T: Usługi domenowe w usłudze Active Directory.

Zrozumienie infrastruktury Active Directory (AD.0)

Active Directory (AD) to

- usługa katalogowa dla systemów Windows od wersji 2008 otrzymała nazwę **Active Directory Domain Services (AD DS)**, zapewnia uwierzytelnianie zasobów w obrębie organizacji, w której usługi sieciowe kontroluje domena, zarządzanie nimi, opisuje strukturę sieci i jej składników.
- technologia Microsoft to rozproszona baza danych, która przechowuje obiekty w hierarchicznym, ustrukturyzowanym i bezpiecznym formacie.

Obiekt AD to wyróżniony, nazwany zbiór atrybutów reprezentujący zazwyczaj reprezentują użytkowników, komputery, urządzenia peryferyjne i usługi sieciowe.

Każdy obiekt jest jednoznacznie identyfikowany poprzez nazwę i atrybuty.

Zbiór klas – zestaw możliwych rodzajów obiektów występujących w AD.

Zbiór wszystkich możliwych rodzajów obiektów występujących w Active Directory i związanych z nimi atrybutów to **schemat** *(schema).*

Domena, las i drzewo reprezentują logiczne podziały infrastruktury AD.

AD używa następujących protokołów i usług:

Lightweight Directory Access Protocol (LDAP): służy do uzyskiwania dostępu do danych usług katalogowych

Kerberos: Kerberos bezpiecznie uwierzytelnia i potwierdza tożsamość między użytkownikami i serwerami w sieci

System nazw domen (DNS): DNS służy do tłumaczenia nazw domen na adresy IP

AD zarządza się za pomocą następujących przystawek w Microsoft Management (MMC) (mmc.exe):

Active Directory Administrative Center (Centrum administracyjne usługi Active Directory) (dsac.exe): pokazano na rysunku 1.1. Jest to jedno miejsce zatrzymania używane do zarządzania usługami katalogowymi systemu Windows Server

Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) (dsa.msc): Ta konsola służy do zarządzania użytkownikami, komputerami i odpowiednimi informacjami

Active Directory Domains and Trusts (Domeny i relacje zaufania w usłudze Active Directory) (domain.msc): Ta konsola służy do zarządzania domenami, relacjami zaufania i odpowiednimi informacjami

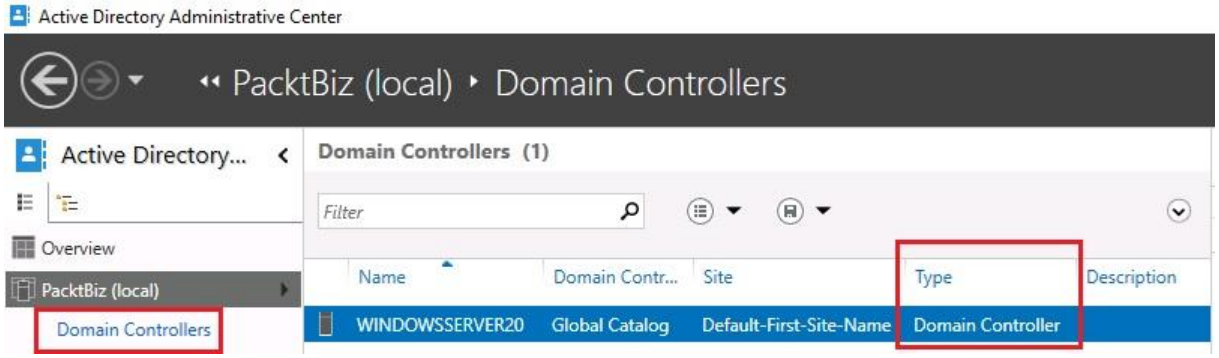
Active Directory Sites and Services (Lokacje i usługi Active Directory) (dssite.msc): Ta konsola służy do zarządzania replikacją i usługami między lokacjami

Active Directory Module for Windows PowerShell (Moduł Active Directory dla Windows PowerShell): Ta konsola służy do zarządzania usługami katalogowymi Windows Server za pomocą poleceń cmdlet

Uwaga Dostęp do Microsoft Script Center można uzyskać pod adresem https://technet.microsoft.com/en-us/scriptcenter/bb410849.aspx oraz PowerShell Gallery pod adresem https://www.powershellgallery.com/. Oba są dobrze znanymi repozytoriami darmowych i publicznych skryptów PowerShell. Dodatkowo uwzględniono znaczną kolekcję wpisów związanych z AD i DNS.

Kontroler domeny (AD.1)

Kontroler domeny (DC) (patrz rysunek 1.1) to serwer odpowiedzialny za bezpieczne uwierzytelnianie żądań dostępu do zasobów w domenie organizacji. W systemie Windows NT jeden kontroler domeny na domenę był skonfigurowany jako główny kontroler domeny (PDC), a wszystkie inne kontrolery domeny działały jako zapasowe kontrolery domeny (BDC). W systemie Windows Server 2016 nie ma podstawowych i zapasowych kontrolerów, w celu identyfikacji priorytetów używane są liczb obok nazwy kontrolerów domeny (na przykład DC1 i DC2):



Rycina 1.1. Dostęp do kontrolerów domeny za pośrednictwem Centrum administracyjnego usługi Active Directory

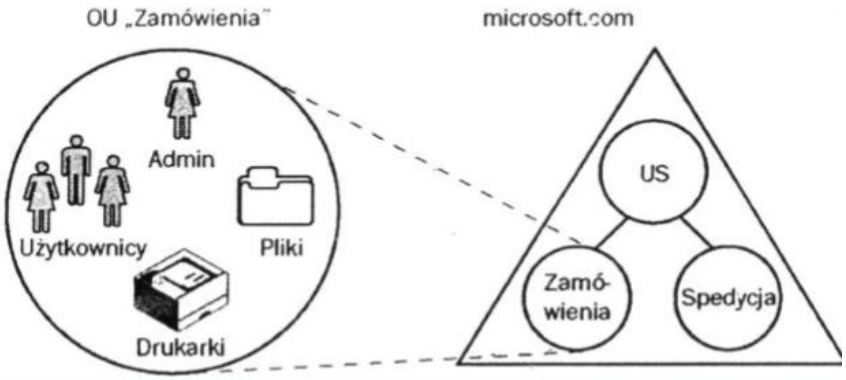
Uwaga Serwer, który nie działa jako kontroler domeny w sieci organizacji, jest znany jako serwer członkowski.

Kontroler domeny przechowuje informacje o użytkownikach sieci i ich uprawnieniach. Informacje te gromadzone są w jednym miejscu i dostępne dla wszystkich klientów, co ułatwia zarządzanie siecią.

W dużych sieciach może być więcej kontrolerów domeny, ale w takim przypadku wymieniają się między sobą przechowywanymi informacjami o sieci.

Kontrolery domeny są równoprawne - każdy ma zapisywalną replikę tej samej bazy danych.

Replika – kopia bazy danych przechowywana przez kontroler domeny.



Partycja – jednostka replikacji bazy danych AD. Podstawowe jednostki replikacji bazy danych AD to:

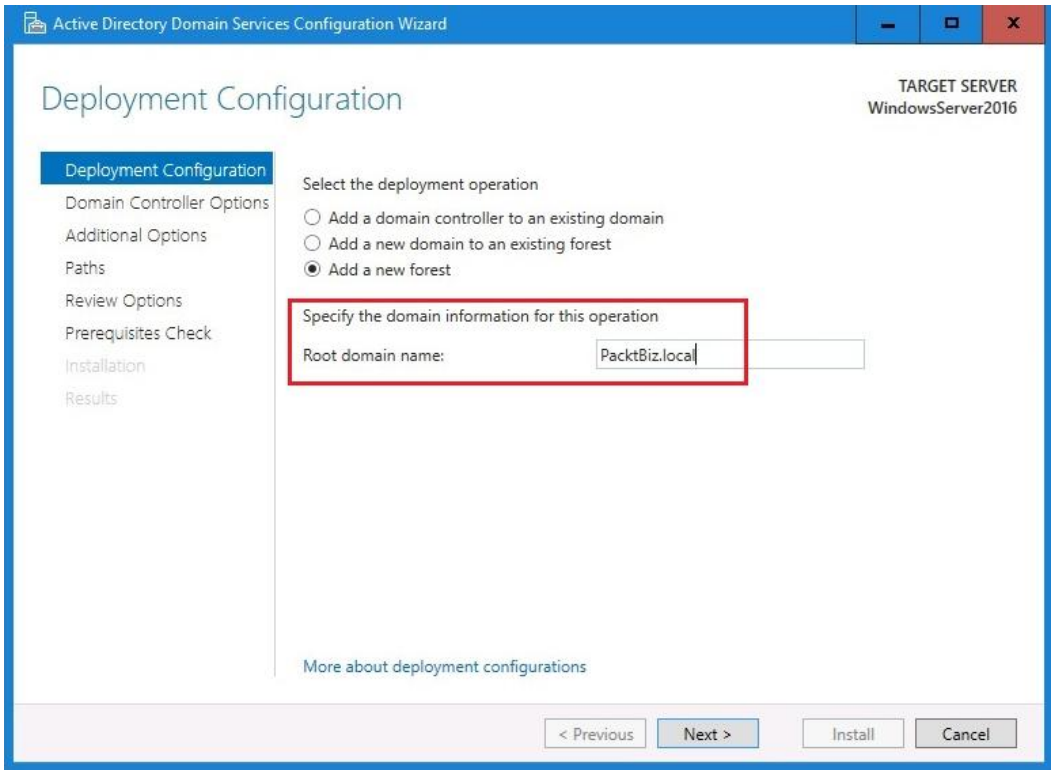
- partycja domeny - informacje o obiektach w domenie,
- partycja schematu - zawiera definicje schematów,
- partycja konfiguracji - informacje o wszystkich domenach w lesie, kontrolerach i topologii replikacji.

Domena

Domena to logiczna grupa użytkowników, komputerów, stacji roboczych - klientów współdzielących bazę katalogową, urządzeń peryferyjnych, usług sieciowych i ustawień bezpieczeństwa, jest zorganizowana hierarchicznie. Z punktu widzenia dostępu do usług sieciowych domeny są zwykle scentralizowanymi środowiskami sieciowymi, w których uwierzytelnianiem zarządza kontroler domeny.

W sieciach opartych na systemie Windows Server domena jest zasilana przez rolę usług AD DS.

Rysunek 1.2 przedstawia krok w Kreatorze konfiguracji usług domenowych w usłudze Active Directory, aby określić domenę:



Rycina 1.2. Konfigurowanie domeny głównej w systemie Windows Server 2016

Musisz zrozumieć, że istnieje głęboka różnica w znaczeniu domeny w kontekście domeny katalogu lub serwera domeny oraz w kontekście nazwy domeny.

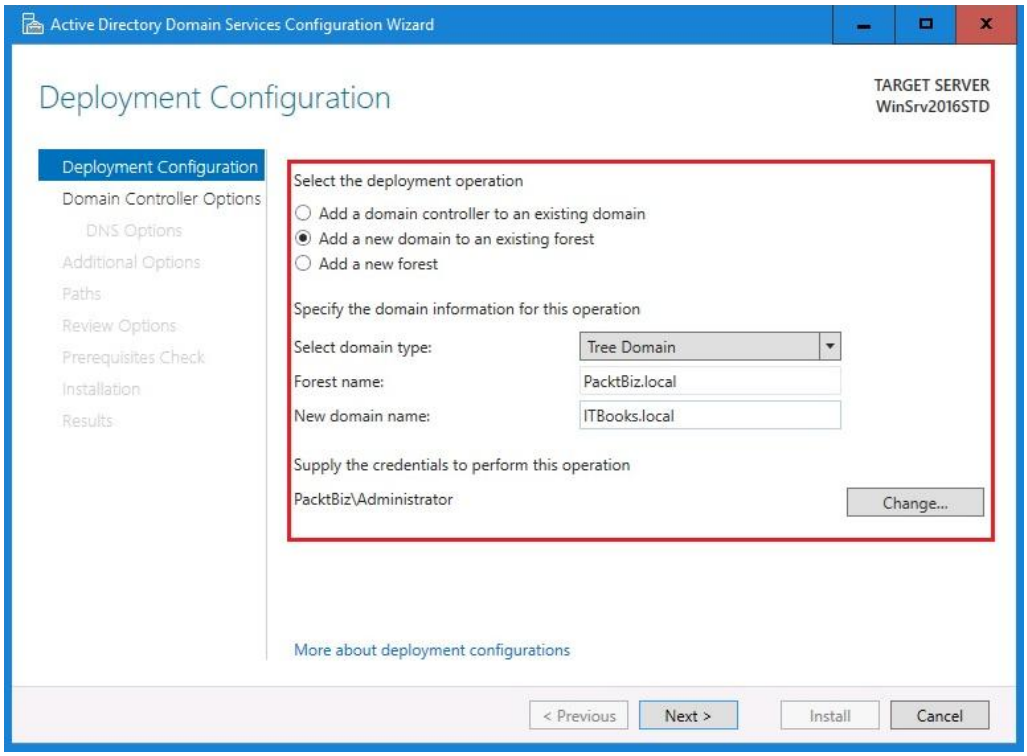
Ten pierwszy oznacza bazę danych użytkowników, serwerów, urządzeń i zasobów w ramach określonego zbioru takich rzeczy.

Ten ostatni oznacza logiczny system nazewnictwa zarządzający Internetem, w tym serwerami i stronami internetowymi.

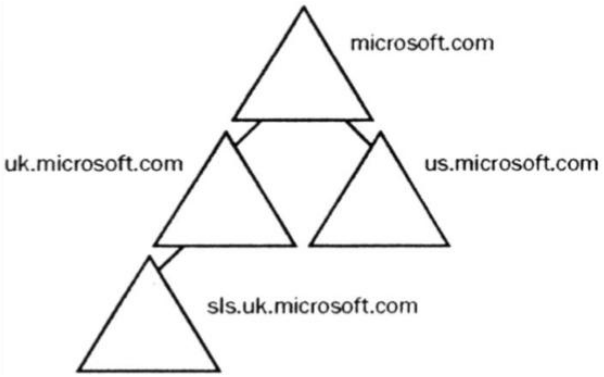
Drzewo

Drzewo w strukturze AD składa się z jednej lub więcej domen mających ten sam schemat, konfigurację i tworzących ciągłą hierarchiczną przestrzeń nazw.

Przyłączenie domeny do drzewa jest określone w momencie instalacji jej pierwszego kontrolera, jak pokazano na rysunku 1.3:



Rycina 1.3. Konfigurowanie domeny drzewa w systemie Windows Server 2016

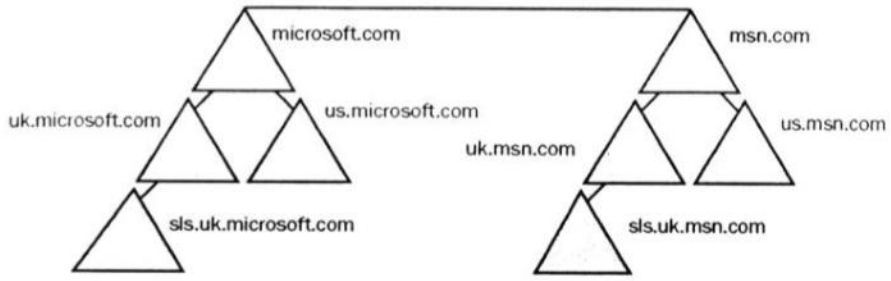


Domeny należące do tego samego drzewa mają jednolitą przestrzeń nazw i hierarchiczną strukturę nazw. Zgodnie ze standardami DNS, nazwa domeny podrzędnej składa się ze względnej nazwy domeny (prefiksu) oraz nazwy jej domeny nadrzędnej.

Las (AD.2)

Las to struktura złożona z wielu drzew, także o wspólnym schemacie i konfiguracji, ale niemająca ciągłej przestrzeni nazw. Las może składać się z jednego drzewa lub wielu drzew.
Przynależność do lasu jest określana w momencie instalacji pierwszego kontrolera domeny - przed

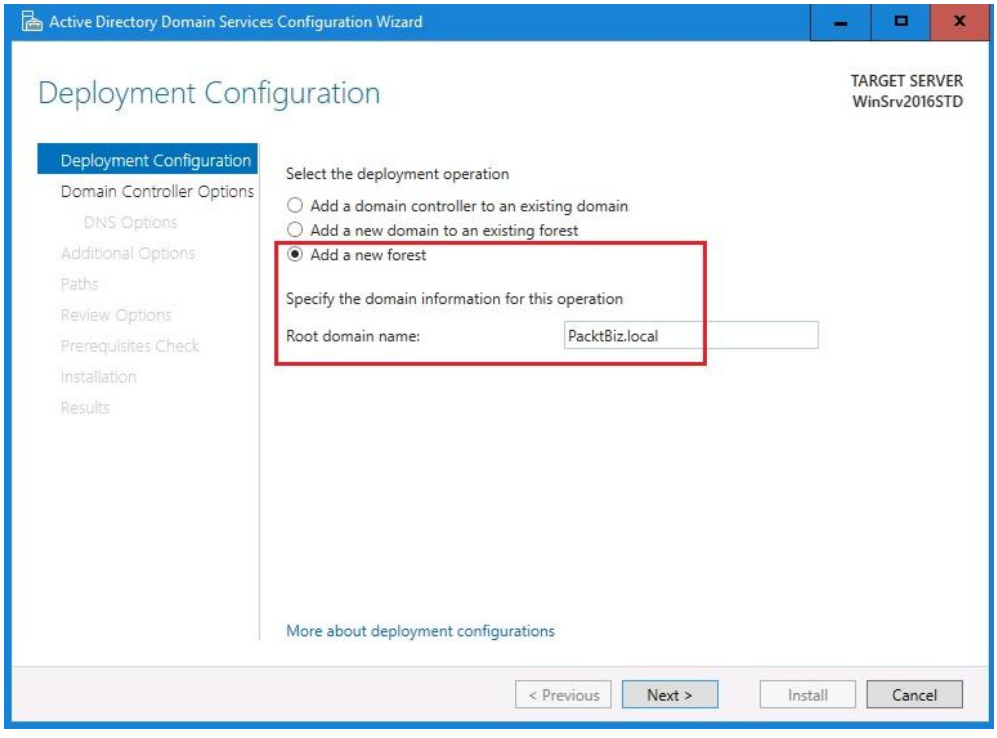
określeniem przynależności do drzewa.



Podstawowe cechy lasów:

- wszystkie domeny w lesie są oparte na wspólnym schemacie;
- wszystkie domeny w lesie wykorzystują wspólny wykaz globalny;
- pomiędzy domenami należącymi do tego samego lasu istnieją domniemane dwukierunkowe przechodnie relacje zaufania;
- poszczególne drzewa mają niezależne struktury nazw, oparte na nazwach domen;
- domeny w lesie funkcjonują niezależnie od siebie, ale las służy do umożliwienia komunikacji na poziomie całej organizacji.

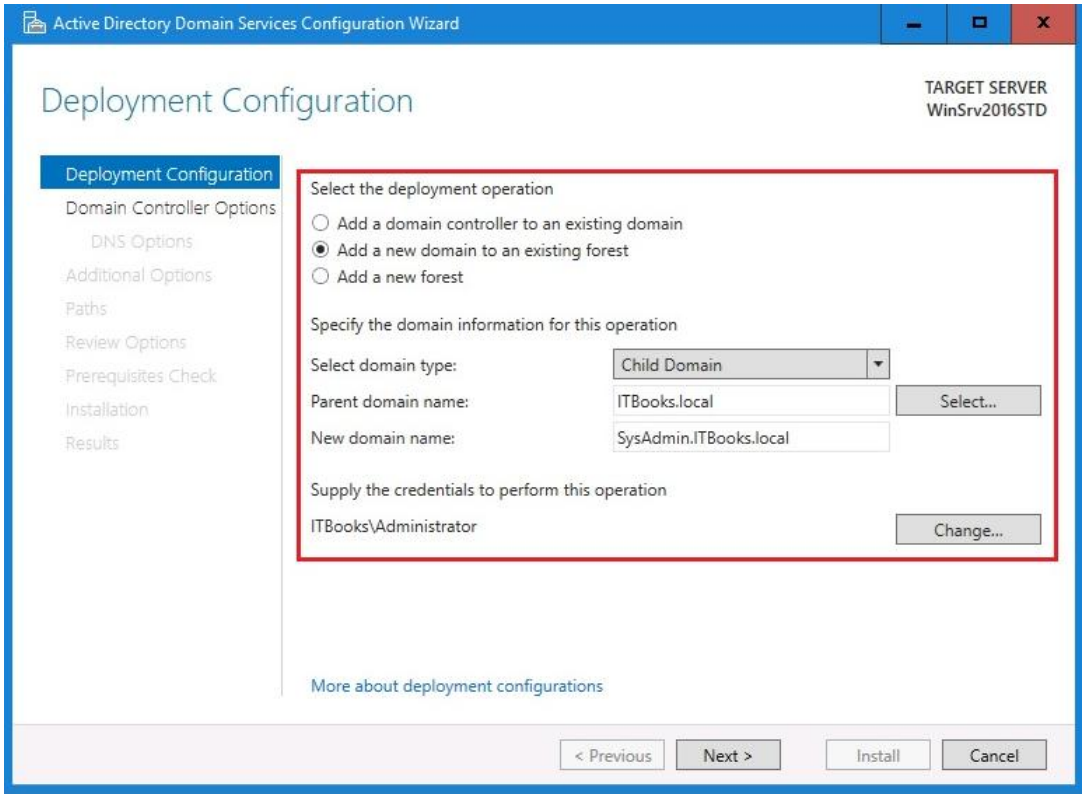
W AD las składa się z kolekcji drzew. Aby skonfigurować las w systemie Windows Server 2016, podobnie jak w przypadku domen i domen drzew, użyj Kreatora konfiguracji usług domenowych w usłudze Active Directory pokazanego na rysunku 1.4:



Rycina 1.4. Konfigurowanie lasu w systemie Windows Server 2016

Domena podrzędna (AD.5)

Aby zrozumieć domenę podrzędną, zilustrujmy ją prawdziwym drzewem. Drzewo składa się z korzeni, pnia, gałęzi i liści. Następnie, na naszej ilustracji, jeśli obrócimy drzewo z korzeniami powyżej i liśćmi poniżej, dochodzimy do wniosku, że domeną nadrzędną jest korzeń, a domeną podrzędną są jego gałęzie. To jako całość stanowi domenę drzewa. Ponadto wiele domen drzewiastych stanowi las.
Z powyższych przykładów PacktBiz.local reprezentuje las, ITBooks.local reprezentuje domenę drzewa w lesie, a SysAdmin.ITBooks.local reprezentuje domenę podrzędną w domenie drzewa.
Aby skonfigurować domenę podrzędną w systemie Windows Server 2016, wykonaj prawie identyczne kroki w celu wcześniejszego skonfigurowania domeny drzewa za pomocą Kreatora konfiguracji usług domenowych w usłudze Active Directory, jak pokazano na rysunku 1.5:



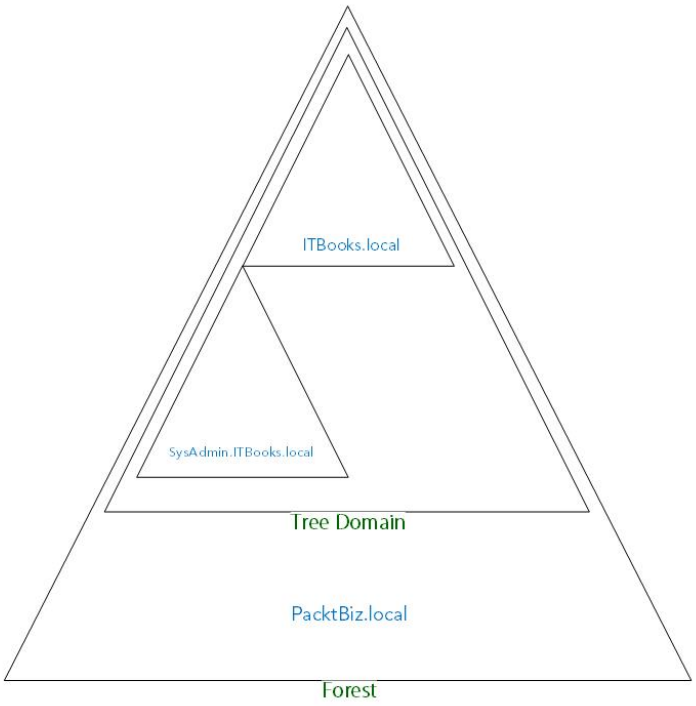
Rycina 1.5. Konfigurowanie domeny podrzędnej w systemie Windows Server 2016

Role wzorca operacji (AD.3)

Usługi AD DS są złożone! Jednak jak tylko zaczniesz go wdrażać, wszystko stanie się wyraźniejsze. Spójrzmy w ten sposób na rolę wzorca operacji. Wcześniej w sekcji Domena utworzyliśmy domenę główną PacktBiz.local, która reprezentuje kontroler domeny w naszym lesie.

Na kontrolerze domeny usługi AD DS automatycznie przypisują pięć ról operacji głównych. Pierwsze dwa, główny schemat i wzorzec nazw domen, to role wzorca operacji ForestWide. Podczas gdy pozostałe trzy, identyfikator względny (RID), emulator podstawowego kontrolera domeny (PDC) i wzorzec infrastruktury są rolami wzorca operacji DomainWide.

Jest tylko jeden schemat główny i jedna nazwa domeny w całym lesie, czyli PacktBiz.local, i każda domena, czyli ITBooks.local w lesie, ma swój własny wzorzec RID, emulator PDC i wzorzec infrastruktury (patrz rysunek 1.6).



Rysunek 1.6. Struktura usług AD DS.

Domena a grupa robocza (AD.4)

W wprowadzeniu do systemu Windows Server, w sekcji dotyczącej architektury sieci wyjaśniono sieci peer-to-peer (P2P) oraz sieci klient / serwer. Sieć klient/serwer jest najlepszym przykładem domeny, w której do świadczenia usług wykorzystywany jest serwer dedykowany. Podobnie sieć P2P stanowi najlepszy przykład grupy roboczej, w której komputery współużytkują zasoby bez korzystania z dedykowanego serwera.

Relacja zaufania (AD.6)

Domeny w drzewie są połączone poprzez relacje zaufania. W zaufaniu przechodnim, jeśli A ufa B, a B ufa C, to A ufa C, gdy nowa domena jest dołącza do istniejącego drzewa, wówczas nowa domena automatycznie ufa wszystkim istniejącym domenom w drzewie.

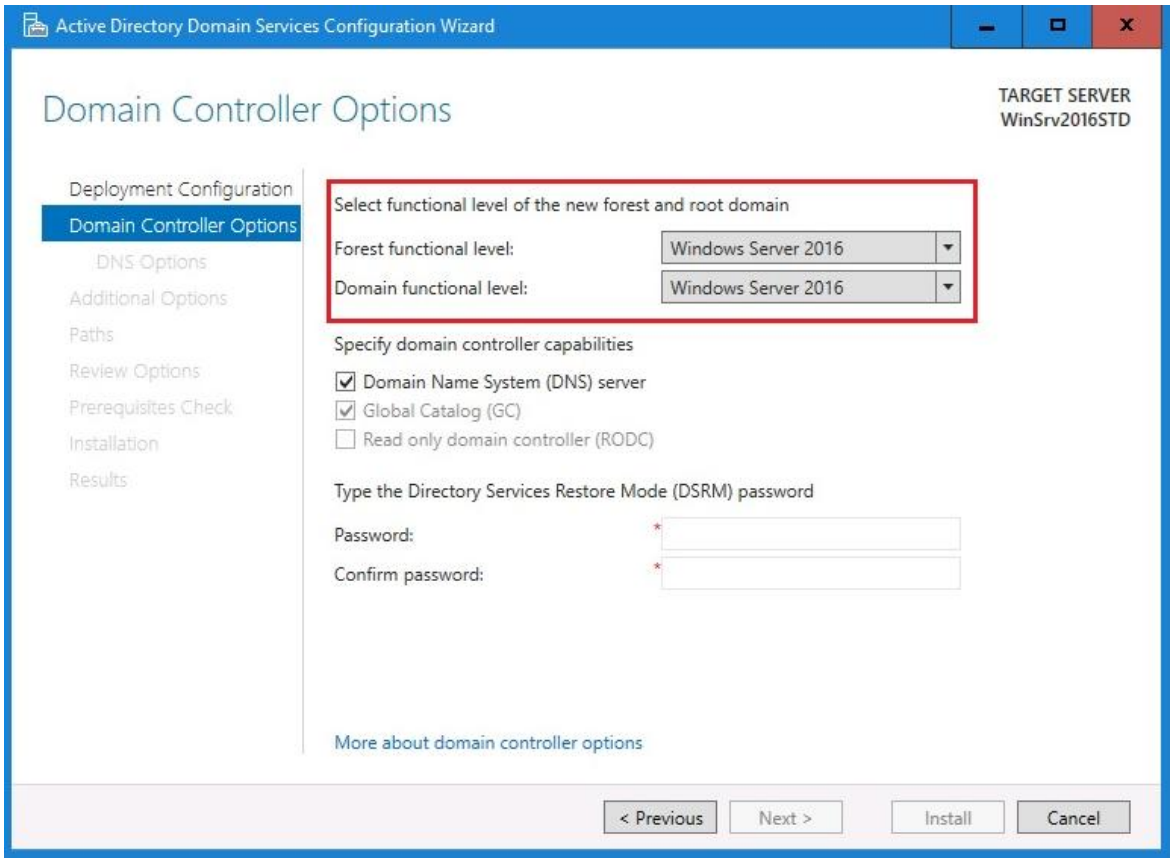
Głównym powodem istnienia Active Directory jest uwierzytelnienie obiektów (np. użytkowników, komputerów), i autoryzacja (lub jej odmowa) dostępu do innych obiektów Active Directory (dowolnych, np. kontenera lub obiektu użytkownika) oraz do zasobów innych, w tym dyskowych, sieciowych oraz aplikacji.
Aby była możliwa automatyczna autoryzacja użytkownika wobec innej usługi Active Directory lub zasobów korzystających z tej innej usługi (np. zasobu sieciowego), musi istnieć relacja zaufania pomiędzy domenami Active Directory.
Domeny połączone przez relacje zaufania weryfikowane są przez protokół Kerberos.

W usługach AD DS istnieje relacja zaufania między stacją roboczą a domeną oraz relacja zaufania między domenami. Gdy komputer dołącza do domeny, **Security Account Manager (SAM)** na komputerze lokalnym ufa mechanizmowi uwierzytelniania AD DS. W ten sposób użytkownik jest uwierzytelniany przez domenę w sieci, a nie przez lokalny SAM. Podobnie mechanizm uwierzytelniania dla każdej domeny drzewa ufa mechanizmowi uwierzytelniania dla innych zaufanych domen drzewa w lesie. Jeśli użytkownik jest uwierzytelniany przez ITBooks.local, jego uwierzytelnianie jest akceptowane przez BusinessBooks.local i ScienceBooks.local ponieważ te domeny drzew są częścią domeny głównej lasu PacktBiz.local.

Poziom funkcjonalny (AD.7)

Poziom funkcjonalny określa dostępne możliwości usług AD DS. W zależności od ustawionego dla lasu lub domeny poziomu funkcjonalności, wersje systemu Windows Server można uruchomić w lesie lub domenie.

Aby skonfigurować poziom funkcjonalności w systemie Windows Server 2016, użyj Kreatora konfiguracji usług domenowych w usłudze Active Directory, jak pokazano na rysunku 1.7:



Rysunek 1.7. Konfigurowanie poziomu funkcjonalności w systemie Windows Server 2016

Przestrzeń nazw (AD.8)

Przestrzeń nazw w Active Directory została zorganizowana hierarchicznie.

Obiekty typu kontenery mogą przechowywać inne obiekty.

Nazwa obiektu w Active Directory opisuje jego położenie w strukturze hierarchicznej.

Taką nazwę określa się mianem pełnej nazwy DN (Distinguished Name).

Podstawowe składniki DN to:
DC - komponent domenowy *(domain component)*,
CN - nazwa *(common name)*,
OU- jednostka organizacyjna *(organizational unit)*,
O - organizacja *(organization)*.

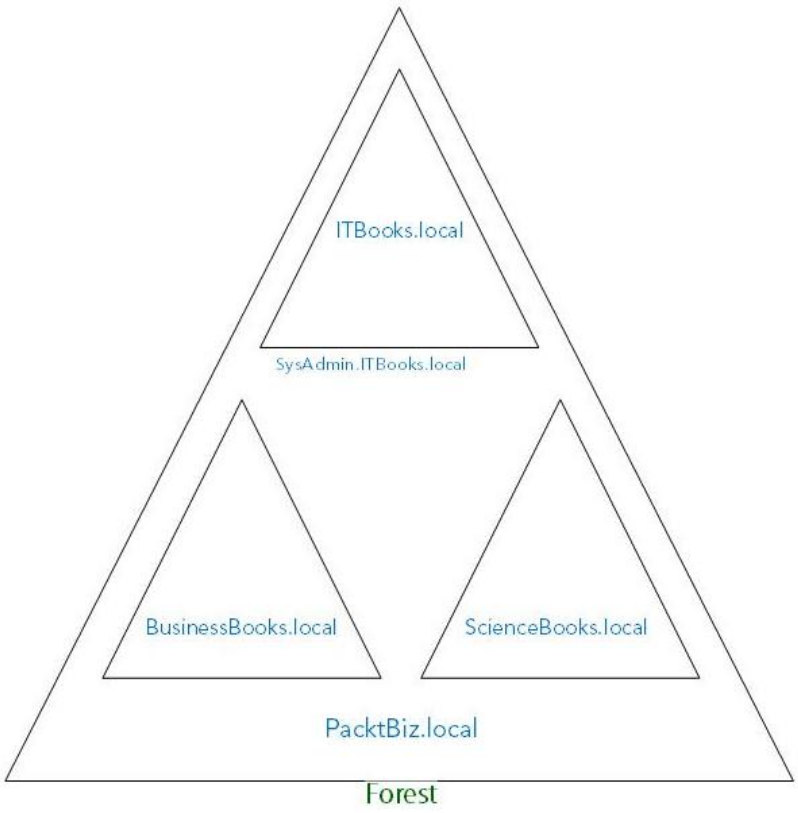
Na przykład zapis **O=Internet/DC=PL/OU=szkola/CN=uczen** oznacza, że obiekt **uczen** jest

zlokalizowany w jednostce organizacyjnej szkola domeny PL w organizacji Internet.

Nazwa względna obiektu RDN (Relative Distinguished Name) jest to część pełnej nazwy DN, zawierająca tylko atrybuty obiektu, np. w nazwie DN atrybutem obiektu jest „uczen" i jest to nazwa RDN tego obiektu.

W domenie jeden obiekt może mieć dwie identyczne nazwy RDN ale nie mogą istnieć dwa obiekty o takiej samej nazwie RDN.

W naszym lesie PacktBiz.local utworzyliśmy domeny drzew ITBooks.local, BusinessBooks.local i ScienceBooks.local. Wewnątrz domeny drzewa ITBooks.local utworzyliśmy domenę podrzędną SysAdmin.ITBooks.local. Jak widać, wszystkie te domeny drzew mają wspólną przestrzeń nazw w lesie. Jest to ciągła przestrzeń nazw (patrz rysunek 1.8):



Rysunek 1.8. Koncepcja przestrzeni nazw w usługach AD DS.

Replikacja (AD.09)

W infrastrukturze AD DS replikacja jest procesem synchronizującym wspólną partycję katalogu między wszystkimi kontrolerami domeny w lesie. Ponadto topologia replikacji to zestaw ścieżek komunikacyjnych, przez które przemieszczają się dane replikacji kontrolerów domeny.

Witryna / Strona (AD.10)

W AD DS istnieją topologie fizyczne i logiczne. Domena reprezentuje topologię logiczną, a witryna reprezentuje topologię fizyczną infrastruktury usług AD DS.

Komponentami fizycznymi Active Directory (AD.11) są: lokacje, kontrolery domen.
Lokacja jest zbiorem jednej lub większej liczby podsieci IP, pomiędzy którymi istnieją połączenia o dużej szybkości i dostępności.
Zazwyczaj granice lokacji są jednocześnie granicami sieci LAN. Podsieci powinny zostać razem zgrupowane tylko w przypadku, gdy istnieją między nimi szybkie i tanie połączenia sieciowe o wysokim poziomie dostępności. Jedna domena może obejmować kilka lokacji, a jedna lokacja może obejmować konta użytkowników i komputery należące do różnych domen.

Katalog (AD.12)

Informacje przechowywane w katalogu (w pliku Ntds.dit) są podzielone na cztery kategorie logiczne nazywane partycjami katalogu (lub kontekstem nazwy). Partycja katalogu jest jednostką replikacji.
Katalog składa się z partycji:

- Schemat- definicje obiektów, jakie mogą zostać utworzone w katalogu, oraz definicje możliwych atrybutów tych obiektów.
- Konfiguracja-służy do opisania struktury logicznej systemu. Do informacji zawartych w tej partycji należą dane dotyczące struktury domen i topologii replikacji.
- Domena- informacje o wszystkich obiektach należących do domen.
- Katalog aplikacji-służy do przechowywania danych dynamicznych należących do określonych aplikacji.

Schemat (AD.13.1)

AD, przechowuje ona obiekty. Ponieważ te obiekty są identyfikowane za pomocą nazw i atrybutów, oznacza to, że tak naprawdę to schemat jest składnikiem przechowywanym w katalogu.
Replikacja synchronizuje schemat między wszystkimi kontrolerami domeny w lesie.

Sposób replikacji informacji (13.2)

Active Directory obsługuje dwa rodzaje replikacji:

- Replikację wewnątrzlokacyjną
- Replikację międzylokacyjną (pomiędzy lokacjami).

Składniki usługi AD (14.1)

Directory System Agent (DSA) (Agent systemu) – tworzy hierarchię składowania danych w katalogu.

Database Layer (Warstwa bazy danych) – warstwa abstrakcyjna, pośrednia dla odwołań do bazy danych.

Extensible Storage Engine (Silnik pamięci masowej) – komunikuje się bezpośrednio z rekordami w magazynie katalogu.

Data store (Magazyn danych) – plik bazy danych (Ntds.dit) zarządzany przez motor bazy danych.

Zrozumienie jednostek organizacyjnych (OU) i kontenerów (AD.15)

Aby ułatwić administrowanie obiektami, konsola AD Użytkownicy i komputery DS zapewnia jednostki OU i kontenery domyślne.

Podstawowym składnikiem domeny AD jest jednostka organizacyjna (Organizational Unit) - jest kontenerem, dzięki czemu może zawierać w sobie inne obiekty, co pozwala grupować zasoby i użytkowników oraz delegować prawa administracyjne.

Jednostki organizacyjne mogą być uporządkowane hierarchicznie, np. w modelu geograficznym jednostki są tworzone zgodnie z lokalizacjami oddziałów firmy, natomiast w modelu organizacyjnym struktura jednostek powinna odpowiadać strukturze organizacyjnej firmy.

Poza jednostkami organizacyjnymi w Active Directory można tworzyć obiekty reprezentujące:

- użytkowników,
- komputery,
- drukarki,
- grupy,
- udostępnione foldery,

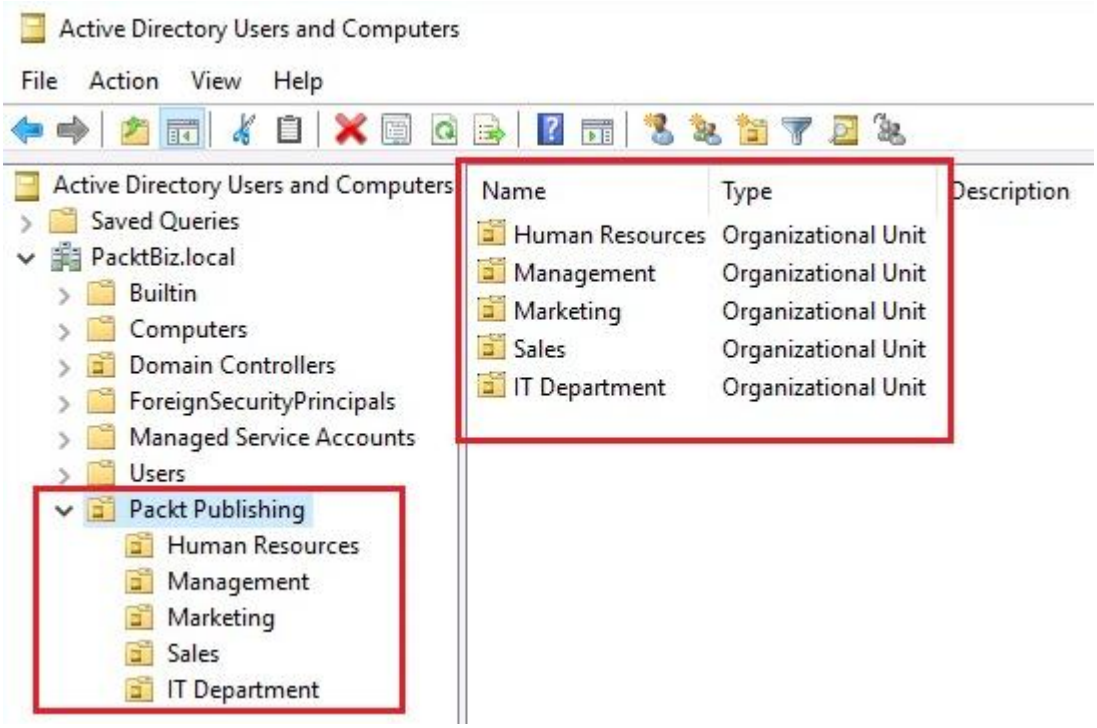
- kontakty.

Oprócz nazwy obiekt w magazynie AD ma unikalną tożsamość.
Nazwa może ulegać zmianie, tożsamość pozostaje niezmieniona.
Tożsamość definiuje Unikalny identyfikator globalny (GUID – Globally Unique Identifier).
GUID – liczba 128 – bitowa przyznana przez agenta systemu katalogowego (DSA) w momencie tworzenia obiektu. Identyfikator GUID jest przechowywany w atrybucie o nazwie objectGUID (każdy obiekt).

Nazwa główna użytkownika - User Principal Name (UPN) jest „przyjazną", krótszą -> łatwiejszą do zapamiętania od DN. Składa się ze skróconej nazwy użytkownika i zazwyczaj nazwy DNS domeny oddzielonych „@" (kowalski@szkola.com.pl). UPN jest niezależna od DN obiektu, dzięki czemu obiekt może zostać przeniesiony lub usunięty bez wpływu na sposób logowania.

Cel jednostek organizacyjnych (AD.16)

Aby ułatwić administrowanie swoimi obiektami, AD używa OU.
Zwykle użytkownicy, grupy, komputery i inne jednostki organizacyjne są umieszczane w jednostkach organizacyjnych.
Często organizacje tworzą jednostki organizacyjne w celu odzwierciedlenia swoich struktur organizacyjnych firmy.
Niezależnie od liczby domen drzew w lesie, każda domena może mieć własną hierarchię jednostek organizacyjnych, jak pokazano na rysunku 1.16:



Rysunek 1.16. Przykład hierarchii jednostek organizacyjnych w systemie Windows Server 2016

Zastosowania dla różnych obiektów kontenerowych (AD.17)

Poniżej przedstawiono proste zastosowania niektórych domyślnych kontenerów w systemie Windows Server 2016:

Komputery (Computers): jest to domyślny kontener dla uaktualnionych kont komputerów

Kontrolery domeny (Domain Controllers): Jest to domyślny kontener dla kontrolerów domeny

Zewnętrzni zarządcy bezpieczeństwa (Foreign Security Principals): Jest to domyślny kontener dla identyfikatorów bezpieczeństwa (SID)

Klucze (Keys): jest to domyślny pojemnik na kluczowe obiekty

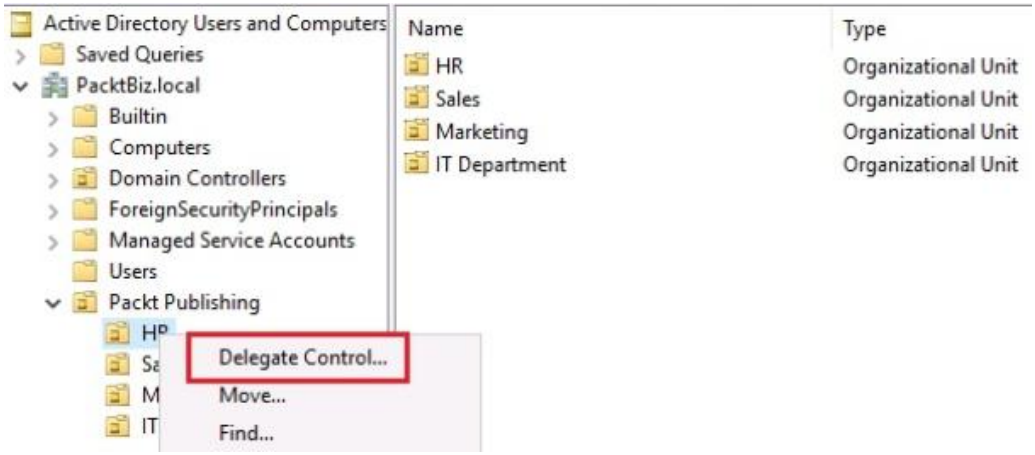
LostandFound: jest to domyślny kontener dla osieroconych obiektów

Konta usług zarządzanych (Managed Service Accounts): Jest to domyślny kontener dla kont usług zarządzanych

Użytkownicy (Users): jest to domyślny kontener dla uaktualnionych kont użytkowników

Przekazanie kontroli jednostce organizacyjnej (AD.18)

Wiedząc, że jednostki organizacyjne ułatwiają organizację obiektów AD, ilekroć chcesz udzielić uprawnień określonemu użytkownikowi lub grupie użytkowników w AD, wybór polega na przekazaniu kontroli do jednostki organizacyjnej. Wymagane jest jednak, aby przed przypisaniem uprawnień użytkownikowi lub grupie użytkowników zostali umieszczeni w jednostce organizacyjnej (1.15):

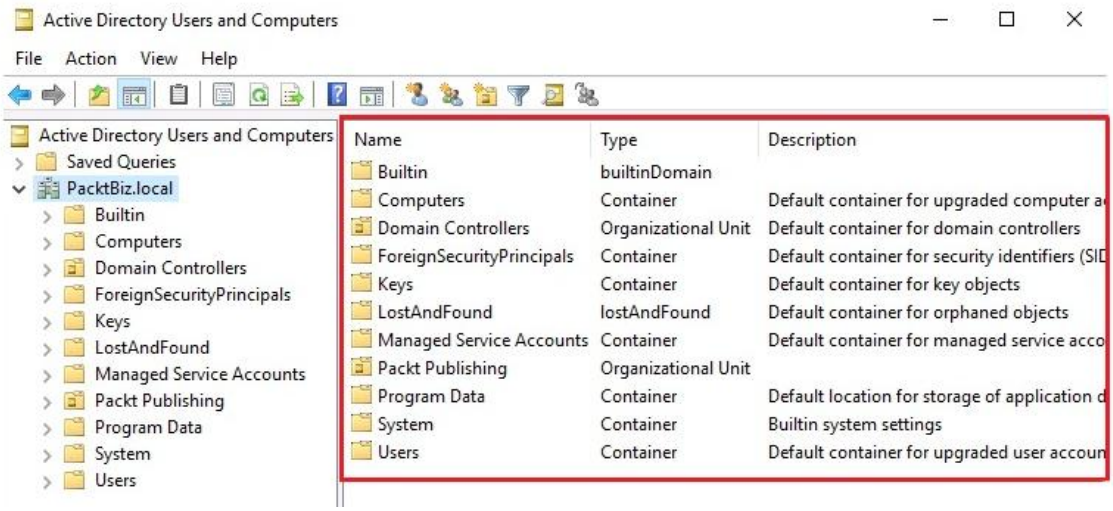


Rycina 1.18. Delegowanie kontroli do jednostki organizacyjnej w systemie Windows Server 2016

Domyślne kontenery (AD.19.1)

Po awansowaniu serwera na kontroler domeny powstaje kilka domyślnych kontenerów (patrz rysunek 1.19). Te domyślne kontenery są unikalne, ponieważ nie można zmieniać nazw, usuwać, tworzyć nowych ani kojarzyć obiektów zasad grupy (GPO) z tymi kontenerami.

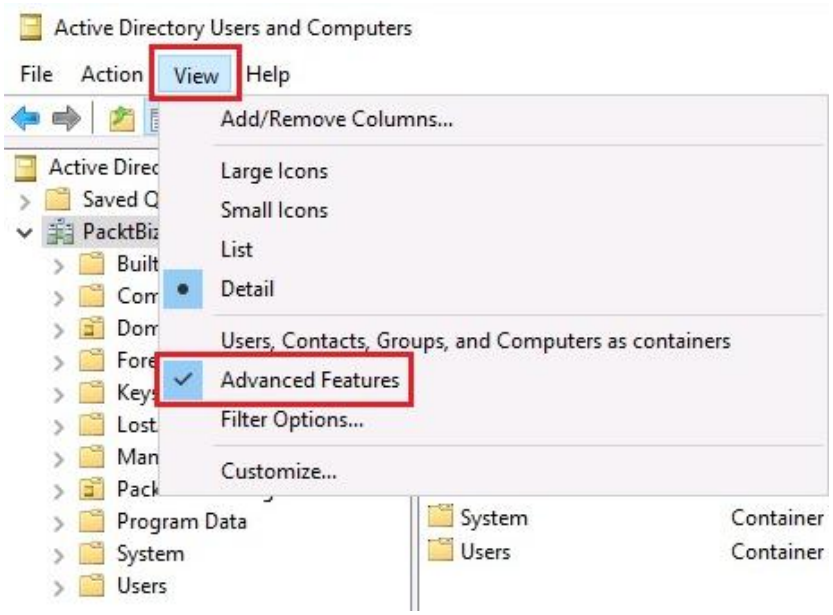
Domyślne kontenery w systemie Windows Server 2016 pokazano na rysunku 1.19.1:



Rycina 1.19.1. Domyślne kontenery w systemie Windows Server 2016

Domyślne ukryte i widoczne kontenery (AD.19.2)

Nie wszystkie domyślne kontenery są potrzebne do codziennej pracy administratora systemu.
Z tego powodu z pewnością są ukryte kontenery. Jednym z powodów, dla których domyślnie są ukryte kontenery, jest uniknięcie bałaganu w konsoli Użytkownicy i komputery usługi Active Directory.
Ponadto, gdy zaczniesz dodawać własne jednostki organizacyjne, bałagan może się pogorszyć.
Jednak bezpieczeństwo jest największym powodem, dla którego w AD są ukryte kontenery.
Aby były widoczne jak na rysunku 1.16.2, włącz opcję *Funkcje zaawansowane* z menu Widok:



Rysunek 1.16.2. Domyślne ukryte kontenery w systemie Windows Server 2016

AD a DNS (AD.20)

Głównym mechanizmem, wykorzystywanym przez Active Directory do identyfikacji obiektów, jest system DNS (Domain Name System).
DNS służy do kojarzenia nazw i adresów IP. Domeny DNS budowane są w sposób hierarchiczny.

Na różnych poziomach hierarchii występują domeny główne, podrzędne, a także komputery, np. **www. szkola.pl**

gdzie **www** jest nazwą komputera, a **szkola** - nazwą domeny szkoły w domenie **pl.**

Nie można zainstalować Active Directory bez zainstalowanego serwera DNS obsługującego tę domenę.