + ' "e:\dokumenty\' + $sAMAccountName + '" ' +  '/grant ' + '"' + $sAMAccountName +':f"'
cmd /c $polecenie
$objUser.SetInfo()
}
```

Źródło: opracowanie własne

Spowoduje to zwiększanie bezpieczeństwa, ponieważ tylko użytkownik będzie znał swoje hasło. Kolejną rzeczą, którą zablokuję w tej chwili jest wyłączenie możliwości dodawania komputera przez użytkownika.

Rysunek nr 29 Edytor ADSI część I



Źródło: *opracowanie własne*

6.2.6. Ustawienia GPO

6.2.6.1. Skrypty logowania

Tworzenie zasobów – jak napisałem w projekcie każdy użytkownik dodatkowo będzie dysponował zasobami, które utworzę za pomocą skryptów logowania.

Tabela nr 11 Nazwy zasobów

Etykieta zasobu	Kod skryptu logowania	Cel oraz dostęp
Y: (nazwa grupy)	net use y: /delete /yes net use y: *jaskulek.com**grupy**nazwagrypy*	Zasób przeznaczony do użytku na dane w grupie. Mają do niego dostęp wszystkie osoby z grupy; osoby z innych grup nie maja dostępu do niego.
X: wnioski	net use x: /delete /yes net use x: *jaskulek.com**pliki**wnioski*	Zasób przeznaczony jest dla wszystkich osób, przechowywane są na nim dane typu wnioski, wszystkie grupy poza zarządem mają tylko prawa odczytu, natomiast zarząd ma pełną kontrolę.
W: wymianaplikow	net use w: /delete /yes net use w: *jaskulek.com**plik**wymianaplikow*	Zasób przeznaczony na wymianę danych pomiędzy użytkownikami. Każdy użytkownik ma pełen dostęp.
V: sterowniki	net use v: /delete /yes net use v: *jaskulek.com**it**sterowniki*	Zasób przeznaczony dla administratorów oraz helpdesku. Nikt inny nie ma dostępu do niego

Źródło: opracowanie własne

6.2.6.2. Ustawianie haseł

Zanim przystąpię do konfiguracji haseł chciałbym nadmienić, że system Windows Server 2008 wprowadził nową opcję, mianowicie możliwość tworzenia różnych zasad haseł w domenie. Opcja ta zostanie przeze mnie wykorzystana, dlatego poświęcę chwilę na jej omówienie. Wcześniejsze systemy firmy Microsoft nie dawały możliwości tworzenia dowolnych zasad haseł. Wyjściem z takiej sytuacji było tworzenie dodatkowych domen.

W systemie przeze mnie omawianym (Windows 2008) opcja ta nazwana została **szczegółowymi zasadami haseł**. Do zaimplementowania tejże opcji istnieje inna klasa

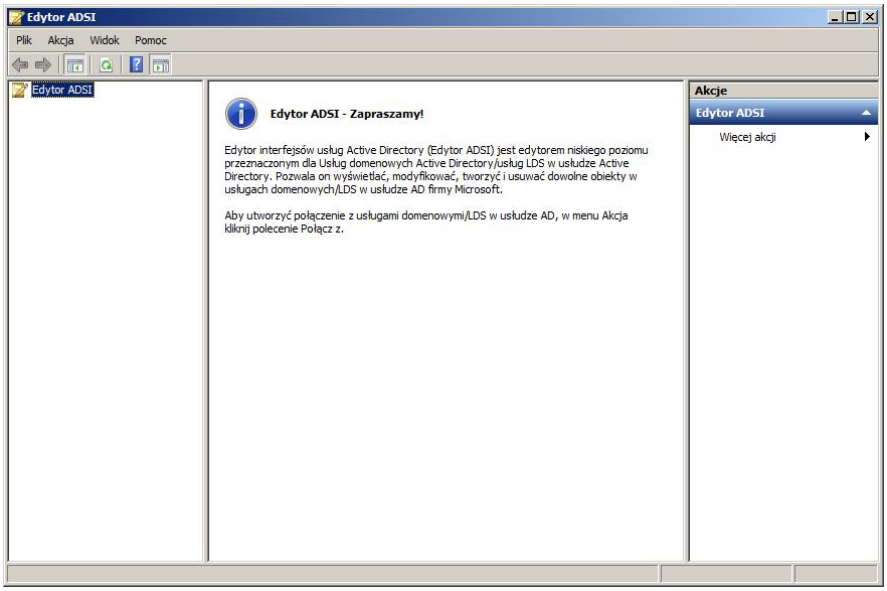
obiektu w Active Directory. Odpowiedzialna jest ona za utrzymywanie ustawień szczegółowych zasad haseł. Mowa tutaj o PSO czyli Password Setting Object. Do zarządzania ustawieniami szczegółowych zasad haseł w systemie Windows Server 2008 wykorzystuje się **Edytor ADSI**. Microsoft niestety nie utworzył własnego interfejsu graficznego do zarządzania szczegółowymi zasadami haseł. Istnieje jednak oprogramowanie firm nie związanych z koncernem Microsoft do zarządzania szczegółowymi zasadami haseł. Jednym ze znanych mi tego typu narzędzi jest program **Password Policy Basic** firmy **Special Operations Software**. Obiekty PSO mogę przyłączyć do **użytkowników** bądź **grup zabezpieczeń**. Ponadto każdy użytkownik lub grupa może mieć przyłączony więcej niż jeden obiekt PSO. Obiekty PSO nie mogą być natomiast przyłączone do jednostek organizacyjnych. Każdy obiekt PSO ma atrybut określający pierwszeństwo, stanowi to wartość większa **od 0 (liczbą minimalną, zarazem liczbą mającą najwyższe pierwszeństwo jest liczba 1)**. Atrybut ten będzie odgrywał istotne znaczenie w przypadku, gdy do użytkownika zostaną przypięte dwa inne obiekty PSO. W takiej sytuacji priorytetowym obiektem będzie obiekt PSO posiadający najwyższą wartość pierwszeństwa. Reguły określające taką wartość to:

- kiedy do grup zostało przyłączonych wiele obiektów GPO, a użytkownik należy do tych grup to stosowany jest obiekt PSO z priorytetowym pierwszeństwem.
- gdy do danego użytkownika zostało przypięte kilka obiektów PSO, należy przyjąć, że obiekty, które są przypięte do grup zostaną ignorowane. Sytuacja ma miejsce nawet wtedy, gdy obiekt podłączony do grupy ma najwyższe pierwszeństwo niż te przypięte do użytkownika. Obiektem, który zostanie zastosowany będzie obiekt przypięty do użytkownika z najwyższym pierwszeństwem.
- kiedy zajdzie sytuacja, gdy kilka obiektów PSO ma identyczną wartość pierwszeństwa, to samo Active Directory dokonuje wyboru. W takim przypadku zostanie wybrany obiekt PSO o najniższym globalnym unikatowym identyfikatorze (GUID). Identyfikatory te są unikatowe dla każdego obiektu PSO ale w szerszym aspekcie nie mają one konkretnego znaczenia.[2]

Jak wspominałem w projekcie zabezpieczeń, główne konto administratora będzie posiadało dziesięcioznakowe hasło a konta administracyjne będą korzystały z tej samej zasady.

Jak wspominałem istnieją dwie metody ustawiania szczegółowych zasad haseł. Ja będę korzystał z domyślnej opcji wbudowanej w system. W tym celu otwieram **Edytor ASDI**, który dostępny jest w **narzędziach administracyjnych**.

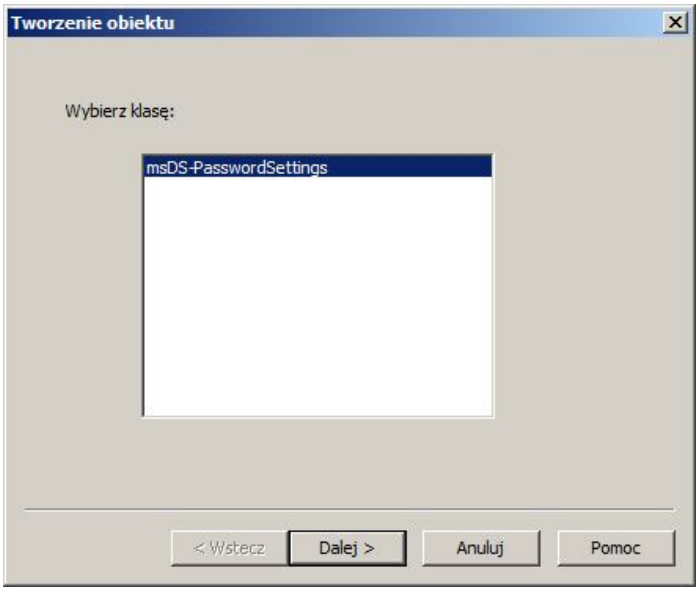
Rysunek nr 30 Edytor ADSI część II



Źródło: *opracowanie własne*

Następnie klikam prawym klawiszem myszy na **Edytor ADSI,** i wybieram z menu rozwijanego opcję **połącz z**. W następnym kroku wchodzę w węzeł **CN=system**, i wyszukuję w tym węźle linię **CN=Password Settings Container.** Klikam na nią prawym klawiszem myszy. Kiedy pojawi się **menu rozwijane** wybieram **opcję nowy** a następnie **obiekt**. Ukazuje się kreator tworzenia nowego obiektu.

Rysunek nr 31 Tworzenie obiektu PSO



Źródło: *opracowanie własne*

W tym kreatorze ustawiam szczegółowe zasady haseł. Tabelka (nr 12)przedstawia wszystkie opcje, przez które przeprowadza mnie kreator, ich wyjaśnienie oraz podane ustawienia. W niektórych atrybutach obowiązuje zapis **00:00:00:00** co oznacza **dni:godziny:minuty:sekundy**

Tabela nr 12 Opcje ustawień PSO

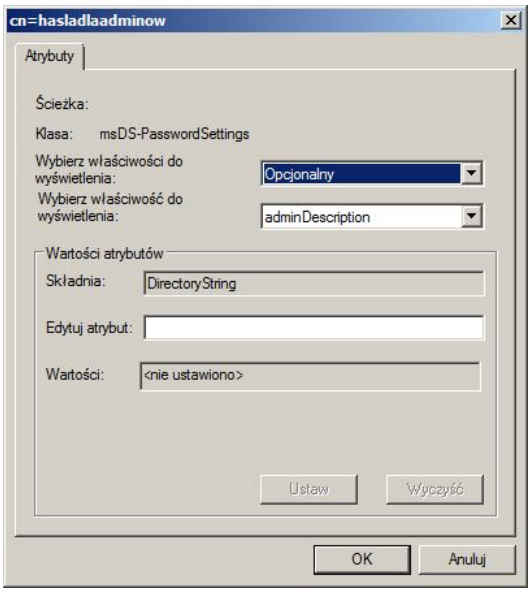
Nazwa	**opis**	**Podane przeze mnie dane**
Common-Name	Nazwa obiektu.	hasladlaadminow
msDS-PasswordSettingPrecedence	Określa pierwszeństwa obiektu.	1
msDS-PasswordReversibleEncryptionEnabled	Określa, czy hasło będzie przechowywane przy użyciu szyfrowania odwracalnego.	False
msDS-PasswordHistoryLength	Ilość zapamiętanych haseł(cała całkowita).	30
msDS-PasswordCompexityEnabled	Określa, czy zostały	True

	włączone reguły skomplikowanych haseł.	
msDS-MinimumPasswordLength	Określa minimalną długość hasła w znakach (całkowita wartość).	15
msDS-MinimumPasswordAge	Określa minimalny czas kiedy użytkownik może zmienić hasło, od poprzedniej zmiany.	2:00:00:00
msDS-MaximumPasswordAge	Określa co ile hasło musi być zmienione.	60:00:00:00
msDS-LockoutThreshold	Określa ilość niepoprawnych logowań (wartość całkowita). Atrybut ten jest powiązany z atrybutem poniżej, ponieważ ilość logowań odnosi się do czasu w jakim te logowania następują.	5
msDS-LockoutObservationWindow	Czas w jakim ilość nieporwanych logowań spowoduje blokadę konta.	0:02:00:00
msDS-LockoutDuration	Określa czas w jakim konto pozostanie zablokowane. Wartość 0 spowoduje opcję, że tylko administrator musi odblokować konto	2:00:00:00

Źródło: *opracowanie własne*

Taka konfiguracja **nie ustawi** dla danego użytkownika bądź grupy szczegółowych zasad hasła. Aby to się stało, na ostatniej stronie kreatora wybieram opcję **edytor atrybutów**.

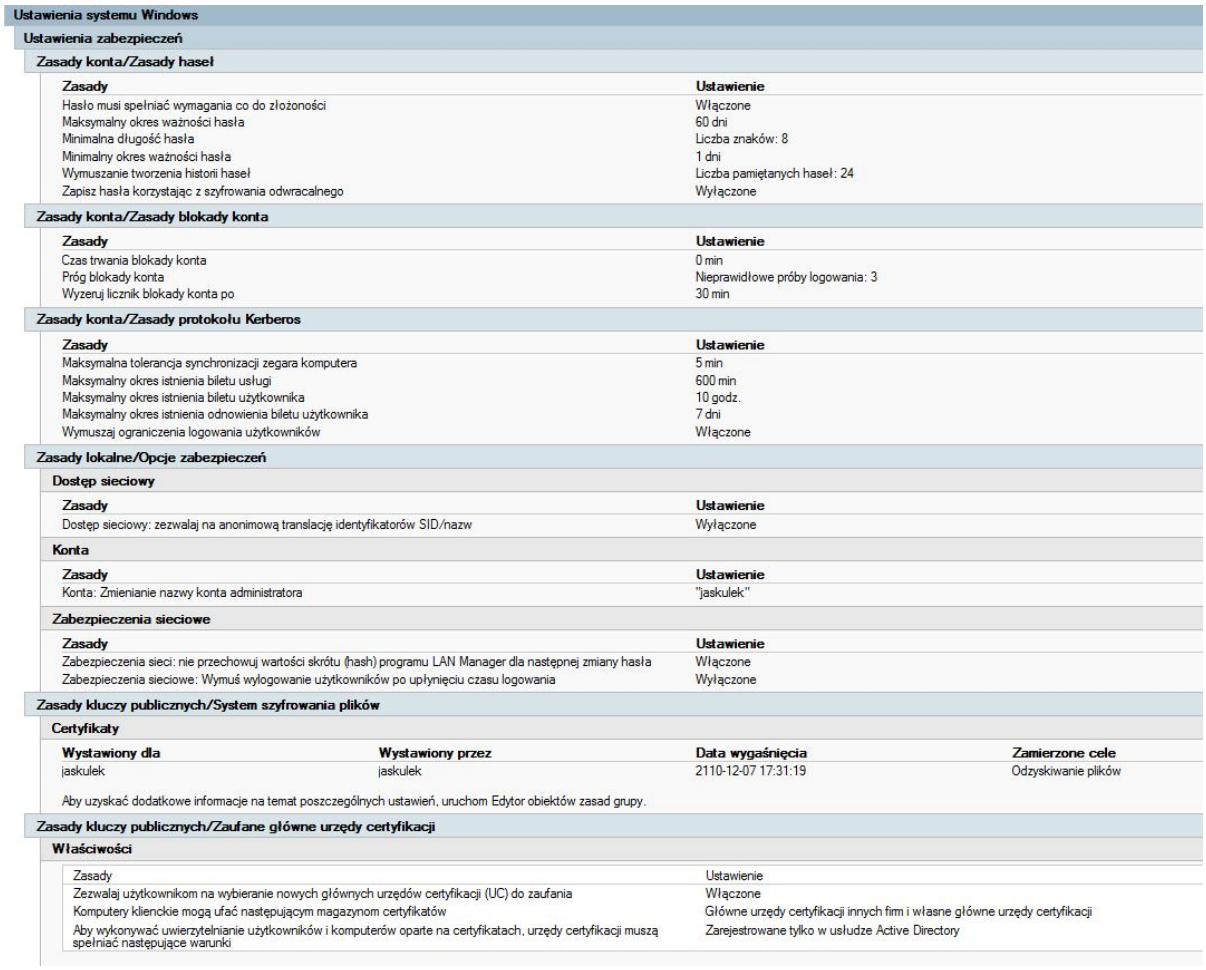
Rysunek nr 32 Dodanie obiektu PSO do gruby lub użytkownika



Źródło: *opracowanie własne*

Następnie wybieram z **drugiego menu** rozwianego opcję **msDS-PSOAppliesTo** i w polu **Edytuj atrybut** wpisuję **CN=DomainAdmins,CN=Users,DC=jaskulek,DC=com**. Dopiero teraz szczegółowe zasady haseł zostały ustawione dla **grupy Domain Admins i grup z nią powiązanych**. Konta dla helpdesku będą korzystały z ogólnych zasad haseł. Dla wszystkich innych kont zaktualizowałem domyślne ustawienia zasad haseł w ustawieniach GPO. Zmiany dotyczyć będą **długości haseł,** natomiast czas zamiany hasła przez użytkownika będzie wynosił **sześćdziesiąt dni**. Nadmieniam, że **trzy błędne** próby zalogowania na konto użytkownika spowodują jego **blokadę.** Dodatkowo ustawiłem politykę, która w swoim założeniu zmienia **nazwę konta administratora**. Poszczególne ustawienia przedstawia poniższy rysunek.

Rysunek nr 33 Ustawienia globalne haseł poprzez GPO



Ustawienia systemu Windows

Ustawienia zabezpieczeń

Zasady konta/Zasady haseł

Zasady	Ustawienie
Hasło musi spełniać wymagania co do złożoności	Włączone
Maksymalny okres ważności hasła	60 dni
Minimalna długość hasła	Liczba znaków: 8
Minimalny okres ważności hasła	1 dni
Wymuszanie tworzenia historii haseł	Liczba pamiętanych haseł: 24
Zapisz hasła korzystając z szyfrowania odwracalnego	Wyłączone

Zasady konta/Zasady blokady konta

Zasady	Ustawienie
Czas trwania blokady konta	0 min
Próg blokady konta	Nieprawidłowe próby logowania: 3
Wyzeruj licznik blokady konta po	30 min

Zasady konta/Zasady protokołu Kerberos

Zasady	Ustawienie
Maksymalna tolerancja synchronizacji zegara komputera	5 min
Maksymalny okres istnienia biletu usługi	600 min
Maksymalny okres istnienia biletu użytkownika	10 godz.
Maksymalny okres istnienia odnowienia biletu użytkownika	7 dni
Wymuszaj ograniczenia logowania użytkowników	Włączone

Zasady lokalne/Opcje zabezpieczeń

Dostęp sieciowy

Zasady	Ustawienie
Dostęp sieciowy: zezwalaj na anonimową translację identyfikatorów SID/nazw	Wyłączone

Konta

Zasady	Ustawienie
Konta: Zmienianie nazwy konta administratora	"jaskulek"

Zabezpieczenia sieciowe

Zasady	Ustawienie
Zabezpieczenia sieci: nie przechowuj wartości skrótu (hash) programu LAN Manager dla następnej zmiany hasła	Włączone
Zabezpieczenia sieciowe: Wymuś wylogowanie użytkowników po upłynięciu czasu logowania	Wyłączone

Zasady kluczy publicznych/System szyfrowania plików

Certyfikaty

Wystawiony dla	Wystawiony przez	Data wygaśnięcia	Zamierzone cele
jaskulek	jaskulek	2110-12-07 17:31:19	Odzyskiwanie plików

Aby uzyskać dodatkowe informacje na temat poszczególnych ustawień, uruchom Edytor obiektów zasad grupy.

Zasady kluczy publicznych/Zaufane główne urzędy certyfikacji

Właściwości

Zasady	Ustawienie
Zezwalaj użytkownikom na wybieranie nowych głównych urzędów certyfikacji (UC) do zaufania	Włączone
Komputery klienckie mogą ufać następującym magazynom certyfikatów	Główne urzędy certyfikacji innych firm i własne główne urzędy certyfikacji
Aby wykonywać uwierzytelnianie użytkowników i komputerów oparte na certyfikatach, urzędy certyfikacji muszą spełniać następujące warunki	Zarejestrowane tylko w usłudze Active Directory

Źródło: *opracowanie własne*

6.2.6.3. Zabezpieczania GPO dla pracowników, zarządu, księgowych.

Ustawienia zasad GPO jest szeroko rozumianym spektrum podczas konfiguracji. Dlatego w tym punkcie omówię kilka ustawień które postanowiłem zaimplementować w opisywanym systemie. Na początku wyłączyłem użytkownikom możliwość dodawania i usuwania **mapowania dysków sieciowych**. Następnie zablokowałem możliwość zapisu na płytach CD/DVD oraz na nośnikach wymiennych. Ponadto poszerzyłem już domyślne ustawienia zmian konfiguracji komputera przez użytkownika. Szczegółowe opcje bieżącej konfiguracji przedstawia rysunek 34.

Rysunek nr 34 Ustawienia GPO

Zasady

Szablony administracyjne

Definicje zasad (pliki ADMX) pobrane z komputera lokalnego.

Menu Start i pasek zadań

Zasady	Ustawienie
Dodaj element Wyloguj do menu Start	Włączone
Dodaj łącze Wyszukaj w Internecie do menu Start	Włączone
Dodaj pole wyboru „Uruchom w oddzielnym obszarze pamięci" do okna dialogowego Uruchamianie	Wyłączone
Dodaj polecenie Uruchom do menu Start	Wyłączone
Nie przechowuj historii niedawno otwieranych dokumentów	Wyłączone
Nie używaj metody opartej na śledzeniu podczas rozpoznawania skrótów powłoki	Wyłączone
Nie używaj metody opartej na wyszukiwaniu podczas rozpoznawania skrótów powłoki	Wyłączone
Nie wyszukuj komunikacji	Wyłączone
Nie wyszukuj plików	Wyłączone
Nie wyszukuj programów i elementów Panelu sterowania	Włączone
Nie wyszukuj w Internecie	Włączone
Nie wyświetlaj i nie śledź elementów list szybkiego dostępu znajdujących się w lokalizacjach zdalnych	Wyłączone
Nie wyświetlaj żadnych niestandardowych pasków narzędzi na pasku zadań	Włączone
Nie zezwalaj na przypinanie elementów do list szybkiego dostępu	Wyłączone
Nie zezwalaj na przypinanie programów do paska zadań	Wyłączone
Pokaż obszar szybkiego uruchamiania na pasku zadań	Włączone
Ukryj obszar powiadomień	Wyłączone
Uniemożliwiaj użytkownikom dodawanie lub usuwanie pasków narzędzi	Włączone
Uniemożliwiaj użytkownikom przenoszenie paska zadań do innej lokalizacji dokowania ekranu	Włączone
Uniemożliwiaj użytkownikom zmianę rozmiaru paska zadań	Włączone
Uniemożliwiaj użytkownikom zmianę rozmieszczenia pasków narzędzi	Włączone
Usuń element Połączenia sieciowe z menu Start	Wyłączone
Usuń foldery użytkownika z menu Start	Wyłączone
Usuń ikonę Centrum akcji	Wyłączone
Usuń ikonę Dokumenty z menu Start	Wyłączone
Usuń ikonę Muzyka z menu Start	Wyłączone
Usuń ikonę Obrazy z menu Start	Wyłączone
Usuń ikonę regulacji głośności	Wyłączone
Usuń ikonę sieci	Wyłączone
Usuń ikonę Sieć z menu Start	Wyłączone
Usuń listę często używanych programów z menu Start	Wyłączone
Usuń listę programów przypiętych do menu Start	Wyłączone
Usuń listę Wszystkie programy z menu Start	Wyłączone
Usuń łącza i wyłącz dostęp do witryny Windows Update	Włączone
Usuń łącze do folderu użytkownika z menu Start	Wyłączone
Usuń łącze Grupa domowa z menu Start	Włączone
Usuń łącze Gry z menu Start	Włączone
Usuń łącze Nagrania telewizyjne z menu Start	Włączone
Usuń łącze Pobieranie z menu Start	Wyłączone
Usuń łącze Programy domyślne z menu Start	Wyłączone
Usuń łącze Wideo z menu Start	Wyłączone
Usuń łącze Wyszukaj na komputerze	Wyłączone
Usuń łącze Wyszukaj z menu Start	Wyłączone
Usuń łącze Wyświetl więcej wyników/Szukaj wszędzie	Wyłączone
Usuń menu Bieżące elementy z menu Start	Wyłączone

c.d

Usuń menu Pomoc z menu Start	Wyłączone
Usuń menu Ulubione z menu Start	Wyłączone
Usuń menu Uruchom z menu Start	Włączone
Usuń miernik baterii	Wyłączone
Usuń nazwę użytkownika z menu Start	Wyłączone
Usuń opcję przeciągania i upuszczania oraz menu kontekstowe z menu Start	Włączone
Usuń opcję Wyloguj z menu Start	Wyłączone
Usuń polecenia Zamknij, Uruchom ponownie, Uśpienie i Hibernacja oraz wyłącz dostęp do nich	Wyłączone
Usuń porady dymkowe dla elementów menu Start	Wyłączone
Usuń programy z menu Ustawienia	Włączone
Usuń przycisk „Oddokuj komputer" z menu Start	Wyłączone
Usuń przypięte programy z paska zadań	Wyłączone
Usuń wspólne grupy programów z menu Start	Włączone
Usuń zegar z obszaru powiadomień systemu	Wyłączone
Wyczyść historię niedawno otwieranych dokumentów przy zakończeniu	Włączone
Wyczyść listę ostatnio uruchamianych programów dla nowych użytkowników	Włączone
Wygaś skróty niedostępnych programów Instalatora Windows w menu Start	Włączone
Wyłącz automatyczne przenoszenie ikon powiadomień na pasek zadań	Wyłączone
Wyłącz dostęp do kontekstowych menu paska zadań	Włączone
Wyłącz dymki powiadomień z anonsami funkcji	Wyłączone
Wyłącz menu spersonalizowane	Wyłączone
Wyłącz miniatury paska zadań	Wyłączone
Wyłącz oczyszczanie obszaru powiadomień	Włączone
Wyłącz śledzenie użytkownika	Wyłączone
Wyłącz wszystkie dymki powiadomień	Wyłączone
Wymuszaj klasyczne menu Start	Wyłączone
Zablokuj pasek zadań	Włączone
Zablokuj wszystkie ustawienia paska zadań	Włączone
Zapobiegaj grupowaniu elementów paska zadań	Włączone
Zapobiegaj zmianom ustawień Paska zadań i menu Start	Włączone
Zmień przycisk zasilania w menu Start	Wyłączone

Panel sterowania

Zasady	Ustawienie
Zabroń dostępu do Panelu sterowania	Wyłączone

Panel sterowania/Dodaj lub usuń programy

Zasady	Ustawienie
Określ domyślną kategorię dla strony Dodaj nowe programy	Wyłączone
Przejdź bezpośrednio do Kreatora składników	Włączone
Ukryj opcję „Dodaj program z dysku CD-ROM lub z dyskietki"	Włączone
Ukryj opcję „Dodaj programy z firmy Microsoft"	Włączone
Ukryj opcję „Dodaj programy z sieci lokalnej"	Włączone
Ukryj stronę Dodaj nowe programy	Włączone
Ukryj stronę Dodaj/Usuń składniki systemu Windows	Włączone
Ukryj stronę Określ dostęp do programów i ustawienia domyślne	Włączone
Ukryj stronę Zmień lub usuń programy	Włączone
Usuń aplet Dodaj lub usuń programy	Włączone
Usuń informacje pomocy technicznej	Wyłączone

Panel sterowania/Drukarki

Zasady	Ustawienie
Pakietowa funkcja wskazywania i drukowania — zatwierdzone serwery	Wyłączone
Przeglądaj sieć w poszukiwaniu drukarek	Włączone

c.d

Przeglądaj wspólną witrynę sieci Web w poszukiwaniu drukarek	Wyłączone
Wskazywanie i drukowanie wyłącznie pakietów	Wyłączone
Zapobiegaj dodawaniu drukarek	Włączone
Zapobiegaj usuwaniu drukarek	Włączone

Panel sterowania/Ekran

Zasady	Ustawienie
Ukryj kartę Ustawienia	Włączone
Wyłącz element Ekran w Panelu sterowania	Włączone

Panel sterowania/Opcje regionalne i językowe

Zasady	Ustawienie
Ogranicz języki interfejsu użytkownika, które powinny być używane przez system Windows dla wybranego użytkownika	Włączone
Ogranicz użytkowników do następującego języka:	

Zasady	Ustawienie
Ukryj opcje administracyjne apletu Opcje regionalne i językowe	Włączone
Ukryj opcje grupowe wyboru języka	Włączone
Ukryj opcje wybierania i dostosowywania ustawień regionalnych użytkownika	Włączone
Ukryj opcję lokalizacji geograficznej	Włączone

Panel sterowania/Personalizacja

Zasady	Ustawienie
Limit czasu wygaszacza ekranu	Włączone
Czas oczekiwania na włączenie wygaszacza ekranu w sekundach Sekundy:	

Zasady	Ustawienie
Ładuj określoną kompozycję	Wyłączone
Włącz wygaszacz ekranu	Włączone
Wygaszacz ekranu chroniony hasłem	Włączone
Wymuszaj określony styl wizualny lub wymuszaj zastosowanie stylu Klasyczny Windows	Wyłączone
Wymuszaj określony wygaszacz ekranu	Wyłączone
Zabroń wybierania rozmiaru czcionki stylu wizualnego	Włączone
Zapobiegaj zmienianiu dźwięków	Włączone
Zapobiegaj zmienianiu ikon pulpitu	Włączone
Zapobiegaj zmienianiu kolorów i wyglądu okien	Włączone
Zapobiegaj zmienianiu kompozycji	Włączone
Zapobiegaj zmienianiu schematu kolorów	Włączone
Zapobiegaj zmienianiu stylu wizualnego okien i przycisków	Włączone
Zapobiegaj zmienianiu tła pulpitu	Włączone
Zapobiegaj zmienianiu wskaźników myszy	Włączone
Zapobiegaj zmienianiu wygaszacza ekranu	Włączone

Panel sterowania/Programy

Zasady	Ustawienie
Ukryj aplet Funkcje systemu Windows	Włączone
Ukryj aplet Programy w Panelu sterowania	Włączone
Ukryj stronę Określ dostęp do programów i ich ustawienia domyślne	Włączone
Ukryj stronę Programy i funkcje	Włączone
Ukryj stronę Uzyskaj programy	Włączone
Ukryj stronę Zainstalowane aktualizacje	Wyłączone
Ukryj witrynę Windows Marketplace	Włączone

c.d

Pulpit

Zasady	Ustawienie
Nie dodawaj udziałów niedawno otwieranych dokumentów do folderu Miejsca w sieci	Włączone
Nie zapisuj ustawień przy zakończeniu	Wyłączone
Ukryj i wyłącz wszystkie elementy pulpitu	Wyłączone
Ukryj ikonę Miejsca w sieci na pulpicie	Wyłączone
Ukryj ikonę programu Internet Explorer na pulpicie	Wyłączone
Usuń ikonę Komputer z pulpitu	Wyłączone
Usuń ikonę Kosz z pulpitu	Wyłączone
Usuń ikonę Moje dokumenty z pulpitu	Wyłączone
Usuń Kreatora oczyszczania pulpitu	Wyłączone
Usuń polecenie Właściwości z menu kontekstowego ikony Komputer	Włączone
Usuń polecenie Właściwości z menu kontekstowego ikony Kosz	Wyłączone
Wyłącz gest wstrząsania myszy interfejsu Aero minimalizujący okna	Wyłączone
Zabroń dodawania, przeciągania, upuszczania i zamykania pasków narzędzi paska zadań	Włączone
Zabroń dopasowywania pasków narzędzi pulpitu	Włączone
Zabroń użytkownikowi ręcznego przekierowywania folderów profilów	Wyłączone

Pulpit/Active Desktop

Zasady	Ustawienie
Tapeta pulpitu	Wyłączone
Włącz pulpit Active Desktop	Włączone

Zezwalaj na tapetę HTML i JPEG

Zasady	Ustawienie
Wyłącz pulpit Active Desktop	Wyłączone
Wyłącz wszystkie elementy	Wyłączone
Zabroń dodawania elementów	Włączone
Zabroń edytowania elementów	Włączone
Zabroń usuwania elementów	Włączone
Zabroń zamykania elementów	Włączone
Zabroń zmian	Włączone
Zezwalaj tylko na tapetę w formacie mapy bitowej	Wyłączone

Pulpit/Usługa Active Directory

Zasady	Ustawienie
Ukryj folder Active Directory	Włączone
Włącz filtr w oknie Znajdowanie	Włączone

Sieć/Połączenia sieciowe

Zasady	Ustawienie
Możliwość usuwania połączeń dostępu zdalnego wszystkich użytkowników	Włączone
Możliwość włączenia/wyłączenia połączenia LAN	Włączone
Możliwość zmiany nazw połączeń dostępu zdalnego wszystkich użytkowników	Wyłączone
Możliwość zmiany nazw połączeń sieci LAN	Wyłączone
Możliwość zmiany nazw połączeń sieci LAN lub połączeń dostępu zdalnego dostępnych dla wszystkich użytkowników	Wyłączone
Możliwość zmiany właściwości połączenia dostępu zdalnego dla wszystkich użytkowników	Włączone
Włącz ustawienia połączeń sieciowych systemu Windows 2000 dla administratorów	Włączone
Wyłącz powiadomienia, jeśli połączenie ma ograniczoną łączność lub brak łączności	Wyłączone
Zabroń dodawania i usuwania składników dla połączenia sieci LAN lub dostępu zdalnego	Włączone
Zabroń dostępu do elementu Preferencje dostępu zdalnego w menu Zaawansowane	Włączone
Zabroń dostępu do elementu Ustawienia zaawansowane w menu Zaawansowane	Włączone

c.d

Zabroń dostępu do Kreatora nowego połączenia	Włączone
Zabroń dostępu do właściwości połączenia LAN	Włączone
Zabroń dostępu do właściwości składników połączenia dostępu zdalnego	Włączone
Zabroń dostępu do właściwości składników połączenia LAN	Włączone
Zabroń konfiguracji zaawansowanej TCP/IP	Włączone
Zabroń podłączania i rozłączania połączenia dostępu zdalnego	Włączone
Zabroń usuwania połączeń dostępu zdalnego	Włączone
Zabroń włączania/wyłączania składników połączenia LAN	Wyłączone
Zabroń wyświetlania stanu aktywnego połączenia	Wyłączone
Zabroń zmiany nazwy prywatnych połączeń dostępu zdalnego	Wyłączone
Zabroń zmiany właściwości prywatnego połączenia dostępu zdalnego	Włączone

Składniki systemu Windows/Eksplorator Windows

Zasady	Ustawienie
Maksymalna liczba niedawno otwieranych dokumentów	Włączone

Maksymalna liczba niedawno otwieranych dokumentów

Zasady	Ustawienie
Nie śledź skrótów powłoki podczas przechodzenia	Wyłączone
Nie wyświetlaj składnika System Windows — Zapraszamy! przy logowaniu użytkownika	Włączone
Nie zezwalaj użytkownikom na dodawanie plików do ich głównego folderu Pliki użytkowników.	Wyłączone
Nie żądaj alternatywnych poświadczeń	Wyłączone
Przypnij witryny wyszukiwania w Internecie do łączy „Wyszukaj ponownie" i menu Start	Wyłączone
Ukryj element Zarządzaj w menu kontekstowym Eksploratora Windows	Włączone
Ukryj określone tutaj dyski w oknie Mój komputer	Włączone

Wybierz jedną z następujących kombinacji

Zasady	Ustawienie
Usuń domyślne menu kontekstowe Eksploratora Windows	Wyłączone
Usuń folder Dokumenty udostępnione z folderu Mój komputer	Wyłączone
Usuń funkcje nagrywania dysków CD	Włączone
Usuń interfejs użytkownika do zmiany ustawienia animacji menu	Wyłączone
Usuń interfejs użytkownika do zmiany ustawienia wskaźnika nawigacji klawiaturą	Wyłączone
Usuń kartę DFS	Wyłączone
Usuń kartę Sprzęt	Włączone
Usuń kartę Zabezpieczenia	Włączone
Usuń łącze wyszukiwania w Internecie „Wyszukaj ponownie"	Włączone
Usuń menu Plik z Eksploratora Windows	Wyłączone
Usuń opcje „Mapuj dysk sieciowy" i „Odłącz dysk sieciowy"	Włączone
Usuń przycisk Wyszukaj z Eksploratora Windows	Wyłączone
Usuwa element menu Opcje folderów z menu Narzędzia	Włączone
Włącz powłokę klasyczną	Wyłączone
Wyłącz bezpośrednie powiązanie z interfejsem IPropertySetStorage bez warstw pośrednich.	Wyłączone
Wyłącz buforowanie miniatur	Wyłączone
Wyłącz buforowanie miniatur w ukrytych plikach thumbs.db	Wyłączone
Wyłącz funkcje bibliotek systemu Windows, które zależą od indeksowanych danych pliku	Wyłączone
Wyłącz sortowanie liczbowe w Eksploratorze Windows	Wyłączone
Wyłącz wyświetlanie miniatur i wyświetlaj tylko ikony	Wyłączone
Wyłącz wyświetlanie miniatur i wyświetlaj tylko ikony w folderach sieciowych	Wyłączone
Wyłącz wyświetlanie niedawnych wpisów wyszukiwania w polu wyszukiwania Eksploratora Windows	Wyłączone

c.d

Zasady	Ustawienie
Wyświetl okno dialogowe potwierdzenia podczas usuwania plików	Włączone
Wyświetl pasek menu w Eksploratorze Windows	Włączone

Składniki systemu Windows/Gadżety pulpitu

Zasady	Ustawienie
Ogranicz rozpakowywanie i instalację gadżetów bez podpisu cyfrowego.	Włączone
Wyłącz gadżety pulpitu	Wyłączone
Wyłącz gadżety pulpitu zainstalowane przez użytkownika	Wyłączone
Zastąp łącze Więcej gadżetów	Wyłączone

Składniki systemu Windows/Harmonogram zadań

Zasady	Ustawienie
Ukryj pole wyboru Właściwości zaawansowane w Kreatorze dodawania zaplanowanego zadania	Włączone
Ukryj strony właściwości	Włączone
Zabroń przeglądania	Włączone
Zabroń stosowania metody przeciągnij i upuść	Wyłączone
Zabroń tworzenia nowych zadań	Włączone
Zabroń usuwania zadań	Włączone
Zapobiegaj uruchamianiu i kończeniu zadań	Włączone

Składniki systemu Windows/Instalator Windows

Zasady	Ustawienie
Wyłącz źródło nośników wymiennych dla każdej instalacji	Włączone
Zabroń wycofywania	Włączone
To ustawienie można określić dla komputera lub dla użytkownika.	

Składniki systemu Windows/Internet Explorer/Internetowy panel sterowania/Strona Zaawansowane

Zasady	Ustawienie
Zezwalaj na uruchamianie aktywnej zawartości dysków CD na komputerach użytkowników	Włączone

Składniki systemu Windows/Internet Explorer/Usuń historię przeglądania

Zasady	Ustawienie
Zapobiegaj usuwaniu haseł	Włączone

Składniki systemu Windows/Kalendarz systemu Windows

Zasady	Ustawienie
Wyłącz Kalendarz systemu Windows	Wyłączone

Składniki systemu Windows/Kolory w systemie Windows

Zasady	Ustawienie
Zabroń instalowania lub odinstalowywania profili kolorów	Włączone

Składniki systemu Windows/Kopia zapasowa/Klient

Zasady	Ustawienie
Nie zezwalaj użytkownikowi na uruchamianie programu Stan i konfiguracja kopii zapasowej	Włączone
Wyłącz funkcję przywracania	Włączone
Wyłącz możliwość tworzenia obrazu systemu	Włączone
Wyłącz możliwość wykonywania kopii zapasowych plików danych	Włączone
Zapobiegaj tworzeniu kopii zapasowych na dyskach lokalnych	Włączone
Zapobiegaj tworzeniu kopii zapasowych na nośnikach optycznych (CD/DVD)	Włączone

c.d

Zapobiegaj tworzeniu kopii zapasowych w lokalizacji sieciowej	Włączone

Składniki systemu Windows/Lokalizacja i czujniki

Zasady	Ustawienie
Wyłącz czujniki	Włączone
Wyłącz lokalizację	Włączone
Wyłącz skrypty lokalizacji	Włączone

Składniki systemu Windows/Menedżer okien pulpitu

Zasady	Ustawienie
Nie zezwalaj na animacje okien	Wyłączone
Nie zezwalaj na kompozycje pulpitu	Wyłączone
Nie zezwalaj na wywołanie funkcji przerzucania 3W	Wyłączone

Składniki systemu Windows/Opcje logowania systemu Windows

Zasady	Ustawienie
Ustaw akcję wykonywaną po upływie czasu logowania	Włączone
Ustaw akcję wykonywaną po upływie czasu logowania	

Zasady	Ustawienie
Usuń ostrzeżenia o upłynięciu czasu logowania	Wyłączone
Zgłoś, gdy serwer logowania był niedostępny podczas logowania użytkownika	Włączone

Składniki systemu Windows/Program Microsoft Management Console/Przystawki zabronione/dopuszczalne

Zasady	Ustawienie
Konfiguracja usług pulpitu zdalnego	Włączone
Zarządzanie dyskami	Wyłączone
Zarządzanie komputerem	Wyłączone
Zarządzanie magazynami wymiennymi	Wyłączone
Zarządzanie modułem TPM	Wyłączone

Składniki systemu Windows/Program Microsoft Management Console/Przystawki zabronione/dopuszczalne/Przystawki rozszerzeń

Zasady	Ustawienie
Zarządzanie protokołem DHCP Relay	Wyłączone

Składniki systemu Windows/Udostępnianie w sieci

Zasady	Ustawienie
Zapobiegaj udostępnianiu przez użytkowników plików w obrębie ich profilu	Włączone

Składniki systemu Windows/Usługa Windows Update

Zasady	Ustawienie
Usuń dostęp do używania wszystkich funkcji witryny Windows Update	Wyłączone

Składniki systemu Windows/Usługi pulpitu zdalnego/Host sesji pulpitu zdalnego/Połączenia

Zasady	Ustawienie
Ustaw reguły zdalnego sterowania dla sesji użytkowników usług pulpitu zdalnego	Włączone
Opcje:	

Składniki systemu Windows/Windows Anytime Upgrade

Zasady	Ustawienie
Zapobiega uruchomieniu usługi Windows Anytime Upgrade.	Wyłączone

c.d

Składniki systemu Windows/Windows Media Center	
Zasady	**Ustawienie**
Nie zezwalaj na uruchamianie programu Windows Media Center	Włączone

Składniki systemu Windows/Windows PowerShell	
Zasady	**Ustawienie**
Turn on Script Execution	Wyłączone

System	
Zasady	**Ustawienie**
Zapobiegaj dostępowi do narzędzi edycji rejestru	Włączone
Czy wyłączyć pracę programu regedit w trybie cichym?	

System/Dostęp do magazynu wymiennego	
Zasady	**Ustawienie**
Dysk CD i DVD: odmowa dostępu do odczytu	Wyłączone
Dysk CD i DVD: odmowa prawa do zapisu	Włączone
Dyski wymienne: odmowa dostępu do odczytu	Wyłączone
Dyski wymienne: odmowa prawa do zapisu	Włączone
Klasy niestandardowe: odmowa dostępu do odczytu	Wyłączone
Stacje dyskietek: odmowa dostępu do odczytu	Wyłączone
Stacje dyskietek: odmowa prawa do zapisu	Włączone
Stacje taśm: odmowa dostępu do odczytu	Wyłączone
Stacje taśm: odmowa prawa do zapisu	Włączone
Urządzenia WPD: odmowa dostępu do odczytu	Wyłączone
Urządzenia WPD: odmowa prawa do zapisu	Włączone
Wszystkie klasy magazynów wymiennych: odmowa dostępu	Wyłączone

System/Funkcja Windows HotStart	
Zasady	**Ustawienie**
Wyłącz funkcję Windows HotStart	Wyłączone

System/Instalacja sterowników	
Zasady	**Ustawienie**
Konfiguruj lokalizacje wyszukiwania sterowników	Włączone
Nie wyszukuj w stacjach dyskietek	
Nie wyszukuj w stacjach CD-ROM	
Nie wyszukuj w witrynie Windows Update	
Zasady	**Ustawienie**
Podpisywanie kodu dla sterowników urządzeń	Włączone
Kiedy system Windows wykryje plik sterownika bez podpisu cyfrowego:	
Zasady	**Ustawienie**
Wyłącz monit wyszukiwania sterowników urządzeń w witrynie Windows Update	Włączone

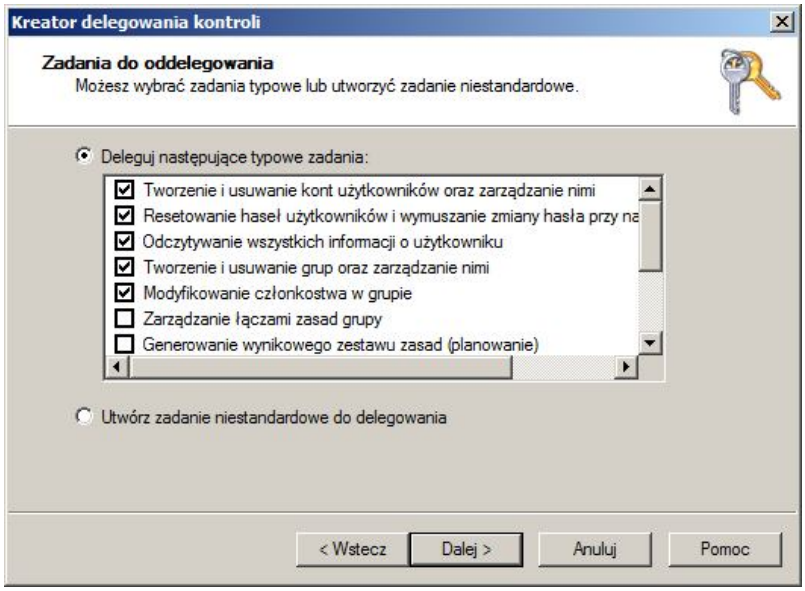
System/Logowanie	
Zasady	**Ustawienie**
Nie przetwarzaj listy jednokrotnego uruchamiania	Włączone
Nie przetwarzaj starszej listy uruchamiania	Włączone

Źródło: *opracowanie własne*

6.2.7. Delegowanie uprawnień dla grupy helpdesk

Jak wcześniej wspomniałem, w przedsiębiorstwie znajduje się grupa helpdesk. Jej zadaniem będzie tworzenie nowych użytkowników, resetowanie haseł oraz modyfikowanie członkowstwa w grupie. Na jednostce organizacyjnej „jaskulek" uruchomiłem kreatora delegowania. Nadałem następujące uprawnienia grupie:

Rysunek nr 35 Kreator delegowania kontroli

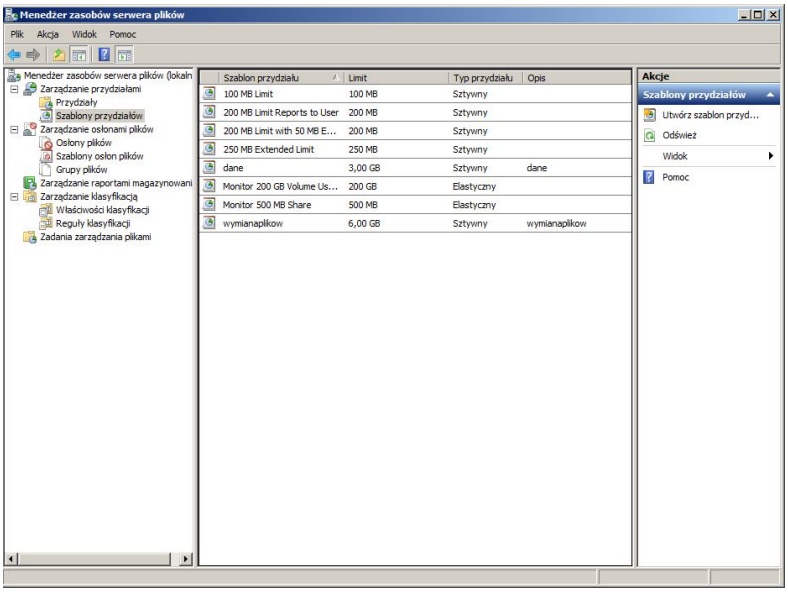


Źródło: *opracowanie własne*

6.2.8 Tworzenie przydziałów

Przydziały w systemie Windows Serwer 2008 R2 mogę ustawiać poprzez właściwości dysku lokalnego, bądź szczegółowych zasad grup. Metody te odnoszą się jednak do nadania przydziału dla całego dysku. Według mnie, metoda ta nie jest rozwiązaniem satysfakcjonującym, gdyż poprzez ustawienie przydziału na danym dysku, będzie on istniał na wszystkich folderach, które tenże dysk zawiera. Aby uniknąć takiej sytuacji mogę skorzystać z dodatkowej roli „menadżera zasobów serwera plików". Rolę tą instaluję na obu serwerach. Konsola **Menedżer zasobów serwera plików** umożliwia mi taka operację.

Rysunek nr 36 Menedżer zasobów serwera plików

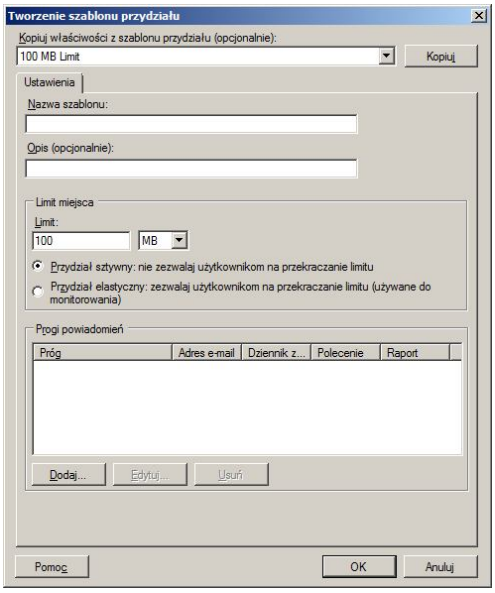


Źródło: *opracowanie własne*

W konsoli tej występuje kilka węzłów, **pierwszy z nich umożliwia ustawianie przydziałów**, **drugi pozwala na zablokowanie przechowywania określonych plików** w miejscu w folderze bądź dysku na jakim reguła ta została ustawiona. Niestety minusem tej reguły jest to, że jeśli użytkownik zmieni rozszerzenie pliku który jest zabroniony na dowolne inne, plik będzie mógł być zapisany.

Będę korzystał tylko z węzła **zarządzanie przydziałami**. Aby dodać przydział w pierwszej kolejności muszę stworzyć szablon. W tym celu rozwijam węzeł **zarządzanie przydziałami** i klikam prawym **klawiszem myszy** na **szablony przydziałów** po chwili otwiera się okno **tworzenie szablonu przydziału.**

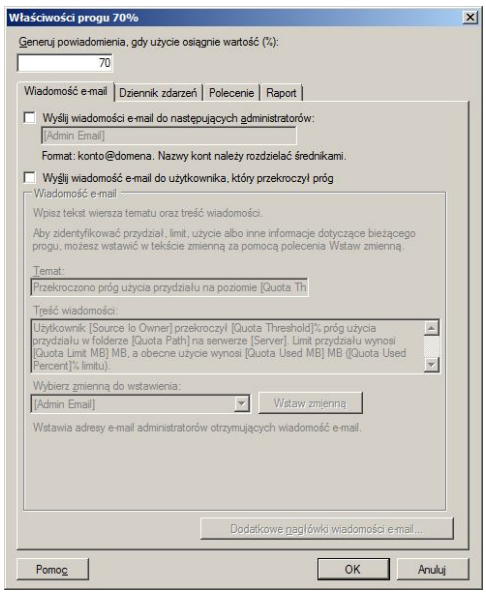
Rysunek nr 37 Tworzenie szablonu przydziału



Źródło: *opracowanie własne*

W tym oknie podaję między innymi: nazwę przydziału, limit miejsca, progi powiadomień. Mogę skopiować już istniejący przydział, zmodyfikować go oraz wybrać **dwie bardzo ważne opcje.** Mam na myśli **zezwolenie użytkownikowi** na powiększenie przydziału w razie wyczerpania miejsca bądź **zakazanie** tej opcji. Następnie sam mogę zadecydować o progu powiadomień i sposobie zgłaszania tego zdarzenia.

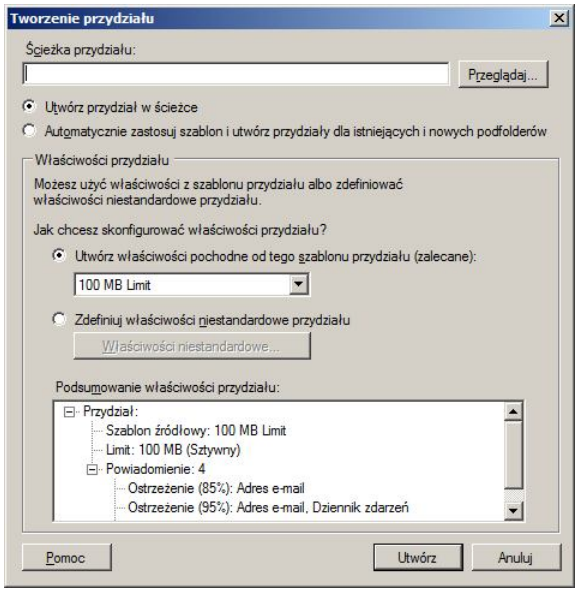
Rysunek nr 38 Właściwości progu powiadomień



Źródło: *opracowanie własne*

Dla wszystkich utworzonych przeze mnie szablonów ustawiłem próg na **poziomie 70%.** Po stworzeniu szablonu przydziału mogę przystąpić do ustawiania przydziałów na **dysku** bądź **folderze**. W celu dodania przydziału **klikam prawym klawiszem** myszy na **węzeł przydziały,** a następnie wybieram opcję **nowy przydział**. Otworzy się okno tworzenie przydziału.

Rysunek nr 39 Tworzenie przydziału



Źródło: *opracowanie własne*

W oknie mogę ustalić ścieżkę docelową, wybrać istniejący limit bądź stworzy nowy. Na obu serwerach stworzyłem trzy szablony przydziałów

Tabela nr 13 Utworzone szablony przydziałów

Nazwa	Wielkość	Poziom powiadomień	Rodzaj
Dane	3GB	70%	Sztywny
Wnioski	3GB	70%	Sztywny
Wymianaplikow	6GB	70%	Sztywny

Źródło: *opracowanie własne*

Tabelka (nr 14)ilustruje przydziały, które utworzyłem

Tabela nr 14 Utworzone przydziały

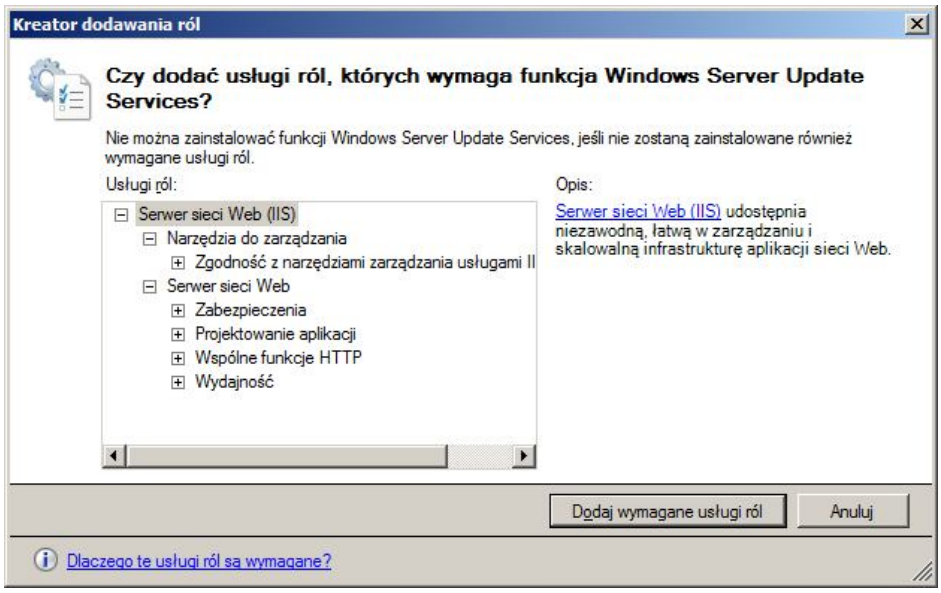
Nazwa obszaru	Miejsce docelowe	Nazwa szablonu przydziału	Wielkość przydziału
\\jaskulek.com\dane\dokumenty\	katalog użytkownika	Dane	3GB
\\jaskulek.com\dane\grupy\	Admini	Brak	
	Helpdesk	Brak	
	Księgowi	wymianaplikow	6GB
	Pracownicy	wymianaplikow	6GB
	Zarząd	wymianaplikow	6GB
	zwyklekontadmini	wymianaplikow	6GB
	zwyklekontahelpdesk	wymianaplikow	6GB
\\jaskulek.com\dane\it\	Sterowniki	Brak	
\\jaskulek.com\pliki\	Wnioski	wnioski	3GB
	Wymianaplikow	wymianaplikow	6GB

Źródło: *opracowanie własne*

6.3. Instalacja i konfiguracja Windows Server Update Services

System Windows Server 2008 R2 umożliwia instalację WSUS za pomocą okna „menedżer serwera” Gdy instaluję rolę WSUS, instalują się również role dodatkowe pokazane na rysunku.

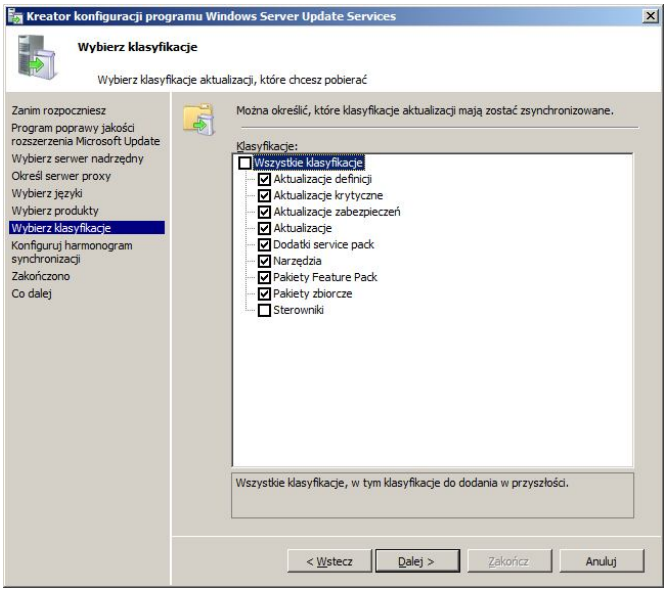
Rysunek nr 40 Kreator dodawania ról



Źródło: *opracowanie własne*

Żeby instalacja WSUS powiodła się, serwer na którym dokonuję instalacji musi być podłączony do Internetu. WSUS do swojego prawidłowego działania wymaga instalacji **pakietu redystrybucji narzędzia Microsoft Report Viewer 2008**. Podczas instalacji WSUS ustawiam lokalizację folderu, gdzie będą znajdować się aktualizacje, oraz ustalam lokalizację wewnętrznej bazy danych. **Lokalizacją folderu** dla **aktualizacji** i wewnętrznej **bazy danych**, będzie folder WSUS na **partycji „F”.** Gdy konfiguruję ustawienia WSUS, mam możliwość wyboru, to znaczy, czy WSUS będzie się **synchronizował z innym serwerem**, czy z **witryną Microsoft Update** w celu pobrania **aktualizacji.** Instalując **pierwszy** serwer WSUS, wybieram synchronizację z **witryną Microsoft Update**. Usługa ta umożliwia mi wybór aktualizacji w **wielu językach.** Wybieram aktualizacje w językach **angielskim i polskim**. Dodatkowo istnieje możliwość pobrania aktualizacji dla wielu programów **oferowanych przez Microsoft**. Mój wybór padł na **aktualizacje** dla **Windows 7** i **Windows Server 2008 R2**. Kolejnym krokiem będzie ustalenie jakie **rodzaje klasyfikacji aktualizacji** będą pobierane.

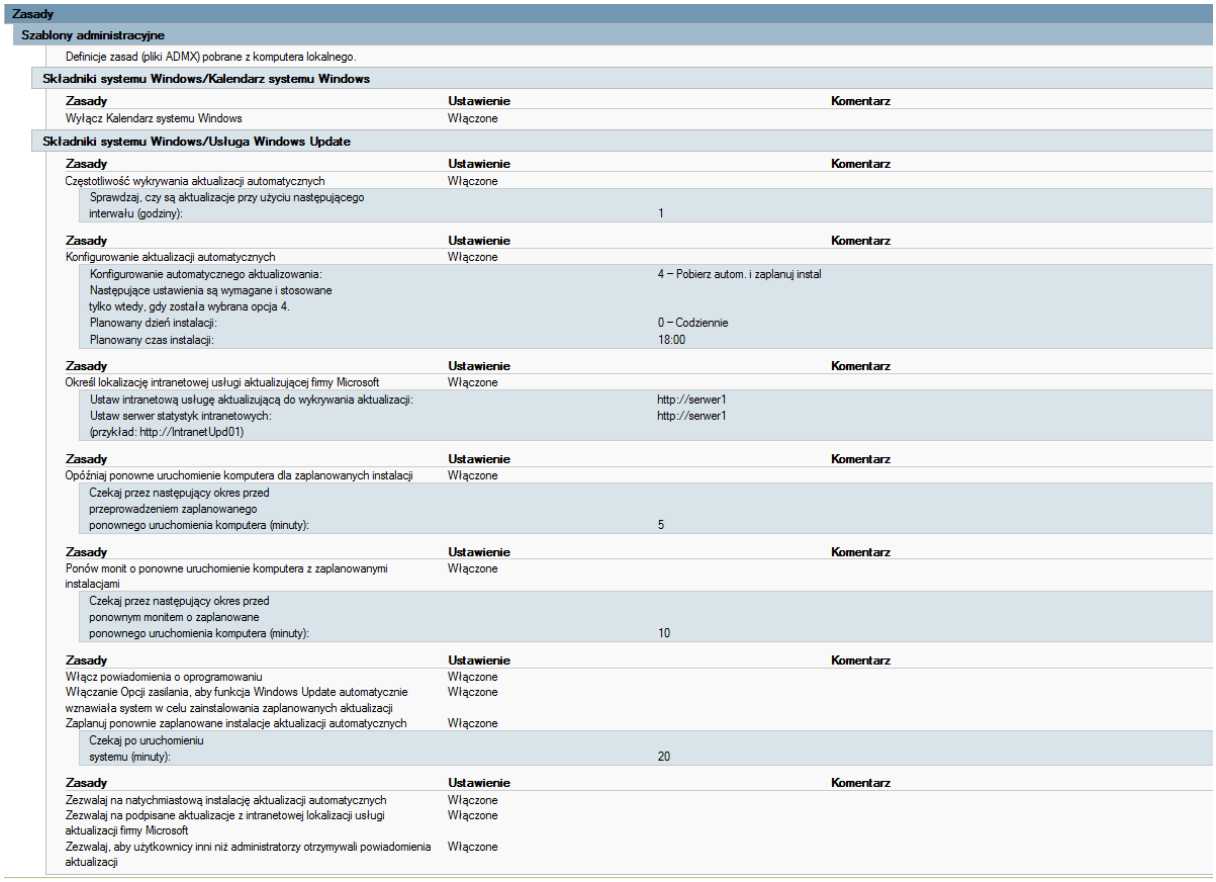
Rysunek nr 41 Kreator konfiguracji programu Windows Server Update Services



Źródło: *opracowanie własne*

Po konfiguracji serwera WSUS synchronizuję go, w celu pobrania wszystkich aktualizacji. Żeby prościej można było je instalować utworzę trzy nowe grupy, to znaczy „windows7", „WindowsServer2008R2" oraz „test". Komputery będą dodane do grup ręcznie, natomiast do komunikacji **komputerów** z serwerem **WSUS** użyję **zasad grup.** Konfiguracja taka wygląda następująco(Rysunek nr 42):

Rysunek nr 42 Ustawienia GPO dla komunikacji komputerów z serwerem WSUS



Zasady

Szablony administracyjne

Definicje zasad (pliki ADMX) pobrane z komputera lokalnego.

Składniki systemu Windows/Kalendarz systemu Windows

Zasady	Ustawienie	Komentarz
Wyłącz Kalendarz systemu Windows	Włączone	

Składniki systemu Windows/Usługa Windows Update

Zasady	Ustawienie	Komentarz
Częstotliwość wykrywania aktualizacji automatycznych	Włączone	
Sprawdzaj, czy są aktualizacje przy użyciu następującego interwału (godziny):	1	

Zasady	Ustawienie	Komentarz
Konfigurowanie aktualizacji automatycznych	Włączone	
Konfigurowanie automatycznego aktualizowania:	4 – Pobierz autom. i zaplanuj instal	
Następujące ustawienia są wymagane i stosowane tylko wtedy, gdy została wybrana opcja 4.		
Planowany dzień instalacji:	0 – Codziennie	
Planowany czas instalacji:	18:00	

Zasady	Ustawienie	Komentarz
Określ lokalizację intranetowej usługi aktualizującej firmy Microsoft	Włączone	
Ustaw intranetową usługę aktualizującą do wykrywania aktualizacji:	http://serwer1	
Ustaw serwer statystyk intranetowych:	http://serwer1	
(przykład: http://IntranetUpd01)		

Zasady	Ustawienie	Komentarz
Opóźniaj ponowne uruchomienie komputera dla zaplanowanych instalacji	Włączone	
Czekaj przez następujący okres przed przeprowadzeniem zaplanowanego ponownego uruchomienia komputera (minuty):	5	

Zasady	Ustawienie	Komentarz
Ponów monit o ponowne uruchomienie komputera z zaplanowanymi instalacjami	Włączone	
Czekaj przez następujący okres przed ponownym monitem o zaplanowane ponownego uruchomienia komputera (minuty):	10	

Zasady	Ustawienie	Komentarz
Włącz powiadomienia o oprogramowaniu	Włączone	
Włączanie Opcji zasilania, aby funkcja Windows Update automatycznie wznawiała system w celu zainstalowania zaplanowanych aktualizacji	Włączone	
Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznych	Włączone	
Czekaj po uruchomieniu systemu (minuty):	20	

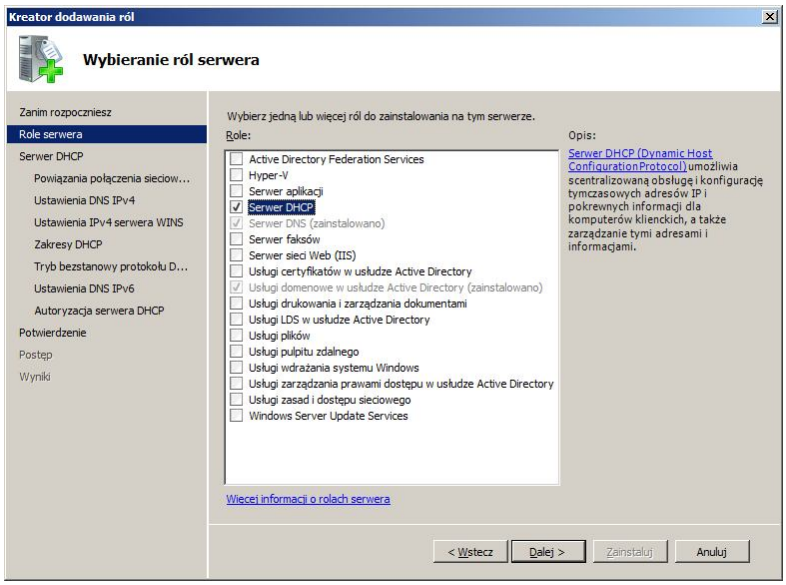
Zasady	Ustawienie	Komentarz
Zezwalaj na natychmiastową instalację aktualizacji automatycznych	Włączone	
Zezwalaj na podpisane aktualizacje z intranetowej lokalizacji usługi aktualizacji firmy Microsoft	Włączone	
Zezwalaj, aby użytkownicy inni niż administratorzy otrzymywali powiadomienia aktualizacji	Włączone	

Źródło: opracowanie własne

6.4 Instalacja Dynamic Host Configuration Protocol

Usługę DHCP dodam do serwera2. Żeby dodać usługę do serwera uruchamiam **konsolę menadżer serwera**. Klikam prawym klawiszem myszy na **węzeł role** i wybieram opcje **dodaj rolę**. Po uruchomieniu kreatora wybieram opcje serwera **DHCP**.

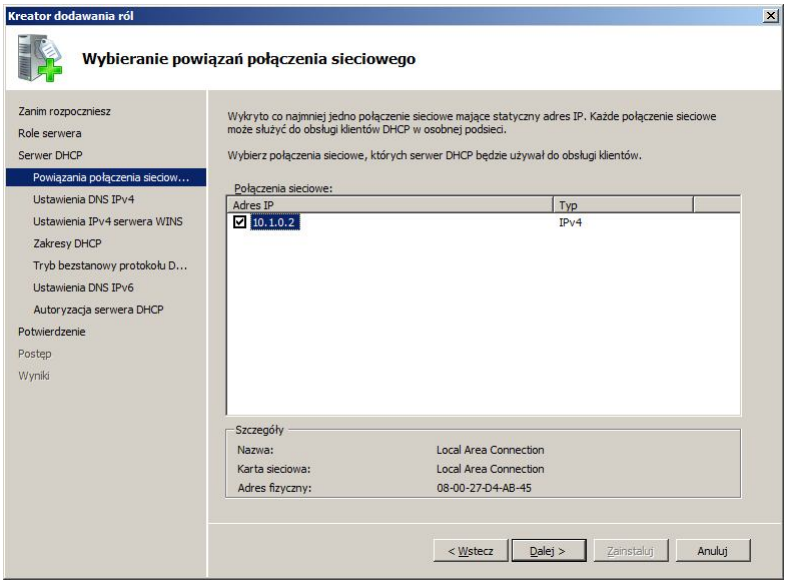
Rysunek nr 43 Kreator dodawania ról(dodanie DHCP)



Źródło*: opracowanie własne*

Następnie klikam przycisk dalej**, konfiguracja** DHCP przebiega w trochę innych sposób niż w przypadku **innych usług**. **Podstawową konfigurację** mogę wykonać w tym **samym oknie konsolowym**. Jak widać na obrazku (**podmenu Serwer DHCP**) kreator przeprowadzi mnie poprzez **poszczególne ustawienia**. Pierwszą opcją jest **wybranie powiązań połączenia sieciowego**. Opcja ta umożliwia mi wybór, na jakich interfejsach będzie działał serwer DHCP. Wybrałem jedyny dostępny interfejs.

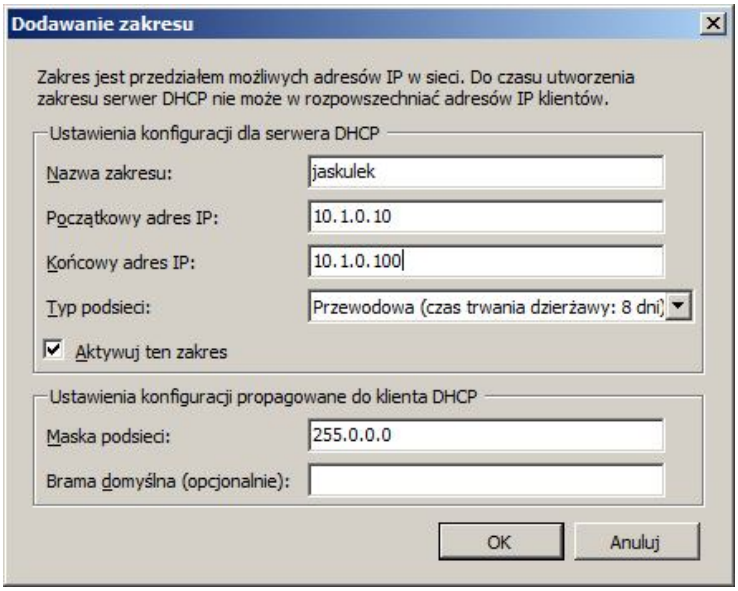
Rysunek nr 44 Wybieranie powiązań połączenia sieciowego



Źródło: *opracowanie własne*

W **drugiej opcji** (ustawienia DNS IPv4) ustawiam adresy **serwerów DNS** które będą **rozgłaszane** przez usługę **DHCP.** Podałem **dwa adresy**, tzn. adres **DNS serwera1 (10.1.0.1)** i **serwera2 (10.1.0.2)**. Ponadto w tej opcji określam **nazwę domeny DNS**. Nazwa ta została **wygenerowana automatycznie**, jest nią **jaskulek.com**. Trzecią opcją jest ustawienie **IPv4 serwera WINS. Nie korzystam z tej opcji**, dlatego nie będę jej konfigurował. Czwarta opcja to **zakresy serwera DHCP**. Aby dodać taki zakres muszę kliknąć klawisz „dodaj". Po chwili pojawi się nowe okno, w którym podałem zakresy adresów IP.

Rysunek nr 45 Dodanie zakresu adresów IP



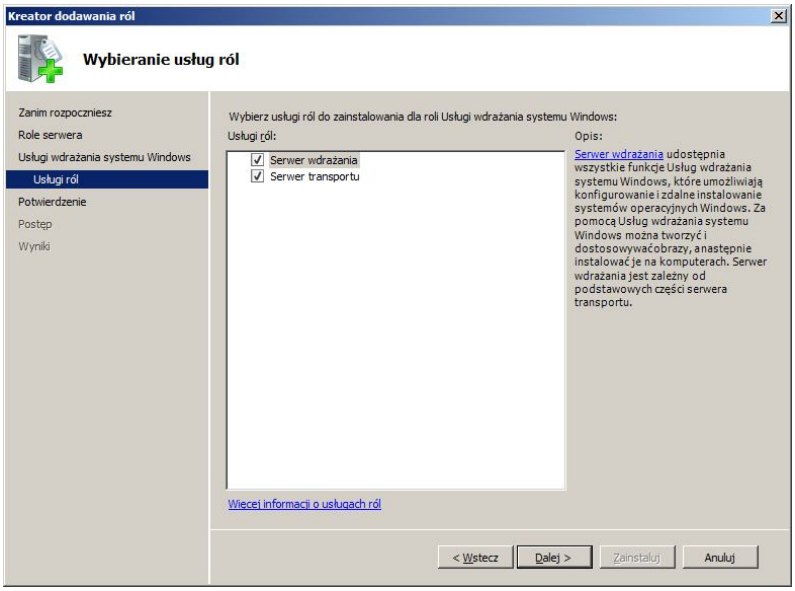
Źródło: *opracowanie własne*

Piątą opcją jest **tryb bezstanowego protokołu DHCPv6**. Opcja ta umożliwia przydzielanie adresów **IPv6** poprzez serwer **DHCP**. W **projekcie nie przewidziałem adresacji IPv6** dlatego opcja ta **została wyłączona**. Ostatnim krokiem będzie ustalenie **autoryzacji serwera DHCP**.

6.5 Instalacja Windows Deployment Services

Usługę WDS dodam do **serwera2**, gdzie zainstalowałem i skonfigurowałem **usługę DHCP.** Na początku wchodzę w znaną już konsolę **menadżer serwera**. Następnie wybieram opcję **usługi wdrażania systemu Windows** i klikam przycisk dalej. **Usługa WDS** instalowana jest z dwoma **dodatkowymi rolami: serwer wdrażania** oraz **serwer transportu**. Opcje te domyślnie są zaznaczone.

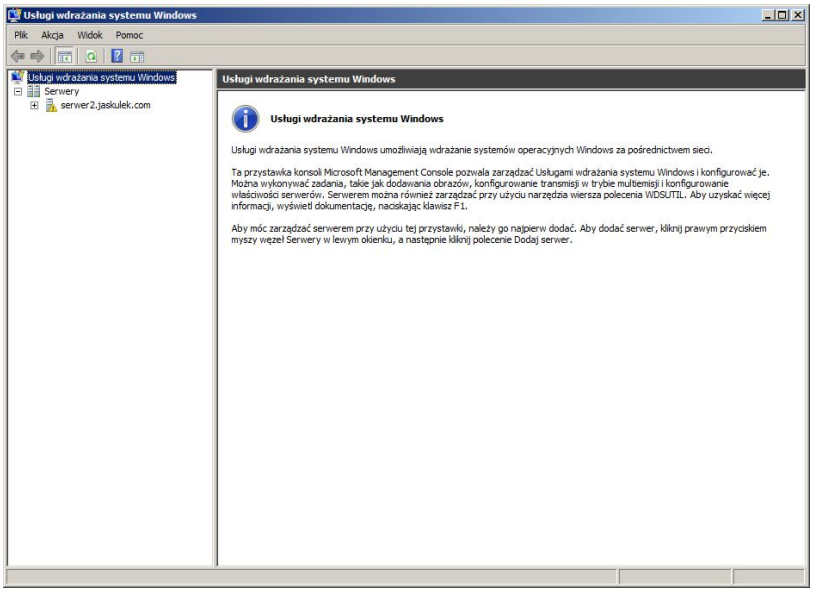
Rysunek 46 Dodatkowe usługi ról



Źródło: *opracowanie własne*

Po zainstalowaniu roli WDS przystępuję do konfigurowania usługi. Skorzystam więc z konsoli **Usługi wdrażania systemu Windows**, która znajduje się w menu: **start - narzędzia administracyjne - Usługi wdrażania systemu Windows**.

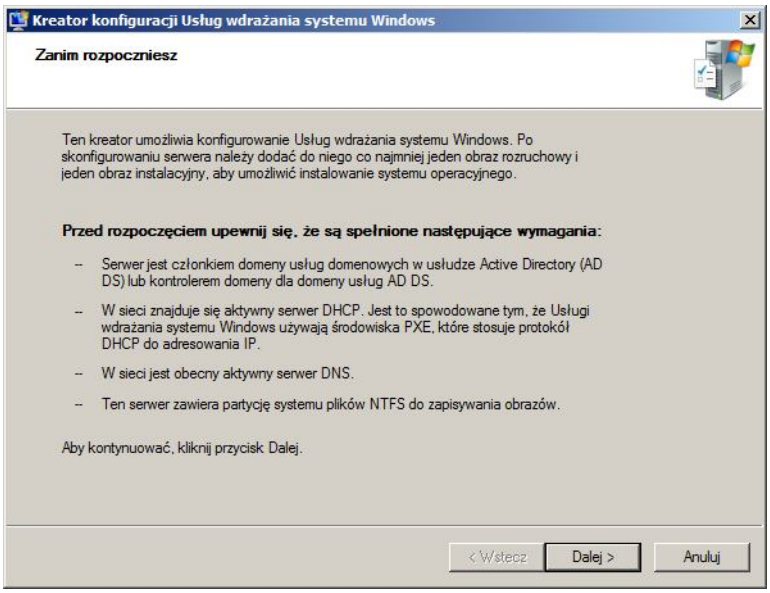
Rysunek 47 Konsola Usług wdrażania systemu Windows



Źródło: *opracowanie własne*

Mimo ze **usługa WDS** jest zainstalowana, to tak naprawdę jeszcze **nie działa**. Aby mogła ona **działać,** należy **ją skonfigurować.** W tym celu klikam **prawym klawiszem** na węzeł **serwer2.jaskulek.com**. Po chwili uruchomi **się okno kreatora,** które przedstawia rysunek nr 48.

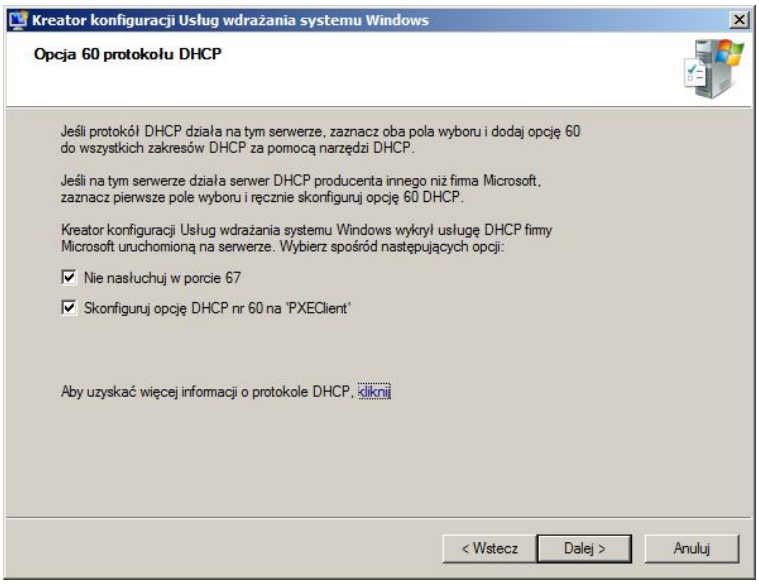
Rysunek 48 Kreator konfiguracji Usług wdrażania systemu Windows



Źródło: *opracowanie własne*

Aby usługa WDS mogła zostać uruchomiona,. wszystkie powyższe założenia muszą zostać spełnione. Następnym etapem konfiguracji będzie lokalizacja folderu zawierającego obrazy systemów. W tym celu na serwerze2 z**ainstalowałem osobny dysk,** który zgłasza się w systemie pod **literą F**. Domyślną lokalizacją, proponowaną przez kreator jest następująca lokalizacja: **C:\RemoteInstall**, natomiast moją lokalizacją jest **F:\RemoteInstall**. W następnym kroku wybieram opcję ustawienia **WDS w ramach konfiguracji usługi DHCP**, kiedy klienci będą wysyłać zapytania o adres IP serwera WDS.

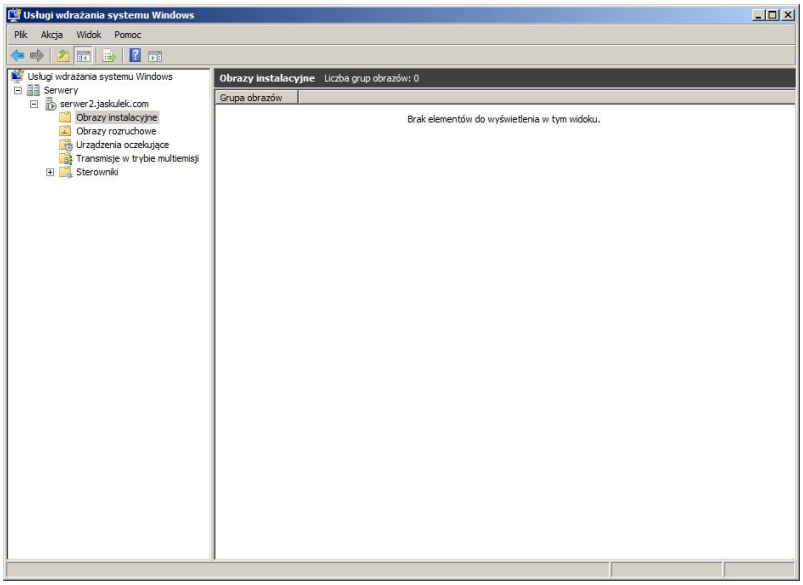
Rysunek 49 Kreator konfiguracji Usług wdrażania systemu Windows (opcje DHCP)



Źródło: *opracowanie własne*

Ostatnią konfigurowalną opcją będzie ustawienie serwera WDS dla zapytania klientów. Do wyboru mam **trzy opcje**. Wybrałem taką, w której serwer WDS odpowiada znanym i nieznanym komputerom, z zastrzeżeniem ze kiedy nieznany komputer zgłosi się do serwera WDS, administrator musi zatwierdzić to zgłoszenie. Po konfiguracji okno konsoli usług wdrażania systemu Windows wygląda następująco.

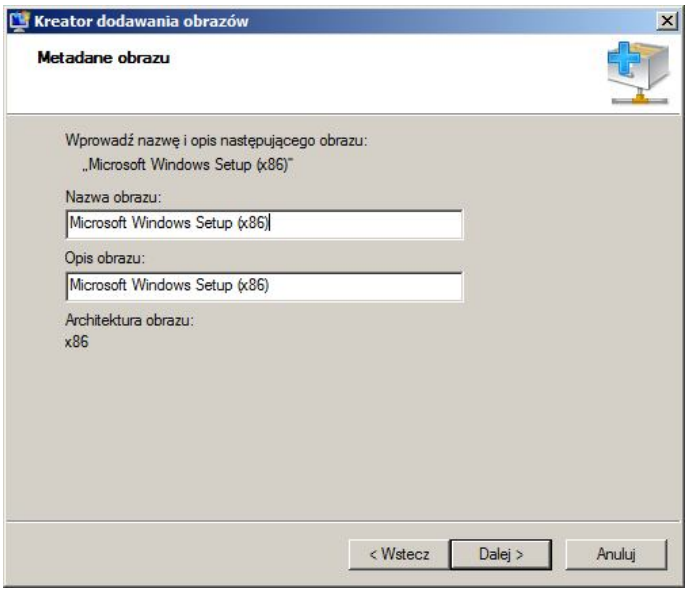
Rysunek 50 Konsola Usług wdrażania systemu Windows(skonfigurowana)



Źródło: *opracowanie własne*

WDS umożliwia mi dodanie do swojej bazy czystego **obrazu systemu**, bądź **obrazów wcześniej już przygotowanych**. Mam tutaj na myśli **dwa rodzaje** instalacji: **nadzorowaną** i **nienadzorowaną**. W instalacji **nienadzorowanej** system instaluje się **automatycznie.** Ustawienia początkowe konfigurowane będą **automatycznie**. Aby taka zależność miała miejsce muszą zostać **przygotowane odpowiednie pliki** w **formacie XML**. **Pliki** te można **przygotować** za pomocą narzędzi **Windows Automated Installation Kit**. Instalacja **nadzorowana** natomiast polega na tym, ze **kopiowane** są tylko pliki **instalacyjne** a **administrator** sam **konfiguruje** pozostałe **ustawienia**. W moim projekcie dodam **jeden** obraz w typie nadzorowanym. Będzie to **czysty obraz systemu** Windows 7 Professional. Abym mógł dodać obraz systemu do serwera WSUS muszę najpierw dodać plik **boot.wim** znajdujący się w folderze **sources,** zawierającym się na nośniku oryginalnego obraz systemu. W tym celu klikam prawym klawiszem myszy na węzeł **obrazy rozruchowe** i wybieram opcję **dodaj nowy obraz rozruchowy**. Po chwili uruchamia się kreator. W pierwszej opcji kreatora ustalam lokalizację pliku **boot.wim**. Następnie podaję nazwę obrazu, którą będzie domyślna nazwa, Microsoft Windows Setup (x86).

Rysunek 51 Kreator dodawanie obrazów



Źródło: *opracowanie własne*

Obrazy instalacyjne w usłudze WDS można podzielić na grupy. Utworzyłem jedną grupę o nazwie **7**, która będzie zawierała obraz instalacyjny. Aby dodać obraz instalacyjny klikam prawym klawiszem na węzeł **obrazy instalacyjne** i wybieram opcję **dodaj obraz instalacyjny.** Po chwili otworzy się kreator dodawania obrazu. Następnie w pierwszej opcji wybieram grupę którą utworzyłem wcześniej - do niej zostanie dodany obraz. W drugim kroku, z folderu **sources** wybieram plik **install.wim**. W miejscu wyboru wersji systemu wybieram opcję Professional. Po kliknięciu przycisku **dalej** kreator doda obraz do usługi WDS.

Rozdział 7
Podsumowanie i wnioski

Celem mojej pracy był projekt i implementacja środowiska Active Directory w firmie „Jaskulek". Od zarządu firmy dostałem konkretne wytyczne i model aktualnego zarządzania przedsiębiorstwem. W projekcie uwzględniłem wszystkie aspekty pierwotnych założeń. Zanim jednak projekt został zrealizowany postanowiłem przeprowadzić instalację w środowisku testowym. Wykorzystałem do tego system maszyn wirtualnych virtualbox. Dzięki temu problemy, które mogłyby wyniknąć podczas instalacji na urządzeniach i w istniejącym środowisku IT firmy „Jaskulek" zostały zniwelowane do poziomu 1%. Wdrożenie przebiegało bez widocznych problemów, te które się jednak pojawiły zostały rozwiązane.

Jedną z trudności, jakie napotkałem przy instalacji systemu, był problem przy replikacji folderów w usłudze DFS. Polegał on na tym, że replikowane są tylko uprawnienia NTFS, natomiast uprawnienia share nie są replikowane. Takie zagadnienie rozwiązałem nadając ręcznie uprawnienia w miejscu, gdzie foldery są replikowane. Tu natomiast rodzi się kolejny problem traktujący udostępnianie dużej ilość folderów. Ręcznie nadawanie uprawnień zajmowało by bardzo dużo czasu, rozwiązałem więc ten problem za pomocą skryptów PowerShell.

Drugie problematyczne zagadnienie, to źle działająca usługa WDS. Okazało się, że pliki bootujące bardzo długo kopiowały się na stację roboczą. Początkowo myślałem ze problem stanowi nieprawidłowo działająca karta sieciowa. Po wymianie tejże karty pojawił się kolejny problem. Po ponownym skopiowaniu plików bootujących instalacja nie mogła zostać ukończona, z powodu braku sterowników do karty sieciowej. Wynika z tego, że problem, nie polegał na konfiguracji usługi WDS, lecz tkwił w programie służącym do wirtualizacji. Po zmianie aplikacji i skonfigurowaniu systemu i usługi w takim sam sposób wszystkie błędy zostały wyeliminowane.

Zrealizowałem wszystkie postawione przede mną cele. Dzięki tej pracy i dzięki projektowi który stworzyłem, mogę przeprowadzać podobne instalacje środowiska AD w przedsiębiorstwach, mających zbliżone założenia informatyczne do firmy „Jaskulek". Do wykorzystania będą np. wszystkie przygotowane przeze mnie skrypty, których

przekształcenie dla konkretnych potrzeb przedsiębiorstwa nie będzie już tak bardzo czasochłonną czynnością.

BIBLIOGRAFIA:

Pozycje książkowe:

1. **Reimer S., Kezema C., Mulcare M., Wright B.** oraz **Microsoft Active Directory Team**, *Active Directory Windows Server 2008 Resource Kit,* Microsoft Press, Warszawa 2008.

2. **Holme D., Ruest D., Ruest N**., *Konfigurowanie Active Directory w Windows Server 2008 Training Kit,* t. I i II, Microsoft Press, Warszawa 2009.

3. **Thomas O. Policelli J., McLean I., Mackin J.C., Manuso P., Miller David R.,** przy współpracy **GrandMasters**, *Administrowanie systemem Windows Server 2008 w skali przedsiębiorstwa, Training Kit,* Microsoft Press, Warszawa 2009.

4. **Stanek William R.**, *Vademecum Administratora Windows Server 2008 R2*,wyd.2, Microsoft Press, Warszawa 2010.

Adresy internetowe:

5. Omówienie Windows Deployment Services cz. 1 http://wss.pl/Articles/10409/Comments.aspx stan na dzień 19.01.2011

6. Instalacja Server Core systemu Windows Server 2008 http://wss.pl/Articles/9645.aspx stan na dzien 19.01.2011

7. DHCP od podszewki w Windows Server 2008 http://wss.pl/Articles/10054.aspx stan na dzien 19.01.2011

Przypisy w tekście znajdujące się w nawiasach kwadratowych mówią o źródle na podstawie którego został opracowany dany fragment. ([…])

SPIS RYSUNKÓW:

SPIS TABEL:

ZAŁĄCZNIKI

Do niniejszej pracy załączyłem płytę CD, która zawiera elektroniczną jej wersję (Praca_inżynierska–Jakub_Sułkowski.doc)