DO NOWEJ PODSTAWY PROGRAMOWEJ

Część 4

Sieciowe systemy operacyjne

Kwalifikacja INF.02

Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych



Podręcznik do nauki zawodu
technik informatyk

Jarosław Orczykowski, Artur Rudnicki

Helion

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiejkolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autorzy oraz Helion SA dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autorzy oraz Helion SA nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Redaktor prowadzący: Joanna Zaręba
Projekt okładki: Jan Paluch
Ilustracja na okładce została wykorzystana za zgodą Shutterstock.

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie?inf024_ebook
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-8051-6

Copyright © Helion SA 2021

- Poleć książkę na Facebook.com
- Kup w wersji papierowej
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Spis treści

Wstęp ... 5

Rozdział 1. Sieciowe systemy operacyjne ... 7
1.1. Role i zadania sieciowych systemów operacyjnych ... 7
1.2. Licencjonowanie ... 9
1.3. Wymagania sieciowych systemów operacyjnych ... 11
1.4. Przygotowanie do instalacji ... 12
1.5. Wirtualizacja systemów operacyjnych ... 13

Rozdział 2. Sieciowy system operacyjny openSUSE ... 23
2.1. Instalacja systemu operacyjnego openSUSE ... 24
2.2. Konfiguracja interfejsów sieciowych oraz aktualizacja systemu ... 32
2.3. Zabezpieczenia systemu ... 36
2.4. Zarządzanie użytkownikami i grupami ... 37
2.5. Serwer telnet ... 44
2.6. Serwer SSH ... 48
2.7. Serwer DHCP ... 51
2.8. Serwer DNS ... 57
2.9. Serwer FTP ... 68
2.10. Serwer WWW oraz uruchomienie strony internetowej ... 72
2.11. Konfiguracja i udostępnianie drukarki sieciowej ... 80
2.12. Poczta elektroniczna ... 86
2.13. Przydziały dyskowe użytkowników i grup ... 91
2.14. Automatyzacja uruchamiania zadań — cron ... 97
2.15. Serwer Samba ... 99

Rozdział 3. Sieciowy system operacyjny Windows Server 105
3.1. Przygotowanie i instalacja systemu operacyjnego Microsoft Windows Server 2016/2019 106
3.2. Konfiguracja systemu Windows Server 2016/2019 po instalacji 112
3.3. Usługa Active Directory Domain Services (AD DS) 116
3.4. Kontroler domeny 120
3.5. Tworzenie kont użytkowników i jednostek organizacyjnych w domenie oraz zarządzanie nimi 125
3.6. Automatyzacja procesu tworzenia kont użytkowników za pomocą konsoli 134
3.7. Zarządzanie kontami komputerów oraz przyłączanie ich do domeny 140
3.8. Profile użytkowników 145
3.9. Serwer DHCP 149
3.10. Serwer DNS 153
3.11. Usługi plików i magazynowania oraz mapowanie udziałów 162
3.12. Dostęp zdalny i routing 170
3.13. Usługa drukowania i zarządzania dokumentami 173
3.14. Serwery IIS, WWW i FTP 182
3.15. Zasady grupy 192
3.16. Kopie zapasowe 196
3.17. Monitorowanie pracy i wydajności serwera 199
3.18. Zdalne zarządzanie serwerem 203

Bibliografia 208
Skorowidz 209

Wstęp

Ten podręcznik jest przeznaczony dla uczniów technikum uczących się w zawodzie technik informatyk na podbudowie szkoły podstawowej, gimnazjum oraz szkoły branżowej I stopnia. Może być pomocny również dla osób, które chciałyby samodzielnie wzbogacić swoją wiedzę w zakresie konfigurowania i użytkowania sieciowych systemów operacyjnych oraz zarządzania nimi.

Treści, które zawiera podręcznik, są zgodne z podstawą programową, co oznacza, że każdy uczeń lub słuchacz musi je znać, rozumieć i umieć z nich skorzystać. Ich znajomość jest niezbędna także na dalszych etapach nauki przedmiotu oraz na egzaminie kończącym kształcenie w kwalifikacji INF.02. W podręczniku postawiliśmy na zastosowanie praktycznego wykorzystania sieciowych systemów operacyjnych, a ćwiczenia są szczegółowo opisane i poparte zrzutami ekranu, tak aby czytelnik w pełni zrozumiał omawianą tematykę.

Książka składa się z trzech rozdziałów, które są podzielone na podrozdziały zawierające omówienie poszczególnych usług i funkcji sieciowych systemów operacyjnych. Nauczyciel może realizować materiał zawarty w poszczególnych podrozdziałach po kolei lub wybiórczo.

Rozdział 1. Sieciowe systemy operacyjne

W tym miejscu czytelnik rozpoczyna przygodę z sieciowymi systemami operacyjnymi. Na początku rozdziału znajduje się krótkie wprowadzenie teoretyczne, a następnie omawiane są role i zadania, wymagania sprzętowe oraz proces instalacji. Ten rozdział zawiera także informacje na temat oprogramowania do wirtualizacji, w tym narzędzia Oracle VirtualBox, które zostało wykorzystane w umieszczonych w książce ćwiczeniach.

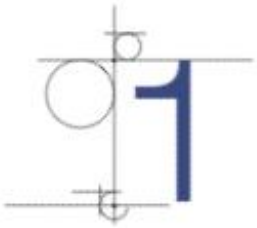
Rozdział 2. Sieciowy system operacyjny openSUSE

Drugi rozdział w sposób praktyczny, poparty licznymi zrzutami ekranu, przedstawia możliwości systemu operacyjnego openSUSE Leap 15.2. Czytelnik zainstaluje ten system, a następnie skonfiguruje jego poszczególne usługi i funkcje. Dowie się, jak zarządzać użytkownikami i grupami oraz skonfigurować i uruchomić serwery telnet i SSH. W dalszych podrozdziałach pozna szczegółową konfigurację serwerów DHCP, DNS, WWW oraz poczty elektronicznej. Nauczy się też udostępniać drukarki w sieci, tworzyć przydziały dyskowe, a na koniec skonfiguruje serwer Samba.

Rozdział 3. Sieciowy system operacyjny Windows Server

Trzeci rozdział przedstawia praktyczne wykorzystanie systemów operacyjnych Windows Server 2016 oraz Windows Server 2019. Najpierw omówiony jest proces instalowania systemu, a następnie instalowania głównej roli, jaką są usługi domenowe Active Directory. Czytelnik dowie się, jak tworzyć użytkowników, grupy zabezpieczeń, profile, zasady grupy

oraz jednostki organizacyjne, a następnie nimi zarządzać. Wdroży także serwery DHCP, DNS, WWW i wydruku. Ponadto uruchomi dostęp do internetu na komputerach, które zostały dołączone do domeny, udostępni zasoby w sieci oraz nauczy się wykonywać kopie zapasowe i zarządzać zdalnie serwerem.



1 Sieciowe systemy operacyjne

Rozpoczynając naukę o sieciowych systemach operacyjnych, najpierw należy poznać podstawowe informacje o nich i związane z nimi zagadnienia. Dowiesz się o licencjonowaniu produktów, ich wymaganiach co do sprzętu i środowiska pracy, instalacji oraz tak ważnej w dzisiejszych czasach wirtualizacji. To wszystko w skrócie omawiamy w tym rozdziale. W dalszych rozdziałach powiemy o sposobach konfiguracji usług i możliwościach ich wykorzystania.

1.1. Role i zadania sieciowych systemów operacyjnych

DEFINICJA

Sieciowy system operacyjny (ang. *network operating system*) to rodzaj systemu operacyjnego pozwalający na zaawansowaną pracę w sieci komputerowej. Tworzy środowisko współpracy dla wielu różnego rodzaju urządzeń oraz zapewnia efektywne gospodarowanie i zarządzanie ich zasobami. Najpopularniejsze sieciowe systemy operacyjne to:

- Microsoft Windows Server 2008/2012/2016/2019,
- Linux (m.in. SUSE Linux Enterprise Server, Red Hat Enterprise Linux),
- UNIX (AIX firmy IBM, FreeBSD),
- Apple macOS.

Sieciowy system operacyjny zapewnia ogromne możliwości pracy w sieci, takie jak udostępnianie zasobów oraz konfigurowanie i kontrolowanie praw i zasad przeznaczonych dla jego użytkowników i przyłączonych do niego komputerów. Koordynuje pracę całej sieci, monitoruje ją oraz pozwala na znaczącą automatyzację działań przez centralne zarządzanie użytkownikami i komputerami z poziomu serwera. Administrator ma pełną kontrolę nad siecią i wiele operacji może wykonywać w sposób zdalny. Tym wszystkim zajmuje się serwer

(komputer centralny zazwyczaj o dużej mocy obliczeniowej), na którym sieciowy system operacyjny jest zainstalowany.

Do najważniejszych ról sieciowego systemu operacyjnego zaliczamy:

- **Kontroler usług domenowych** — kontrolerem domeny może być komputer, na którym zainstalowano oprogramowanie serwerowe z rodziny Windows Server albo Linux, np. OpenSUSE. Jest to narzędzie, które zarządza realizacją zadań bezpieczeństwa pomiędzy użytkownikiem a domeną oraz określa sposób, w jaki użytkownicy domeny mogą uzyskiwać do niej dostęp, konfigurować ją, a także korzystać z jej zasobów. Więcej informacji na ten temat, w tym omówienie sposobu instalacji i konfiguracji kontrolera usług domenowych, znajdziesz w rozdziale 2. (system OpenSUSE) i rozdziale 3. (system Windows Server).
- **Serwer DHCP** (ang. *Dynamic Host Configuration Protocol*) — protokół DHCP służy do dynamicznej konfiguracji interfejsów sieciowych komputerów, urządzeń przenośnych, drukarek i wielu innych urządzeń pracujących w sieci komputerowej. Narzędzie potrzebuje serwera, na którym konfiguruje się wszystkie parametry usługi, a urządzenia powinny być skonfigurowane do pobrania ustawień z serwera DHCP. Konfiguracja serwera oraz klienta zostaną obszerniej omówione w dalszych rozdziałach podręcznika.
- **Serwer DNS** (ang. *Domain Name System*) — protokół DNS opiera się na hierarchicznej i logicznej strukturze drzewa nazywanej obszarem nazw domen. Pozwala na tłumaczenie nazw w sieciach opartych na protokołach TCP/IP na adresy IP serwerów. Działa w sieciach lokalnych, w których tłumaczy nazwy komputerów i urządzeń sieciowych, oraz w globalnej sieci internet, w której tłumaczy np. nazwy stron WWW. Więcej na temat serwera DNS oraz jego konfiguracji dowiesz się z dalszych rozdziałów.
- **Serwer WWW** (ang. *World Wide Web*) — pozwala publikować w sieci internetowej strony WWW przy użyciu protokołów HTTP oraz HTTPS. Wymaga zainstalowania odpowiedniego oprogramowania, w zależności od potrzeb i systemu operacyjnego serwera (Linux — patrz rozdział 2., Windows — patrz rozdział 3.). W dalszych rozdziałach poznasz sposoby konfiguracji tej usługi oraz możliwości jej wykorzystania.
- **Serwer FTP** (ang. *File Transfer Protocol*) — protokół FTP jest jednym z najpopularniejszych protokołów służących do transmisji plików w internecie. Jego działanie opiera się na protokołach TCP/IP. Standardowo działa na portach 20 (transmisja danych) oraz 21 (kontrola transmisji). Istnieje także jego wersja szyfrowana, **FTPS**, działająca na portach 989 (transmisja danych) oraz 990 (kontrola transmisji). W rzeczywistości wykorzystywane numery portów zależą od konfiguracji serwera. Zaletą protokołu FTP jest możliwość wznawiania transmisji plików w razie zerwania połączenia. Działa on w architekturze klient-serwer i wymaga użycia dodatkowego oprogramowania po stronie klienta. Więcej na temat konfiguracji oraz metod wykorzystania tego serwera w praktyce dowiesz się z dalszych rozdziałów.
- **Serwer SSH** (ang. *Secure Shell*) — SSH jest to standard protokołów komunikacyjnych opartych na protokołach TCP/IP. Działa na porcie 22 w architekturze klient-serwer oraz serwer-klient. Ma zastosowanie w zdalnym logowaniu i zarządzaniu serwerem najczęściej opartym na systemie Linux. Pozwala na wykonywanie poleceń i przesyłanie plików. Więcej na temat SSH, jego konfiguracji oraz wykorzystania dowiesz się z rozdziału 2.
- **Usługi pulpitu zdalnego** (ang. *Remote Desktop Services*, RDS) — działają w oparciu o protokół RDP (ang. *Remote Desktop Protocol*), umożliwiający komunikację z usługą terminala graficznego w systemach z rodziny Microsoft Windows. Pozwala na zdalną obsługę systemu operacyjnego przy użyciu trybu graficznego. Jest oparty na protokołach TCP/IP oraz działa na portach TCP 3389 i UDP 3389. Począwszy od systemu Windows 2000, pulpit zdalny jest na stałe implementowany we wszystkich wersjach Windows. Więcej informacji na jego temat, w tym omówienie jego konfiguracji i sposobów wykorzystania, znajdziesz w rozdziale 3.
- **Serwer plików** — jest to rola serwera, dzięki której można utworzyć centralne repozytorium plików dla użytkowników. To pozwala przechowywać w sieci i udostępniać wybrane zasoby użytkownikom. Każdy użytkownik może mieć przydzieloną określoną ilość miejsca na dysku, w której przechowuje swoje pliki, a także dostęp do innych zasobów w sieci. O konfiguracji serwera plików, jak również jego praktycznym wykorzystaniu piszemy w dalszych rozdziałach.
- **Serwer wydruku** — jest to usługa pozwalająca zarządzać drukarkami oraz kolejkami wydruku w sieci. Dzięki temu użytkownik nie musi mieć lokalnie podłączonej drukarki, tylko może korzystać z drukarek zlokalizowanych w sieci, w zależności od potrzeb i konfiguracji wykonanej przez administratora. To oszczędza czas i zasoby sieciowe oraz zmniejsza koszty drukowania. Konfigurację serwera wydruku i możliwości jego zastosowania poznasz w rozdziale 3.

Zadania kontrolne

1. Czym jest sieciowy system operacyjny i jakie są jego zadania?
2. Co to jest DHCP?
3. Jaka jest różnica między protokołem FTP a FTPS?
4. W jakim celu używamy protokołu SSH?

1.2. Licencjonowanie

DEFINICJA

Licencja na oprogramowanie to umowa zawierana pomiędzy podmiotem, któremu przysługują majątkowe prawa autorskie do oprogramowania, a osobą, która zamierza z takiego oprogramowania korzystać. Umowa taka określa warunki, na jakich licencjobiorca jest uprawniony do korzystania z programu. W Polsce normy prawne dotyczące rozpowszechniania programów komputerowych i ochrony praw autorskich określa *Ustawa o prawie autorskim i prawach pokrewnych* z 4 lutego 1994 roku, tekst jednolity z 2016 roku.

Programy komputerowe są rozpowszechniane na trzy podstawowe sposoby:

- W wersji pudełkowej, popularnie zwanej **BOX**. Oprogramowanie jest kupowane jako osobny produkt, który może być przenoszony pomiędzy komputerami.
- Z nowym komputerem, do którego jest ściśle przypisane. To tzw. wersja **OEM** (ang. *Original Equipment Manufacturer*). Licencja nie może być przenoszona pomiędzy komputerami.
- W formie **subskrypcji**. To nowy sposób dystrybucji oprogramowania, który polega na tym, że licencja jest przypisywana do konkretnego użytkownika, np. na podstawie adresu e-mailowego.

Można wyróżnić kilka najczęściej spotykanych licencji oprogramowania komputerowego:

- **Freeware** — program może być użytkowany i rozpowszechniany bez żadnych ograniczeń oraz opłat. Kod źródłowy nie jest jawny i nie może być zmieniany przez użytkownika. Licencja freeware może zawierać ograniczenia, które pozwalają używać programu tylko w domu, a zabraniają wykorzystania komercyjnego. Twórcy tego typu oprogramowania zakazują czerpania korzyści finansowych z jego dystrybucji przez osoby trzecie, ale nie dotyczy to produktów wytworzonych przez te programy.
- **Shareware** — wersja próbna programu komputerowego. Program może być użytkowany i rozpowszechniany bez żadnych ograniczeń, ale żeby uzyskać jego pełną funkcjonalność, trzeba wnieść opłatę lub kupić licencję. Kod źródłowy nie jest jawny i nie może być zmieniany przez użytkownika.
- **Trialware** — próbna wersja programu, który może być użytkowany w pełnej wersji przez określony czas, np. 30 dni, lub — co się często zdarza — uruchamiany określoną liczbę razy. Po upływie limitu czasu lub osiągnięciu limitu uruchomień program blokuje większość funkcji i trzeba go kupić albo usunąć z dysku komputera.
- **Adware** — rodzaj oprogramowania rozpowszechnianego najczęściej za darmo, które udostępnia pewne funkcje w zamian za wyświetlanie reklam. Autor programu często oferuje po uiszczeniu opłaty pełną funkcjonalność i brak reklam.
- **Public domain** — rodzaj oprogramowania, które zostało przekazane na użytek ogółu jako dobro publiczne. Jego dalsza dystrybucja nie wymaga zgody autora.
- **Licencja GPL** (ang. *General Public License*) — oprogramowanie jest rozprowadzane wraz z kodami źródłowymi i może być zmieniane. Szczegółowe zasady zostały określone przez Free Software Foundation.

Licencjonowanie serwerów zaprezentujemy na przykładzie Microsoft Windows Server 2016. Windows Server 2016 jest licencjonowany w modelu rdzeni (Core), procesorów (CPU) oraz licencji dostępowych (CAL).

- **Windows Server 2016 DataCenter** (przeznaczony dla wysoce zwirtualizowanych centrów danych oraz środowisk chmurowych) — licencjonowanie na rdzenie, wymagane są licencje Windows Server CAL.

- **Windows Server 2016 Standard** (przeznaczony dla zwirtualizowanych w małym stopniu lub niezwirtualizowanych środowisk fizycznych) — licencjonowanie na rdzenie, wymagane są licencje Windows Server CAL.
- **Windows Server 2016 Essentials** (przeznaczony dla małych firm, do 50 urządzeń i 25 użytkowników) — licencjonowanie na procesory.
- **Windows Storage Server 2016** (przeznaczony dla producentów sprzętu do składowania danych, dostępny w dwóch wersjach: Standard i Workgroup, a dystrybuowany tylko w kanale OEM) — licencjonowanie na procesory.
- **Windows Hyper-V Server 2016** (bezpłatny wirtualizator w wersji Core).

Oprogramowanie OpenSUSE, którego użyjemy w rozdziale 2., jest rozpowszechniane na zasadach licencji GNU GPL i ma wsparcie społeczności zgromadzonej wokół projektu. Istnieje również wersja komercyjna SUSE Linux, w której SUSE oferuje m.in. oprogramowanie SUSE Linux Enterprise Server 15 SP2 i SUSE Linux Enterprise Desktop 15 SP2 oraz pełne komercyjne wsparcie techniczne swoich produktów.

Zadania kontrolne

1. Czym jest licencja oprogramowania?
2. Czym się różni licencja freeware od licencji GPL?
3. Czym się różni licencja typu BOX od licencji OEM?

1.3. Wymagania sieciowych systemów operacyjnych

UWAGA

Każdy producent oprogramowania określa dla swoich produktów minimalne wymagania sprzętowe. To parametry, które pozwalają uruchomić program w wersji podstawowej. Żeby można było uruchomić dodatkowe usługi serwera, sprzęt musi mieć parametry lepsze od minimalnych. W szkolnych warunkach do obsłużenia niewielkiej sieci, takiej jak wykorzystana w ćwiczeniach, wystarcza procesor klasy Intel i3 oraz 3 GB pamięci operacyjnej (RAM).

Wymagania minimalne dla typowych serwerów używanych w małych firmach są następujące:

- procesor w architekturze x86-64 lub inny w zależności od systemu, taktowany z częstotliwością co najmniej 1,4 GHz;
- pamięć operacyjna o rozmiarze minimum 512 MB, jeśli użyte zostanie środowisko tekstowe, i 2 GB, jeśli ma być dostępne środowisko graficzne;
- powierzchnia dyskowa nie mniejsza niż 32 GB (lub więcej, jeśli rozmiar pamięci operacyjnej przekracza 16 GB, ze względu na wielkość pliku stronicowania, pliku hibernacji i kopii bezpieczeństwa).

Elementy komputera przeznaczonego do obsługi sieciowego systemu operacyjnego powinny być przystosowane do pracy w maszynach serwerowych. Są to wysoko wydajne podzespoły, np. procesory z rodziny Intel Xeon, serwerowe dyski twarde wyposażone w złącza typu SAS-3, zapewniające przepustowość na poziomie 12 Gb/s, płyty główne z obsługą dwóch procesorów oraz moduły RAM o bardzo dużej łącznej pojemności, np. 2048 GB. Parametry serwera dobiera się zależnie od jego przeznaczenia, dlatego mogą być bardzo różne.

Zadanie kontrolne

1. Na podstawie stron internetowych producentów oprogramowania zaproponuj parametry techniczne serwerów dla oprogramowania z rodziny Microsoft Windows Server oraz OpenSUSE działającego z interfejsem graficznym w sieci komputerowej z 25 komputerami i 20 użytkownikami.

1.4. Przygotowanie do instalacji

Przed rozpoczęciem instalacji sieciowego systemu operacyjnego warto przemyśleć, do czego będzie służył, i zaplanować, jakie usługi będą w nim uruchamiane. Wykorzystamy dwa bardzo popularne systemy operacyjne: Microsoft Windows Serwer 2016 oraz OpenSUSE Leap 15.1. Zaczniemy od pobrania obrazów ISO i przygotowania nośników instalacyjnych serwera.

- Microsoft Windows Server 2016 pobieramy ze strony *https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016*. Wybieramy na niej *Windows Server 2016*. Jedyna dostępna opcja, *ISO*, będzie zaznaczona, zatem wystarczy kliknąć *Continue*. Następnie musimy się zarejestrować, uzupełnić swoje dane i pobrać obraz instalacyjny w wersji próbnej, działającej przez 180 dni.
- OpenSUSE Leap 15.2 pobieramy ze strony *https://www.opensuse.org/*. Do wyboru mamy dwie wersje: Tumbleweed i Leap. Wskazujemy myszą tę drugą i klikamy *Zainstaluj Leap*. W aktywnej karcie *Installation x86-64* klikamy przycisk *Obraz DVD*, a następnie zapisujemy obraz na nośniku komputera.

By zainstalować system z płyty DVD, wystarczy nagrać pobrany obraz na czysty nośnik. Do zainstalowania systemu z pamięci USB można użyć darmowego narzędzia Rufus, dostępnego na stronie *https://rufus.ie*. My zainstalujemy oba systemy w maszynie wirtualnej, więc będziemy potrzebować tylko obrazu ISO systemu, który podłączymy do VM. Instalacja sieciowych systemów operacyjnych przebiega podobnie jak instalacja innych systemów klienckich, np. Windows 10 czy OpenSUSE. Dokładnie proces ten omówimy w rozdziałach poświęconych poszczególnym systemom.

Zadanie kontrolne

1. Pobierz obraz systemu operacyjnego ze strony WWW producenta.

1.5. Wirtualizacja systemów operacyjnych

ZAPAMIĘTAJ

Wirtualizacja polega na symulowaniu przez specjalne oprogramowanie procesów logicznych, które wykorzystują do tego określone podczas konfiguracji zasoby fizyczne. Dzięki temu można uruchomić w działającym systemie operacyjnym drugi system, niezależny od pierwszego. Informatycy na całym świecie bardzo chętnie wykorzystują wirtualizację. Jest ona także cennym narzędziem do nauki. Pozwala na szybkie wykonywanie kopii zapasowych, przenoszenie całych maszyn i uruchamianie na jednej fizycznej maszynie kilku wirtualnych, co umożliwia wykorzystanie w pełni mocy obliczeniowej sprzętu.

Z programów do wirtualizacji najpopularniejsze są:

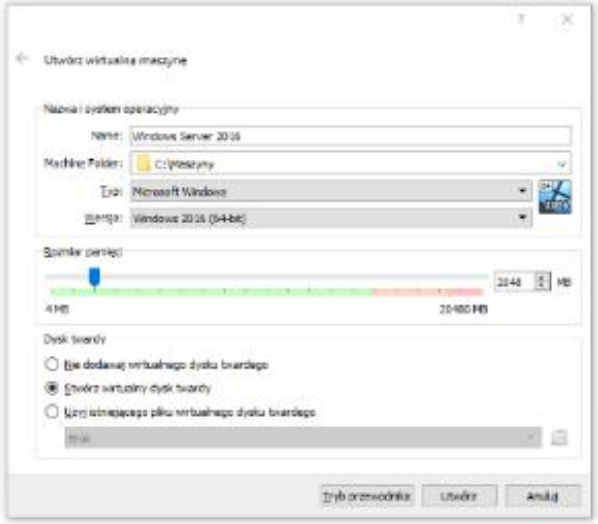
- **VMware Workstation Player** — darmowe oprogramowanie do użytku niekomercyjnego i edukacyjnego, służące do uruchamiania pojedynczych maszyn wirtualnych ze środowiskami Windows i Linux.
- **Microsoft Hyper-V** — potężne narzędzie do wirtualizacji wbudowane w system Windows 10 Pro, występujące w wersjach Windows Hyper-V Server 2016 oraz Windows Hyper-V Server 2019. Pozwala wirtualizować w tym samym czasie wiele maszyn, łącznie z wykorzystaniem wirtualnego przełącznika oraz wirtualnej sieci, a przy tym uruchamiać systemy nie tylko z rodziny Windows, ale i Linux.
- **Oracle VirtualBox** — wszechstronne i darmowe narzędzie *open source*, rozpowszechniane na warunkach licencji GNU General Public License (GPL), przeznaczone do wirtualizacji w zastosowaniach komercyjnych i domowych. Pozwala na wirtualizację wielu maszyn naraz oraz tworzenie wirtualnych sieci i przełączników. Jest ciągle rozwijane, a każde wydanie otrzymuje nowe funkcje.

Na potrzeby ćwiczeń w szkole wykorzystamy oprogramowanie Oracle VirtualBox. Okno programu pokazano na rysunku 1.1. Program jest intuicyjny i ma polski interfejs, dzięki czemu jego obsługa nie powinna Ci sprawić większych trudności. W sekcji *Globalne ustawienia* można zmienić ustawienia programu, a ustawienia maszyn wirtualnych zmienia się dla każdej oddzielnie. Program zapewnia opcje importowania i eksportowania gotowych maszyn wykonanych według standardu OVF (ang. *Open Virtualization Format*) wraz z ich ustawieniami.



Rysunek 1.1. Okno programu Oracle VirtualBox

Z głównego ekranu można dodać gotową maszynę oraz utworzyć nową. Podczas tworzenia nowej maszyny wybieramy *Tryb eksperta*, a następnie wpisujemy nazwę maszyny (w naszym przypadku to „Windows Server 2016"), wskazujemy miejsce zapisu folderu maszyny i określamy rodzinę systemu. Wówczas program wybierze zalecane ustawienia. W zależności od rozmiaru pamięci operacyjnej w systemie hosta ustalamy ilość przydzieloną dla maszyny wirtualnej. Zaznaczamy *Stwórz wirtualny dysk twardy* i wybieramy *Utwórz*. Jeśli w komputerze jest już zapisany gotowy obraz dysku, można wybrać *Użyj istniejącego pliku wirtualnego dysku twardego*, a następnie wskazać lokalizację tego pliku (rysunek 1.2).



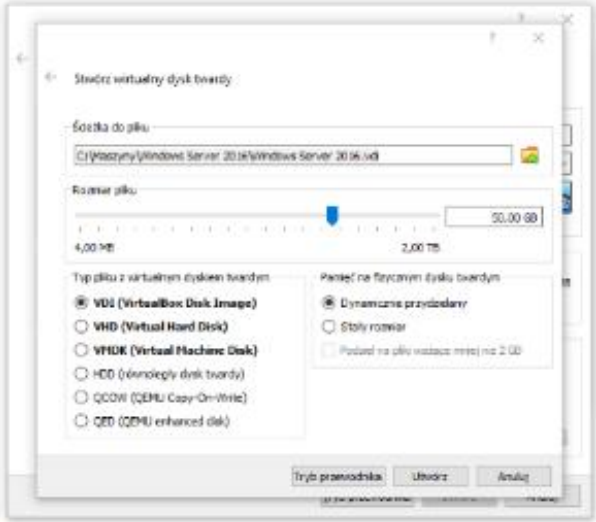
Rysunek 1.2. Okno tworzenia nowej maszyny programu Oracle VirtualBox

Teraz musimy wskazać ścieżkę zapisu pliku dysku i jego nazwę, ustalić rozmiar pliku, jego typ (VDI) i sposób przechowywania pamięci na dysku twardym, a na koniec utworzyć wirtualną maszynę przez kliknięcie przycisku *Utwórz* (rysunek 1.3). Dynamicznie przydzielany rozmiar pozwoli zaoszczędzić miejsce na dysku hosta i będzie rósł, w miarę jak będzie przybywać danych w maszynie. Stały rozmiar zapewni zaś, że na dysku hosta nie zabraknie miejsca niezbędnego maszynie wirtualnej do pracy (tworzony jest plik o wielkości odpowiadającej wybranemu rozmiarowi woluminu).

Wyróżniamy następujące rodzaje plików dysków twardych wykorzystywanych w oprogramowaniu Oracle VirtualBox:

- **VDI** — domyślny kontener dysku twardego Oracle VirtualBox, szeroko wykorzystywany przez to oprogramowanie. Producent zaleca stosowanie tego standardu ze względu na pełną kompatybilność wsteczną.

- **VHD** — kontener wykorzystywany przez Oracle VirtualBox, w pełni obsługiwany przez oprogramowanie do wirtualizacji firmy Microsoft.
- **VMDK** — kontener wykorzystywany przez Oracle VirtualBox, który również w pełni obsługuje popularny i otwarty format kontenera, używany przez wiele innych produktów do wirtualizacji, takich jak VMware.

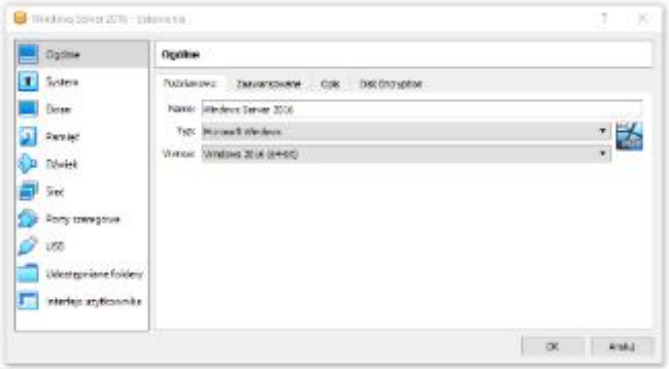


Rysunek 1.3. Okno konfiguracji wirtualnego dysku

Każda maszyna wirtualna ma szereg opcji konfiguracyjnych, które ustawia się oddzielnie dla poszczególnych maszyn. Aby zmienić opcje maszyny, należy ją zaznaczyć w programie Oracle VirtualBox, a następnie po prawej stronie kliknąć *Ustawienia*. W nowo otwartym oknie po lewej stronie zobaczysz spis poszczególnych kart ustawień, a po prawej zawartość ustawień poszczególnych elementów (rysunek 1.4).

Karta *Ogólne* zawiera następujące zakładki:

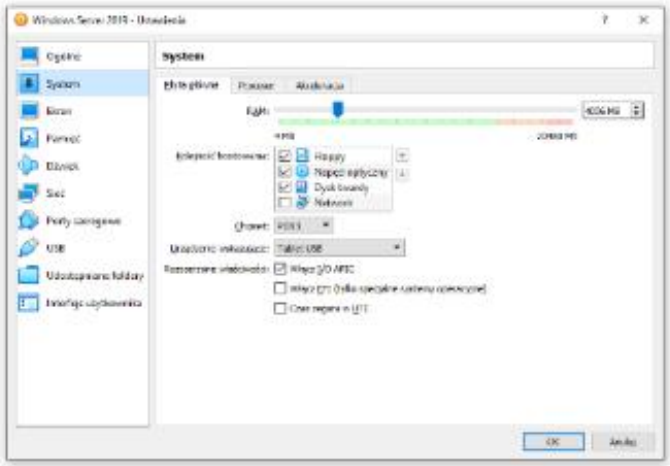
- *Podstawowe* — pozwala określić nazwę wyświetlanej maszyny oraz jej typ i wersję.
- *Zaawansowane* — umożliwia zmianę folderu przechowywania migawek, czyli zapisanych stanów maszyny wirtualnej, aby w razie potrzeby można było przywrócić ją do stanu z chwili wykonania migawki, oraz pozwala włączyć *Współdzielony schowek* (schowek komputera hosta jest współdzielony ze schowkiem maszyny wirtualnej) i *Przeciąganie i upuszczanie* (kopiowanie plików przez przeciąganie).
- *Opis* — opis maszyny i informacje użytkownika na jej temat.
- *Disk Encryption* — możliwość zaszyfrowania dysku maszyny wirtualnej.



Rysunek 1.4. Ustawienia karty Ogólne programu Oracle VirtualBox

Karta *System* zawiera następujące zakładki (rysunek 1.5):

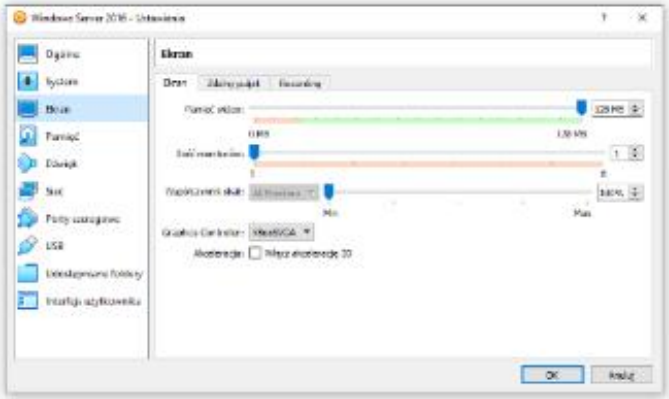
- *Płyta główna* — pozwala na zmianę przydzielonej ilości pamięci operacyjnej, kolejności bootowania (kolejności, w jakiej wybierane są nośniki rozruchowe systemu), wykorzystywanego chipsetu czy też trybu EFI.
- *Procesor* — umożliwia przypisanie do maszyny wirtualnych procesorów i określenie stopnia ich wykorzystania.
- *Akceleracja* — pozwala włączyć wirtualizację sprzętową, co przyspiesza działanie maszyny wirtualnej.



Rysunek 1.5. Ustawienia karty System programu Oracle VirtualBox

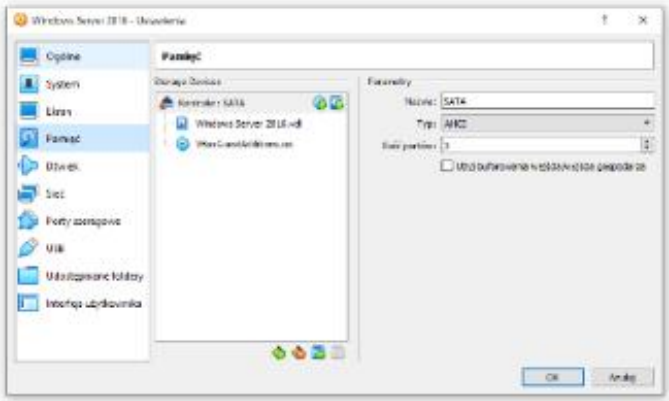
Karta *Ekran* zawiera następujące karty (rysunek 1.6):

- *Ekran* — pozwala zmienić ilość pamięci przydzielonej dla karty graficznej maszyny wirtualnej, liczbę obsługiwanych przez nią monitorów oraz kontroler grafiki.
- *Zdalny pulpit* — umożliwia utworzenie serwera usług pulpitu zdalnego, pozwalającego obsługiwać maszynę wirtualną zdalnie.
- *Przechwytywanie obrazu* (w wersji dostępnej w czasie, gdy ta książka powstawała, wróciła nieprzetłumaczona nazwa *Recording*) — umożliwia skonfigurowanie funkcji przechwytywania obrazu oraz ustawienie parametrów ekranu maszyny wirtualnej.



Rysunek 1.6. Ustawienia karty Ekran programu Oracle VirtualBox

Karta *Pamięć* umożliwia montowanie dodatkowych kontrolerów i napędów wirtualnych, takich jak obrazy ISO i obrazy dysków twardych (rysunek 1.7).



Rysunek 1.7. Ustawienia karty Pamięć programu Oracle VirtualBox

Karta *Dźwięk* pozwala włączyć dźwięki maszyny wirtualnej oraz wybrać sterownik i kontroler dźwięku (rysunek 1.8).



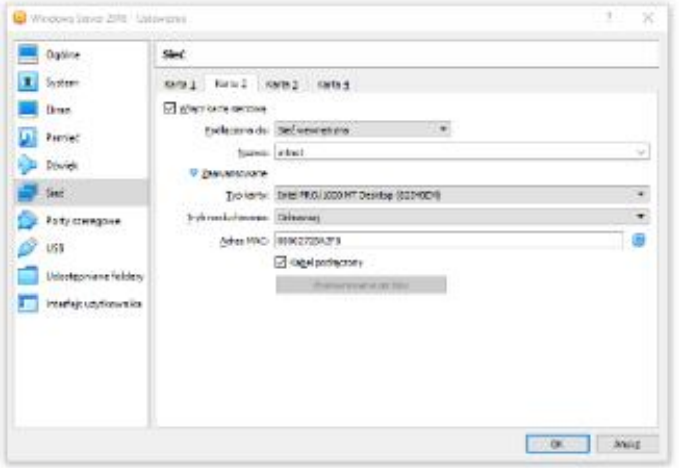
Rysunek 1.8. Ustawienia karty Dźwięk programu Oracle VirtualBox

Karta *Sieć* umożliwia włączenie i skonfigurowanie interfejsu sieciowego (rysunek 1.9). W naszym przypadku do poprawnego działania serwera będą potrzebne dwie karty sieciowe. Pierwszy interfejs będzie podłączony do NAT (ang. *Network Address Translation*), dzięki czemu uzyskamy dostęp do sieci internet w maszynie wirtualnej.



Rysunek 1.9. Ustawienia karty Sieć programu Oracle VirtualBox — konfiguracja pierwszej karty

Drugi interfejs będzie podłączony do sieci wewnętrznej i pozwoli nam w późniejszych ćwiczeniach podłączać klienta do serwera za pomocą wirtualnego przełącznika (rysunek 1.10). Jak widać na rysunkach, obydwie karty sieciowe są kartami domyślnymi i mają różne adresy MAC.



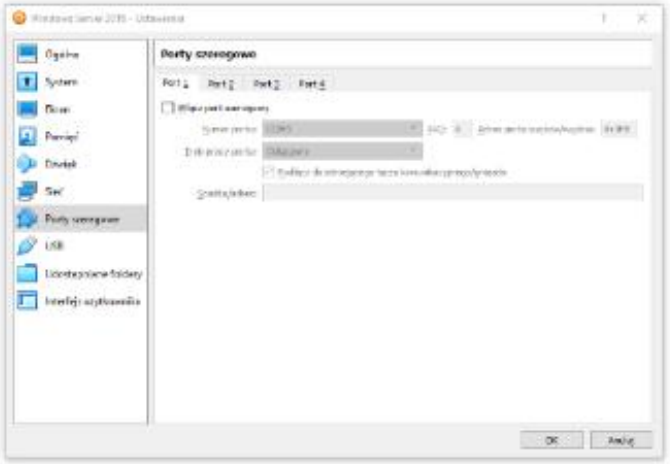
Rysunek 1.10. Ustawienia karty Sieć programu Oracle VirtualBox — konfiguracja drugiej karty

Każda z kart sieciowych może być oddzielnie skonfigurowana do działania w jednym z następujących trybów (do wyboru z listy rozwijanej *Podłączona do*):

- **NAT** (ang. *Network Address Translation* — translacja adresów sieciowych) — jeśli w planach jest tylko przeglądanie internetu, pobieranie plików i przeglądanie poczty e-mail w trybie gościa, to ten domyślny tryb będzie wystarczający.
- **Mostkowana karta sieciowa (bridged)** — jest wykorzystywana w bardziej zaawansowanych zastosowaniach sieciowych, takich jak symulacje sieci i uruchamianie serwerów w trybie gościa. Gdy ta funkcja jest włączona, Oracle VirtualBox łączy się z jedną z zainstalowanych kart sieciowych i wymienia pakiety sieciowe bezpośrednio, omijając stos sieciowy systemu operacyjnego hosta.
- **Sieć wewnętrzna** — jest wykorzystywana do utworzenia innego rodzaju sieci, opartej na oprogramowaniu, która może być widoczna dla wybranej maszyny wirtualnej, ale nie dla aplikacji działających na hoście lub w sieci zewnętrznej.
- **Karta sieci izolowanej (host-only)** — może być wykorzystywana do utworzenia sieci zawierającej hosta i zestaw maszyn wirtualnych, bez stosowania fizycznego interfejsu sieciowego hosta. Zamiast tego na hoście tworzony jest wirtualny interfejs sieciowy, podobny do interfejsu pętli zwrotnej, zapewniający łączność między maszynami wirtualnymi a hostem.
- **Rodzajowy sterownik** — ten tryb jest rzadko wykorzystywany. Ma ten sam ogólny interfejs sieciowy, umożliwiający wybór sterownika, który może być dołączony do Oracle VirtualBox lub rozprowadzany w pakiecie rozszerzeń.

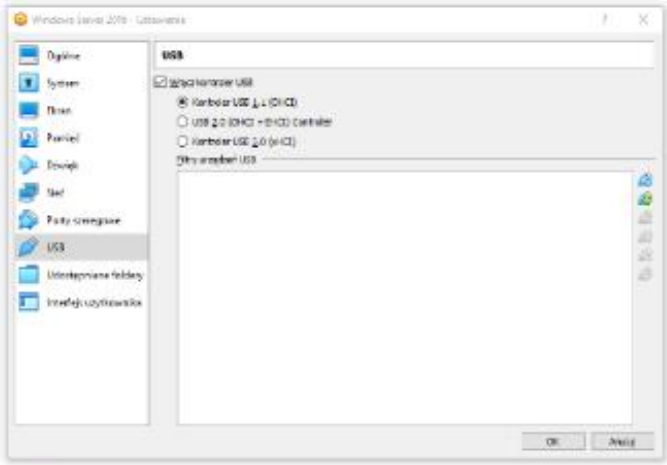
- **Sieć NAT** — to typ sieci wewnętrznej, która umożliwia połączenia wychodzące. Usługa translacji adresów sieciowych (NAT) działa w podobny sposób jak router domowy: grupuje systemy, które korzystają z niej, w sieci i uniemożliwia systemom spoza tej sieci bezpośredni dostęp do systemów wewnątrz, ale pozwala systemom wewnątrz komunikować się ze sobą i z systemami zewnętrznymi z użyciem protokołów TCP i UDP przez IPv4 i IPv6. Usługa NAT jest podłączona do sieci wewnętrznej. Maszyny wirtualne, które mają z niej korzystać, powinny być podłączone do tej samej sieci wewnętrznej. Nazwa sieci wewnętrznej jest wybierana podczas tworzenia usługi NAT w globalnych ustawieniach sieci programu Oracle VirtualBox.
- **Niepodłączona** — w tym trybie Oracle VirtualBox zgłasza gościowi, że karta sieciowa jest obecna, ale nie ma połączenia. To tak, jakby do karty nie był podłączony żaden przewód ethernet. Pozwala przerwać przewód wirtualnej sieci ethernet i tym samym połączenie, co jest przydatne do poinformowania systemu operacyjnego gościa o braku połączenia sieciowego i wymuszenia ponownej konfiguracji.

Karta *Porty szeregowe* pozwala na emulację portów szeregowych, tak aby można było korzystać na maszynie wirtualnej z rzeczywistych portów komputera hosta (rysunek 1.11).



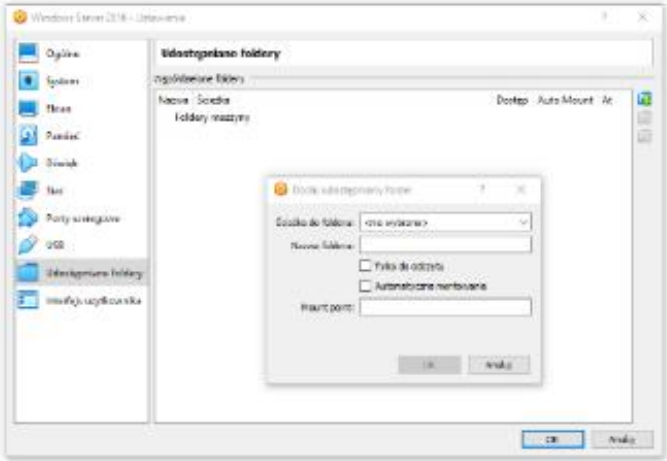
Rysunek 1.11. Ustawienia karty Porty szeregowe programu Oracle VirtualBox

Karta *USB* pozwala włączyć obsługę bezpośredniego dostępu do urządzenia USB, dzięki czemu można korzystać np. z funkcji zasilacza awaryjnego, który jest kontrolowany poprzez interfejs USB (rysunek 1.12).



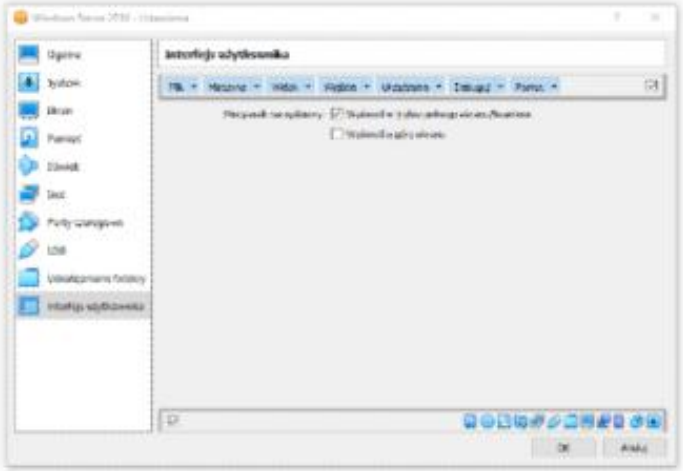
Rysunek 1.12. Ustawienia karty USB programu Oracle VirtualBox

Karta *Udostępniane foldery* pozwala utworzyć folder wspólny dla komputera hosta oraz maszyny wirtualnej (rysunek 1.13).



Rysunek 1.13. Ustawienia karty Udostępniane foldery programu Oracle VirtualBox

W karcie *Interfejs użytkownika* można skonfigurować menu dostępne w maszynie wirtualnej (rysunek 1.14).



Rysunek 1.14. Ustawienia karty Interfejs użytkownika programu Oracle VirtualBox

Zadania kontrolne

1. Przygotuj maszynę wirtualną do pracy z systemem OpenSUSE w wersji serwer oraz skonfiguruj bootowanie z obrazu ISO.
2. Przygotuj maszynę wirtualną do pracy z systemem Microsoft Windows Server 2016, a następnie skonfiguruj bootowanie ISO oraz interfejs sieciowy z obsługą internetu.

2

Sieciowy system operacyjny openSUSE

W tym rozdziale rozpoczniesz przygodę z systemem operacyjnym openSUSE, który uważa się za jedną z najlepszych dostępnych dystrybucji systemu Linux. Tworzy go ogólnoświatowa społeczność wolnego i otwartego oprogramowania, dzięki czemu jest w pełni darmowy zarówno do użytku domowego, jak i edukacyjnego czy komercyjnego. OpenSUSE stanowi bazę dla produktów linii komercyjnej SUSE Linux Enterprise. Użytkownicy cenią go za oprogramowanie YaST (ang. *Yet another Setup Tool* — jeszcze jedno narzędzie do konfiguracji) przeznaczone do zarządzania instalacją oraz konfiguracją systemu. W tym narzędziu skonfigurujemy sprzęt, sieć, usługi systemowe i wiele innych parametrów systemu.

Wymagania sprzętowe

Jak każde oprogramowanie, także openSUSE ma określone wymagania co do parametrów sprzętu, które społeczność zgromadzona wokół projektu nazywa zalecaną konfiguracją sprzętową (ang. *recommended system requirements*):

- dwurdzeniowy procesor taktowany z częstotliwością 2 GHz bądź lepszy,
- 2 GB pamięci operacyjnej,
- co najmniej 40 GB wolnej przestrzeni na dysku twardym,
- napęd DVD lub port USB do uruchomienia nośnika instalacyjnego,
- dostęp do internetu jest przydatny, a do wykonania instalacji sieciowej — wymagany.

Obecnie każdy nowy komputer ma parametry pozwalające zainstalować system i z niego korzystać. Warto pamiętać, że powyższe wymagania dotyczą systemu typu desktop; jeśli będzie pracował jako serwer, z pewnością będzie potrzebował większej mocy obliczeniowej, pojemniejszej pamięci operacyjnej (RAM) oraz większej przestrzeni dyskowej. W warunkach

edukacyjnych konfiguracja typu desktop będzie wystarczająca i pozwoli bezproblemowo wykonać ćwiczenia zawarte w tym rozdziale.

Pobranie obrazu nośnika instalacyjnego

Zaczynamy od pobrania nośnika, z którego wykonamy instalację. Aby pobrać openSUSE, musimy uruchomić stronę *http://www.opensuse.com* i wybrać jedną z dwóch ścieżek dystrybucji systemu:

- **Tumbleweed** — stabilne wydanie zawierające najnowsze wersje oprogramowania, przeznaczone głównie dla miłośników nowinek technicznych oraz twórców oprogramowania (deweloperów);
- **Leap** — stabilne wydanie długoterminowe, które zawiera stabilne i przetestowane oprogramowanie. Jest polecane do zastosowań wymagających pełnej stabilności i niezawodności oraz dla administratorów, którzy będą uruchamiać system w środowiskach produkcyjnych.

My wybieramy ścieżkę dystrybucji *Leap*. Następnie zostajemy przeniesieni do miejsca pobierania, gdzie mamy do wyboru dwie możliwości instalacji:

- *Obraz DVD* — opcja zalecana, ponieważ obraz tego typu zawiera większość potrzebnych pakietów dostępnych w dystrybucji i nie wymaga dostępu do sieci podczas instalacji (rozmiar obrazu DVD wynosi 3,99 GB);
- *Obraz sieciowy* — zalecany dla użytkowników połączeń internetowych o ograniczonej przepustowości, gdyż instalator pobierze tylko pakiety wybrane w czasie instalacji, a zatem ilość pobranych danych będzie zdecydowanie mniejsza od rozmiaru obrazu DVD.

My wybieramy pierwszą opcję, *Obraz DVD*. Możemy to zrobić na kilka sposobów, m.in. bezpośrednio z użyciem przeglądarki lub za pośrednictwem łącza typu *.torrent*. Po pobraniu obrazu jesteśmy gotowi do rozpoczęcia instalacji, której przebieg został przedstawiony w podrozdziale 2.1.

2.1. Instalacja systemu operacyjnego openSUSE

Przed przystąpieniem do instalacji systemu operacyjnego w wersji serwerowej warto zaplanować, jakie funkcje będzie pełnił w sieci, przy czym ich dobór zawsze można zmienić po zainstalowaniu systemu. My będziemy omawiać poszczególne role i funkcje serwera w kolejnych podrozdziałach, dlatego teraz przeprowadzimy tylko podstawową instalację. Zakładamy, że w warunkach edukacyjnych będziesz pracować na maszynie wirtualnej, której obsługa została zaprezentowana w rozdziale 1. Przygotowując maszynę, zastosujmy parametry zalecane do obsługi środowiska openSUSE oraz podłączmy do niej dwie karty sieciowe, z których jedna będzie podłączona do NAT, a druga do sieci wewnętrznej.

UWAGA

Nie musisz instalować systemu openSUSE zamiast systemu operacyjnego, z którego korzystasz na co dzień; warto w tym celu użyć maszyny wirtualnej (Oracle VirtualBox). Sposób jej konfiguracji został opisany w rozdziale 1. tego podręcznika.

Uruchamiamy nowo utworzoną maszynę z podmontowanym obrazem openSUSE i bootujemy system z wirtualnego nośnika. Pojawi się ekran przedstawiony na rysunku 2.1, który jest ekranem startowym instalatora openSUSE. Zacznijmy od wciśnięcia klawisza funkcyjnego *F2* i zmiany języka instalatora na polski. Pozostałe opcje dostępne za pośrednictwem klawiszy funkcyjnych to:

- *Pomoc* (*F1*) — pomoc dotycząca dowolnego bieżącego momentu instalacji i dostępnych w nim funkcji;
- *Tryb wideo* (*F3*) — zmiana rozdzielczości ekranu w trybie graficznym instalatora;
- *Źródło* (*F4*) — wybór źródła instalacji;
- *Jądro* (*F5*) — wybór sposobu instalacji: *Domyślny* — przeznaczony dla większości obecnie produkowanych komputerów, *Ustawienia bezpieczne* — stosowany w razie niepowodzenia instalacji domyślnej;
- *Program obsługi* (*F6*) — ma zastosowanie, gdy użytkownik chce dodać sterownik najnowszego sprzętu, którego system jeszcze nie zawiera.



Rysunek 2.1. Ekran instalatora systemu openSUSE

W głównym menu instalatora dostępne są następujące pozycje:

- *Uruchom system z dysku twardego* — pozwala uruchomić już zainstalowany system operacyjny;
- *Instalacja* — rozpoczyna proces instalacji systemu;
- *Aktualizuj* — pozwala zaktualizować system zainstalowany na dysku twardym komputera do nowszej wersji;
- *Więcej...* — dodatkowe opcje instalatora.

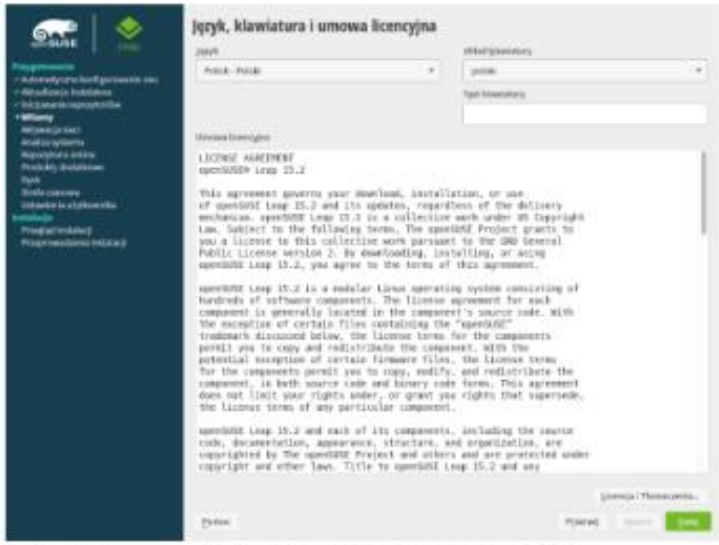
Po kliknięciu *Więcej...* instalator wyświetli następujące opcje (rysunek 2.2):

- *System ratunkowy* — uruchamia system w wersji „live", która zapewnia dostęp do dysku i umożliwia ewentualną naprawę uszkodzonego środowiska systemu operacyjnego;
- *Uruchom system Linux* — uruchamia system Linux z dysku twardego;
- *Sprawdź nośnik instalacyjny* — sprawdza poprawność nośnika instalacyjnego, a następnie uruchamia instalację;
- *Test pamięci* — uruchamia program MemTest86+, który służy do testowania pamięci operacyjnej komputera.



Rysunek 2.2. Dodatkowe opcje instalatora openSUSE

Rozpoczynając instalację, warto wykonać sprawdzenie nośnika instalacyjnego, aby mieć pewność, że obraz pobrany ze strony WWW jest poprawny. Operacja trwa kilka minut, a po zatwierdzeniu jej podsumowania zostajemy przeniesieni do okna pokazanego na rysunku 2.3, w którym należy zaakceptować umowę licencyjną, a także można zmienić wersję językową instalowanego oprogramowania oraz układ klawiatury. Aby zaakceptować ustawienia, klikamy *Dalej*.

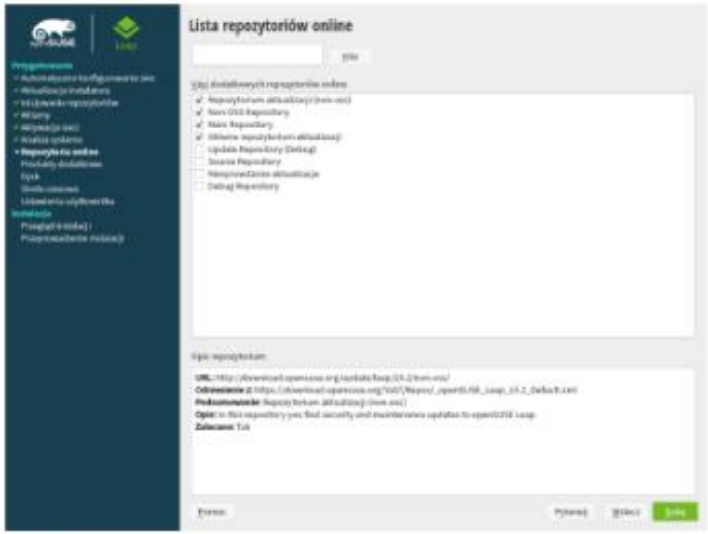


Rysunek 2.3. Ustawienia języka i klawiatury systemu openSUSE oraz umowa licencyjna

Teraz następują kolejne etapy instalacji: *Aktywacja sieci* i *Analiza systemu* (wykrywane są urządzenia komputera, urządzenia USB oraz dyski twarde, które są sprawdzane pod kątem zapisanych na nich plików, szczególnie systemowych). Jeśli system wykryje aktywne połączenie z siecią internet, na następnym etapie, *Repozytoria online*, zapyta o możliwość aktywacji repozytoriów oprogramowania online, co pozwala zainstalować dodatkowe aplikacje i zaktualizować już zainstalowane. Potwierdzamy aktywację repozytoriów online i wybieramy dostępne repozytoria, jak na rysunku 2.4:

- *Repozytorium aktualizacji (non-oss)* — zapewnia aktualizacje bezpieczeństwa i poprawki dla openSUSE Leap;
- *Non-OSS Repository* — oficjalne repozytorium openSUSE Leap dla całego oprogramowania innego niż open source, takiego jak Opera i Steam;
- *Main Repository* — duże repozytorium oprogramowania open source (OSS) dla openSUSE Leap, zapewniające dostęp do tysięcy pakietów obsługiwanych przez społeczność openSUSE;
- *Główne repozytorium aktualizacji* — zapewnia aktualizacje zarówno systemu, jak i bezpieczeństwa przeznaczone dla openSUSE Leap.

Wybieramy tylko te cztery repozytoria; reszta dostępnych jest przeznaczona dla użytkowników, którzy zajmują się projektowaniem i testowaniem oprogramowania openSUSE. Następnie klikamy *Dalej*. Instalator aktualizuje repozytoria i przechodzi do kolejnego etapu.



Rysunek 2.4. Wybór repozytoriów online

Teraz musimy wybrać funkcję, jaką będzie pełnił nasz nowo instalowany system. Role systemu przedstawia rysunek 2.5. Każda z wybranych ról może być na późniejszym etapie dowolnie modyfikowana, a system podpowiada te najbardziej uniwersalne. My wybierzemy *Pulpit standardowy* i potem doinstalujemy dodatkowe pakiety.



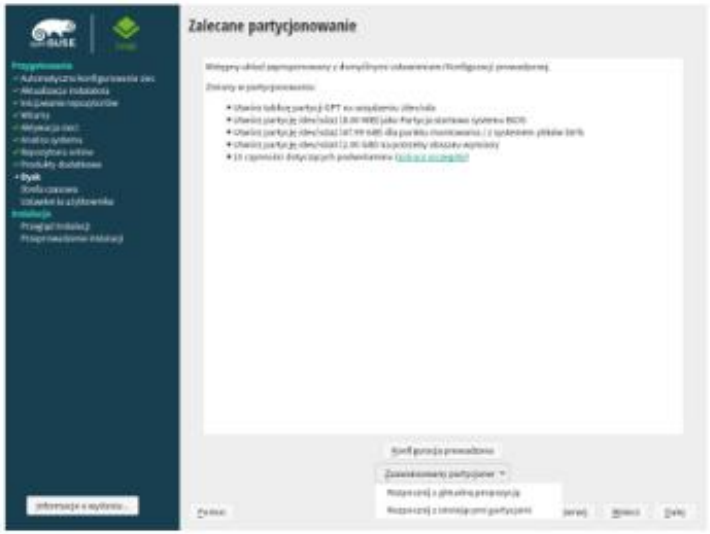
Rysunek 2.5. Wybór roli systemu openSUSE

Kolejnym etapem jest wybór sposobu partycjonowania (rysunek 2.6). Instalator proponuje optymalne ustawienia z niezbędnymi partycjami:

- *sda1* — partycja startowa o pojemności 8 MB,
- *sda3* — partycja wymiany o pojemności 2 GB,
- *sda2* — partycja punktu montowania, która zajmuje pozostałą część powierzchni dysku.

Możemy skorzystać także z dodatkowych opcji:

- *Konfiguracja prowadzona* — kreator poprowadzi nas przez proces tworzenia partycji,
- *Zaawansowany partycjoner* — udostępnia zaawansowane ustawienia partycjonowania przy zachowaniu podziału zaproponowanego przez instalator lub podziału istniejącego.

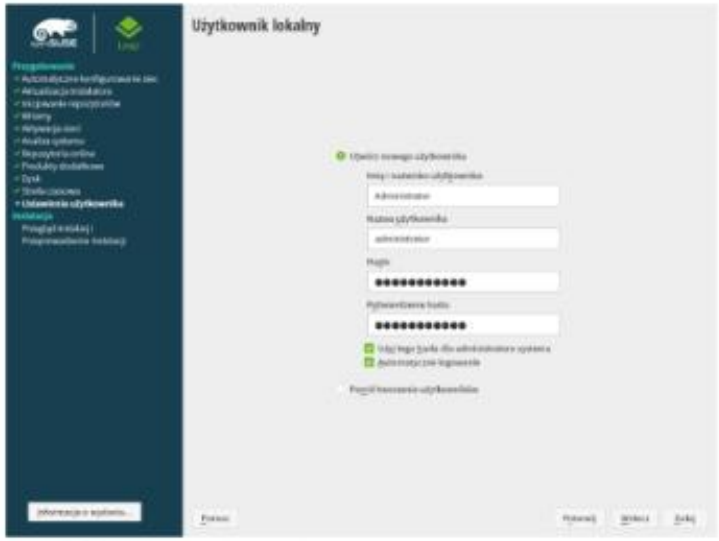


Rysunek 2.6. Schematy partycjonowania

Wybierzmy ustawienia standardowe, które zaproponował nam instalator. W tym celu od razu klikamy *Dalej* i w ten sposób przechodzimy do ustawień strefy czasowej. Ponieważ wcześniej wybraliśmy w instalatorze polskie ustawienia, podpowiada nam on, że znajdujemy się w Polsce. Sprawdzamy, czy czas systemu zgadza się z czasem rzeczywistym, a jeśli nie, klikamy *Inne ustawienia…* i zmieniamy ręcznie datę i godzinę lub synchronizujemy je z serwerem czasu za pomocą usługi **NTP** (ang. *Network Time Protocol*). Po zakończeniu klikamy *Dalej* i przechodzimy do etapu tworzenia użytkownika (rysunek 2.7). Tworzymy użytkownika lokalnego — wpisujemy imię i nazwisko, nazwę użytkownika oraz hasło. Możemy oczywiście pominąć tworzenie użytkownika, ale tylko wtedy, gdy system będzie pracował pod kontrolą innego serwera. Nasz system będzie pełnił funkcję serwera, dlatego tworzymy użytkownika. Następnie klikamy *Dalej*.

ZAPAMIĘTAJ

Hasło konta *Administrator* powinno być długie, najlepiej dłuższe niż 15 znaków, aby było trudne do złamania przez automatyczne narzędzia. Unikaj w hasłach imion, nazw i dat, które mogłyby się z Tobą kojarzyć. Dodatkowo warto użyć cyfr i znaków specjalnych. Zapisz lub zapamiętaj hasło do konta *Administrator*, ponieważ bez niego nie będziesz mógł się zalogować ani go zmienić.



Rysunek 2.7. Tworzenie konta użytkownika lokalnego

Rozpoczyna się właściwa instalacja. Pierwsza karta, *Przegląd instalacji*, wyświetla podgląd wszystkich dotąd wprowadzonych ustawień (rysunek 2.8). Na razie jeszcze żadne nie zostały zastosowane, dlatego teraz zmodyfikujemy je tak, aby system pełnił w naszej sieci funkcję serwera. W tym miejscu możemy zmodyfikować m.in. następujące ustawienia:

- *Uruchamianie systemu* — pozwala zmienić opcje dotyczące rozruchu systemu, takie jak program rozruchowy, kolejność rozruchu dysków i parametry rozruchu jądra systemu;
- *Oprogramowanie* — pozwala dołączyć lub usunąć wzorce oprogramowania i zadania systemu;
- *Domyślny element docelowy systemd* — pozwala wskazać, w jakim trybie uruchamiany będzie system, graficzny lub tekstowy;
- *System* — pozwala ponownie sprawdzić sprzęt zainstalowany w komputerze;
- *Zabezpieczenia* — pozwala włączyć lub wyłączyć zaporę sieciową (wskazane jest pozostawienie włączonej zapory) oraz włączyć lub wyłączyć protokół SSH (ang. *Secure Shell*), który umożliwia zdalne zarządzanie systemem z użyciem przeznaczonego do tego narzędzia;
- *Konfiguracja sieci* — pozwala skonfigurować sieć oraz zmienić adres IP i inne ustawienia.



Rysunek 2.8. Podsumowanie instalacji

Wszystkie elementy są skonfigurowane poprawnie, ale nieco zmienimy wzorce oprogramowania w grupie *Oprogramowanie*:

- *Base Technologies* — zaznaczamy wzorzec *Software Management*, który pozwoli nam zarządzać oprogramowaniem w trybie graficznym;
- *Graphical Environments* — zaznaczamy wzorzec *GNOME Desktop Environment (Basic)*, który pozwoli nam pracować za pomocą pulpitu graficznego GNOME;
- *Desktop Functions* — usuwamy wszystkie ewentualne zaznaczenia, ponieważ konfigurujemy maszynę z myślą o roli serwera i obsługa multimediów nie będzie nam potrzebna;
- *Server Functions* — zaznaczamy na razie tylko *Network Administration*, co umożliwi zarządzanie siecią;
- *Documentation* — zaznaczamy wszystkie opcje, aby móc korzystać z dokumentacji offline.

Ponadto w grupie *Zabezpieczenia* wprowadzamy następujące ustawienia:

- *Włącz zaporę sieciową*,
- *Włącz usługę SSH*.

Po zatwierdzeniu wyboru instalator ponownie wyświetli podsumowanie (rysunek 2.9).



Rysunek 2.9. Podsumowanie instalacji po modyfikacji

Teraz pozostaje nacisnąć przycisk *Instaluj*, a następnie w wyświetlonym oknie *Zatwierdzenie instalacji* ponownie kliknąć *Instaluj* i cierpliwie poczekać, aż instalacja się zakończy. Na koniec zostanie wykonany ponowny rozruch systemu i pojawi się okno logowania.

2.2. Konfiguracja interfejsów sieciowych oraz aktualizacja systemu

W dzisiejszych czasach nie wyobrażamy sobie pracy bez komputera i bez dostępu do sieci lokalnej lub internetowej. Niemalże każdy komputer ma obecnie interfejs sieciowy, dzięki któremu można uzyskać dostęp do internetu z dowolnego miejsca. Użytkowanie openSUSE rozpoczniemy od skonfigurowania interfejsów sieciowych, tak aby zapewnić sobie dostęp do internetu oraz sieci lokalnej. Nasz system będzie pełnił funkcję serwera, dlatego potrzebujemy dwóch kart sieciowych: pierwsza zapewni dostęp do internetu, a druga do sieci wewnętrznej. Karta podłączona do sieci NAT będzie otrzymywała adres z serwera DHCP maszyny wirtualnej, a karta podłączona do sieci wewnętrznej otrzyma adres przypisany przez nas w sposób statyczny, `192.168.0.1/24`.

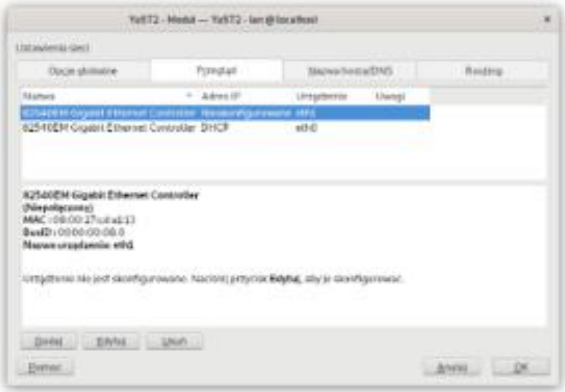
UWAGA

Interfejsy sieciowe w systemie Linux są nazywane: *eth0*, *eth1*, *eth2* itd., w zależności od liczby interfejsów w komputerze.

Ćwiczenie 2.1

Aby sprawdzić i zmienić adres IP, zalogujemy się do systemu i uruchomimy usługę YaST.

1. Klikamy w lewym górnym rogu *Podgląd/Wyświetl programy/YaST*. Po wpisaniu hasła użytkownika wybieramy *System/Ustawienia sieciowe* (rysunek 2.10).
2. Zostaniemy poinformowani, że sieć jest obsługiwana przez narzędzie NetworkManager. Potwierdzamy i w zakładce *Opcje globalne*, w sekcji *Ogólne ustawienia sieci* zmieniamy w menu *Metoda ustawiania sieci* ustawienie *Usługa NetworkManager* na *Usługa Wicked*, a następnie przechodzimy do zakładki *Przegląd*.
3. Widzimy, że interfejs sieciowy *eth0* jest skonfigurowany do pracy z DHCP, a interfejs *eth1* jest nieskonfigurowany.



Rysunek 2.10. Ustawienia kart sieciowych w YaST

4. Naciskamy *Edytuj*, zaznaczamy opcję *Adresy IP przypisane statycznie*, a następnie wprowadzamy adres IP `192.168.0.1`, maskę podsieci `/24` oraz nazwę hosta `serwer`. Potwierdzamy ustawienia przyciskiem *Dalej*. Na koniec naciskamy *OK*.

Skonfigurowaliśmy kartę sieciową, która będzie odpowiadała za pracę w sieci lokalnej.

Narzędzie YaST jest także dostępne z wiersza poleceń, czyli terminala. Aby uruchomić terminal, klikamy *Podgląd* i wpisujemy `terminal`. System sam będzie podpowiadał, jakie programy znalazł. Uruchamiamy *Terminal*.

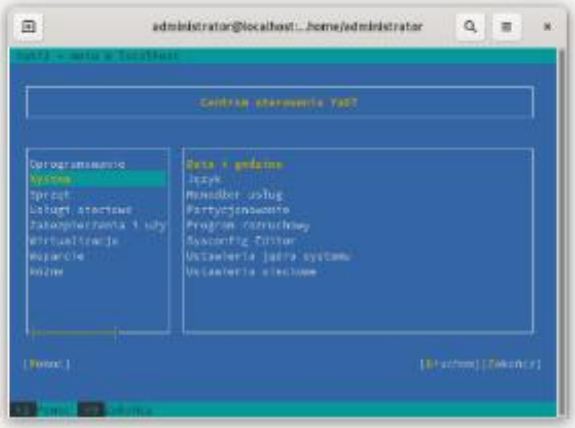
5. W oknie terminala musimy zalogować się jako *root* z użyciem polecenia su (ang. *substitute user*), jak na rysunku 2.11.



Rysunek 2.11. Uruchomiony terminal

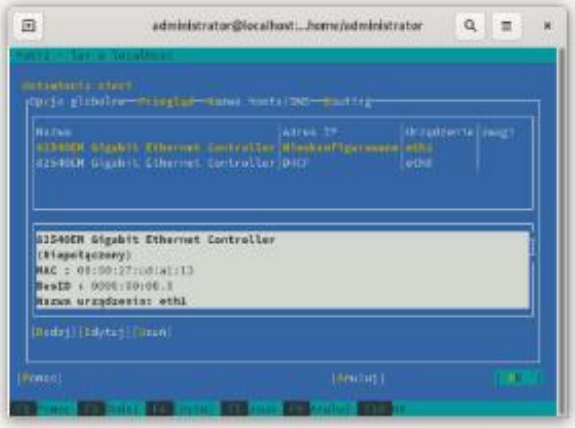
6. Z poziomu użytkownika *root* możemy uruchomić narzędzie YaST, które może być przydatne w sytuacjach krytycznych, kiedy nie mamy dostępu do trybu graficznego. Aby to zrobić, wystarczy wpisać `yast` w oknie terminala.

Obsługa narzędzia YaST z użyciem terminala jest prosta i zbliżona do obsługi w trybie graficznym. Co więcej, oprogramowanie to jest dostępne w polskiej wersji językowej (rysunek 2.12).



Rysunek 2.12. Narzędzie YaST w wersji na terminal

7. Aby skonfigurować kartę sieciową, wybieramy *System/Ustawienia sieciowe*. Pojawi się okno konfiguracji sieci bliźniaczo podobne do okna wyświetlanego w trybie graficznym (rysunek 2.13). Klawiszami strzałek przełączamy się pomiędzy oknami, a klawiszem tabulacji pomiędzy poszczególnymi kartami, aby zaznaczyć interfejs, który chcemy skonfigurować. Po zaznaczeniu karty i wciśnięciu *F4* wyświetlane są ustawienia.



Rysunek 2.13. Wybór karty do edycji w programie YaST

8. Wpisujemy adres IP `192.168.0.1`, maskę podsieci `/24` oraz nazwę hosta `serwer`. Klawiszem tabulacji przechodzimy na przycisk *Dalej*, którym zatwierdzimy zmiany, a na koniec wciskamy *OK*.

Zmiany trzeba wprowadzać za pomocą klawiatury, gdyż terminal nie obsługuje myszki.

Pokazaliśmy dwa sposoby konfigurowania karty sieciowej przy użyciu tego samego oprogramowania, ale przeznaczonego do dwóch różnych środowisk.

Instalacja aktualizacji

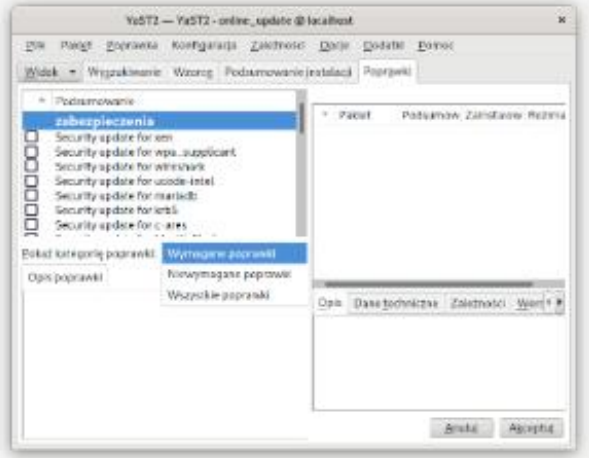
Następną czynnością, którą warto wykonać po zainstalowaniu systemu, jest instalacja aktualizacji. Dzięki temu uzyskamy najnowsze środowisko pracy. Taką aktualizację można wykonać w narzędziu YaST zarówno z terminala, jak i pulpitu graficznego.

Uruchamiamy narzędzie YaST i przechodzimy do *Oprogramowanie/Aktualizacja online*, gdzie możemy wybrać jeden z trzech schematów aktualizacji. Aby to zrobić, w zakładce *Poprawki* rozwijamy menu *Pokaż kategorie poprawki*, w którym mamy do wyboru:

- *Wymagane poprawki* — wszystkie najważniejsze poprawki bezpieczeństwa systemu oraz programów;
- *Niewymagane poprawki* — poprawki, które nie mają wpływu na bezpieczeństwo i stabilność działania systemu;
- *Wszystkie poprawki* — wszystkie dostępne poprawki systemu oraz zainstalowanych programów.

Najbezpieczniejszą i zalecaną opcją jest ta pierwsza. Po jej wybraniu potwierdzamy instalację przyciskiem *Akceptuj* (rysunek 2.14).

Pobranie i instalacja aktualizacji trwają łącznie kilka minut, w zależności od łącza internetowego. Po zainstalowaniu poprawek warto uruchomić komputer ponownie.



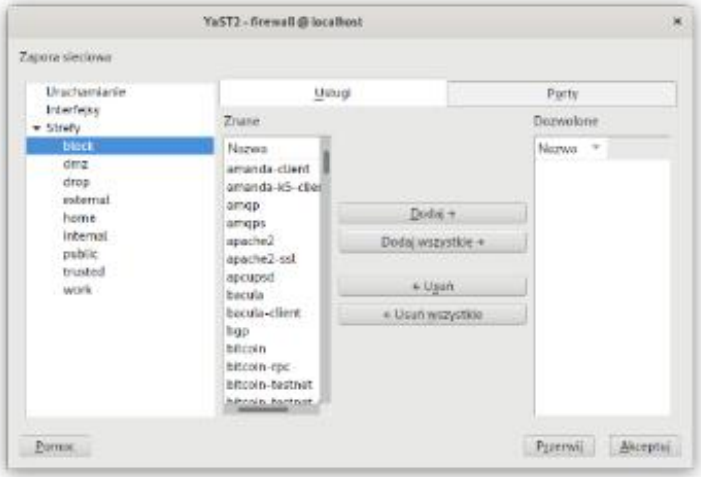
Rysunek 2.14. Instalacja aktualizacji systemu i oprogramowania

2.3. Zabezpieczenia systemu

Zabezpieczenia to bardzo ważny element każdego systemu. OpenSUSE, jak każdy system operacyjny, jest narażony na zamierzone awarie, włamania, sabotaż czy też wirusy. Pierwszą linią obrony jest zabezpieczony dostęp do plików w postaci konta typu *root*. Niestety słabe hasło do takiego konta albo jego kradzież umożliwiają atakującemu całkowitą destrukcję systemu. *Root* to uprawnienia, ale i konsekwencje. To konto, które ma pod sobą wszystkie inne konta w systemie, o czym trzeba szczególnie dobrze pamiętać.

Mówiąc o kwestiach bezpieczeństwa, należy wspomnieć o aktualizacjach systemowych. Bardzo często są to aktualizacje zabezpieczeń i poprawki błędów, które mogą w poważny sposób zagrozić bezpieczeństwu systemu. To także aktualizacje oprogramowania, które nie tylko łatają błędy, ale także dodają nowe ustawienia lub nową funkcjonalność.

OpenSUSE ma świetną zaporę sieciową (ang. *firewall*). My na potrzeby ćwiczeń wyłączyliśmy ją, ale w rzeczywistym systemie jest wskazana. To ona w 99 procentach chroni nasz system z zewnątrz. Zapora jest zlokalizowana w oprogramowaniu YaST. Uruchamiamy ją przez kliknięcie *Zabezpieczenia i użytkownicy/Zapora sieciowa* (rysunek 2.15). Okno zarządzania jest podzielone na dwie części. W pierwszej są pokazane zdefiniowane strefy, a w drugiej — poszczególne usługi i porty, które można ustawić jako dozwolone lub nie. Dodatkowo większość programów, które konfigurujemy w systemie, umożliwia automatyczne dopisanie się do wybranej strefy.



Rysunek 2.15. Widok zapory sieciowej

Innym elementem, który pozwoli zadbać o bezpieczeństwo, jest program antywirusowy, np. ClamAV, dostępny w większości dystrybucji systemu Linux. Jest instalowany z wiersza poleceń,

ale ma także nakładkę graficzną. Instalujemy go poleceniem `sudo zypper install clamav`, a jego nakładkę graficzną poleceniem `sudo zypper install clamtk`. Interfejs graficzny tego narzędzia jest bardzo intuicyjny w użyciu (rysunek 2.16).

Istnieje jeszcze wiele innych zagrożeń, na których omówienie nie starczy tu miejsca, pochodzących zarówno z zewnątrz, jak i z wewnętrznej sieci. Dlatego administrator systemu musi cały czas pogłębiać także wiedzę z tej dziedziny. Trzeba pamiętać, że nie ma bezpiecznego systemu, ale często zagrożenie wynika z ludzkiego błędu.



Rysunek 2.16. Program ClamAV z nakładką ClamTK

2.4. Zarządzanie użytkownikami i grupami

Konto użytkownika to bardzo ważny element systemu operacyjnego. Zapewnia bezpieczeństwo, a także umożliwia pracę w systemie wielu osobom w jednym czasie. Aby można było tworzyć nowe konta, trzeba użyć konta użytkownika, który ma do tego uprawnienia. W różnych systemach operacyjnych tacy użytkownicy mają różne nazwy. W systemach z rodziny Linux najwyższe uprawnienia ma konto *root*. Ma ono nieograniczoną władzę nad systemem i jest tworzone jako pierwsze, podczas instalacji systemu.

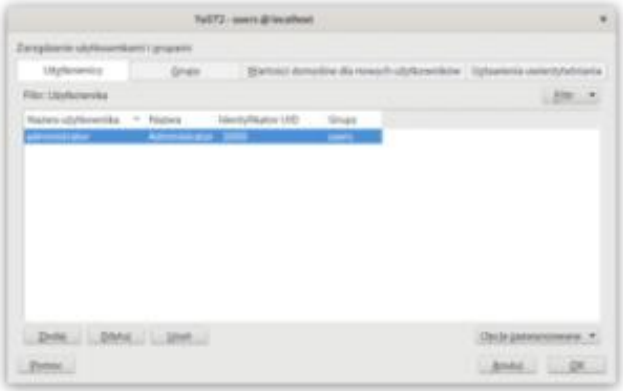
Tworzenie i edytowanie kont użytkowników

Poniższe ćwiczenie przedstawia sposób dodawania użytkownika za pomocą oprogramowania YaST.

Ćwiczenie 2.2

1. Aby utworzyć użytkownika, musimy uruchomić program YaST, a w nim wybrać *Zabezpieczenia i użytkownicy/Zarządzanie użytkownikami i grupami*. Otworzy się okno zawierające listę kont użytkowników (rysunek 2.17).

   Na razie skupimy się na karcie *Użytkownicy*. Na dole są trzy przyciski: *Dodaj* (dodawanie konta), *Edytuj* (edycja utworzonego konta) i *Usuń* (usuwanie konta).

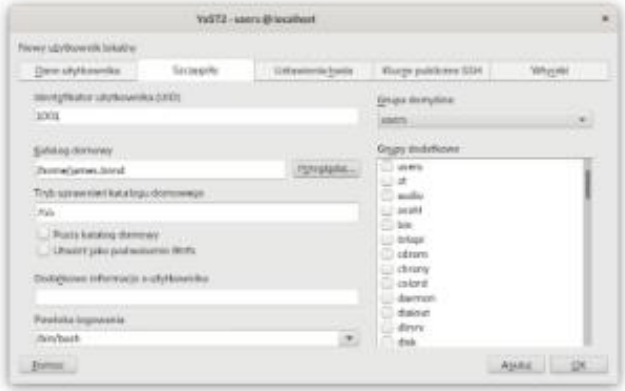


Rysunek 2.17. Moduł dodawania użytkowników YaST

2. Wybieramy *Dodaj* i na karcie *Dane użytkownika* uzupełniamy pola: *Imię i nazwisko użytkownika*, *Nazwa użytkownika*, *Hasło* oraz *Potwierdzenie hasła*. Hasło powinno mieć od 6 do 127 znaków i nie może zawierać polskich znaków ze względu na to, że w razie awarii może być konieczne zalogowanie się za pomocą klawiatury o innym układzie i nieobsługującej polskich znaków. Dodatkowo na dole możemy zaznaczyć dwie opcje (rysunek 2.18):
   - *Odbiera pocztę systemową* — system będzie wysyłał do użytkownika ważne powiadomienia;
   - *Wyłącz logowanie użytkownika* — konto zostanie utworzone, ale użytkownik nie będzie mógł się zalogować.
3. Przechodzimy do karty *Szczegóły*, w której musimy wprowadzić dodatkowe informacje o użytkowniku.

   Na tej karcie można ustawić następujące parametry konta:
   - *Identyfikator użytkownika (UID)* — unikatowy numer przydzielany każdemu użytkownikowi systemu. Zwykli użytkownicy mają numery większe od 499, mniejsze zaś są zarezerwowane przez system do celów specjalnych. YaST zapobiegliwie zaczyna numerację od numeru 1000, który przyznaje użytkownikowi tworzonemu podczas instalacji.
   - *Katalog domowy* — katalog, w którym użytkownik przechowuje swoje pliki i dokumenty. Domyślną lokalizacją jest */home/nazwa_użytkownika*. Aby ją zmienić, naciskamy *Przeglądaj*.
   - *Tryb uprawnień katalogu domowego* — domyślnie ustawiony tryb 755 oznacza, że właściciel konta ma prawa do odczytu, zapisu i wykonywania plików, a grupa, do której należy, oraz pozostali użytkownicy — tylko do odczytu i wykonywania. Na tym etapie możemy to zmienić.

- *Pusty katalog domowy* — po zaznaczeniu tej opcji zostanie utworzony pusty katalog domowy.
- *Utwórz jako podwolumin Btrfs* — pozwala utworzyć katalog domowy użytkownika jako podwolumin zamiast zwykłego katalogu, gdy jest dostępny system plików Btrfs.
- *Dodatkowe informacje o użytkowniku* — może zawierać trzyczęściowe dodatkowe informacje oddzielone przecinkami, np. telefon służbowy, telefon domowy, numer pokoju.
- *Powłoka logowania* — określa powłokę logowania (interpreter poleceń) dla danego użytkownika.
- *Grupa domyślna* — domyślna grupa, do której będzie należał tworzony użytkownik. System podpowiada grupę *users*, którą można zmienić.
- *Grupy dodatkowe* — możemy zaznaczyć grupy, których członkiem będzie tworzony użytkownik.



Rysunek 2.18. Karta Szczegóły zawierająca szczegółowe parametry nowego konta użytkownika

4. Otwieramy kartę *Ustawienia hasła*, w której dostępne są następujące opcje (rysunek 2.19):
   - *Wymuś zmianę hasła* — pozwala wymusić na użytkowniku zmianę hasła podczas pierwszego logowania.
   - *Ostrzeż na podaną liczbę dni przed wygaśnięciem hasła* — określa, ile dni przed wygaśnięciem hasła wyświetlane będzie ostrzeżenie. Po ustawieniu -1 komunikat nie będzie wyświetlany.
   - *Określ, przez ile dni po wygaśnięciu hasła dopuszczać logowanie* — określa, ile dni po wygaśnięciu hasła użytkownicy mogą się logować. Wartość -1 ustawia nieograniczony dostęp.

- *Maksymalna liczba dni z tym samym hasłem* — określa, przez ile dni użytkownik może używać jednego hasła.
- *Minimalna liczba dni z tym samym hasłem* — określa minimalną liczbę dni, po której można zmienić hasło.
- *Data wygaśnięcia* — określa, kiedy konto wygaśnie. Data powinna być podana w formacie *RRRR-MM-DD*. Puste pole oznacza, że konto nigdy nie wygaśnie.



Rysunek 2.19. Ustawienia hasła dla tworzonego użytkownika

5. Aby utworzyć użytkownika, wystarczy teraz nacisnąć *OK*. Powracamy w ten sposób do karty *Zarządzanie użytkownikami i grupami*. W tym miejscu możemy utworzyć kolejnego użytkownika. Jeśli nie chcemy tego robić, naciskamy *OK*, aby potwierdzić utworzenie nowego użytkownika w systemie.

Aby zmienić ustawienia istniejącego konta użytkownika, należy w karcie *Zarządzanie użytkownikami i grupami* kliknąć *Edycja*. Robi się to w taki sam sposób jak podczas tworzenia nowego konta.

Aby zaś usunąć użytkownika, wystarczy zaznaczyć konto i nacisnąć *Usuń*, a następnie zatwierdzić operację.

Konto użytkownika można dodać z użyciem terminala za pomocą polecenia `useradd`. Wystarczy zalogować się w terminalu na konto z uprawnieniami *root* i wpisać:

```
sudo useradd jacek.nowak,
```

a wtedy konto o nazwie *jacek.nowak* zostanie utworzone.

Jednak tak utworzone konto nie będzie miało ustawionego hasła ani innych opcji. Aby je skonfigurować w trakcie tworzenia, w poleceniu musimy zastosować przełączniki. Oto niektóre z nich:

- `-c komentarz` — dodanie komentarza do pola komentarza w pliku haseł.
- `-d katalog_domowy` — ustawienie katalogu domowego dla nowego użytkownika. W standardowej konfiguracji odbywa się to przez dostawienie do domyślnego katalogu nazwy użytkownika.
- `-e data_wygaśnięcia` — określenie, kiedy konto użytkownika zostanie zablokowane (wyłączone). Datę należy podać w formacie *RRRR-MM-DD* (miesiąc i dzień muszą być podane w postaci dwucyfrowej).
- `-f czas_nieaktywności` — ustawienie liczby dni, po której konto ma być definitywnie wyłączone. Podanie wartości 0 sprawi, że konto zostanie wyłączone zaraz po wygaśnięciu hasła, a wartość -1 dezaktywuje tę funkcję (jest to wartość domyślna).
- `-g początkowa_grupa` — numer lub nazwa początkowej grupy logowania użytkownika. Grupa musi istnieć. Domyślnym numerem grupy jest 1.
- `-G grupa` — grupa lub lista grup, do których ma należeć tworzony użytkownik. Każda grupa powinna być oddzielona od poprzedniej przecinkiem bez spacji. Użytkownik domyślnie należy tylko do grupy początkowej.
- `-m katalog_z_profilem` — ustawienie tej opcji spowoduje, że jeżeli katalog domowy użytkownika nie istnieje, to zostanie utworzony.
- `-s powłoka` — ustawienie powłoki systemowej użytkownika. Jeśli użytkownik nie postanowi inaczej, wybierana jest domyślna powłoka systemowa.
- `-u id_użytkownika` — podanie numerycznej wartości identyfikatora użytkownika (UID). Numer ten musi być dodatni i unikatowy. Domyślnie ustawiana jest wartość najmniejsza, począwszy od wartości 500 (wartości od 0 do 499 są przeznaczone dla kont systemowych).
- `nazwa_użytkownika` — tutaj należy podać nazwę tworzonego konta użytkownika.

Spróbujmy teraz utworzyć konto o nazwie *jacek.nowak* z katalogiem domowym */home/jacek.nowak*, do którego hasło wygaśnie 31.12.2022 i które po wygaśnięciu hasła nie zostanie wyłączone (rysunek 2.20).

```
sudo useradd -d /home/jacek.nowak -e 2022-12-31 -f -1 jacek.nowak
```



Rysunek 2.20. Utworzenie konta użytkownika za pomocą terminala

W terminalu jest dostępnych kilka przydatnych narzędzi:

- `sudo passwd` — zmiana hasła zalogowanego użytkownika. Użytkownik zostanie poproszony o wpisanie obecnego hasła, a następnie nowego.
- `sudo passwd` **`nazwa_użytkownika`** — zmiana hasła użytkownika, wymaga uprawnień *root*.
- `sudo usermod` — zmiana ustawień konta. Tej opcji używa się w ten sam sposób co polecenia `useradd`.
- `sudo userdel` **`nazwa_użytkownika`** — usuwa konto, ale bez katalogu domowego.
- `sudo userdel -r` **`nazwa_użytkownika`** — usuwa konto razem z katalogiem domowym.

Tworzenie grup

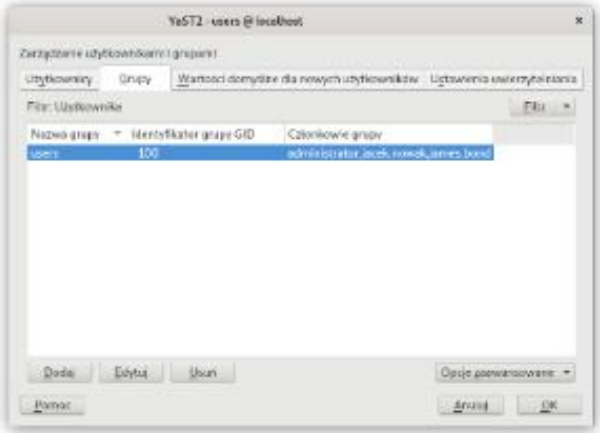
Czas omówić grupy. Z systemów wieloużytkownikowych w tym samym czasie może korzystać dużo osób, przez co mogą wystąpić problemy z dostępem do poszczególnych zasobów. Przypisywanie poszczególnych użytkowników do zasobów jest czasochłonne i może prowadzić do pomyłek. Aby rozwiązać ten problem, należy skorzystać z funkcji *Grupy*, pozwalającej określić użytkowników należących do konkretnej grupy, a prawa do zasobu określić jako prawa grupy. W nowo zainstalowanym systemie istnieje już szereg grup. Najczęściej wykorzystywana jest *Users*, do której domyślnie należą wszyscy użytkownicy (o ile nie zostanie to zmienione podczas tworzenia użytkownika).

W ćwiczeniu 2.3 pokażemy, jak utworzyć grupę oraz przypisać do niej użytkowników.

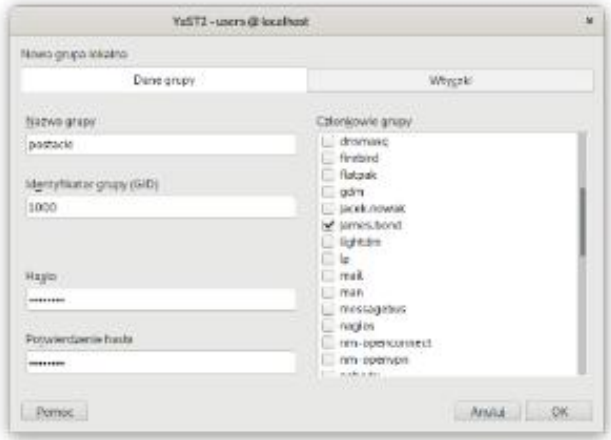
Ćwiczenie 2.3

1. Uruchamiamy program YaST, a następnie wybieramy *Zabezpieczenia i użytkownicy/ Zarządzanie użytkownikami i grupami*. Otworzy się to samo okno, które oglądaliśmy już we wcześniejszej części tego podrozdziału, kiedy to tworzyliśmy użytkowników i zarządzaliśmy nimi.
2. Przechodzimy do karty *Grupy*, w której możemy dodawać nowe grupy (*Dodaj*), edytować istniejące (*Edytuj*) oraz je usuwać (*Usuń*), jak na rysunku 2.21.
3. Wybieramy *Dodaj* i uzupełniamy poszczególne dane na karcie (rysunek 2.22):
   - *Nazwa grupy* — pod tą nazwą grupa będzie dostępna. Producent openSUSE zaleca stosowanie krótkich nazw, o długości od dwóch do ośmiu znaków.
   - *Identyfikator grupowy (GID)* — tak samo jak użytkownicy, grupy mają unikatowe identyfikatory. Zasadniczo można im przypisywać numery od 0 do 60000, ale YaST, aby uniknąć problemów z dublowaniem identyfikatorów, zaproponuje wartości od 1000.
   - *Hasło* i *Potwierdzenie hasła* — przez ustawienie hasła zabezpieczymy dostępność grupy dla użytkowników. Użytkownik, który będzie chciał dołączyć do grupy, będzie musiał wprowadzić hasło.

Rysunek 2.21. Zarządzanie grupami w narzędziu YaST



Rysunek 2.22. Dodawanie nowej grupy w narzędziu YaST



- *Członkowie grupy* — na tym etapie możemy już przypisać użytkowników do tej grupy.

4. Naciskamy *OK*, a wtedy grupa zostaje utworzona. Aby potwierdzić operację i zapisać nowo utworzoną grupę w systemie, na karcie *Zarządzanie użytkownikami i grupami* naciskamy *OK*.

Grupa, którą utworzyliśmy, będzie już dostępna podczas tworzenia nowych użytkowników i będziemy mogli konfigurować uprawnienia grupy do zasobów.

Za pomocą terminala tworzy się grupy w podobny sposób jak użytkowników, z zastosowaniem polecenia `groupadd`:

- `sudo groupadd pracownicy` — tworzy grupę *pracownicy* z domyślnymi ustawieniami;
- `sudo groupdel pracownicy` — usuwa grupę *pracownicy*.

W tym miejscu warto wspomnieć o hasłach, gdyż to od nich zależy bezpieczeństwo użytkowników i systemów. Nawet najsilniejsze hasło jest dużym zagrożeniem, jeśli jest używane w wielu miejscach. Do wycieków lub kradzieży haseł dochodzi tak często, a liczba zagrożonych w ten sposób kont jest tak duża, że warto się zastanowić nad sposobem budowania i zmiany haseł.

ZAPAMIĘTAJ

Oto kilka przydatnych zaleceń:

- Hasło należy zmieniać maksymalnie co 30 dni, aby w razie wycieku nie zostało użyte do niecnych celów.
- Długość hasła powinna się mieścić w przedziale od 8 do 40 znaków.
- Warto użyć małych i wielkich liter, cyfr oraz znaków specjalnych. Nie zaleca się stosowania znaków narodowych (w języku polskim są to: ą, ć, ę, ł, ń, ó, ś, ź, ż).
- Hasło nie powinno się składać z wyrażeń słownikowych.
- Nie należy używać imion, nazwisk albo słów, które mogą się kojarzyć z użytkownikiem.
- Jest wskazane, aby hasło było różne od ośmiu wcześniejszych.

Zadania kontrolne

1. Utwórz w dowolny sposób konto *Superman*, ustal dla niego katalog domowy */home/superman* z hasłem *ZAQ!2wsx* i UID *1234* oraz dodaj go do grupy *root*.
2. Utwórz grupę *bohater* z GID *1234* i dodaj do niej użytkownika *Superman*.
3. Usuń konto użytkownika i grupę za pomocą terminala.

2.5. Serwer telnet

DEFINICJA

Telnet jest protokołem aplikacji używanym w sieci internet lub sieci lokalnej, który zapewnia dwukierunkową, interaktywną komunikację tekstową z wykorzystaniem połączenia wirtualnego terminala. Dane użytkownika są przeplatane w paśmie z informacjami sterującymi telnet za pośrednictwem protokołu kontroli transmisji (TCP).

Telnet to narzędzie do zarządzania systemami, które są wyposażone w serwer telnet i mogą być zarządzane za pomocą terminala. Jest szybkie, małe i dostępne w licznych komercyjnych i darmowych narzędziach. Wiele systemów ma już zaimplementowanego na stałe klienta telnet.

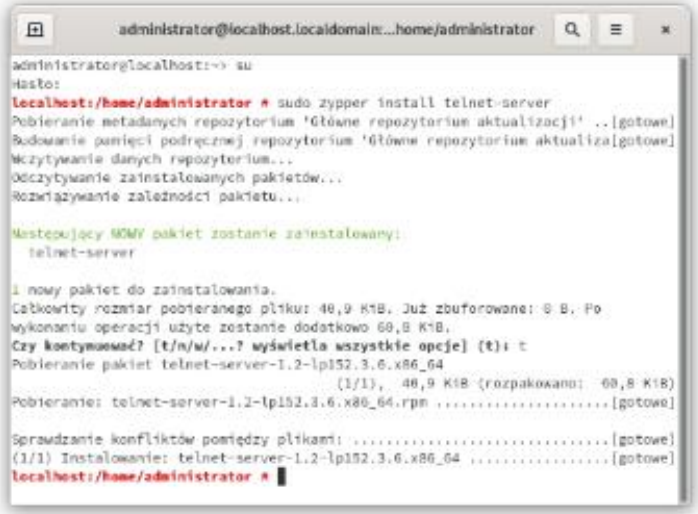
Wadą telnetu jest niezabezpieczone w żaden sposób połączenie, przez co łatwo jest podsłuchać dane wymieniane pomiędzy klientem a serwerem, łącznie z hasłem i loginem. Dlatego nie zaleca się korzystania z protokołu telnet.

Instalacja i uruchomienie serwera telnet

Spróbujmy uruchomić teraz serwer telnet na serwerze openSUSE. Narzędzie YaST nie obsługuje telnetu, dlatego zainstalujemy je z konsoli.

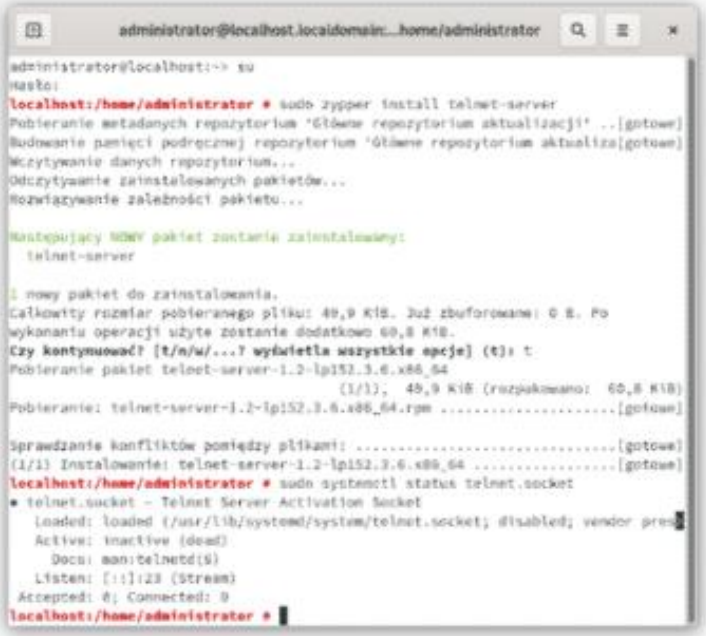
Ćwiczenie 2.4

1. Uruchamiamy *Terminal*, zmieniamy użytkownika na *root* poleceniem `su` i wpisujemy `sudo zypper install telnet-server`, co spowoduje zainstalowanie pakietu *telnet-server*. System poprosi o potwierdzenie, a następnie rozpocznie się instalacja (rysunek 2.23).



Rysunek 2.23. Instalacja serwera telnet za pomocą terminala

2. Teraz sprawdzimy z użyciem polecenia `sudo systemctl status telnet.socket`, czy nasz serwer działa. Jak widać na rysunku 2.24, proces jest nieaktywny.

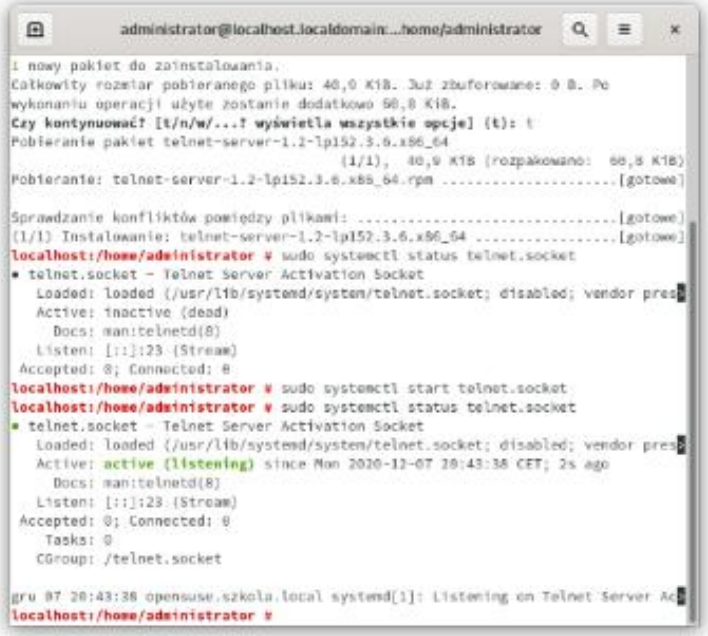


Rysunek 2.24. Sprawdzenie, czy proces telnet działa

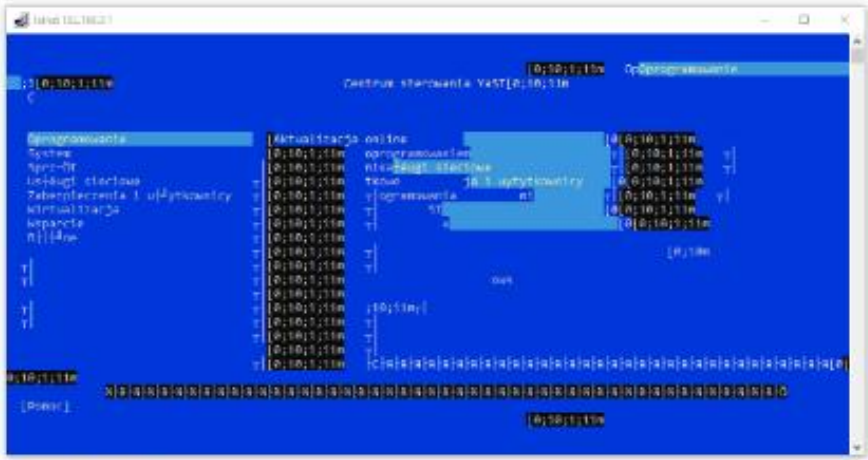
3. Uruchamiamy serwer poleceniem `sudo systemctl start telnet.socket` i ponownie sprawdzamy, czy serwer się uruchomił (rysunek 2.25). Widzimy, że serwer się uruchomił i nasłuchuje na porcie 23. Jeśli serwer telnet ma się uruchamiać za każdym razem po uruchomieniu systemu, musimy użyć polecenia `sudo systemctl enable telnet.socket`.
4. Za pomocą klienta próbujemy się połączyć z serwerem przez wpisanie `telnet 192.168.0.1`. Jeśli na komputerze z openSUSE klient jeszcze nie jest zainstalowany, instalujemy go poleceniem `sudo zypper install telnet`.
5. Podłączając się z systemu Windows, użyliśmy klienta telnet wbudowanego w system i uruchomiliśmy narzędzie YaST w wersji graficznej. Wbudowany klient telnet systemu Windows nie pozwala na prawidłową obsługę wszystkich elementów graficznego interfejsu tekstowego (rysunek 2.26).

Zadanie kontrolne

1. Wyszukaj w sieci internet informacje na temat wad i zalet protokołu telnet.



Rysunek 2.25. Uruchomienie procesu telnet i sprawdzenie jego statusu



Rysunek 2.26. Narzędzie YaST uruchomione za pomocą klienta telnet w systemie Windows 10

2.6. Serwer SSH

DEFINICJA

SSH (ang. *Secure Shell*) to kryptograficzny protokół do bezpiecznego świadczenia usług sieciowych. Pozwala zalogować się do systemu zdalnego i zarządzać nim za pomocą zdalnego wiersza poleceń. Zapewnia bezpieczny kanał w niezabezpieczonej sieci z wykorzystaniem architektury klient-serwer, przez połączenie aplikacji klienckiej SSH z serwerem SSH.

SSH jest następcą popularnego, ale niezabezpieczonego protokołu telnet, od którego się odchodzi.

Łączenie się z komputerem za pośrednictwem usługi SSH

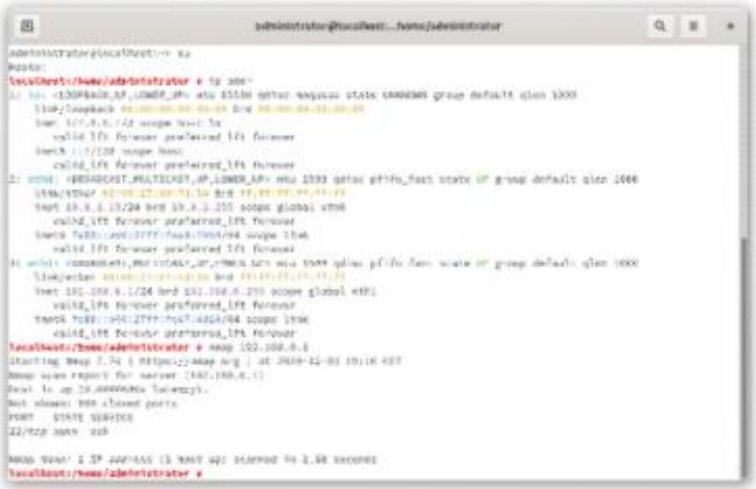
Podczas instalacji openSUSE zaznaczaliśmy opcję *Włącz usługę SSH*, dzięki czemu usługa serwera SSH już jest uruchomiona. W ćwiczeniu 2.5 pokażemy, jak się podłączyć do openSUSE z systemu Windows 10 na dwa sposoby:

- poprzez wbudowanego klienta SSH w Windows 10,
- poprzez darmowe oprogramowanie PuTTY.

Ćwiczenie 2.5

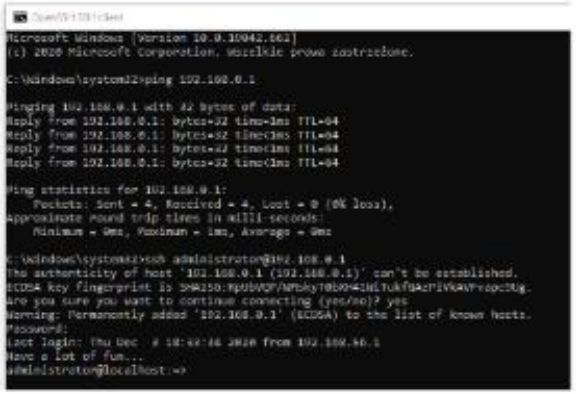
1. Uruchamiamy terminal i poleceniem `su` logujemy się jako *root*.
2. Sprawdzamy adresy IP poleceniem `ip addr` oraz upewniamy się, czy port usługi SSH dla adresu `192.168.0.1` jest otwarty, za pomocą polecenia `nmap 192.168.0.1` (rysunek 2.27).

Rysunek 2.27. Użycie poleceń ip addr oraz nmap



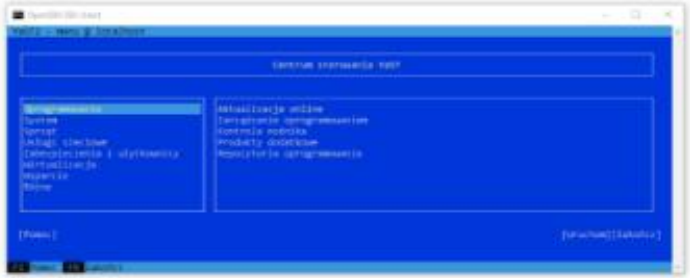
3. Port TCP 22 jest otwarty i dostępny dla usługi SSH.
4. W ustawieniach Oracle VirtualBox dla naszej maszyny zmieniamy sposób podłączenia karty sieciowej 2 na *Karta sieci izolowanej (host-only)*, dzięki czemu zostanie utworzony wspólny interfejs pomiędzy maszyną wirtualną a komputerem hosta.
5. W komputerze hosta wchodzimy w ustawienia sieciowe i zmieniamy adres IP dla *VirtualBox Host-Only Network* na `192.168.0.10/24`. Teraz mamy już ustanowione połączenie pomiędzy maszyną wirtualną a hostem.
6. Uruchamiamy na komputerze hosta wiersz poleceń (*cmd.exe*) i sprawdzamy poprawność komunikacji z maszyną wirtualną poleceniem `ping 192.168.0.1`.
7. Jeśli komunikacja przebiega poprawnie, uruchamiamy połączenie SSH poleceniem `ssh administrator@192.168.0.1` i potwierdzamy klucz szyfrujący przez wpisanie `yes`, a następnie wpisujemy hasło (rysunek 2.28).

Rysunek 2.28. Podłączenie do systemu openSUSE za pomocą klienta SSH wbudowanego w Windows 10



8. Przełączamy się na konto *root* poleceniem `su` i możemy dowolnie zarządzać serwerem z trybu tekstowego.
9. Aby skorzystać z narzędzia YaST, wystarczy wpisać polecenie `yast` (rysunek 2.29).

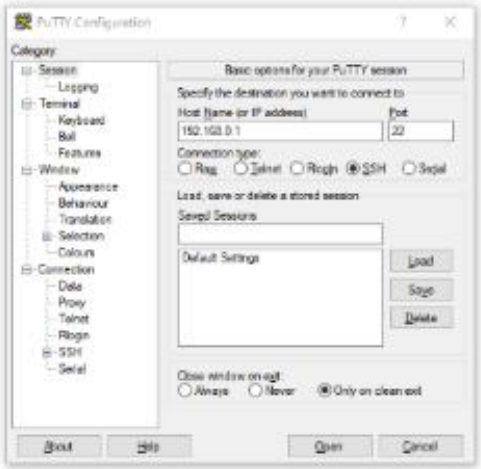
Rysunek 2.29. Oprogramowanie YaST uruchomione z klienta SSH w Windows 10



10. Aby zakończyć pracę z klientem SSH, wpisujemy `exit`. Zostaniemy wylogowani z konta z uprawnieniami *root*. Ponowne wpisanie `exit` zakończy połączenie z serwerem SSH.

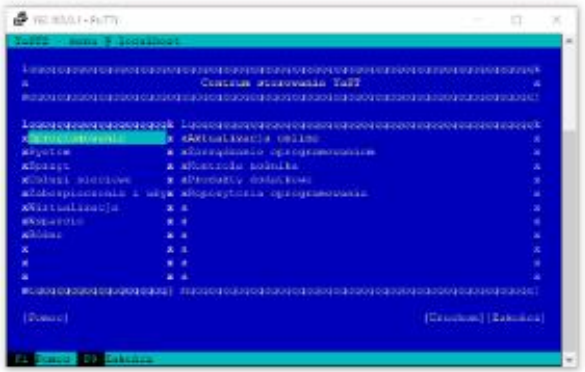
Ćwiczenie 2.6

1. Teraz pokażemy drugi sposób połączenia z serwerem SSH — za pomocą otwartoźródłowego programu PuTTY, który można pobrać ze strony domowej *www.putty.org*.
2. Polecenia 1. – 6. z ćwiczenia 2.5 można uznać za wykonane, uruchamiamy zatem program PuTTY i wprowadzamy dane do połączenia, jak na rysunku 2.30. Wpisujemy adres IP serwera SSH `192.168.0.1`, numer portu `22`, zaznaczamy typ połączenia i klikamy *Open*. Jak widać, PuTTY to bardzo uniwersalne narzędzie, które pozwoli nam skorzystać nie tylko z protokołu SSH, ale także z innych rodzajów połączeń.



Rysunek 2.30. Okno programu PuTTY gotowe do nawiązania połączenia

3. Przy pierwszym użyciu pojawi się informacja o kluczu szyfrującym, którą akceptujemy. Następnie zostajemy przeniesieni do ekranu terminala, gdzie logujemy się loginem i hasłem.
4. Po zalogowaniu mamy dostęp do wszystkich opcji terminala, łącznie z narzędziem YaST, którego okno jest pokazane na rysunku 2.31. Aby zakończyć sesję, wychodzimy z niej za pomocą polecenia `exit`.



Rysunek 2.31. Okno narzędzia YaST w programie PuTTY

Zadania kontrolne

1. Połącz się za pomocą SSH z openSUSE.
2. Utwórz użytkownika *jan.kowalski* z hasłem *ZAQ!2wsx* i przyznaj mu uprawnienia *root*.
3. Zaloguj się na nowo utworzonego użytkownika i sprawdź, co się wydarzy po wpisaniu polecenia `sudo shutdown -r now` oraz `sudo shutdown -h now`. Jaka jest różnica pomiędzy tymi poleceniami?

2.7. Serwer DHCP

DEFINICJA

DHCP (ang. *Dynamic Host Configuration Protocol*) to protokół zarządzania siecią wykorzystujący adresy IP. Serwer DHCP dynamicznie przypisuje adresy IP i inne parametry konfiguracji sieciowej do każdego urządzenia w sieci, dzięki czemu poszczególne urządzenia mogą się komunikować z innymi, które są do niej podłączone. W razie braku serwera DHCP urządzenie w sieci musi mieć statycznie przypisany adres IP, aby mogło w niej działać.

Serwer DHCP jest bardzo przydatny administratorom sieci, ponieważ zdecydowanie ułatwia im pracę. Dzięki niemu administrator nie musi konfigurować każdego urządzenia indywidualnie ani prowadzić własnej bazy przydzielanych adresów i w razie zmiany parametrów wykonuje konfigurację na serwerze, a wszystkie urządzenia w sieci widzą tę zmianę i ją stosują. Każde urządzenie, które ma interfejs sieciowy, bez względu na system operacyjny, może pracować w trybie klienta DHCP i dzięki temu uzyskiwać z serwera adres IP oraz inne parametry sieci, takie jak adresy bram domyślnych, serwerów DNS i serwerów czasu NTP.

Zasada działania serwera DHCP jest bardzo prosta. Administrator uruchamia go w sieci i konfiguruje jego obowiązkowe parametry, takie jak pula adresów, maska podsieci i czas dzierżawy, oraz liczne dodatkowe, takie jak brama domyślna i DNS, w zależności od potrzeb. Klient podłączony do sieci, w której działa serwer DHCP, wysyła na adres rozgłoszeniowy zapytanie o przydział adresu IP oraz innych skonfigurowanych danych. Serwer, odebrawszy takie zapytanie, sprawdza w swojej bazie, czy dany adres MAC urządzenia już w niej istnieje.

- Jeśli adres MAC urządzenia nie istnieje w bazie serwera DHCP, serwer przypisuje mu wszystkie parametry oraz najczęściej pierwszy wolny adres IP z puli adresów. Takie urządzenie jest dopisywane do bazy serwera DHCP.
- Jeśli adres MAC urządzenia istnieje w bazie serwera DHCP, to oznacza, że dane urządzenie już wcześniej podłączało się do sieci i ma aktywną dzierżawę adresu, dlatego serwer DHCP przypisuje mu przydzielony wcześniej adres IP.

Klient DHCP odbiera ustawienia od serwera i konfiguruje swój interfejs. Często się zdarza, że jakieś urządzenie w sieci wymaga od administratora niezmiennego adresu IP. Tak jest w przypadku serwerów, drukarek czy też komputerów, które pełnią określone funkcje w sieci. Wówczas administrator ma możliwość przypisania do interfejsu stałej dzierżawy adresu.

ZAPAMIĘTAJ

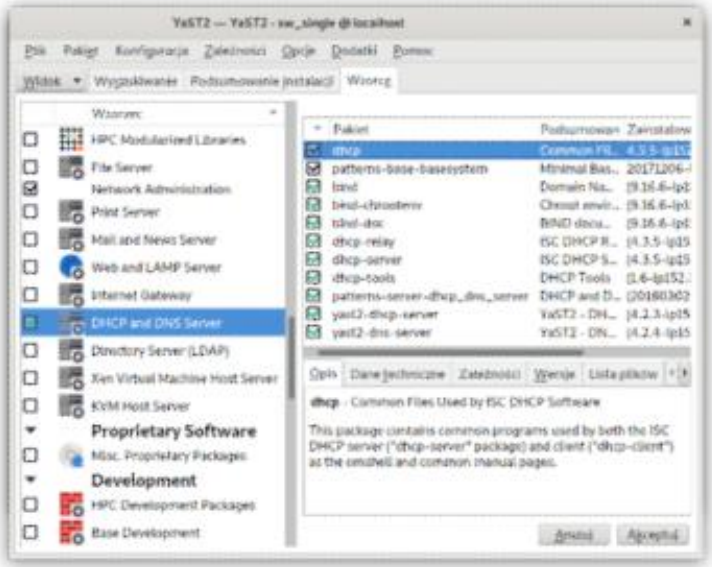
Serwer DHCP musi pracować na karcie sieciowej, która ma przypisany statyczny adres IP. Zarazem ten adres nie powinien się znajdować w puli adresów przydzielanych klientom.

Konfiguracja serwera DHCP

Działanie serwera DHCP przedstawimy w formie ćwiczenia.

Ćwiczenie 2.7

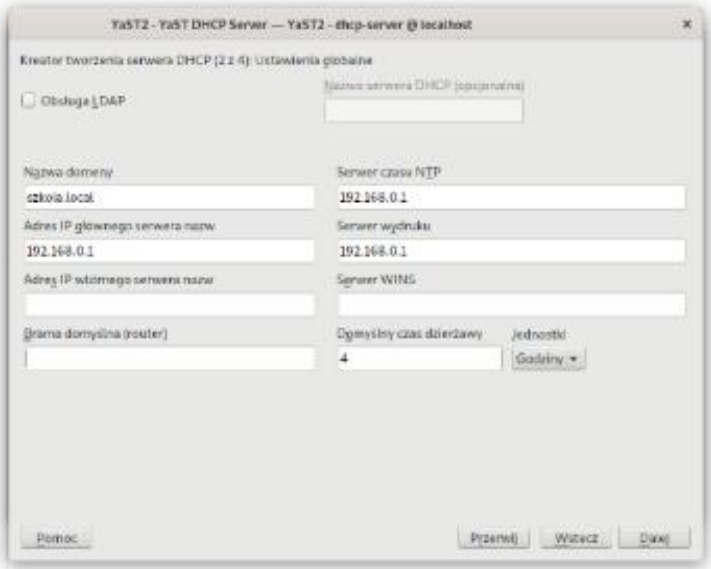
1. Aby rozpocząć pracę z serwerem DHCP, musimy go najpierw zainstalować. Uruchamiamy narzędzie YaST, a następnie przechodzimy do *Oprogramowanie/Zarządzanie oprogramowaniem*.
2. W menu *Widok* wybieramy *Wzorce*. Na karcie wzorców w grupie *Server Functions* zaznaczamy opcję *DHCP and DNS Server* i zatwierdzamy instalację przyciskiem *Akceptuj* (rysunek 2.32).



Rysunek 2.32. Instalacja wzorca DHCP and DNS Server w narzędziu YaST

3. W oknie *Pakiety zmienione – YaST2* wybieramy *Kontynuuj*. Na koniec klikamy *Zakończ*.
4. Zamykamy narzędzie YaST i uruchamiamy je ponownie, a następnie przechodzimy do *Usługi sieciowe/Serwer DHCP*.

5. Po uruchomieniu funkcji *Serwer DHCP* zaznaczamy kartę sieciową *eth1* ze skonfigurowanym adresem statycznym `192.168.0.1` i klikamy *Wybierz*, a następnie *Dalej*.
6. Konfigurujemy ustawienia globalne i klikamy *Dalej* (rysunek 2.33):
   - *Nazwa domeny* — określa domenę, dla której przydzielane będą adresy z serwera DHCP;
   - *Adres IP głównego serwera nazw* — określa adres serwera, który odpowiada za nazwy w sieci;
   - *Serwer czasu NTP* — określa adres serwera do synchronizacji czasu;
   - *Serwer wydruku* — określa adres serwera wydruku;
   - *Brama domyślna (router)* — określa adres interfejsu służącego do połączenia z internetem.

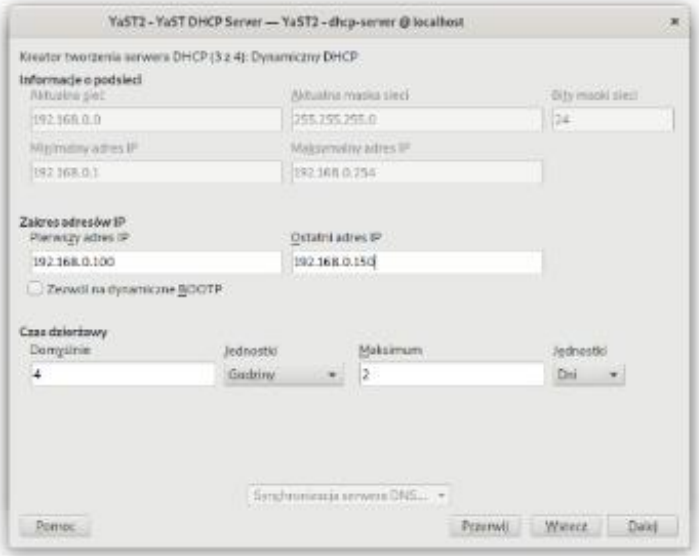


Rysunek 2.33. Ustawienia globalne serwera DHCP

7. Na rysunku 2.34 jest pokazana karta konfiguracji:
   - *Zakres adresów IP* — wprowadzamy początkowy i końcowy adres puli adresów DHCP;
   - *Czas dzierżawy* — określa czas, przez jaki adres IP będzie przypisany interfejsowi (adresowi MAC);
   - *Maksimum* (opcja niewymagana) — określa maksymalny czas zablokowania adresu dla interfejsu (po upływie tego czasu adres wróci do puli).

Dodatkowo na górze są wyświetlane informacje o podsieci, a wśród nich: adres sieci, maska podsieci oraz zakres adresów tej podsieci możliwych do wykorzystania.

Jeśli wszystko zostało skonfigurowane, klikamy *Dalej*.



Rysunek 2.34. Konfiguracja zakresu serwera DHCP

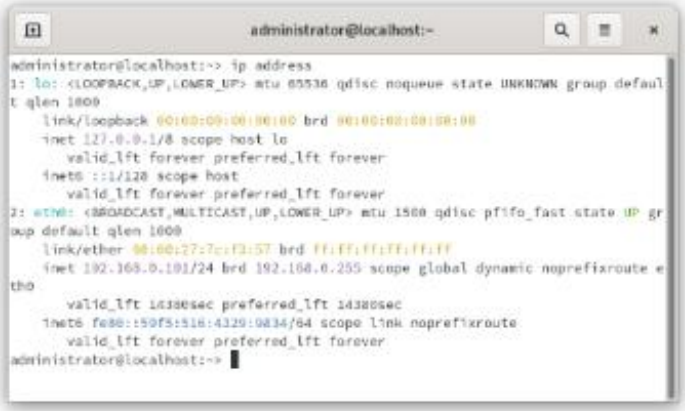
8. Następna karta kończy konfigurację serwera DHCP. Określamy na niej zachowanie serwera po jego skonfigurowaniu.
   - *Po zapisaniu konfiguracji* — określa, jak ma się zachować serwer po zapisaniu konfiguracji. Mamy do wyboru dwie opcje:
     - *Zachowaj bieżący stan* — pozostawia usługę nieuruchomioną;
     - *Uruchom* — uruchamia usługę natychmiast.
   - *Po ponownym rozruchu* — określa, jak ma się zachować serwer po ponownym uruchomieniu. Tu także mamy do wyboru dwie opcje:
     - *Nie uruchamiaj* — spowoduje, że serwer DHCP będzie uruchamiany na żądanie;
     - *Uruchom przy rozruchu* — spowoduje, że serwer DHCP będzie uruchamiany automatycznie.

   Zakładamy, że serwer DHCP ma działać przez cały czas już od momentu zapisania konfiguracji, i klikamy *Zakończ* (rysunek 2.35).

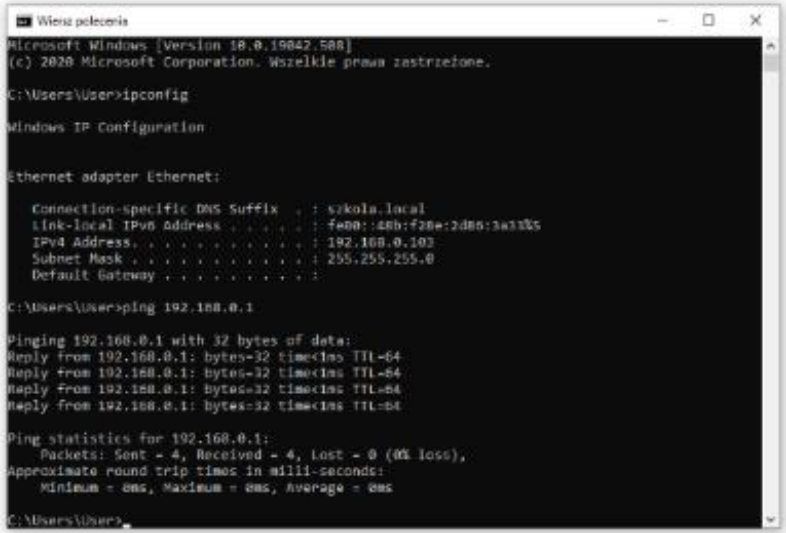


Rysunek 2.35. Końcowa konfiguracja serwera DHCP

9. Aby sprawdzić poprawność działania serwera DHCP, należy zastosować komputer kliencki z dowolnym systemem operacyjnym. My wykorzystaliśmy dwie maszyny — z systemem openSUSE oraz Windows 10.
10. Karty sieciowe w Oracle VirtualBox, za których pośrednictwem będzie się odbywała komunikacja, powinny być przestawione na sieć wewnętrzną.
11. Rysunek 2.36 pokazuje test przeprowadzony przy użyciu maszyny z systemem openSUSE, a rysunek 2.37 — z systemem Windows 10.



Rysunek 2.36. Adres IP na maszynie z openSUSE przypisany za pomocą serwera DHCP



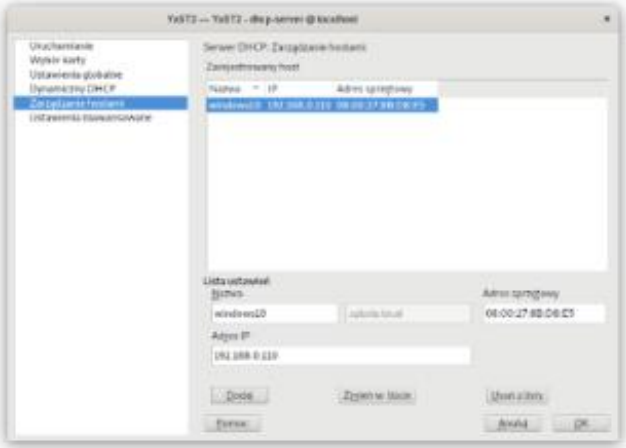
Rysunek 2.37. Adres IP na maszynie z Windows 10 przypisany za pomocą serwera DHCP

Przypisywanie stałej dzierżawy adresu IP

W poniższym ćwiczeniu pokażemy, jak przypisać stałą dzierżawę adresu IP do komputerów.

Ćwiczenie 2.8

1. Uruchamiamy narzędzie YaST, a następnie przechodzimy do *Usługi sieciowe/Serwer DHCP*.
2. Wybieramy kartę *Zarządzanie hostami* i uzupełniamy pola jak na rysunku 2.38:
   - *Nazwa* — nazwa, pod jaką będzie widoczny komputer;
   - *Adres sprzętowy* — adres MAC;
   - *Adres IP* — adres IP, który będzie przypisany do komputera.
3. Klikamy *Dodaj* i potwierdzamy *OK*.
4. Na rysunku 2.38 jest pokazany efekt zmiany w postaci adresu IP przypisanego do komputera o nazwie *windows10*.



Rysunek 2.38. Dodawanie stałej dzierżawy adresu do DHCP

Zadania kontrolne

1. Zmień adres karty sieciowej serwera na `172.16.20.100/16`.
2. Skonfiguruj serwer DHCP tak, aby pula adresów obejmowała całą sieć.
3. Zastrzeż adres `172.16.20.100/16` dla interfejsu serwera.
4. Podłącz dowolną maszynę do sieci i sprawdź, jaki otrzymała adres.
5. Zastrzeż adres `172.16.20.250/16` dla dowolnej maszyny podłączonej do sieci oraz sprawdź jej działanie.

2.8. Serwer DNS

DEFINICJA

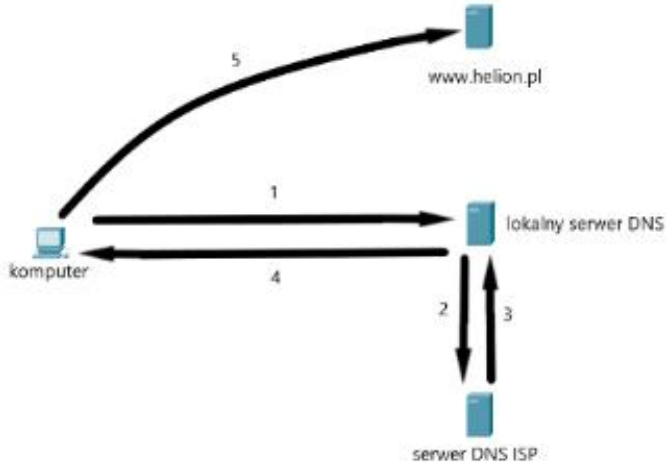
DNS (ang, *Domain Name System*) to hierarchiczny i zdecentralizowany system nazewnictwa komputerów, usług lub innych zasobów podłączonych do internetu lub sieci prywatnej. Łączy różne informacje z nazwami domen przypisanymi do każdego z uczestniczących podmiotów. Przede wszystkim tłumaczy łatwe do zapamiętania nazwy domen na adresy IP, potrzebne do lokalizowania oraz identyfikowania usług i urządzeń komputerowych za pomocą podstawowych protokołów sieciowych.

Gdyby trzeba było w jak najprostszy sposób wytłumaczyć zasadę działania usługi DNS lub porównać ją do czegoś oczywistego, naszym zdaniem najlepszym wyborem byłaby książka telefoniczna. Każdy z nas posiada telefon, w którym znajduje się taka książka. Spis kontak-

tów może mieć od kilku pozycji do nawet kilku tysięcy. Wyobraźmy sobie zatem, że musimy zapamiętać taką ogromną liczbę numerów. Jest to na pewno niewykonalne, za to możemy zapamiętać albo odszukać kontakt po nazwie. Tak samo jest w przypadku DNS — nie zapamiętamy niezliczonej liczby adresów IP, ale jesteśmy w stanie zapamiętać nazwę domeny lub możemy ją odszukać. Oczywiście DNS jest znacznie bardziej rozbudowaną bazą i nie sposób tutaj w pełni wytłumaczyć zasady jego działania, można tylko ją przybliżyć.

Szerzej zasadę działania DNS wyjaśnia rysunek 2.39. Na przykładzie tego schematu omówimy przepływ zapytań od użytkownika, który uruchamia stronę *www.helion.pl*.

1. Użytkownik wpisuje w swoją przeglądarkę adres *https://www.helion.pl*. Ponieważ sama przeglądarka nie zna ani nazwy strony, ani jej adresu, przepytuje lokalny plik *hosts*. Jeśli nie ma w nim ustawionego wpisu *www.helion.pl*, zaczyna odpytywać lokalny serwer DNS.
2. Jeśli po raz pierwszy próbujemy odwiedzić stronę *www.helion.pl*, nasz lokalny serwer DNS także nie zna informacji na temat tej domeny, dlatego przekazuje zapytanie do serwera DNS dostawcy internetu (ISP). Jeśli ten serwer zna adres, to w odpowiedzi przesyła adres IP `188.117.147.116`. Jeśli natomiast nie ma takiej informacji, wysyła zapytanie do serwera wyższego rzędu, którego poniższy schemat już nie obejmuje.
3. Lokalny serwer, znając powiązanie *www.helion.pl* z IP `188.117.147.116`, wprowadza taki wpis na swoim serwerze, dzięki czemu następne wywołanie strony przez klienta będzie już szybsze.
4. Lokalny serwer DNS zwraca odpowiedź na żądanie do komputera klienta.
5. Klient łączy się z adresem IP `188.117.147.116`, aby wyświetlić stronę *www.helion.pl*.



Rysunek 2.39. Zasada działania usługi DNS

Każdy serwer DNS składa się z dwóch stref:

- *strefa wyszukiwania do przodu* — umożliwia rozwiązywanie nazw mnemonicznych na adresy IP;
- *strefa wyszukiwania wstecz* — umożliwia rozwiązywanie adresów IP na nazwy mnemoniczne.

Powszechnie używane są następujące rekordy DNS:

- **A** (ang. *Address IPv4*) — mapuje nazwy hostów na adresy IPv4;
- **AAAA** (ang. *Address IPv6*) — mapuje nazwę hosta na adres IPv6;
- **PTR** (ang. *Pointer*) — tworzy powiązanie adresu IP z nazwą hosta w strefie wyszukiwania wstecz;
- **MX** (ang. *Mail Exchanger*) — identyfikuje serwer poczty w domenie;
- **CNAME** (ang. *Canonical Name*) — tworzy alias dla nazwy hosta (jest używany z istniejącymi rekordami A);
- **NS** (ang. *Name Server*) — określa serwer nazw dla domeny;
- **SOA** (ang. *Start of Authority*) — pierwszy rekord w pliku strefy, definiujący ogólne właściwości strefy dla serwera nazw.

Serwer DNS może być **serwerem głównym** (ang. *primary name server*) lub **serwerem pomocniczym** (ang. *secondary name server*). Podstawowym serwerem strefy jest serwer przechowujący ostateczne wersje wszystkich rekordów w tej strefie. Jest on identyfikowany w rekordzie SOA. Serwer pomocniczy dla strefy używa mechanizmu automatycznej aktualizacji, aby przechowywać aktualną kopię bazy danych podstawowego serwera dla strefy. Przykładami takich mechanizmów są transfery stref DNS i protokoły przesyłania plików. DNS zapewnia mechanizm, za pomocą którego podstawowa strefa może powiadamiać wszystkie znane pomocnicze usługi dla tej strefy, gdy zawartość strefy się zmienia. Zawartość strefy jest konfigurowana ręcznie przez administratora lub zarządzana za pomocą dynamicznego DNS.

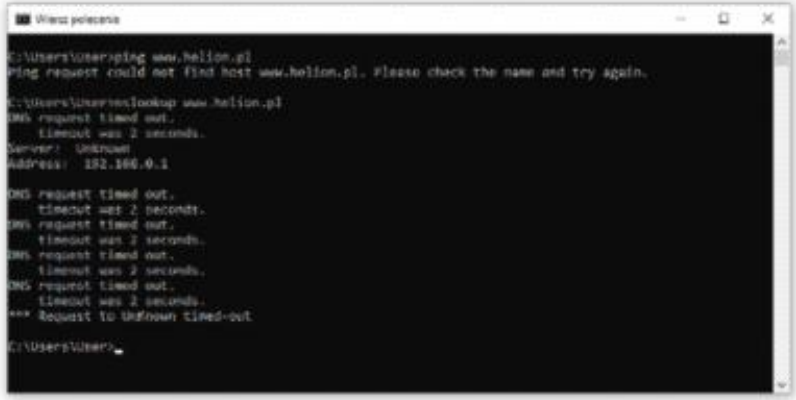
Serwery nazw pamięci podręcznej (ang. *caching name server*) przechowują wyniki zapytań DNS przez czas (ang. *time-to-live*) określony w konfiguracji każdego rekordu nazwy domeny. Pamięć podręczna DNS zwiększa wydajność DNS w ten sposób, że zmniejsza ruch DNS w sieci internet oraz obciążenie autorytatywnych serwerów nazw, zwłaszcza głównych serwerów nazw. Ze względu na to, że może szybciej odpowiadać na pytania, zwiększa również wydajność aplikacji użytkowników końcowych korzystających z DNS.

Konfiguracja serwera DNS

Ćwiczenie 2.9

1. Zanim zaczniemy ćwiczenie, sprawdzimy, czy maszyna z systemem Windows 10 podłączona do naszego serwera z openSUSE może rozpoznawać nazwy DNS. Aby to zrobić, wykonujemy polecenia `ping www.helion.pl` oraz `nslookup www.helion.pl`. Jak widać

na rysunku 2.40, polecenia nie rozpoznają domeny i nie znają adresu IP hosta. Mamy pewność, że serwer DNS nie działa.



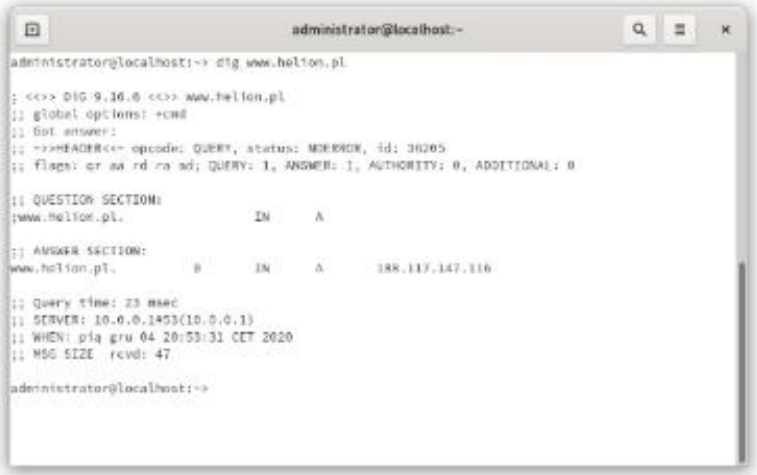
Rysunek 2.40. Sprawdzenie działania serwera DNS

2. To samo sprawdzimy na serwerze przy użyciu polecenia `dig www.helion.pl` (rysunek 2.41). Widzimy, że polecenie wczytało informacje o domenie, ale z wykorzystaniem serwera DNS `10.0.0.1`, czyli lokalnego routera, ponieważ maszyna ma dostęp do internetu.

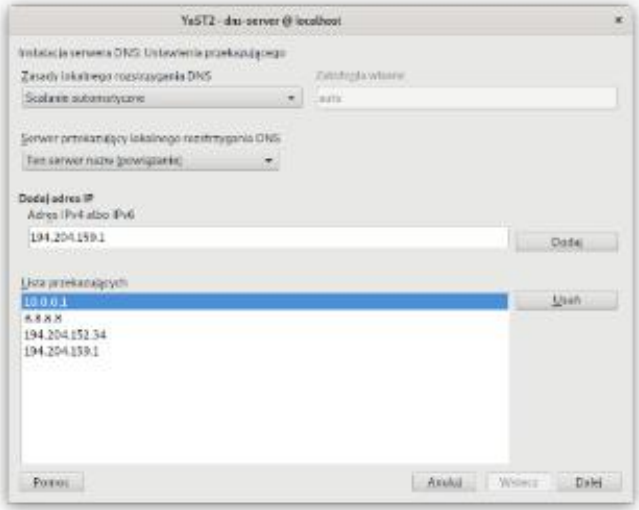
   Polecenie `dig` jest narzędziem podobnym do `nslookup`, powszechnie stosowanym w systemach Linux oraz Windows, o którym obszerniej powiemy w rozdziale 3. W tym miejscu wymienimy kilka jego przełączników:

   - `dig` — wyświetli adresy głównych serwerów DNS (*root-servers*) dla naszej lokalizacji;
   - `dig -h` — wyświetli wszystkie możliwe opcje;
   - `dig www.helion.pl. +trace` — odpyta wszystkie serwery w dół hierarchii, aż dojdzie do serwera obsługującego domenę *www.helion.pl*;
   - `dig -x 188.117.147.116` — zamieni adres IP na domenę.

3. Możemy przystąpić do konfigurowania serwera DNS. Serwer ten został przez nas zainstalowany przy okazji instalacji serwera DHCP (ćwiczenie 2.7).
4. Uruchamiamy narzędzie YaST i przechodzimy do *Usługi sieciowe/Serwer DNS*.
5. Na pierwszej karcie, *Instalacja serwera DNS: Ustawienia przekazującego*, dodajemy adresy DNS, np. dostawcy internetu, co pozwoli w razie niemożności rozwiązania nazwy odpytać inne serwery. Dobrze jest wpisać adresy kilku serwerów, aby przyspieszyć działanie usługi DNS. Ja użyłem serwera lokalnego oraz trzech serwerów globalnych. Po dodaniu adresów klikamy *Dalej* (rysunek 2.42).



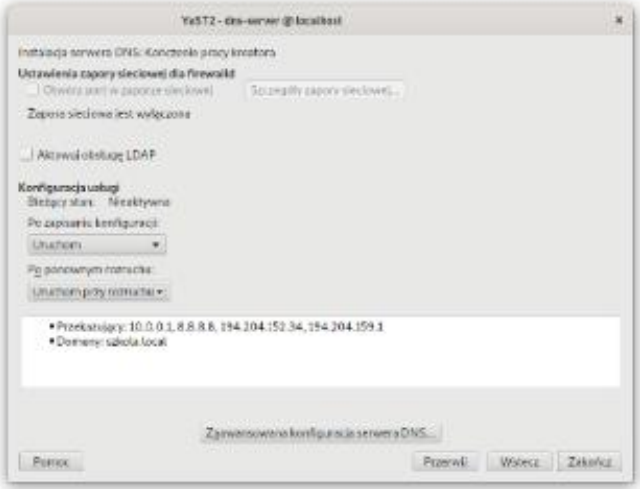
Rysunek 2.41. Sprawdzenie informacji o domenie poleceniem dig



Rysunek 2.42. Konfiguracja serwerów przekazujących

6. Na karcie *Instalacja serwera DNS: Strefy DNS* dodajemy strefę główną: wpisujemy `szkola.local` i naciskamy *Dodaj*. Następnie naciskamy *Dalej*.
7. Na ostatniej karcie, *Instalacja serwera DNS: Kończenie pracy kreatora*, zmieniamy ustawienia (rysunek 2.43):
   - *Po zapisaniu konfiguracji — Uruchom*,
   - *Po ponownym rozruchu — Uruchom przy rozruchu*.

Dzięki temu po zapisaniu konfiguracji serwer DNS zacznie natychmiast działać, a po ponownym uruchomieniu komputera włączy się automatycznie. Na koniec klikamy *Zakończ*.

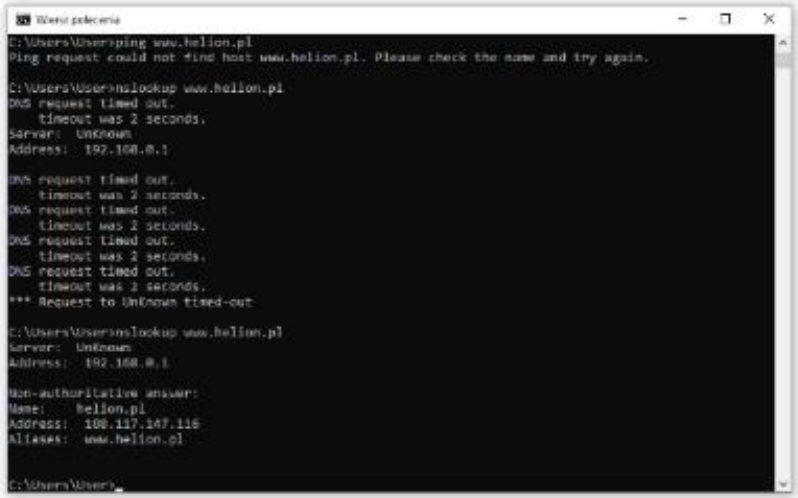


Rysunek 2.43. Podsumowanie instalacji serwera DNS

8. Teraz sprawdzimy, czy funkcja przekazywania działa na serwerze właściwie. Potrzeba na to 2 – 3 minut. Zaczynamy od serwera openSUSE, na którym używamy polecenia `dig www.helion.pl`. Jak widać na rysunku 2.44, otrzymaliśmy informacje o domenie, ale tym razem od nowo uruchomionego serwera DNS oznaczonego jako 127.0.0.1 (localhost).
9. Pora sprawdzić działanie serwera DNS na komputerze klienta z systemem Windows 10. Użyjemy do tego polecenia `nslookup www.helion.pl`. Jak widać na rysunku 2.45, także tu serwer DNS działa i pozwala odczytać informacje na temat domeny.



Rysunek 2.44. Sprawdzenie poprawności działania serwera DNS za pomocą polecenia dig



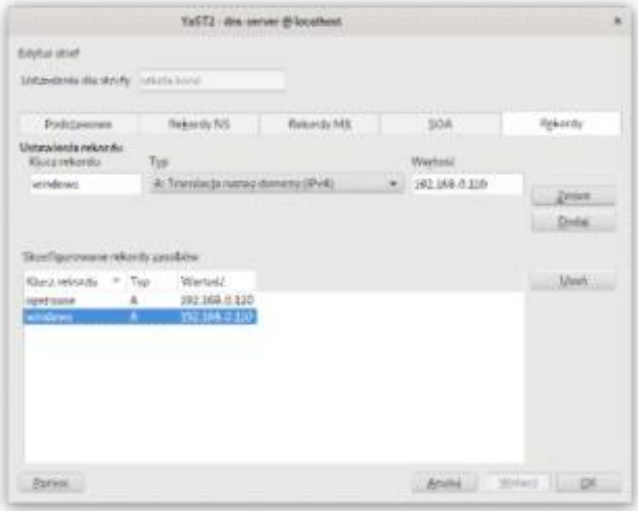
Rysunek 2.45. Sprawdzenie działania serwera DNS za pomocą polecenia nslookup

Dodawanie rekordów do serwera DNS

Ćwiczenie 2.10

Teraz spróbujmy dopisać nazwy komputerów do adresów IP w serwerze DNS.

1. Uruchamiamy narzędzie YaST i przechodzimy do *Usługi sieciowe/Serwer DNS*.
2. Przechodzimy do karty *Strefy DNS*, zaznaczamy domenę *szkola.local* i klikamy *Edytuj*.
3. Wybieramy kartę *Rekordy* i dodajemy wartości jak na rysunku 2.46:
   - *Klucz rekordu* — wprowadzamy nazwę komputera;
   - *Typ* — wybieramy typ A, który odpowiada za mapowanie nazwy na adres IP;
   - *Wartość* — wpisujemy adres IP, na który ma kierować nazwa.



Rysunek 2.46. Dodawanie rekordów A do strefy wyszukiwania do przodu

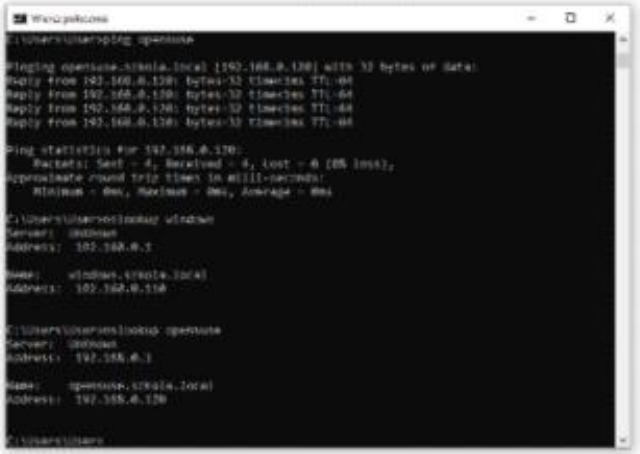
4. Zatwierdzamy przyciskiem *OK* i możemy przystąpić do sprawdzania, czy wpisy istnieją w systemie, zarówno przy użyciu polecenia `dig` (tu: `dig windows.szkola.local`, patrz rysunek 2.47), jak też `nslookup` (tu: `nslookup windows` oraz `nslookup opensuse`, patrz rysunek 2.48).

ZAPAMIĘTAJ

Wyszukiwanie wsteczne ma to do siebie, że adresy podaje odwrotnie, dodając na końcu `in-addr.arpa`, np. adres `192.168.0.100` w strefie wyszukiwania wstecznego będzie zapisany jako `100.0.168.192.in-addr.arpa`.



Rysunek 2.47. Sprawdzenie informacji na temat hostów za pomocą polecenia dig



Rysunek 2.48. Sprawdzenie informacji na temat hostów za pomocą polecenia nslookup

Konfiguracja strefy wyszukiwania wstecz

Spróbujmy teraz skonfigurować strefę wyszukiwania wstecz, czyli odwzorowanie adresu IP na nazwę.

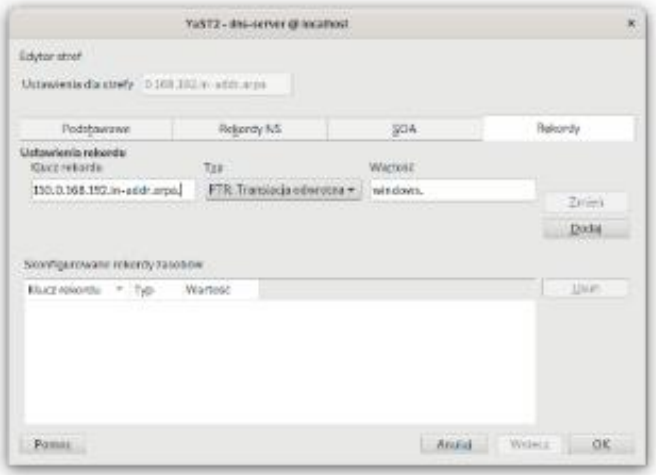
Ćwiczenie 2.11

1. Uruchamiamy narzędzie YaST i przechodzimy do *Usługi sieciowe/Serwer DNS*.
2. Przechodzimy do karty *Strefy DNS* i wpisujemy w polu *Nazwa* `0.168.192.in-addr.arpa`, a następnie klikamy *Dodaj* i *OK*.
3. Ponownie otwieramy *Usługi sieciowe/Serwer DNS* i kartę *Strefy DNS*. Zaznaczamy domenę *0.168.192.in-addr.arpa* i klikamy *Edytuj*.
4. Możemy na karcie *Podstawowe* zaznaczyć *Automatyczne generowanie rekordów z* dla strefy *szkola.local*, a wtedy system sam utworzy rekordy wstecznego wyszukiwania dla wszystkich wpisów z tej strefy (rysunek 2.49). W przeciwnym razie przechodzimy do zakładki *Rekordy*.

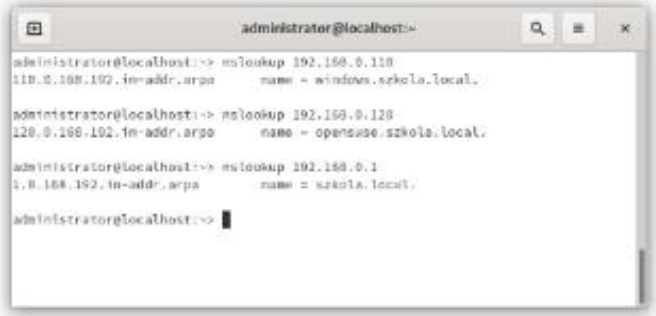


Rysunek 2.49. Edytor strefy wyszukiwania wstecz

5. Jeśli opcja *Automatyczne generowanie rekordów z* nie została zaznaczona, trzeba wszystkie rekordy dodać ręcznie, jak na rysunku 2.50.
6. Na zakończenie sprawdzamy konfigurację przez wykonanie polecenia `nslookup 192.168.0.110` na serwerze (rysunek 2.51), który potwierdza działanie strefy wyszukiwania wstecz.



Rysunek 2.50. Dopisanie hosta w strefie wyszukiwania wstecz



Rysunek 2.51. Potwierdzenie działania strefy wyszukiwania wstecz serwera DNS

Zadania kontrolne

1. Usuń wszystkie istniejące strefy w serwerze DNS.
2. Utwórz i skonfiguruj strefę wyszukiwania do przodu dla pięciu komputerów, gdzie nazwami będą marki samochodów.
3. Skonfiguruj strefę wyszukiwania wstecz, przy czym wszystkie rekordy dodaj ręcznie.
4. Wymień różnicę pomiędzy strefami wyszukiwania.

2.9. Serwer FTP

DEFINICJA

FTP (ang. *File Transfer Protocol*) to standardowy protokół sieciowy używany do przesyłania plików komputerowych między klientem a serwerem w sieci komputerowej. Jest zbudowany w architekturze klient-serwer i wykorzystuje oddzielne połączenia do sterowania oraz do przesyłania danych pomiędzy klientem a serwerem.

Użytkownicy FTP mogą się uwierzytelniać za pomocą protokołu logowania opartego na zwykłym tekście, z reguły w postaci nazwy użytkownika i hasła, ale mogą też łączyć się anonimowo, jeśli konfiguracja serwera na to pozwala. Aby transmisja była bezpieczna — chroniła nazwę użytkownika i hasło oraz szyfrowała zawartość — FTP jest często zabezpieczone przy użyciu SSL/TLS (**FTPS**) lub zastępowane protokołem **SFTP** (ang. *SSH File Transfer Protocol*).

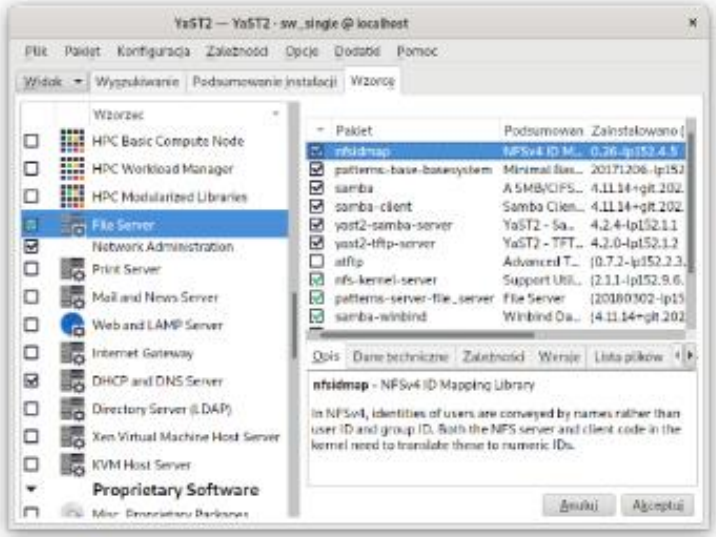
Pierwsze aplikacje klienckie FTP były programami wiersza poleceń opracowanymi, zanim systemy operacyjne miały graficzny interfejs użytkownika. Nadal są dostarczane z większością systemów operacyjnych. Od tamtego czasu opracowano wiele klientów FTP i narzędzi do automatyzacji przeznaczonych do komputerów stacjonarnych, serwerów, urządzeń przenośnych i innego sprzętu, np. skanerów sieciowych, a protokół FTP został włączony do aplikacji zwiększających wydajność pracy, takich jak edytory HTML.

Instalacja serwera FTP

Teraz zobaczymy, jak uruchomić serwer FTP na serwerze openSUSE. Najpierw musimy go zainstalować.

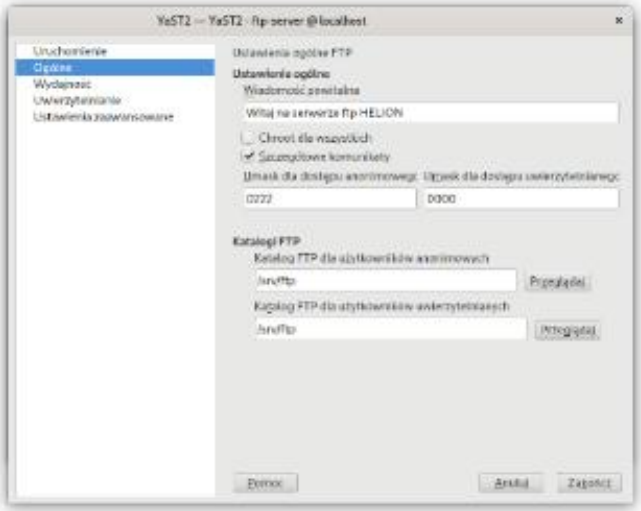
Ćwiczenie 2.12

1. Przechodzimy do narzędzia YaST, a następnie uruchamiamy *Oprogramowanie/Zarządzanie oprogramowaniem*.
2. W menu *Widok* wybieramy *Wzorce*. W nowo otwartej karcie *Wzorce*, w grupie *Server Functions*, zaznaczamy pozycję *File Server* i potwierdzamy instalację przyciskiem *Akceptuj* (rysunek 2.52).
3. Na karcie *Zmiany automatyczne* klikamy *Kontynuuj*, czekamy, aż usługa zostanie zainstalowana, i klikamy *Zakończ*.
4. Następnie ponownie uruchamiamy narzędzie YaST, przechodzimy do *Usługi sieciowe/Serwer FTP* i na pierwszej karcie, *Uruchomienie*, ustawiamy:
   - *Po zapisaniu konfiguracji* — *Uruchom*,
   - *Po ponownym rozruchu* — *Uruchom przy rozruchu*.



Rysunek 2.52. Instalacja usługi File Server

5. Na karcie *Ogólne* ustawiamy (rysunek 2.53):
   - *Wiadomość powitalna* — wiadomość, która będzie wyświetlana w momencie podłączenia do serwera;
   - *Chroot dla wszystkich* — jeśli opcja będzie włączona, wszyscy użytkownicy będą domyślnie umieszczani w środowisku chroot, w ich katalogach domowych (ta opcja dotyczy bezpieczeństwa, dzięki czemu użytkownicy nie będą mieli możliwości podejrzenia plików spoza swoich katalogów domowych);
   - *Szczegółowe komunikaty* — po włączeniu tej opcji wszystkie żądania i odpowiedzi FTP będą zapisywane w dzienniku;
   - *Umask dla dostępu anonimowego* — wybieramy `0222` (wszyscy mogą odczytywać i wykonywać, ale nie mogą zapisywać);
   - *Umask dla dostępu uwierzytelnianego* — wybieramy `0000` (wszyscy mogą odczytywać, zapisywać i wykonywać);
   - *Katalog FTP dla użytkowników anonimowych* — pozwala określić katalog dla użytkowników anonimowych;
   - *Katalog FTP dla użytkowników uwierzytelnianych* — pozwala określić katalog dla użytkowników uwierzytelnianych.

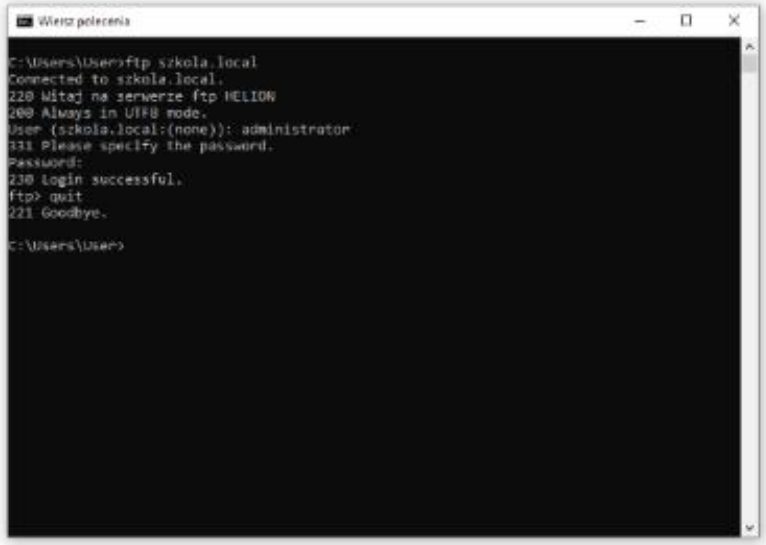


Rysunek 2.53. Konfiguracja serwera FTP — karta Ogólne

6. Na karcie *Wydajność* pozostawiamy ustawienia bez zmian:
   - *Maksymalny czas bezczynności w minutach* (15) — maksymalny czas, jaki może upłynąć pomiędzy poleceniami zdalnego klienta (po takim czasie bezczynności serwer rozłączy sesję);
   - *Maksymalna liczba klientów z jednego IP* (3) — liczba klientów z jednego adresu IP, które mogą się podłączyć w jednym czasie;
   - *Maksymalna liczba klientów* — liczba klientów, które mogą się podłączyć w jednym czasie;
   - *Maksymalny transfer lokalny [KB/s]* — maksymalna prędkość transferu dozwolona dla lokalnie uwierzytelnionych użytkowników;
   - *Maksymalny transfer anonimowy [KB/s]* — maksymalna prędkość transferu dozwolona dla anonimowych użytkowników.
7. Na karcie *Uwierzytelnianie* znajdują się następujące opcje:
   - *Wł./Wył. użytkownika anonimowego lub lokalnego*:
     - *Tylko dla anonimowych* — dostęp do serwera FTP tylko dla użytkowników anonimowych;
     - *Tylko dla uwierzytelnianych* — dostęp do serwera FTP tylko dla użytkowników uwierzytelnionych;
     - *Dla wszystkich* — dostęp do serwera FTP dla wszystkich użytkowników.

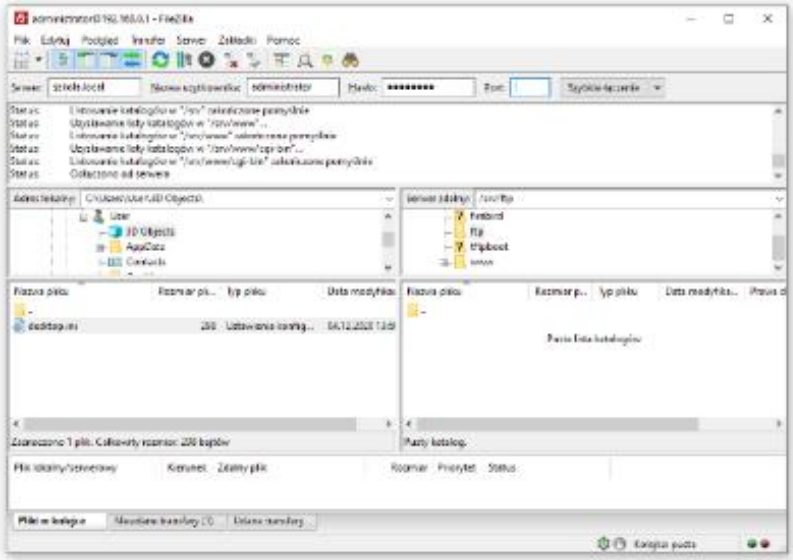
   - *Włącz przesyłanie*:
     - *Użytkownicy anonimowi mogą przesyłać* — określa, czy użytkownicy anonimowi mogą przesyłać dane na serwer — jeśli opcja zostanie zaznaczona, będzie trzeba pamiętać o przygotowaniu katalogu z prawami zapisu w katalogu domowym;
     - *Anonimowi mogą tworzyć katalogi* — określa, czy użytkownicy anonimowi mogą tworzyć katalogi na serwerze — jeśli opcja zostanie zaznaczona, będzie trzeba pamiętać o przygotowaniu katalogu z prawami zapisu w katalogu domowym.
8. Ostatnia karta, *Ustawienia zaawansowane*, pozwala zmienić porty trybu pasywnego, a także włączyć SSL (to wymaga certyfikatu dla połączeń szyfrowanych SSL).
9. Na koniec klikamy *Zakończ*.

Pora sprawdzić działanie serwera FTP. Na początek spróbujemy się z nim połączyć za pomocą konsoli (*cmd.exe*) z systemu Windows 10 (rysunek 2.54). Jak widać na rysunku, można się zalogować oraz działają komunikaty.



Rysunek 2.54. Podłączenie do serwera FTP poprzez cmd.exe

Następny test wykonamy za pomocą programu FileZilla (*https://filezilla-project.org*). Jak pokazuje rysunek 2.55, udało nam się podłączyć do serwera FTP.



Rysunek 2.55. Podłączenie do serwera FTP za pomocą programu FileZilla

Zadania kontrolne

1. Uruchom dostęp do serwera FTP tylko dla użytkowników anonimowych.
2. Skonfiguruj serwer FTP w taki sposób, aby użytkownicy anonimowi mogli zapisywać pliki.
3. Skonfiguruj uprawnienia *umask* tak, aby użytkownik uwierzytelniony mógł tylko odczytywać zawartość serwera.

2.10. Serwer WWW oraz uruchomienie strony internetowej

DEFINICJA

Serwer WWW (ang. *web server*) — oprogramowanie działające na serwerze, które obsługuje żądania protokołów komunikacyjnych HTTP i HTTPS. Przeglądarka internetowa, będąca klientem serwera WWW, łączy się z nim, aby pobrać wskazaną stronę WWW.

DEFINICJA

WWW (ang. *World Wide Web*) — ogólnoświatowa rozległa sieć komputerowa to hipertekstowy, multimedialny, internetowy system informacyjny oparty na publicznie dostępnych, otwartych standardach IETF (ang. *Internet Engineering Task Force*) i W3C (ang. *World Wide Web Consortium*). WWW jest usługą internetową, która ze względu na popularność bywa błędnie utożsamiana z całym internetem, szczególnie przez początkujących użytkowników komputera.

Najpopularniejszymi serwerami według danych z kwietnia 2020 r., opublikowanych przez serwis Netcraft, są:

- **nginx** — oprogramowanie serwera WWW dla systemów FreeBSD, Linux i Solaris,
- **Apache** — oprogramowanie serwera WWW instalowane w systemach serwerowych opartych na systemie Linux,
- **IIS** (ang. *Internet Information Services*) — oprogramowanie serwera WWW dla systemów z rodziny Windows Server.

Komunikacja pomiędzy klientem a serwerem odbywa się z wykorzystaniem następujących protokołów:

- **HTTP** (ang. *Hypertext Transfer Protocol*) — protokół przesyłania hipertekstu działający w warstwie aplikacji modelu ISO/OSI. Jest podstawą przesyłania danych w sieci WWW. Dokumenty hipertekstowe zawierają hiperłącza do innych zasobów, do których użytkownik ma łatwy dostęp, np. przez kliknięcie myszą lub dotknięcie ekranu w przeglądarce internetowej. W standardowej konfiguracji HTTP działa na porcie 80.
- **HTTPS** (ang. *Hypertext Transfer Protocol Secure*) — rozszerzenie protokołu HTTP. Służy do bezpiecznej komunikacji w sieci komputerowej i jest szeroko stosowany w internecie. W HTTPS protokół komunikacyjny jest szyfrowany przy użyciu **TLS** (ang. *Transport Layer Security*), a wcześniej **SSL** (ang. *Secure Sockets Layer*). Głównymi zaletami są uwierzytelnianie odwiedzanej strony internetowej oraz ochrona prywatności i integralności danych podczas przesyłania. HTTPS chroni przed atakami typu man-in-the-middle, a dwukierunkowe szyfrowanie komunikacji między klientem a serwerem chroni komunikację przed podsłuchaniem i zmianą zawartości. W praktyce daje to użytkownikowi wystarczającą pewność, że komunikuje się z właściwą stroną internetową bez ingerencji z zewnątrz. W standardowej konfiguracji HTTPS działa na porcie 443.

Określenia „World Wide Web" i „internet" często są zamiennie stosowane w życiu codziennym. W rzeczywistości WWW i internet nie są tym samym. Internet jest globalnym systemem połączonych ze sobą sieci komputerowych, a WWW to jedna z usług działających w internecie.

Instalacja serwera WWW

Serwer WWW jest prosty w instalacji. Instaluje się go w taki sam sposób jak inne usługi.

Przechodzimy do narzędzia YaST, a następnie uruchamiamy *Oprogramowanie/Zarządzanie oprogramowaniem* i w menu *Widok* wybieramy *Wzorce*. Na karcie *Wzorce* z grupy *Server Functions* zaznaczamy opcję *Web and LAMP Server* i potwierdzamy instalację przyciskiem *Akceptuj*, a w nowo otwartej karcie *Zmiany automatyczne* naciskamy *Kontynuuj*.

Dodatkowo, aby móc konfigurować serwer HTTP za pomocą narzędzia YaST, musimy doinstalować moduł do jego obsługi. Ponownie uruchamiamy w narzędziu YaST *Oprogramowanie/Zarządzanie oprogramowaniem* i w oknie wyszukiwania wpisujemy `yast2-http-server`, zaznaczamy wyświetlony w prawej części okna pakiet o tej nazwie i naciskamy *Akceptuj*.

Drugi sposób instalacji serwera WWW to uruchomienie terminala i wpisanie w nim `sudo zypper install apache2`.

Serwer WWW można obsługiwać za pomocą narzędzia YaST lub terminala.

Aby uruchomić serwer, wpisujemy polecenie `sudo service apache2 start`. Sprawdzamy poleceniem `nmap 192.168.0.1`, czy serwer działa i czy otwarty jest port 80 dla protokołu HTTP (rysunek 2.56).



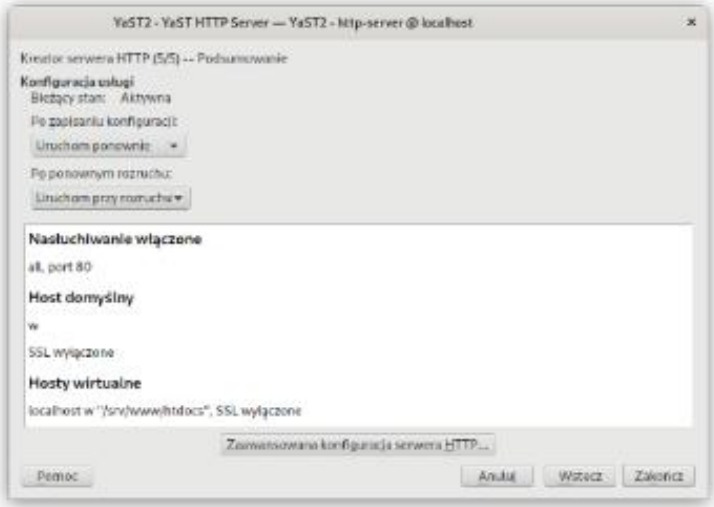
Rysunek 2.56. Uruchomienie usługi serwera WWW Apache

Aby zatrzymać serwer, używamy polecenia `sudo service apache2 stop`, aby zaś uruchomić go ponownie, wpisujemy `sudo service apache2 restart`.

Ćwiczenie 2.13

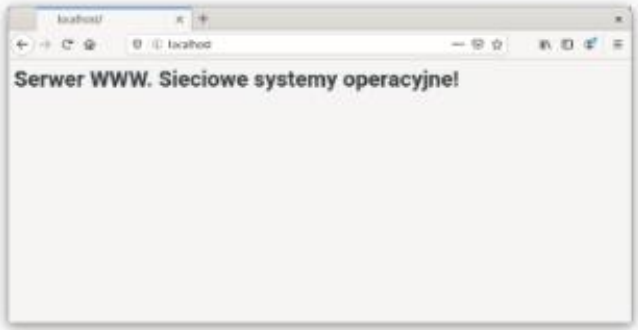
Skonfigurujemy funkcję *Serwer HTTP* za pomocą oprogramowania YaST.

1. Uruchamiamy narzędzie YaST, a następnie przechodzimy do *Usługi sieciowe/Serwer HTTP*. Uruchomi się kreator konfiguracji.
2. Na karcie *Kreator serwera HTTP (1/5) -- Wybór urządzeń sieciowych* konfigurujemy następujące ustawienia:
   - *Port* — wpisujemy port, na którym nasłuchiwał będzie Apache. W standardowej konfiguracji jest to port `80` protokołu HTTP.
   - *Nasłuchuj na interfejsach* — zaznaczamy, na których interfejsach sieciowych Apache będzie nasłuchiwał. Domyślnie zaznaczony jest port 80 w sieci lokalnej (`192.168.0.1`) oraz *localhost* (`127.0.0.1`).
3. Na karcie *Kreator serwera HTTP (2/5) -- Moduły* zaznaczamy, z jakich języków skryptowych będziemy korzystać. W domyślnej konfiguracji dostępne są trzy moduły: PHP, Perl i Python.
4. Na karcie *Kreator serwera HTTP (3/5) -- Host domyślny* pozostawiamy domyślne ustawienia hosta zaproponowane przez serwer.
5. Na karcie *Kreator serwera HTTP (4/5) -- Hosty wirtualne* na razie nic nie dodajemy — zrobimy to później.
6. Karta *Kreator serwera HTTP (5/5) -- Podsumowanie* zawiera przegląd wszystkich opcji. Aby zakończyć, klikamy *Zakończ* (rysunek 2.57).



Rysunek 2.57. Podsumowanie konfiguracji serwera HTTP

Zakończyliśmy konfigurację serwera HTTP. Poleceniem `gedit /srv/www/htdocs/index.html` przeprowadzimy edycję domyślnej strony WWW serwera Apache i w nagłówku *<h1>* zamiast domyślnego tekstu wpiszemy: `Serwer WWW. Sieciowe systemy operacyjne!`, a następnie zapiszemy stronę przyciskiem *Zapisz*. Teraz uruchomimy przeglądarkę, aby sprawdzić działanie strony. W tym celu wpisujemy w pasku adresu `localhost`. Powinniśmy uzyskać efekt jak na rysunku 2.58.



Rysunek 2.58. Uruchomienie domyślnej strony serwera Apache w przeglądarce

Aby uruchomić na fizycznym serwerze więcej niż jedną stronę WWW, można skorzystać z funkcji serwerów wirtualnych. Do wyboru mamy dwie możliwości:

- **wirtualne serwery rozróżniane po nazwie** — dla serwera używamy jednego adresu IP, a serwer odpowiada na zapytania o nazwę strony;
- **wirtualne serwery rozróżniane po adresie IP** — dla każdego serwera przypisuje się dodatkowy adres IP, który określa konkretną witrynę.

Te rozwiązania są wykorzystywane przez systemy hostingowe, które współdzielą poszczególne wirtualne serwery HTTP.

Ćwiczenie 2.14

Skonfigurujemy teraz wirtualny serwer rozróżniany po nazwie.

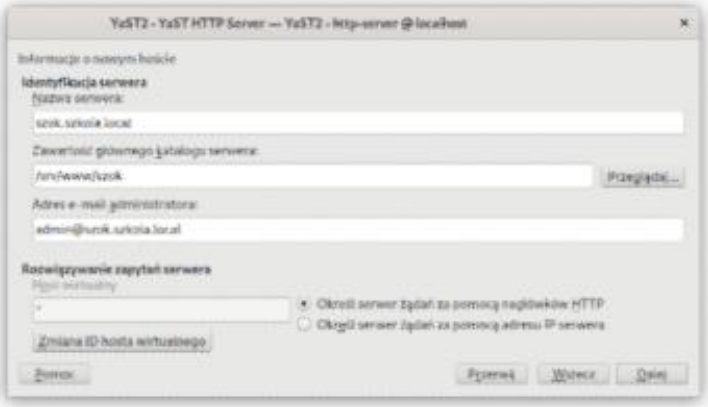
1. Tworzymy katalog, w którym przechowywana będzie zawartość strony. Użyjemy do tego polecenia wykonywanego w terminalu: `sudo mkdir /srv/www/szok`, zakładając, że wszystkie foldery stron WWW będziemy przechowywać w folderze */srv/www*.
2. Nadajemy uprawnienia do folderu: pełne prawa dla właściciela i grupy (4+2+1) oraz odczyt i wykonanie (4+1) dla pozostałych użytkowników:

```
sudo chmod 775 /srv/www/szok
```


3. Tworzymy plik */srv/www/szok/index.html* z zawartością do wyświetlenia, np.:

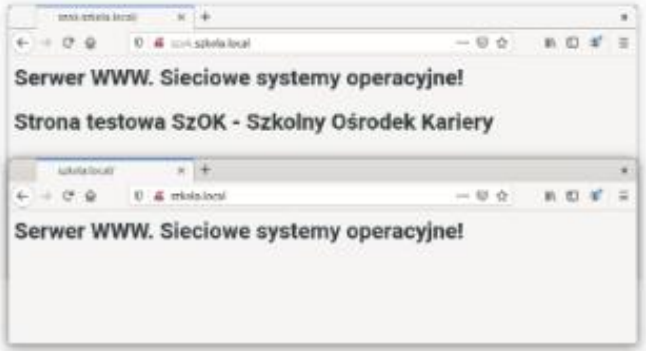
```
<html>
<head>
<meta charset="UTF-8">
</head>
<body>
<h1>Serwer WWW. Sieciowe systemy operacyjne!</h1>
<h1>Strona testowa SzOK - Szkolny Ośrodek Kariery</h1>
</body>
</html>
```

4. W narzędziu YaST przechodzimy do *Usługi sieciowe/Serwer DNS* i na karcie *Strefy DNS* w strefie głównej *szkola.local* dodajemy w zakładce *Rekordy* rekord A *szok.szkola.local*, kierujący na adres `192.168.0.1`, a następnie zatwierdzamy przyciskiem *OK*.
5. W narzędziu YaST przechodzimy do *Usługi sieciowe/Serwer HTTP*, wybieramy kartę *Hosty* i klikamy *Dodaj*. Następnie uzupełniamy dane jak na rysunku 2.59, klikamy *Zmiana ID hosta wirtualnego*, zaznaczamy *Wszystkie adresy (*)* i zatwierdzamy przyciskiem *OK*. Aby przejść do następnej karty, klikamy *Dalej*.



Rysunek 2.59. Dodawanie wirtualnego hosta

6. Na karcie *Szczegóły hostów wirtualnych*, w polu *Indeks katalogu* wpisujemy nazwę pliku, który ma się uruchamiać przy wywołaniu strony, `index.html`, i klikamy *Dalej*. Na karcie *Konfiguracja serwera HTTP* klikamy *Zakończ*.
7. Ponieważ dodajemy wirtualnego hosta, musimy dodać w ten sam sposób drugiego hosta, o nazwie *szkola.local*, który będzie prowadził do katalogu */srv/www/htdocs*.
8. Sprawdzamy działanie stron WWW w przeglądarce, jak na rysunku 2.60.

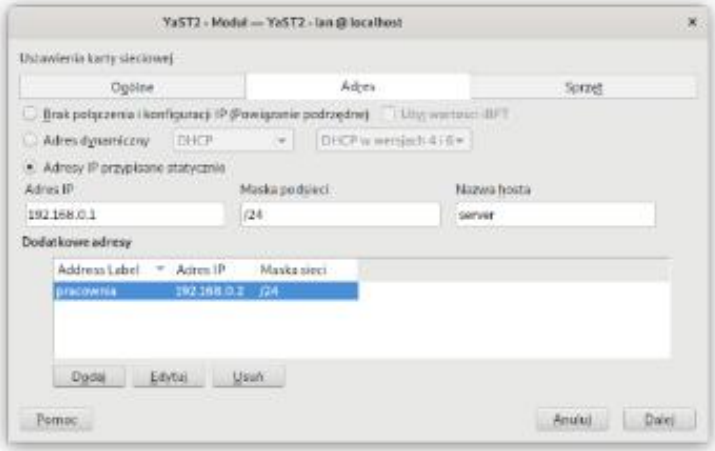


Rysunek 2.60. Sprawdzenie działania stron WWW z jednego serwera

Ćwiczenie 2.15

Teraz skonfigurujemy wirtualnego hosta na dodatkowym adresie IP.

1. Zaczynamy od ustawienia dodatkowego adresu IP. Uruchamiamy narzędzie YaST, przechodzimy do *System/Ustawienia sieciowe*, zaznaczamy lokalny interfejs *eth1* i klikamy *Edytuj*. W zakładce *Adres* klikamy *Dodaj*, z listy *Typ urządzenia* wybieramy *Ethernet*, w nowo otwartym okienku wpisujemy nazwę `pracownia`, adres IP `192.168.0.2` i maskę `/24`, a następnie klikamy *OK*. Uzyskaliśmy efekt jak na rysunku 2.61.



Rysunek 2.61. Dodawanie dodatkowego adresu IP do interfejsu

2. Klikamy *Dalej* i potwierdzamy przyciskiem *OK*. Możemy sprawdzić działanie hosta poleceniem `ping 192.168.0.2`, np. z drugiej maszyny.

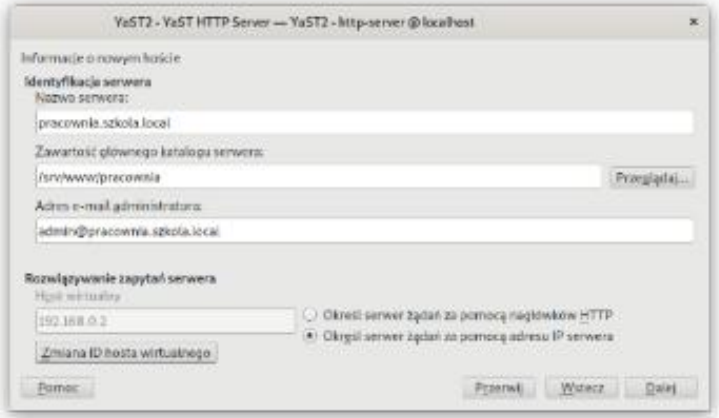
3. Ponownie tworzymy katalog, w którym przechowywana będzie zawartość strony, poleceniem `sudo mkdir /srv/www/pracownia`.
4. Nadajemy uprawnienia do katalogu: pełne prawa dla właściciela i grupy oraz odczyt i wykonanie dla pozostałych użytkowników:

```
sudo chmod 775 /srv/www/pracownia
```

5. Tworzymy plik */srv/www/pracownia/index.html* z zawartością do wyświetlenia, np.:

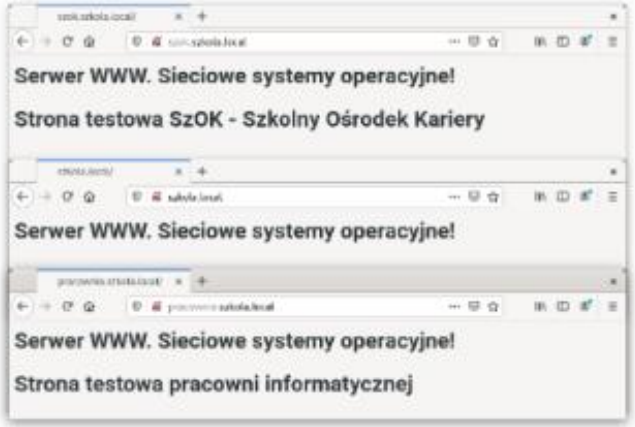
```
<html>
<head>
<meta charset="UTF-8">
</head>
<body>
<h1>Serwer WWW. Sieciowe systemy operacyjne!</h1>
<h1>Strona testowa pracowni informatycznej</h1>
</body>
</html>
```

6. Przechodzimy do *Usługi sieciowe/Serwer DNS*, wybieramy kartę *Strefy DNS*, zaznaczamy strefę główną *szkola.local*, klikamy *Edytuj* i dodajemy w zakładce *Rekordy* rekord A *pracownia.szkola.local*, kierujący na adres `192.168.0.2`, a następnie dwukrotnie zatwierdzamy przyciskiem *OK*.
7. W narzędziu YaST przechodzimy do *Usługi sieciowe/Serwer HTTP*, wybieramy kartę *Hosty*, klikamy *Dodaj* i uzupełniamy pola jak w poprzednim ćwiczeniu, uwzględniając nowe dane, jak na rysunku 2.62, a następnie klikamy *Dalej*.



Rysunek 2.62. Konfiguracja wirtualnego hosta opartą na adresie IP

8. Na karcie *Szczegóły hostów wirtualnych*, w polu *Indeks katalogu* wpisujemy nazwę pliku, który ma się uruchamiać przy wywołaniu strony, `index.html`, i klikamy *Dalej*. Na karcie *Konfiguracja serwera HTTP* klikamy *Zakończ*.
9. Sprawdzamy działanie stron WWW w przeglądarce, jak na rysunku 2.63.



Rysunek 2.63. Sprawdzenie działania stron WWW z jednego serwera

Zadania kontrolne

1. Uruchom na wirtualnym serwerze stronę WWW opartą na rozróżnianiu na podstawie domeny o nazwie *twoje_imie.pl*.
2. Uruchom na wirtualnym serwerze stronę WWW opartą na rozróżnianiu na podstawie adresu IP `192.168.0.50` o nazwie *twoje_nazwisko.pl*.

2.11. Konfiguracja i udostępnianie drukarki sieciowej

Drukarki mają różne interfejsy do łączenia się z komputerem:

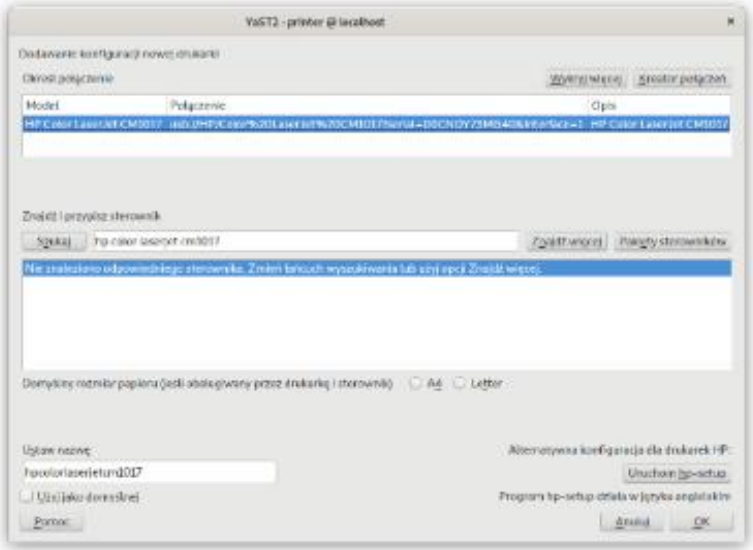
- USB — służy do lokalnego podłączenia drukarki,
- Ethernet — służy do połączenia drukarki za pomocą sieci LAN,
- Wi-Fi — służy do bezprzewodowego podłączenia drukarki za pomocą sieci bezprzewodowej.

Aby z drukarki mogło korzystać więcej osób, trzeba ją udostępnić. O ile z drukarką podłączoną za pośrednictwem sieci przewodowej i bezprzewodowej nie będzie problemu, o tyle drukarkę podłączoną za pomocą interfejsu USB trzeba udostępnić na komputerze, do którego

jest podłączona. Zarazem, aby można było drukować, komputer, który udostępnia drukarkę, musi być włączony.

Ćwiczenie 2.16

1. Zacznijmy od zainstalowania drukarki USB. Drukarka po podłączeniu zostanie rozpoznana i automatycznie zainstalowana. Uruchamiamy narzędzie YaST, a następnie przechodzimy do *Sprzęt/Drukarka*. Możemy wybrać opcję *Konfiguracja automatyczna* i zaznaczyć w niej *Przeprowadź automatyczną konfigurację drukarek podłączonych lokalnie*. Drukarka zostanie wykryta i skonfigurowana. Na zakończenie klikamy *OK*.
2. Jeśli drukarka nie została skonfigurowana, klikamy *Dodaj*. Otworzy się okno *Dodawanie konfiguracji nowej drukarki* (rysunek 2.64).



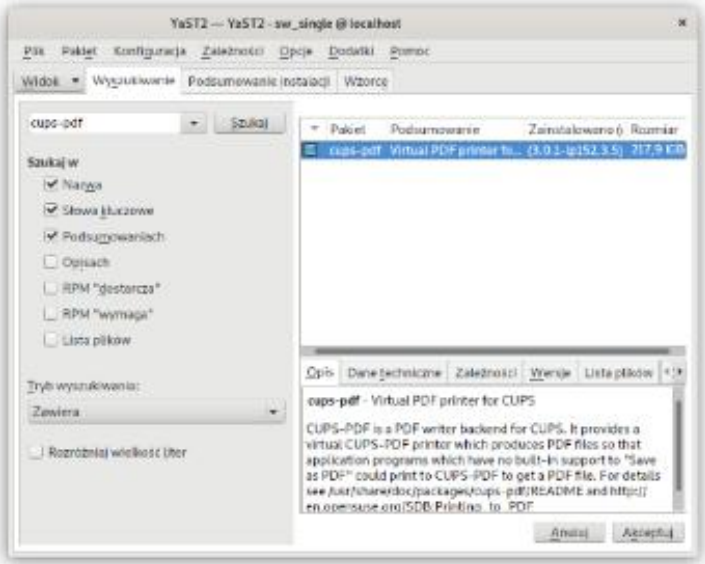
Rysunek 2.64. Dodawanie drukarki

3. Jeśli system nie znalazł sterownika do drukarki, klikamy *Pakiety sterowników* i wybieramy pakiet producenta sprzętu. Producent drukarki użytej w przykładzie to Hewlett-Packard (HP), zatem trzeba było zainstalować pakiet o nazwie *hplip + hplip-hpijs : Sterownik dla drukarek i urządzeń wielofunkcyjnych HP*. Po zaznaczeniu pakietu wystarczy kliknąć przycisk *OK*, by rozpoczął się proces instalowania dodatkowych sterowników.
4. Po zakończeniu instalacji zatwierdzamy przyciskiem *OK*.

Drukarka została zainstalowana, jednakże w trakcie zajęć możemy mieć problem z rzeczywistą drukarką, dlatego wykorzystamy drukarkę wirtualną PDF, jaką oferuje openSUSE. Następnie udostępnimy ją w sieci.

Ćwiczenie 2.17

1. Uruchamiamy narzędzie YaST i otwieramy *Oprogramowanie/Zarządzanie oprogramowaniem*. W polu wyszukiwania wpisujemy `cups-pdf`. Zostanie wyświetlony tylko jeden pakiet. Zaznaczamy go i klikamy *Akceptuj* (rysunek 2.65).



Rysunek 2.65. Instalacja drukarki PDF

2. Nastąpi proces instalacji i drukarka PDF zostanie automatycznie skonfigurowana w systemie. Na koniec klikamy *Zakończ*.
3. W systemie openSUSE za udostępnianie drukarek sieciowych odpowiada usługa CUPS. Usługa ta po aktywowaniu działa na porcie 631. Domyślnie powinna być zainstalowana, w przeciwnym razie w terminalu logujemy się jako *root* (poleceniem `su`) i wpisujemy `sudo zypper install cups`.
4. Po zainstalowaniu usługa CUPS jest gotowa do pracy, ale tylko na drukarce lokalnej. Aby móc udostępniać drukarkę w sieci, musimy zmienić konfigurację w pliku ustawień *cupsd.conf*. W tym celu w konsoli wykonujemy z uprawnieniami *root* polecenie `gedit /etc/cups/cupsd.conf` i wprowadzamy poniższe zmiany (pogrubione):
   - Wskazujemy interfejs, na którym usługa CUPS będzie nasłuchiwała zadań drukowania:

```
# Only listen for connections from the local machine.
Listen localhost:631
Listen 192.168.0.1:631
```



```
Listen /run/cups/cups.sock
```

   - Rozgłaszanie w sieci lokalnej udostępnionej drukarki:

```
# Show shared printers on the local network.
Browsing On
BrowseOrder allow,deny
BrowseAllow all
BrowseLocalProtocols dnssd
BrowseAddress @LOCAL
```

   - Dodajemy lokalny dostęp do serwera wydruku:

```
# Restrict access to the server...
<Location />
Order allow,deny
Allow @LOCAL
<Location />
```

   - Dodajemy lokalny dostęp do strony administratora:

```
# Restrict access to the admin pages...
<Location />
Order allow,deny
Allow @LOCAL
<Location />
```

   - Dodajemy lokalny dostęp do plików konfiguracyjnych:

```
# Restrict access to configuration files...
<Location /admin/conf>
Authtype Default
Require user @LOCAL
Order allow,deny
Allow @LOCAL
<Location />
```

   ...i na koniec zapisujemy.

5. W terminalu uruchamiamy ponownie usługę wprowadzonym z uprawnieniami *root* poleceniem `sudo systemctl restart cups`. Następnie możemy sprawdzić status usługi poleceniem `sudo systemctl status cups`.
6. Usługą CUPS zarządza się poprzez przeglądarkę. Uruchamiamy ją i w pasku adresu wpisujemy `192.168.0.1:631`. Po przejściu do zakładki *Printers* widzimy dostępną drukarkę (rysunek 2.66).



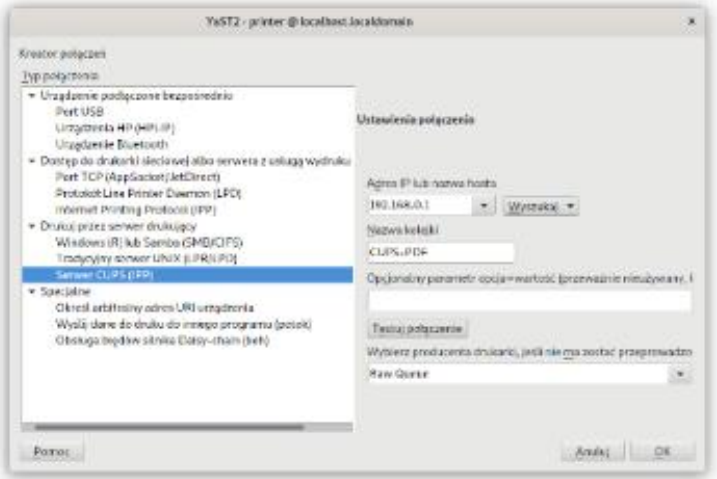
Rysunek 2.66. Strona usługi CUPS zawierająca informacje o drukarce

7. Usługa CUPS cały czas ogłasza w sieci informacje o dostępności drukarek i wymaga, by w systemie klienta działał pakiet cups-browsed (instalowany domyślnie). Pakiet ten przegląda transmisje protokołu Bonjour współdzielonych zdalnych drukarek CUPS i udostępnia te drukarki lokalnie. Aby na kliencie można było dodać drukarkę sieciową, trzeba wykonać polecenie uruchamiające `sudo systemctl start cups-browsed`. Aby mieć za każdym razem uruchomioną usługę przeglądania, należy wykonać polecenie `sudo systemctl enable cups-browsed` (rysunek 2.67).

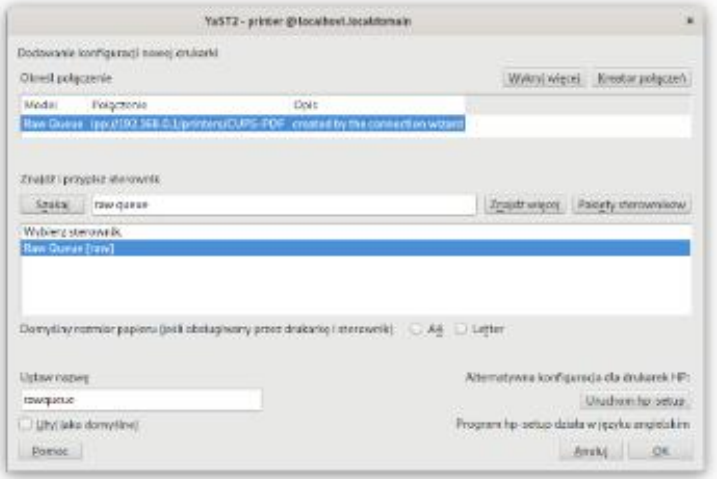


Rysunek 2.67. Wykonanie polecenia uruchamiania pakietu cups-browsed

8. Aby doinstalować drukarkę sieciową na kliencie, w narzędziu YaST przechodzimy do *Sprzęt/Drukarka* i wybieramy *Dodaj*. W nowo otwartej karcie klikamy *Kreator połączeń*, wskazujemy *Serwer CUPS (IPP)*, a następnie uzupełniamy pola: *Adres IP lub nazwa hosta* — `192.168.0.1`, *Nazwa kolejki* — `CUPS-PDF`. Na koniec klikamy *Testuj połączenie* (rysunek 2.68).
9. Po wykonaniu testu połączenia, jeśli został wyświetlony komunikat `Test zakończony powodzeniem`, potwierdzamy przyciskiem *OK*.
10. Na karcie *Dodawanie konfiguracji nowej drukarki* zaznaczamy sterownik *Raw Queue [raw]* i klikamy *OK* (rysunek 2.69).
11. Teraz następuje instalacja sterownika. Po jej zakończeniu klikamy *OK* i możemy rozpocząć drukowanie na drukarce sieciowej.



Rysunek 2.68. Kreator połączenia z serwerem CUPS



Rysunek 2.69. Wybór sterownika drukarki

Zadania kontrolne

1. Wydrukuj przy użyciu zainstalowanej drukarki sieciowej dowolne trzy dokumenty. Następnie za pomocą narzędzia CUPS usuń te zadania.
2. Jakie zadania w sieci ma drukarka sieciowa i jakie są jej zalety?

2.12. Poczta elektroniczna

DEFINICJA

Poczta elektroniczna (e-mail, mail) jest usługą internetową przeznaczoną do wymiany wiadomości pomiędzy użytkownikami urządzeń elektronicznych z wykorzystaniem serwera poczty oraz oprogramowania klienta.

Poczta elektroniczna działa w sieciach komputerowych, głównie w internecie. Serwery e-mail akceptują, przekazują, dostarczają i przechowują wiadomości. Komputery nadawcy i odbiorcy nie muszą być jednocześnie online — mogą się łączyć z serwerem pocztowym lub interfejsem poczty internetowej, aby wysyłać, odbierać lub pobierać wiadomości.

Spróbujemy w prosty sposób wytłumaczyć działanie poczty elektronicznej. Załóżmy, że wysyłamy wiadomość na adres *admin@szkola.local*. Jesteśmy klientem, dlatego nasza poczta trafia najpierw do serwera SMTP. **MTA** (ang. *Mail Transfer Agent*) serwera pyta serwer DNS o adres IP hosta, czyli *szkola.local*, i w tym samym czasie wstawia wiadomość do kolejki doręczenia. Serwer SMTP kontaktuje się z MTA pod adresem *szkola.local* przy użyciu portu 25 (w przypadku połączenia szyfrowanego port 465). Jeśli serwer *szkola.local* potwierdzi kontakt, serwer SMTP wysyła wiadomość. MTA serwera *szkola.local* sprawdza, czy podany odbiorca, *admin*, jest dostępny na liście użytkowników. Jeśli jest dostępny, serwer dostarcza wiadomość i umieszcza ją w skrzynce odbiorczej użytkownika, a następnie zamyka połączenie. Odbiorca odbiera wiadomość ze skrzynki pocztowej przy użyciu protokołu POP3, na porcie 110 (w przypadku połączenia szyfrowanego port 995), lub protokołu IMAP, na porcie 143 (w przypadku połączenia szyfrowanego port 993). Jeśli MTA serwera *szkola.local* nie znajdzie użytkownika, odsyła do nadawcy wiadomość zwrotną o niemożności dostarczenia poczty.

SMTP (ang. *Simple Mail Transfer Protocol*) to protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w sieci. SMTP jest prostym, tekstowym protokołem, w którym określa się co najmniej jednego odbiorcę wiadomości, a następnie przekazuje jej treść. W standardowej konfiguracji SMTP działa na porcie 25. Najprostszym sposobem przetestowania serwera SMTP jest użycie programu telnet, za pomocą którego można wysłać i odczytać wiadomość w postaci zwykłego tekstu. Do pobierania wiadomości z serwera zdalnego służą zaś protokoły POP3 i IMAP. Największym ograniczeniem SMTP jest niemożność zweryfikowania nadawcy, co ułatwia rozpowszechnianie niepożądanych treści poprzez pocztę elektroniczną (takich jak wirusy i spam).

Wyróżniamy następujące rodzaje programów poczty elektronicznej:

- **MTA** (ang. *Mail Transfer Agent*) — program poczty elektronicznej przesyłający wiadomości internetowe pomiędzy adresami poczty elektronicznej, wykorzystujący architekturę klient-serwer;
- **MUA** (ang. *Mail User Agent*) — klient poczty elektronicznej; pobiera pocztę od MRA, a następnie odczytuje ją, redaguje i wysyła do MSA;

- **MSA** (ang. *Mail Submission Agent*) — odbiera pocztę od MUA i wysyła ją do MTA;
- **MTA** (ang. *Mail Transfer Agent*) — serwer poczty elektronicznej, odbiera pocztę od MSA;
- **MDA** (ang. *Mail Delivery Agent*) — pobiera pocztę od MTA i przekazuje ją do skrzynek;
- **MAA** (ang. *Mail Access Agent*) — pobiera pocztę ze skrzynek i wysyła ją do MRA;
- **MRA** (ang. *Mail Retrieval Agent*) — pobiera pocztę od MAA.

Protokół **POP3** (ang. *Post Office Protocol 3*) jest przeznaczony do pracy w trybie offline. Po połączeniu z serwerem cała poczta wraz z załącznikami jest transmitowana ze skrzynki pocztowej na serwerze do programu pocztowego znajdującego się np. w komputerze lokalnym. Takie wiadomości są oznaczane jako przeczytane i w standardowej konfiguracji usuwane z serwera, dlatego odczytanie ich jest możliwe tylko na tym komputerze lokalnym. Jeżeli protokół POP3 zostanie ustawiony jako domyślny dla serwera, może powodować problemy ze względu na niemożność odczytania wiadomości na kilku klientach pocztowych, np. zainstalowanych na komputerze i telefonie. Co więcej, jeśli otrzymamy e-mail z załącznikiem, to rozpocznie się jego automatyczne pobieranie i nawet jeśli trwa ono długo, nie można go anulować. Jeśli przerwiemy tę operację, to i tak po ponownym połączeniu program pobierze wiadomości od nowa. Dodatkową wadą protokołu POP3 jest to, że nie obsługuje folderów pocztowych na serwerze.

Protokół **IMAP** (ang. *Internet Message Access Protocol*) działa w zupełnie inny sposób. Cała poczta jest przechowywana na serwerze w skrzynce pocztowej i może się znajdować w utworzonych przez użytkownika folderach. Gdy klient łączy się z serwerem pocztowym, pobierane są tylko nagłówki wiadomości i jeśli wiadomości nie zostaną usunięte, pozostaną na serwerze, dzięki czemu można odbierać pocztę na kilku urządzeniach. Dodatkowo transmisja wiadomości oraz załączników następuje dopiero po otwarciu wiadomości na kliencie.

Instalacja serwera poczty elektronicznej

Teraz omówimy zagadnienie poczty e-mail wewnątrz sieci lokalnej. Musimy zainstalować serwer poczty elektronicznej **Postfix**, a następnie go skonfigurować. Serwer Postfix konfiguruje się przez edycję pliku konfiguracyjnego */etc/postfix/main.cf*.

Ćwiczenie 2.18

1. Uruchamiamy terminal i instalujemy z uprawnieniami *root* serwer poczty Postfix poleceniem `sudo zypper install postfix`.
2. Wykonujemy kopię zapasową pliku konfiguracji poleceniem `cp /etc/postfix/main.cf /etc/postfix/main.cf.org`.
3. Otwieramy do edycji plik konfiguracyjny poleceniem `gedit /etc/postfix/main.cf`. W pliku musimy wprowadzić zmiany w odpowiednich wierszach, przy czym znaczenie ma kolejność występowania wpisów w pliku (edytor gedit w prawym dolnym rogu pokazuje numer wiersza).

UWAGA

Jeśli Postfix zostanie zaktualizowany do nowszej wersji, może nastąpić zmiana numerów wierszy, ale sama konfiguracja nie ulegnie zmianie. W takiej sytuacji należy odszukać konkretne ustawienie i wprowadzić wymaganą zmianę.

Konfigurujemy następujące parametry:

- *wiersz 110* — usuwamy znacznik komentarza # i zmieniamy zapis — określamy nazwę domeny:

```
mydomain = localhost;
```

- *wiersz 125* — usuwamy znacznik komentarza # — wiersz wskazuje, co będzie dodawane po @, gdy nie ma wpisanej domeny w adresie z pola *from* (np. w polu *from* wpisaliśmy `root`, a system sam dopisze `@localhost`):

```
myorigin = $myhostname;
```

- *wiersz 287* — usuwamy znacznik komentarza # — wskazujemy adresy komputerów, z których będziemy przekazywać pocztę:

```
mynetworks = 127.0.0.0/8, 192.168.0.0/24;
```

- *wiersz 420* — usuwamy znacznik komentarza # — określamy bazy aliasów skrzynek:

```
alias_database = hash:/etc/aliases;
```

- *wiersz 432* — usuwamy znacznik komentarza #

```
recipient_delimiter = +;
```

- *wiersz 442* — usuwamy znacznik komentarza # — wiadomości mają być przenoszone do *Maildir/*:

```
home_mailbox = Maildir/;
```

- *wiersz 578* — podajemy, w jaki sposób przedstawia się serwer:

```
smtpd_banner = $myhostname ESMTP $mail_name (OpenSUSE/GNU Wydawnictwo
HELION.PL);
```

- *wiersz 705* — zmieniamy na:

```
inet_interfaces = all;
```

- *wiersz 706* — zmieniamy na:

```
inet_protocols = ipv4;
```

- *wiersz 710* — zmieniamy na domeny docelowe (poza wirtualnymi), które mają być akceptowane:

```
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain;
```

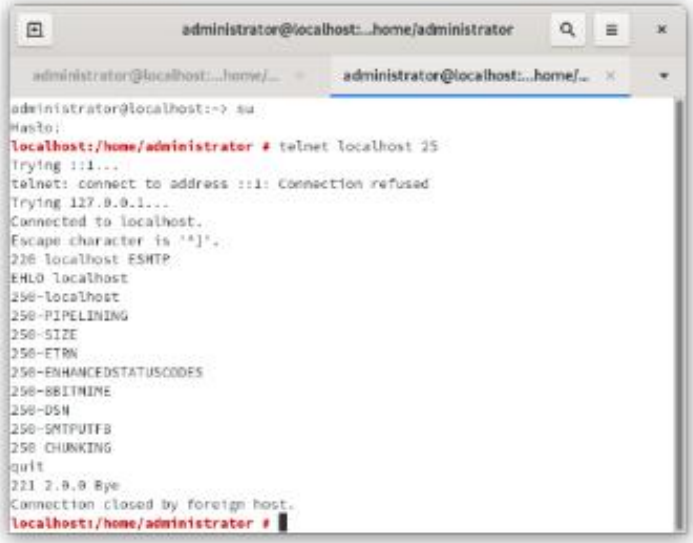

- *wiersz 720* — zmieniamy nazwę katalogu:

```
mail_spool_directory = /home/;
```

- *wiersz 725* — ustalamy limit rozmiaru skrzynki pocztowej, dla przykładu użyjemy 20 MB:

```
mailbox_size_limit = 20971520.
```

4. Po wprowadzeniu zmian należy uruchomić serwer Postfix poleceniem `systemctl start postfix` oraz ustawić uruchamianie przy starcie systemu `systemctl enable postfix`. Aby sprawdzić status działania usługi, wpisujemy `systemctl status postfix`.
5. Tworzymy teraz bazę aliasów poleceniem `newaliases`, a następnie sprawdzamy konfigurację serwera poleceniem `postfix check`.
6. Teraz restartujemy serwer poleceniem `systemctl restart postfix` i testujemy działanie SMTP poleceniem `telnet localhost 25` (rysunek 2.70).



Rysunek 2.70. Sprawdzenie działania SMTP

7. Przystępujemy do instalacji serwera POP3 i IMAP, którym będzie Dovecot, poleceniem `sudo zypper install dovecot`.
8. Następnie ustawiamy prawa do katalogu */var/run/dovecot* poleceniem `chmod 755 /var/run/dovecot`.
9. Przypisujemy katalog do grupy poleceniem `chgrp dovecot /var/run/dovecot/login/`.
10. Konfigurujemy serwer Dovecot. Musimy do pliku `/etc/dovecot/dovecot.conf` przepisać następującą konfigurację po usunięciu całej wcześniejszej:

```
# OS: Linux 5.3.18-lp152.57-default x86_64
# Hostname: localhost
auth_debug = yes
auth_verbose = yes
listen = *
#log_path = /var/log/dovecot.log
log_timestamp = "%Y-%m-%d %H:%M:%S "
login_greeting = POP ready
mail_location = maildir:~/Maildir
mail_privileged_group = postfix
managesieve_notify_capability = mailto
managesieve_sieve_capability = fileinto reject envelope encoded-char-
acter vacation subaddress comparator-i;ascii-numeric relational regex
imap4flags copy include variables body enotify environment mailbox
date index ihave duplicate mime foreverypart extracttext
passdb {
  driver = pam
}
protocols = imap pop3
service auth {
  user = root
}
userdb {
  driver = passwd
}
verbose_proctitle = yes
verbose_ssl = no
protocol pop3 {
  pop3_uidl_format = %08Xu%08Xv
}
protocol lda {
  postmaster_address = postmaster@localhost
}
```

11. Zapisujemy konfigurację i uruchamiamy serwer poleceniem `sudo systemctl start dovecot`.
12. Działanie serwera SMTP możemy sprawdzić przez uruchomienie polecenia `telnet localhost 25`, a następnie wysłanie poniższej wiadomości do użytkownika *james.bond*, utworzonego wcześniej (po wpisaniu każdej linii naciskamy *Enter*):

```
mail from: root@localhost
rcpt to: james.bond@localhost
Data
Subject: Wiadomosc testowa
To jest wiadomosc testowa
.
quit
```

13. Aby sprawdzić skrzynkę pocztową, uruchamiamy `telnet localhost 110`, następnie logujemy się i wykonujemy poniższe polecenia, ponownie wciskając *Enter* po wpisaniu każdej linii:

```
user james.bond
pass (wpisujemy hasło)
stat
```

Powinniśmy otrzymać informację na temat liczby wiadomości.

14. Aby zakończyć, wpisujemy `quit`.

Zadania kontrolne

1. Skonfiguruj domenę pocztową @Twojenazwisko.pl oraz serwery Postfix i Dovecot.
2. Wyślij wiadomość ze skrzynki pocztowej Twoje_imię@Twoje_nazwisko.pl na adres biuro@Twoje_nazwisko.pl.
3. Sprawdź, czy wiadomości są poprawnie wysyłane i odbierane.

2.13. Przydziały dyskowe użytkowników i grup

Ważnym elementem zarządzania każdym systemem operacyjnym, z którego korzysta wielu użytkowników, są przydziały dyskowe, czyli określenie miejsca, jakie ma do wykorzystania dany użytkownik. To miejsce może być przydzielone na jednej lub kilku partycjach, ale trzeba pamiętać, aby dla każdej partycji wykonać niezależny przydział. (Dotyczy to zarówno systemów z rodziny Linux, jak i Windows). Oprócz przydziałów dla poszczególnych użytkowników stosuje się przydziały dla grup. Przydziały dla grup są o tyle wygodniejsze, że nie trzeba ich konfigurować dla poszczególnych użytkowników. Przydział skonfigurowany dla grupy ma zastosowanie do wszystkich jej członków.

Do obsługi przydziałów dyskowych używamy pakietu quota. W systemie openSUSE ten pakiet jest już zainstalowany, ale w razie potrzeby można to zrobić poleceniem `sudo zypper install quota` bądź za pomocą narzędzia YaST, w grupie ustawień *Oprogramowanie/Zarządzanie oprogramowaniem*.

System Linux przechowuje informacje o punktach montowania w pliku `/etc/fstab`. Dodatkowo w każdym punkcie montowania umieszczony jest plik *aquota.user*, który odpowiada za przydziały dla poszczególnych użytkowników.

Spróbujmy teraz ustawić przydział dyskowy dla użytkownika *James Bond*. Na potrzeby ćwiczenia dołożyliśmy do Oracle VirtualBox dodatkowy dysk o wielkości 10 GB.

Montowanie partycji

Zaczniemy teraz od zamontowania partycji */dev/sdb1* do folderu */Bond*.

Ćwiczenie 2.19

1. Uruchamiamy terminal, a w nim program *fdisk*, którym będziemy partycjonować nasz nowo dodany dysk */dev/sdb*, poleceniem `sudo fdisk /dev/sdb` (rysunek 2.71).

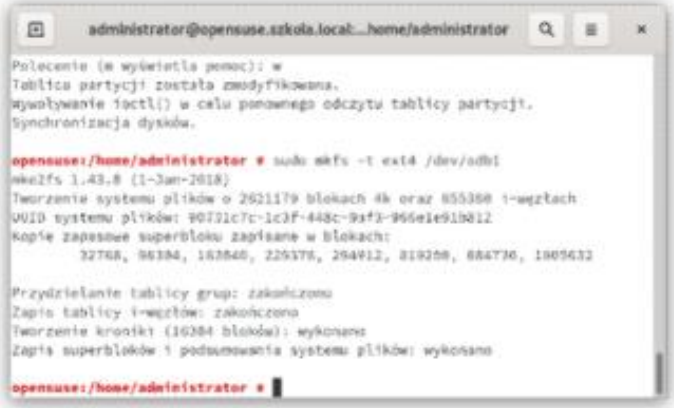


Rysunek 2.71. Program fdisk do partycjonowania dysku

2. Wybieramy po kolei:
   - *g* — utworzenie nowej, pustej tablicy partycji GPT,
   - *n* — dodanie nowej partycji,

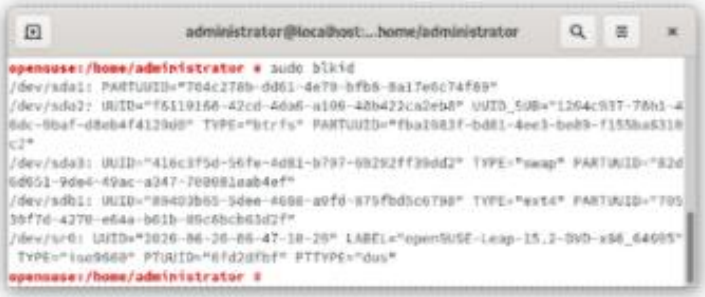
   - *1* — numer partycji,
   - *2048* — pierwszy sektor partycji lub domyślnie,
   - *20971486* — ostatni sektor partycji lub domyślnie,
   - *w* — zapis tablicy partycji na dysk i zakończenie.

3. Partycja została ukończona i zapisana na dysku. Formatujemy ją w systemie plików ext4 poleceniem `sudo mkfs -t ext4 /dev/sdb1` (rysunek 2.72).



Rysunek 2.72. Formatowanie partycji w systemie plików ext4

4. Tworzymy punkt montowania. Zaczniemy od utworzenia folderu */Bond* poleceniem `sudo mkdir /Bond` oraz zwiększenia mu uprawnień poleceniem `sudo chmod 777 /Bond`.
5. Teraz musimy wprowadzić zmiany w pliku */etc/fstab*, ale zanim to zrobimy, wykonajmy jego kopię poleceniem `sudo cp /etc/fstab /etc/fstab.bak`.
6. Uruchamiamy polecenie `sudo blkid`, które pokaże nam klucz *UUID* partycji *sdb1*. Będzie potrzebny do utworzenia punktu montowania (rysunek 2.73).



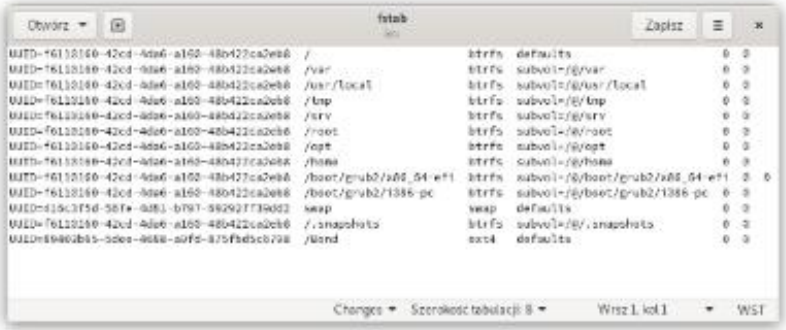
Rysunek 2.73. Pobranie UUID nowej partycji

7. Edytujemy plik */etc/fstab* poleceniem `gedit /etc/fstab`. Dodajemy na końcu pliku następujące wartości (rysunek 2.74):

   ```
   UUID="12345678-90ab-cdef-1234-567890abcdef" /Bond ext4 defaults 0 0
   ```

   gdzie:

   - *UUID* — generowany automatycznie 32-znakowy, teoretycznie unikatowy identyfikator używany do oznaczania partycji;
   - */Bond* — katalog montowania;
   - *ext4* — system plików partycji;
   - *defaults* — dodatkowe opcje (my użyjemy domyślnych ustawień);
   - *0* — parametry dla programu dump, który archiwizuje partycje;
   - *0* — kolejność sprawdzania systemu plików na partycjach przez program fsck, który jest uruchamiany, jeżeli podczas uruchamiania systemu zostały wykryte błędy.



Rysunek 2.74. Widok pliku /etc/fstab z wpisem montowania partycji w katalogu /Bond

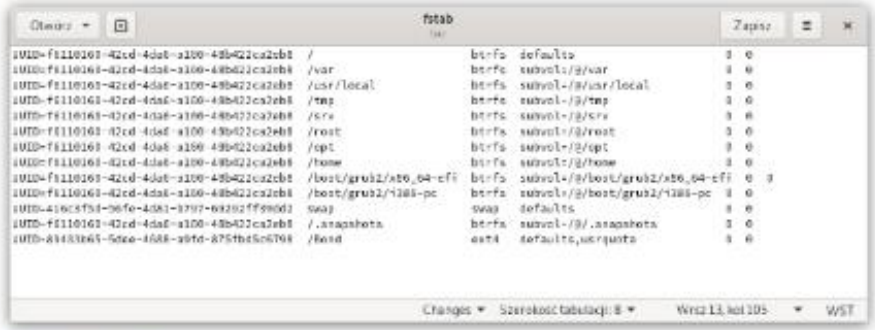
8. Teraz możemy użyć polecenia `mount -a`, które montuje wszystkie systemy plików ujęte w pliku `/etc/fstab`, lub ponownie uruchamiamy komputer, który uruchomi się już z partycją zamontowaną do katalogu.

Przydzielanie przestrzeni dyskowej

Teraz wykonamy przydział przestrzeni dyskowej dla użytkownika *James Bond* (*james.bond*).

Ćwiczenie 2.20

1. Ponownie otwieramy do edycji plik */etc/fstab* poleceniem `gedit /etc/fstab`.
2. W wierszu dotyczącym montowania partycji */dev/sdb1* do katalogu */Bond* zamieniamy `default` na `defaults,usrquota`, jak na rysunku 2.75, i zapisujemy plik.



Rysunek 2.75. Efekt dopisania polecenia usrquota w pliku /etc/fstab

3. Aby zmiany zadziałały, musimy wykonać polecenie `sudo mount -o remount /Bond` lub ponownie uruchomić komputer.
4. Wszystkie informacje na temat przydziałów dyskowych poszczególnych użytkowników znajdują się w pliku *aquota.user*. Taki plik musi się znajdować w każdym katalogu, który jest punktem montowania i do którego stosujemy przydziały. W naszym przypadku jest to */Bond*.
5. Uruchamiamy polecenie `sudo quotacheck -ugm /Bond/`.
6. Po wykonaniu polecenia zostanie utworzony plik */Bond/aquota.user*, w którym będą zawarte wszystkie przydziały miejsca dla użytkowników.
7. Wykonujemy polecenie `sudo quotaon -avug`, które włączy przydziały dla użytkowników. Aby te przydziały wyłączyć, używamy polecenia `sudo quotaoff -avug` (rysunek 2.76).



Rysunek 2.76. Sprawdzenie i włączenie obsługi przydziałów

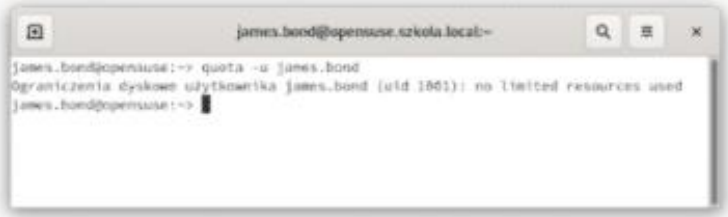
8. Teraz musimy przypisać przydziały dla każdego użytkownika z osobna. W przypadku użytkownika *James Bond* robimy to poleceniem `sudo edquota -u james.bond`. Uruchomimy w ten sposób edytor vi, w którym przypiszemy przydziały (rysunek 2.77). Limity użytkownika będziemy ustalać za pomocą bloków (1 blok = 1 kB). Są dwa rodzaje limitów:

- **Limit miękki** — jest to limit czasowy. Oznacza to, że użytkownik może go przekraczać dowolną liczbę razy. Użytkownik musi pamiętać, że limit może być przekroczony tylko przez określony czas (ang. *grace period* — domyślnie 7 dni) i że w tym czasie trzeba usunąć nadmiar plików. Jeśli tego nie zrobi, zostaną one skasowane do przydzielonego limitu.
- **Limit twardy** — jest to wartość określająca maksymalny rozmiar zasobu dyskowego udostępnionego użytkownikowi, którego użytkownik nie może przekroczyć.



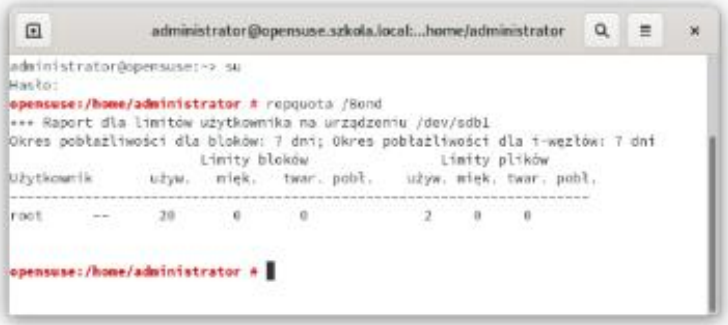
Rysunek 2.77. Edycja przydziałów w edytorze vi

Skonfigurowaliśmy przydziały dla użytkownika *James Bond* (*james.bond*). Teraz pokażemy, jak użytkownik może sam sprawdzić stan przydzielonej przestrzeni dyskowej poleceniem `quota -u james.bond` (rysunek 2.78).



Rysunek 2.78. Wynik użycia polecenia quota

Administrator może wykonać raport, w którym sprawdzi stan wykorzystania obszaru dyskowego dla danego użytkownika z przydziałem, za pomocą polecenia `sudo repquota /Bond` (rysunek 2.79).



Rysunek 2.79. Wynik działania polecenia repquota

Grupom przydziały dyskowe nadajemy w ten sam sposób co poszczególnym użytkownikom. Jedyna różnica polega na tym, że to w pliku */etc/fstab* obok `usrquota` dopisujemy `grquota`. Grupy do przydziałów dopisujemy z wykorzystaniem polecenia `sudo edquota -g users`.

Zadanie kontrolne

1. Utwórz grupę użytkowników o nazwie *Nauczyciele*, a następnie utwórz i dodaj do niej konta trzech użytkowników. Skonfiguruj dla grupy *Nauczyciele* przydziały dyskowe dla katalogu */Nauczyciele* o wielkościach, odpowiednio, 12 500 bloków i 25 000 bloków. Pokaż, że przydziały działają.

2.14. Automatyzacja uruchamiania zadań — cron

W tym podrozdziale omówimy automatyczne uruchamianie zadań. Wszystkie polecenia, jakie do tej pory wykonywaliśmy, były uruchamiane natychmiast. Jednakże czasami chcemy, aby pewne polecenia wykonywały się automatycznie o określonej porze. Takim zadaniem może być aktualizacja bazy wirusów czy też sporządzenie kopii zapasowej. W systemach Windows służy do tego narzędzie Harmonogram zadań, a w systemach z rodziny Linux — cron.

Cron to demon wbudowany w większość systemów linuksowych i powinien działać automatycznie. W przeciwnym razie musimy go uruchomić. Robimy to poleceniem `sudo service crond start`. Aby zatrzymać jego działanie, używamy polecenia `sudo service crond stop`, a żeby uruchomić go ponownie — `sudo service crond restart`.

Zasadniczo cron jest przeznaczony dla użytkowników o uprawnieniach *root*, ale możemy go tak skonfigurować, aby zwykły użytkownik także mógł z niego korzystać. W tym celu tworzymy dwa pliki:

- */etc/cron.deny* — użytkownicy wymienieni w tym pliku nie mogą użyć polecenia `crontab -e`, aby dodać regułę zadania cron, ale ich zadania, jeśli zostały wcześniej zdefiniowane, zostaną wykonane;
- */etc/cron.allow* — użytkownicy wymienieni w tym pliku mogą używać polecenia `crontab -e`.

Wszystkie wpisy zadań znajdują się w tabelach pliku *crontab*. Zobaczmy teraz, jak wygląda wpis w takim pliku:

`minuta | godzina | dzień_miesiąca | miesiąc | dzień_tygodnia | polecenie`

Poszczególne pozycje przyjmują następujące wartości:

- **`minuta`** — od 0 do 59,
- **`godzina`** — od 0 do 23,
- **`dzień_miesiąca`** — od 0 do 31,
- **`miesiąc`** — od 1 do 12,
- **`dzień_tygodnia`** — od 0 do 7 (0 i 7 to niedziela) lub trzy pierwsze litery angielskiej nazwy dnia tygodnia,
- **`polecenie`** — polecenie konsolowe lub skrypt,
- `*` — dowolna wartość.

Aby dodać zadanie, używamy polecenia `crontab -e`, aby zaś podejrzeć istniejące zadania, wpisujemy `crontab -l` (rysunek 2.80). Polecenia generują wpis w pliku */root/cron.txt* z ustaloną w nich częstotliwością.



Rysunek 2.80. Polecenie dodania zadania oraz polecenie wyświetlające działające zadania

Aby sprawdzić wykonanie polecenia, wystarczy otworzyć plik */root/cron.txt*.

Zadania kontrolne

1. Zaplanuj wykonanie polecenia wpisującego Twoje imię i nazwisko w pliku */root/dane* co 1 godzinę oraz nazwisko i imię w każdą środę i niedzielę o godzinie 12:34.
2. Pozwól użytkownikowi *James Bond* (*james.bond*) na wykonanie polecenia `crontab -e` i sprawdź działanie tego polecenia.

2.15. Serwer Samba

DEFINICJA

Samba to serwer plików oraz drukarek dostępny dla każdego systemu operacyjnego, co pozwala udostępniać zasoby pomiędzy różnymi systemami. Jest rozpowszechniany bezpłatnie na licencji GPL (ang. *GNU General Public License*).

Samba korzysta z implementacji protokołu **SMB** (ang. *Server Message Block*), dzięki czemu obok siebie mogą działać systemy z rodziny Linux, Unix i Windows. Samba może funkcjonować jako darmowy odpowiednik serwera Windows NT w środowisku Active Directory. Głównymi cechami Samby są:

- współdzielenie plików i drukarek,
- serwer logowania dla sieci Windows,
- podstawowy kontroler domeny,
- serwer przeglądania Windows,
- obsługa WINS (internetowego serwera nazw),
- obsługa OpLock (buforowania plików w komputerach klientach),
- obsługa LDAP,
- synchronizacja haseł pomiędzy systemami Linux i Windows,
- obsługa SSL.

Serwer Samba składa się z dwóch podstawowych demonów: SMBD i NMBD.

SMBD (ang. *Server Message Block Daemon*) to demon odpowiedzialny za poprawne działanie serwera. Każdemu klientowi podłączonemu do serwera Samba odpowiada oddzielny demon SMBD. Ponadto SMBD obsługuje dostęp do plików i drukarek.

NMBD (ang. *Network Message Block Daemon*) to demon usługi nazw NetBIOS. W poprawnie skonfigurowanym serwerze powinien działać przynajmniej jeden proces NMBD. Jeżeli w serwerze został skonfigurowany parametr pozwalający Sambie pracować jako serwer WINS (`wins server = yes`), zostanie utworzona kolejna kopia demona NMBD. Ponadto NMDB obsługuje przeszukiwanie nazw NetBIOS oraz żądania WINS.

Dodatkowym demonem jest **Winbind**. Samba za pomocą Winbind pobiera dane na temat użytkowników i grup z systemu Windows oraz odwzorowuje je na lokalne numery UID. Winbind kontroluje usługę winbindd, a do jego włączenia nie jest potrzebny działający demon SMBD.

Instalacja i konfiguracja serwera Samba

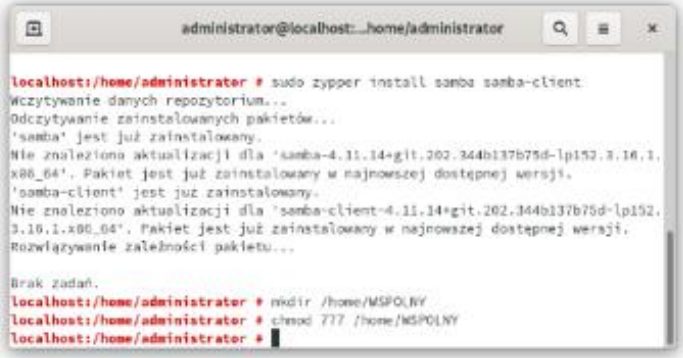
Najpierw pokażemy, jak skonfigurować Sambę jako serwer plików dostępny dla wszystkich. Udział będzie miał nazwę *WSPOLNY*.

Ćwiczenie 2.21

1. Uruchamiamy terminal, przełączamy się na konto z uprawnieniami *root* poleceniem su, a następnie instalujemy pakiety samba i samba-client:

   ```
   sudo zypper install samba samba-client
   ```

2. Tworzymy folder */home/WSPOLNY* poleceniem `mkdir /home/WSPOLNY`.
3. Nadajemy pełne prawa dla wszystkich poleceniem `chmod 777 /home/WSPOLNY` (rysunek 2.81).



Rysunek 2.81. Instalacja Samby oraz tworzenie katalogu do udostępnienia

4. Teraz przechodzimy do konfiguracji środowiska Samba. Główny plik przechowujący jej ustawienia znajduje się w katalogu */etc/samba/smb.conf*. Najpierw wykonamy jego kopię:

   ```
   cp /etc/samba/smb.conf /etc/samba/smb.conf.org
   ```

5. Następnie otworzymy go do edycji:

   ```
   gedit /etc/samba/smb.conf
   ```

6. W pliku możemy usunąć całą konfigurację. Dodajemy następujące wpisy:
   - sekcja `[Global]` — sekcja ustawień globalnych:
     - `unix charset = UTF-8` — kodowanie znaków,
     - `netbios name = SERVER` — nazwa NetBIOS komputera,
     - `server string = szkola.local` — nazwa serwera;
   - sekcja `[WSPOLNY]` — sekcja nazwy udziału:

     - `path = /home/WSPOLNY` — ścieżka udostępnionego udziału,
     - `comment = Dysk Wspolny` — opis udostępnionego udziału,
     - `browsable = yes` — widoczność udziału w sieci,
     - `writable = yes` — zapisywalność udziału,
     - `guest ok = yes` — dostęp gościa,
     - `guest only = yes` — dostęp tylko dla gości,
     - `create mode = 0777` — określa, z jakimi prawami tworzone są pliki poprzez sieć,
     - `directory mode = 0777` — określa, z jakimi prawami tworzone są katalogi poprzez sieć.

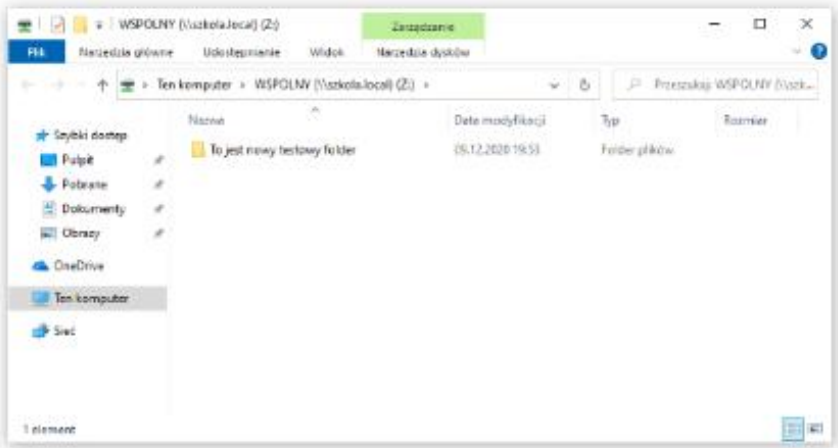
7. Zapisujemy plik i zamykamy. Następnie musimy uruchomić serwer Samba:

   ```
   systemctl start smb nmb
   ```

   oraz włączyć uruchamianie usługi wraz z systemem:

   ```
   systemctl enable smb nmb
   ```

8. Teraz do sprawdzenia konfiguracji możemy użyć np. komputera z Windows 10. Podłączamy go do sieci wewnętrznej, ustawiamy, żeby adres IP był pozyskiwany z DHCP, i w menu *Start* wpisujemy `\\192.168.0.1\`, a wtedy system pokaże nam udostępniony folder. Mapujemy go i mamy stały dostęp do zasobu sieciowego o nazwie *WSPOLNY* (rysunek 2.82).



Rysunek 2.82. Zamapowany dysk sieciowy w systemie Windows 10

Udostępnianie folderu w sieci

Teraz spróbujmy udostępnić folder w sieci, ale z ograniczeniem, aby użytkownicy musieli się zalogować i nie wszyscy mieli do niego dostęp.

Ćwiczenie 2.22

1. Zakładamy, że pakiety samba i samba-client są już zainstalowane. Utworzymy teraz następny katalog; nadamy pełne prawa do niego właścicielowi i grupie, a odmówimy wszystkim innym. Utworzymy także grupę zabezpieczeń o takiej samej nazwie. Tym razem będzie to katalog */home/Dokumenty*, który zostanie dodany do grupy *Dokumenty*. Użyjemy do tego następujących poleceń (rysunek 2.83):

```
mkdir /home/Dokumenty
chmod 770 /home/Dokumenty
groupadd Dokumenty
chgrp Dokumenty /home/Dokumenty
```



Rysunek 2.83. Tworzenie katalogu i grupy, zmiana uprawnień katalogu i dopisanie go do grupy zabezpieczeń

2. Otwieramy do edycji plik */etc/samba/smb.conf* i uzupełniamy zgodnie z poniższym schematem:
   - sekcja `[Global]`:
     - `#map to guest = Bad User` — dodajemy `#` przed parametrem i tym samym wyłączamy go. To ustawienie zezwala użytkownikom bez kont w systemie z serwerem Samba na zalogowanie się i przypisanie sobie konta gościa;
   - sekcja `[Dokumenty]` (tworzymy ją):
     - `path = /home/Dokumenty`,
     - `comment = Dokumenty bezpieczne`,
     - `writable = yes`,
     - `guest ok = no` — bez dostępu gości,
     - `create mode = 0770`,
     - `directory mode = 0770`,
     - `valid users = @Dokumenty` — akceptowani użytkownicy należący do grupy *Dokumenty*.

3. Zmiany przedstawia rysunek 2.84. Widzimy, że dołożony został kolejny udział, bez usuwania poprzedniego.



Rysunek 2.84. Modyfikacja pliku /etc/samba/smb.conf

4. Ponownie uruchamiamy Sambę poleceniem `systemctl restart smb nmb`.
5. Teraz musimy dodać do Samby użytkownika. Robimy to poleceniem `smbpasswd -a james.bond`.
6. W trakcie wykonywania polecenia musimy dwa razy wpisać hasło użytkownika. Następnie dodajemy użytkownika *james.bond* do grupy zabezpieczeń *Dokumenty* poleceniem `usermod -G Dokumenty james.bond` (rysunek 2.85).



Rysunek 2.85. Dodanie użytkownika do serwera Samba oraz do grupy zabezpieczeń Dokumenty

7. W tym momencie mamy już dostęp w systemie Windows 10 do plików udostępnionych w zasobie *Dokumenty* i możemy go np. zamapować. Zarazem odłączyliśmy wcześniej udostępniony zasób *WSPOLNY*.

Zadania kontrolne

1. Utwórz i udostępnij tylko do odczytu udział */home/samba*.
2. Utwórz i udostępnij udział */home/bohater* tylko dla dwóch użytkowników: *Superman* i *Batman*, z pełnymi prawami. Folder nie może być widoczny publicznie — by uzyskać dostęp, będzie trzeba wpisać ścieżkę.



3

Sieciowy system operacyjny Windows Server

W tym rozdziale rozpoczniesz swoją przygodę z systemami Windows Server 2016 oraz Windows Server 2019, należącymi do rodziny Windows NT i rozwijanymi równolegle z Windows 10. Jeśli jednak masz starszą wersję, nie będziesz mieć trudności z wykonaniem ćwiczeń w tym rozdziale, ponieważ w obsłudze obydwa systemy są bardzo podobne do swoich poprzedników. W Windows Server 2016 wprowadzono kilka nowości, które pokażemy w kolejnych podrozdziałach.

Microsoft Windows Server 2016 jest oprogramowaniem serwerowym, dzięki któremu będziemy zarządzać naszą siecią, jej użytkownikami oraz pracującymi w niej urządzeniami. Szczególny nacisk w systemach serwerowych kładzie się na wydajność i niezawodność, gdyż to od nich zależy stabilność działania całej sieci.

Oprogramowanie z rodziny Windows Server jest oprogramowaniem komercyjnym, które wymaga wykupienia licencji. Jeśli jej nie masz, możesz pobrać wersję próbną **Windows Server**, którą wolno użytkować po zarejestrowaniu przez 180 dni. O tym, jak pobrać ten system w wersji 2016 lub 2019, napisaliśmy w rozdziale 1.

Microsoft Windows Server 2016 jest dostępny w następujących edycjach:

- *Essentials* — przeznaczona dla organizacji z nie więcej niż 25 użytkownikami i 50 urządzeniami (świetny alternatywny wybór dla klientów używających odmiany Foundation, która to nie jest już dostępna w wersji 2016);
- *Standard* — podstawowa edycja systemu, z ograniczoną funkcją wirtualizacji, przeznaczona do niezwirtualizowanych środowisk fizycznych lub zwirtualizowanych w minimalnym stopniu;

- *Datacenter* — najbardziej zaawansowana, która udostępnia wszystkie możliwości systemu, w tym nieograniczoną wirtualizację, zalecana do wysoce zwirtualizowanych centrów danych oraz środowisk chmurowych;
- *MultiPoint Premium Server* — przeznaczona dla organizacji edukacyjnych, pozwalająca korzystać z jednego komputera wielu osobom jednocześnie za pomocą uproszczonych stacji użytkowników, popularnie zwanych terminalami, składających się z monitora, klawiatury i myszy;
- *Storage* — dostępna w kanale sprzedaży OEM na potrzeby pamięci masowych i przeznaczona dla producentów sprzętu do składowania danych;
- *Hyper-V* — darmowa, do użycia wyłącznie jako serwer host na potrzeby wirtualizacji.

Microsoft Windows Server 2019 jest dostępny tylko w trzech edycjach:

- *Essentials* — przeznaczona dla małych organizacji, które mają tylko podstawowe wymagania względem IT;
- *Standard* — przeznaczona dla organizacji, które wymagają zaawansowanych funkcji lub są zwirtualizowane w minimalnym stopniu;
- *Datacenter* — przeznaczona dla dużych organizacji o wysokich wymaganiach w zakresie obciążenia IT, wykorzystujących dużą liczbę systemów wirtualnych.

W tym rozdziale poznasz funkcje systemu Windows Server 2016/2019. Nauczysz się, jak konfigurować i instalować system serwerowy, a następnie nim zarządzać. Poznasz takie usługi jak: Active Directory, DHCP, DNS, GPO oraz dowiesz się, jak zarządzać użytkownikami, jednostkami organizacyjnymi i komputerami klienckimi. Dowiesz się też, jak uruchomić dostęp do internetu na komputerze klienta, uruchomić serwer stron WWW oraz wykonać kopię zapasową systemu.

3.1. Przygotowanie i instalacja systemu operacyjnego Microsoft Windows Server 2016/2019

Zanim rozpocznie się pracę z serwerem, warto zaplanować, do czego będzie służył, sprawdzić jego wymagania i przygotować odpowiedni sprzęt. Do tego będą nam przydatne minimalne wymagania sprzętowe systemu oraz informacje o zalecanej konfiguracji, które producent oprogramowania udostępnia na swoich stronach WWW. W tabeli 3.1 znajdziesz porównanie parametrów minimalnych oraz zalecanych dla Windows Server 2016/2019. Zarazem potrzebna nam będzie lista zgodności sprzętu zawierająca listę urządzeń, które przeszły testy zgodności z systemem operacyjnym. Firma Microsoft bada sprzęt różnych producentów pod względem kompatybilności ze swoimi systemami serwerowymi. Podzespoły używane do budowy serwerów mają znacznie wyższe parametry pracy od elementów przeznaczonych

do zwykłych komputerów oraz zapewniają większą niezawodność. Najczęściej są również droższe, jednak dzięki ich użyciu serwer będzie pracował wydajnie i stabilnie. Producenci, których sprzęt pomyślnie przeszedł proces testowania i certyfikacji, mogą umieszczać informację o przeznaczeniu tych urządzeń do współpracy w wybranymi systemami serwerowymi.

Minimalne wymagania to parametry, które pozwalają zainstalować system. Jeśli nie zostaną spełnione, instalacja się nie powiedzie.

Konfiguracja zalecana to parametry, które pozwalają zainstalować system, chociaż nie gwarantują, że nie zgłosi ostrzeżeń.

Lista zgodności sprzętu (ang. *hardware compatibility list*, HCL) to baza danych podzespołów komputerowych oraz urządzeń peryferyjnych, które są kompatybilne z wybranym systemem operacyjnym. Dla systemów z rodziny Windows Server firma Microsoft przygotowała stronę *https://www.windowsservercatalog.com/*, na której można znaleźć listę sprzętu oraz gotowych serwerów.

Tabela 3.1. Parametry minimalne i zalecane Windows Server 2016/2019

Opis	Parametry minimalne	Parametry zalecane
Procesor	1,4 GHz	3,1 GHz lub szybszy
Architektura procesora	x86-64	x86-64
Pamięć operacyjna (RAM)	wersja 2016 — 512 MB bez trybu graficznego wersja 2019 — 1024 MB bez trybu graficznego	przy włączonym trybie graficznym — min. 4 GB
Ilość miejsca na dysku	32 GB	60 GB dla partycji systemowej

Nie musisz instalować systemu Windows Server zamiast systemu operacyjnego, z którego korzystasz na co dzień; warto w tym celu użyć maszyny wirtualnej (np. Oracle VirtualBox, Microsoft Hyper-V). Sposób jej konfiguracji został opisany w rozdziale 1. tego podręcznika.

Instalacja systemu operacyjnego jest bardzo ważną czynnością i nie powinna Ci sprawić większych problemów, gdyż przebiega podobnie jak instalacja systemów klienckich. Instalator Windows Server 2016 jest zbliżony do instalatora Windows 10, także różnice względem wcześniejszych wersji systemu są niewielkie.

Po pobraniu obrazu *.iso* wybranego systemu operacyjnego przystępujemy do instalacji serwera. Komputer musi być skonfigurowany do rozruchu z nośnika instalacyjnego, niezależnie od tego, czy będzie to płyta, obraz *.iso*, czy pamięć masowa USB. Trzeba pamiętać, aby podczas instalacji komputer był wyposażony w dwie karty sieciowe, które w późniejszych ćwiczeniach będą używane do symulowania środowiska pracy zarówno z siecią lokalną, jak i siecią internet.

Po uruchomieniu maszyny z zamontowanym obrazem *.iso* system zostaje wczytany z obrazu i jest wyświetlane okno instalatora, w którym wybieramy ustawienia regionalne instalacji oraz systemu (rysunek 3.1).

Rysunek 3.1. Ustawienia regionalne instalatora



ZAPAMIĘTAJ

Należy sprawdzić ustawienia regionalne, a szczególnie to, czy w ustawieniach klawiatury jest poprawnie wybrany język *Polski (programisty)*, aby później uniknąć problemów np. z hasłem, w którym zostały użyte polskie znaki.

Po naciśnięciu przycisku *Dalej* przechodzimy do następnego etapu instalacji. Możemy potwierdzić chęć instalacji przyciskiem *Zainstaluj teraz* lub wybrać opcję *Napraw komputer* (rysunek 3.2). Opcja naprawy pozwala rozwiązać problem — przywrócić wcześniej wykonaną kopię zapasową systemu bądź naprawić system z użyciem wiersza poleceń.

Rysunek 3.2. Potwierdzenie chęci zainstalowania systemu lub jego naprawy



Kliknięcie przycisku *Zainstaluj teraz* przenosi do następnego okna, w którym wybieramy wersję Windows: Server 2016 Standard lub Server 2016 Datacenter. Dodatkowo do wyboru mamy wersję ze **środowiskiem pulpitu** lub bez niego (rysunek 3.3).

Rysunek 3.3. Wybór systemu operacyjnego do zainstalowania



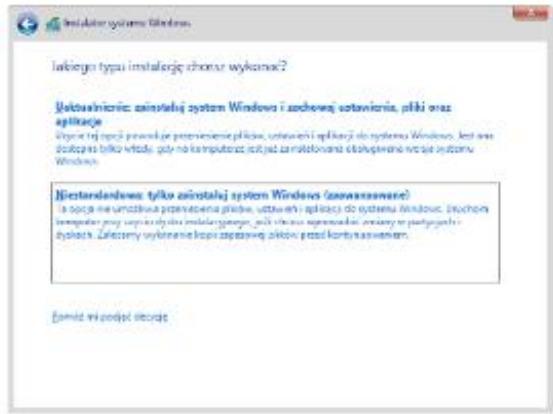
Windows Server 2016 Standard (środowisko pulpitu) — ta opcja jest przydatna, gdy wymagany jest graficzny interfejs użytkownika (GUI) do zapewnienia obsługi aplikacji, których nie można uruchamiać w instalacji **Server Core (bez środowiska pulpitu)**. Są w niej obsługiwane wszystkie role i funkcje serwera.

Windows Server 2016 Standard (popularnie nazywana Core bez trybu graficznego) — ta opcja pozwala zmniejszyć nakłady na zarządzanie systemem i jego obsługę, ponieważ instalowane są tylko składniki potrzebne do uruchamiania większości aplikacji i ról serwera. Graficzny interfejs użytkownika (GUI) nie jest instalowany, ale serwerem można w pełni zarządzać lokalnie lub zdalnie za pomocą programu Windows PowerShell lub innych narzędzi.

My wybierzemy opcję *Windows Server 2016 Standard (środowisko pulpitu)*.

Po wybraniu wersji systemu musimy zaakceptować uwagi i postanowienia licencyjne, aby rozpocząć dalszą instalację. W kolejnym oknie wybieramy typ instalacji: uaktualnienie lub instalację niestandardową. My wybierzemy typ instalacji *Niestandardowa: tylko zainstaluj system Windows (zaawansowane)*, gdyż instalujemy nowy serwer (rysunek 3.4).

Rysunek 3.4. Wybór typu instalacji



Opcja **uaktualnienia** jest dostępna tylko wtedy, kiedy zainstalowana jest już obsługiwana wersja systemu i użytkownik chce zachować jego ustawienia, niektóre role serwera i pliki lokalne z poprzednich wersji systemu. Pliki osobiste użytkownika zostaną przeniesione do folderu *Windows.old*.

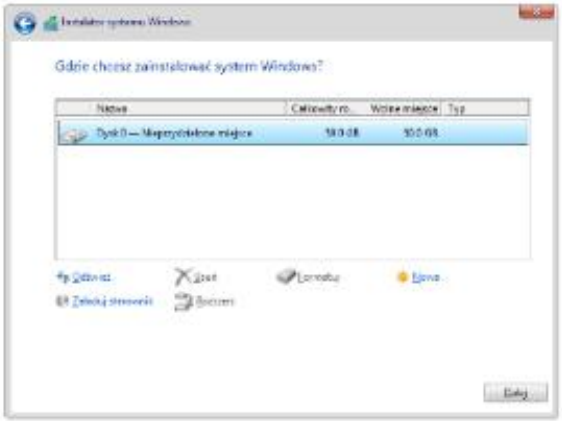
Opcję **instalacji niestandardowej** należy wybrać, jeśli na komputerze nie jest jeszcze zainstalowany system operacyjny, użytkownik chce usunąć wszystkie poprzednie wersje systemu i pliki lokalne albo nie jest możliwe uaktualnienie obecnie zainstalowanej wersji systemu. Ta opcja umożliwia partycjonowanie dysku twardego komputera.

UWAGA

Przeprowadzając uaktualnienie, musisz wykonać kopię zapasową plików na zewnętrznym nośniku danych lub w lokalizacji sieciowej. Musisz mieć wersje instalacyjne oraz klucze licencyjne oprogramowania, które zostanie ponownie zainstalowane w systemie. Jeśli przy logowaniu do systemu używane były czytniki linii papilarnych lub inne urządzenia biometryczne, pamiętaj o zanotowaniu haseł.

Następnym krokiem jest wybór miejsca, w którym zostanie przeprowadzona instalacja (rysunek 3.5). Na tym etapie możemy tworzyć nowe partycje oraz usuwać, formatować i rozszerzać już istniejące.

Rysunek 3.5. Okno wyboru miejsca instalacji systemu



ZAPAMIĘTAJ

Dodatkową opcją dostępną podczas instalacji jest *Załaduj sterownik*. Pozwoli ona zainstalować sterowniki producenta sprzętu, który nie jest widoczny w ramce wyboru dysku.

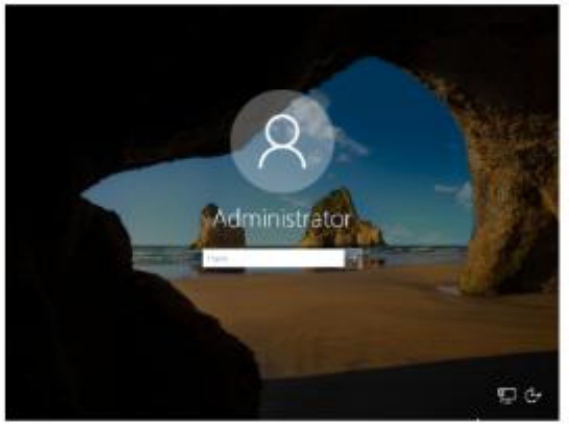
Po wykonaniu partycjonowania i wskazaniu partycji, na której ma być zainstalowany system, wybieramy *Dalej*. Rozpocznie się instalowanie systemu na wybranym nośniku. Proces instalacji trwa kilka minut i komputer zostanie w tym czasie parę razy ponownie uruchomiony. Na koniec instalator poprosi o dwukrotne wpisanie hasła dla konta *Administrator*. Następnie należy nacisnąć przycisk *Zakończ*, a wtedy proces instalacji systemu serwerowego się zakończy i zostanie wyświetlony ekran logowania.

UWAGA

Hasło konta *Administrator* powinno mieć co najmniej osiem znaków, składać się z małych i wielkich liter, cyfr oraz znaków specjalnych, a ponadto nie powinno tworzyć logicznej całości. Unikaj w hasłach imion, nazw i dat, które mogłyby się z Tobą kojarzyć. Im hasło jest trudniejsze do zapamiętania, tym trudniej będzie je złamać. Zapisz lub zapamiętaj hasło do konta *Administrator*, ponieważ bez niego nie będzie można się zalogować ani go zmienić.

Ekran logowania systemów serwerowych nie ma przycisku zasilania, przez co użytkownik niezalogowany nie może zamknąć systemu ani go ponownie uruchomić (rysunek 3.6). Wynika to z charakteru pracy serwera. Każde zamknięcie systemu, jak również jego ponowne uruchomienie wiąże się z podaniem powodu, dla którego się to robi, dzięki czemu administrator może to kontrolować.

Rysunek 3.6. Ekran logowania serwera



Zadania kontrolne

1. Wymień różnice między instalacją niestandardową a uaktualnieniem.
2. Wymień czynności, które trzeba wykonać podczas instalacji systemu Windows Server.
3. Przygotuj nośnik do zainstalowania systemu serwerowego na maszynie wirtualnej Oracle VirtualBox.
4. Zainstaluj system Windows Server.

3.2. Konfiguracja systemu Windows Server 2016/2019 po instalacji

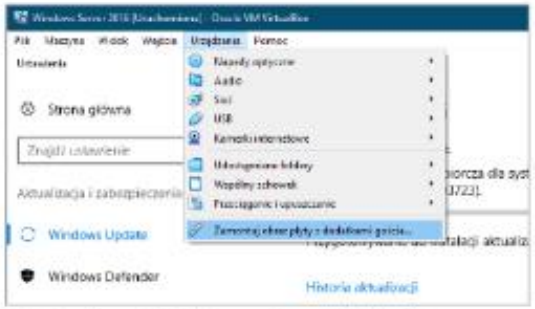
Po zainstalowaniu na maszynie wirtualnej Oracle VirtualBox systemu operacyjnego musimy wykonać kilka czynności, które zapewnią jego bezproblemowe i stabilne działanie.

Na początek warto zainstalować polski pakiet językowy. Klikamy *Start/Settings/Time & Language/Language*, a następnie wybieramy język polski (system zaproponuje go automatycznie), klikamy *Options* i w sekcji *Language Pack* przycisk *Download*. Pakiet zostanie pobrany i będzie aktywny po ponownym zalogowaniu się do systemu.

Następnie instalujemy dodatki gościa w Virtual Box i konfigurujemy w systemie karty sieciowe.

- *Dodatki gościa w VirtualBox (Guest Additions)* — instalacja tylko dla systemów pracujących w Oracle VirtualBox.

Dodatki gościa to opcjonalne oprogramowanie dla maszyn wirtualnych, które pozwoli uaktywnić dodatkowe funkcje Oracle VirtualBox: tryb pełnoekranowy, automatyczne rozszerzanie okna z systemem, przenoszenie plików przez przeciąganie, współdzielenie schowka oraz wiele innych. Aby zainstalować dodatki, w oknie maszyny wirtualnej należy kliknąć *Urządzenia/Zamontuj obraz płyty z dodatkami gościa…* (rysunek 3.7).



Rysunek 3.7. Instalacja Guest Additions w Oracle VirtualBox

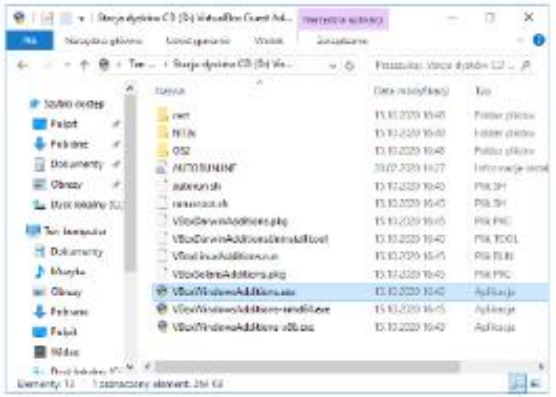
W systemie serwerowym zamontowany zostanie obraz płyty CD i to z niego będzie uruchamiany instalator, który poprowadzi nas przez proces instalacji (rysunek 3.8).

Instalator wymusi zainstalowanie dodatkowego sterownika o nazwie *Oracle Corporation Urządzenia systemowe*, który jest wymagany do obsługi dodatków. Taką samą instalację warto wykonać w przypadku Windows 10, który w dalszej części książki będzie nam służył jako system klienta. Na koniec instalator poprosi o ponowne uruchomienie komputera.

- *Konfiguracja kart sieciowych*

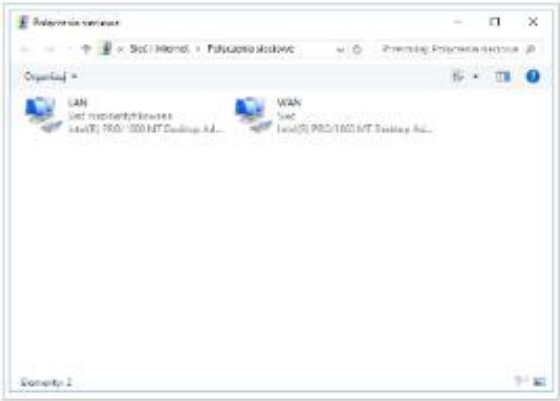
Aby można było korzystać z sieci, musimy skonfigurować karty sieciowe w naszym serwerze. Na samym początku założyliśmy, że będziemy używać dwóch kart sieciowych przeznaczonych, odpowiednio, do obsługi internetu (WAN) oraz sieci lokalnej (LAN). Zacznijmy od zmiany

Rysunek 3.8. Uruchomienie instalatora Guest Additions w Oracle VirtualBox



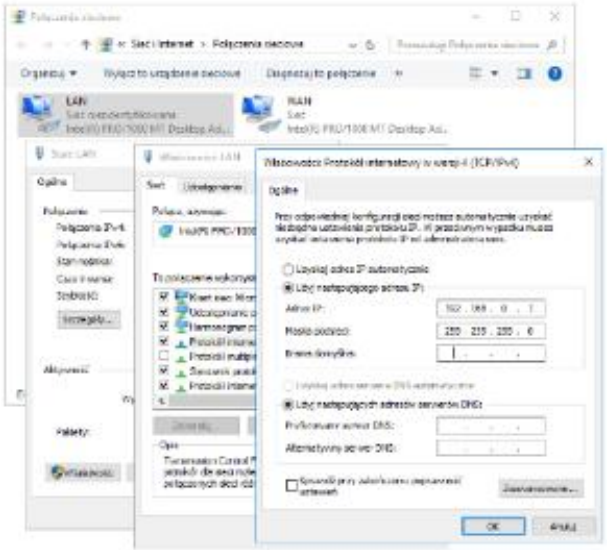
nazwy połączeń serwera, aby można w nim było rozróżnić interfejsy sieciowe. W tym celu klikamy *Start/Ustawienia/Sieć i internet/Ethernet/Zmień opcje karty*. Wybieramy pierwszą kartę, *Ethernet*, i klikamy prawym przyciskiem myszy, po czym z menu kontekstowego wybieramy *Zmień nazwę*. Pierwszy interfejs będzie służył do obsługi sieci internet, zatem nazwijmy go *WAN*, drugi zaś będzie używany do obsługi sieci lokalnej, dlatego nazwiemy go *LAN*. Poprawnie nazwane interfejsy przedstawia rysunek 3.9.

Rysunek 3.9. Nazwy interfejsów sieciowych



W Oracle VirtualBox w menu *Ustawienia* maszyny, na karcie *Sieć* możemy przypisać karty sieciowe: pierwszą (*Karta 1*) do *NAT*, a drugą (*Karta 2*) do *Sieć wewnętrzna*. NAT spowoduje automatyczne przypisanie konfiguracji sieciowej do interfejsu WAN, dzięki czemu uzyskamy w serwerze dostęp do sieci internet, a interfejs karty sieciowej wpiętej w sieć wewnętrzną utworzy wirtualny przełącznik, do którego w późniejszym czasie dołączymy klienta z systemem Windows 10.

Aby skonfigurować karty sieciowe, najpierw w oknie *Połączenia sieciowe* (w którym to zmienialiśmy nazwę połączenia, dostępnym po kliknięciu *Zmień opcje karty*) klikamy wybrany interfejs prawym przyciskiem myszy i wybieramy z menu *Właściwości*. Następnie wybieramy *Protokół internetowy w wersji 4 (TCP/IPv4)*, klikamy przycisk *Właściwości*, zaznaczamy *Użyj następującego adresu IP* i wpisujemy adres IP (rysunek 3.10). My użyjemy adresu `IP 192.168.0.1/24`. Na koniec naciskamy *OK*.



Rysunek 3.10. Konfiguracja interfejsu sieciowego

Teraz należy wykonać następujące czynności:

- **Aktywacja systemu** to proces, w którym potwierdzamy legalność używanego oprogramowania za pomocą klucza lub adresu e-mail. Aby aktywować produkt w Windows Server 2016/2019, należy wybrać przycisk *Start/Ustawienia/Aktualizacje i zabezpieczenia*, a następnie z menu po lewej stronie wybrać *Aktywacja*. Jeśli klucz produktu nie został dodany podczas instalacji systemu, w tym oknie można go wpisać i aktywować przyciskiem *Zmień klucz produktu*, aby w pełni legalnie korzystać z oprogramowania.
- **Pobranie aktualizacji** oznacza pobranie poprawek systemu, łat bezpieczeństwa, uaktualnionych sterowników oraz nowych funkcji w systemie Windows Server. Proces ten jest automatyczny i wymaga jedynie kliknięcia przycisku *Start/Ustawienia/Aktualizacje i zabezpieczenia*, co uruchomi wyszukiwanie dostępnych aktualizacji. Po sprawdzeniu wystarczy kliknąć *Zainstaluj teraz*, aby rozpoczął się proces aktualizacji. Ważną cechą systemów serwerowych, która odróżnia je od systemów klienckich, jest to, że po aktualizacji nie jest wymagane ponowne uruchomienie komputera w określonym czasie. To administrator decyduje, kiedy to nastąpi.

- **Instalowanie sterowników** to po każdej instalacji systemu operacyjnego jedna z najważniejszych czynności, które powinieneś wykonać. Bez sterowników urządzeń niektóre elementy komputera mogą nie działać lub działać błędnie. We współczesnych systemach operacyjnych większość sterowników zapewnia usługa aktualizacji systemu. Aby sprawdzić, czy wszystkie sterowniki zostały zainstalowane, wystarczy uruchomić menedżer zadań (kombinacją *Windows+X*).
- **Zmiana nazwy serwera** to operacja, która umożliwi rozpoznanie nazwy serwera w sieci. Nazwę serwera zmienia się tak samo jak nazwę komputera z systemem klienckim: wciskamy kombinację *Windows+R*, wpisujemy `sysdm.cpl`, klikamy przycisk *Zmień* i wprowadzamy nową nazwę. Na koniec zatwierdzamy przyciskiem *OK* i uruchamiamy komputer ponownie.

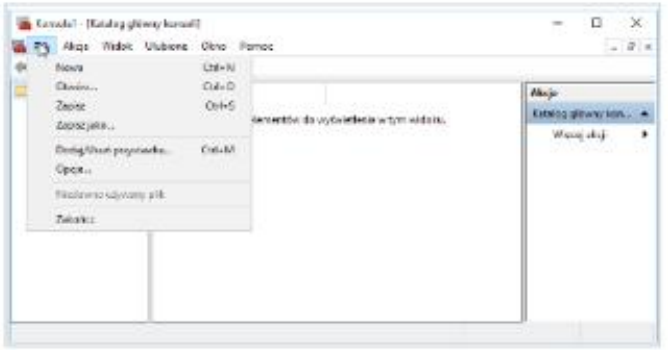
Wartym poznania narzędziem jest Microsoft Management Console (MMC), które ułatwia zarządzanie serwerem.

DEFINICJA

Microsoft Management Console (MMC) to składnik obecnych systemów Microsoft Windows zarówno w wersji konsumenckiej (Windows 10), jak i serwerowej (Windows Server 2016/2019), który zapewnia administratorom systemu i zaawansowanym użytkownikom interfejs do konfigurowania i monitorowania systemu.

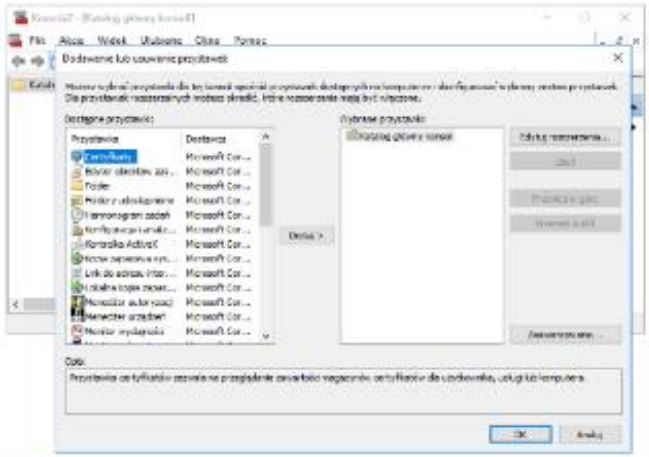
Konsola zarządzania może obsługiwać komponenty **modelu obiektowego** zwane **przystawkami**. Większość narzędzi administracyjnych firmy Microsoft jest zaimplementowana jako **przystawki MMC**, a inni producenci mogą wdrażać własne przystawki za pomocą interfejsów programistycznych **aplikacji MMC**.

Konsolę zarządzania uruchamiamy przez naciśnięcie przycisku *Start* i wpisanie `mmc`. Otworzy się puste okno konsoli, które pozwoli dodać wybrane przystawki (rysunek 3.11).



Rysunek 3.11. Konsola Microsoft Management Console

Aby dodać przystawkę do konsoli MMC, wystarczy wskazać ją na liście po lewej stronie okna, kliknąć *Dodaj*, a na koniec zatwierdzić wybór przyciskiem *OK* (rysunek 3.12).



Rysunek 3.12. Dodawanie przystawek do konsoli

Zadania kontrolne

1. Sprawdź, czy w systemie operacyjnym zainstalowane są wszystkie sterowniki.
2. Znajdź inne sposoby na zmianę nazwy serwera niż opisany w rozdziale i zmień jego nazwę.
3. Aktywuj swój system serwerowy.
4. Dodaj do konsoli MMC przystawkę do zarządzania komputerem.

3.3. Usługa Active Directory Domain Services (AD DS)

W tej części rozdziału zajmiemy się usługą katalogową Active Directory, którą zainstalujemy i skonfigurujemy. Najpierw omówimy podstawowe pojęcia, których znajomość przyda się w dalszej pracy.

DEFINICJA

Active Directory (AD) to rozszerzalna i skalowalna usługa katalogowa opracowana przez firmę Microsoft dla sieci domen Windows, dostępna w systemach operacyjnych Windows Server. Umożliwia wydajne zarządzanie zasobami sieci jako zestawem procesów i usług.

Usługa domenowa Active Directory (AD) jest hierarchiczną strukturą przechowującą informacje o obiektach w sieci. Zapewnia metody przechowywania danych katalogowych oraz udostępniania tych danych użytkownikom sieci i administratorom. Między innymi przechowuje informacje o kontach użytkowników, takie jak nazwiska, hasła i numery telefonów, oraz umożliwia innym autoryzowanym użytkownikom danej sieci dostęp do tych informacji. Te obiekty obejmują także współużytkowane zasoby, takie jak serwery, woluminy, drukarki oraz konta użytkowników i komputerów w sieci.

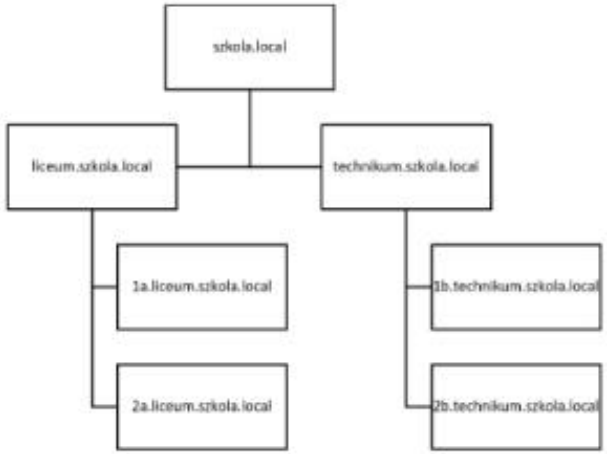
Usługa Active Directory zapewnia również funkcje bezpieczeństwa — uwierzytelnianie logowania i kontrolę dostępu do obiektów w katalogu. Po jednokrotnym zalogowaniu się w sieci administratorzy mogą zarządzać danymi katalogowymi organizacji, a jej autoryzowani użytkownicy mogą uzyskiwać dostęp do zasobów w dowolnym miejscu w jej obrębie. Administrowanie usługą opiera się na zasadach, które ułatwiają zarządzanie nawet najbardziej złożoną siecią.

Usługa Active Directory obejmuje również:

- Zestaw reguł i schematów, który definiuje klasy obiektów i atrybutów zawartych w katalogu, ograniczenia dotyczące instancji (kopii) tych obiektów oraz format ich nazw.
- Globalny katalog, który zawiera informacje na temat każdego zawartego w nim obiektu. Dzięki temu użytkownicy i administratorzy mogą znaleźć informacje o katalogu niezależnie od tego, która domena w nim faktycznie zawiera dane.
- Mechanizm zapytań i indeksów, dzięki któremu obiekty i ich właściwości mogą być publikowane i wyszukiwane przez użytkowników lub aplikacje sieciowe.
- Usługę replikacji, która dystrybuuje dane katalogowe w sieci. Wszystkie kontrolery domeny w domenie uczestniczą w replikacji i zawierają pełną kopię wszystkich danych o katalogu dla swoich domen. Wszelkie zmiany danych katalogu są replikowane na wszystkich kontrolerach domeny w domenie.

Active Directory ma strukturę hierarchiczną o kształcie drzewa. Omówimy teraz poszczególne jej elementy:

- **Domeny** — domena Active Directory jest grupą komputerów i użytkowników wykorzystujących wspólną bazę danych katalogowych. Nazwy tych domen muszą być unikatowe, a zatem nie mogą istnieć dwie takie same domeny, np. *szkola.local*, ale można utworzyć w domenie nadrzędnej *szkola.local* domeny potomne, np. *technikum.szkola.local* oraz *liceum.szkola.local*. Domena to także grupa komputerów połączonych w sieć wraz z serwerem pełniącym funkcję kontrolera domeny.
- **Drzewo domen** — domeny tworzące ciągłą strukturę nazw (przykład drzewa domen jest pokazany na rysunku 3.13). Domena główna *szkola.local* ma dwie domeny potomne — *liceum.szkola.local* oraz *technikum.szkola.local*, które z kolei mają własne poddomeny. Wszystkie te domeny są częścią jednego drzewa, gdyż mają główną domenę wspólną (korzeń) *szkola.local*.



Rysunek 3.13. Drzewo domen

- **Las domen** — składa się z co najmniej jednego drzewa. Każde z drzew, które są w lesie, ma własną, odrębną domenę. Domena nie może istnieć samodzielnie i potrzebuje do tego drzewa oraz lasu.
- **Jednostki organizacyjne** (ang. *organizational unit*, OU) — kontenery, czyli podgrupy wewnątrz domeny, które odzwierciedlają strukturę funkcjonalną organizacji. Można w nich umieszczać konta użytkowników, konta komputerów czy udostępnione zasoby. Jednostki organizacyjne mają kilka zalet, m.in.:
  - Umożliwiają przypisanie zasad grupy do mniejszych zbiorów zasobów, dzięki czemu nie trzeba stosować zasad dla całej domeny.
  - Pozwalają tworzyć mniejsze i łatwiejsze do zarządzania widoki obiektów katalogowych, co ułatwia i usprawnia zarządzanie użytkownikami.
  - Pozwalają na delegowanie uprawnień administracyjnych i łatwą kontrolę dostępu do zasobów domenowych. Dzięki temu można przyznać użytkownikowi uprawnienia do jednej jednostki organizacyjnej, ale nie do innych, a jednocześnie można innemu użytkownikowi nadać uprawnienia do wszystkich jednostek organizacyjnych.

  Windows Server ma domyślnie skonfigurowane jednostki organizacyjne, takie jak:
  - *Builtin* — zawiera domyślne grupy użytkowników, pełniące określone funkcje w systemie,
  - *Computers* — zawiera komputery dodane do domeny,
  - *Users* — zawiera użytkowników i grupy domeny.

- **Obiekt** — nazwany zbiór atrybutów, który określa w sieci np. użytkownika, komputer czy drukarkę.
- **Schemat** — zbiór wszystkich możliwych typów obiektów i danych, które można przechowywać w Active Directory.

W systemach Windows Server występują dwa rodzaje kont i grup użytkowników:

- **Konta użytkowników i grup lokalnych** — konta oraz grupy tworzone i przechowywane na lokalnym komputerze, które umożliwiają korzystanie z jego zasobów. Informacje na ich temat są przechowywane w lokalnej bazie **SAM** (ang. *Security Accounts Manager*). Konta lokalne tworzy się przy użyciu narzędzia *Użytkownicy i grupy lokalne*.
- **Konta użytkowników i grup domenowych** — konta oraz grupy tworzone i przechowywane w Active Directory, co umożliwia korzystanie z zasobów dowolnego serwera lub komputera klienckiego przyłączonego do domeny. Dzięki temu użytkownik może się logować i korzystać z komputerów w domenie, a administrator może nimi w bezpieczny i wygodny sposób zarządzać. Konta domenowe tworzy się za pomocą narzędzia *Użytkownicy i komputery usługi Active Directory*.

W usługach domenowych Active Directory (AD) istnieją dwa typy grup:

- **Grupy dystrybucyjne** — służą do tworzenia list dystrybucyjnych e-mail. Grup dystrybucyjnych można używać tylko z aplikacjami e-mail (takimi jak Exchange Server) do wysyłania wiadomości e-mail do użytkowników. Grupy dystrybucyjne nie mają włączonych zabezpieczeń, co oznacza, że nie mogą być wymienione na listach uznaniowej kontroli dostępu (ang. *discretionary access control lists*, DACL).
- **Grupy zabezpieczeń** — służą do przypisywania uprawnień do współdzielonych zasobów. Grupy zabezpieczeń mogą zapewnić skuteczny sposób przydzielania dostępu do zasobów w sieci. Z wykorzystaniem grup zabezpieczeń można:
  - Przypisać prawa użytkownika do grup zabezpieczeń w usłudze Active Directory. Prawa użytkownika przypisuje się do grupy zabezpieczeń, aby określić, co członkowie tej grupy mogą zrobić w zakresie domeny lub lasu. Prawa użytkownika są automatycznie przypisywane do niektórych grup zabezpieczeń po zainstalowaniu usługi Active Directory, aby pomóc administratorom w zdefiniowaniu roli administracyjnej osoby w domenie. Dla przykładu: użytkownik dodany do grupy *Operatorzy kopii zapasowych* w usłudze Active Directory ma możliwość tworzenia kopii zapasowych oraz przywracania plików i katalogów znajdujących się na wszystkich kontrolerach w domenie. Jest to możliwe, ponieważ domyślnie prawa użytkownika *Kopia zapasowa plików i katalogów* oraz *Przywróć pliki i katalogi* są automatycznie przypisywane do grupy *Operatorzy kopii zapasowych*. Dlatego członkowie tej grupy dziedziczą prawa użytkownika przypisane do tej grupy.
  - Przypisać uprawnienia użytkownika do grup zabezpieczeń dla zasobów. Uprawnienia są przypisywane do grupy zabezpieczeń dla udostępnionego zasobu. Uprawnienia określają, kto może uzyskać dostęp do zasobu, i poziom dostępu, np. *Pełna*

kontrola. Niektóre uprawnienia ustawione dla obiektów domeny są przypisywane automatycznie, aby umożliwić różne poziomy dostępu do domyślnych grup zabezpieczeń, takich jak grupa *Operatorzy kont* lub grupa *Administratorzy domeny*.

Grupy zabezpieczeń są wymienione na listach uznaniowej kontroli dostępu (DACL), które definiują uprawnienia do zasobów i obiektów. Administratorzy, przypisując uprawnienia do zasobów i obiektów (udziałów plików, drukarek itp.), powinni przypisać je do grupy zabezpieczeń, a nie do poszczególnych użytkowników. Uprawnienia są przypisywane raz (grupie), a nie kilka razy (każdemu użytkownikowi z osobna). Każde konto dodane do grupy otrzymuje prawa przypisane do tej grupy w usłudze Active Directory, a użytkownik otrzymuje uprawnienia zdefiniowane dla tej grupy.

Podobnie jak grupy dystrybucyjne, grupy zabezpieczeń mogą być używane jako adresaci e-mail. Wysłanie wiadomości e-mail do grupy powoduje wysłanie wiadomości do wszystkich jej członków.

3.4. Kontroler domeny

Teraz zainstalujemy na naszym serwerze usługę Active Directory Domain Services (AD DS) i promujemy nasz serwer do roli kontrolera domeny. Dobrą praktyką jest instalacja Active Directory oraz promowanie serwera do roli kontrolera domeny zaraz po zainstalowaniu systemu Windows Server 2016/2019.

DEFINICJA

Kontroler domeny (DC) to serwer w sieci, który odpowiada za umożliwienie hostowi dostępu do zasobów domeny. Uwierzytelnia użytkowników, przechowuje informacje o koncie użytkownika i egzekwuje zasady bezpieczeństwa dla domeny.

W małych sieciach wystarcza jeden kontroler domeny. Aby zagwarantować użytkownikom możliwość logowania się do sieci w razie awarii oraz zwiększyć bezpieczeństwo i niezawodność działania, dobrze jest użyć co najmniej dwóch kontrolerów domeny. Podczas instalacji musimy zainstalować także serwer DNS, który jest wymagany do działania kontrolera domeny. My na potrzeby ćwiczeń użyjemy — także ze względu na ograniczone możliwości — tylko jednego serwera, z jednym kontrolerem domeny.

Instalacja ról i funkcji w Windows Server 2016 i Windows Server 2019 przebiega w identyczny sposób. Po zalogowaniu do systemu automatycznie uruchamia się okno Menedżera serwera, w którym to będziemy kontrolować stan serwera oraz zarządzać wszystkimi uruchomionymi na nim usługami i rolami.

Spróbujmy zobrazować sytuację po zainstalowaniu kontrolera domeny na przykładzie szkoły. Załóżmy, że szkoła ma kilka pracowni komputerowych oraz komputer w każdej sali. W każdej pracowni uczeń zajmuje zawsze to samo miejsce, gdyż na lokalnym koncie ma zapisane

swoje prace, i często się zdarza, że jego dokumenty są usuwane przez innych użytkowników, ponieważ wszyscy korzystają z tego samego konta. Nauczyciele do komputerów w salach logują się kontem lokalnym. Wszyscy użytkownicy są w stanie podejrzeć historię działań danego komputera i jeśli któryś zapisał hasło w przeglądarce, istnieje ryzyko, że zostanie wykorzystane przez inne osoby. Administrator nie ma żadnej kontroli nad komputerami; co więcej, próba przeinstalowania systemu na każdym z komputerów to ogromna i czasochłonna praca. Po zainstalowaniu usług domenowych komputery będą zarządzane z centralnego punktu — serwera, w sieci będą pracować tylko komputery, które dołączymy do domeny, dzięki czemu zwiększy się bezpieczeństwo sieci, a każdy użytkownik będzie miał indywidualny login i własne hasło, co pozwoli uniknąć niebezpiecznych sytuacji i umożliwi administratorowi nadzorowanie użytkowników. Zamieszczone poniżej ćwiczenia przedstawiają sposób instalacji i konfiguracji kontrolera domeny.

Ćwiczenie 3.1

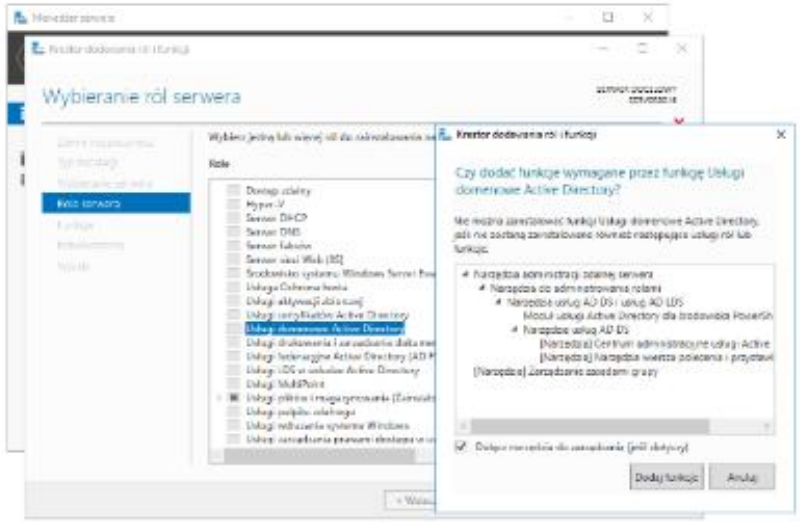
Instalacja Active Directory oraz promowanie serwera do roli kontrolera domeny.

W tym ćwiczeniu zainstalujemy Active Directory wraz z zestawem narzędzi do zarządzania domeną i zasadami grupy. Do celów instalacji posłużymy się domeną *szkola.local*. Hasło użyte do instalacji to *Q@wertyuiop*.

1. Mając uruchomione okno Menedżera serwera, wybieramy *Dodaj role i funkcje*, co uruchomi kreatora instalacji. Kreator poprowadzi nas przez proces instalacji w bardzo prosty sposób. Należy pamiętać o czytaniu komunikatów, które wyświetla instalator.
2. Kreator rozpoczyna od wyświetlenia karty *Zanim rozpoczniesz*, na której zostaniemy zapytani, czy konto *Administrator* ma silne hasło, czy został wpisany statyczny adres IP w interfejsie sieciowym oraz czy zainstalowaliśmy aktualizacje systemu. Wszystkie te czynności zostały omówione w podrozdziale 3.2, „Konfiguracja systemu Windows Server 2016/2019 po instalacji". Następnie klikamy *Dalej* i przechodzimy do kolejnej karty.
3. Wybieramy teraz typ instalacji. Do wyboru są dwa typy:
   - *Instalacja oparta na rolach lub oparta na funkcjach* — pozwoli skonfigurować pojedynczy serwer przez dodanie do niego ról i funkcji,
   - *Instalacja usług pulpitu zdalnego* — wymagana we wdrożeniach opartych na maszynach wirtualnych.

   Zaznaczamy *Instalacja oparta na rolach lub oparta na funkcjach*, gdyż konfigurować będziemy rzeczywisty serwer, i naciskamy *Dalej*.
4. W karcie *Wybieranie serwera docelowego* wybieramy z listy serwer — będzie dostępny pod nazwą domyślną lub zmienioną przez użytkownika. Oprócz nazwy jest wyświetlany adres IP serwera oraz wersja zainstalowanego systemu operacyjnego. Wskazujemy serwer i naciskamy *Dalej*.
5. Na karcie *Wybieranie ról serwera* zaznaczamy wybrane role, czyli *Usługi domenowe Active Directory*.

6. Otworzy się dodatkowa karta, *Wybieranie funkcji*. Kreator proponuje instalację dodatkowych funkcji, takich jak *Narzędzia administracji zdalnej serwera*, które zawierają przystawki i narzędzia wiersza poleceń służące do zarządzania zdalnego rolami i funkcjami, oraz *Zarządzanie zasadami grupy*, czyli przystawkę Microsoft Management Console (MMC), która udostępnia standardowe narzędzia administracyjne do zarządzania zasadami grupy w całej organizacji. Aby przejść do kolejnego kroku, naciskamy *Dodaj funkcje*, a następnie *Dalej* (rysunek 3.14).



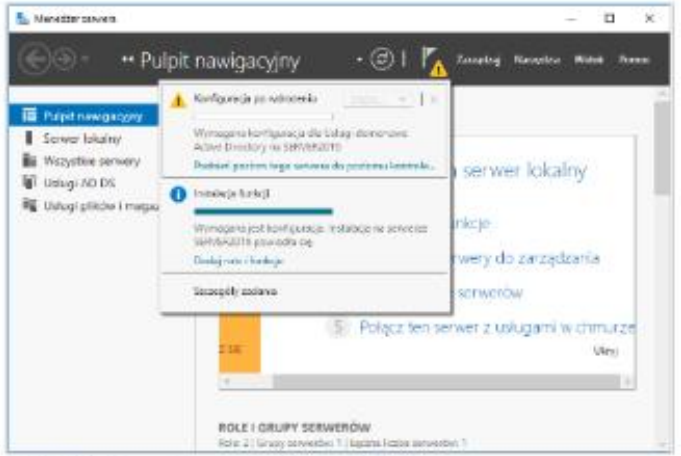
Rysunek 3.14. Wybór ról serwera

7. Karta *Usługi domenowe Active Directory* służy do konfiguracji narzędzia Azure Active Directory Connect, dzięki któremu użytkownicy mogą np. logować się do lokalnej sieci przy użyciu tych samych poświadczeń co do usługi Microsoft 365 i na odwrót. My nie będziemy go konfigurować, dlatego od razu naciskamy przycisk *Dalej*.
8. *Potwierdzenie opcji instalacji* to karta podsumowująca instalację. Zawiera ustawienie *Automatycznie uruchom ponownie serwer docelowy, jeśli będzie to potrzebne*. Jeśli to ustawienie zostanie zaznaczone, w razie potrzeby w trakcie instalacji będzie możliwe automatyczne ponowne uruchomienie systemu. Na tym etapie instalacji, gdy serwer nie jest jeszcze maszyną produkcyjną, możemy na to pozwolić, aby uniknąć późniejszych komplikacji. Warto pamiętać, że serwery wymagają ponownego uruchomienia tylko wtedy, gdy jest to naprawdę konieczne. Jeśli wszystkie opcje są ustawione zgodnie z zamierzeniem, możemy nacisnąć przycisk *Zainstaluj*, a wówczas rozpocznie się proces instalacji.
9. Ostatnia karta instalatora, *Postęp instalacji*, pozwala podejrzeć, co w danym momencie jest instalowane. Na dole znajduje się przycisk *Zamknij*, który zamyka kartę postępu (instalacja będzie trwała).

Zakończyliśmy proces instalacji Active Directory Domain Services (AD DS). Teraz czas, aby podnieść poziom serwera do poziomu kontrolera domeny. Zrobimy to w ćwiczeniu 3.2.

Ćwiczenie 3.2

1. W Menedżerze serwera po zainstalowaniu AD DS pojawia się żółty trójkąt ostrzegawczy. To tzw. menu akcji, które informuje o tym, że mamy coś do wykonania. Po kliknięciu tej ikony zostanie wyświetlone zadanie przeprowadzenia konfiguracji po wdrożeniu. Klikamy je, aby rozpocząć konfigurowanie usług domenowych Active Directory (rysunek 3.15).

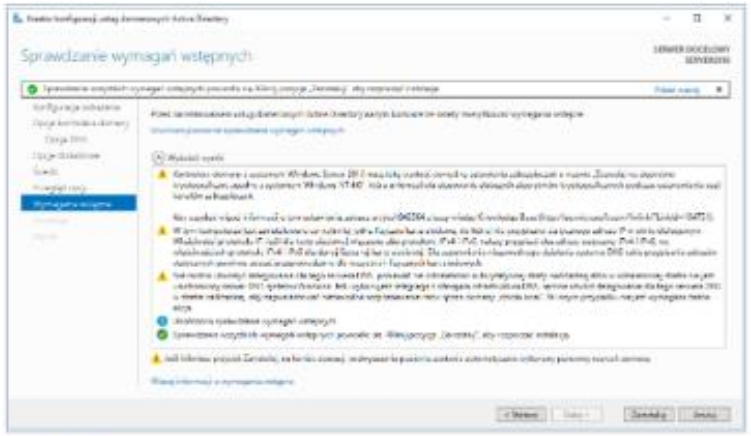


Rysunek 3.15. Konfiguracja po wdrożeniu AD DS

2. Teraz następuje *Konfiguracja wdrażania*, czyli dodajemy nowy las (*Dodaj nowy las*), wpisujemy nazwę domeny głównej *szkola.local* oraz naciskamy *Dalej*.
3. Zostaje wyświetlone okno *Opcje kontrolera domeny*, w którym ustawiamy poziom funkcjonalności lasu i domeny na najwyższy możliwy, gdyż nie jest dostępny w sieci żaden niższy kontroler domeny. Kreator podpowiada nam konieczność zainstalowania serwera DNS oraz prosi o wpisanie hasła dla trybu przywracania usług katalogowych. **Tryb przywracania usług katalogowych** (DSRM) pozwoli nam w razie awarii naprawić usługę Active Directory. Naciskamy *Dalej*.
4. Zostaje wyświetlona karta *Opcje DNS*, czyli ustawienia serwera, który nie jest zainstalowany, o czym informuje nas komunikat ostrzegawczy. Naciskamy *Dalej*.
5. Teraz w karcie *Opcje dodatkowe* podajemy nazwę NetBIOS naszej domeny. Ta nazwa służy do współdziałania ze starszymi komputerami i usługami i można ją zmienić. System proponuje nam nazwę *SZKOLA*. Następnie klikamy *Dalej*.
6. Ścieżki — system proponuje nam ścieżki dla folderów bazy danych AD DS, plików dziennika oraz *SYSVOL*, czyli folderu, w którym przechowywane są pliki publiczne

domeny znajdujące się na serwerze. Folder *SYSVOL* jest replikowany do wszystkich kontrolerów domeny w obrębie danej domeny. My, ponieważ mamy tylko jeden dysk twardy, pozostawiamy domyślne ustawienia folderów i klikamy *Dalej*.

7. Karta *Przegląd opcji* zawiera podsumowanie konfiguracji, jaką zamierzamy wprowadzić. W tym miejscu można się cofnąć do wcześniejszych kart kreatora, by coś zmienić, lub kontynuować proces konfiguracji przez kliknięcie *Dalej*.
8. Następuje sprawdzenie wymagań wstępnych, czyli konfiguracji, którą zaplanowaliśmy do wdrożenia. Jeśli zakończy się powodzeniem, powinniśmy uzyskać informację, że możemy rozpocząć instalowanie (rysunek 3.16). Pozostaje kliknąć przycisk *Zainstaluj*. System podczas instalacji uruchomi się ponownie automatycznie.



Rysunek 3.16. Instalacja kontrolera domeny

9. Po ponownym uruchomieniu serwera będziemy mogli zalogować się do domeny *szkola.local* (rysunek 3.17).



Rysunek 3.17. Logowanie do serwera po zainstalowaniu Active Directory

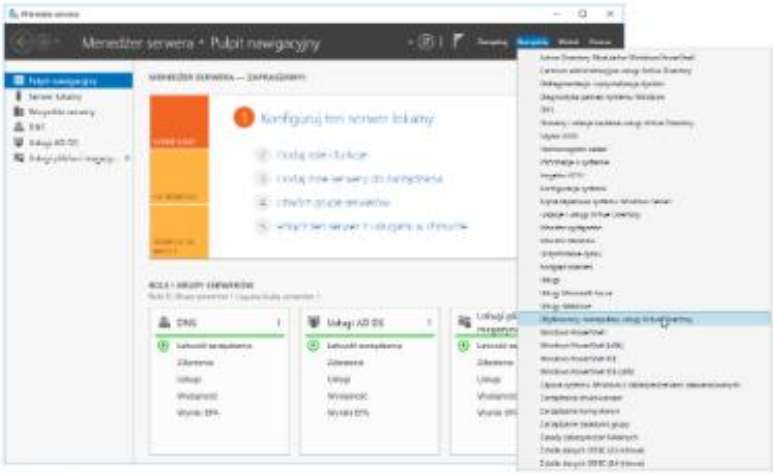
Zadania kontrolne

1. Zainstaluj samodzielnie Active Directory Domain Services i podnieś poziom serwera do roli kontrolera domeny z wykorzystaniem domeny *TwojeNazwisko.local*.
2. Omów, co to jest kontroler domeny.

3.5. Tworzenie kont użytkowników i jednostek organizacyjnych w domenie oraz zarządzanie nimi

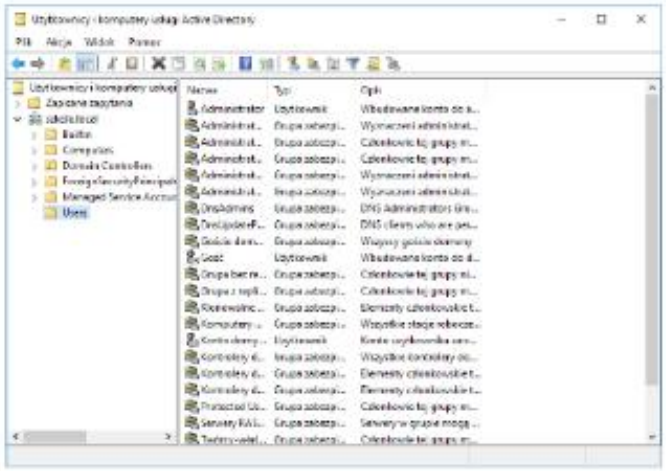
Każdy użytkownik, który łączy się za pomocą domeny, musi mieć w Active Directory swoje konto. W ten sposób uczniowie i nauczyciele w szkole otrzymają indywidualne loginy i hasła, dzięki czemu będą mogli logować się do dowolnych komputerów, które zostaną dołączone do szkolnej domeny. Teraz ich dokumenty zostaną zsynchronizowane i nie będą usuwać sobie nawzajem plików. Ustawienia przeglądarek czy też systemu będą zachowywane i synchronizowane z serwerem, a administrator będzie mógł np. ustalić, w jakich godzinach wybrany użytkownik może się logować. Sposoby tworzenia kont użytkowników oraz jednostek organizacyjnych zostaną przedstawione w poniższych ćwiczeniach.

Do zarządzania kontami służy przystawka *Użytkownicy i komputery usługi Active Directory*, którą można uruchomić przez wybranie w Menedżerze serwera *Narzędzia/Użytkownicy i komputery usługi Active Directory* (rysunek 3.18).



Rysunek 3.18. Uruchamianie przystawki Użytkownicy i komputery usługi Active Directory

Przystawkę *Użytkownicy i komputery usługi Active Directory* przedstawia rysunek 3.19. Spróbujmy teraz dodać konto użytkownika oraz je zmodyfikować.

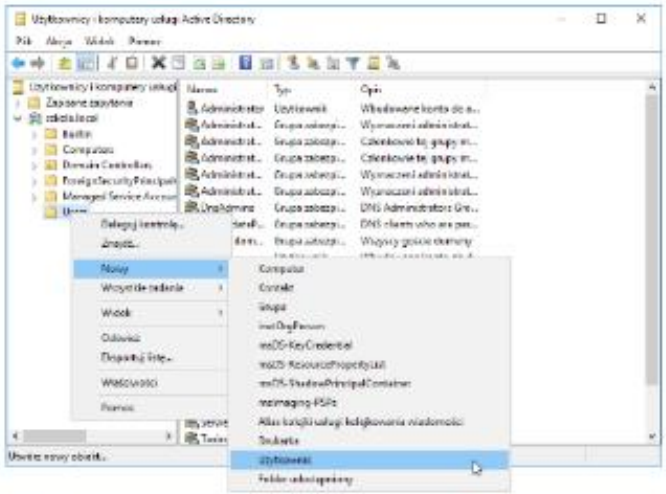


Rysunek 3.19. Przystawka Użytkownicy i komputery usługi Active Directory

Ćwiczenie 3.3

Tworzenie oraz modyfikowanie kont użytkowników.

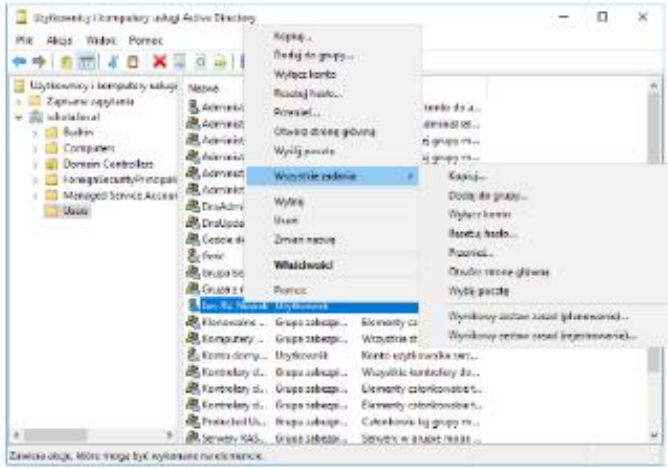
1. Uruchamiamy przystawkę *Użytkownicy i komputery usługi Active Directory*.
2. Rozwijamy domenę *szkola.local* i klikamy prawym przyciskiem myszy kontener *Users*.
3. Wybieramy *Nowy/Użytkownik* (rysunek 3.20).



Rysunek 3.20. Dodawanie nowego użytkownika

4. Uzupełniamy dane o użytkowniku. Użyjmy przykładowych danych:
   - imię: `Jan`,
   - nazwisko: `Nowak`,
   - inicjały: `JN`,
   - pełna nazwa, czyli wyświetlana nazwa konta: `Jan JN. Nowak`,
   - nazwa logowania użytkownika: `jan.nowak@szkola.local`,
   - nazwa logowania użytkownika (w systemach starszych od Windows 2000): `jan.nowak`.

   Po wpisaniu danych klikamy *Dalej*.
5. Uzupełniamy dane dotyczące hasła oraz ustawiamy dostępne opcje:
   - *Hasło* oraz *Potwierdź hasło* — hasło wpisujemy dwa razy, by potwierdzić jego poprawność.
   - *Użytkownik musi zmienić hasło przy następnym logowaniu* — zmusza użytkownika do zmiany hasła przy następnym logowaniu do sieci. Włącz tę opcję, jeśli chcesz mieć pewność, że użytkownik będzie jedyną osobą znającą hasło.
   - *Użytkownik nie może zmienić hasła* — zapobiega zmianie hasła przez użytkownika. Włącz tę opcję, jeśli chcesz zachować kontrolę nad kontem użytkownika, takim jak konto gościa lub tymczasowe.
   - *Hasło nigdy nie wygasa* — spowoduje pominięcie zasad dotyczących haseł i hasło do tego konta nie wygaśnie.
   - *Konto jest wyłączone* — zapobiega logowaniu się przy użyciu wybranego konta. Wielu administratorów korzysta z wyłączonych kont jako szablonów do tworzenia kont użytkowników.
6. Klikamy *Dalej* i tym samym przechodzimy do podsumowania tworzonego konta. Następnie wybieramy *Zakończ* i sprawdzamy, czy w zakładce *Users* pojawiło się utworzone przez nas konto.
7. Aby zmodyfikować konto użytkownika, klikamy je prawym przyciskiem myszy. W menu kontekstowym mamy do wyboru szereg opcji (rysunek 3.21).
8. Najważniejsze opcje występujące w menu podręcznym obiektu typu *User* to:
   - *Kopiuj...* — utworzenie nowego obiektu przy użyciu obiektu kopiowanego,
   - *Dodaj do grupy...* — bezpośrednie dodanie konta użytkownika do grupy zabezpieczeń,
   - *Wyłącz konto...* — wyłączenie konta bez jego usuwania, co pozwala czasowo wyłączyć konto, a następnie je włączyć,
   - *Resetuj hasło...* — zmiana hasła i odblokowanie konta użytkownika,
   - *Przenieś...* — przenoszenie obiektów między kontenerami,
   - *Wytnij* — wycięcie obiektu z kontenera,

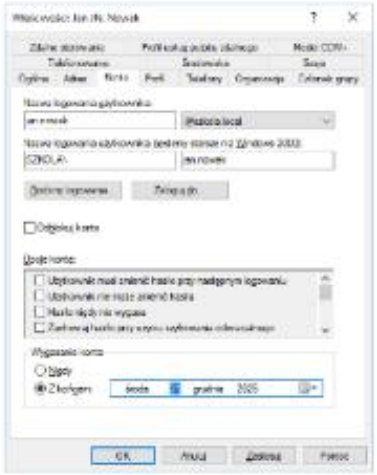


Rysunek 3.21. Menu użytkownika

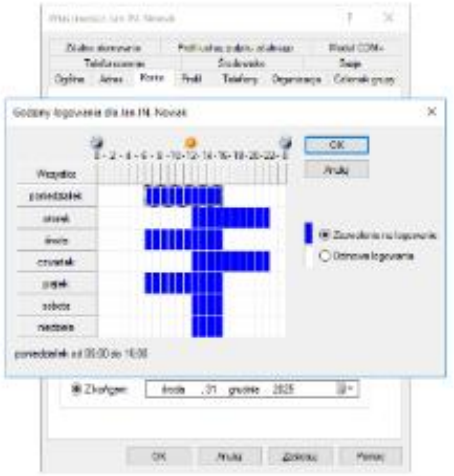
- *Usuń* — usunięcie obiektu z kontenera,
- *Zmień nazwę* — zmiana nazwy przez otwarcie okna do wykonania zmian,
- *Właściwości* — otwarcie okna konfiguracji użytkownika, którego poszczególne elementy omówimy także w dalszych podrozdziałach podręcznika,
- *Pomoc* — otwarcie strony WWW dotyczącej pomocy związanej z obsługą serwera.

9. Wybieramy *Właściwości*, a następnie otwieramy kartę *Konto*, na której ustawiamy datę wygaśnięcia konta na 31 grudnia 2025 roku (rysunek 3.22).

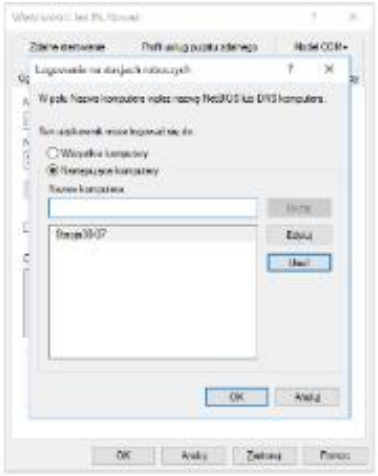
Rysunek 3.22. Ustawienie daty wygaśnięcia konta



10. Klikamy *Godziny logowania* oraz ustalamy dni tygodnia i godziny, w których użytkownik może się logować do domeny (rysunek 3.23). Zaznaczamy na niebiesko godziny, w których będzie możliwość logowania, i na biało godziny, w których nie będzie to możliwe, a na koniec zatwierdzamy wybór przyciskiem *OK*. My na potrzeby ćwiczenia ustawiliśmy następujące godziny logowania: poniedziałek, środa, piątek — od 6:00 do 16:00; wtorek, czwartek — od 12:00 do 22:00; sobota, niedziela — od 12:00 do 16:00.
11. Po kliknięciu *Zaloguj do...* możemy określić, do których komputerów w sieci dany użytkownik może się logować, lub pozwolić mu na logowanie do wszystkich komputerów. Na koniec klikamy *OK*, aby zatwierdzić wybór. My ustawimy użytkownikowi możliwość logowania tylko do komputera o nazwie *Stacja30-07* (rysunek 3.24).



Rysunek 3.23. Ustawienie dni i godzin logowania użytkownika



Rysunek 3.24. Wybór komputerów, do których użytkownik może się logować

W zakładce *Właściwości/Konto* możemy też odblokować zablokowane konto.

Tworzyć i usuwać konta użytkowników można także za pomocą konsoli Windows PowerShell:

- `dsadd` — pozwala tworzyć obiekty w kontenerach domeny:

```
dsadd user nazwa_obiektu_DN [przełączniki]
```

- `dsrm` — pozwala usuwać obiekty w kontenerach domeny:

```
dsrm nazwa_obiektu_DN
```

W poleceniu `dsadd` możemy użyć szeregu przełączników, m.in.:

- `-fn` (ang. *first name*) — imię użytkownika,
- `-ln` (ang. *last name*) — nazwisko użytkownika,

- `-upn` (ang. *user principal name*) — nazwa logowania,
- `-pwd` (ang. *password*) — hasło użytkownika,
- `-mustchpwd [yes | no]` (ang. *must change password*) — wymuszenie na użytkowniku zmiany hasła,
- `-disabled [yes | no]` — konto włączone lub wyłączone,
- `-canchpwd [yes | no]` (ang. *can change password*) — użytkownik może zmienić hasło (trzeba ustawić `yes`, jeśli użyło się przełącznika `-mustchpwd`),
- `-pwdneverexpires [yes | no]` (ang. *password never expires*) — hasło nie wygasa.

Oba polecenia mają jeszcze więcej przełączników, które można znaleźć w dokumentacji dostępnej na stronie producenta.

Teraz spróbujemy utworzyć za pomocą polecenia w Windows PowerShell nowego użytkownika w domenie, a następnie go usunąć.

Ćwiczenie 3.4

1. Uruchamiamy konsolę Windows PowerShell. Aby to zrobić, klikamy *Start*, wpisujemy `PowerShell`, by odnaleźć aplikację Windows PowerShell, i uruchamiamy ją.
2. Po uruchomieniu aplikacji musimy wpisać polecenie tworzące użytkownika o nazwie *Jacek JK. Kowalski* z hasłem *zaq1@WSX*, z przełącznikiem wymuszającym zmianę hasła przez użytkownika (rysunek 3.25).

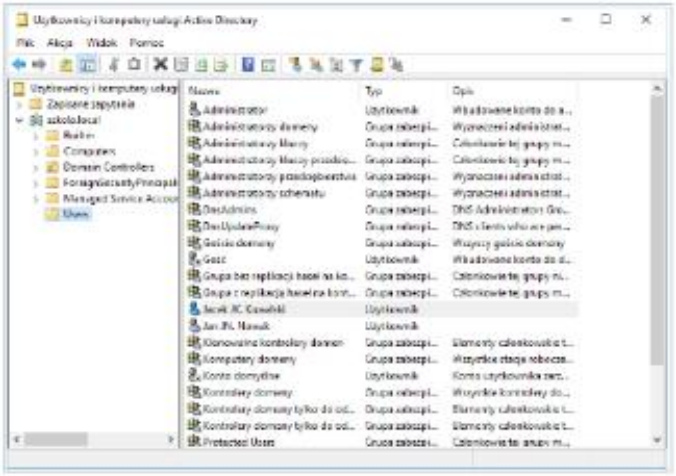
   ```
   dsadd user "CN=Jacek JK. Kowalski, CN=Users, DC=szkola, DC=local" -fn
   Jacek -ln Kowalski -upn jacek.kowalski -pwd zaq1@WSX -mustchpwd yes
   -canchpwd yes -pwdneverexpires yes -disabled no
   ```



Rysunek 3.25. Wykonanie polecenia dsadd — dodanie użytkownika domeny

   - `CN` (ang. *common name*) — nazwa tworzonego użytkownika (`CN=Jacek JK. Kowalski`), nazwa kontenera, w którym znajdzie się użytkownik (`CN=Users`),
   - `DC` (ang. *domain component*) — komponent domeny *szkola.local* (`DC=szkola, DC=local`).
3. Sprawdzamy w przystawce *Użytkownicy i komputery usługi Active Directory*, czy w kontenerze *Users* został utworzony nowy użytkownik *Jacek JK. Kowalski* (rysunek 3.26).

Rysunek 3.26. Sprawdzenie, czy został utworzony nowy użytkownik



4. Teraz usuniemy nowo utworzonego użytkownika poleceniem `dsrm`. Wpisujemy polecenie:

   ```
   dsrm "CN=Jacek JK. Kowalski, CN=Users, DC=szkola, DC=local"
   ```
5. System zapyta, czy na pewno usunąć użytkownika. Potwierdzamy klawiszem *Y*, a wtedy użytkownik zostanie usunięty (rysunek 3.27).



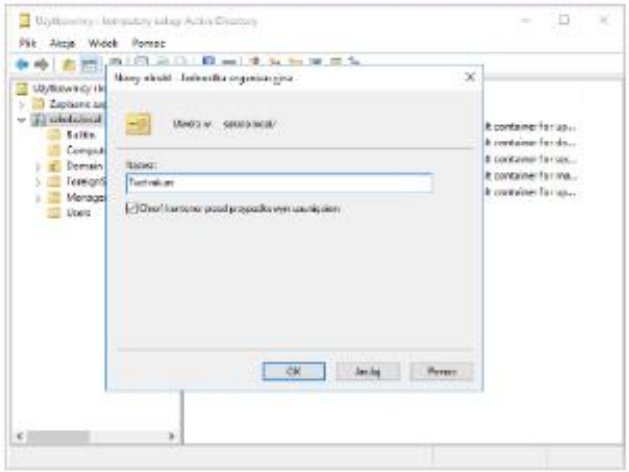
Rysunek 3.27. Usuwanie konta użytkownika za pomocą konsoli Windows PowerShell i polecenia dsrm

Pokazaliśmy, jak utworzyć i usunąć użytkowników na dwa różne sposoby. Teraz utworzymy jednostkę organizacyjną *Technikum*, a następnie pokażemy, jak ją usunąć.

Ćwiczenie 3.5

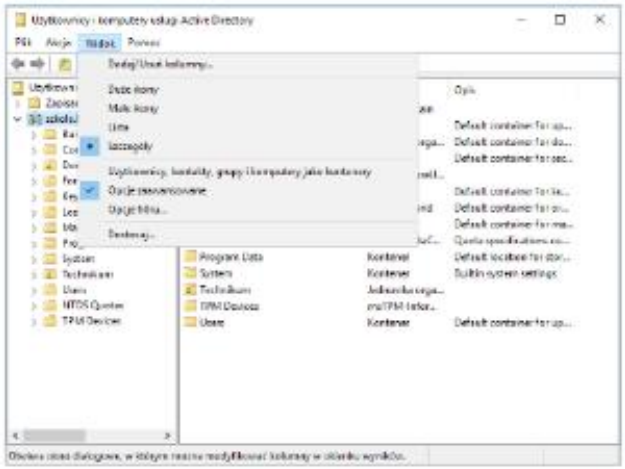
1. Uruchamiamy przystawkę *Użytkownicy i komputery usługi Active Directory*.
2. Rozwijamy domenę *szkola.local* i klikamy ją prawym przyciskiem myszy.
3. Wybieramy *Nowy/Jednostka organizacyjna*, wpisujemy nazwę `Technikum` i potwierdzamy przyciskiem *OK* (rysunek 3.28). Zwróćmy uwagę na opcję *Chroń kontener przed przypadkowym usunięciem*, która zablokuje możliwość przypadkowego usunięcia jednostki organizacyjnej, a wraz z nią zawartości tej jednostki.

Rysunek 3.28. Tworzenie nowej jednostki organizacyjnej



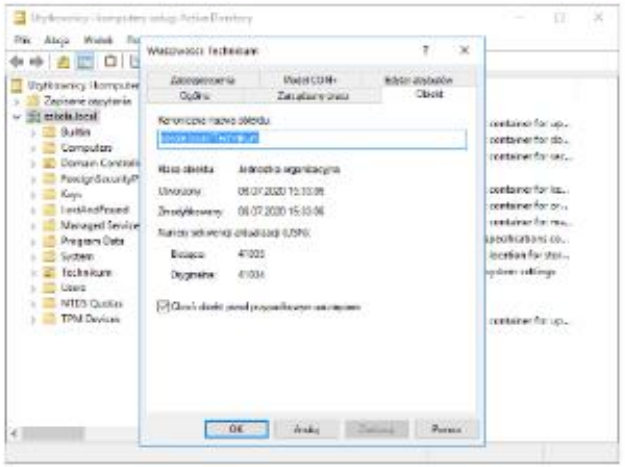
4. Aby usunąć jednostkę organizacyjną, wystarczy ją kliknąć prawym przyciskiem myszy i wybrać *Usuń*, a następnie potwierdzić zamiar. Jeśli wcześniej została zaznaczona opcja ochrony, musimy w przystawce *Użytkownicy i komputery usługi Active Directory* kliknąć *Widok* i zaznaczyć *Opcje zaawansowane* (rysunek 3.29).

Rysunek 3.29. Włączanie opcji zaawansowanych w przystawce



5. Klikamy prawym przyciskiem myszy wybraną jednostkę organizacyjną i wybieramy *Właściwości*, następnie otwieramy kartę *Obiekt* i usuwamy zaznaczenie opcji *Chroń obiekt przed przypadkowym usunięciem*, a na koniec zatwierdzamy przyciskiem *OK* (rysunek 3.30). Teraz możemy po kliknięciu prawym przyciskiem myszy usunąć jednostkę organizacyjną.

Rysunek 3.30. Odblokowanie ochrony jednostki organizacyjnej

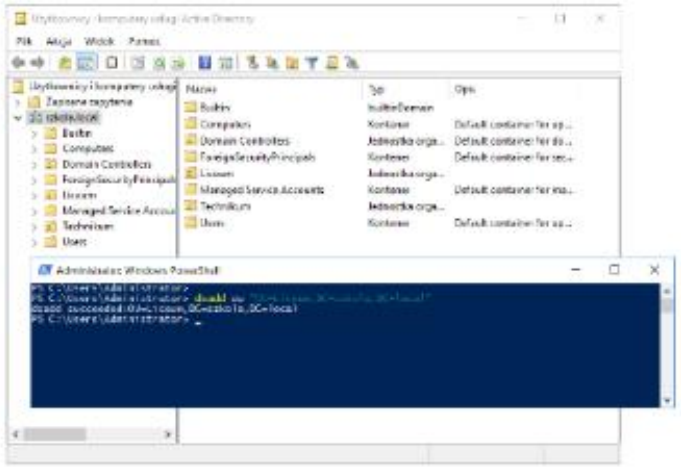


Innym sposobem dodania lub usunięcia jednostki organizacyjnej jest użycie konsoli Windows PowerShell.

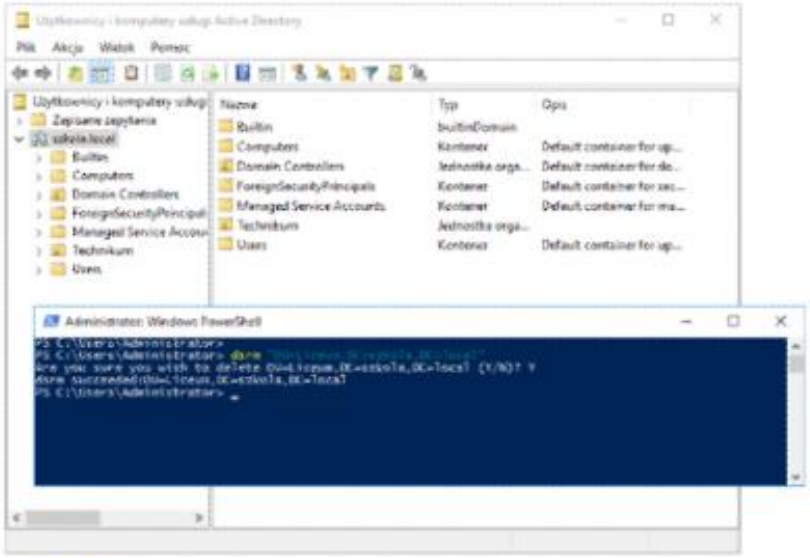
Ćwiczenie 3.6

1. Uruchamiamy konsolę Windows PowerShell.
2. Wpisujemy polecenie `dsadd ou "OU=Liceum,DC=szkola,DC=local"` i wciskamy *Enter*.
3. Jednostka organizacyjna *Liceum* w domenie *szkola.local* została utworzona, co możemy sprawdzić w przystawce konsoli MMC (rysunek 3.31).

Rysunek 3.31. Dodanie nowej jednostki organizacyjnej Liceum za pomocą konsoli



W podobny sposób usuwamy jednostkę organizacyjną przy użyciu polecenia `dsrm "OU=Liceum,DC=szkola,DC=local"`. Po wpisaniu polecenia zatwierdzamy operację klawiszem *Y*. Wówczas jednostka organizacyjna *Liceum* zostaje usunięta, co możemy sprawdzić w konsoli MMC (rysunek 3.32).



Rysunek 3.32. Usunięcie jednostki organizacyjnej Liceum za pomocą konsoli

Zadania kontrolne

1. Za pomocą przystawki *Użytkownicy i komputery usługi Active Directory* utwórz konto użytkownika o nazwie składającej się z Twojego imienia i nazwiska, które wygaśnie 1 stycznia 2029 roku, z możliwością logowania od poniedziałku do piątku w godzinach od 8:30 do 10:30, przy czym niech hasło użytkownika nigdy nie wygasa.
2. Za pomocą konsoli Windows PowerShell utwórz jednostkę organizacyjną *Szkoła*, a w niej użytkownika *Uczeń*. Po sprawdzeniu usuń za pomocą konsoli konto *Uczeń* oraz jednostkę organizacyjną *Szkoła*.

3.6. Automatyzacja procesu tworzenia kont użytkowników za pomocą konsoli

Sposób tworzenia kont użytkowników pokazany w poprzednim podrozdziale jest bardzo prosty, pod warunkiem że mamy do utworzenia kilka kont. Jeśli nasza szkoła miałaby 500 uczniów i 50 nauczycieli, byłoby to zadanie żmudne i czasochłonne. Aby sobie pomóc, możemy skorzystać z konsoli Windows PowerShell oraz dwóch programów:

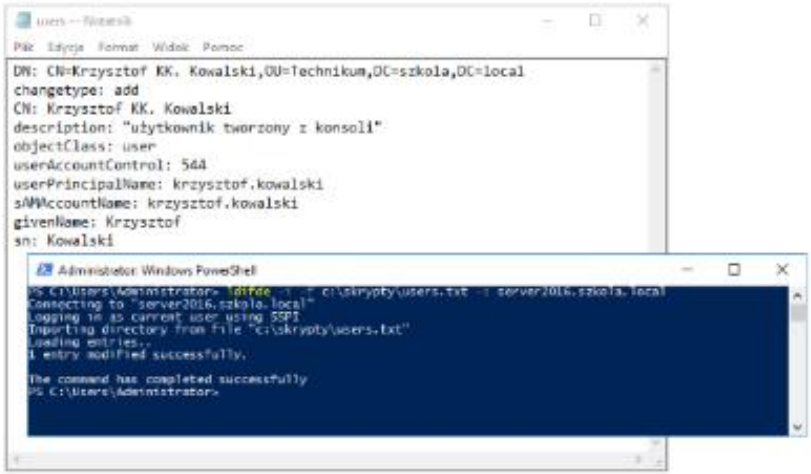
- **LDIFDE** — narzędzie wiersza poleceń, które tworzy, modyfikuje i usuwa obiekty w katalogu, a także eksportuje informacje o użytkownikach i grupach usługi Active Directory. Wadą tego polecenia jest brak możliwości ustawienia hasła.
- **CSVDE** — narzędzie wiersza poleceń, które importuje i eksportuje dane z usług domenowych Active Directory. Robi to przy użyciu plików, które przechowują dane w formie wartości rozdzielanych przecinkami (CSV).

Ćwiczenie 3.7

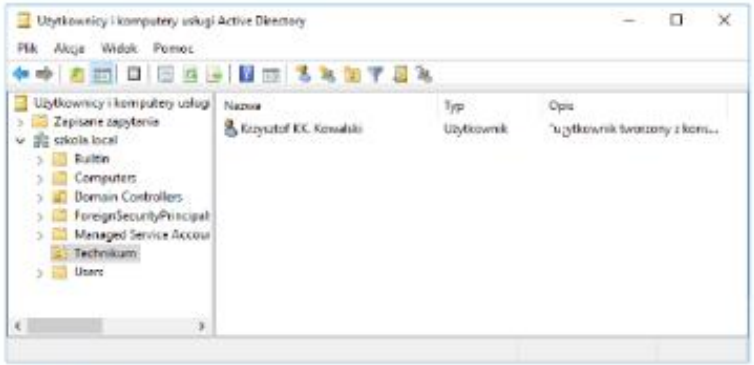
Spróbujmy teraz utworzyć i usunąć konta za pomocą narzędzia LDIFDE.

1. Tworzymy w Notatniku plik z danymi kont do zaimportowania z następującą zawartością:
   - `DN: CN=Krzysztof KK. Kowalski, OU=Technikum, DC=szkola, DC=local` — nazwa DN, w której `CN` oznacza nazwę użytkownika, `OU` jednostkę organizacyjną, a `DC` domenę,
   - `changetype: add` — dodawanie obiektu,
   - `CN: Krzysztof KK. Kowalski` — pełna nazwa użytkownika,
   - `description: "użytkownik tworzony z konsoli"` — opis tworzonego obiektu,
   - `objectClass: user` — typ tworzonego obiektu,
   - `userAccountControl: 544` — konto po utworzeniu zostanie włączone, żadne hasło nie jest wymagane,
   - `userAccountControl: 514` — konto po utworzeniu zostanie wyłączone,
   - `userPrincipalName: krzysztof.kowalski` — nazwa główna użytkownika,
   - `sAMAccountName: krzysztof.kowalski` — nazwa konta,
   - `givenName: Krzysztof` — imię użytkownika,
   - `sn: Kowalski` — nazwisko użytkownika.

   Zapisujemy plik jako *users.txt* w nowo utworzonym folderze *C:\skrypty*, który będzie nam służył do dalszych ćwiczeń.
2. Teraz wystarczy wpisać w Windows PowerShell polecenie `ldifde -i -f c:\skrypty\users.txt -s server2016.szkola.local` i potwierdzić je klawiszem *Enter*. Wówczas konto zostanie dodane (rysunek 3.33). Przełączniki użyte w poleceniu to:
   - `-i` — import danych,
   - `-f` — ścieżka i nazwa pliku użytego do importu lub eksportu danych,
   - `-s` — nazwa serwera.
3. Konto zostało utworzone, co możemy potwierdzić w konsoli MMC (rysunek 3.34).



Rysunek 3.33. Dodanie użytkownika z pliku users.txt za pomocą polecenia LDIFDE



Rysunek 3.34. Potwierdzenie utworzenia użytkownika w jednostce organizacyjnej Technikum

4. Teraz usuniemy za pomocą konsoli nowo utworzone konto. Utworzymy nowy plik o nazwie *users_delete.txt* z poniższą zawartością. Ważne, aby ustawić changetype na delete:

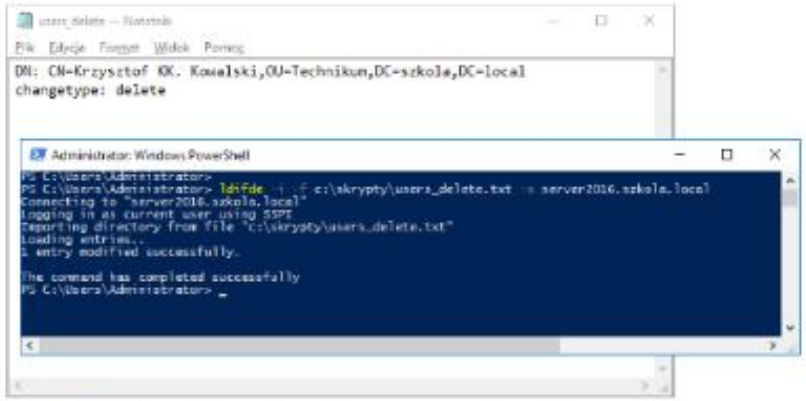
```
DN: CN=Krzysztof KK. Kowalski,OU=Technikum,DC=szkola,DC=local

changetype: delete
```

i wykonać następujące polecenie w konsoli:

```
ldifde -i -f c:\skrypty\users_delete.txt -s server2016.szkola.local
```

Rezultat wykonania polecenia jest pokazany na rysunku 3.35.



Rysunek 3.35. Usunięcie użytkownika za pomocą konsoli

Tak samo możemy dodać lub usunąć większą liczbę użytkowników. Jedyne, co musimy zrobić, to utworzyć plik z odpowiednimi danymi użytkowników i wykonać polecenie w konsoli.

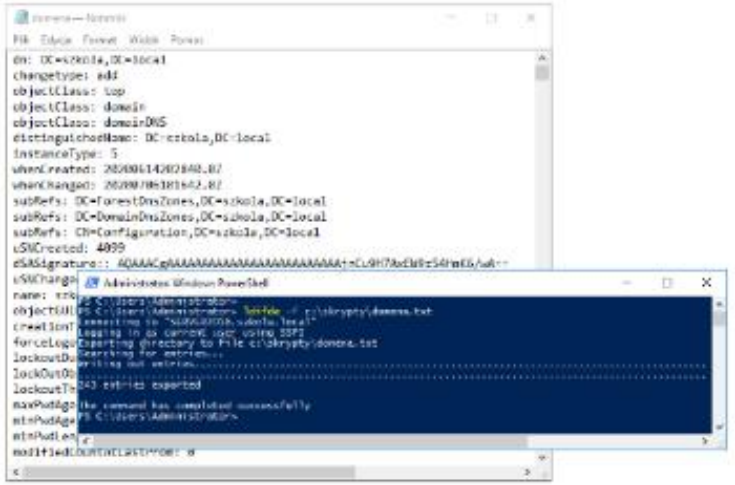
Tego samego polecenia możemy użyć do wyeksportowania informacji o domenie lub konkretnym obiekcie. Zrobimy to w poniższym ćwiczeniu.

Ćwiczenie 3.8

1. Uruchamiamy konsolę Windows PowerShell i wpisujemy polecenie:

```
ldifde -f c:\skrypty\domena.txt
```

Po potwierdzeniu klawiszem *Enter* otrzymujemy wszystkie informacje na temat naszej domeny wyeksportowane do pliku *C:\skrypty\domena.txt* (rysunek 3.36).



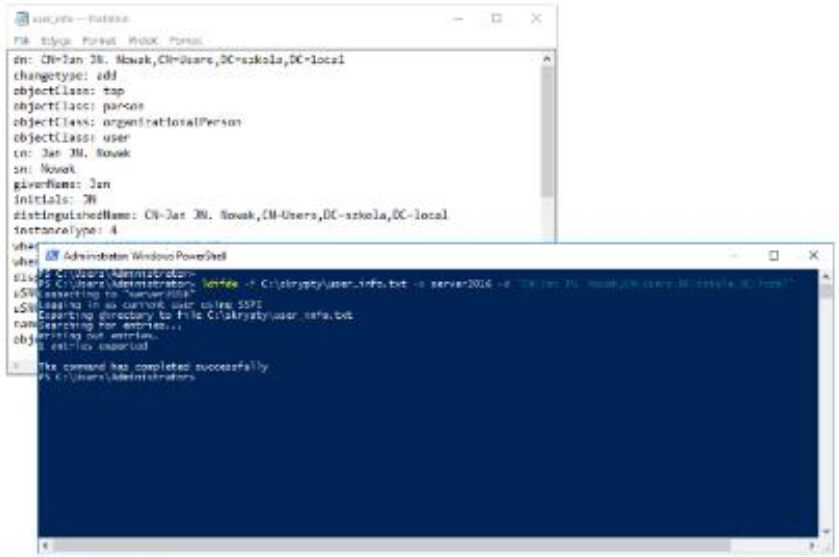
Rysunek 3.36. Eksport danych dotyczących domeny szkola.local

2. Teraz wykonamy polecenie, w którym wyeksportujemy informacje na temat konkretnego obiektu w domenie; w naszym przypadku będzie to użytkownik *Jan Nowak*. Aby to zrobić, musimy w poleceniu podać więcej informacji:

   ```
   ldifde -f C:\skrypty\user_info.txt -s server2016 -d "CN=Jan JN. Nowak,CN=Users,DC=szkola,DC=local"
   ```

   gdzie przełącznik `-d` to domyślne ustawienie wymuszające przeszukanie folderu głównego domeny.

3. Po wykonaniu polecenia otrzymamy plik *C:\skrypty\user_info.txt*, zawierający informacje o wybranym użytkowniku (rysunek 3.37).

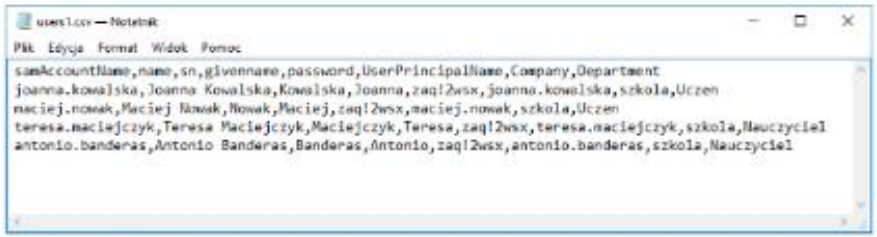


Rysunek 3.37. Eksportowanie informacji o użytkowniku za pomocą konsoli

W następnym ćwiczeniu zaimportujemy dane z pliku *.csv*, czyli dane oddzielone przecinkiem, za pomocą dwóch narzędzi: kombinacji Import-CSV i New-ADUser oraz CSVDE. Zaletą tej metody jest możliwość ustawienia hasła dla użytkownika.

Ćwiczenie 3.9

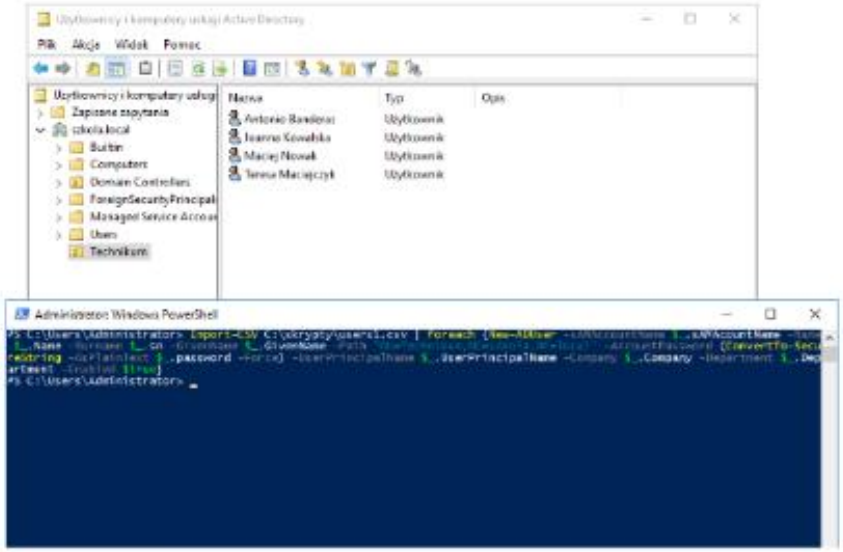
1. W folderze *C:\skrypty* tworzymy w sposób pokazany na rysunku 3.38 plik *users1.csv*, w którym zawieramy nazwy użytkowników oraz hasła. Bardzo ważne jest, aby wszystkie dane znajdowały się w jednym wierszu, oddzielone tylko przecinkami, oraz były umieszczone w ściśle określonej kolejności wskazanej w pierwszej linii pliku.



Rysunek 3.38. Plik .csv gotowy do importu danych

2. Uruchamiamy polecenie do importu w Windows PowerShell, jak na rysunku 3.39, i sprawdzamy w konsoli MMC, czy konta zostały utworzone.

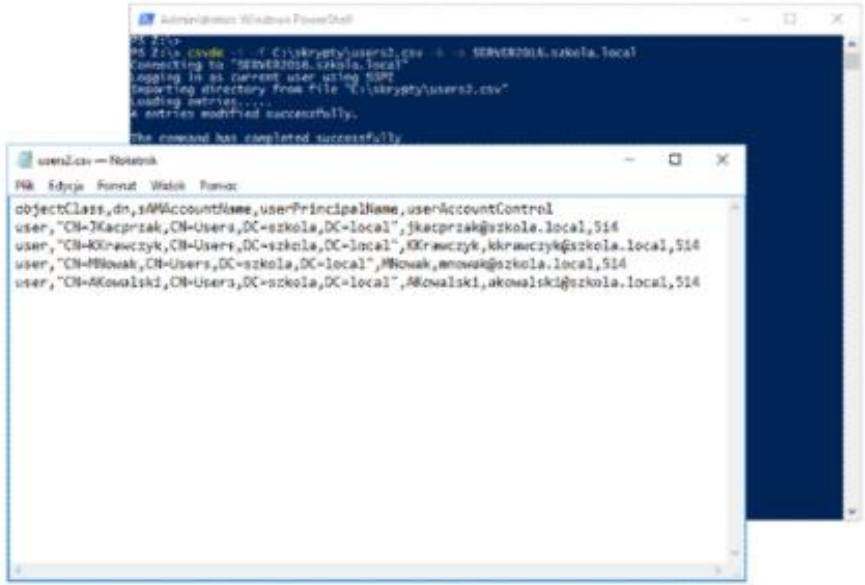
   ```
   Import-CSV C:\skrypty\users1.csv | foreach {New-ADUser -SamAccountName $_.SamAccountName -Name $_.Name -Surname $_.sn -GivenName $_.GivenName -Path "OU=Technikum,DC=szkola,DC=local" -AccountPassword (ConvertTo-SecureString -AsPlainText $_.password -Force) -UserPrincipalName $_.UserPrincipalName -Company $_.Company -Department $_.Department -Enabled $true}
   ```



Rysunek 3.39. Import kont z pliku .csv

3. W folderze *C:\skrypty* tworzymy kolejny plik, *users2.csv*, tym razem do użycia poprzez polecenie CSVDE. Plik utworzony został w sposób bardzo podobny do poprzedniego, ale posiada inną strukturę. Przykładowa struktura to: `objectClass,dn,sAMAccountName,userPrincipalName,userAccountControl`.

Teraz wystarczy tylko uruchomić polecenie `csvde -i -f C:\skrypty\users2.csv -k -s SERVER2016.szkola.local`. Wykonane polecenie oraz plik z danymi widoczny jest na rysunku 3.40.



Rysunek 3.40. Dodawanie kont użytkowników za pomocą polecenia CSVDE

Porównując obydwa polecenia do importu kont z pliku *.csv*, widzimy, że polecenie CSVDE — dzięki temu, że ma prostszą składnię — jest łatwiej zastosować.

Zadania kontrolne

1. Utwórz za pomocą wiersza poleceń trzy konta użytkowników o nazwach: *Anna Kowalska*, *Michał Kowalski* i *Mikołaj Zieliński*, z hasłem *Q@wertyuiop*.
2. Za pomocą Windows PowerShell usuń nowo utworzone konta użytkowników.

3.7. Zarządzanie kontami komputerów oraz przyłączanie ich do domeny

Poznaliśmy już sposoby dodawania i edytowania kont użytkowników, pora zatem na dodanie komputera do naszej domeny. Do tego jest potrzebny zainstalowany system kliencki pozwalający na współpracę z domeną, np. Windows 10 w wersji Professional, Enterprise lub Education. Należy pamiętać, że Windows 10 Home nie ma rozbudowanych opcji sieciowych opartych

na domenach, dlatego nie można go dołączyć do serwera. Przed wykonaniem ćwiczenia za pomocą oprogramowania Oracle VirtualBox należy pamiętać, by w ustawieniach maszyny podłączyć kartę sieciową do sieci wewnętrznej, aby możliwe było nawiązanie komunikacji z serwerem.

Klienta do serwera możemy dołączyć w bardzo prosty sposób. Polega on na utworzeniu konta komputera na serwerze, a następnie zalogowaniu się na kliencie i dołączeniu do domeny. Zaletą tego rozwiązania jest to, że możemy jeszcze przed dołączeniem do domeny wskazać, w którym kontenerze lub której jednostce organizacyjnej znajdzie się konto komputera oraz który użytkownik (niekoniecznie z uprawnieniami administratora) będzie zarządzał komputerem lub będzie mógł dołączyć ten komputer do domeny. W przypadku tego rozwiązania ważne jest, aby pamiętać, jakiej nazwy komputera użyło się podczas zakładania jego konta. Przedstawimy to w ćwiczeniu 3.10. Po wykonaniu operacji pokazanych w ćwiczeniach uczniowie i nauczyciele naszej przykładowej szkoły będą mogli pracować na komputerach podłączonych do domeny.

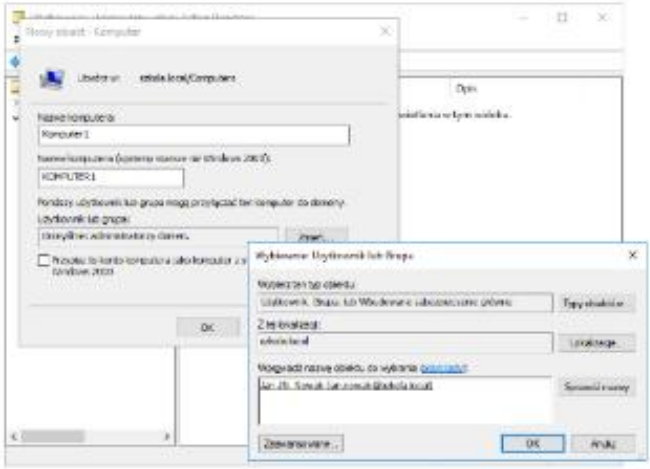
Ćwiczenie 3.10

1. Uruchamiamy przystawkę konsoli MMC *Użytkownicy i komputery usługi Active Directory*, a następnie rozwijamy domenę i pozycję *Computers*.
2. Klikamy *Computers* prawym przyciskiem myszy i wybieramy *Nowy/Komputer* (rysunek 3.41).



Rysunek 3.41. Dodawanie konta komputera do domeny

3. Uzupełniamy dane komputera, przy polu *Użytkownik lub grupa* klikamy *Zmień* i w karcie *Wybieranie: Użytkownik lub Grupa* wskazujemy, kto będzie mógł podłączyć komputer do domeny, a następnie zatwierdzamy przyciskiem *OK* (rysunek 3.42).



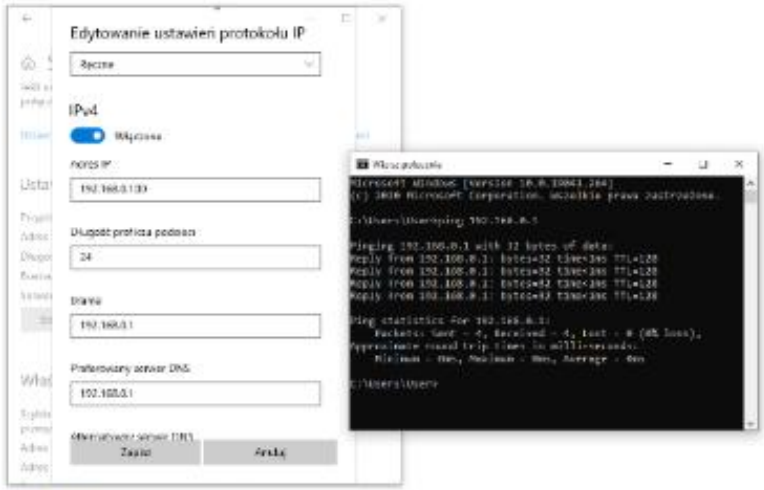
Rysunek 3.42. Konfiguracja konta komputera

4. Teraz przechodzimy do komputera klienta i konfigurujemy ustawienia karty sieciowej. Aby wejść do konfiguracji karty sieciowej, naciskamy *Start/Ustawienia/Sieć i internet/Ethernet*, a następnie klikamy dostępne połączenie sieciowe i wybieramy *Ustawienia protokołu IP/Edytuj*. Domyślne ustawienie protokołu to *Automatyczne (DHCP)*. Oznacza ono, że komputer automatycznie odbierze informacje z serwera DHCP, który na razie w naszym serwerze nie działa. Zmieniamy to ustawienie na *Ręczne*, włączamy protokół IPv4 i wprowadzamy ustawienia: *Adres IP* — `192.168.0.100/24` (adres sieci `192.168.0.0/24`, serwer i komputer klienta muszą należeć do jednej sieci), *Brama* — `192.168.0.1` (brama domyślna — adres komputera, który będzie udostępniał w przyszłości internet), *Preferowany serwer DNS* — `192.168.0.1` (na naszym serwerze jest już zainstalowana rola serwera DNS, która będzie obsługiwać nazwy domenowe Active Directory).

   Na koniec możemy sprawdzić poprawność wprowadzonych ustawień oraz połączenie przez uruchomienie wiersza poleceń i wpisanie polecenia `ping 192.168.0.1`.

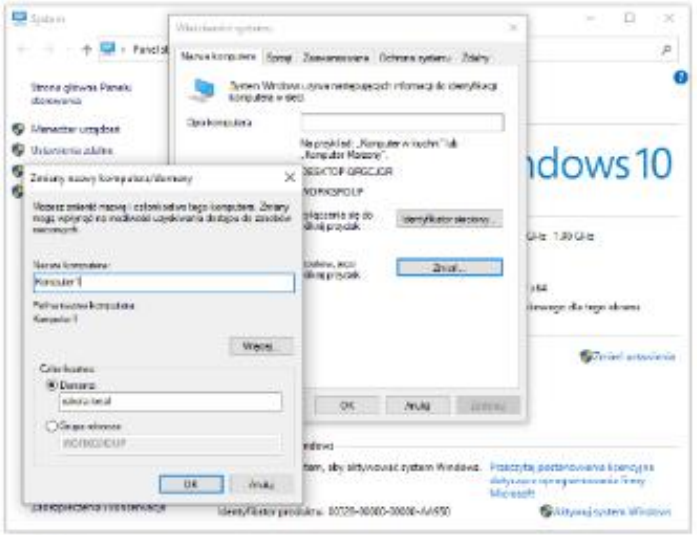
   Jeśli adres odpowiada, to oznacza, że wszystko zostało skonfigurowane poprawnie (rysunek 3.43).

5. Teraz zmienimy nazwę komputera i przyłączymy go do domeny. W tym celu musimy uruchomić kartę *System*. Uruchamiamy Eksploratora plików. W oknie programu prawym przyciskiem myszy klikamy ikonę *Ten komputer* po lewej stronie i wybieramy *Właściwości*. W nowo otwartym oknie klikamy *Zmień ustawienia*. W oknie *Właściwości systemu* klikamy przycisk *Zmień…*, a następnie wpisujemy nazwę konta komputera, które wcześniej utworzyliśmy, *Komputer1*, poniżej zaś nazwę domeny, *szkola.local*, jak na rysunku 3.44. Na koniec zatwierdzamy przyciskiem *OK*. System poprosi o wpisanie nazwy użytkownika (*jan.nowak*) oraz hasła. Takie prawo ma użytkownik z upraw-



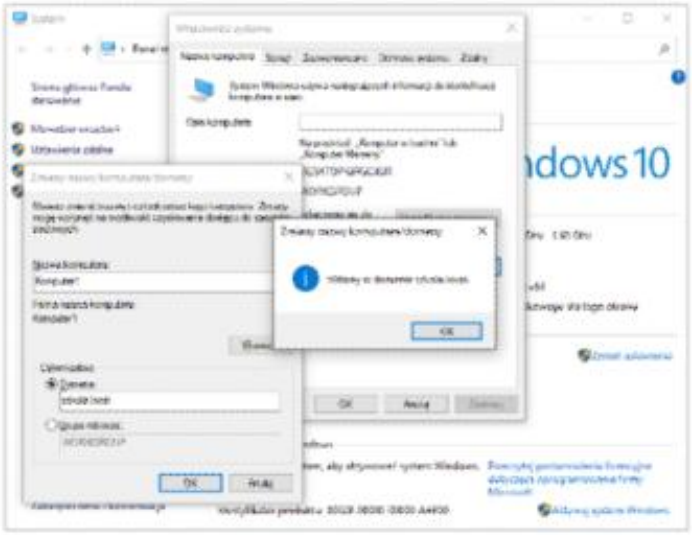
Rysunek 3.43. Konfiguracja karty sieciowej klienta oraz sprawdzenie połączenia poleceniem ping

nieniami administratora. My, tworząc konto komputera, dodaliśmy użytkownika *Jan JN. Nowak*, który wprawdzie nie jest administratorem, ale ma prawo przyłączać ten komputer do domeny.



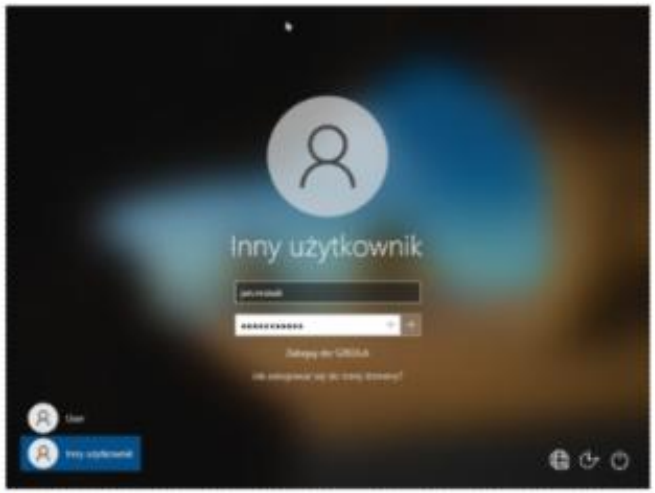
Rysunek 3.44. Dodawanie komputera do domeny i zmiana jego nazwy

6. Zostanie wyświetlony komunikat informujący o tym, że komputer został podłączony do domeny (rysunek 3.45). Potwierdzamy przyciskiem *OK* i ponownie uruchamiamy komputer.



Rysunek 3.45. Potwierdzenie przyłączenia do domeny

7. Teraz wystarczy zalogować się na któreś z kont domenowych, aby rozpocząć korzystanie z domeny *szkola.local* (rysunek 3.46).



Rysunek 3.46. Ekran logowania komputera klienta do domeny

Aby usunąć komputer z domeny, wystarczy w przystawce MMC *Użytkownicy i komputery* usługi Active Directory odnaleźć konto komputera, kliknąć jego nazwę prawym przyciskiem myszy, wybrać *Usuń* i potwierdzić jego usunięcie. Komputer, który nie jest w domenie, już nie będzie mógł być używany do pracy w sieci opartej na Active Directory.

Użytkownik, który ma konto z prawami administratora, może przyłączyć komputer do domeny bez wcześniejszego tworzenia jego konta. Wystarczy, że wykona polecenia z powyższego ćwiczenia od punktu 5., używając do potwierdzenia dołączenia do domeny swojego loginu i hasła.

Zadania kontrolne

1. Zmień nazwę komputera klienta na *Eukaliptus*, a następnie przyłącz komputer do domeny.
2. W Active Directory utwórz konto komputera o nazwie *BRATEK* i przypisz do niego dwóch użytkowników bez uprawnień administratora, którzy będą zarządzać komputerem.

3.8. Profile użytkowników

W tym podrozdziale omówimy profile użytkowników oraz foldery macierzyste.

DEFINICJA

Profil użytkownika to zbiór ustawień konkretnego użytkownika, w których określone jest zachowanie systemu, m.in. wygląd pulpitu, motyw kolorystyczny i sposób wyświetlania plików.

Folder macierzysty to udział sieciowy serwera, mapowany jako dysk sieciowy, w którym użytkownik może przechowywać własne pliki, by uzyskiwać do nich dostęp podczas pracy w sieci.

W systemach z rodziny Windows Server rozróżniamy następujące rodzaje profili:

- **Lokalny profil użytkownika** — tworzony przy pierwszym logowaniu użytkownika na komputerze i przechowywany na lokalnym dysku twardym. Zmiany wprowadzone w lokalnym profilu użytkownika są specyficzne dla tego użytkownika i komputera, na którym profil jest zapisany.
- **Mobilny profil użytkownika** — jest kopią profilu lokalnego, który jest kopiowany i zapisywany w udziale serwera. Ten profil jest pobierany na dowolny komputer, na którym użytkownik loguje się w sieci. Zmiany wprowadzone w profilu użytkownika mobilnego są synchronizowane z kopią profilu przechowywaną na serwerze po wylogowaniu użytkownika. Zaletą profilu mobilnego jest to, że użytkownik nie musi tworzyć profilu na każdym komputerze, którego używa w sieci.
- **Obowiązkowy profil użytkownika** — rodzaj profilu, którego administratorzy mogą używać do określania ustawień dla użytkowników. Tylko administratorzy systemu mogą

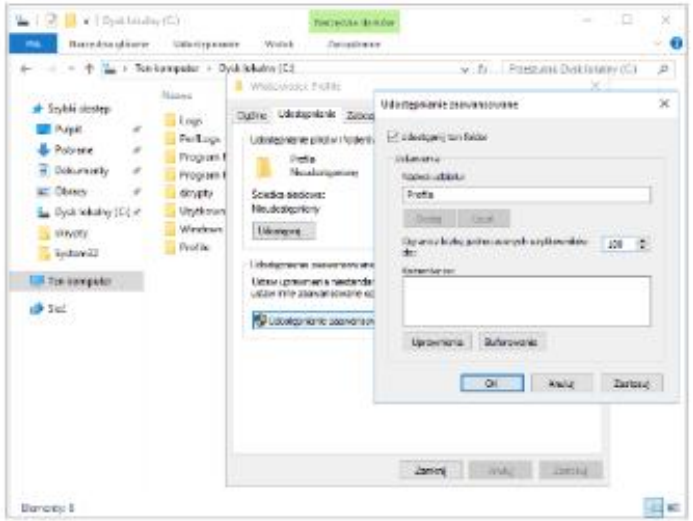
wprowadzać zmiany w obowiązkowych profilach użytkowników. Zmiany w ustawieniach pulpitu wprowadzone przez użytkownika są tracone, gdy ten się wyloguje.

- **Tymczasowy profil użytkownika** — ładowany za każdym razem, gdy błąd uniemożliwia załadowanie profilu użytkownika. Profil tymczasowy jest usuwany na koniec każdej sesji, a zmiany w ustawieniach pulpitu i plikach dokonane przez użytkownika są tracone po jego wylogowaniu. Profile tymczasowe są dostępne tylko na komputerach z systemem Windows 2000 i nowszymi.

W ćwiczeniu 3.11 utworzymy folder, w którym będziemy przechowywać profile mobilne naszych użytkowników, oraz skonfigurujemy ustawienia profili użytkownika. Na koniec utworzymy i przypiszemy użytkownikom foldery macierzyste. Każdy administrator, który ma do dyspozycji dodatkowe dyski twarde, będzie przechowywał dane użytkowników na oddzielnym nośniku, my jednak, ze względu na ograniczone możliwości, wykorzystamy do tego dysk *C*. W rzeczywistości te dane są bardzo ważne i to w folderach macierzystych uczniowie i nauczyciele z naszej przykładowej szkoły będą przechowywać swoje dane.

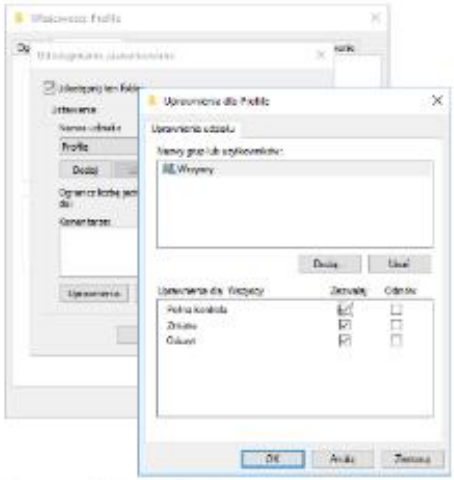
Ćwiczenie 3.11

1. Na dysku *C* tworzymy folder o nazwie *Profile*, w którym będziemy przechowywali profile mobilne naszych użytkowników (*C:\Profile*).
2. Prawym przyciskiem myszy klikamy nowo utworzony folder i wybieramy *Właściwości/Udostępnianie/Udostępnianie zaawansowane*. Następnie zaznaczamy *Udostępnij ten folder* i wprowadzamy maksymalną liczbę użytkowników w pozycji *Ogranicz liczbę jednoczesnych użytkowników do:*. My ustawimy tę wartość na 100, tak jak na rysunku 3.47.

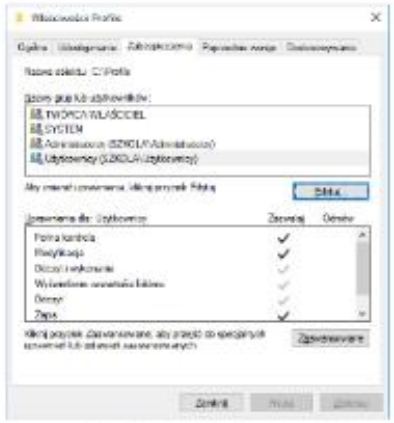


Rysunek 3.47. Udostępnianie zaawansowane folderu profili mobilnych

3. Następnie wybieramy *Uprawnienia* i dla grupy *Wszyscy* zaznaczamy wszystkie uprawnienia na *Zezwalaj* (rysunek 3.48).
4. Dodatkowo musimy włączyć we *Właściwości/Zabezpieczenia* opcję *Pełna kontrola* dla grupy *Użytkownicy* (rysunek 3.49).



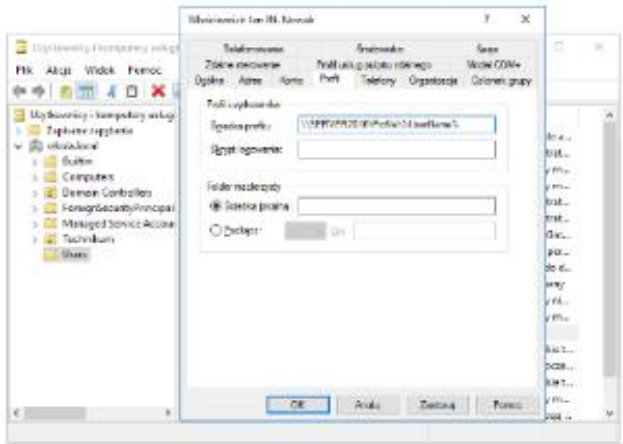
Rysunek 3.48. Zmiana uprawnień dla folderu Profile



Rysunek 3.49. Ustawienie pełnej kontroli dla grupy Użytkownicy

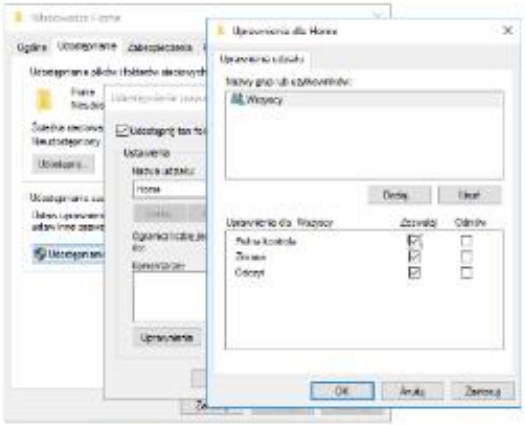
5. Teraz dopiszemy we właściwościach użytkowników ścieżkę przechowywania profilu na serwerze. Aby to zrobić, uruchamiamy przystawkę *Użytkownicy i komputery usługi Active Directory*, wskazujemy użytkownika, wybieramy *Właściwości* i przechodzimy do zakładki *Profil*, w której w polu *Ścieżka profilu* wpisujemy ścieżkę do profilu użytkownika: `\\SERVER2016\Profile\%UserName%` (rysunek 3.50).

Rysunek 3.50. Ustawienie ścieżki profilu



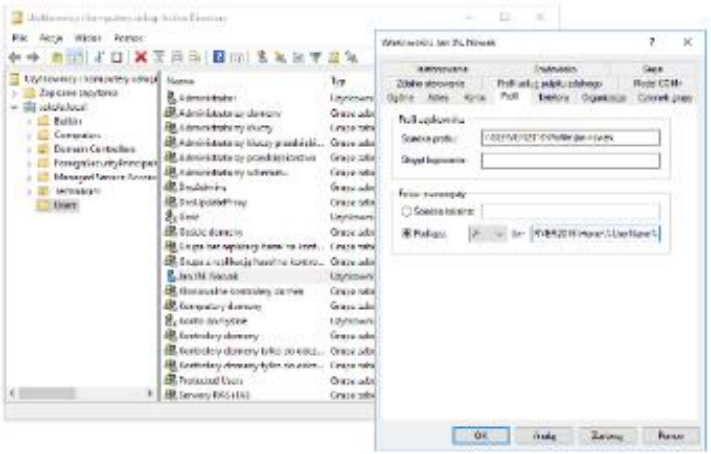
6. Po naciśnięciu *Zastosuj* zmienna w ścieżce powinna się zmienić na konkretną nazwę użytkownika i powinna wyglądać tak: `\\SERVER2016\Profile\jan.nowak`. Zatwierdzamy przyciskiem *OK* i na kliencie Windows 10 podłączonym do domeny logujemy się za pomocą użytego konta, a następnie po wylogowaniu sprawdzamy, czy został utworzony folder z nazwą użytkownika.
7. Kolejnym krokiem jest utworzenie folderu *C:\Home* i udostępnienie go z pełnymi uprawnieniami dla grupy użytkowników *Wszyscy* (rysunek 3.51). Będziemy w nim przechowywać foldery macierzyste użytkowników.

Rysunek 3.51. Ustawienia udostępniania folderu Home



8. Uruchamiamy przystawkę *Użytkownicy i komputery usługi Active Directory*, wskazujemy użytkownika, klikamy *Właściwości* i przechodzimy do zakładki *Profil*, gdzie zaznaczamy *Podłącz* i wybieramy literę dysku (*Z*), pod którą będzie dostępny folder macierzysty, a następnie wpisujemy ścieżkę dla konkretnego użytkownika: `\\SERVER2016\Home\%UserName%` (rysunek 3.52).

Rysunek 3.52. Ustawienia ścieżki folderu macierzystego



9. Po zatwierdzeniu, a następnie zalogowaniu się na kliencie Windows 10 zostanie automatycznie utworzony folder *C:\Home\%Username%* (w naszym przypadku *C:\Home\jan.nowak*). W systemie klienckim został zamapowany udział sieciowy (jako dysk *Z*).

Zadania kontrolne

1. Utwórz pięć nowych kont użytkownika, których profile będą przechowywane w folderze *C:\Profile\{nazwa użytkownika}*.
2. Dla nowo utworzonych kont ustaw folder macierzysty zlokalizowany w folderze *C:\Foldery\{nazwa użytkownika}* jako dysk *W*.

3.9. Serwer DHCP

O usłudze DHCP mówiliśmy już w poprzednim rozdziale, podczas omawiania serwera Linux. Teraz zajmiemy się jej instalacją i konfiguracją w Windows Server 2016/2019.

DEFINICJA

Protokół DHCP (ang. *Dynamic Host Configuration Protocol*) umożliwia serwerom przypisywanie (przyznawanie dzierżawy) adresów IP komputerom i innym urządzeniom, które są ustawione jako klienty DHCP. Wdrożenie serwera DHCP w sieci powoduje automatyczne dostarczenie komputerom i innym urządzeniom sieciowym obsługującym protokół TCP/IP adresów IP i innych potrzebnych im parametrów konfiguracyjnych nazywanych opcjami DHCP. Dzięki temu komputery i urządzenia mogą się łączyć z innymi zasobami sieciowymi, takimi jak serwery DNS, serwery WINS i routery.

ZAPAMIĘTAJ

Interfejs sieciowy serwera, na którym będzie działała usługa DHCP, musi mieć skonfigurowany statyczny adres sieciowy. Adres tego interfejsu nie powinien wchodzić w pulę adresów do przydzielenia DHCP.

W danym segmencie sieci komputerowej może działać tylko jeden serwer DHCP.

Aby zainstalować usługę, musimy uruchomić Menedżer serwera. Na pulpicie nawigacyjnym wybieramy *Dodaj role i funkcje*. Na karcie *Zanim rozpoczniesz* klikamy *Dalej* i wybieramy *Typ instalacji*, tj. *Instalacja oparta na rolach lub oparta na funkcjach*. Teraz wybieramy serwer i klikamy *Dalej*, aby przejść do karty *Wybieranie ról serwera*, i zaznaczamy *Serwer DHCP*. Zostanie wyświetlone okno dodawania funkcji, w którym klikamy *Dodaj funkcje*, a następnie *Dalej*. Na karcie *Wybieranie funkcji* klikamy *Dalej*, aby przejść do zakładki *Serwer DHCP*, w której możemy przeczytać podstawowe informacje na temat DHCP, i ponownie klikamy *Dalej*. Nowo otwarta karta *Potwierdzanie opcji instalacji* pokaże podsumowanie instalacji. Możemy na niej zaznaczyć, aby serwer automatycznie się uruchomił ponownie w razie

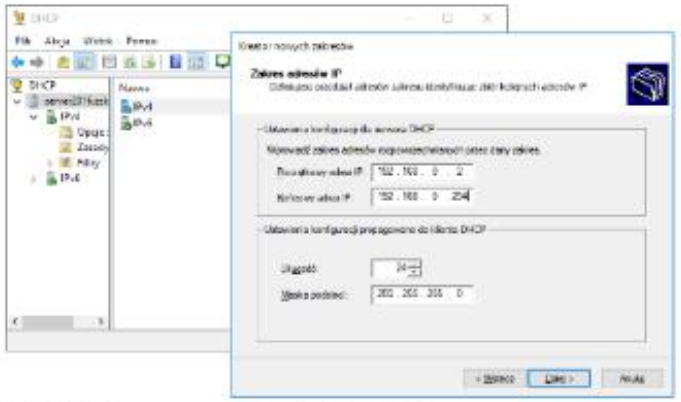
potrzeby, w przeciwnym przypadku od razu naciskamy *Zainstaluj*, po czym rozpocznie się proces instalowania usługi. Po zakończeniu instalacji musimy skonfigurować usługę DHCP. W górnej części okna Menedżera serwera pojawi się ikona przedstawiająca żółty trójkąt z wykrzyknikiem. Klikamy ją i wybieramy *Dokończ konfigurację funkcji DHCP*, a następnie klikamy *Dalej*. Aby autoryzować serwer DHCP w AD DS, wybieramy poświadczenia użytkownika z prawami administratora (w naszym przypadku jest to użytkownik *Administrator*) i klikamy *Potwierdź*. Autoryzacja serwera została przeprowadzona, klikamy zatem *Zamknij*. W ćwiczeniu 3.12 wykonamy i omówimy konfigurację serwera DHCP. Zanim to zrobimy, przedstawimy kilka informacji, których będziesz do tego potrzebował:

- **Zakres DHCP** jest przedziałem adresów IP przyporządkowanych do komputerów żądających dynamicznych adresów IP.
- **Opcje serwera** to dodatkowe parametry konfiguracyjne, które serwer DHCP może przypisać do klientów DHCP — adresy serwerów DNS, adres routera i wiele innych.
- **Wykluczenie** to adresy lub zakresy adresów, które nie są rozpowszechniane przez serwer.
- **Czas dzierżawy** określa, jak długo klient może używać adresu IP z zakresu. Czas trwania dzierżawy powinien na ogół równać się przeciętnemu czasowi połączenia komputera z daną siecią fizyczną. Dla sieci ruchomych, złożonych głównie z komputerów przenośnych lub klientów połączeń telefonicznych, przydatne mogą być krótsze czasy trwania dzierżawy. Odwrotnie jest w przypadku sieci złożonych głównie z komputerów stacjonarnych o stałej lokalizacji — tu stosowane są dłuższe czasy trwania dzierżawy.
- **Zastrzeżenie** gwarantuje, że klient DHCP zawsze ma przyporządkowany ten sam adres IP.

Dzięki uruchomieniu na serwerze usługi DHCP porządkujemy infrastrukturę sieciową naszej szkoły. Odciążymy router od obsługi DHCP i zostawimy go jako bramę domyślną (urządzenie styku z internetem). Dzięki temu administrator zyska możliwość zarządzania usługą z poziomu serwera, a szkoła będzie miała zapewnioną niezawodność działania i bezpieczeństwo sieci. Kolejne usługi, które omówimy w dalszych podrozdziałach, będą wykorzystywać usługę DHCP i pozwolą w przyszłości usunąć z naszej szkolnej sieci niepotrzebny już router. Ćwiczenia, które teraz wykonamy, pozwolą zapoznać się z konfiguracją DHCP.

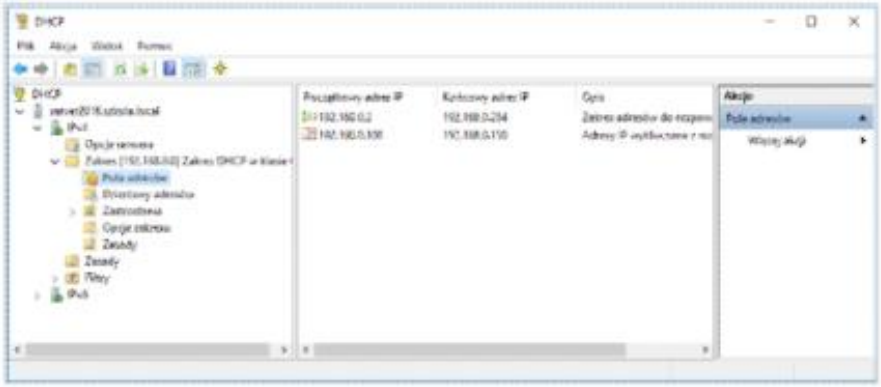
Ćwiczenie 3.12

1. Uruchamiamy Menedżer serwera i w menu *Narzędzia* wybieramy *DHCP*, co spowoduje uruchomienie przystawki zarządzania usługą DHCP. Rozwijamy nazwę serwera, a następnie wskazujemy protokół *IPv4*, klikamy prawym przyciskiem myszy wybraną wersję protokołu IP i z menu wybieramy *Nowy zakres*.
2. Uruchomi się *Kreator nowych zakresów*. Klikamy *Dalej* i przechodzimy do kolejnego etapu, w którym wprowadzamy nazwę i opis zakresu. Następnie ponownie klikamy *Dalej*.
3. Wprowadzamy adres początkowy, `192.168.0.2` (adres `192.168.0.1` jest już przypisany do interfejsu serwera), oraz adres końcowy, `192.168.0.254`. Niżej, w polu *Długość*, wpisujemy `24`, pole *Maska podsieci* uzupełni się automatycznie — `255.255.255.0`, klikamy *Dalej* (rysunek 3.53).



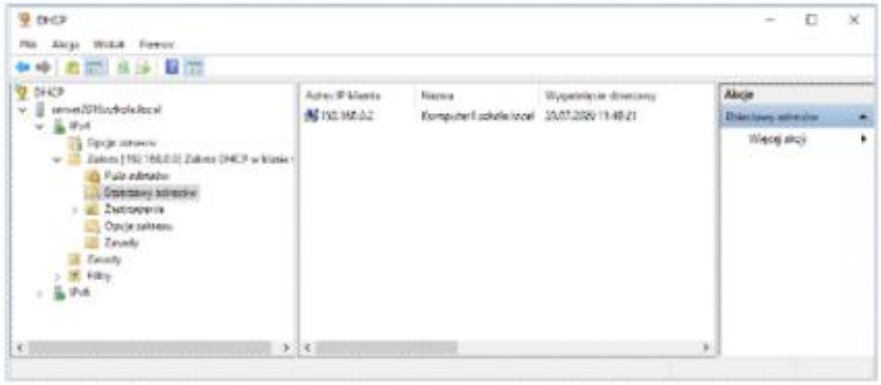
Rysunek 3.53. Konfigurowanie adresów IP w DHCP

4. Następny etap to wpisanie zakresu adresów wykluczenia: `192.168.0.100`–`192.168.0.150`. Wpisujemy adres początkowy oraz końcowy i klikamy *Dodaj*. Takich zakresów wykluczenia może być kilka. Po wpisaniu zakresów klikamy *Dalej*.
5. Na karcie *Czas dzierżawy* ustawiamy wybraną wartość, np. jedną godzinę. Po kliknięciu *Dalej* wyświetli się karta, na której musimy określić, czy chcemy konfigurować dodatkowe opcje dla DHCP. Jeśli wybierzemy opcję *Nie, skonfiguruję te opcje później*, to na kolejnej karcie zakończymy konfigurację. My wybieramy opcję *Tak, chcę teraz skonfigurować te opcje* i naciskamy *Dalej*.
6. Na karcie *Router (brama domyślna)* wprowadzamy adres bramy domyślnej, czyli adres interfejsu, dzięki któremu uzyskamy dostęp do sieci internet. My użyjemy adresu `192.168.0.1`, gdyż w dalszych ćwiczeniach to ten interfejs będzie nam służył jako interfejs dostępowy do sieci globalnej. Klikamy *Dalej*.
7. Na karcie *Nazwa domeny i serwery DNS* wprowadzamy domenę, w której pracuje serwer, `szkola.local`, i adres serwera DNS, czyli `192.168.0.1`, a następnie przechodzimy do kolejnej karty za pomocą przycisku *Dalej*.
8. Na karcie *Serwery WINS* nie wprowadzamy żadnych zmian i ponownie klikamy *Dalej*.
9. Na koniec karta *Uaktywnij zakres* pozwala wybrać, czy wprowadzona konfiguracja ma być uaktywniona, czy też nie. My zaznaczamy *Tak, chcę uaktywnić ten zakres teraz*, klikamy *Dalej* i na następnej karcie klikamy *Zakończ*. Konfiguracja DHCP jest zakończona. Po poprawnym skonfigurowaniu usługi powinniśmy otrzymać rezultat pokazany na rysunku 3.54.



Rysunek 3.54. Skonfigurowany serwer DHCP

10. Aby sprawdzić poprawność konfiguracji, należy na komputerze klienta zmienić ustawienia interfejsu sieciowego ze statycznego na DHCP i przekonać się, czy został przypisany adres z serwera DHCP. W przystawce zarządzania DHCP w pozycji *Dzierżawy adresów* możemy sprawdzić, które komputery otrzymały adresy z naszej puli (rysunek 3.55).



Rysunek 3.55. Dzierżawy adresów

Z tego poziomu możemy również zastrzec, aby komputer zawsze otrzymywał ten sam adres. W tym celu klikamy prawym przyciskiem myszy urządzenie wyszczególnione w pozycji *Dzierżawy adresów* i klikamy *Dodaj do zastrzeżenia*, a wtedy nasze urządzenie znajdzie się w pozycji *Zastrzeżenia*.

Dla całego zakresu możemy skonfigurować dodatkowe opcje w pozycji *Opcje zakresu*. Można również skonfigurować indywidualnie dla każdego urządzenia opcje dodatkowe, ale żeby to zrobić, trzeba najpierw utworzyć zastrzeżenie dla konkretnego urządzenia.

Zadanie kontrolne

1. Ustaw adres serwera na `10.20.30.1/24`, skonfiguruj nową pulę adresów w zakresie od `10.20.30.100` do `10.20.30.200` z maską `255.255.255.0`, wykluczając z tego adresy od `10.20.30.111` do `10.20.30.122` oraz od `10.20.30.150` do `10.20.30.160`. Zastrzeż adres `10.20.30.199` dla komputera klienta, przy czym bramą domyślną ma być adres `10.20.30.1`, a adres DNS ma być ustawiony na `194.204.152.34`.

3.10. Serwer DNS

O usłudze DNS mówiliśmy już w poprzednim rozdziale, podczas omawiania serwera Linux. Teraz zajmiemy się jej instalacją i konfiguracją w Windows Server 2016/2019.

UWAGA

System nazw domen, DNS (ang. *Domain Name System*) zapewnia standardową metodę kojarzenia nazw z numerycznymi adresami internetowymi. Dzięki temu użytkownicy mogą odwoływać się do komputerów w sieci przy użyciu łatwych do zapamiętania nazw, a nie długich serii liczb. Ponadto DNS zapewnia hierarchiczną przestrzeń nazw gwarantującą, że każda nazwa hosta będzie unikatowa w sieci lokalnej lub rozległej. Usługi DNS można zintegrować z usługami protokołu DHCP w systemie Windows, co sprawia, że nie trzeba dodawać rekordów DNS przy dodawaniu komputerów do sieci.

Dla przypomnienia, w DNS wyróżniamy dwie strefy wyszukiwania:

- strefę wyszukiwania do przodu — wykorzystywaną do tłumaczenia nazw w sieci lokalnej na adresy IP,
- strefę wyszukiwania wstecznego — wykorzystywaną do tłumaczenia adresów IP na nazwy w sieci lokalnej.

W DNS są stosowane najczęściej następujące rodzaje rekordów:

- **SOA** (ang. *Start of Authority*) — autorytatywny serwer dla strefy (na jedną strefę może przypadać tylko jeden taki rekord),
- **A** (ang. *Address IPv4*) — mapowanie nazwy hosta na adres IPv4,
- **AAAA** (ang. *Address IPv6*) — mapowanie nazwy hosta na adres IPv6,
- **CNAME** (ang. *Canonical Name*) — określenie aliasu nazwy hosta,
- **PTR** (ang. *Pointer*) — wskaźnik, który mapuje adres IP na nazwę hosta (przy wstecznym wyszukiwaniu),
- **NS** (ang. *Name Server*) — określenie serwera nazw dla domeny, dzięki czemu możliwe są wyszukiwania DNS wewnątrz różnych stref,
- **MX** (ang. *Mail Exchanger*) — określenie domeny serwera wymiany poczty elektronicznej.

Serwer DNS jest instalowany automatycznie wraz z usługą Active Directory, dzięki czemu możemy liczyć na dynamiczną aktualizację danych klientów. Automatyczna aktualizacja pozwala komputerom klientów na rejestrowanie i aktualizację ich rekordów w strefach przeszukiwania DNS za każdym razem, gdy zmienia się nazwa lub adres IP, co sprawia, że administrator nie musi wykonywać tego ręcznie.

Dzięki uruchomieniu DNS w naszej przykładowej szkole możliwa będzie praca z wykorzystaniem nazw mnemonicznych komputerów, a w późniejszym czasie także nazw drukarek i udziałów sieciowych. W poniższych ćwiczeniach zaprezentowany zostanie sposób instalacji i konfiguracji serwera DNS dla Windows Server 2016/2019.

Ćwiczenie 3.13

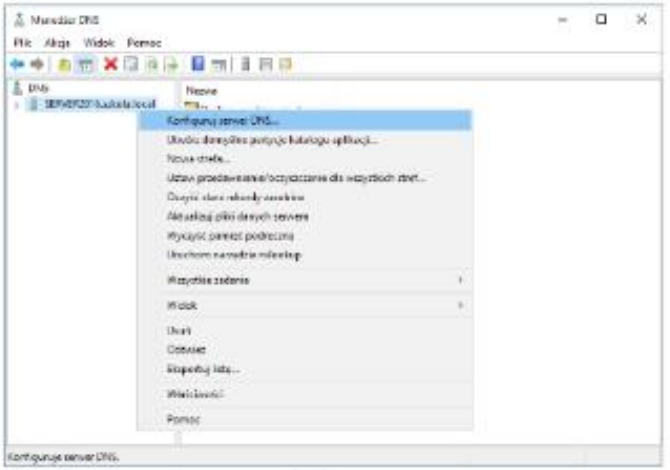
Wprawdzie serwer DNS w naszym przypadku jest już zainstalowany, ale gdyby trzeba było zainstalować usługę od podstaw, będzie to bardzo proste. Robi się to podobnie jak w przypadku innych usług:

1. Uruchamiamy Menedżer serwera i klikamy *Dodaj role i funkcje*.
2. Wybieramy opcję *Instalacja oparta na rolach lub funkcjach* i klikamy *Dalej*.
3. Wskazujemy serwer, na którym usługa ma zostać zainstalowana, i klikamy *Dalej*.
4. Na karcie *Wybieranie ról serwera* zaznaczamy opcję *Serwer DNS* i klikamy *Dalej*.
5. W nowo otwartym oknie *Kreator dodawania ról i funkcji* klikamy *Dodaj funkcje*.
6. Na karcie *Wybieranie funkcji* klikamy *Dalej*.
7. Teraz możemy przeczytać kilka informacji o DNS. Potem przechodzimy do następnej karty.
8. Na karcie *Potwierdzanie opcji instalacji* możemy podejrzeć, co będzie instalowane. Możemy zaznaczyć opcję, która pozwoli instalatorowi ponownie uruchomić komputer w razie potrzeby. Teraz pozostaje nacisnąć przycisk *Zainstaluj*, a wtedy instalacja się rozpocznie.

Ćwiczenie 3.14

W tym ćwiczeniu skonfigurujemy rekord nowego hosta (A) strefy przeszukiwania do przodu oraz alias hosta (CNAME).

1. W Menedżerze serwera wybieramy *Narzędzia*, a następnie *DNS*.
2. W nowo otwartym oknie *Menedżer DNS* klikamy prawym przyciskiem myszy nasz serwer (*SERVER2016.szkola.local*) i wybieramy *Konfiguruj serwer DNS...*, jak na rysunku 3.56, a następnie na pierwszej karcie klikamy *Dalej*.
3. Przechodzimy do karty *Wybierz akcję konfiguracji*, na której musimy wybrać strefę do instalacji. Do wyboru mamy następujące opcje:
   - *Utwórz strefę wyszukiwania do przodu* — konfiguracja przeznaczona dla małych sieci,



Rysunek 3.56. Konfiguracja serwera DNS

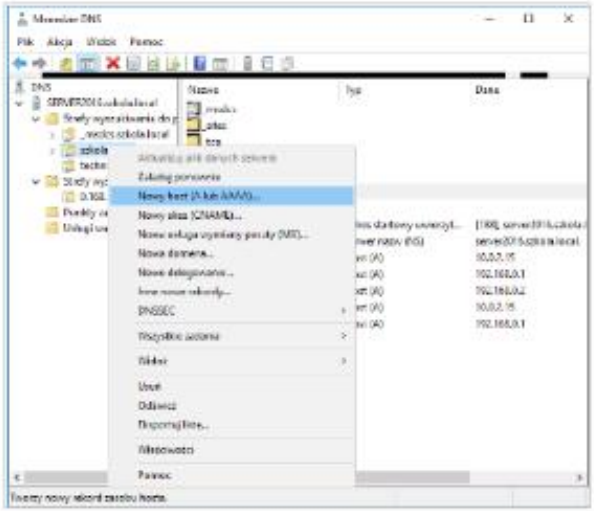
   - *Utwórz strefy wyszukiwania do przodu i wyszukiwania wstecznego* — konfiguracja przeznaczona dla dużych sieci,
   - *Skonfiguruj tylko wskazówki dotyczące serwerów głównych* — konfiguracja zalecana dla zaawansowanych użytkowników.

   Na potrzeby ćwiczenia wybieramy drugą opcję, a następnie klikamy *Dalej*.
4. Zaznaczamy *Tak, utwórz teraz strefę wyszukiwania do przodu* i klikamy *Dalej*.
5. Na karcie *Typ strefy* wybieramy *Strefa podstawowa* i klikamy *Dalej*.
6. Na karcie *Zakres replikacji strefy usługi Active Directory* zaznaczamy opcję *Do wszystkich serwerów DNS uruchomionych na kontrolerach domeny w tej domenie: szkola.local* i klikamy *Dalej*.
7. Na karcie *Nazwa strefy* wpisujemy `technikum.szkola.local` i klikamy *Dalej*.
8. Na karcie *Aktualizacja dynamiczna* wybieramy *Nie zezwalaj na aktualizacje dynamiczne*. Wszystkie dane będą wprowadzane przez użytkownika *Administrator*. Klikamy *Dalej*.
9. Teraz skonfigurujemy strefę wyszukiwania wstecznego. Potwierdzamy wybór opcji *Tak, utwórz teraz strefę wyszukiwania wstecznego* i klikamy *Dalej*.
10. Na karcie *Typ strefy* wybieramy *Strefa podstawowa* i klikamy *Dalej*.
11. Na karcie *Zakres replikacji strefy usługi Active Directory* wybieramy *Do wszystkich serwerów DNS uruchomionych na kontrolerach domeny w tej domenie: szkola.local* i klikamy *Dalej*.
12. Na karcie *Nazwa strefy wyszukiwania wstecznego* wybieramy opcję *Strefa wyszukiwania wstecznego IPv4* i klikamy *Dalej*.
13. Wpisujemy identyfikator sieci `192.168.0` i klikamy *Dalej*.

14. Na karcie *Aktualizacja dynamiczna* zaznaczamy *Nie zezwalaj na aktualizacje dynamiczne* i klikamy *Dalej*.
15. Na karcie *Usługi przesyłania dalej* zaznaczamy *Nie, nie powinien przesyłać zapytań dalej* i klikamy *Dalej*.
16. Aby zakończyć, klikamy *Zakończ*.

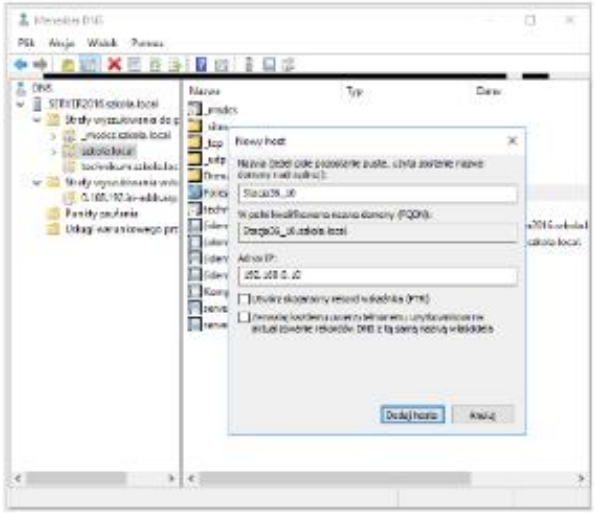
W konfigurowaniu stref wyszukiwania nie zezwoliliśmy na aktualizacje dynamiczne, teraz zatem musimy dodać rekordy do konfiguracji serwera DNS.

17. W oknie *Menedżer DNS* rozwijamy nazwę serwera, a następnie pozycję *Strefy wyszukiwania do przodu*, po czym dodajemy nowy wpis hosta (rekord typu A). Wskazujemy strefę *szkola.local*, klikamy ją prawym przyciskiem myszy i z menu wybieramy *Nowy host (A lub AAAA)...* (rysunek 3.57).

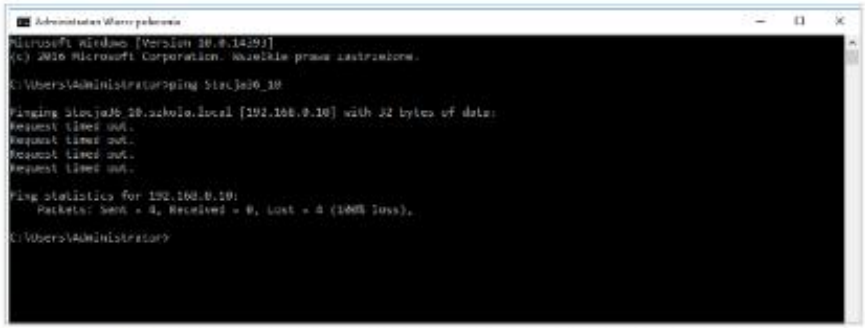


Rysunek 3.57. Dodawanie nowego hosta

18. Wprowadzamy nazwę hosta oraz jego adres IP w sieci, tak jak na rysunku 3.58, i klikamy *Dodaj hosta*. Jeśli zaznaczymy opcję *Utwórz skojarzony rekord wskaźnika (PTR)*, zostanie utworzony odpowiedni wpis w strefie przeszukiwania wstecznego.
19. Sprawdzamy, czy dodany wpis działa, np. poleceniem `ping stacja36-10` w konsoli (*cmd.exe*). Mimo że komputer nie jest podłączony, nastąpi próba pingowania adresu `192.168.0.10`, jak na rysunku 3.59.



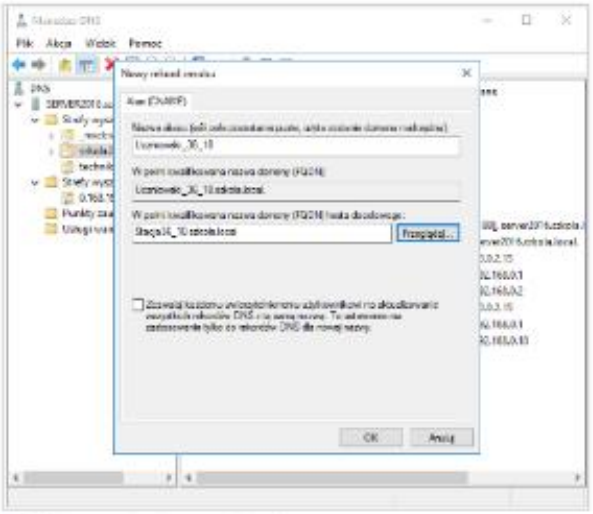
Rysunek 3.58. Konfigurowanie nowego hosta



Rysunek 3.59. Sprawdzenie działania DNS po dopisaniu rekordu nowego hosta

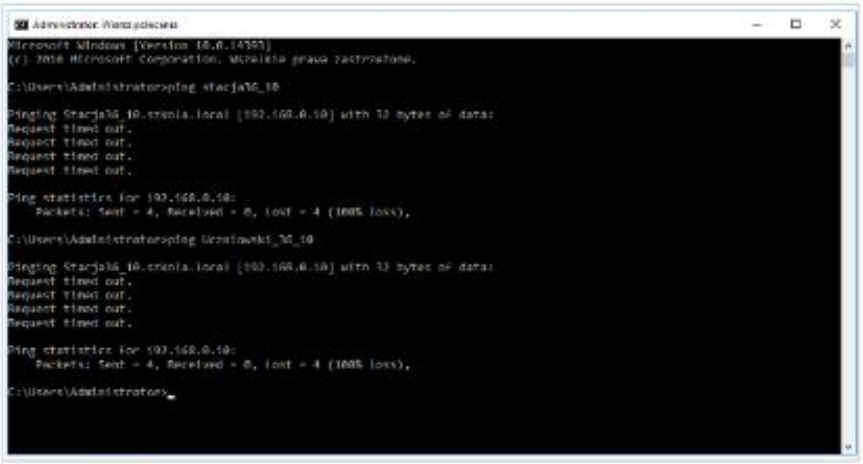
System DNS pozwala na dopisywanie do adresu IP jego aliasów (rekordów CNAME), czyli różnych nazw, za pomocą których można odwoływać się do tego samego hosta.

20. Klikamy prawym przyciskiem myszy wybraną strefę (*szkola.local*) i z menu kontekstowego wybieramy *Nowy alias (CNAME)...*.
21. Uzupełniamy pole *Nazwa aliasu* oraz pole *W pełni kwalifikowana nazwa domeny (FQDN)* (w tym celu należy kliknąć przycisk *Przeglądaj*) dla hosta docelowego (czyli tego, który utworzyliśmy w poprzednim ćwiczeniu), jak na rysunku 3.60.



Rysunek 3.60. Dodawanie aliasu do hosta

22. Po zatwierdzeniu sprawdzamy, czy system DNS poprawnie odwołuje się do hosta (rysunek 3.61).



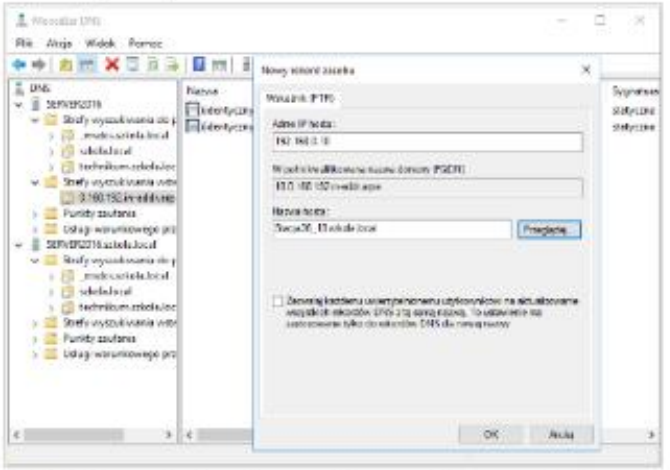
Rysunek 3.61. Sprawdzenie poprawności działania Alias (CNAME)

Jak widać na rysunku 3.61, oba polecenia `ping`, pomimo że zostały wykonane do różnych nazw (nazwy hosta, *Stacja36_10*, oraz jego aliasu, *Uczniowski_36_10*), prowadzą do tego samego adresu IP, `192.168.0.10`, który został przypisany podczas tworzenia nowego hosta.

Ćwiczenie 3.15

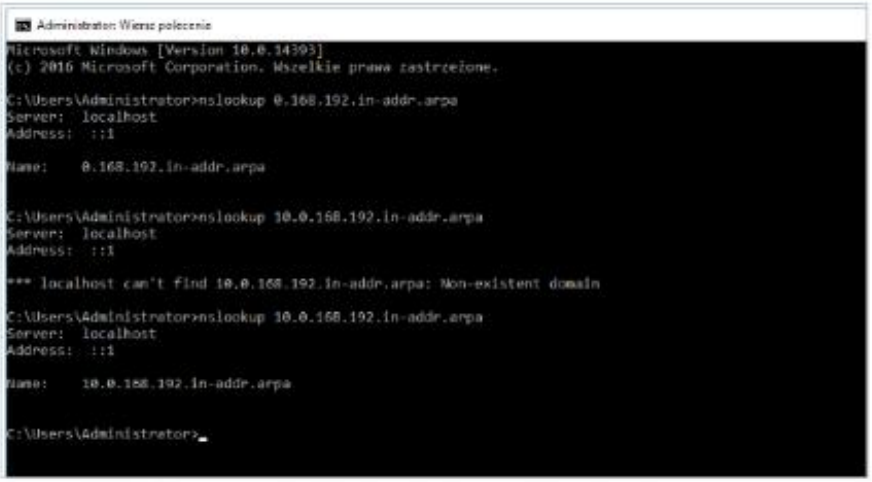
Teraz utworzymy wskaźnik przeszukiwania wstecz oraz jego alias.

1. Klikamy prawym przyciskiem myszy wybraną strefę przeszukiwania wstecz (*0.168.192.in-addr.arpa*) i z menu wybieramy *Nowy wskaźnik (PTR)...*.
2. W oknie wpisujemy adres IP hosta, `192.168.0.10`, oraz nazwę hosta, `Stacja36_10.szkola.local`, jak na rysunku 3.62.

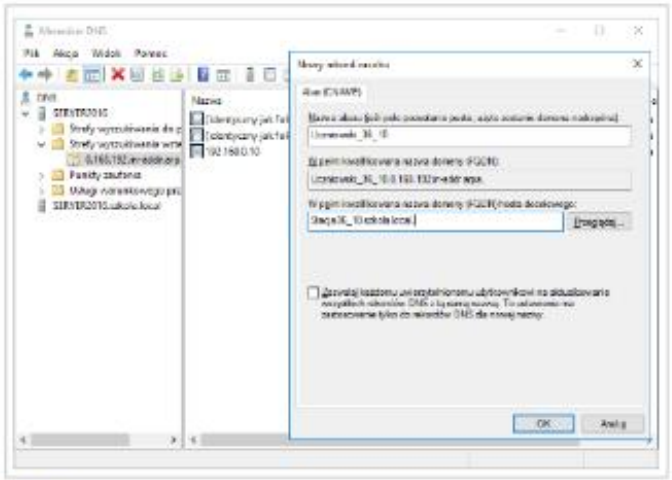


Rysunek 3.62. Dodawanie rekordu wyszukiwania wstecznego (PTR)

3. Zatwierdzamy przyciskiem *OK* i sprawdzamy ustawienia w konsoli, jak na rysunku 3.63, który pokazuje, jak będziemy sprawdzać istnienie poszczególnych stref na kolejnych etapach ćwiczenia:
   - przez wpisanie `nslookup 0.168.192.in-addr.arpa` sprawdziliśmy, czy istnieje podstawowa strefa wyszukiwania wstecznego, i wynik był pozytywny;
   - przez wpisanie `nslookup 10.0.168.192.in-addr.arpa` jeszcze przed tym, zanim dodaliśmy rekord nowego wskaźnika PTR wyszukiwania wstecznego, sprawdziliśmy, że nie istnieje taki wpis;
   - przez wpisanie `nslookup 10.0.168.192.in-addr.arpa` już po tym, jak dodaliśmy rekord nowego wskaźnika PTR wyszukiwania wstecznego, potwierdziliśmy istnienie i działanie tego wpisu.
4. W strefie wyszukiwania wstecz, tak samo jak w strefie wyszukiwania do przodu, możemy utworzyć alias przez kliknięcie prawym przyciskiem myszy wybranej strefy, a następnie wybranie z menu kontekstowego *Nowy alias (CNAME)...*.
5. W polu *Nazwa aliasu* wpisujemy `Uczniowski_36_10`, a w polu *W pełni kwalifikowana nazwa domeny (FQDN) hosta docelowego* wskazujemy wpis hosta docelowego, `Stacja36_10.szkola.local`, jak na rysunku 3.64.

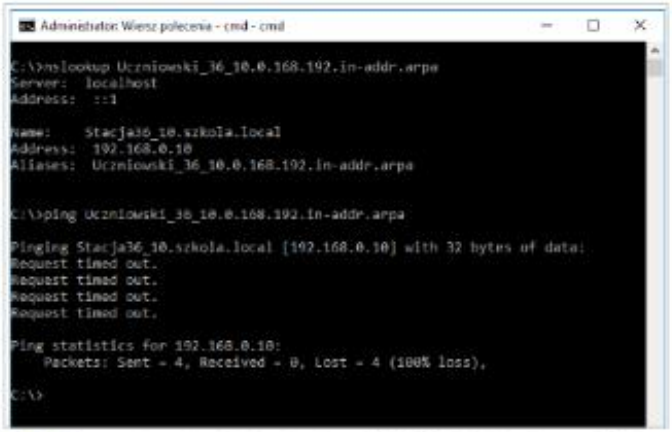


Rysunek 3.63. Sprawdzenie istnienia wpisów wyszukiwania wstecz poleceniem nslookup



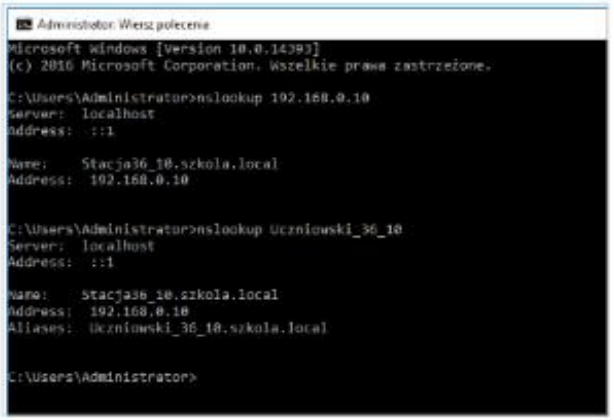
Rysunek 3.64. Konfiguracja aliasu (CNAME) dla hosta w strefie wyszukiwania wstecznego

6. Sprawdzamy poprawność konfiguracji w konsoli poleceniem `nslookup Uczniowski_36_10.0.168.192.in-addr.arpa` oraz `ping Uczniowski_36_10.0.168.192.in-addr.arpa`, jak na rysunku 3.65.



Rysunek 3.65. Sprawdzenie działania aliasu (CNAME) dla hosta w strefie wyszukiwania wstecznego

7. Z użyciem polecenia `nslookup 192.168.0.10` sprawdzimy przeszukiwanie wsteczne po adresie IP, a polecenie `nslookup Uczniowski_36_10` pozwoli nam zobaczyć przypisanie tej nazwy jako aliasu (CNAME), jak na rysunku 3.66.



Rysunek 3.66. Sprawdzenie działania wpisów przeszukiwania wstecznego za pomocą nslookup

Zadania kontrolne

1. Dodaj nowy wpis w DNS, który przypisze nazwę hosta *Dyrektor* do adresu `192.168.0.100`.
2. Dopisz w DNS dla hosta o nazwie *Dyrektor* dwa aliasy, *Jacek* i *Kowalski*.
3. Uzupełnij wpisy dla strefy wyszukiwania wstecznego.

3.11. Usługi plików i magazynowania oraz mapowanie udziałów

DEFINICJA

Serwer plików (Usługi plików i magazynowania) to rola serwera pozwalająca na utworzenie centralnego repozytorium plików, dzięki któremu pliki można przechowywać i udostępniać użytkownikom w zależności od nadanych uprawnień.

Na samym początku warto zaznaczyć, że usługa plików i magazynowania w podstawowej wersji jest już zainstalowana i nie można jej odinstalować. My doinstalujemy do niej następujące elementy:

- **Menedżer zasobów serwera plików** — ułatwi nam zarządzanie plikami i folderami na serwerze plików, co umożliwi planowanie zadań zarządzania plikami i generowanie raportów magazynowania, klasyfikowanie plików i przydziałów folderów, a także definiowanie zasad osłon plików.
- **Przestrzenie nazw systemu plików DFS** — umożliwi nam grupowanie folderów udostępnionych znajdujących się na różnych serwerach w co najmniej jedną przestrzeń nazw o logicznej strukturze. Dzięki temu użytkownicy będą widzieli każdą przestrzeń nazw jako jeden folder udostępniony zawierający podfoldery.
- **Replikacja systemu plików DFS** — aparat replikacji z wieloma wzorcami, który umożliwia synchronizowanie folderów na wielu serwerach za pośrednictwem połączeń sieciowych w sieciach lokalnych i WAN. Zastosowanie protokołu kompresji RDC (ang. *Remote Differential Compression*) pozwala na aktualizowanie tylko tych części plików, które zmieniły się od ostatniej replikacji.
- **Serwer systemu plików NFS** — udostępnia pliki komputerom z systemem UNIX i innym komputerom korzystającym z protokołu NFS.

Wiemy już, co należy doinstalować, pora zatem przystąpić do wykonania ćwiczenia. Dzięki temu uczniowie i nauczyciele „naszej szkoły" otrzymają możliwość udostępnienia np. udziału, do którego będą mieli dostęp wszyscy, a uczniowie — tylko możliwość odczytu. Dla każdego ucznia zamapujemy jego własną przestrzeń dyskową dostępną pod konkretną literą dysku.

Ćwiczenie 3.16

Dodatkowe funkcje usługi *Usługi plików i magazynowania* instaluje się w ten sam sposób jak inne role i usługi serwera.

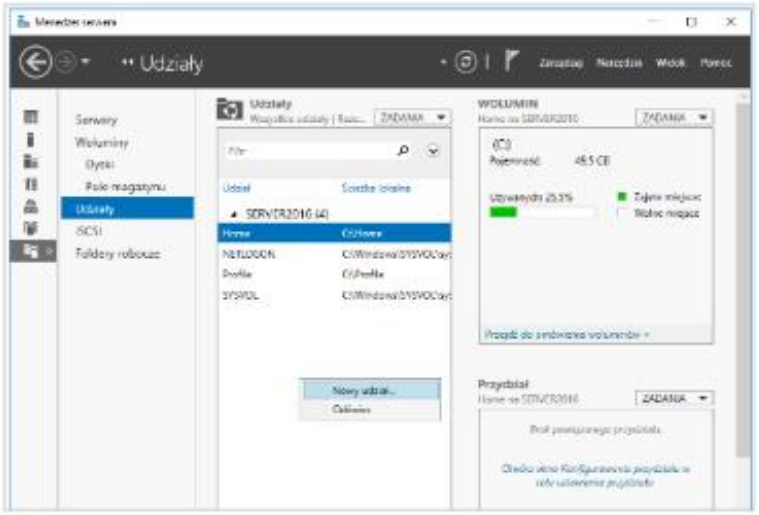
1. W Menedżerze serwera klikamy *Dodaj role i funkcje*, co uruchomi kreatora instalacji, a następnie wybieramy *Instalacja oparta na rolach lub oparta na funkcjach* i klikamy *Dalej*.
2. Wskazujemy serwer i klikamy *Dalej*.

3. Na karcie *Wybieranie ról serwera* rozwijamy *Usługi plików i magazynowania*, a dalej *Usługi plików i iSCSI* i wskazujemy następujące role: *Menedżer zasobów serwera plików*, *Przestrzeń nazw systemu plików DFS*, *Replikacja systemu plików DFS* oraz *Serwer systemu plików NFS*. Dodanie każdej z tych ról potwierdzamy przyciskiem *Dodaj funkcję*. Na koniec klikamy *Dalej*.
4. Funkcje zostały wybrane automatycznie, zatem klikamy *Dalej*.
5. Po sprawdzeniu podsumowania instalacji klikamy *Zainstaluj* i czekamy, aż instalacja się zakończy. Po jej ukończeniu klikamy *Zamknij*.

Ćwiczenie 3.17

Spróbujmy teraz udostępnić zasób o nazwie *WSPOLNY* z pełną kontrolą dla wszystkich użytkowników w naszej domenie.

1. W Menedżerze serwera klikamy *Usługi plików i magazynowania*, a następnie *Udziały*.
2. W kolumnie *Udziały* klikamy prawym przyciskiem myszy i wybieramy *Nowy udział*, jak na rysunku 3.67.

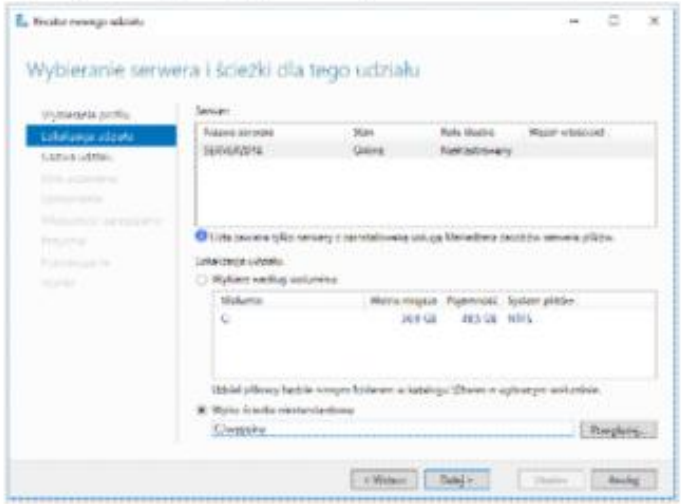


Rysunek 3.67. Dodawanie nowego udziału

3. Teraz musimy wybrać dla udziału jeden z pięciu profili:
   - *Udział SMB — szybkie* — najszybszy sposób na skonfigurowanie udziału plikowego SMB. Służy do udostępniania plików komputerom z systemem Windows. Zaawansowane opcje można skonfigurować później w oknie dialogowym *Właściwości*.
   - *Udział SMB — zaawansowane* — zaawansowany sposób udostępniania udziału plikowego SMB. Wszystkie opcje są ustawiane w trakcie konfiguracji.

- *Udział SMB — aplikacje* — profil wykorzystywany do tworzenia udziału plikowego SMB z ustawieniami odpowiednimi dla funkcji Hyper-V, baz danych i innych aplikacji serwerowych.
- *Udział NFS — szybkie* — podstawowy profil do szybkiego tworzenia i konfigurowania udziału plikowego NFS.
- *Udział NFS — zaawansowane* — zaawansowany profil do tworzenia i konfigurowania udziału plikowego NFS.

4. Wybieramy profil *Udział SMB — zaawansowane* i klikamy *Dalej*.
5. Wybieramy lokalizację udziału — my wybieramy opcję *Wpisz ścieżkę niestandardową* i tworzymy folder *C:\wspolny*, jak na rysunku 3.68, a następnie klikamy *Dalej*. Jeśli dostępny jest dodatkowy dysk, można także udostępnić cały wolumin, ale tylko jeśli nie jest to dysk systemowy (ze względu na bezpieczeństwo serwera).

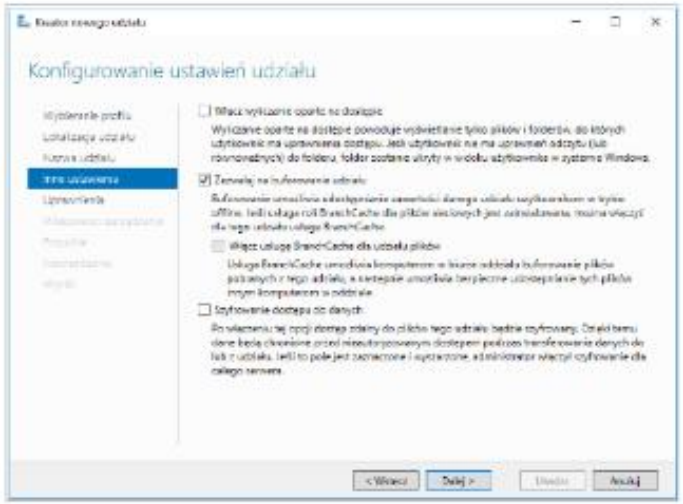


Rysunek 3.68. Konfiguracja udziału wspólnego

6. Teraz w polu *Nazwa udziału* wpisujemy nazwę udziału, `WSPOLNY`, i wypełniamy pole *Opis udziału*. Następnie klikamy *Dalej*.
7. Wyświetli się okno z szeregiem opcji (rysunek 3.69):
   - *Włącz wyliczanie oparte na dostępie* — pozwoli na ukrywanie zasobów niedostępnych dla konkretnego użytkownika;
   - *Zezwalaj na buforowanie udziału* — pozwoli na dostęp do plików w trybie offline;
   - *Szyfrowanie dostępu do danych* — pozwoli na szyfrowanie danych, dzięki czemu zwiększymy ich bezpieczeństwo.

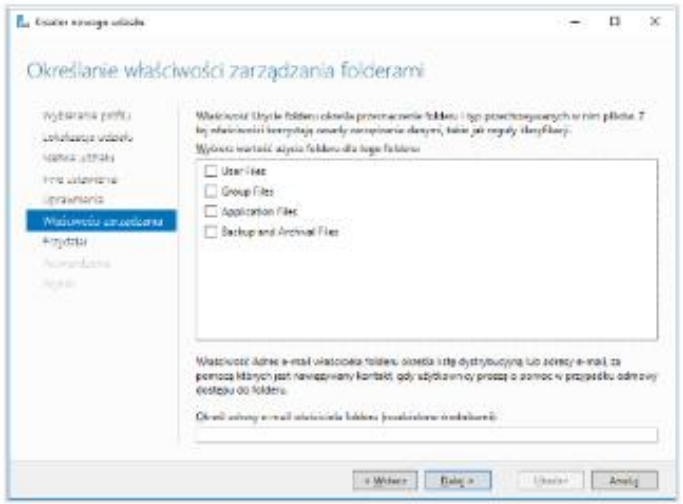
   My wybieramy tylko opcję drugą, *Zezwalaj na buforowanie udziału*, i klikamy *Dalej*.

Rysunek 3.69. Konfigurowanie innych ustawień udziału



8. Kolejnym krokiem jest ustalenie uprawnień do udziału. Jeśli nie zmienimy nic, wszyscy użytkownicy otrzymają uprawnienia *Pełnej kontroli*. Aby móc zmodyfikować ustawienia, musimy kliknąć *Dostosowywanie uprawnień*. Po zatwierdzeniu zmian przyciskiem *OK* klikamy *Dalej*.
9. Teraz na karcie *Określanie właściwości zarządzania folderami* możemy określić charakter przechowywanych danych oraz wskazać właścicieli folderu, do których będą wysyłane prośby przez użytkowników w razie problemów z dostępem do plików, a także informacje o stanach krytycznych poziomu danych (rysunek 3.70). Klikamy *Dalej*, aby przejść do następnego etapu.

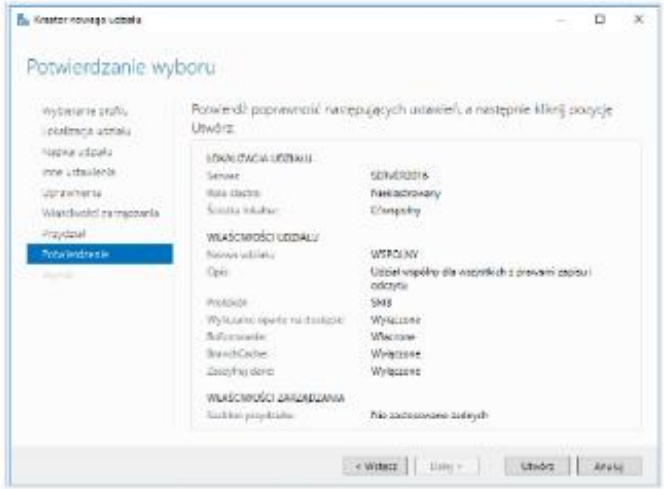
Rysunek 3.70. Określenie właściwości zarządzania folderami



10. Kolejna karta to *Stosowanie przydziału do folderu lub woluminu* — tu wybieramy jedną z dwóch opcji:
    - *Nie stosuj przydziału* — żaden przydział nie zostanie zastosowany i ilość miejsca dostępnego dla udziału będzie ograniczona ilością wolnego miejsca w woluminie;
    - *Zastosuj przydział na podstawie szablonu* — możemy określić wielkość przydziału na podstawie szablonu wraz z parametrami monitorowania.

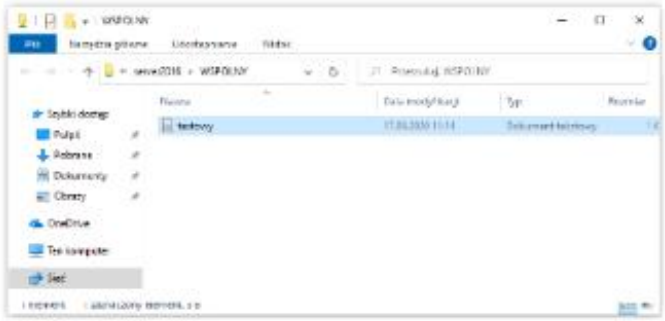
    Na potrzeby ćwiczenia wybieramy opcję *Nie stosuj przydziału*, aby w późniejszym czasie przyjrzeć się możliwości zmiany tych ustawień, i klikamy *Dalej*.

11. Ostatnim etapem jest *Potwierdzanie wyboru*. Jeśli wszystkie ustawienia są zgodne z zamierzeniem, klikamy *Utwórz* (rysunek 3.71).



Rysunek 3.71. Podsumowanie i potwierdzenie wyboru

12. Po zakończeniu działania na karcie *Wyświetl wyniki* klikamy *Zamknij*.
13. Teraz pozostaje sprawdzić działanie udostępnionego udziału za pomocą komputera klienta, do którego logujemy się z użyciem konta *Jan Nowak*.
14. Wpisujemy w pasku wyszukiwania `\\nazwa_serwera\nazwa_udziału`, w tym przypadku `\\server2016\WSPOLNY`, i uruchamiamy polecenie. Następnie tworzymy w udostępnionym udziale plik tekstowy o nazwie *testowy.txt*, jak na rysunku 3.72.
15. Teraz przechodzimy do serwera i sprawdzamy, czy w udostępnionym udziale znajduje się tak utworzony plik. Jeśli plik istnieje, to oznacza, że wszystko działa dobrze.

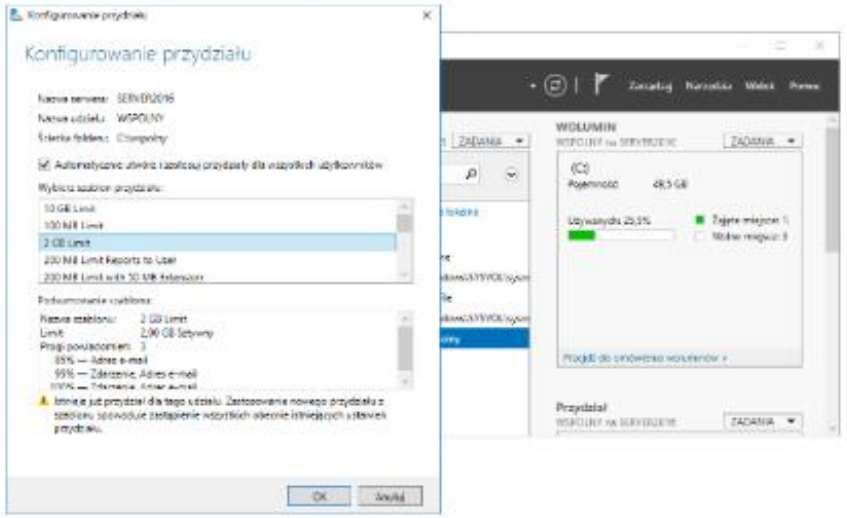


Rysunek 3.72. Sprawdzenie działania udziału na komputerze klienta

Ćwiczenie 3.18

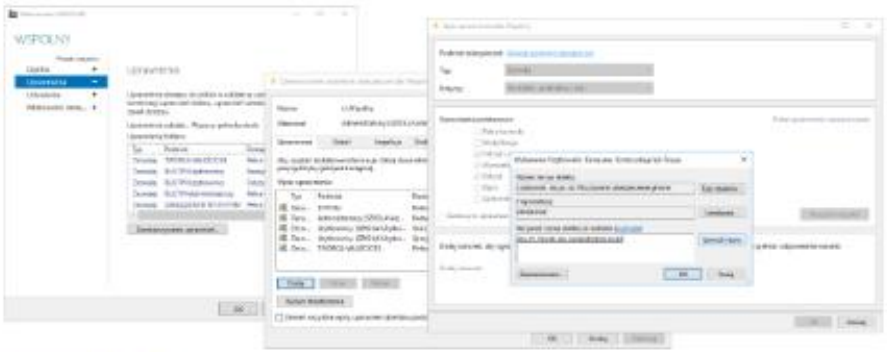
W poprzednim ćwiczeniu utworzyliśmy i udostępniliśmy udział sieciowy. Teraz spróbujemy go zmodyfikować.

1. W Menedżerze serwera klikamy *Usługi plików i magazynowania*, a następnie *Udziały*.
2. Wskazujemy udział do modyfikacji (*WSPOLNY*) i klikamy prawym przyciskiem myszy, a następnie wybieramy *Konfiguruj przydział…*, wskazujemy odpowiednią wartość przydziału i zatwierdzamy przyciskiem *OK* (rysunek 3.73).



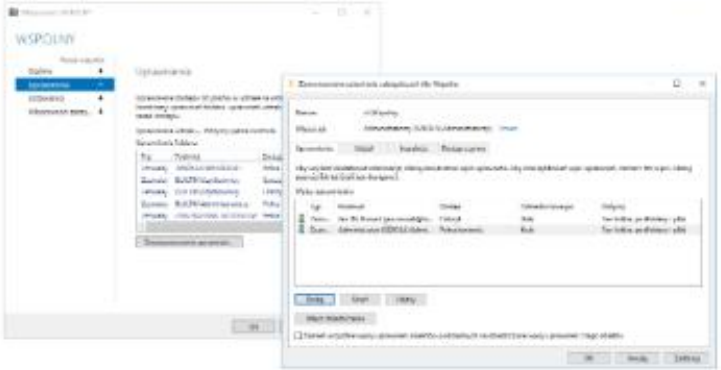
Rysunek 3.73. Ponowna konfiguracja przydziału

3. Następnie klikamy ponownie prawym przyciskiem myszy udział przeznaczony do zmodyfikowania, wybieramy *Właściwości*, kartę *Uprawnienia* i klikamy *Dostosowywanie uprawnień...*.
4. Teraz klikamy *Dodaj*, następnie *Wybierz podmiot zabezpieczeń* i wpisujemy nazwę użytkownika, któremu chcemy zmienić uprawnienia, czyli `Jan JN. Nowak`.
5. Klikamy *Sprawdź nazwy*. Zawartość pola zmieni się jak na rysunku 3.74. Klikamy *OK*. Na karcie *Wpis uprawnienia dla: Wspolny* zaznaczamy tylko *Odczyt*, usuwamy zaznaczenie pozostałych opcji i ponownie klikamy *OK*.



Rysunek 3.74. Edycja uprawnień użytkowników

6. Na karcie *Zaawansowane ustawienia zabezpieczeń dla:* klikamy *Wyłącz dziedziczenie* i w nowo otwartym oknie klikamy *Usuń wszystkie uprawnienia odziedziczone z tego obiektu*, co spowoduje usunięcie wszystkich uprawnień oprócz uprawnień naszego użytkownika.
7. Dodamy jeszcze użytkownika *Administrator* — w ten sam sposób co poprzednio, ale z uprawnieniami *Pełna kontrola*, jak na rysunku 3.75. Na koniec klikamy *OK*.



Rysunek 3.75. Podsumowanie zmiany uprawnień dla udziału

8. Logujemy się do komputera klienta na konto, które miało ograniczone uprawnienia (*Jan JN. Nowak*), i sprawdzamy, czy możemy odczytać plik znajdujący się w udostępnionym udziale oraz czy możemy w tym udziale utworzyć nowy plik. Według uprawnień, które nadaliśmy użytkownik będzie mógł odczytać plik, ale edycja i tworzenie nowego pliku będą zabronione. W ten sposób skonfigurowaliśmy udział pod konkretnego użytkownika. Tak samo konfigurujemy uprawnienia dla grup użytkowników.

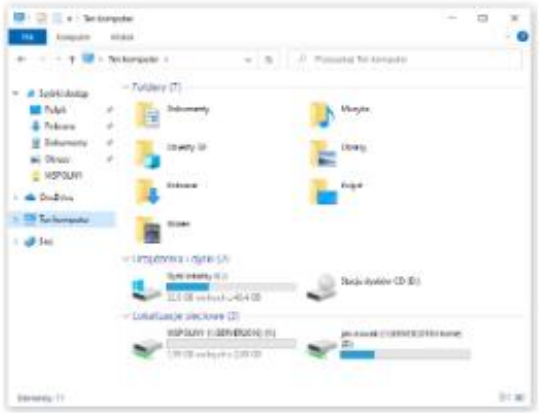
ZAPAMIĘTAJ

Mapowanie dysków sieciowych pozwala uzyskać dostęp do udziału sieciowego z poziomu Eksploratora plików bez konieczności wyszukiwania lub wpisywania za każdym razem adresu sieciowego. Dzięki mapowaniu na konkretny udział sieciowy przypisywana jest litera dysku.

Aby zamapować udział sieciowy w systemie klienta, tak aby użytkownik po zalogowaniu na swoje konto miał podpięty w systemie dysk o literze *Y* kierujący do udziału *\\SERVER 2016\WSPOLNY*, musimy wykonać skrypt z poleceniem: `net use Y: \\SERVER2016\WSPOLNY` i podpiąć go pod użytkownika. Sposób postępowania przedstawia następne ćwiczenie.

Ćwiczenie 3.19

1. Uruchamiamy Notatnik, w którym wpisujemy polecenie `net use Y: \\SERVER2016\WSPOLNY`. Plik zapisujemy jako *mapowanie.bat*.
2. Następnie przenosimy tak utworzony plik do lokalizacji *%SystemRoot%\SYSVOL\sysvol\{nazwadomeny}\scripts* (domyślna lokalizacja skryptów w systemie Windows), w naszym przypadku *C:\Windows\SYSVOL\sysvol\szkola.local\scripts*.
3. Teraz musimy uruchomić przystawkę *Użytkownicy i komputery usługi Active Directory*. Klikamy kontener *Users* i wskazujemy użytkownika, któremu chcemy podpiąć mapowanie udziału sieciowego. W naszym przypadku jest to użytkownik *Jan JN. Nowak*.
4. Klikamy wybranego użytkownika prawym przyciskiem myszy, a następnie *Właściwości*.
5. Klikamy kartę *Profil* i w miejscu *Skrypt logowania* wpisujemy nazwę skryptu, który będzie wykonywał mapowanie wybranego udziału sieciowego (*mapowanie.bat*). Nie musimy podawać całej ścieżki, gdyż skrypt znajduje się w domyślnej lokalizacji skryptów. Zatwierdzamy przyciskiem *OK*.
6. Teraz możemy się logować przez konto użytkownika *Jan JN. Nowak* na komputerze klienta w celu sprawdzenia zamapowania udziału sieciowego (rysunek 3.76). Widzimy, że udział został zamapowany pod literą *Y*, oraz widzimy ilość przydzielonego udziałowi miejsca, którą w ćwiczeniu 3.18 ustaliliśmy na 2 GB.



Rysunek 3.76. Sprawdzenie zamapowania udziału sieciowego pod literą Y

Zadania kontrolne

1. Utwórz użytkownika domeny o nazwie *Jacek JK. Kowalski*.
2. Utwórz udział sieciowy *C:\Zasoby* o nazwie udziału *ZASOBY* o limicie danych 10 GB, do którego użytkownik *Jacek JK. Kowalski* ma uprawnienia *Pełna kontrola* i który wszystkim pozostałym użytkownikom umożliwia tylko odczyt dokumentów.
3. Użytkownik *Jacek JK. Kowalski* ma mieć zamapowany udział sieciowy *ZASOBY* pod literą *J*.

3.12. Dostęp zdalny i routing

Rola serwera *Dostęp zdalny* jest kolejnym składnikiem systemu Windows Server 2016/2019, który integruje w sobie następujące funkcje:

- ***DirectAccess i VPN*** — umożliwia użytkownikom łączenie się z ich sieciami firmowymi, o ile mają dostęp do internetu. DirectAccess pozwala zarządzać komputerami przenośnymi, kiedy są podłączone do internetu, dzięki czemu użytkownicy mobilni mają dostęp do najnowszych zasad bezpieczeństwa. Aby umożliwić nawiązywanie połączeń z klientami i osobami pracującymi zdalnie, sieć VPN korzysta z połączenia internetowego oraz kombinacji technik tunelowania i szyfrowania danych.
- ***Routing*** — zapewnia użytkownikom końcowym możliwość korzystania z internetu na komputerach klientów.
- ***Serwer proxy aplikacji sieci Web*** — umożliwia publikowanie wybranych aplikacji opartych na protokołach HTTP i HTTPS z sieci firmowej na urządzeniach klienckich znajdujących się poza tą siecią.

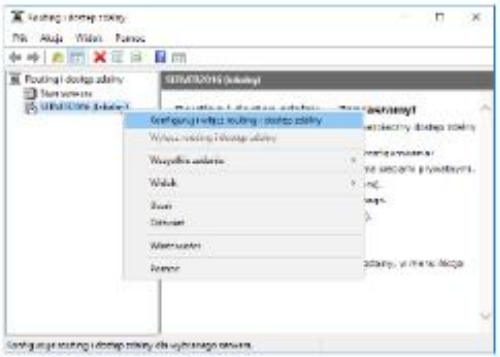
Spróbujmy teraz w ramach ćwiczenia uruchomić dostęp do sieci internet na komputerze klienta. Dla pewności warto się upewnić, czy dostęp do sieci internet jest zarówno na serwerze, jak i komputerze klienta. Najprościej będzie wykonać w konsoli polecenie `ping 194.204.152.34` (to adres serwera DNS jednego z dostawców internetu w Polsce, stale dostępny) — na serwerze adres powinien odpowiadać (serwer ma dostęp do internetu), a na kliencie nie.

To ćwiczenie pozwoli usunąć router z naszej przykładowej szkolnej sieci, gdyż jego funkcję będzie pełnił Windows Server. Dzięki temu zyskamy możliwość zarządzania ustawieniami dostępu do internetu z poziomu tego systemu. W dalszych podrozdziałach zapoznasz się z usługą *Pulpit zdalny*, dzięki czemu dostęp do serwera będziesz mógł uzyskać z każdego miejsca na świecie.

Teraz wykonamy ćwiczenia, które pozwolą na uruchomienie usługi routingu.

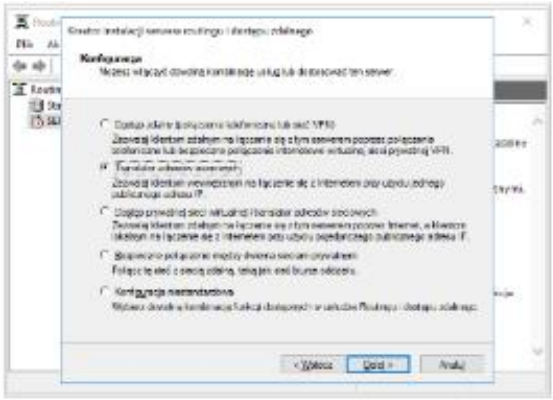
Ćwiczenie 3.20

1. Uruchamiamy Menedżer serwera. Klikamy *Dodaj role i funkcje*, wybieramy *Instalacja oparta na rolach lub oparta na funkcjach* i klikamy *Dalej*.
2. Wskazujemy serwer instalacji i kliknięciem *Dalej* przechodzimy do wyboru roli serwera.
3. Wybieramy *Dostęp zdalny* i przechodzimy *Dalej*.
4. Na karcie *Wybieranie funkcji* klikamy *Dalej* i przechodzimy do wyboru ról, gdzie zaznaczamy *DirectAccess i VPN* oraz *Routing*. Potwierdzamy wybór przyciskiem *Dodaj funkcję* i klikamy *Dalej*.
5. Przy instalacji dostępu zdalnego wymagana jest instalacja *Rola serwera sieci web (IIS)*, którą potwierdzamy bez wprowadzania zmian przyciskiem *Dalej*.
6. W podsumowaniu instalacji podglądamy wybrane opcje i jeśli wszystko się zgadza, klikamy *Zainstaluj*.
7. Po zakończeniu instalacji klikamy *Zamknij*. Następnym etapem będzie konfiguracja routingu.
8. W Menedżerze serwera klikamy *Narzędzia* i wybieramy *Routing i dostęp zdalny*.
9. W przystawce konsoli MMC wskazujemy prawym przyciskiem myszy nasz serwer i wybieramy *Konfiguruj i włącz routing i dostęp zdalny* (rysunek 3.77). Uruchomi się kreator, który przeprowadzi nas przez proces konfiguracji.



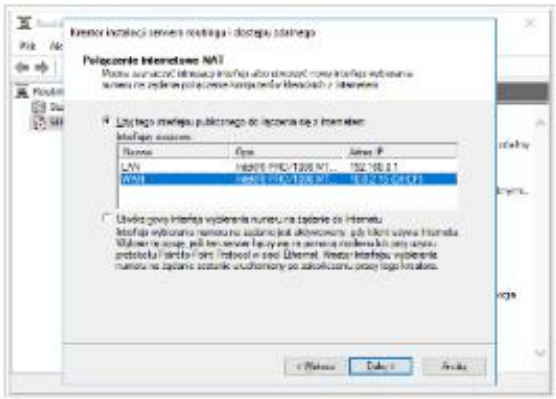
Rysunek 3.77. Przystawka Routing i dostęp zdalny

10. Na karcie z informacjami wstępnymi klikamy *Dalej* i przechodzimy do karty wyboru profilu konfiguracji (rysunek 3.78).



Rysunek 3.78. Wybór profilu konfiguracji routingu i dostępu zdalnego

11. Wybieramy *Translator adresów sieciowych* i klikamy *Dalej*. Następnie wskazujemy interfejs sieciowy odpowiedzialny za dostęp do internetu (w naszym przypadku jest to interfejs opisany jako *WAN*) i klikamy *Dalej* (rysunek 3.79).



Rysunek 3.79. Wybór połączenia internetowego dla NAT

12. Na koniec klikamy *Zakończ*, by zakończyć konfigurację funkcji *Routing i dostęp zdalny*. W przystawce konsoli ikona serwera zmieni się z czerwonej na zieloną, a po uruchomieniu internetu na komputerze klienta będą zmieniały się wartości w informacji o liczbie bajtów przychodzących i wychodzących, co będzie świadczyło o działaniu usługi (rysunek 3.80). Aby sprawdzić poprawność konfiguracji, uruchamiamy przeglądarkę na komputerze klienta lub w konsoli wpisujemy polecenie `ping 194.204.152.34`.



Rysunek 3.80. Analiza pakietów routingu

Zadania kontrolne

1. Wyłącz serwer routingu na serwerze, uruchom ponownie klienta i sprawdź, czy masz na kliencie dostęp do sieci internet.
2. Zmień adres IP klienta na inny, np. przez zmianę zastrzeżenia na serwerze DHCP.
3. Poprawnie skonfiguruj serwer routingu na serwerze i sprawdź, czy na kliencie jest dostępna sieć internet.

3.13. Usługa drukowania i zarządzania dokumentami

DEFINICJA

Serwer wydruku (ang. *Print Server*) to komputer bądź inne urządzenie, które odbiera zadania drukowania od klientów i przekazuje je do urządzeń drukujących w sieci lub lokalnie. Serwer wydruku może używać priorytetów drukarek, komputerów lub użytkowników w celu usprawnienia pracy.

Usługa drukowania i zarządzania dokumentami, popularnie zwana serwerem wydruku, umożliwia użytkownikom scentralizowanie zadań zarządzania serwerami wydruku i drukarkami sieciowymi. Dzięki niej możemy ustalić m.in., kto może drukować, w jakich godzinach drukarka ma być dostępna czy też pule wydruków. Za pomocą tej roli można również pobierać dokumenty zeskanowane przez połączone z siecią skanery i kierować je do udostępnionych zasobów sieciowych.

Drukarka łączy się z komputerem przy użyciu jednego z trzech podstawowych interfejsów. Są to:

- interfejs USB — jest to połączenie lokalne; aby zatem można było udostępnić drukarkę w sieci, komputer, do którego drukarka jest podłączona, musi pracować w momencie wysyłania dokumentu do wydrukowania;

- interfejs sieciowy przewodowy — pozwala na przyłączenie drukarki bezpośrednio do sieci za pomocą przewodu ethernetowego, dzięki czemu jest ona dostępna w każdej chwili, gdyż nie jest zależna od żadnego komputera w sieci;
- interfejs sieciowy bezprzewodowy (Wi-Fi) — pozwala korzystać z drukarki w ten sam sposób jak z użyciem interfejsu sieciowego przewodowego, tyle że drukarka do łączenia się z siecią wykorzystuje technikę bezprzewodową.

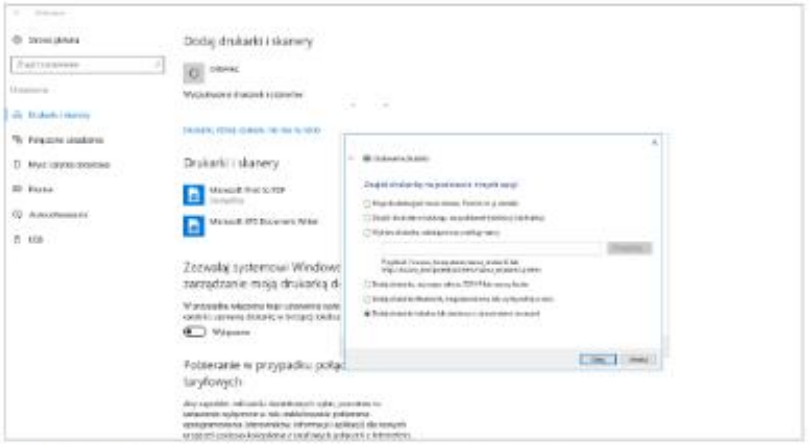
Dzięki tej usłudze nasi uczniowie oraz nauczyciele zyskają możliwość drukowania na konkretnych drukarkach. Dodatkowo drukarki mogą być ustawione w różnych miejscach w szkole (takich jak pokój nauczycielski, dyrektor, pracownia informatyczna), ale do zarządzania nimi używa się serwera, co sprawia, że administrator szkoły nie musi podłączać drukarek do komputerów ani ich udostępniać. Wystarczy podłączyć sprzęt do sieci i zainstalować sterowniki.

Również w przypadku tej funkcji, aby zobrazować działanie usługi, posłużymy się przykładem i wykonamy ćwiczenie, w którym użyjemy połączenia LPT, gdyż dzięki temu nie będzie wymagana obecność drukarki w trakcie instalacji.

Ćwiczenie 3.21

Zacznijmy od zainstalowania usługi *Usługa drukowania i zarządzania dokumentami*.

1. Aby zainstalować usługę, standardowo uruchamiamy Menedżer serwera, wybieramy *Dodaj role i funkcje*, a następnie *Instalacja oparta na rolach lub oparta na funkcjach* i klikamy *Dalej*.
2. Wskazujemy nasz serwer i klikamy *Dalej*, wybieramy *Usługi drukowania i zarządzania dokumentami*, potwierdzamy przyciskiem *Dodaj funkcje*, a następnie klikamy *Dalej*.
3. Na karcie *Wybieranie funkcji* klikamy *Dalej*. Na karcie *Wybieranie usług ról* mamy do wyboru następujące opcje:
   - *Serwer wydruku* — instaluje przystawkę *Zarządzanie drukowaniem*, która pozwoli nam konfigurować wiele drukarek lub serwerów wydruku, zarządzać nimi, a także migrować drukarki na innych serwerach wydruku opartych na systemie Windows;
   - *Drukowanie internetowe* — konfiguruje witrynę internetową po to, aby użytkownicy mogli zarządzać zadaniami drukowania na serwerze poprzez przeglądarkę;
   - *Serwer skanów rozproszonych* — pozwala konfigurować skanery sieciowe i nimi zarządzać, a także zarządzać zadaniami skanowania, dzięki czemu dokumenty ze skanerów trafiają do odpowiedniej lokalizacji;
   - *Usługa LPD* — pozwala drukować na drukarkach sieciowych z komputerów opartych na systemach UNIX i innych.
4. Na potrzeby ćwiczenia wybieramy pierwszą opcję, *Serwer wydruku*, i klikamy *Dalej*.
5. Na stronie, na której potwierdza się parametry instalacji, możemy zaznaczyć opcję *Automatycznie uruchom ponownie serwer docelowy, jeśli będzie to potrzebne*, aby system w razie potrzeby uruchomił się ponownie. Jeśli konfiguracja jest właściwa, klikamy *Zainstaluj* (rysunek 3.81).



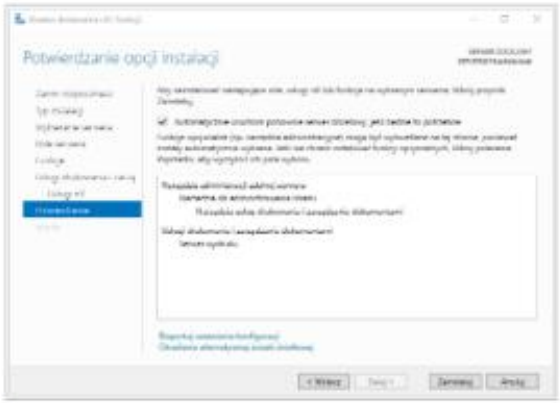
Rysunek 3.81. Podsumowanie instalacji Usługi drukowania i zarządzania dokumentami

6. Po zakończeniu instalacji klikamy *Zamknij*.

Ćwiczenie 3.22

Teraz spróbujemy dodać drukarkę do naszego serwera. Będzie to drukarka z interfejsem LPT, która nie musi być obecna podczas instalacji.

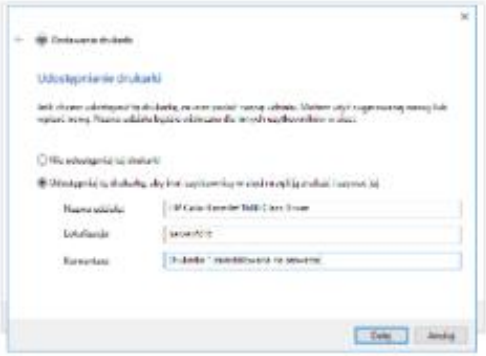
1. Klikamy *Start/Ustawienia/Urządzenia/Drukarki i skanery/Dodaj drukarkę lub skaner*. Rozpocznie się wyszukiwanie sprzętu. Klikamy przycisk *Drukarki, której szukam, nie ma na liście* (rysunek 3.82).



Rysunek 3.82. Dodawanie drukarki

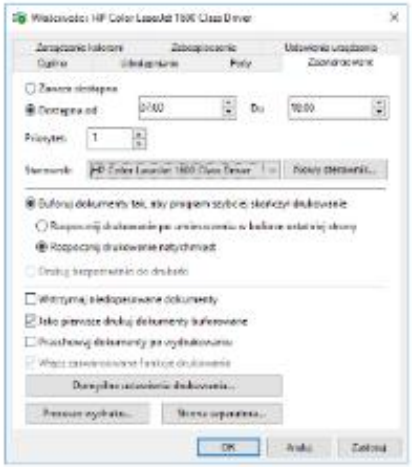
2. Wybieramy *Dodaj drukarkę lokalną lub sieciową z ustawieniami ręcznymi* i klikamy *Dalej*.

3. Wybieramy *LPT1: (Port drukarki)* i klikamy *Dalej*. Są to ustawienia przykładowe zastosowane po to, aby skonfigurować drukarkę bez podłączenia fizycznego urządzenia.
4. Wskazujemy producenta — HP, wybieramy drukarkę — *HP Color LaserJet 1600 Class Driver* i klikamy *Dalej*.
5. System rozpocznie instalowanie sterowników drukarki, a my zatwierdzamy nazwę i klikamy *Dalej*.
6. Udostępniamy drukarkę, dodawszy do niej w razie potrzeby komentarz, jak na rysunku 3.83, i klikamy *Dalej*.
7. Na koniec klikamy *Zakończ*. Drukarka została zainstalowana na serwerze.
8. Uruchamiamy *Panel sterowania/Wyświetl urządzenia i drukarki*, otwieramy zainstalowaną drukarkę, po czym z menu *Drukarka* wybieramy *Właściwości*. Następnie przechodzimy do karty *Zaawansowane*, w której ustawimy godziny dostępności drukarki na 7:00 – 18:00, czyli godziny pracy szkoły, jak na rysunku 3.84.

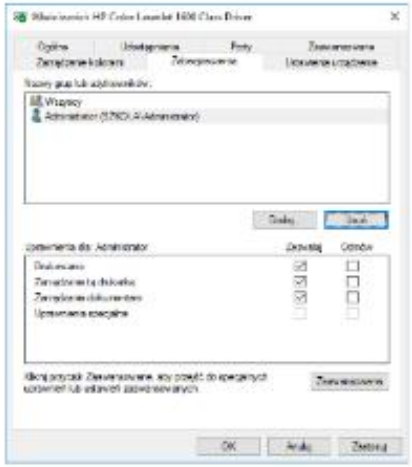


Rysunek 3.83. Udostępnianie instalowanej drukarki

9. Przechodzimy do zakładki *Zabezpieczenia* i nadajemy uprawnienia drukowania grupie *Wszyscy* oraz pełne uprawnienia kontu *Administrator*, jak na rysunku 3.85.

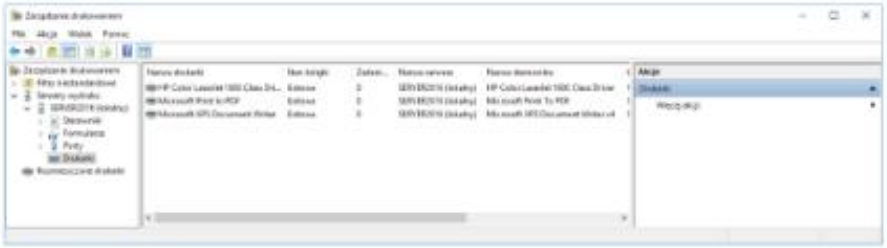


Rysunek 3.84. Ustawianie godzin dostępności drukarki



Rysunek 3.85. Nadawanie uprawnień do drukarki

10. Teraz przechodzimy do Menedżera serwera i wybieramy *Narzędzia/Zarządzanie drukowaniem*.
11. Rozwijamy pozycję *Serwery wydruku*, a następnie *SERVER2016 (lokalny)* i wskazujemy *Drukarki*, by sprawdzić, czy zainstalowana drukarka jest dostępna (rysunek 3.86).

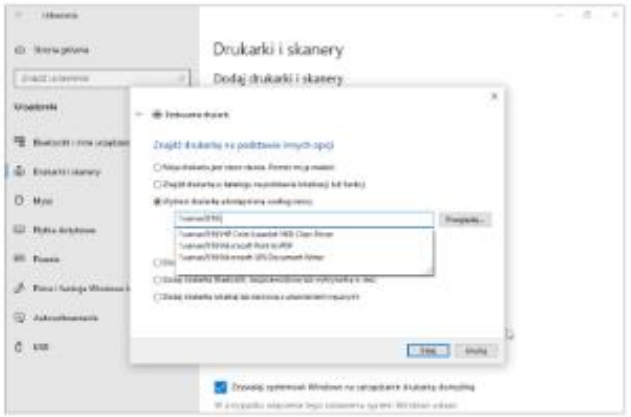


Rysunek 3.86. Przystawka konsoli MMC — Zarządzanie drukarkami

Ćwiczenie 3.23

Teraz musimy zainstalować drukarkę na komputerze klienta.

1. Logujemy się do komputera klienta za pomocą konta z uprawnieniami administratora (w naszym przypadku jest to konto *Administrator*).
2. Klikamy *Start/Ustawienia/Urządzenia/Drukarki i skanery/Dodaj drukarkę lub skaner*.
3. System sam nie znajdzie drukarki, dlatego musimy kliknąć *Drukarki, której szukam, nie ma na liście*.
4. W kreatorze wybieramy *Wybierz drukarkę udostępnioną według nazwy* i wpisujemy `\\server2016\HP Color LaserJet 1600 Class Driver`. Wystarczy, że wpiszemy nazwę serwera, a system sam nam podpowie dostępne drukarki (rysunek 3.87).



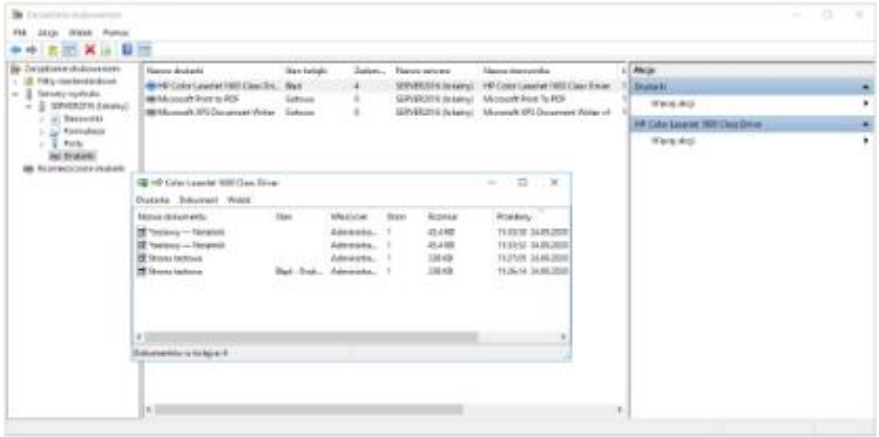
Rysunek 3.87. Dodawanie drukarki sieciowej na komputerze klienta

5. Klikamy *Dalej*. Rozpocznie się proces łączenia z drukarką i jej instalacja, którą kończymy przyciskiem *Zakończ*.
6. Aby sprawdzić działanie drukarki, otwieramy Notatnik, wpisujemy dowolny tekst i wciskamy kombinację klawiszy *Ctrl+P* (*Drukuj*). Widzimy, że drukarka jest dostępna jako domyślna, zatem klikamy *Drukuj* (rysunek 3.88).



Rysunek 3.88. Drukowanie z klienta na drukarce udostępnionej w sieci

7. Wydruk został wysłany do drukarki. Ponieważ drukarka jest zainstalowana, ale nie podłączona, pojawi się komunikat o błędzie, ale na serwerze, w oknie *Zarządzanie drukowaniem* zobaczymy kolejkę wydruków (rysunek 3.89).

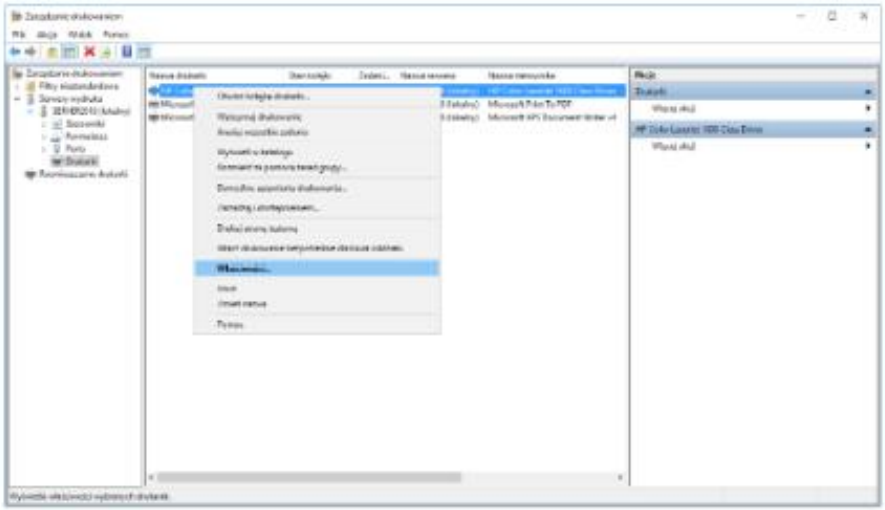


Rysunek 3.89. Podgląd kolejki wydruku w przystawce Zarządzanie drukowaniem konsoli MMC

Ćwiczenie 3.24

Teraz spróbujmy odmówić uprawnień do drukowania konkretnemu użytkownikowi, gdyż na razie drukować mogą wszyscy.

1. Logujemy się na koncie *Jan JN. Nowak* do komputera klienta i instalujemy drukarkę na koncie klienta tak, jak to zrobiliśmy w ćwiczeniu 3.23, a następnie sprawdzamy, czy możliwe jest drukowanie. Ze względu na nadane uprawnienia funkcja drukowania działa.
2. W przystawce *Zarządzanie drukowaniem* klikamy prawym przyciskiem myszy drukarkę i wybieramy *Właściwości...* (rysunek 3.90).



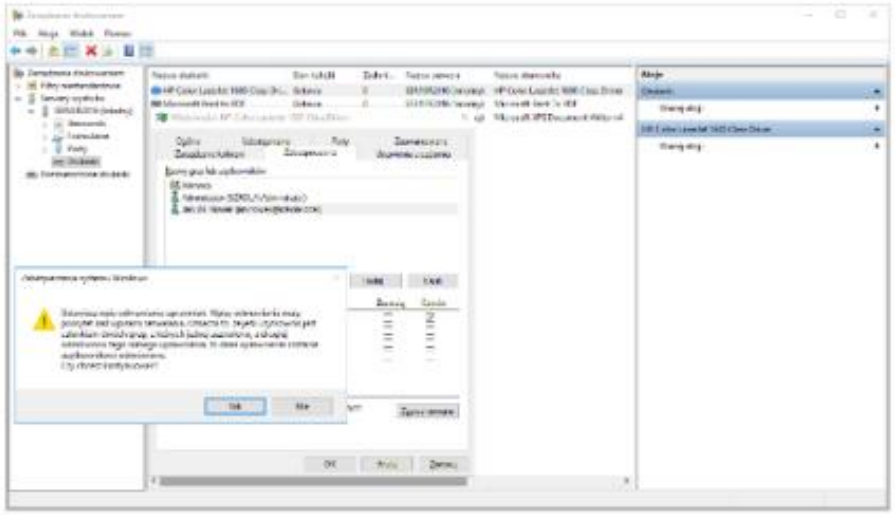
Rysunek 3.90. Wybieranie opcji właściwości drukarki

3. Przechodzimy do zakładki *Zabezpieczenia* i dodajemy użytkownika *Jan JN. Nowak*, któremu odmawiamy uprawnień do drukowania, a następnie klikamy *OK*.

ZAPAMIĘTAJ

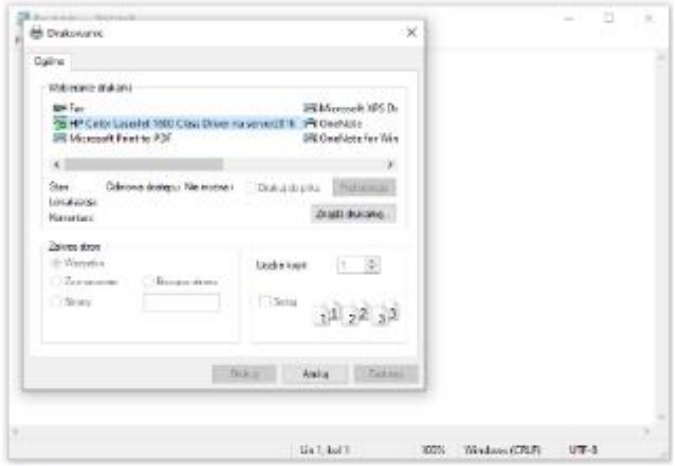
W systemach operacyjnych odmowa ma wyższy priorytet niż zezwolenie, tzn. jeśli użytkownik należy do dwóch grup i w pierwszej z nich pozwolono mu na drukowanie, a w drugiej odmówiono, to system automatycznie odmówi mu tych uprawnień. Dzięki temu unikamy niezamierzonego przydzielenia uprawnienia użytkownikowi, który nie powinien go mieć.

4. Potwierdzamy informacje o odmowie uprawnień drukowania (rysunek 3.91).



Rysunek 3.91. Odmawianie uprawnień drukowania użytkownikowi

5. Logujemy się na komputerze klienta za pomocą konta *Jan JN. Nowak*, uruchamiamy Notatnik i kombinacją klawiszy *Ctrl+P* próbujemy wydrukować zawartość pliku. Nasza drukarka jest dostępna, ale nie możemy na niej drukować ze względu na ograniczone uprawnienia (rysunek 3.92).



Rysunek 3.92. Sprawdzanie możliwości drukowania z konta z ograniczonymi uprawnieniami

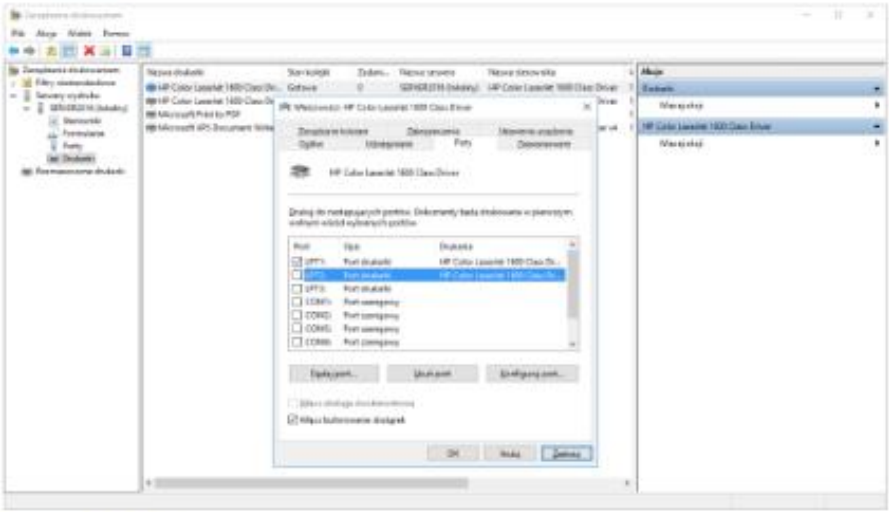
UWAGA

Pula drukarek pozwala efektywniej drukować dokumenty. Pulę drukarek tworzy się z minimum dwóch urządzeń. Dzięki temu każde zadanie wydruku, które dotrze do serwera, zostanie wysłane na pierwszą wolną drukarkę, co usprawni proces drukowania.

W ostatnim ćwiczeniu tego rozdziału utworzymy pulę drukarek. Musimy zacząć od zainstalowania drugiej drukarki, dlatego ponownie wykonamy ćwiczenie 3.22. Należy pamiętać, aby podczas instalowania drukarki wybrać port *LPT2*, gdyż *LPT1* jest już wykorzystywany.

Ćwiczenie 3.25

1. Klikamy prawym przyciskiem myszy drukarkę przeznaczoną do puli i wybieramy *Właściwości*.
2. Przechodzimy do karty *Porty*, zaznaczamy *Włącz buforowanie drukarek* i klikamy *Zastosuj* (rysunek 3.93).



Rysunek 3.93. Włączanie buforowania drukarek

3. Po włączeniu buforowania drukarek możemy zaznaczyć port nowo dodanej drukarki, która będzie pracowała w puli drukarek, i klikamy *OK*.

Pula drukarek została utworzona. Dodatkowo we właściwościach zaawansowanych każdej drukarki możemy ustawić priorytet, dzięki czemu drukarka o wyższym priorytecie będzie drukowała w pierwszej kolejności.

łania kontrolne

1. Odinstaluj z systemu dwie drukarki *HP Color LaserJet 1600 Class Driver*.
2. Zainstaluj drukarkę *HP Color LaserJet 2500 PCL6 Class Driver* na porcie *LPT1* i udostępnij ją pod nazwą *Drukarka technikum*.
3. Zainstaluj drukarkę *HP Color LaserJet 2700 PCL6 Class Driver* na porcie *LPT2* i udostępnij ją pod nazwą *Drukarka liceum*.
4. Przypisz możliwość drukowania na obu zainstalowanych drukarkach oraz zarządzania nimi wszystkim użytkownikom, a użytkownikowi *Administrator* przypisz pełne uprawnienia do obu urządzeń.
5. Sprawdź, czy użytkownicy *Joanna Kowalska* i *Maciej Nowak* mogą zainstalować drukarki na komputerze klienta i na nich drukować.
6. Po sprawdzeniu odmów drukowania użytkownikom *Joanna Kowalska* i *Maciej Nowak*, a następnie sprawdź, czy mogą drukować.
7. Ustaw dostępność drukarek w godzinach 9:00 – 15:00.
8. Skonfiguruj pulę drukarek z obydwu zainstalowanych, w której HP Color LaserJet 2700 PCL6 Class Driver będzie miała priorytet 10, a HP Color LaserJet 2700 PCL6 Class Driver — priorytet 4.

3.14. Serwery IIS, WWW i FTP

W tym podrozdziale omówimy internetowe usługi informacyjne, a także uruchomimy własną stronę WWW i uzyskamy dostęp do niej za pomocą protokołu FTP, dzięki czemu nasza szkoła będzie mogła przechowywać swoją stronę internetową na własnym serwerze.

DEFINICJA

Internetowe usługi informacyjne (ang. *Internet Information Services*, IIS) to usługa dostępna w systemach Windows Server, odpowiedzialna za obsługę oraz utrzymanie stron WWW i serwerów FTP.

Aby móc uruchomić na serwerze stronę WWW, musimy rozpocząć od zainstalowania usługi IIS — jeśli jeszcze nie jest zainstalowana. Usługa IIS bardzo często jest automatycznie instalowana wraz z innymi rolami serwera. Tak też jest w naszym przypadku — usługa została zainstalowana przy okazji instalacji roli *Routing* (ćwiczenie 3.20). Oprócz serwera WWW uruchomimy serwer FTP, który doinstalujemy w następnym ćwiczeniu.

DEFINICJA

FTP (ang. *File Transfer Protocol*) to protokół komunikacyjny działający na porcie 21, używany do przesyłania plików pomiędzy **klientem** a **serwerem**. Do działania wymaga oprogramowania serwera FTP oraz oprogramowania klienta FTP.

DEFINICJA

Serwer FTP to komputer w sieci, który ma zainstalowane oprogramowanie pozwalające na realizowanie połączeń i udostępnianie zasobów za pomocą protokołu FTP.

DEFINICJA

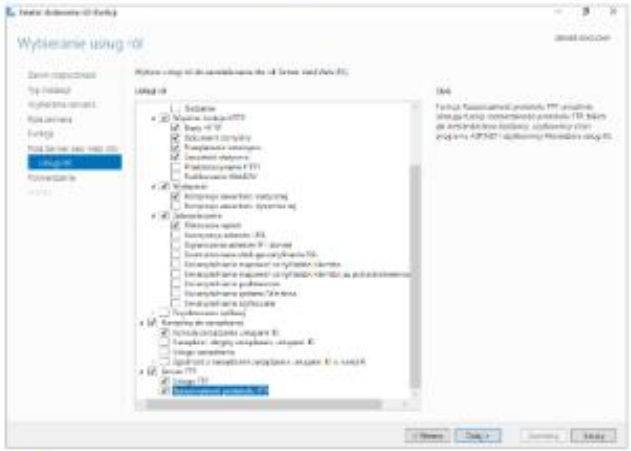
Klient FTP to oprogramowanie zdolne do nawiązywania połączeń za pomocą protokołu FTP, takie jak FileZilla.

Użytkownicy FTP mogą się uwierzytelniać przez logowanie zwykłym tekstem, zazwyczaj w postaci nazwy użytkownika i hasła, ale mogą też łączyć się anonimowo, jeśli serwer jest skonfigurowany tak, aby na to zezwalał. Do transmisji FTP często stosuje się technikę SSL/TLS (FTPS), która szyfruje nazwę użytkownika, hasło oraz zawartość.

Jeśli usługa IIS jeszcze nie została zainstalowana, wykonajmy ćwiczenie, które pokaże, jak to zrobić.

Ćwiczenie 3.26

1. Uruchamiamy Menedżer serwera, wybieramy *Dodaj role i funkcje/Instalacja oparta na rolach lub oparta na funkcjach* i klikamy *Dalej*. Wskazujemy serwer i ponownie klikamy *Dalej*.
2. Wybieramy rolę *Serwer sieci Web (IIS)*, potwierdzamy *Dodaj funkcje* i klikamy *Dalej*.
3. Na karcie *Wybieranie funkcji* klikamy *Dalej*.
4. Na karcie *Usługi ról* wybieramy potrzebne role, czyli zaznaczamy dodatkowo *Serwer FTP*, jak na rysunku 3.94, i klikamy *Dalej*.



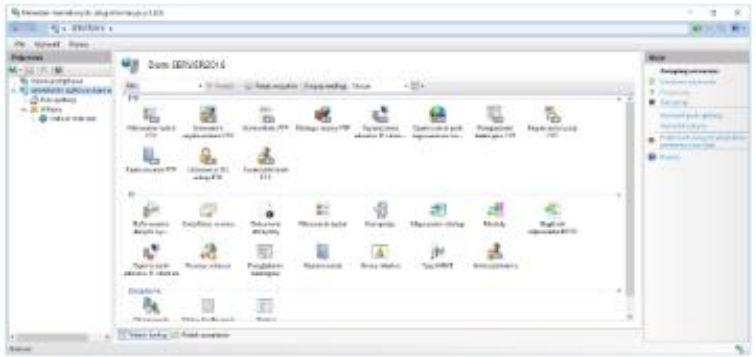
Rysunek 3.94. Instalacja IIS, doinstalowywanie roli serwera FTP

5. Na karcie *Potwierdzanie opcji instalacji* sprawdzamy, co będzie instalowane, i klikamy *Zainstaluj*.
6. Czekamy na zakończenie instalacji.

UWAGA

Jeśli rola serwera IIS była już zainstalowana, wykonujemy następujące operacje, aby zainstalować *Serwer FTP*, który nie jest standardowo instalowany. Na karcie *Wybieranie usług ról* rozwijamy *Serwer sieci Web (IIS)*, zaznaczamy *Serwer FTP* i klikamy *Dalej*. Następnie na karcie *Wybieranie funkcji* klikamy *Dalej*, by przejść do ostatniej karty, *Potwierdzanie opcji instalacji*, na której klikamy przycisk *Zainstaluj*. W ten sposób *Serwer FTP* zostanie doinstalowany.

7. Po zainstalowaniu usług ISS, aby je uruchomić, klikamy w Menedżerze serwera *Narzędzia* i wybieramy *Menedżer internetowych usług informacyjnych IIS*, co uruchomi przystawkę do zarządzania IIS (rysunek 3.95).

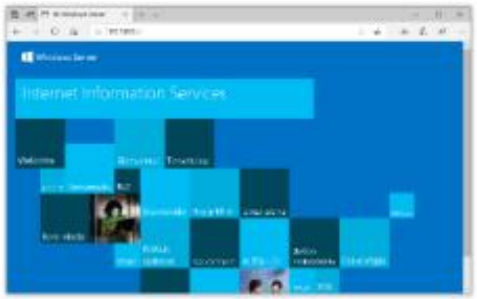


Rysunek 3.95. Menedżer internetowych usług informacyjnych IIS

Teraz możemy już zobaczyć pierwszą stronę internetową umieszczoną na naszym serwerze. Wystarczy wpisać w pasku adresu przeglądarki następujące adresy:

- na serwerze — `http://localhost/` lub adres IP serwera (w naszym przypadku `192.168.0.1`),
- na komputerze klienta — adres IP serwera (w naszym przypadku `192.168.0.1`).

W przeglądarce zostanie uruchomiona strona WWW usługi IIS (rysunek 3.96).



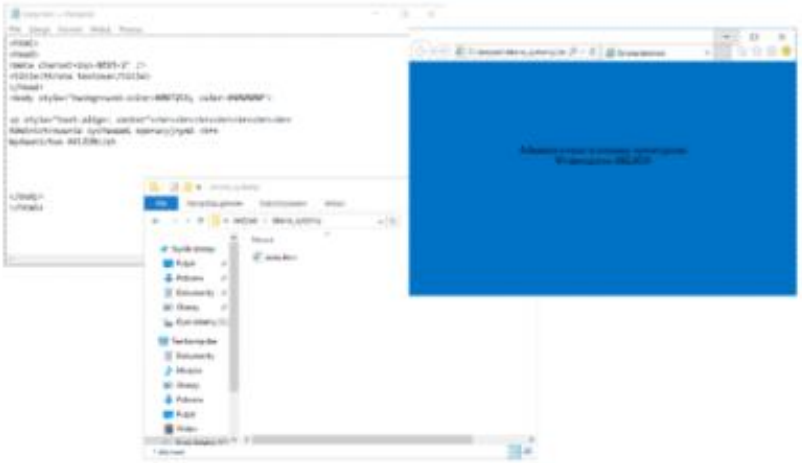
Rysunek 3.96. Lokalna strona internetowa usługi IIS uruchomiona na komputerze klienta

Jest to domyślna strona internetowa opisana w Menedżerze internetowych usług informacyjnych jako *Default Web Site*. Strona jest zlokalizowana w domyślnym folderze stron WWW: *%SystemDrive%\inetpub\wwwroot*, czyli w naszym przypadku *C:\inetpub\wwwroot*.

Ćwiczenie 3.27

Teraz spróbujemy utworzyć nową stronę WWW, która będzie dostępna z naszego serwera.

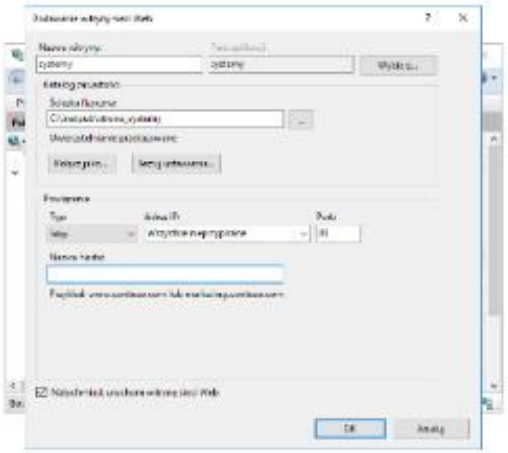
1. Zacznijmy od utworzenia folderu, w którym będzie przechowywana nasza strona, czyli *C:\inetpub\strona_systemy*.
2. Teraz utworzymy plik o nazwie *index.html*, w którym zawrzemy nazwę i treść strony, jak na rysunku 3.97.



Rysunek 3.97. Przygotowywanie przykładowej strony internetowej

3. Kiedy już mamy utworzone pliki strony WWW, opublikujemy ją na naszym serwerze. Uruchamiamy Menedżer internetowych usług informacyjnych, rozwijamy nazwę naszego serwera, a następnie klikamy *Witryny*.
4. Klikamy prawym przyciskiem myszy *Witryny* i wybieramy *Dodaj witrynę sieci Web*.
5. Uzupełniamy dane jak na rysunku 3.98:
   - *Nazwa witryny* — nazwa, pod jaką będzie widoczna witryna w Menedżerze internetowych usług informacyjnych;
   - *Ścieżka fizyczna* — lokalizacja folderu, w którym przechowywane są pliki strony;
   - *Powiązanie* — tu wskazujemy nazwę domeny, pod którą strona będzie dostępna, oraz port, za pomocą którego witryna będzie wywoływana.
6. Potwierdzamy przyciskiem *OK*. Podczas przypisywania portu 80 otrzymamy komunikat, że już jest przypisany do domyślnej witryny i może być używany tylko z jedną z nich. Potwierdzamy *Tak*, a wtedy konfiguracja zostanie zakończona.

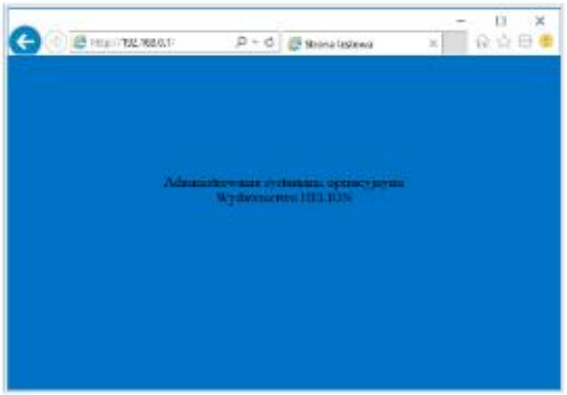
Rysunek 3.98. Dodawanie witryny sieci Web



7. Teraz aby sprawdzić działanie naszej witryny, klikamy w Menedżerze internetowych usług informacyjnych (IIS) domyślną witrynę (*Default Web Site*) prawym przyciskiem myszy, wybieramy *Zarządzanie witryną sieci Web* i klikamy *Zatrzymaj*.
8. Klikamy w Menedżerze internetowych usług informacyjnych utworzoną witrynę o nazwie *systemy* prawym przyciskiem myszy, wybieramy *Zarządzanie witryną sieci Web* i klikamy *Uruchom*.
9. Logujemy się na komputer klienta i wpisujemy w przeglądarce adres serwera (`http://192.168.0.1`). Powinniśmy uzyskać widok utworzonej witryny, jak na rysunku 3.99.

Warto pamiętać, że gdybyśmy przy dodawaniu witryny WWW podali inny port niż 80 (np. 70), nie musielibyśmy wyłączać domyślnej witryny, a jej wywołanie wyglądałoby tak: *http://localhost:70* lub *http://192.168.0.1:70*.

Rysunek 3.99. Strona uruchomiona w przeglądarce na komputerze klienta

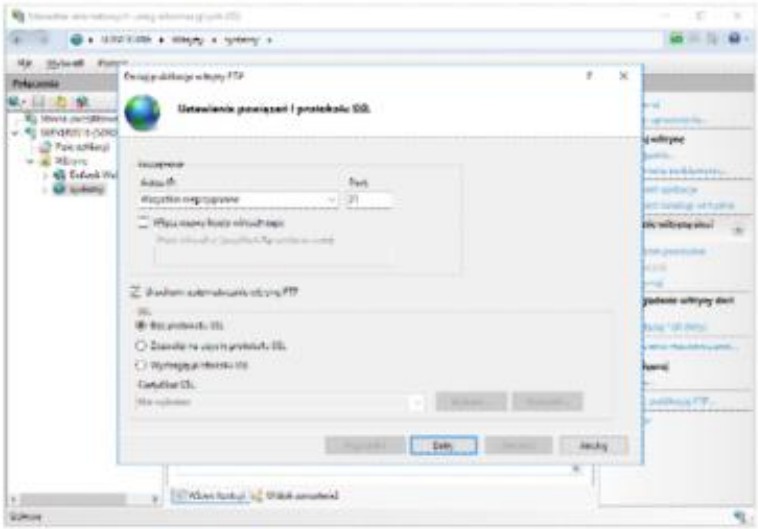


Zainstalowaliśmy internetowe usługi informacyjne (IIS) i uruchomiliśmy własną stronę internetową.

Ćwiczenie 3.28

Teraz skonfigurujemy serwer FTP i opublikujemy stronę, którą utworzyliśmy.

1. W Menedżerze internetowych usług informacyjnych klikamy prawym przyciskiem myszy naszą witrynę (*systemy*), wybieramy *Dodaj publikację FTP*, zaznaczamy opcje jak na rysunku 3.100 i klikamy *Dalej*.
   - *Adres IP* — określa adres IP, który ma być powiązany z serwerem FTP (*Wszystkie nieprzypisane*);
   - *Port* — określa numer portu, na którym będzie działać usługa; domyślnie FTP działa na porcie 21;
   - *Włącz nazwy hosta wirtualnego* — tu podajemy domenę publiczną, pod którą będzie dostępny serwer;
   - *Uruchom automatycznie witrynę FTP* — po zakończeniu pracy kreatora witryna zostanie automatycznie uruchomiona;
   - *SSL* — pozwala wybrać certyfikat SSL (jeśli jest dostępny) do zabezpieczania połączeń.



Rysunek 3.100. Kreator publikacji witryny FTP

2. Następna karta kreatora zawiera ustawienia uwierzytelniania i publikacji, które uzupełniamy jak na rysunku 3.101. Na koniec klikamy *Zakończ*. Dostępne są dwie grupy

ustawień: *Uwierzytelnianie* i *Autoryzacja*. Grupa *Uwierzytelnianie* obejmuje następujące opcje:

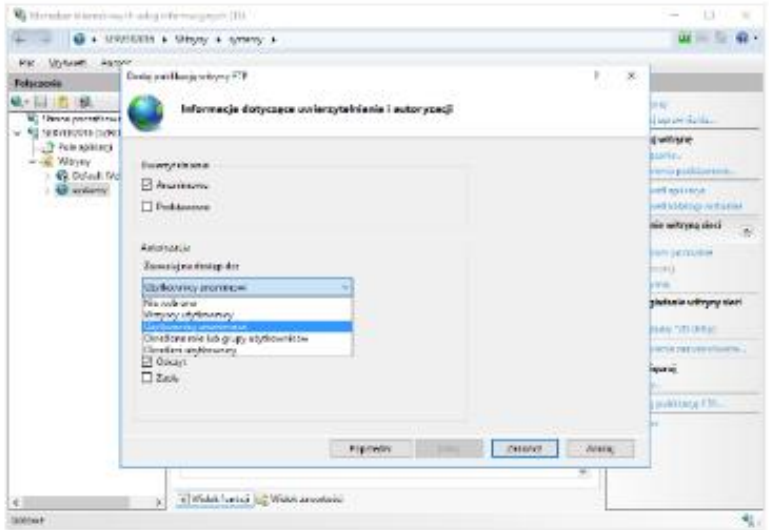
- *Anonimowe* — wbudowana metoda uwierzytelniania, która pozwala każdemu użytkownikowi uzyskać dostęp do udostępnionego zasobu FTP przez podanie anonimowej nazwy użytkownika i hasła;
- *Podstawowe* — wbudowana metoda uwierzytelniania, która wymaga podania nazwy użytkownika i hasła.

W grupie ustawień *Autoryzacja* są zaś dostępne następujące ustawienia:

- *Nie wybrano* — żaden użytkownik nie ma dostępu do udziału FTP;
- *Wszyscy użytkownicy* — wszyscy użytkownicy, zarówno lokalni, jak i domenowi, mają dostęp do udziału FTP;
- *Użytkownicy anonimowi* — tylko użytkownicy anonimowi mają dostęp do udziału FTP;
- *Określone role lub grupy użytkowników* — dostęp do udziału FTP mają użytkownicy z dostępem do ról lub należący do grup;
- *Określeni użytkownicy* — dostęp do udziału FTP mają konkretni użytkownicy;

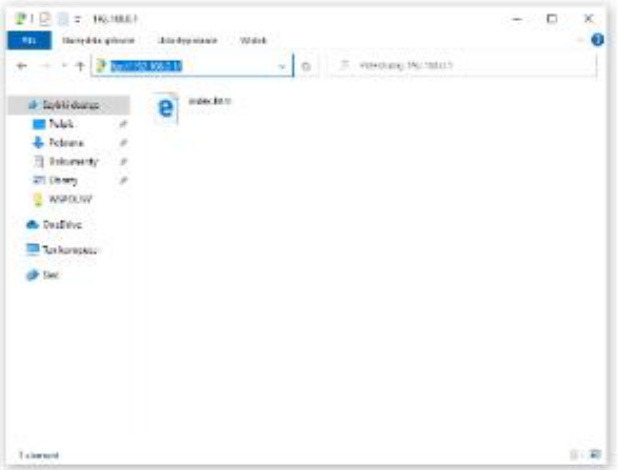
…i uprawnienia:

- *Odczyt* — użytkownicy mogą tylko odczytywać zawartość udziału FTP;
- *Zapis* — użytkownicy mogą zapisywać dane w udziale FTP.



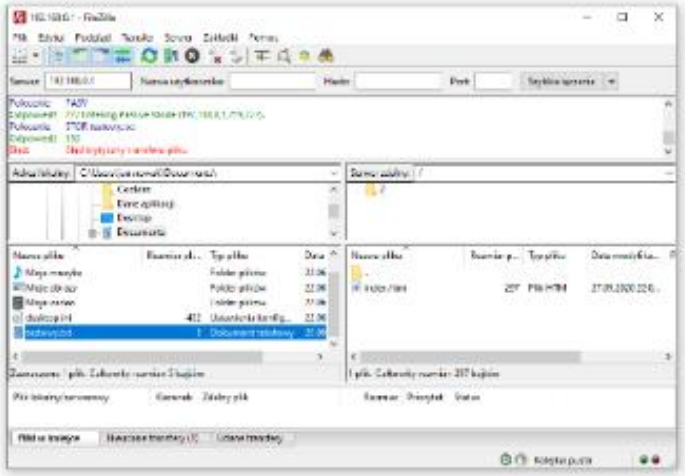
Rysunek 3.101. Informacje dotyczące uwierzytelniania i autoryzacji

3. Testujemy dostęp do FTP na komputerze klienta. W tym celu wpisujemy w Eksploratorze plików `ftp://192.168.0.1`. Bez żadnych poświadczeń mamy dostęp jak na rysunku 3.102.



Rysunek 3.102. Testowanie dostępu do FTP z komputera klienta

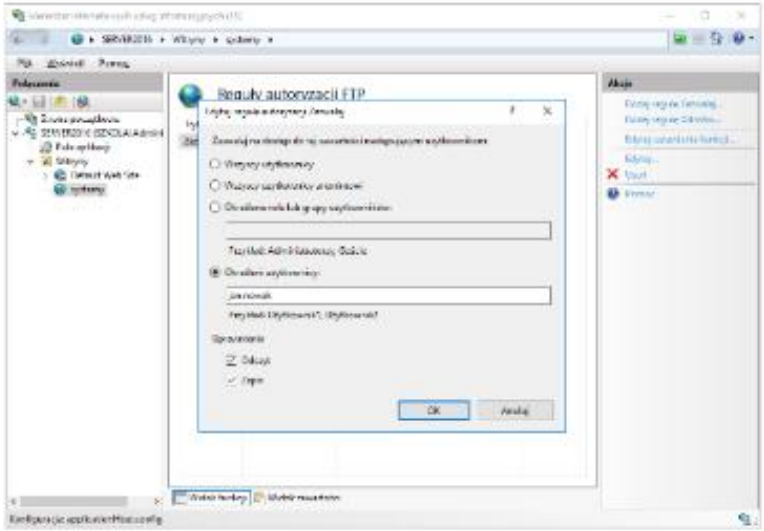
4. Teraz pobieramy i instalujemy program FileZilla, a następnie ustanawiamy połączenie i próbujemy przesłać plik z użyciem protokołu FTP. Operacja się nie powiedzie, gdyż nie mamy do tego uprawnień (rysunek 3.103).



Rysunek 3.103. Próba wysłania pliku poprzez FTP

Następnym krokiem będzie zmiana uprawnień i ustawienie możliwości zapisu dla użytkownika *Jan JN. Nowak*.

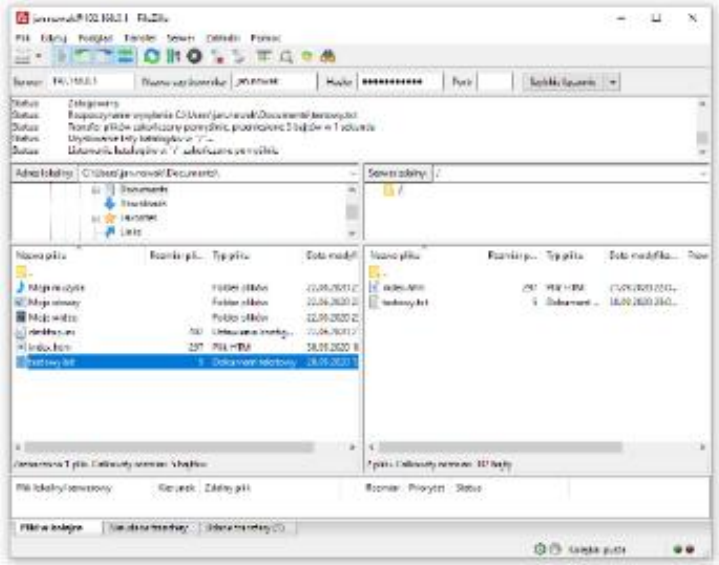
5. W Menedżerze internetowych usług informacyjnych klikamy prawym przyciskiem myszy witrynę, którą chcemy edytować (*systemy*), i wybieramy *Edytuj uprawnienia*. Teraz klikamy zakładkę *Zabezpieczenia* i wybieramy *Edytuj*. Klikamy *Dodaj* i dodajemy użytkownika, któremu nadamy uprawnienia zapisu (*jan.nowak*), gdyż cała grupa *Użytkownicy* nie ma takich uprawnień. Zatwierdzamy przyciskiem *OK* i przechodzimy do środkowego okna, w którym uruchamiamy *Reguły autoryzacji FTP*.
6. Wybieramy *Dodaj regułę/Zezwalaj*, zaznaczamy *Określeni użytkownicy* i wpisujemy nazwę `jan.nowak`, a w uprawnieniach zaznaczamy dodatkowo *Odczyt* oraz *Zapis* i klikamy *OK* (rysunek 3.104).



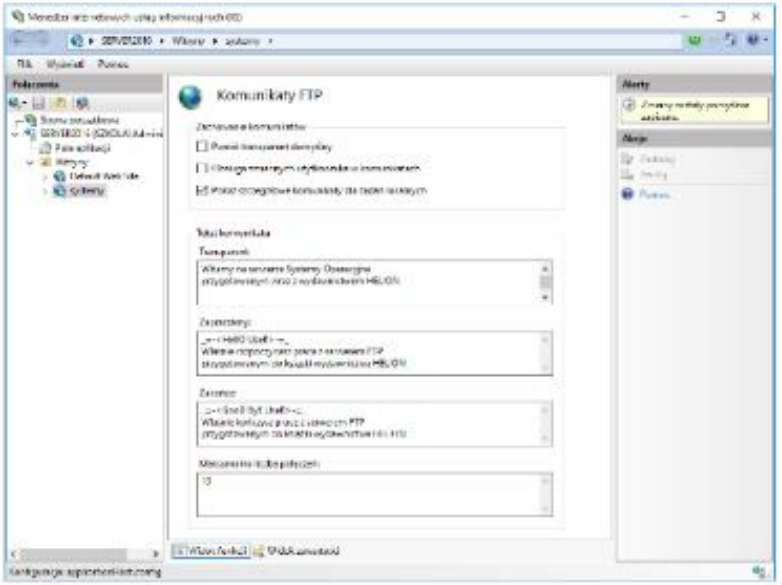
Rysunek 3.104. Edycja reguły autoryzacji

7. Wybieramy *Uwierzytelnianie FTP* i włączamy *Uwierzytelnianie podstawowe*.
8. Teraz nasza reguła pozwala na odczyt wszystkim anonimowym użytkownikom, a zapis jest możliwy tylko dla użytkownika *Jan JN. Nowak* (*jan.nowak*).
9. Sprawdzamy poprawność konfiguracji za pomocą programu FileZilla (rysunek 3.105).

W formie ciekawostki wspomnimy o komunikatach serwera FTP, które dodajemy przez wybranie *Komunikaty FTP* (rysunek 3.106).

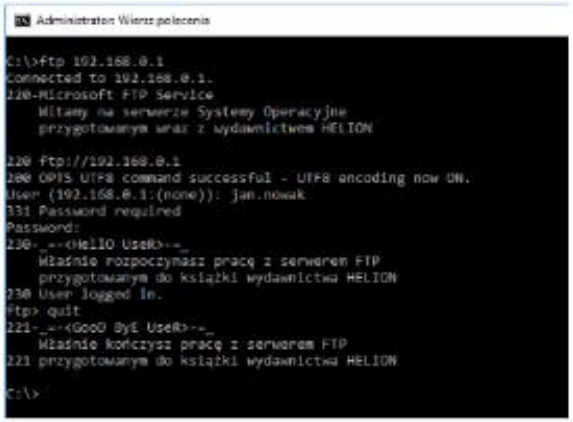


Rysunek 3.105. Transfer plików z użyciem klienta FTP FileZilla



Rysunek 3.106. Dodawanie komunikatów do serwera FTP

Nie wszystkie programy pokazują komunikaty, my zatem spróbujemy połączyć się z FTP za pomocą konsoli, która takie komunikaty pokazuje (rysunek 3.107).



Rysunek 3.107. Połączenie za pomocą konsoli z widocznymi komunikatami

Zadania kontrolne

1. Uruchom stronę internetową z własną zawartością, dostępną na porcie 345.
2. Do utworzonej strony WWW uruchom serwer FTP z dostępem anonimowym tylko do odczytu.
3. Nadaj uprawnienia do odczytu i zapisu dla użytkowników *Joanna Kowalska* i *Antonio Banderas*.
4. Odmów dostępu do FTP użytkownikowi *Maciej Nowak*.
5. Ustaw własne komunikaty na serwerze FTP.
6. Sprawdź uprawnienia nadane poszczególnym użytkownikom.

3.15. Zasady grupy

Windows Server 2016/2019 jest bardzo rozbudowanym systemem, który może obsługiwać ogromną liczbę komputerów i użytkowników. Dla administratora konfigurowanie każdego komputera i użytkownika z osobna byłoby kłopotliwe, dlatego z pomocą przychodzi mechanizm *Zasady grupy*, który zapewnia możliwość konfiguracji grupowej. W tym systemie można znaleźć ponad dwa tysiące różnego rodzaju ustawień i konfiguracji.

DEFINICJA

Zasady grupy (ang. *group policy*) to reguły i ustawienia, które określają role, a także możliwości użytkowników oraz komputerów lokalnych i pracujących w sieci komputerowej.

Serwer ma zaimplementowane na stałe standardowe zasady, które są zależne od roli, jaką ma komputer bądź użytkownik. Zasady grupy możemy podzielić ze względu na przeznaczenie:

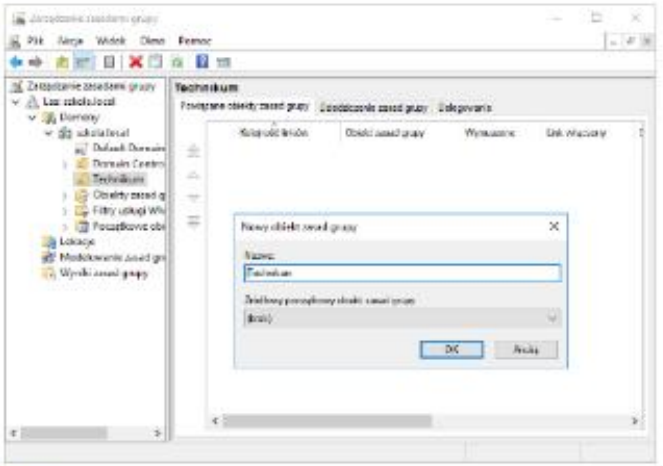
- **zasady lokalne** — mają zastosowanie do komputerów lokalnych;
- **zasady kontrolera domeny** — mają zastosowanie tylko do kontrolera domeny;
- **zasady domenowe** — mają zastosowanie do komputerów w domenie oprócz kontrolera domeny.

Wszystkie zasady dotyczące komputerów są ładowane w trakcie uruchamiania systemu, ale przed zalogowaniem użytkownika, a zasady dotyczące użytkowników są ładowane podczas logowania użytkownika.

Szkolny administrator poprzez zasady grupy będzie w stanie skonfigurować użytkownikom domeny wiele opcji, takich jak brak dostępu do konkretnych dysków i brak możliwości uruchomienia konsoli (*cmd.exe*), czy też ustawić dla wszystkich jednakową tapetę. W poniższym ćwiczeniu pokażemy, jak się tworzy i modyfikuje zasady grupy.

Ćwiczenie 3.29

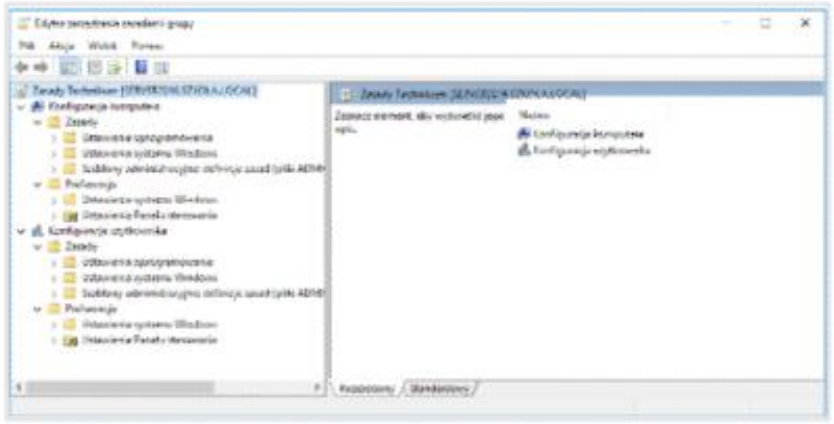
1. Uruchamiamy Menedżer serwera i w menu *Narzędzia* wybieramy *Zarządzanie zasadami grupy*.
2. Po lewej stronie okna rozwijamy po kolei *Las: szkola.local*, *Domeny*, *szkola.local*, wskazujemy prawym przyciskiem myszy *Technikum* i wybieramy *Utwórz obiekt zasad w tej domenie i umieść tu link...* (rysunek 3.108).



Rysunek 3.108. Tworzenie nowego obiektu zasad grupy

3. Wprowadzamy nazwę `Technikum` i klikamy *OK*.

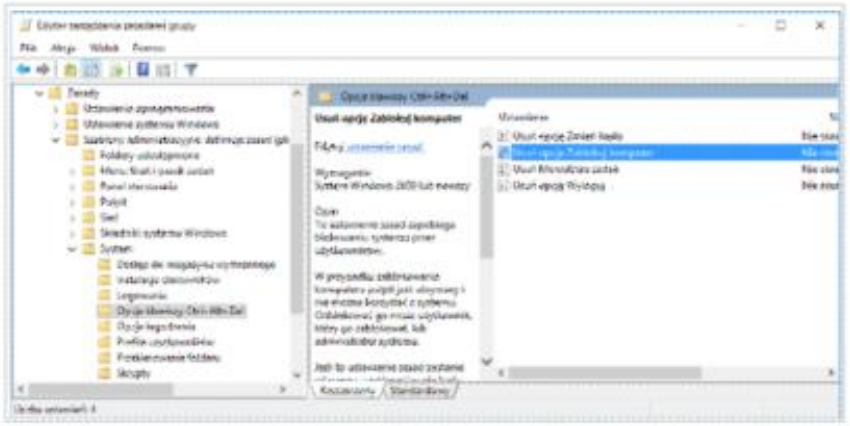
4. Klikamy utworzony obiekt prawym przyciskiem myszy i wybieramy *Edytuj*. Otworzy się *Edytor zarządzania zasadami grupy*, który zawiera konfiguracje zasad oddzielnie dla komputera i użytkownika (rysunek 3.109).



Rysunek 3.109. Edytor zarządzania zasadami grupy

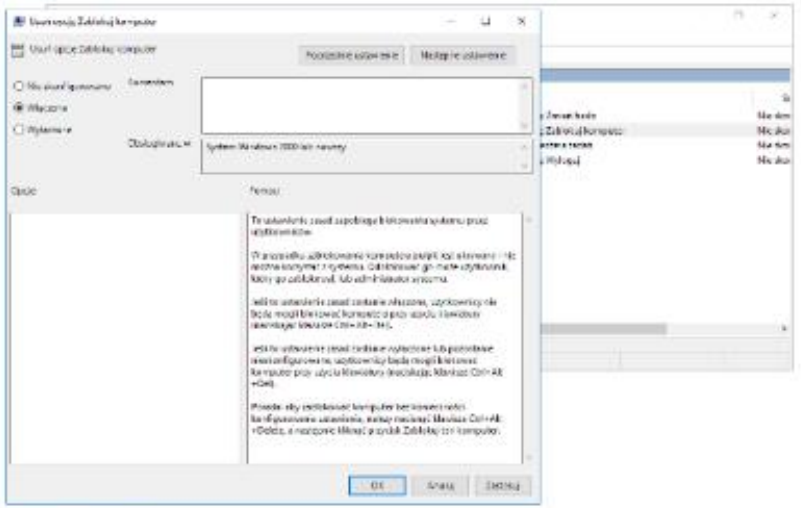
5. Teraz usuniemy użytkownikowi możliwość blokowania komputera po wybraniu kombinacji klawiszy *Ctrl+Alt+Del*.

6. Wybieramy w narzędziu *Edytor zarządzania zasadami grupy* następujące ustawienia: *Konfiguracja użytkownika/Zasady/Szablony administracyjne: definicje zasad (pliki ADMX) pobrane z komputera lokalnego/System/Opcje klawiszy Ctrl+Alt+Del* (rysunek 3.110). Teraz klikamy *Usuń opcję Zablokuj komputer*.



Rysunek 3.110. Dodawanie zasady w narzędziu Edytor zarządzania zasadami grupy

7. Zaznaczamy opcję *Włączone* i zatwierdzamy *OK*. Jak widać na rysunku 3.111, działanie każdej reguły jest dokładnie wytłumaczone, co ułatwia pracę administratorowi.



Rysunek 3.111. Włączanie zasady Usuń opcję Zablokuj komputer

8. Teraz sprawdzamy konfigurację przez zalogowanie się na konto użytkownika należące do jednostki organizacyjnej *Technikum*. My wybraliśmy konto *Maciej Nowak*. Po zalogowaniu naciskamy *Ctrl+Alt+Del*. Ukaże nam się widok jak na rysunku 3.112. Widzimy, że zasada działa i polecenie *Zablokuj komputer* zostało usunięte.



Rysunek 3.112. Sprawdzenie działania zasady grupy

Zadania kontrolne

1. W jednostce organizacyjnej *Technikum* wyłącz możliwość dostępu użytkownika do Panelu sterowania oraz ekranu *Ustawienia komputera*.
2. Wyłącz aplikację Sklep.
3. Usuń ikonę Kosza z Pulpitu.
4. Zaloguj się na konto z jednostki organizacyjnej *Technikum* i sprawdź działanie zasad.

3.16. Kopie zapasowe

Administrator to nie tylko osoba, która instaluje i konfiguruje urządzenia i komputery, ale także ktoś, kto dba o ich bezpieczeństwo i niezawodność. Jedną z funkcji, które zapewnią nam wyższy poziom bezpieczeństwa i niezawodności, jest kopia zapasowa serwera. Szkolny administrator dba również o serwer i wykonuje jego kopie bezpieczeństwa, aby w razie awarii użytkownicy nie utracili dostępu do swoich danych. Dzięki zaprezentowanej poniżej usłudze jego praca stanie się łatwiejsza, a codzienne czynności będą wykonywane automatycznie.

DEFINICJA

Kopia zapasowa to zdublikowana instancja pliku danych, aplikacji, systemu lub serwera utworzona za pomocą oprogramowania do tworzenia kopii zapasowych. Służy do przywracania oryginalnych danych w razie ich usunięcia, uszkodzenia lub utraty. Kopia zapasowa danych powinna być przechowywana w zewnętrznym magazynie lub na zewnętrznym nośniku.

W Windows Server 2016/2019 jest dostępne narzędzie o nazwie *Kopia zapasowa systemu Windows Server*, które umożliwia wykonywanie i przywracanie kopii zapasowych systemu operacyjnego, aplikacji i danych. Pozwala zaplanować wykonywanie kopii zapasowych, a także chronić cały serwer lub konkretne woluminy. Więcej o instalacji tego narzędzia oraz tworzeniu kopii dowiesz się podczas wykonywania poniższego ćwiczenia.

Ćwiczenie 3.30

Spróbujmy teraz zainstalować oprogramowanie Kopia zapasowa systemu Windows Server.

1. Uruchamiamy Menedżer serwera, wybieramy *Dodaj role i funkcje*, a następnie *Instalacja oparta na rolach lub oparta na funkcjach* i klikamy *Dalej*.
2. Wskazujemy nasz serwer i klikamy *Dalej*.
3. Na karcie *Wybieranie ról serwera* od razu klikamy *Dalej*.
4. Na karcie *Wybieranie funkcji* zaznaczamy *Kopia zapasowa systemu Windows Server* i klikamy *Dalej*.
5. Na karcie *Potwierdzanie opcji instalacji* klikamy *Zainstaluj* i po zakończeniu instalacji naciskamy *Zakończ*.

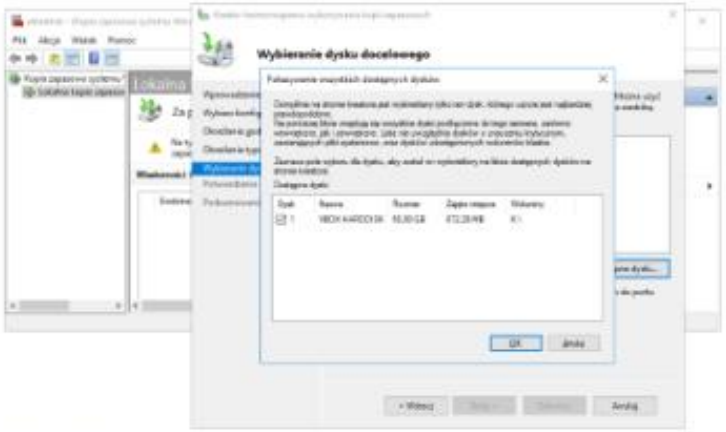
Instalacja funkcji *Kopia zapasowa systemu Windows Server* została zakończona. Teraz pokażemy, jak wykonać kopię zapasową serwera. Jak już zapewne wiesz, kopia zapasowa powinna być wykonywana na zewnętrznym nośniku danych, dlatego dołączymy do naszego serwera kolejny dysk twardy i to na nim wykonamy kopię.

Ćwiczenie 3.31

1. Dysk twardy został domontowany do serwera i zainicjowany oraz została utworzona partycja w systemie plików NTFS. Do partycji została przypisana litera *K* i nazwa *BACKUP*.
2. Uruchamiamy Menedżer serwera i z menu *Narzędzia* wybieramy *Kopia zapasowa systemu Windows Server*.
3. Po uruchomieniu dostajemy informację, że żadna kopia nie jest skonfigurowana, dlatego musimy uruchomić kreatora konfiguracji. Aby to zrobić, klikamy w lewym panelu *Lokalna kopia zapasowa*, a następnie w prawym panelu naciskamy przycisk *Harmonogram wykonywania kopii zapasowych*.
4. Na pierwszej stronie kreatora (*Wprowadzenie*) czytamy informacje i klikamy *Dalej*.
5. Na stronie *Wybierz konfigurację kopii zapasowej* mamy do dyspozycji dwie opcje:
   - *Cały serwer* — zostanie wykonana kopia wszystkich danych serwera, aplikacji oraz stanu systemu. To jest duża kopia i wymaga dużej ilości miejsca na nośniku przeznaczonym na kopie zapasowe.
   - *Niestandardowa* — zostanie wykonana kopia tylko tych danych, które wskażemy. Rozmiar kopii jest dopasowany do ilości archiwizowanych danych.
6. My wykonamy kopię zapasową całego serwera, zatem wybieramy opcję *Cały serwer* i klikamy *Dalej*.
7. Teraz na karcie *Określanie godziny wykonania kopii zapasowej* wskazujemy codzienną godzinę wykonania kopii lub wybieramy częstszą kopię kilka razy dziennie. Warto zapamiętać, że wykonywanie kopii powinno się odbywać w czasie najmniejszego obciążenia serwera, np. w nocy. My wybieramy *Raz dziennie* i ustawiamy czas wykonania kopii na godzinę 1:00. Na koniec klikamy *Dalej*.
8. Na karcie *Określanie typu miejsca docelowego* mamy do wyboru jedną z trzech opcji:
   - *Utwórz kopię zapasową na dysku twardym dla kopii* — zostanie utworzona kopia na nośniku, który będzie niezależnym elementem serwera, np. na wewnętrznym dysku twardym lub dysku podłączanym do USB.
   - *Utwórz kopię zapasową w woluminie* — zostanie utworzona kopia w folderze przeznaczonym do przechowywania kopii.
   - *Utwórz kopię zapasową w udostępnionym folderze sieciowym* — zostanie utworzona kopia w folderze sieciowym, np. w pamięci NAS, która może być dostępna w sieci.

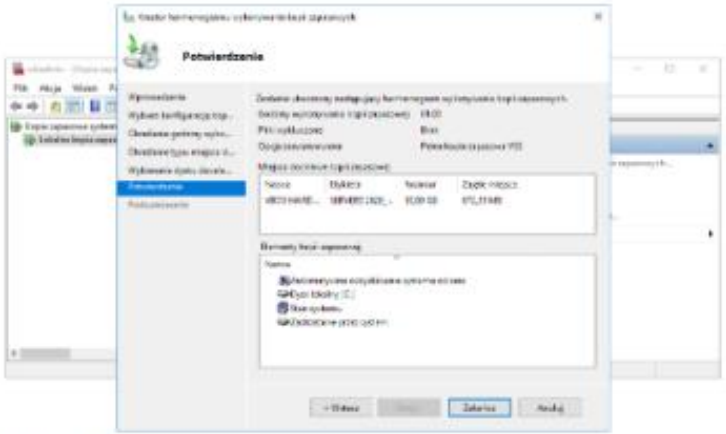
   My wybieramy opcję zalecaną, czyli *Utwórz kopię zapasową na dysku twardym dla kopii*, i klikamy *Dalej*.

9. Na karcie *Wybieranie dysku docelowego* klikamy *Pokaż wszystkie dostępne dyski*, zaznaczamy dostępny dysk i klikamy *OK* (rysunek 3.113).



Rysunek 3.113. Wybór dysku do wykonania kopii zapasowej

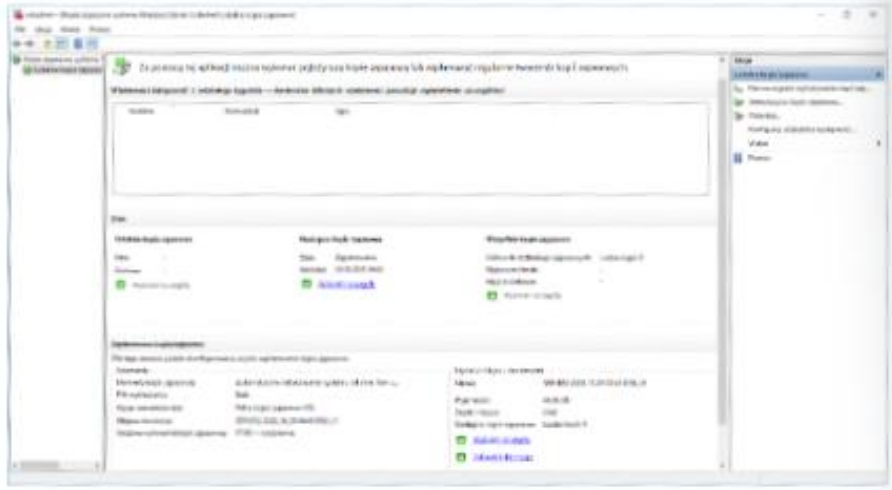
10. Teraz ponownie zaznaczamy dysk i klikamy *Dalej*.
11. System informuje nas, że dysk przeznaczony do przechowywania kopii zapasowych znajduje się w naszym systemie i wybraliśmy pełną kopię serwera. Po naciśnięciu *OK* dysk ten nie będzie brany pod uwagę przy wykonywaniu kopii. Klikamy *OK*.
12. Teraz system informuje nas o konieczności wykonania formatowania dysku oraz o tym, że nośnik nie będzie widoczny w Eksploratorze plików. Potwierdzamy przyciskiem *TAK*.
13. Na zakończenie otrzymujemy *Potwierdzenie kreatora* i klikamy *Zakończ* (rysunek 3.114).



Rysunek 3.114. Podsumowanie harmonogramu kopii zapasowej serwera

14. Następnym etapem jest wykonanie konfiguracji. Na koniec klikamy *Zamknij*.

Rysunek 3.115 przedstawia ekran, który pokazuje informacje o zaplanowanej kopii zapasowej, łącznie z czasem wykonania najbliższej.



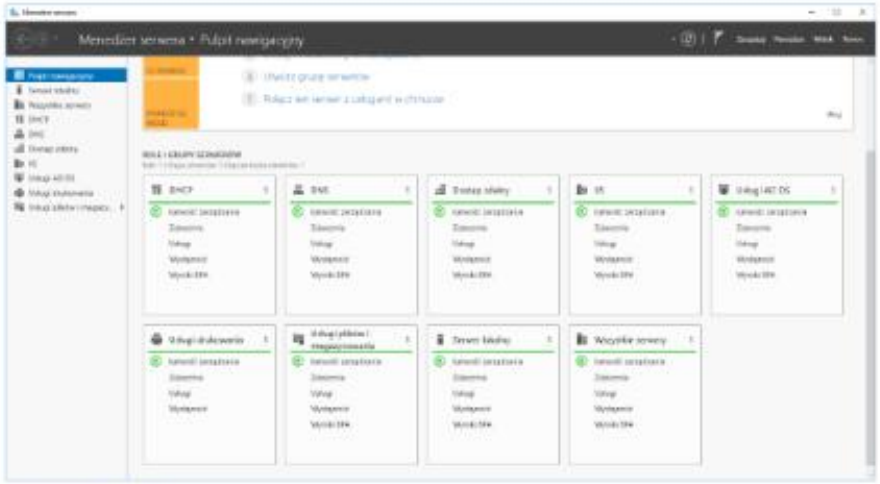
Rysunek 3.115. Widok zaplanowanej kopii zapasowej serwera

Zadania kontrolne

1. Wykonaj kopię zapasową tylko folderów *C:\Skrypty* oraz *C:\Profile* w folderze o nazwie *BACKUP* utworzonym na dysku *C*.
2. Kopia zapasowa tych folderów ma być wykonywana co dwie godziny.

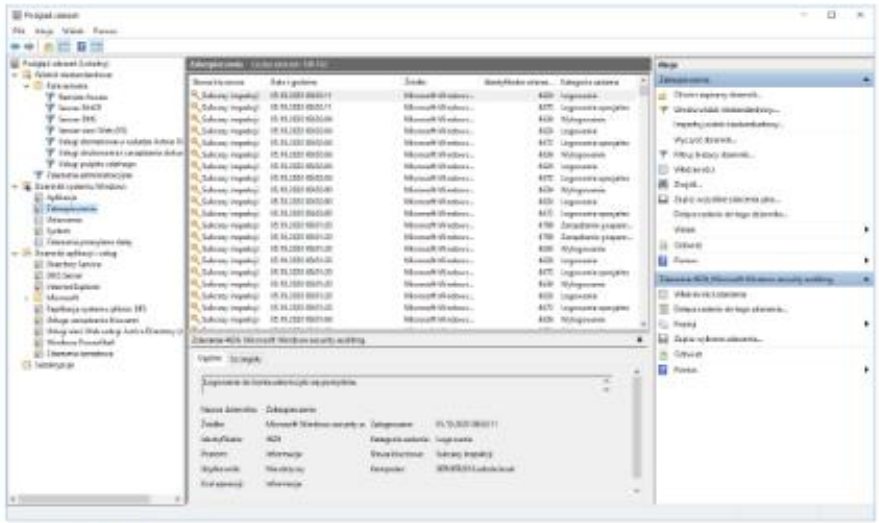
3.17. Monitorowanie pracy i wydajności serwera

Monitorowanie pracy serwera jest bardzo ważne w pracy administratora. Serwer zapisuje szereg informacji na temat swojego stanu w logach systemu, które możemy odczytać za pomocą narzędzia Podgląd zdarzeń. Pierwszym elementem, który podaje informacje na temat stanu serwera oraz uruchomionych na nim ról i funkcji, jest Menedżer serwera. Na pulpicie nawigacyjnym pokazanym na rysunku 3.116 są wyświetlone wszystkie uruchomione usługi. Jeśli system stwierdzi coś niepokojącego w działaniu danej usługi, jej nazwa zaświeci się na czerwono, przy czym poszczególnym stanom odpowiadają różne cyfry.



Rysunek 3.116. Podgląd pulpitu nawigacyjnego Menedżera serwera

Innym narzędziem, które pozwala monitorować pracę serwera, jest Podgląd zdarzeń dostępny w menu *Narzędzia/Podgląd zdarzeń*, pokazany na rysunku 3.117.



Rysunek 3.117. Podgląd zdarzeń

Podgląd zdarzeń przedstawia już szczegółowe dane z podziałem na poszczególne elementy, takie jak:

- *Role serwera* — lista ról serwera, a w nich dokładne informacje dotyczące działania poszczególnych usług.
- *Dzienniki systemu Windows* — pozwalają podejrzeć wszystkie zdarzenia z podziałem na:
  - *Aplikacja* — zdarzenia zarejestrowane przez aplikacje i programy,
  - *Zabezpieczenia* — informacje takie jak poprawne i niepoprawne próby logowania oraz użycie zasobów,
  - *Ustawienia* — zdarzenia dotyczące zmian ustawień w Windows Server,
  - *System* — zdarzenia zebrane przez wszystkie składniki systemu Windows Server, takie jak niepoprawne działanie sterownika urządzenia czy też innych usług systemu,
  - *Zdarzenia przesyłane dalej* — zdarzenia zebrane z komputerów zdalnych.
- *Dzienniki aplikacji i usług* — wyszczególnione aplikacje i usługi, w których przypadku możliwy jest podgląd zdarzeń.

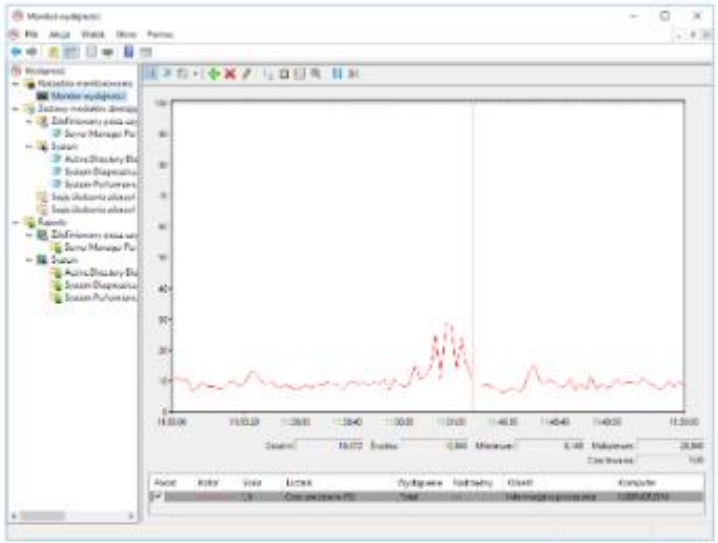
W podglądzie zdarzeń występuje kilka typów zdarzeń:

- *Informacje* — informują o powodzeniu zdarzenia;
- *Ostrzeżenia* — informują o możliwych błędach lub niepoprawnej konfiguracji;
- *Błędy* — informują o poważnych błędach, np. o tym, że usługa się nie uruchomiła;
- *Sukcesy inspekcji* — informują o powodzeniu przeprowadzonej inspekcji, np. poprawnym logowaniu;
- *Inspekcja niepowodzeń* — informują o niepowodzeniu przeprowadzenia inspekcji, np. niepoprawnym logowaniu.

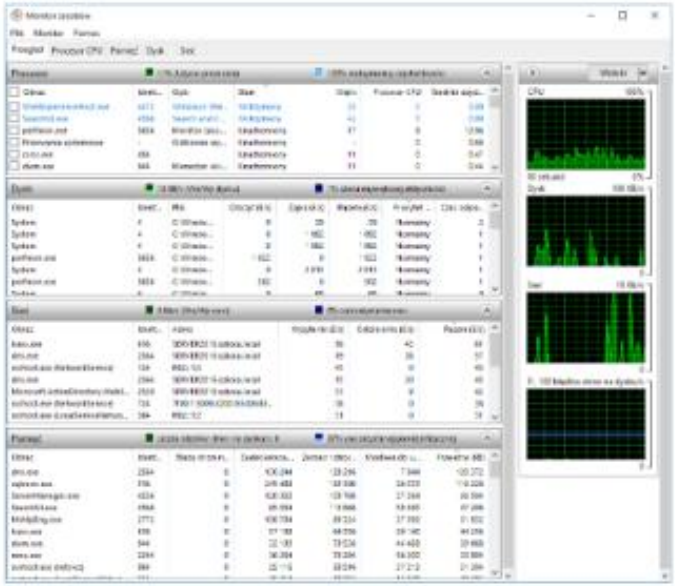
Poszczególne typy zdarzeń po otwarciu informują nas o typie zdarzenia, dacie wystąpienia zdarzenia oraz o tym, kto je wywołał; otrzymujemy także opis całego zdarzenia. Te wszystkie dane są bardzo przydatne w diagnostyce i monitorowaniu pracy serwera.

Dodatkowo w Menedżerze serwera w menu *Narzędzia* można wybrać jeszcze dwa narzędzia przydatne do monitorowania pracy i wydajności serwera. Są to:

- *Monitor wydajności* — narzędzie przeznaczone do sprawdzania wydajności serwera oraz tworzenia raportów wydajności (rysunek 3.118),
- *Monitor zasobów* — narzędzie przeznaczone do sprawdzania wykorzystania zasobów serwera z podziałem na *Procesor*, *Dysk*, *Sieć* i *Pamięć* (rysunek 3.119).



Rysunek 3.118. Monitor wydajności



Rysunek 3.119. Monitor zasobów

Zadania kontrolne

1. Wyszukaj w dziennikach zdarzeń informacje na temat logowania do serwera.
2. Wyszukaj w dziennikach zdarzeń informacje na temat uruchomionych ról serwera.

3.18. Zdalne zarządzanie serwerem

Serwerem można zarządzać w dwojaki sposób — bezpośrednio przy komputerze (serwerze) oraz za pomocą komputera połączonego z siecią lokalną lub internetem. Obecnie bardzo popularną i wygodną metodą jest połączenie przy użyciu pulpitu zdalnego, dzięki czemu administrator może się znajdować w dowolnym miejscu na świecie.

Aby podłączyć się do systemu Windows Server 2016/2019, możemy użyć dowolnego klienta RDP uruchomionego na dowolnym systemie operacyjnym, np. Windows, Linux czy też telefonie komórkowym. Nasz szkolny administrator również będzie musiał się zmierzyć z zarządzaniem szkolną siecią bez dostępu do miejsca, gdzie zlokalizowany jest serwer, np. z domu lub z pracowni. Powszechność aplikacji dostępowych RDP zapewni dostęp do szkolnej sieci z dowolnego miejsca na świecie.

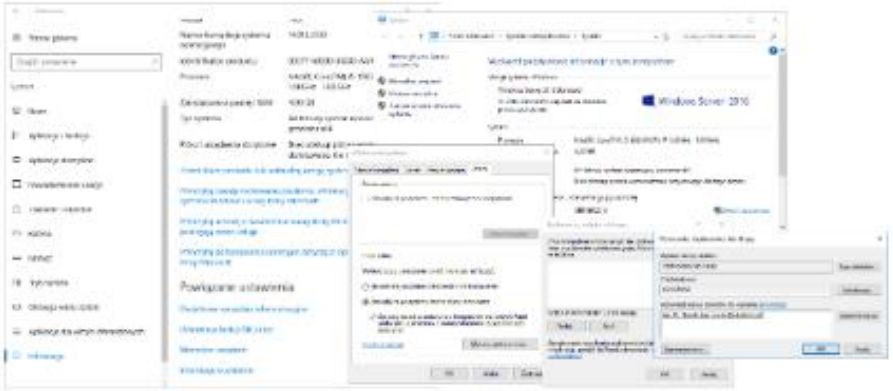
DEFINICJA

RDP (ang. *Remote Desktop Protocol*) to protokół opracowany przez firmę Microsoft, który zapewnia graficzny interfejs do łączenia się z innym komputerem za pośrednictwem połączenia sieciowego. W tym celu użytkownik korzysta z oprogramowania klienta RDP, podczas gdy na drugim komputerze musi być uruchomione oprogramowanie serwera RDP. W standardowej konfiguracji protokół ten działa na porcie TCP/UDP 3389.

Domyślnie w systemach serwerowych nieaktywna jest możliwość podłączania się przy użyciu protokołu RDP. W poniższym ćwiczeniu pokażemy, jak aktywować dostęp za pomocą RDP, i wykonamy przykładowe połączenie.

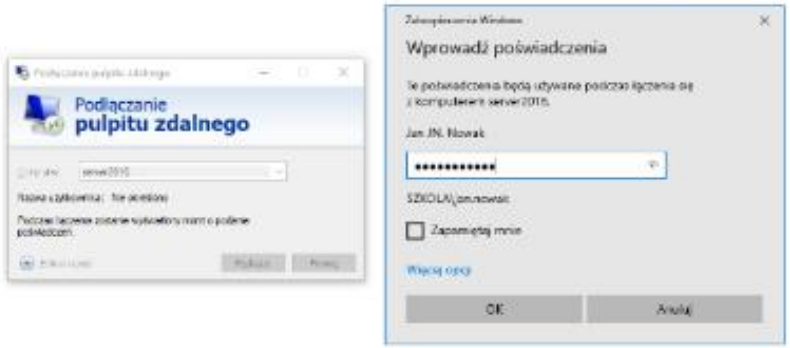
Ćwiczenie 3.32

1. Klikamy *Start/Ustawienia/System/Informacje*.
2. Następnie wybieramy *Informacje o systemie/Zaawansowane ustawienia systemu* i na karcie *Właściwości systemu* klikamy zakładkę *Zdalny*.
3. Zaznaczamy *Zezwalaj na połączenia zdalne z tym komputerem*, wybieramy *Wybierz użytkowników* i wpisujemy `Jan JN. Nowak`, by dodać użytkownika o tej nazwie, jak na rysunku 3.120, a następnie zatwierdzamy wybór.



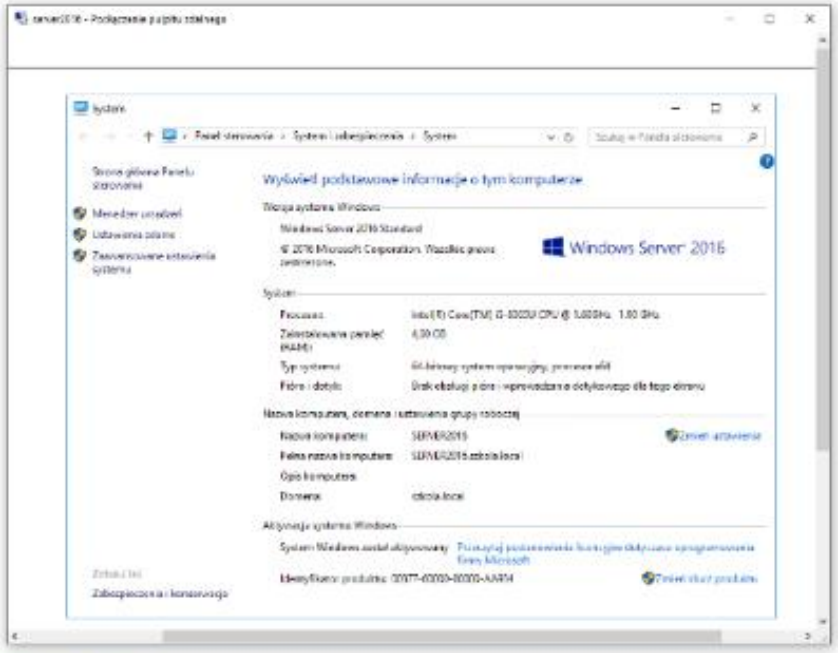
Rysunek 3.120. Włączanie dostępu zdalnego do serwera

4. Standardowo użytkownik *Administrator* ma już dostęp poprzez pulpit zdalny, zatem może się logować.
5. Aby użytkownik *Jan IN. Nowak* mógł się zalogować na serwerze, musi należeć do grupy *Administratorzy*, więc poprzez przystawkę konsoli MMC *Użytkownicy i komputery usługi Active Directory* dodajemy mu przynależność do tej grupy.
6. Przechodzimy do komputera klienta, na którym uruchamiamy program *Podłączenie pulpitu zdalnego*.
7. W miejscu *Komputer* wpisujemy nazwę serwera (`SERVER2016`) lub jego adres IP (lokalny albo publiczny) i klikamy *Podłącz*.
8. Otworzy się karta przeznaczona do wprowadzenia poświadczeń. Login będzie już wprowadzony, wystarczy zatem wpisać hasło i potwierdzić przyciskiem *OK* (rysunek 3.121).



Rysunek 3.121. Podłączenie pulpitu zdalnego z komputera klienta

9. Połączenie zostało ustanowione. Teraz możemy obsługiwać nasz serwer w taki sposób, jakbyśmy się znajdowali bezpośrednio przy nim (rysunek 3.122).

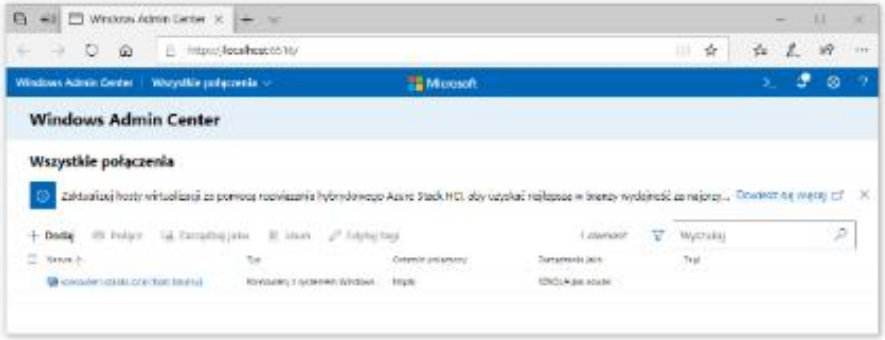


Rysunek 3.122. Okno podłączonego pulpitu zdalnego

10. W systemie Windows Server 2019 możemy wykorzystać nowe narzędzie Windows Admin Center do pracy zdalnej oraz monitorowania serwera. Pobieramy je ze strony *https://www.microsoft.com/pl-pl/windows-server/windows-admin-center* i instalujemy na komputerze, z którego będziemy się łączyć z serwerem. Proces instalacji i konfiguracji omówimy w poniższym ćwiczeniu.

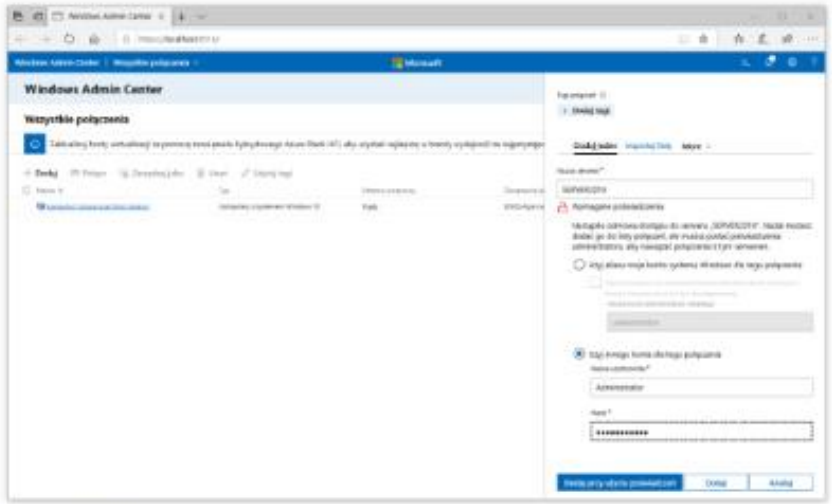
Ćwiczenie 3.33

1. Pobieramy program ze strony *https://www.microsoft.com/pl-pl/windows-server/windows-admin-center*.
2. Instalujemy program na komputerze klienta i uruchamiamy go kliknięciem ikony na pulpicie.
3. Uruchomi się przeglądarka, z której będziemy zarządzać serwerem (rysunek 3.123).



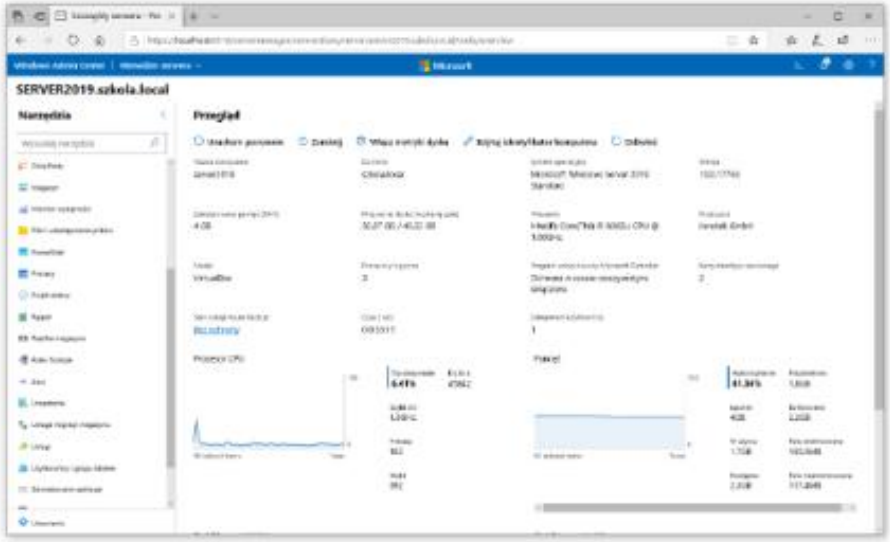
Rysunek 3.123. Konsola zarządzania Windows Admin Center

4. Klikamy *Dodaj*. Zostanie otwarte okno po prawej stronie, gdzie klikamy *Dodaj jeden*, wpisujemy nazwę naszego serwera, `SERVER2019`, i zaznaczamy opcję *Użyj innego konta do tego połączenia*, a następnie wpisujemy dane jak na rysunku 3.124 i klikamy *Dodaj przy użyciu poświadczeń*.



Rysunek 3.124. Dodawanie serwera do zarządzania

5. Następnie klikamy dodany serwer i już możemy nim zarządzać, a także go monitorować. Podgląd zarządzanego serwera jest pokazany na rysunku 3.125.



Rysunek 3.125. Konsola zarządzania serwerem

Podgląd zapewnia pełny zestaw informacji statystycznych serwera. Możemy go w tym miejscu uruchomić ponownie, a także podłączyć się do niego pulpitem zdalnym poprzez przeglądarkę. Narzędzie to nie obsługuje jednak kontrolerów domeny.

Zadania kontrolne

1. Co to jest protokół RDP i do czego możemy go używać?
2. Skonfiguruj połączenie pulpitu zdalnego z serwera na komputer klienta.