Część 4

Administrowanie sieciowymi systemami operacyjnymi

INF.02

KODY

Podręcznik do nauki zawodu

TECHNIK INFORMATYK

WSiP

Autorzy: **Sylwia Osetek**, **Krzysztof Pytel**

Typ szkoły: **technikum**
Zawód: **technik informatyk**
Kwalifikacja: **INF.02. Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych**

© Copyright by Wydawnictwa Szkolne i Pedagogiczne
Warszawa 2022

Wydanie I (2022)

ISBN 978-83-02-20922-2 (część 4.) (podręcznik w postaci elektronicznej – flipbook)
ISBN 978-83-02-20847-8 (całość) (podręcznik w postaci elektronicznej – flipbook)
ISBN 978-83-02-20372-5 (część 4.) (podręcznik w postaci papierowej)
ISBN 978-83-02-20373-2 (całość) (podręcznik w postaci papierowej)

Opracowanie merytoryczne i redakcyjne: **Tomasz Kompanowski**, **Sebastian Jabłoński**
Redakcja językowa: **wizjonerzytekstu.pl**, **Anna Rossa**
Redakcja techniczna: **Elżbieta Walczak**
Projekt okładki: **Dominik Krajewski**
Skład i łamanie: **Ledor**

Zdjęcie na okładce: ZinetroN/Shutterstock.com

Wydawnictwa Szkolne i Pedagogiczne Spółka Akcyjna
00-807 Warszawa, Aleje Jerozolimskie 96
KRS 0000595068
Infolinia: 801 220 555
www.wsip.pl
Druk i oprawa: Drukarnia Pozkal

QR Code (Kod QR) to zarejestrowany znak towarowy DENSO WAVE INCORPORATED
Odczytanie kodu QR wymaga urządzenia z zainstalowaną aplikacją do odczytywania kodów QR, obsługującą co najmniej kody w wersji czwartej, oraz aparatu o minimalnej rozdzielczości 5 Mpix.

Publikacja, którą nabyłaś / nabyłeś, jest dziełem twórcy i wydawcy. Prosimy, abyś przestrzegała / przestrzegał praw, jakie im przysługują. Jej zawartość możesz udostępnić nieodpłatnie osobom bliskim lub osobiście znanym. Ale nie publikuj jej w internecie. Jeśli cytujesz jej fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A kopiując jej część, rób to jedynie na użytek osobisty.

prawolubni

Szanujmy cudzą własność i prawo.
Więcej na www.legalnakultura.pl
Polska Izba Książki

I Sieciowy system operacyjny Linux

1 Konfigurowanie interfejsu sieciowego 8
1.1. Odwzorowanie nazwy na adres IP 12
1.2. Testowanie połączenia sieciowego 13
1.3. Zabezpieczenie dostępu do komputera 13
2 Konfiguracja klienta poczty elektronicznej 16
3 Korzystanie z programu klient FTP. Pobieranie plików z sieci za pomocą programu wget 19

II Administrowanie systemem Linux

4 Zarządzanie użytkownikami i grupami 24
4.1. Polecenia stosowane do zarządzania użytkownikami 26
4.2. Zarządzanie grupami użytkowników 29
4.3. Zarządzanie grupami i użytkownikami w środowisku graficznym 30
5 Konfigurowanie drukarki sieciowej 35
5.1. Drukowanie sieciowe i zarządzanie drukowaniem 36
6 Instalowanie pakietów 40
6.1. Instalacja programów w środowisku tekstowym 41
6.2. Konfiguracja menedżera apt 45

III Usługi sieciowe w systemie Linux

7 Uruchamianie usług sieciowych 52
7.1. Konfigurowanie Firewall w systemie Linux 53
8 Przygotowanie do pracy serwera telnet 58
9 Przygotowanie do pracy serwera SSH 60
10 Przygotowanie do pracy serwera DHCP 62
11 Przygotowanie do pracy serwera DNS 68
12 Uruchamianie i korzystanie z usługi FTP 77
12.1. Konta użytkowników FTP 78
12.2. Instalacja serwera FTP na przykładzie vsftpd w dystrybucji Ubuntu 79
12.3. Konfiguracja serwera vsftpd 79
12.4. Konfiguracja serwera FTP do obsługi użytkowników lokalnych 80
12.5. Konfiguracja serwera FTP do obsługi użytkowników anonimowych 81
12.6. Zapisywanie danych na serwerze przez użytkowników anonimowych 82
12.7. Inne opcje konfiguracyjne serwera FTP 83
13 Konfiguracja serwera poczty elektronicznej 85
14 Uruchamianie usługi WWW 89
14.1 Udostępniane katalogi 89
14.2. Instalacja serwera WWW 90
14.3. Uruchamianie serwera WWW 90
14.4. Konfiguracja serwera Apache 90
14.5. Umieszczanie stron na serwerze WWW 92
14.6. Wielkość liter, nazwy plików 92
14.7. Konfiguracja serwera Apache do obsługi stron użytkowników 93
14.8. Konfigurowanie wirtualnych serwerów WWW 94
14.9. Blokowanie przeglądania zawartości katalogu 100

14.10. Zmiana domyślnie uruchamianego pliku ... 104
14.11. Przeglądanie logów serwera ... 106
15 Automatyczne uruchamianie zadań ... 109
16 Zarządzanie logiczną strukturą dysku ... 113
16.1. Tworzenie nowej partycji w systemie ... 113
16.2. Formatowanie i montowanie partycji ... 115
17 Przydziały dyskowe użytkowników ... 119
17.1. Testowanie przydziałów dyskowych użytkownika ... 121
18 Przydziały dyskowe grupy użytkowników ... 124
19 Udostępnianie zasobów systemu Linux klientom MS Windows ... 127
19.1. Plik konfiguracyjny serwera Samba ... 132
19.2. Konfiguracja serwera Samba w środowisku graficznym ... 134
19.3. Przeglądanie zasobów udostępnianych za pomocą serwera Samba ... 138

IV Sieciowy system operacyjny – Windows Server

20 Podstawowe pojęcia związane z Active Directory ... 142
21 Przygotowanie do instalacji Windows Server 2016 ... 147
21.1. Wymagania sprzętowe Windows Server ... 150
22 Konfiguracja Windows Server po instalacji ... 155
23 Instalacja kontrolera domeny ... 164
24 Zarządzanie kontami komputerów. Dodawanie komputerów do domeny ... 172
25 Zarządzanie kontami użytkowników ... 175
25.1. Zarządzanie kontami użytkowników w konsoli tekstowej ... 181
25.2. Zarządzanie kontami użytkowników w konsoli PowerShell ... 184
26 Uprawnienia w systemie Windows ... 189
27 Udostępnianie zasobów i przypisywanie uprawnień do udostępnianych zasobów ... 194
28 Foldery macierzyste użytkowników ... 196
29 Profile użytkowników Windows ... 198
30 Konfigurowanie roli serwera wydruku ... 202
31 Instalowanie i zarządzanie serwerem DHCP ... 206
32 Konfigurowanie serwera DNS ... 210
33 Internetowe usługi informacyjne ... 215
33.1. Konfigurowanie serwera FTP ... 216
33.2. Konfigurowanie serwera WWW ... 221
34 Konfigurowanie usługi RRAS ... 225
34.1. Sieci wirtualne VPN – narzędzia dostępu zdalnego do serwera ... 226
34.2. Konfigurowanie routingu między sieciami lokalnymi w Windows 2016 ... 232
35 Zarządzanie serwerem za pomocą pulpitu zdalnego ... 235
36 Usługi terminalowe ... 239
37 Konfigurowanie usługi WDS ... 246
38 Usługi serwera aktualizacji Windows ... 255
39 Usługi zasad sieciowych i dostępu sieciowego ... 262
40 Zabezpieczenie kontrolera domeny przed atakami ... 269

V Bezpieczeństwo danych

41 Cyberbezpieczeństwo ... 272
42 Kopie bezpieczeństwa ... 276
43 Zasady grup ... 281
44 Monitorowanie pracy serwera ... 294
45 Monitorowanie wydajności serwera ... 297

- Konfigurowanie interfejsu sieciowego
- Konfiguracja klienta poczty elektronicznej
- Korzystanie z programu klient FTP
- Pobieranie plików z sieci za pomocą programu wget

Sieciowy system operacyjny Linux

1 Konfigurowanie interfejsu sieciowego

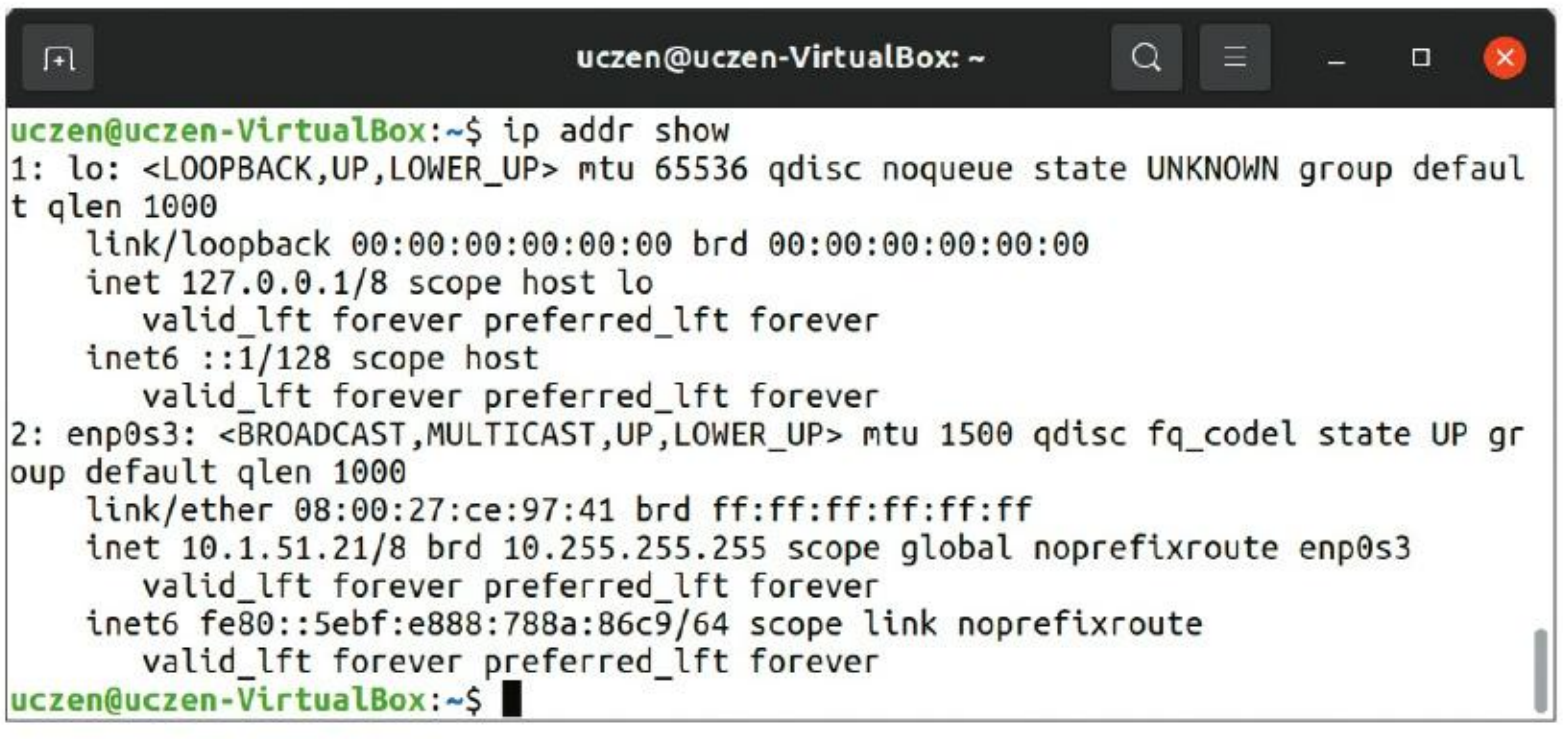
ZAGADNIENIA

Skonfigurowanie interfejsu sieciowego w systemie Linux **Funkcja pakietu narzędzi iproute2** **Skonfigurowanie interfejsu sieciowego za pomocą narzędzia ip** **Skonfigurowanie interfejsu sieciowego w środowisku graficznym** **Narzędzia umożliwiające odwzorowanie nazw na adresy IP** **Wpisy zawarte w przykładowym pliku `/etc/hosts`** **Metody testowania połączenia sieciowego w systemie Linux** **Polecenie `ping` i sposoby korzystania z niego** **Polecenie `traceroute` i sposoby korzystania z niego** **Zabezpieczenie komputera przed dostępem osób nieuprawnionych** **Dostęp do serwera dla wybranego komputera w sieci**

Linux jest systemem operacyjnym zawierającym wszystkie składniki niezbędne do przyłączenia do internetu lub zbudowania sieci lokalnej. Ze względu na stabilność działania i dużą wydajność często używa się go jako systemu operacyjnego serwerów w internecie.

W dystrybucjach umieszcza się wstępnie skonfigurowane serwery umożliwiające świadczenie usług, takich jak udostępnianie stron WWW, FTP, poczty elektronicznej i wielu innych.

Korzystanie z sieci w systemie Linux jest możliwe po wcześniejszym skonfigurowaniu ustawień dla interfejsu sieciowego. Interfejs Ethernet w Linuksie składa się z karty sieciowej i programu obsługi. Elementem sprzętowym jest karta sieciowa. Oprogramowanie interfejsu Ethernet to program obsługi używany przez jądro systemu. W celu wyświetlenia informacji o nazwach i konfiguracji interfejsów sieciowych można użyć polecenia **`ip addr show`** (rys. 1.1).

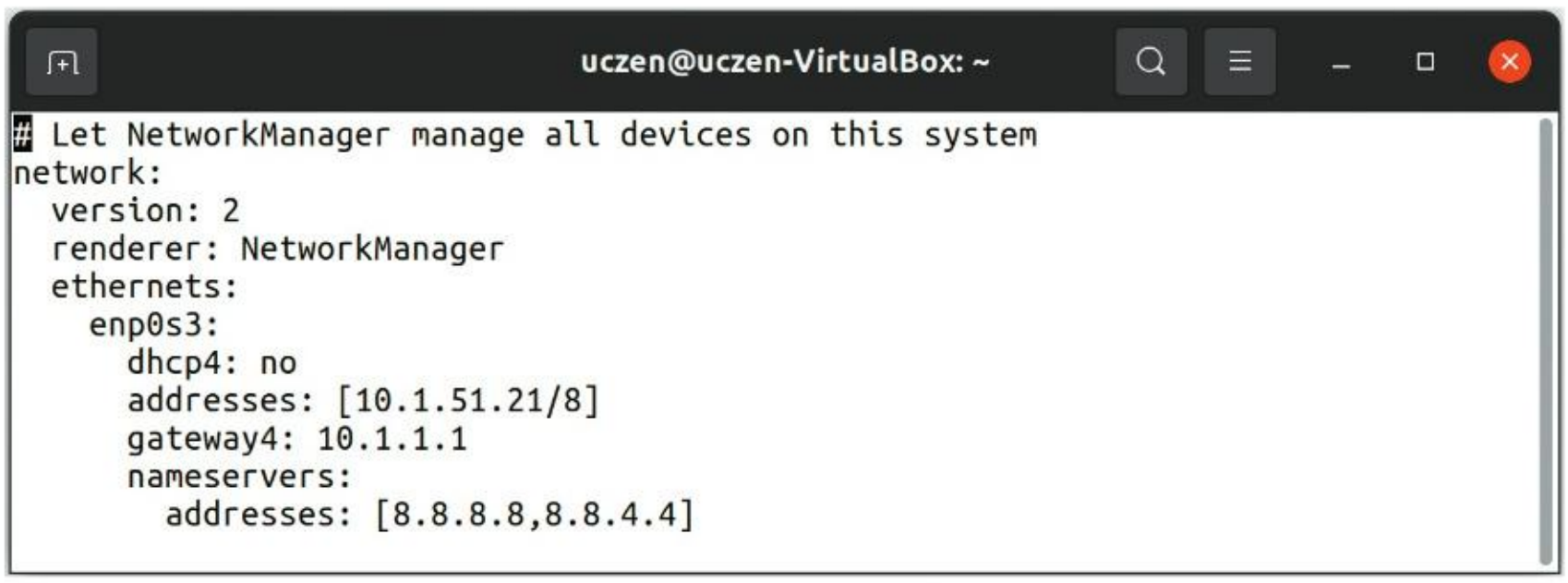


Rys. 1.1. **Informacje o nazwach i konfiguracji interfejsów sieciowych**

Domyślnie interfejsami zarządza **menedżer usług sieciowych** (ang. *network manager*). Konfigurację interfejsu sieciowego można wykonać w środowisku graficznym lub przez edycję pliku konfiguracyjnego.

W Ubuntu 20.04 jest dostępne narzędzie **netplan**, przeznaczone do konfiguracji interfejsów sieciowych w środowisku tekstowym. Ustawienia konfiguracyjne sieci są przechowywane w pliku **/etc/netplan/01-network-manager-all.yaml**.

Do edycji można wykorzystać dowolny edytor tekstu, np. **vi**. Na rys. 1.2 przedstawiono przykładową zawartość tego pliku.



Rys. 1.2. **Plik konfiguracyjny sieci z opisem interfejsu**

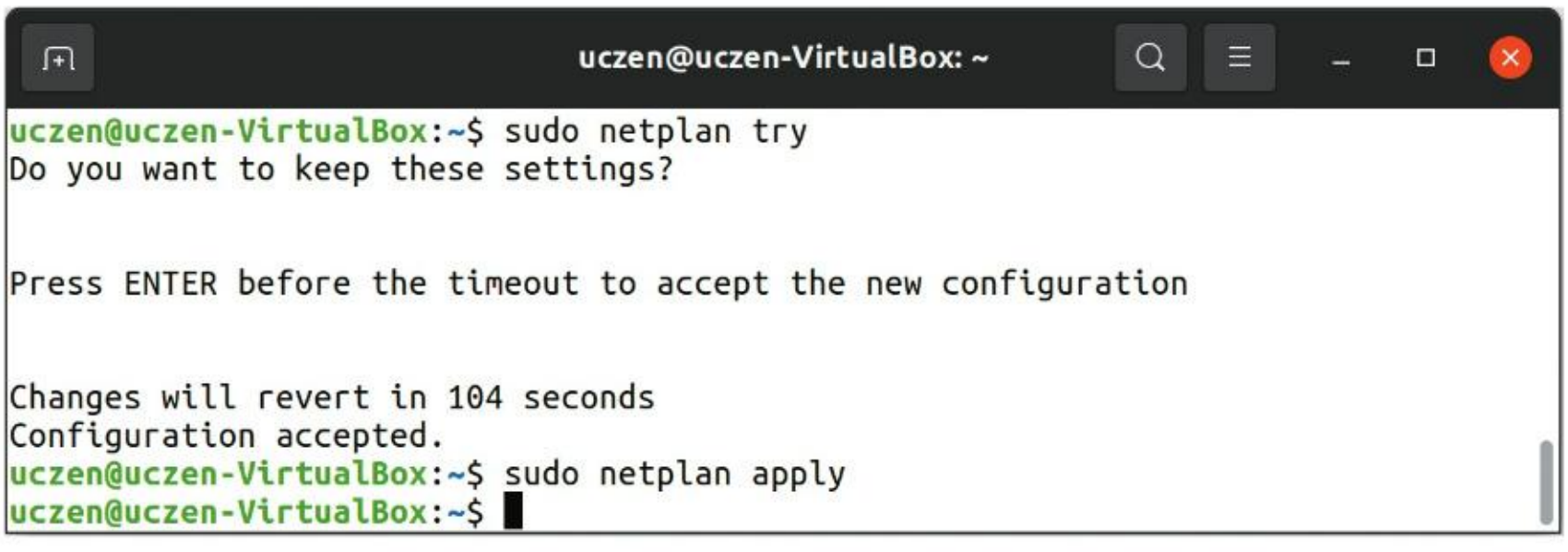
W pliku zdefiniowano konfigurację interfejsu sieciowego enp0s3 – konfigurowanego statycznie. Dla każdego interfejsu sieciowego istnieje sekcja w pliku, w którym są przechowywane ustawienia konfiguracyjne, np. dla interfejsu enp0s3:

- **dhcp4: no** – nie będzie wykorzystywany serwer DHCP;
- **addresses: [10.1.51.21/8]** – adres IP i maska (można wprowadzić kilka adresów oddzielonych przecinkiem);
- **gateway4: 10.1.1.1** – adres bramy sieciowej;
- **nameservers: addresses: [8.8.8.8, 8.8.4.4]** – adresy serwerów DNS.

> **! UWAGA**
> Wcięcia w pliku konfiguracyjnym należy wykonać za pomocą spacji.

Po wprowadzeniu zmian w plikach konfiguracyjnych należy sprawdzić poprawność konfiguracji i ponownie uruchomić interfejsy za pomocą poleceń:

```
sudo netplan try
sudo netplan apply
```



Rys. 1.3. **Testowanie pliku konfiguracyjnego i ponowne włączenie interfejsu**

Do konfigurowania różnych aspektów działania sieci i zarządzania nimi w systemie Linux można wykorzystać również pakiet narzędzi **iproute2**. Zawiera on programy: **tc** i **ip**. Pierwszy udostępnia wiele opcji do klasyfikowania, określania priorytetów, współdzielenia i limitowania przyznawanego pasma zarówno dla ruchu wychodzącego, jak i przychodzącego. Natomiast program ip łączy cechy narzędzi **ifconfig**, **route** i **arp**, używanych dotychczas do konfiguracji Linuksa w roli routera. W skład pakietu iproute2 wchodzi wiele narzędzi, które umożliwiają m.in.:

- konfigurowanie warstwy łącza (włączanie / wyłączanie interfejsów, zmiana adresów MAC, ustawienia MTU);
- konfigurowanie protokołów sąsiedztwa (ARP);
- konfigurowanie warstwy sieci (adresy IPv4 i IPv6);
- konfigurowanie routingu;
- konfigurowanie jakości usługi QoS (ang. *Quality of Service*);
- konfigurowanie interfejsów sieciowych obsługujących VLAN (IEEE 802.1Q);
- tworzenie bezpiecznych tuneli komunikacyjnych;
- uzyskanie informacji o otwartych portach, gniazdach.

Do wywoływania różnych funkcji pakietu służy polecenie **ip**. Ma ono wiele podpoleceń, np.:

- **ip link** – konfigurowanie warstwy łącza, np. tworzenie VLAN-ów;
- **ip address** – konfigurowanie adresów IP;
- **ip route** – konfigurowanie tablic routingu.

Więcej informacji dotyczących pakietu można uzyskać z pomocy (polecenie **man ip**) lub na stronie projektu https://wiki.linuxfoundation.org/networking/iproute2. Przykład konfiguracji interfejsu sieciowego za pomocą narzędzia **ip** przedstawiono na rys. 1.4.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
 qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 08:00:27:ce:97:41 brd ff:ff:ff:ff:ff:ff
    inet 10.1.51.21/8 brd 10.255.255.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fece:9741/64 scope link
       valid_lft forever preferred_lft forever
uczen@uczen-VirtualBox:~$ sudo ip addr add 10.1.51.121/8 brd + dev enp0s3
[sudo] hasło użytkownika uczen:
uczen@uczen-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
 qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 08:00:27:ce:97:41 brd ff:ff:ff:ff:ff:ff
    inet 10.1.51.21/8 brd 10.255.255.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 10.1.51.121/8 brd 10.255.255.255 scope global secondary enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fece:9741/64 scope link
       valid_lft forever preferred_lft forever
uczen@uczen-VirtualBox:~$
```

Rys. 1.4. Konfiguracja interfejsów sieciowych za pomocą `ip addr`

Pierwsze polecenie:

```
ip addr show
```

wyświetla aktualną konfigurację interfejsów sieciowych. Polecenie:

```
sudo ip addr add 10.1.51.121/8 brd + dev enp0s3
```

spowoduje, że interfejs enp0s3 otrzyma dodatkowy adres **10.1.11.121** i maskę **255.0.0.0** oraz domyślny adres rozgłoszeniowy. Ostatnie polecenie pozwala na sprawdzenie, czy konfiguracja została wprowadzona poprawnie.

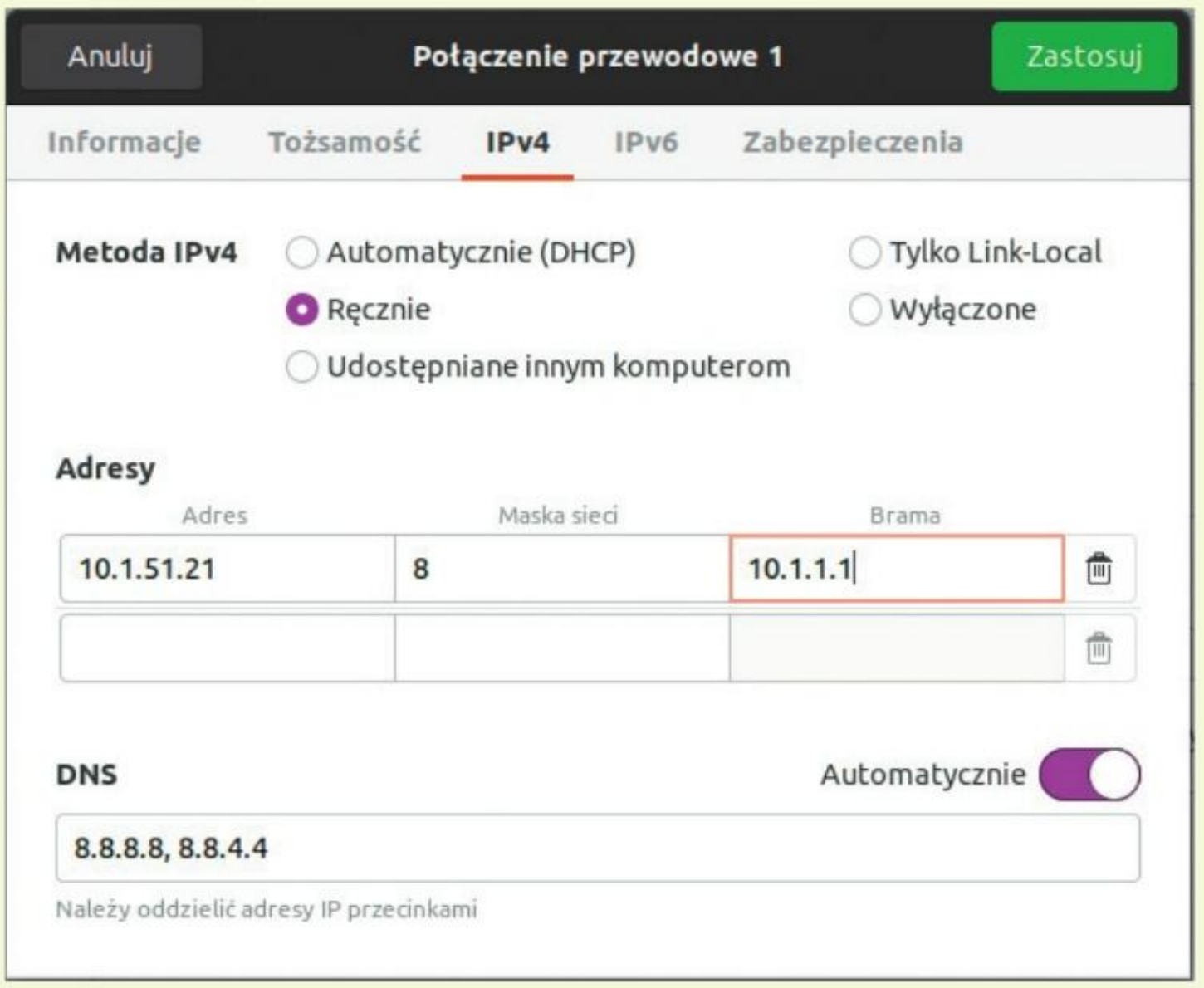
W środowisku graficznym istnieje **Menedżer sieci** – wygodne narzędzie do konfiguracji sieci.

PRZYKŁAD 1.1

Konfiguracja interfejsu sieciowego w środowisku graficznym

Aby skonfigurować interfejs sieciowy w środowisku graficznym, należy:

1. Wybrać **Wyświetl programy/Ustawienia/Sieć**, a w sekcji **Przewodowe** – **Połączenie przewodowe 1** (kliknąć ikonę koła zębatego).
2. W oknie konfiguracyjnym **Połączenie przewodowe 1** w zakładce **IPv4** wprowadzić informacje o konfiguracji połączenia (rys. 1.5). Jeżeli na liście nie ma żadnego połączenia, należy kliknąć przycisk **Dodaj (+)** i przejść do konfiguracji nowego połączenia.



Rys. 1.5. **Okno edycji połączenia sieciowego**

Aby Linux odczytał zmienione ustawienia interfejsu, należy go uruchomić ponownie, np. za pomocą polecenia:

```
sudo systemctl restart NetworkManager.service
```

1.1. Odwzorowanie nazwy na adres IP

Komputer korzysta z systemu DNS za pośrednictwem programu tłumaczącego nazwy na adresy IP – tzw. **resolvera**. Resolver używa pliku **`/etc/resolv.conf`** jako źródła danych o adresach serwerów DNS, do których może wysyłać zapytania. Plik jest zarządzany przez **netplan** i nie może być bezpośrednio edytowany. Jeżeli resolver otrzyma adres komputera, buduje zapytanie i przesyła je do jednego z serwerów zapisanych w pliku **`/etc/resolv.conf`**.

Plik **`/etc/hosts`** pozwala na zamianę adresu IP na nazwę symboliczną. Dzięki temu plikowi można podawać nazwy symboliczne komputerów, zamiast posługiwać się adresami IP. W pliku **`/etc/hosts`** znajduje się lista adresów i odpowiadających im nazw komputerów. Jeżeli używa się adresowania IPv4, w konfiguracji na rys. 1.6 adresowi **`127.0.0.1`** odpowiada nazwa **`localhost`**, a adresowi **`10.1.51.104`** – nazwa **`uczen4`**.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       uczen-VirtualBox
10.1.51.104 uczen4
10.1.51.105 uczen5
10.1.51.106 uczen6

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
uczen@uczen-VirtualBox:~$
```

Rys. 1.6. **Plik konfiguracyjny `/etc/hosts`**

Plik **`/etc/hosts`** zwykle jest używany do identyfikowania komputerów w małych sieciach lokalnych, w których nie skonfigurowano usługi DNS. W kontaktach z komputerami spoza sieci LAN zwykle korzysta się z DNS. W pliku konfiguracyjnym **`/etc/host.conf`** można m.in. określić kolejność, w jakiej resolver będzie używał metod szukania adresów hostów. Zawartość przykładowego pliku **`/etc/host.conf`** przedstawiono na rys. 1.7.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/host.conf
# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on
uczen@uczen-VirtualBox:~$
```

Rys. 1.7. **Plik konfiguracyjny `/etc/host.conf`**

Polecenie **`order hosts, bind`** określa, że komputer najpierw będzie przeszukiwał plik **`/etc/hosts`**, a w drugiej kolejności wysyłał zapytania do DNS. Drugi wiersz zezwala na zwracanie więcej niż jednego adresu IP z pliku **`/etc/hosts`** (jeśli przypisano większą liczbę adresów do nazwy).

1.2. Testowanie połączenia sieciowego

Do testowania połączenia między komputerami w sieci jest wykorzystywane polecenie **`ping`**, wysyłające pakiety testowe do wskazanego komputera, który powinien je natychmiast odesłać z powrotem. Mierzony jest czas między wysłaniem pakietu testowego a jego powrotem. Linux będzie wysyłał pakiety testowe aż do momentu przerwania tego procesu przez użytkownika. Kończymy wysyłanie pakietów kombinacją klawiszy [Ctrl] + [C].

> **! UWAGA**
>
> Aby w poleceniu **`ping`** można było używać nazwy komputera zamiast adresu IP, niezbędne jest poprawne skonfigurowanie pliku **`/etc/hosts`** lub usługi DNS.

> **PRZYKŁAD 1.2**
>
> **Testowanie połączenia sieciowego za pomocą nazw komputerów**
>
> Aby wprowadzić i przetestować prawidłowość przypisania nazw komputerów i połączenia sieciowego, należy:
>
> 1. Zalogować się na konto użytkownika.
> 2. Za pomocą edytora, np. **`vi`**, zmodyfikować plik **`/etc/hosts`**, dopisać do pliku adresy IP i nazwy komputerów kolegów, np. **`10.1.51.107 franek`**.
> 3. Wysłać pakiety testowe, posługując się nazwami komputerów, np. **`ping franek`**.

Poleceniem służącym do badania trasy pakietów w sieci jest **traceroute**. Po wykonaniu polecenie pokazuje trasę, po której pakiet porusza się do miejsca przeznaczenia. Odpowiednikiem linuksowego programu traceroute w systemach Windows jest program **tracert**. Dostępny jest także program **MTR**, który łączy funkcjonalność traceroute z narzędziem ping. Program śledzi trasę połączenia między dwoma punktami, podobnie jak traceroute, i odświeża wyniki w regularnych odstępach czasu.

> **! UWAGA**
>
> Jeżeli program traceroute nie jest zainstalowany, należy wydać polecenie **`sudo apt install traceroute`**, aby go zainstalować.

Dystrybucje Linuksa mogą korzystać z różnych menedżerów pakietów. W tym podręczniku jest wykorzystywany menedżer **apt**, dostępny w dystrybucji Debian, Ubuntu i wielu innych. Jeżeli używana przez ciebie dystrybucja korzysta z innego menedżera pakietów (rpm, yast, yum), poproś nauczyciela o wskazówki dotyczące sposobu instalacji pakietu. W rozdziale 6. szerzej omówiono narzędzia instalacyjne systemu Linux.

1.3. Zabezpieczenie dostępu do komputera

Komputer można zabezpieczyć przed dostępem osób nieuprawnionych przez skonfigurowanie plików **`/etc/hosts.allow`** i **`/etc/hosts.deny`**. Plik **`/etc/hosts.allow`** zawiera listę komputerów uprawnionych do korzystania z usług komputera, np.:

```
ALL: LOCAL @grupa_sieciowa
ALL: .zspsieradz.edu.pl EXCEPT uczen.zspsieradz.edu.pl
```

Reguła pierwsza zezwala na dostęp z komputerów w domenie LOCAL i członkom grupy grupa_sieciowa. Reguła druga zezwala na dostęp z komputerów w domenie **.zspsieradz.edu.pl**, z wyjątkiem komputera **uczen.zspsieradz.edu.pl**.

Plik **/etc/hosts.deny** zawiera listę komputerów nieuprawnionych do korzystania z usług komputera, np.:

```
ALL: .zspsieradz.edu.pl uczniowie.com.pl
```

Reguła nie zezwala na dostęp z komputerów w domenach **.zspsieradz.edu.pl** i **uczniowie.com.pl**. Jeżeli do serwera wpłynie żądanie dostępu do usługi, to serwer pobiera adres IP i nazwę domeny hosta oraz rodzaj usługi, z której użytkownik chce skorzystać. Następnie sprawdza w pliku **/etc/hosts.allow**, czy określony host może korzystać z usługi. Jeśli istnieje odpowiedni wpis zezwalający, to połączenie jest realizowane. Jeżeli takiego wpisu nie ma, jest wówczas sprawdzany plik **/etc/hosts.deny**. Usługę udostępnia się klientowi, jeżeli w pliku **/etc/hosts.deny** nie ma wpisu zabraniającego dostępu. Jeżeli oba pliki **hosts.allow** i **hosts.deny** są puste, to każde połączenie z każdym klientem będzie dopuszczone.

PRZYKŁAD 1.3

Zabezpieczanie dostępu do komputera

Aby zapewnić dostęp do serwera tylko z wybranego komputera w sieci, należy:

1. Zalogować się na konto użytkownika z uprawnieniami **root**.
2. Zablokować dostęp do wszystkich usług serwera. W pliku **/etc/hosts.deny** na końcu dopisać **ALL: ALL**.
3. Umożliwić dostęp tylko dla wybranego komputera. W pliku **/etc/hosts.allow** dopisać adres komputera uprawnionego do korzystania z serwera, np. **ALL: 10.1.51.123**.
4. Umożliwić dostęp tylko dla podsieci komputerów. W pliku **/etc/hosts.allow** dopisać adres podsieci z komputerami uprawnionymi do korzystania z serwera, np. **ALL: 10.1.151.0**.
5. Umożliwić dostęp tylko dla podsieci z wyjątkiem jednego z komputerów. W pliku **/etc/hosts.allow** dopisać adres podsieci z komputerami uprawnionymi do korzystania z serwera, np. **ALL: 10.1.251.0 EXCEPT 10.1.251.124**.
6. Przetestować możliwość nawiązywania połączenia z serwerem.

Skuteczniejszą metodą zapewnienia ochrony systemu komputerowego jest **zapora sieciowa – firewall**. W systemach Linux standardowo jest instalowany pakiet **iptables** oferujący znacznie więcej możliwości filtrowania ruchu sieciowego. Reguły stosowane w systemach zapór sieciowych są bardziej skomplikowane i pozwalają na precyzyjne definiowanie warunków, jakim musi podlegać ruch w sieci, aby został przepuszczony przez zaporę. Zapora sieciowa na podstawie zdefiniowanych reguł podejmuje decyzję, czy pakiet danych przepuścić czy zablokować. Więcej informacji o zaporach sieciowych zostanie przedstawionych w dalszej części podręcznika.

Inną metodą zabezpieczenia dostępu do komputera jest technologia **SELinux** (ang. *Security -Enhanced Linux*). Opiera się ona na koncepcji zapewnienia jak najmniejszej liczby uprawnień dla danego obiektu (np. konta użytkownika, urządzenia, programu), potrzebnych do jego poprawnego funkcjonowania, co ogranicza możliwości uzyskania dostępu do zasobów komputera lub wyrządzenia szkód po przejęciu kontroli nad obiektem przez osoby niepowołane.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyświetl informacje o interfejsach sieciowych twojego komputera:
   - Odczytaj adres IP twojego komputera, maskę podsieci i adres rozgłoszeniowy. Zapisz te informacje w zeszycie przedmiotowym.
   - Jaki jest adres fizyczny MAC karty sieciowej twojego komputera?
2. Za pomocą polecenia **`ip addr`** nadaj swojemu komputerowi dodatkowy adres IP.
3. Przypisz do adresu pętli zwrotnej w twoim komputerze nazwę loopback. Za pomocą polecenia **`ping`** przetestuj działanie pętli zwrotnej (użyj nazwy loopback).
4. Przypisz w pliku **`/etc/hosts`** imiona koleżanki / kolegi siedzących po prawej i lewej stronie do adresów ich komputerów. Za pomocą polecenia **`ping`** przetestuj działanie przypisania.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Sprawdź w pliku **`/etc/resolve.conf`** adresy serwerów DNS, z których korzysta twój komputer.

2 Konfiguracja klienta poczty elektronicznej

ZAGADNIENIA

Skonfigurowanie klienta poczty elektronicznej w systemie Linux **Korzystanie z poczty elektronicznej**

Najczęściej używanymi usługami w internecie są WWW i poczta elektroniczna. Przeglądarka internetowa jest dołączana do większości dystrybucji i dostarcza się ją w stanie umożliwiającym natychmiastowe działanie. Klient poczty elektronicznej również jest dołączany do dystrybucji, ale wymaga wstępnego skonfigurowania przed pierwszym użyciem. Konfiguracja na ogół polega na wprowadzeniu informacji o używanej skrzynce pocztowej oraz adresów serwera. Konfiguracja klienta poczty elektronicznej zostanie pokazana na przykładzie **Thunderbird**. Jeśli nie jest on zainstalowany, to można to zrobić za pomocą polecenia:

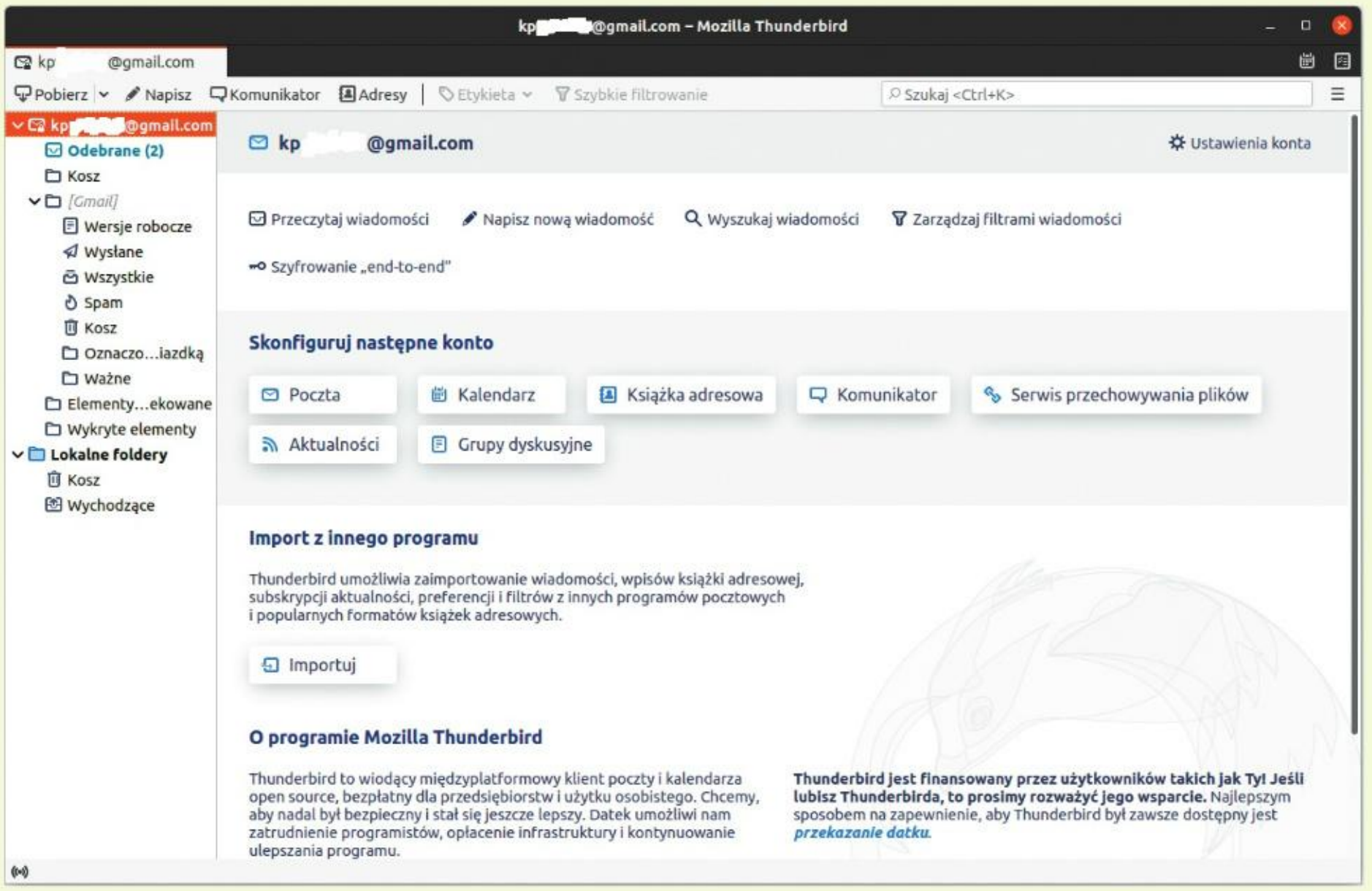
```
sudo apt install thunderbird.
```

PRZYKŁAD 2.1

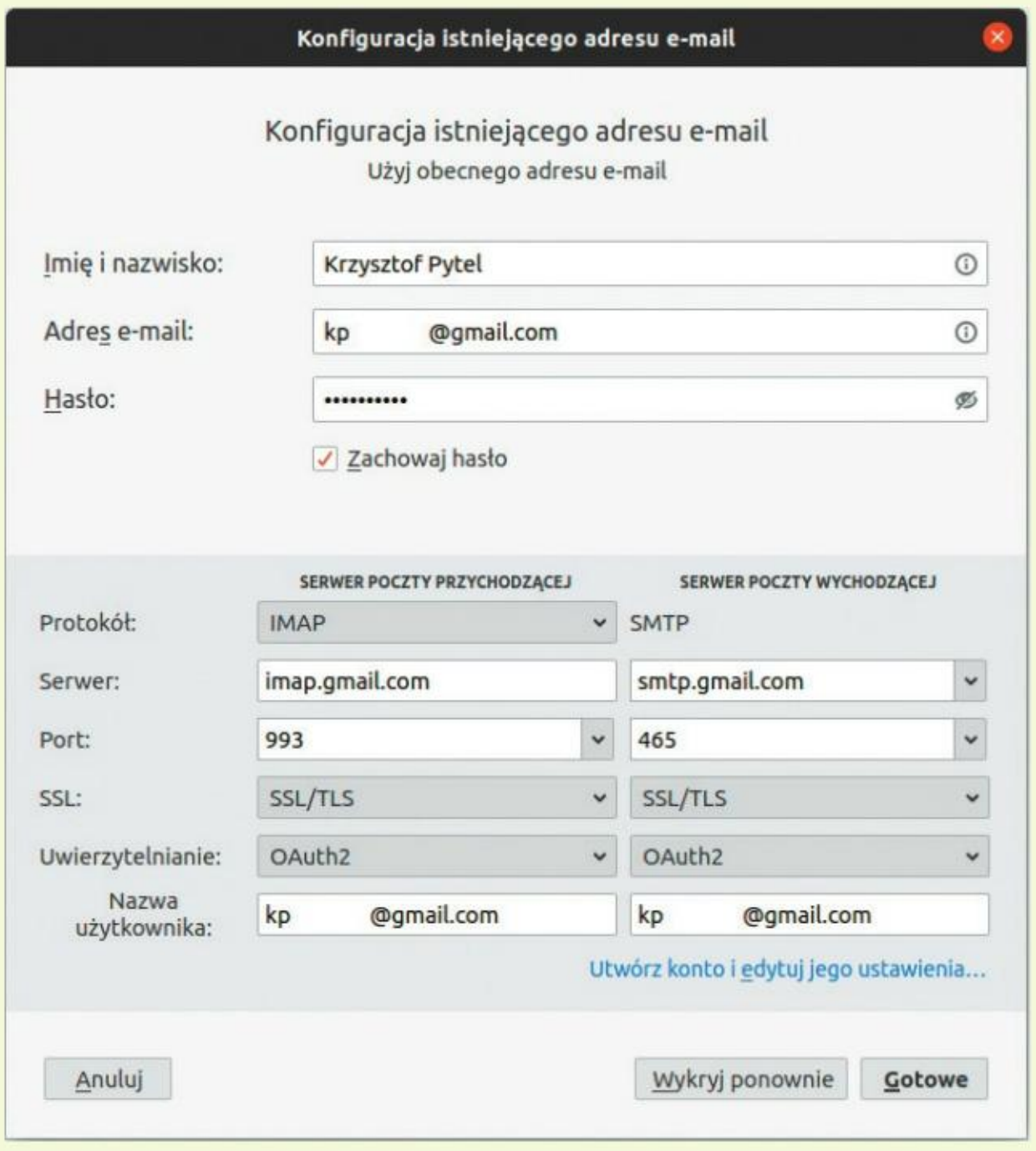
Konfiguracja klienta poczty elektronicznej na przykładzie Thunderbird

Po zainstalowaniu programu, przed uzyskaniem możliwości wymiany poczty elektronicznej, trzeba skonfigurować klienta poczty. W tym celu należy:

1. Uruchomić program. Kliknąć ikonę **`Wyświetl programy`** i w oknie **`Wyszukiwanie`** wpisać **`Thunderbird`**. Kliknąć ikonę **`Klient poczty Thunderbird`** (rys. 2.1).
2. W oknie głównym w sekcji **`Skonfiguruj następujące konta`** (ang. *Accounts*) wybrać typ konta e-mail. W oknie **`Konfiguracja istniejącego adresu e-mail`** wprowadzić nazwę użytkownika oraz adres e-mail i kliknąć przycisk **`Kontynuuj`** (ang. *Continue*).
3. Thunderbird ma dużą bazę danych serwerów pocztowych, więc istnieje szansa na poprawne wykrycie ustawień konfiguracyjnych serwera poczty wychodzącej i przychodzącej. Jeżeli konfiguracja nie zostanie poprawnie zweryfikowana przez kreatora, to można wprowadzić konfigurację ręcznie. W tym celu trzeba kliknąć przycisk **`Konfiguruj ręcznie...`** (ang. *Manual config*), a następnie wprowadzić parametry konfiguracyjne (rys. 2.2). Po weryfikacji lub modyfikacji danych należy kliknąć przycisk **`Gotowe`** (ang. *Done*) (rys. 2.3).

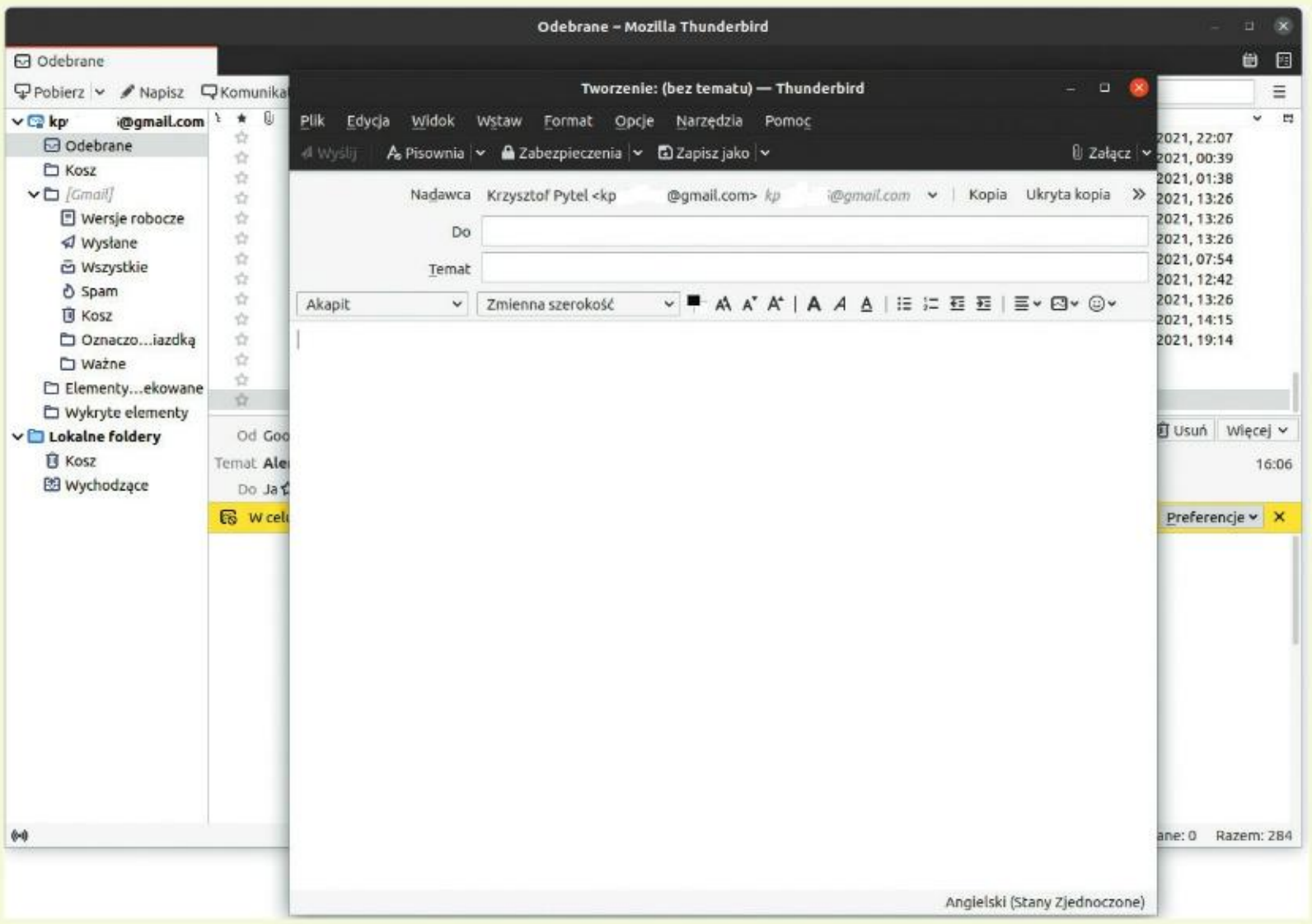


Rys. 2.1. **Okno główne programu Thunderbird**



Rys. 2.2. **Okno konfiguracji odbierania i wysyłania wiadomości w Thunderbird**

4. Jeżeli konfiguracja została przeprowadzona poprawnie, to można wysyłać i odbierać wiadomości e-mail (rys. 2.3).



Rys. 2.3. **Testowanie konfiguracji klienta poczty Thunderbird**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyszukaj na stronie dostawcy usługi informacje o adresach serwerów pocztowych twojego konta e-mail.
2. Skonfiguruj klienta poczty elektronicznej. Wyślij do koleżanki / kolegi e-maila z załącznikiem (dowolny plik). Odbierz wiadomość e-mail od koleżanki / kolegi. Sprawdź, czy można otworzyć załącznik.
3. Do odbierania wiadomości e-mail można wykorzystać protokół POP3 lub IMAP. Wyszukaj w internecie, czym różnią się te protokoły. Jeżeli twój dostawca umożliwia korzystanie z obu, to wybierz protokół, którego będziesz używać. Uzasadnij swój wybór.

3 Korzystanie z programu klient FTP. Pobieranie plików z sieci za pomocą programu wget

ZAGADNIENIA

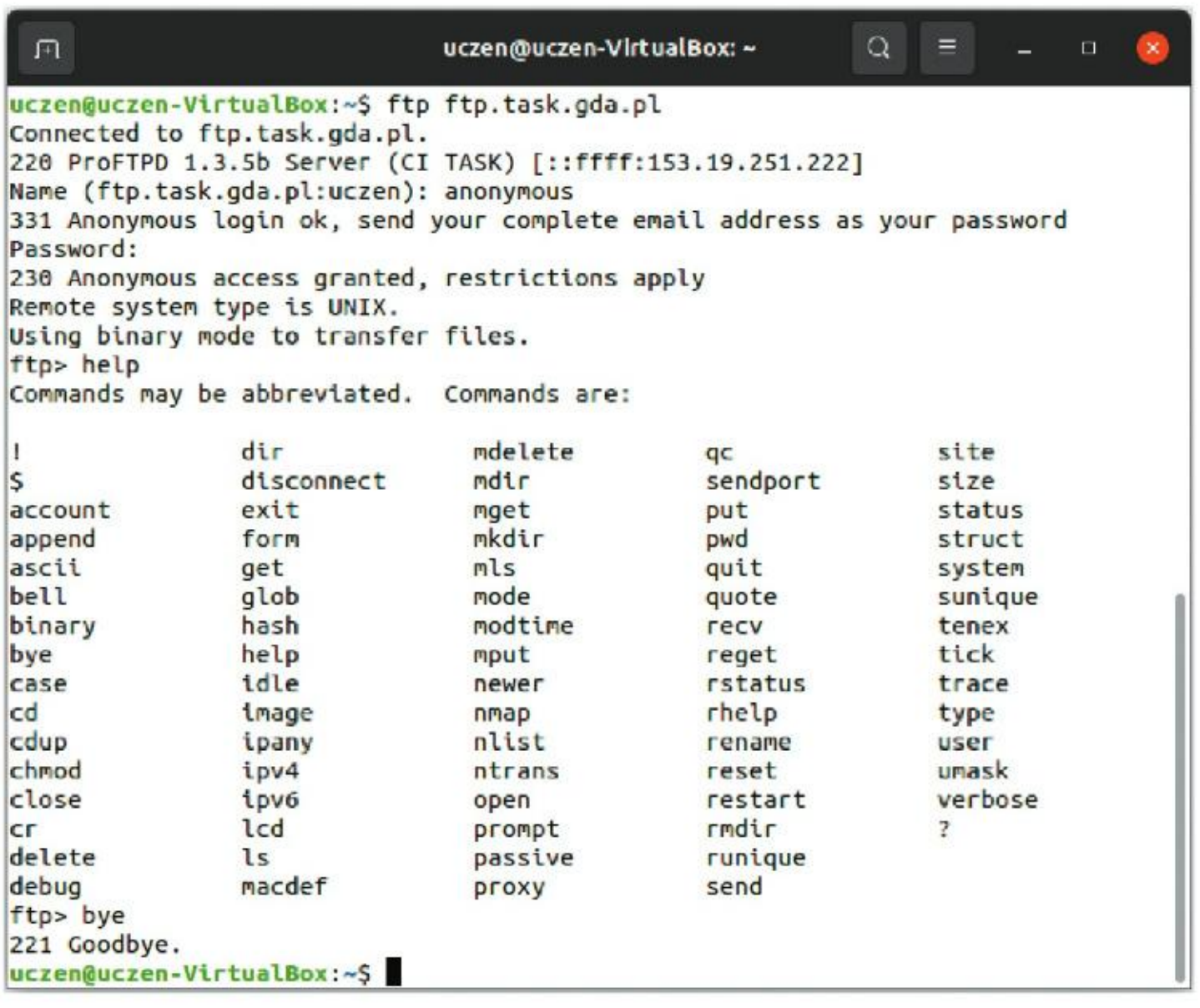
Nawiązanie połączenia z serwerem FTP **Korzystanie z programu gFTP w środowisku graficznym** **Pobieranie danych za pomocą programu wget**

Usługa FTP pozwala na kopiowanie plików między serwerem a klientem. Szerzej omówiono ją w rozdziale 12. Dlatego w tym miejscu zostanie tylko pokazane, jak uruchamiać poszczególne narzędzia.

Najczęściej użytkownicy anonimowi mają jedynie uprawnienia do pobierania plików z serwera. Użytkownik, jeśli korzysta z konta lokalnego na serwerze, ma prawo do kopiowania plików na serwer. Aby uruchomić tę usługę, jest potrzebny program klienta FTP. **Klient FTP** działający w trybie tekstowym jest wbudowany prawie we wszystkie systemy operacyjne. Do korzystania z takiego klienta są niezbędne znajomość poleceń i umiejętność ich właściwego stosowania. Do uruchomienia klienta FTP w trybie tekstowym służy polecenie:

```
ftp nazwa_serwera
```

Zamiast nazwy serwera można podać również jego adres IP. Do uzyskania listy poleceń używa się komendy **help**. Proces nawiązania połączenia z serwerem i sposób uzyskania pomocy przedstawiono na rys. 3.1.

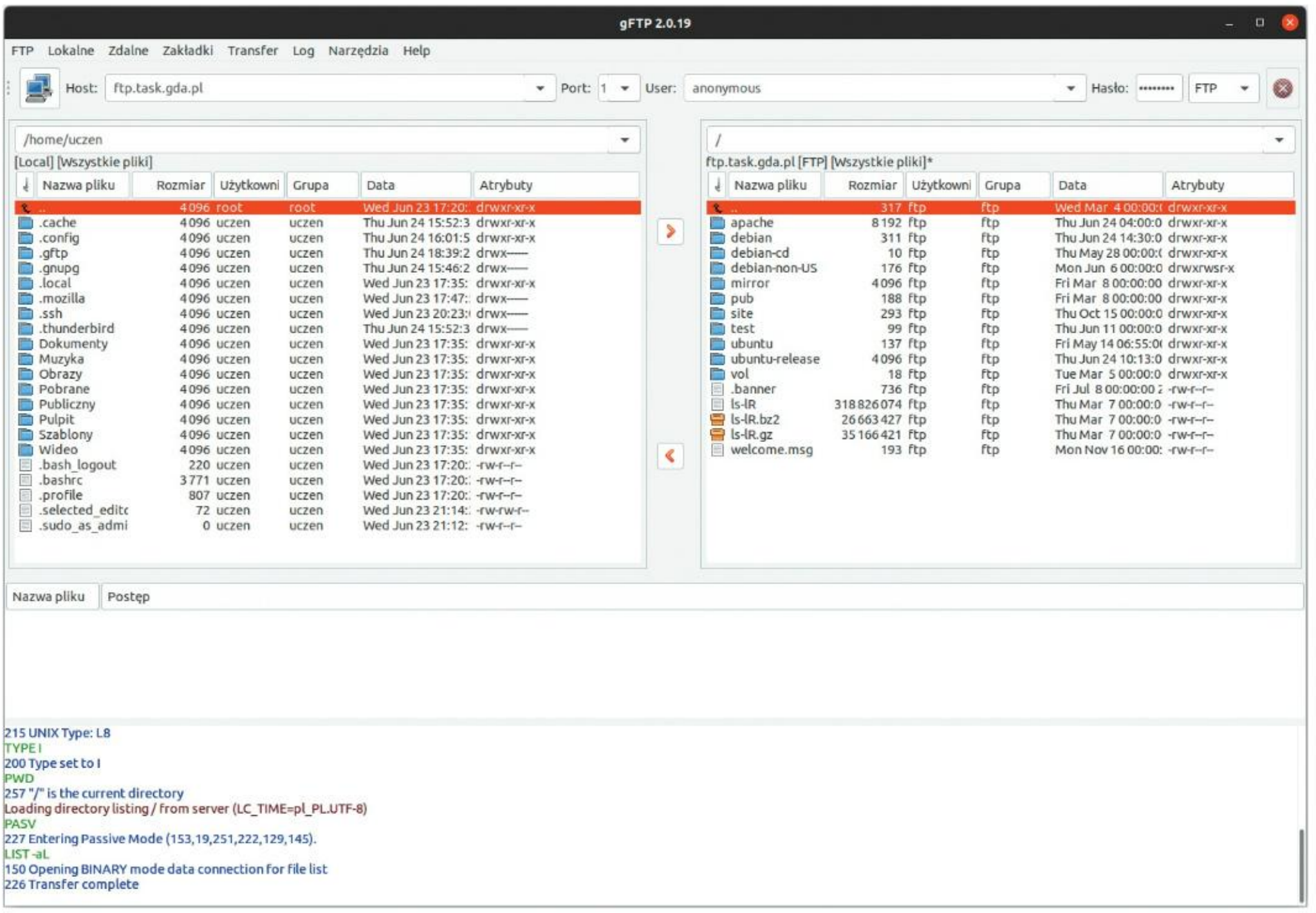


Rys. 3.1. Nawiązanie połączenia z serwerem FTP

W środowisku graficznym można uruchomić **gFTP** – klienta usługi FTP dla tego środowiska. Pakiet nie jest instalowany w konfiguracji domyślnej. Jeżeli nie został zaznaczony podczas instalacji systemu, należy go pobrać i zainstalować za pomocą polecenia:

```
sudo apt install gftp
```

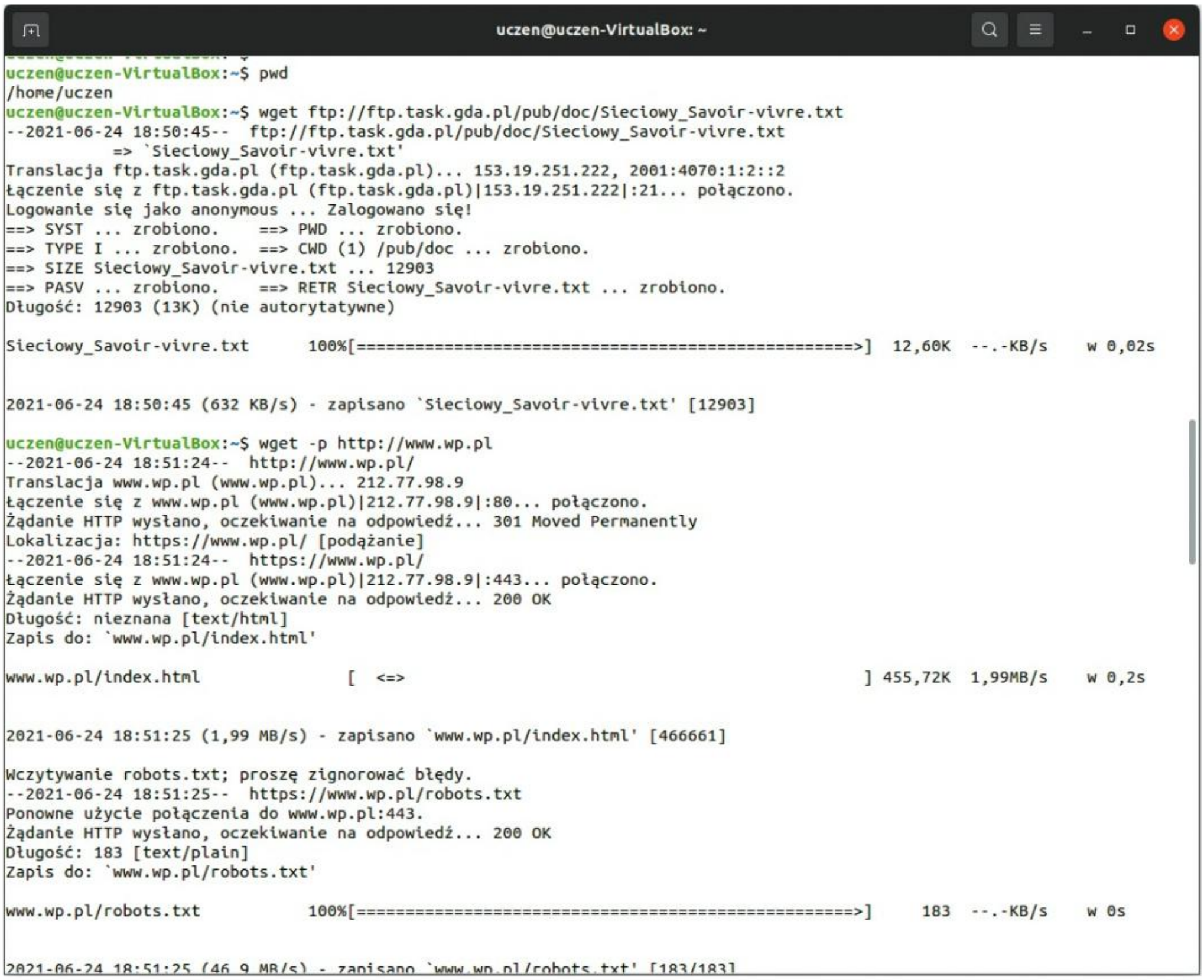
W celu uruchomienia programu należy kliknąć ikonę **Wyświetl programy** i w oknie **Wyszukiwanie** wpisać **gftp**. Kliknąć ikonę aplikacji gFTP. Jak większość tego typu programów, gFTP ma dwa panele, z których lewy służy do wyświetlania zawartości komputera lokalnego, a prawy jest przeznaczony dla serwera. W górnej części okna można wpisać w pole **Host**: adres serwera, z którym jest nawiązywane połączenie, w pole **Port** – numer portu (standardowo 21), a w pola **User** i **Hasło** – odpowiednio nazwę konta i hasło. Przesyłanie plików polega na zaznaczeniu odpowiedniego zbioru, a następnie naciśnięciu przycisku strzałki określającej kierunek przesyłania (rys. 3.2). W dolnej części okna znajdują się kolejka plików i lista poleceń odpowiadających wykonywanym funkcjom. Aby móc przesłać dane na serwer, należy mieć uprawnienia zezwalające na wykonanie takiej operacji.



Rys. 3.2. Pobieranie danych za pomocą gFTP

Oprócz klienta FTP w Linuksie istnieje jeszcze jedno bardzo przydatne narzędzie umożliwiające pobieranie plików ze zdalnych lokalizacji. Za pomocą programu **wget** można pobierać dane z różnych źródeł. Przykład pobierania plików z serwera WWW i FTP przedstawiono na rys. 3.3. Dane są pobierane do katalogu aktualnego w momencie wydania polecenia. Jak większość programów w Linuksie, wget ma wiele opcji, np.:

- i – odczytywania adresów z podanego pliku i pobierania ich po kolei;
- c – pobierania zbioru lub strony, która została już częściowo pobrana, a proces przerwano;
- r – rekursywnego pobierania całej hierarchii katalogów;
- p – pobierania wszystkich plików potrzebnych do wizualnego odwzorowania strony (dotyczy arkuszy stylów i plików graficznych).



Rys. 3.3. Pobieranie danych za pomocą wget

Pomoc dotyczącą obsługi aplikacji **wget** można uzyskać po wpisaniu polecenia: **man wget**. Program **wget**, używany z opcją „-p", odtwarza w bieżącym katalogu drzewo katalogów pobieranych witryn, pobiera wszystkie wymagane pliki graficzne i inne zasoby, do których odwołują się witryny. Zamienia też odnośniki w pobieranych plikach HTML tak, aby wskazywały na lokalnie pobrane pliki, dzięki czemu odnośniki w pobranych stronach działają poprawnie. Program **wget** jako URL dopuszcza również lokalizatory postaci **ftp://host/katalog/maska** (korzysta wówczas z protokołu FTP). Jeśli do dostępu do danego zasobu jest wymagana autoryzacja (dotyczy zwykle FTP), można podać URL postaci **ftp://uzytkownik:haslo@host/katalog**.

PRZYKŁAD 3.1

Pobieranie dokumentów z sieci

Aby pobrać z sieci dokument, należy:

1. Zalogować się na konto użytkownika i przejść do katalogu, w którym użytkownik ma prawo do zapisu, np. katalogu domowego użytkownika.
2. Za pomocą programu **wget** pobrać zawartość kompletnej witryny WWW, np. poleceniem **wget -p www.wp.pl**.
3. Za pomocą programu **wget** pobrać zawartość pliku **HARDWARE**. Plik **HARDWARE** zawiera informacje o sprzęcie zgodnym z systemem Linux. Plik jest dostępny na serwerze **ftp.task.gda.pl** w katalogu **pub/linux/docs**. Można użyć polecenia: **wget ftp.task.gda.pl/pub/linux/docs/HARDWARE**
4. Skorzystać z aplikacji **gFTP** i pobrać z serwera **ftp.task.gda.pl** plik **pub/doc/Sieciowy_Savoir-vivre.txt**.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj interfejs sieciowy w środowisku tekstowym i graficznym. Przetestuj działanie sieci.
2. Skonfiguruj klienta poczty elektronicznej i przetestuj jego działanie – wyślij wiadomość do koleżanki / kolegi.
3. Uruchom program gFTP i pobierz dowolny plik z serwera FTP, np. **ftp.task.gda.pl**, lub z serwera szkolnego.
4. Za pomocą programu wget pobierz dowolną witrynę WWW (wyszukaj witrynę o niewielkim rozmiarze) i plik z serwera FTP.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Do czego służy brama internetowa?
2. Jaka powinna być kolejność testowania urządzeń za pomocą polecenia **ping** w celu zdiagnozowania przyczyny braku połączenia z internetem?
3. Wyjaśnij różnicę między przeznaczeniem pliku **hosts.allow** a **hosts.deny**.
4. W jakim celu jest używany system DNS?
5. Podane poniżej polecenia pochodzą z linuksowego klienta FTP. Pomoc dotyczącą polecenia można uzyskać, jeśli się wpisze **help nazwa_polecenia** w konsoli klienta FTP. Napisz, do czego służą polecenia:
   ftp; **open hostname**; **close**; **quit**; **dir**; **ls**; **pwd**; **cd remote_dir**; **cd ..**; **lcd directory**; **binary**; **ascii**; **get file**; **put file**; **quit**; **delete**; **mkdir**; **rmdir**; **prompt**.

- Zarządzanie użytkownikami i grupami
- Konfigurowanie drukarki sieciowej
- Instalowanie pakietów
- Konfigurowanie Firewall w systemie Linux

Administrowanie systemem Linux

4 Zarządzanie użytkownikami i grupami

ZAGADNIENIA

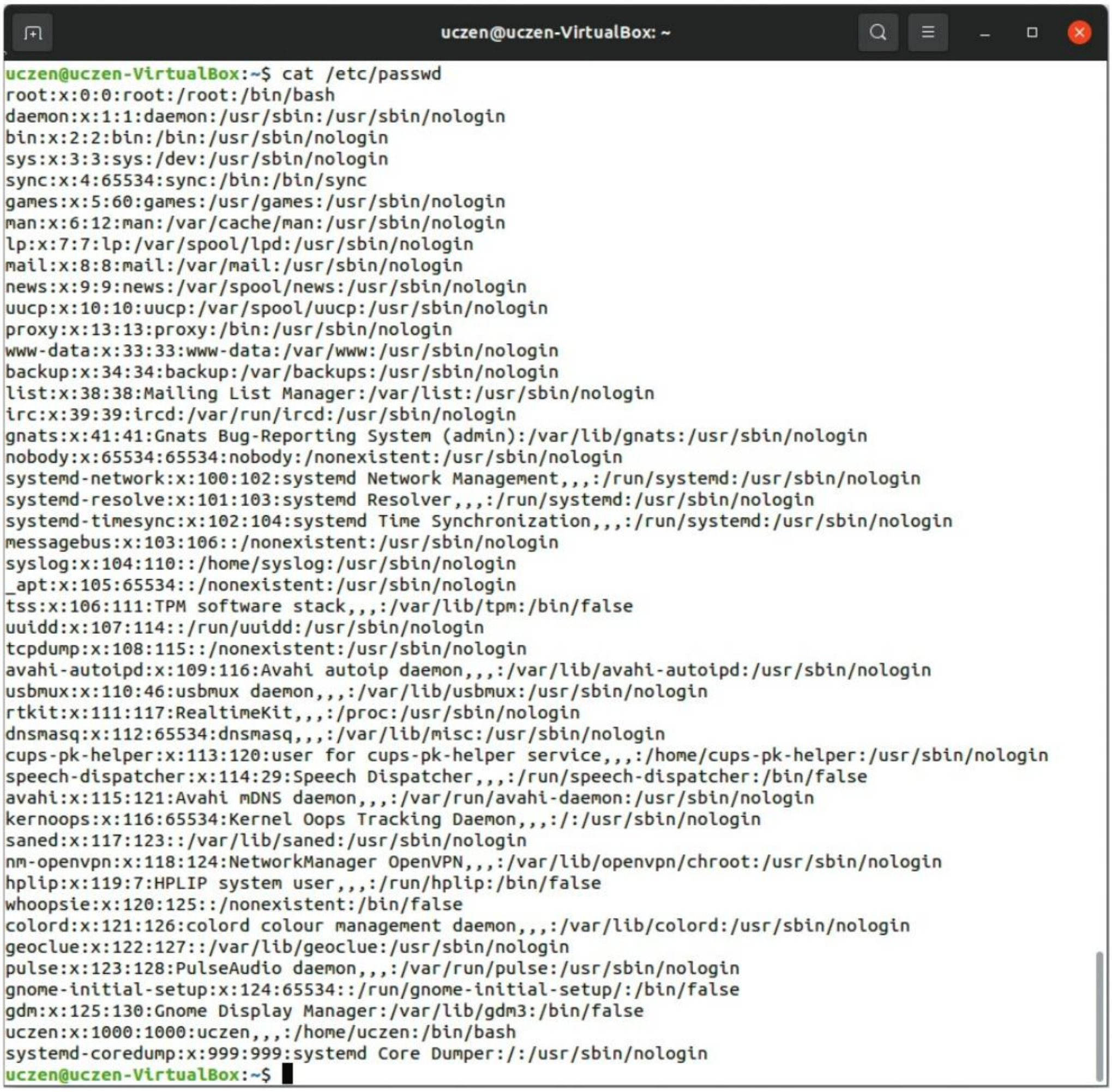
Konta użytkowników w systemie Linux Funkcja pliku `/etc/passwd` Katalogi domowe i ich przeznaczenie Polecenia stosowane w systemie Linux do zarządzania użytkownikami Zarządzanie użytkownikami w trybie tekstowym Zarządzanie użytkownikami w trybie interaktywnym Grupy użytkowników w systemie Linux i ich przeznaczenie Polecenia służące do zarządzania grupami użytkowników Zarządzanie grupami użytkowników w systemie Linux Zarządzanie użytkownikami w środowisku graficznym Zarządzanie grupami użytkowników w systemie Linux w środowisku graficznym

W systemach wielodostępnych z systemu może korzystać jednocześnie wielu użytkowników. Każdy z nich ma przydzielone zasoby, np. pamięć lub czas procesora. W systemie musi więc istnieć system kont pozwalających na zarządzanie poszczególnymi użytkownikami i jednoznaczne ich identyfikowanie za pomocą unikatowych nazw, podawanych podczas logowania. **Konto** to wszystkie pliki, zasoby i informacje należące do użytkownika. Każdy użytkownik jest identyfikowany przez unikatową liczbę całkowitą – **id użytkownika** (UID).

Aby stworzyć użytkownika, należy zmienić bazę użytkowników i utworzyć katalog domowy. Podstawową bazą użytkowników w Linuksie jest plik haseł **`/etc/passwd`**. Znajdują się w nim informacje o wszystkich kontach w systemie. Każdy wiersz pliku zawiera informacje o jednym koncie i składa się z siedmiu pól, oddzielonych dwukropkami. W tych polach są umieszczane:

- nazwa użytkownika – nazwa użytkownika w systemie;
- znacznik hasła w postaci zakodowanej – specjalny znacznik, że hasło znajduje się w innym pliku, lub w starszych wersjach systemu zakodowane hasło użytkownika;
- numeryczny identyfikator użytkownika – liczbowy identyfikator użytkownika UID;
- numeryczny identyfikator grupy – liczbowy identyfikator grupy GID;
- imię i nazwisko oraz dodatkowy opis użytkownika – opisowa nazwa użytkownika;
- katalog domowy – ścieżka do katalogu domowego użytkownika;
- powłoka logowania – program uruchamiany po zalogowaniu się.

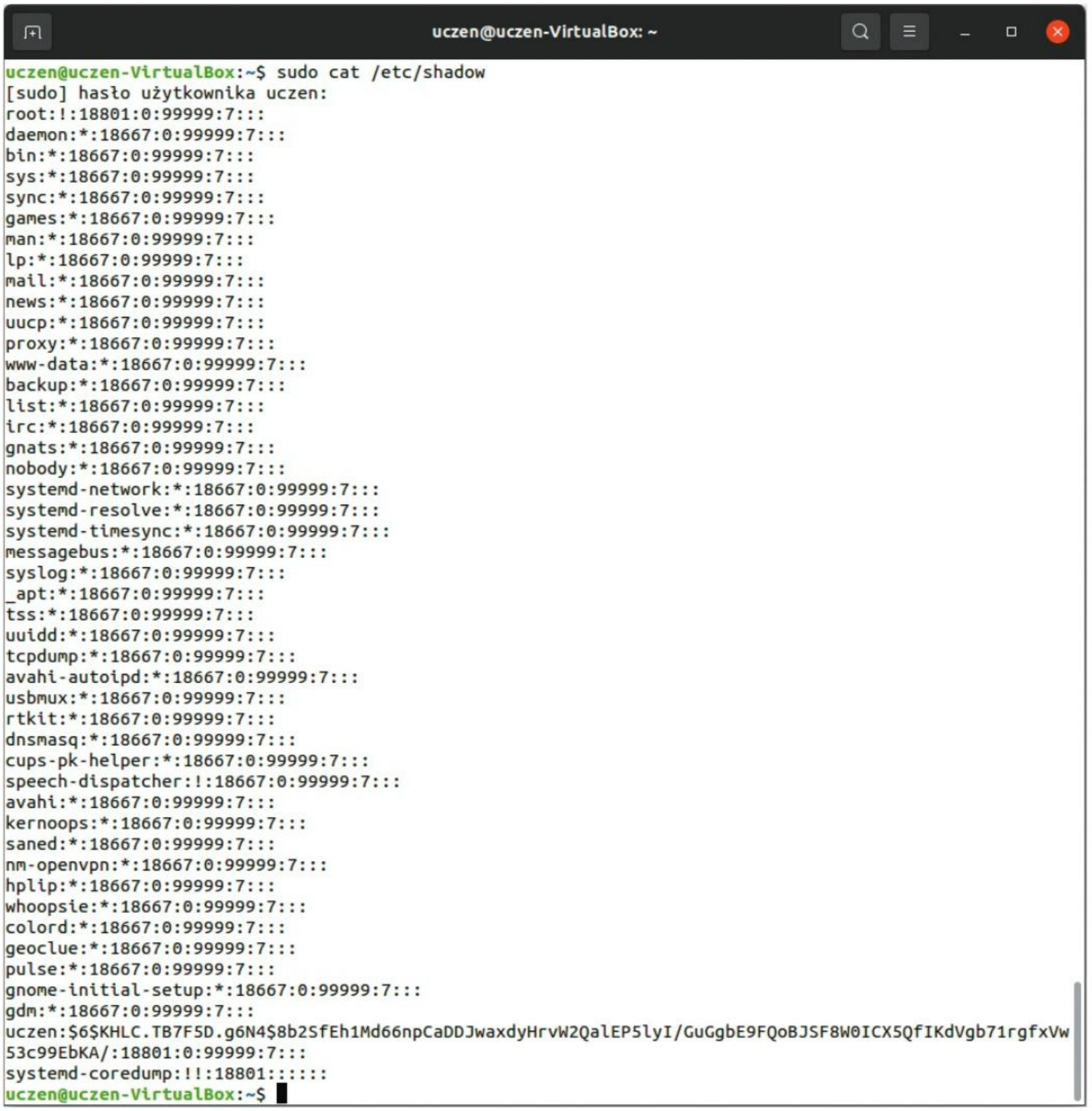
Każdy z użytkowników może odczytać plik haseł i w ten sposób poznać nazwy innych użytkowników. Współczesne systemy przechowują zakodowane hasła w oddzielnym pliku **`/etc/shadow`**. Może go odczytać tylko użytkownik z uprawnieniami administratora (ang. *root*). Plik **`/etc/passwd`** zawiera specjalny znacznik „x" oznaczający, że hasło znajduje się w innym miejscu. Zawartość przykładowego pliku **`/etc/passwd`** przedstawiono na rys. 4.1.



Rys. 4.1. **Zawartość przykładowego pliku `/etc/passwd`**

Katalogi domowe użytkowników są przeznaczone do przechowywania zbiorów określających ich środowisko pracy, np. pulpit, i innych zbiorów prywatnych. Każdy użytkownik ma wszystkie prawa do własnego katalogu domowego. Standardowym miejscem dla katalogów domowych jest **`/home`**. W celu łatwiejszego zarządzania uprawnieniami są tworzone **grupy użytkowników**. Uprawnienia przyznane grupie użytkowników dotyczą wszystkich użytkowników będących członkami tej grupy. Uprawnienia wynikające z przynależności do wielu grup sumują się, np. jeżeli użytkownik *uczen* należy do grupy *Wszyscy* i grupy *Uczniowie*, to jego efektywne uprawnienia są sumą uprawnień nadanych grupie *Wszyscy*, grupie *Uczniowie* i indywidualnie użytkownikowi *uczen*.

Zawartość przykładowego pliku **`/etc/shadow`** przedstawiono na rys. 4.2. W każdej linii pliku jest opisane jedno konto. Pierwsza wartość w linii to nazwa konta, a druga to zaszyfrowana postać hasła do tego konta (wartości są oddzielone dwukropkami).



Rys. 4.2. Zawartość przykładowego pliku `/etc/shadow`

4.1. Polecenia stosowane do zarządzania użytkownikami

Zarządzanie użytkownikami jest jednym z obowiązków administratora. To zadanie może wykonywać również inny użytkownik mający odpowiednie uprawnienia. Domyślnie te uprawnienia ma tylko **administrator** (ang. *root*), ale może je przekazać innemu użytkownikowi. Do zarządzania użytkownikami i grupami najczęściej są używane następujące polecenia:

- **`useradd`** – dodawanie nowego użytkownika, np.:

  `sudo useradd uczen`

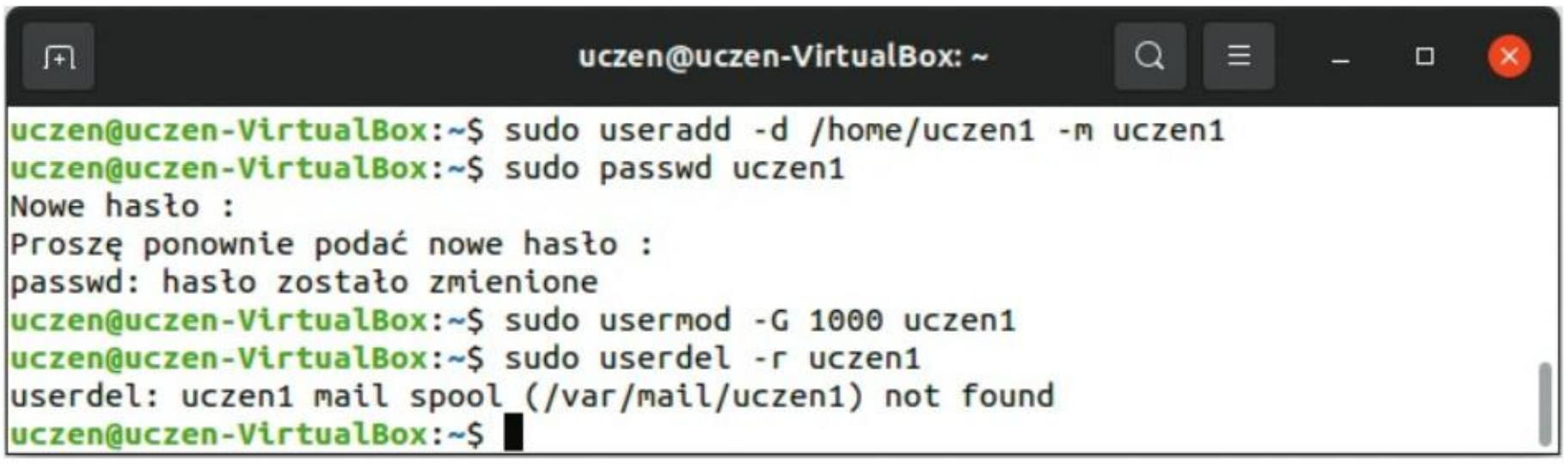
  utworzy konto *uczen*. Konto nie ma ustawionego hasła ani innych właściwości. Najważniejsze opcje polecenia **`useradd`**:

- **`c komentarz`** – dodanie komentarza (imię i nazwisko użytkownika) do pola komentarza w pliku haseł;
- **`d katalog_domowy`** – wskazanie katalogu domowego dla nowego użytkownika, standardowo jest tworzony nowy katalog w **`/home`**;
- **`m`** – tworzenie katalogu domowego, jeśli nie istnieje;
- **`g początkowa_grupa`** – numer lub nazwa początkowej grupy logowania użytkownika;
- **`G grupa[,...]`** – grupa lub lista grup, do których również ma należeć tworzony użytkownik;
- **`s powłoka`** – ustawienie powłoki systemowej użytkownika; ustawienie powłoki na **`/sbin/nologin`** powoduje, że użytkownik nie może się zalogować;
- **`u id_użytkownika`** – podanie numerycznej wartości identyfikatora użytkownika (UID); numer musi być dodatni i unikatowy (domyślnie jest ustawiana wartość najmniejsza wolna, począwszy od 500);
- **`p zakodowane_hasło`** – należy podać hasło w formie zakodowanej, np. takie, jak utworzone poleceniem **`crypt`**;
- **`nazwa_użytkownika`** – nazwa logowania nowego użytkownika;

- **`passwd`** – zmienia hasło użytkownika, np.:

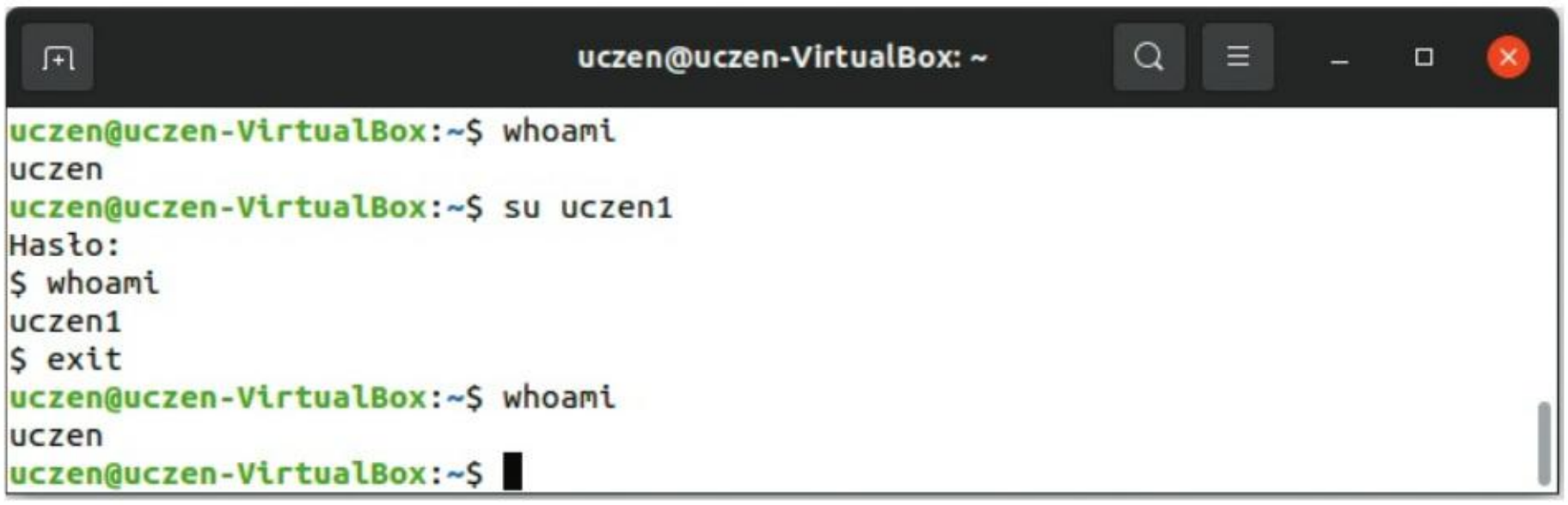
```
sudo passwd uczen
```

  Jeżeli nie zostanie wskazana nazwa konta, dla którego jest zmieniane hasło, to zmieni się hasło użytkownika, z którego konta polecenie zostało wydane. Jeżeli jest zmieniane własne hasło, to program zapyta nas najpierw o stare hasło, a następnie – o nowe. Po wpisaniu dwukrotnie nowego hasła program zweryfikuje je pod kątem wymaganej złożoności. Jeśli hasło jest zbyt łatwe, użytkownik otrzyma stosowny komunikat, ale hasło zostanie przyjęte. Przykład poleceń użytych do utworzenia użytkownika przedstawiono na rys. 4.3;
- **`usermod`** – zmienia ustawienia użytkownika. Można używać takich samych opcji jak w poleceniu **`useradd`** oraz:
  - **`L`** – blokuje konto użytkownika; ta opcja powoduje wstawienie „!” na początku zakodowanego hasła;
  - **`U`** – odblokowuje konto użytkownika;
- **`userdel`** – kasuje konto użytkownika; katalog domowy nie zostanie usunięty (jeżeli katalog domowy ma być również usunięty, trzeba użyć opcji **`-r`**);



Rys. 4.3. **Zarządzanie użytkownikami w trybie tekstowym**

- **`su`** – umożliwia zmianę konta. Administrator może zmienić własne konto na dowolne inne, np. w celu przetestowania uprawnień. Zmiana konta na *root* wymaga podania hasła. Aby powrócić do początkowego konta, należy wpisać polecenie **`exit`**. Przykłady użycia polecenia **`su`** przedstawiono na rys. 4.4.



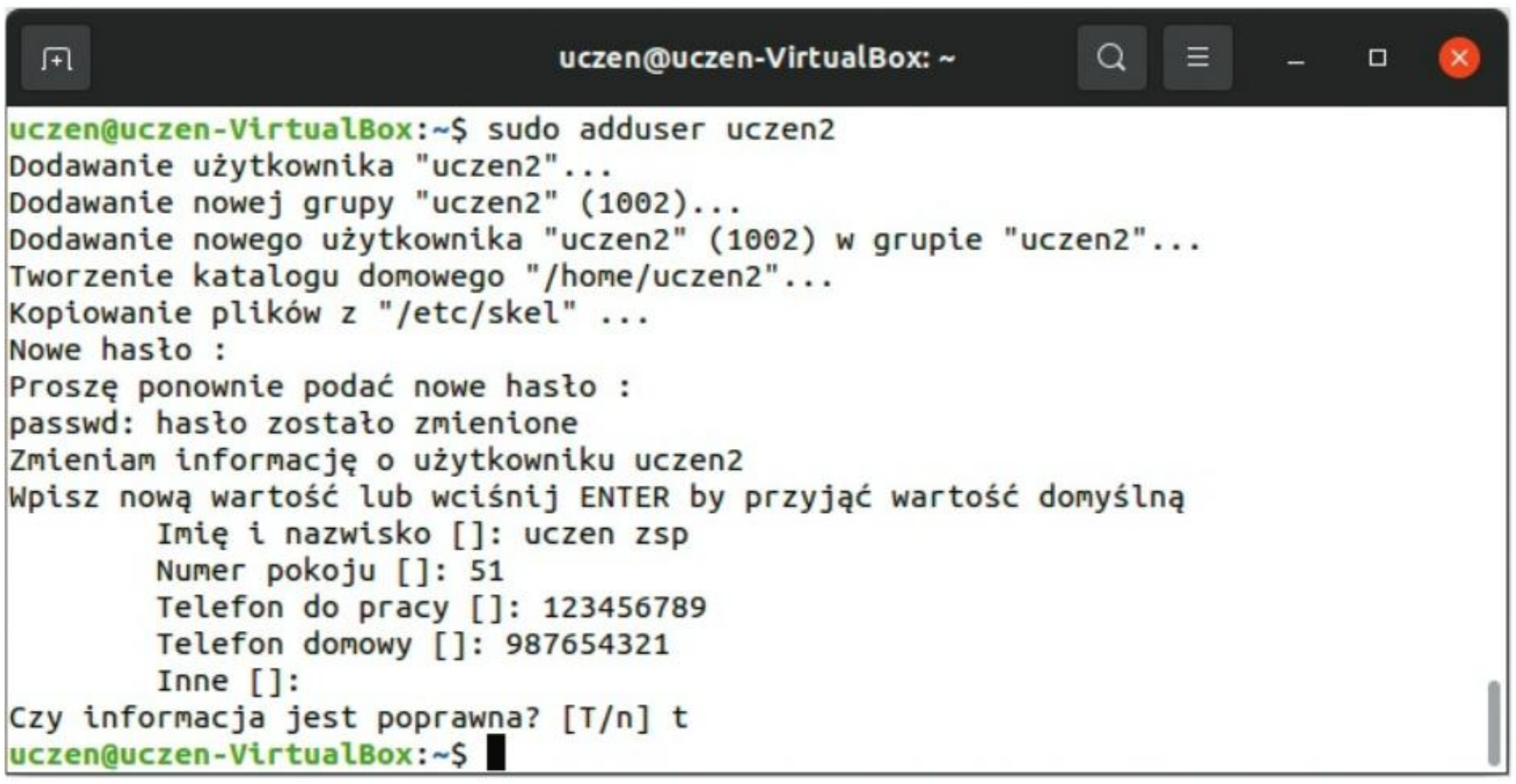
Rys. 4.4. **Użycie polecenia su**

Aby użytkownik mógł zalogować się do systemu, należy:

- utworzyć dla niego konto;
- wprowadzić hasło dla użytkownika.

Użytkowników można tworzyć również w trybie interaktywnym (rys. 4.5) – podczas tworzenia użytkownika będą wprowadzane dodatkowe informacje, np. hasło. Do interaktywnego tworzenia użytkowników wykorzystuje się polecenie **adduser**, np.

```
sudo adduser uczen.
```



Rys. 4.5. **Zarządzanie użytkownikami w trybie interaktywnym**

PRZYKŁAD 4.1

Zarządzanie użytkownikami

Należy utworzyć użytkowników:

- *uczen1, uczen2, ... uczen5* z hasłem *123*;
- *student1, student2, ... student5* z hasłem *qwerty*;
- *nauczyciel1, nauczyciel2, ... nauczyciel5* z hasłem *zsp123*.

Aby wykonać zadanie, należy:

1. Zalogować się na konto użytkownika.

2. Utworzyć konto użytkownika za pomocą polecenia:

   sudo useradd uczen1

3. Zmienić hasło użytkownika za pomocą polecenia:

   sudo passwd uczen1

4. Powtórzyć operacje z punktów 2. i 3. dla każdego użytkownika.
5. Wyświetlić zawartość pliku **/etc/passwd** i sprawdzić, czy konta użytkowników zostały poprawnie utworzone, za pomocą polecenia:

   sudo cat /etc/passwd

6. Odczytać identyfikatory UID utworzonych kont użytkowników.
7. Zalogować się na konto utworzonego użytkownika i sprawdzić zawartość jego katalogu domowego.

4.2. Zarządzanie grupami użytkowników

Grupy użytkowników mają ułatwić administratorowi przypisywanie uprawnień do zasobów. Jeżeli w systemie jest wielu użytkowników, którzy powinni mieć uprawnienia do zasobu, np. katalogu, to przypisywanie tych uprawnień każdemu oddzielnie jest pracochłonne. Można jednak utworzyć grupę, dołączyć do niej wszystkich użytkowników, którzy powinni mieć uprawnienia, a następnie nadać uprawnienia grupie. Jeżeli po jakimś czasie do grupy zostanie dołączony kolejny użytkownik, będzie on miał takie same prawa jak pozostali. Każda grupa ma swój **identyfikator** (GID), wykorzystywany do jednoznacznej identyfikacji grupy. Każdy z użytkowników musi należeć przynajmniej do jednej grupy. Główna grupa, do której należy użytkownik, jest zapisana w pliku **/etc/passwd**. Pozostałe grupy są zapisane w pliku **/etc/group**. W tym pliku każda grupa jest opisana w innym wierszu. Każdy wiersz składa się z czterech pól oddzielonych dwukropkami:

- nazwa grupy;
- hasło – jeżeli pole jest puste, to hasło nie jest wymagane;
- identyfikator grupy (GID);
- lista użytkowników należących do tej grupy.

Aby zarządzać grupami użytkowników, należy mieć odpowiednie uprawnienia (domyślnie ma je *root*). Do zarządzania grupami najczęściej są używane następujące polecenia:

- **groupadd** – dodawanie nowej grupy użytkowników, np.

  sudo groupadd uczniowie

  utworzy grupę uczniowie.
  Najważniejsze opcje polecenia **groupadd**:
  – **g grupa** – identyfikator grupy (GID);
  – **p zakodowane_hasło** – należy podać hasło w formie zakodowanej, np. takie, jak utworzone poleceniem **crypt**;
- **addgroup** – dodawanie nowej grupy użytkowników w trybie interaktywnym, np.:

  sudo addgroup uczniowie;

- **groupmod** – zmienia ustawienia grupy. Można używać takich samych opcji jak w poleceniu **groupadd**;
- **groupdel** – kasuje grupę użytkowników.

Aby zmienić grupę, do której należy zasób, trzeba użyć polecenia **chgrp**. Przykładowo, jeżeli nowym właścicielem pliku o nazwie **plik.txt** ma być grupa *uczniowie*, należy użyć polecenia:

```
sudo chgrp uczniowie plik.txt
```

Grupę może zmienić tylko właściciel pliku i tylko na grupę, do której należy (reguła nie dotyczy administratora).

PRZYKŁAD 4.2

Zarządzanie grupami użytkowników

Aby utworzyć grupę użytkowników i przydzielić do niej użytkowników, należy:

1. Zalogować się na konto użytkownika.
2. Utworzyć grupy użytkowników *uczniowie*, *studenci* i *nauczyciele*, np. użyć polecenia:

   ```
   sudo groupadd uczniowie
   ```

3. Dodać utworzone w przykładzie 4.1 konta *uczen1*, *uczen2*, ... *uczen5*, *student1*, *student2*, ... *student5* i *nauczeciel1*, *nauczyciel2*, ... *nauczyciel5* odpowiednio do grup *uczniowie*, *studenci* i *nauczyciele*, np. użyć polecenia:

   ```
   sudo usermod -G uczniowie uczen1
   ```

4. Wyświetlić zawartość pliku **/etc/group** i sprawdzić poprawność przypisania użytkowników do grup oraz identyfikatory utworzonych grup GID za pomocą polecenia:

   ```
   sudo cat /etc/group
   ```

UWAGA

Nie można usunąć grupy podstawowej użytkownika, jeżeli ma ona przynajmniej jednego członka. Należy najpierw usunąć wszystkich użytkowników albo zmienić ich grupę początkową na inną, a dopiero później usunąć grupę.

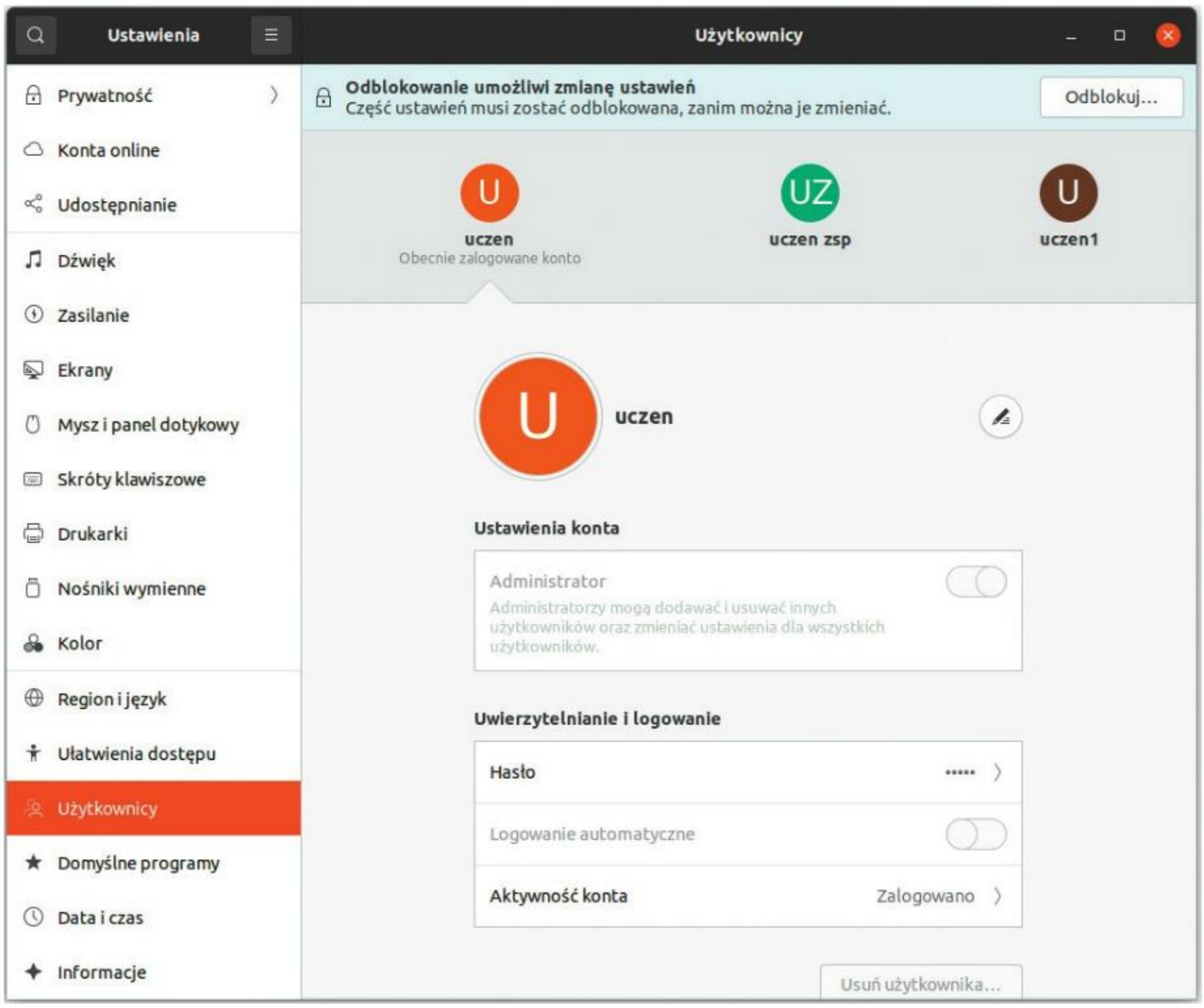
PRZYKŁAD 4.3

Tworzenie i testowanie konta grupy

Utwórz grupę użytkowników *moderatorzy*. Dodaj do niej użytkownika *moderator*.

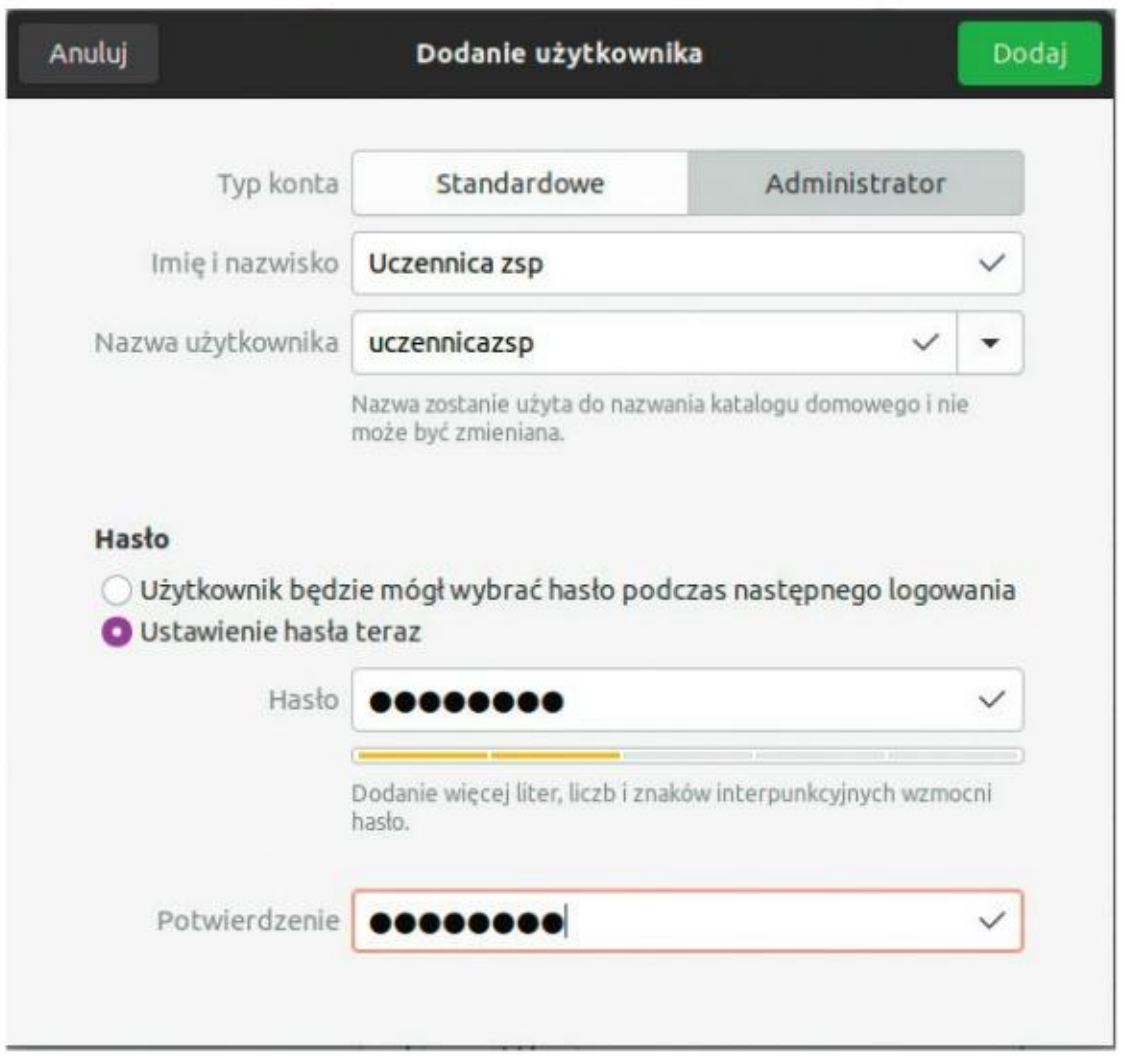
4.3. Zarządzanie grupami i użytkownikami w środowisku graficznym

W środowisku graficznym istnieje **Menedżer użytkowników** – wygodne narzędzie do zarządzania użytkownikami i grupami. Aby je uruchomić, trzeba wybrać **Wyświetl programy/Ustawienia/Użytkownicy**. Jeżeli dane mają być edytowane, to należy odblokować dostęp przez kliknięcie przycisku **Odblokuj** (ang. *Unlock*) w prawym górnym rogu okna (rys. 4.6).



Rys. 4.6. **Menedżer użytkowników**

Aby za pomocą **Menedżera użytkowników** dodać nowe konto, należy kliknąć przycisk **Dodaj użytkownika...** (ang. *Add User...*), a następnie określić właściwości tworzonego konta i kliknąć przycisk **Dodaj** (ang. *Add*). Na rys. 4.7 przedstawiono szczegóły dodawanego konta.

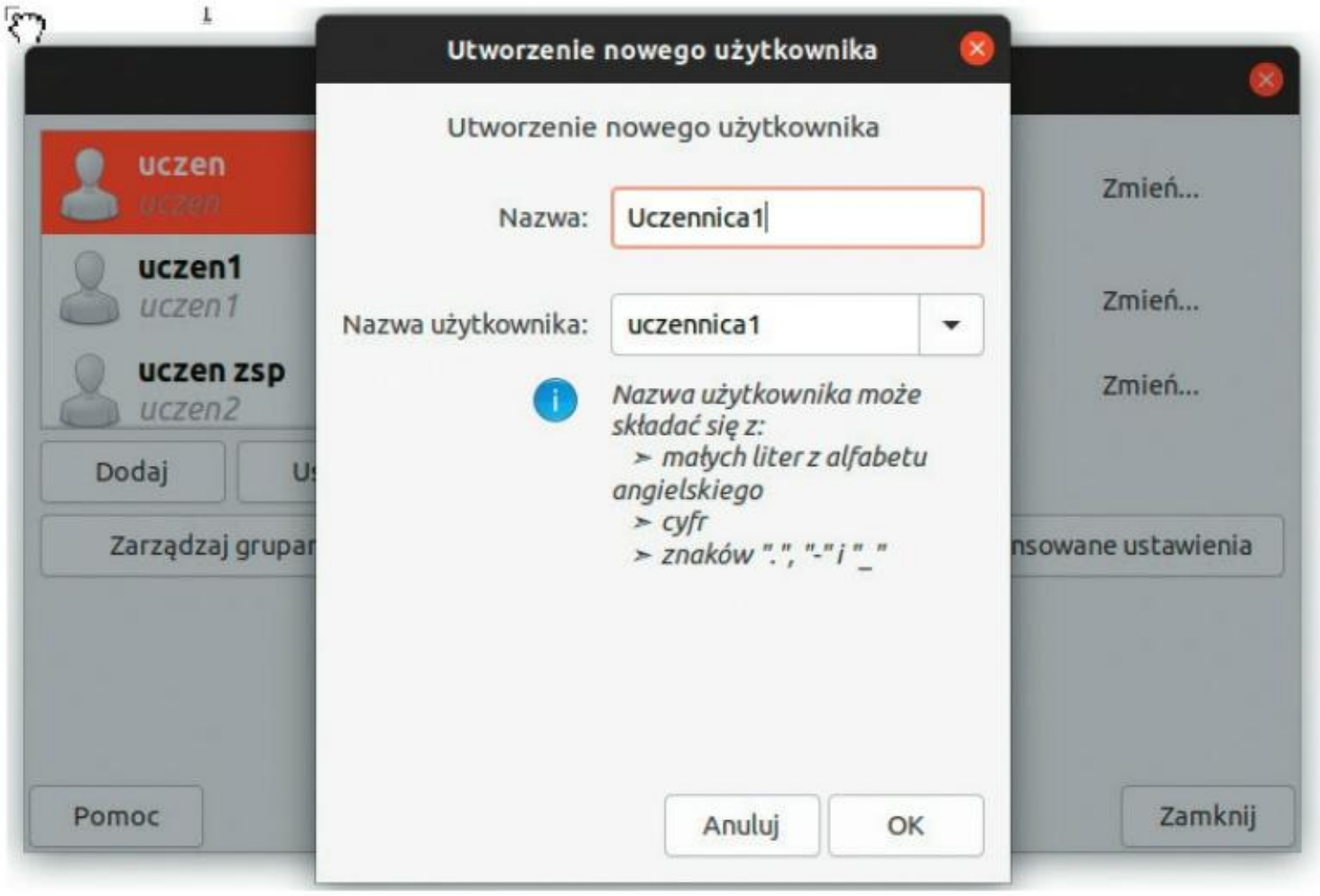


Rys. 4.7. **Szczegóły dodawanego konta**

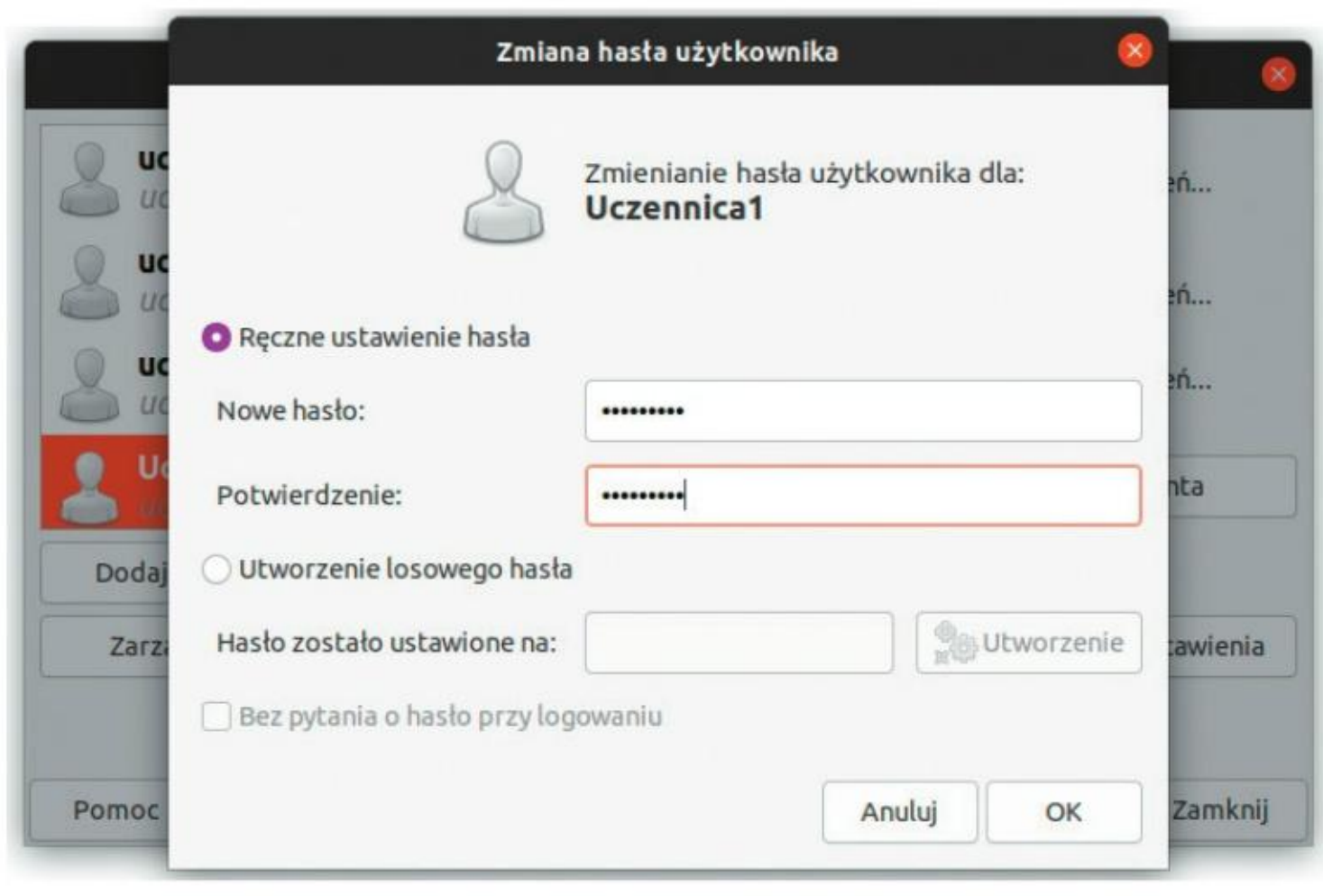
Menedżer użytkowników instalowany domyślnie w środowisku graficznym Ubuntu umożliwia tylko zarządzanie użytkownikami. Zarządzanie grupami w środowisku graficznym jest możliwe po zainstalowaniu dodatkowego zestawu narzędzi, np. **gnome-system-tools**. Aby zainstalować ten zestaw narzędzi, należy wykonać polecenie:

```
sudo apt install gnome-system-tools
```

Aby uruchomić aplikację do zarządzania użytkownikami i grupami, trzeba wybrać **Wyświetl programy**, w polu wyszukiwania wpisać **Użytkownicy** (ang. *Users*) i kliknąć ikonę **Użytkownicy i grupy**. W celu dodania nowego konta użytkownika należy kliknąć przycisk **Dodaj**, a następnie określić właściwości tworzonego konta. Na rys. 4.8 przedstawiono informacje o nazwie dodawanego konta, a na rys. 4.9 wprowadzanie hasła.

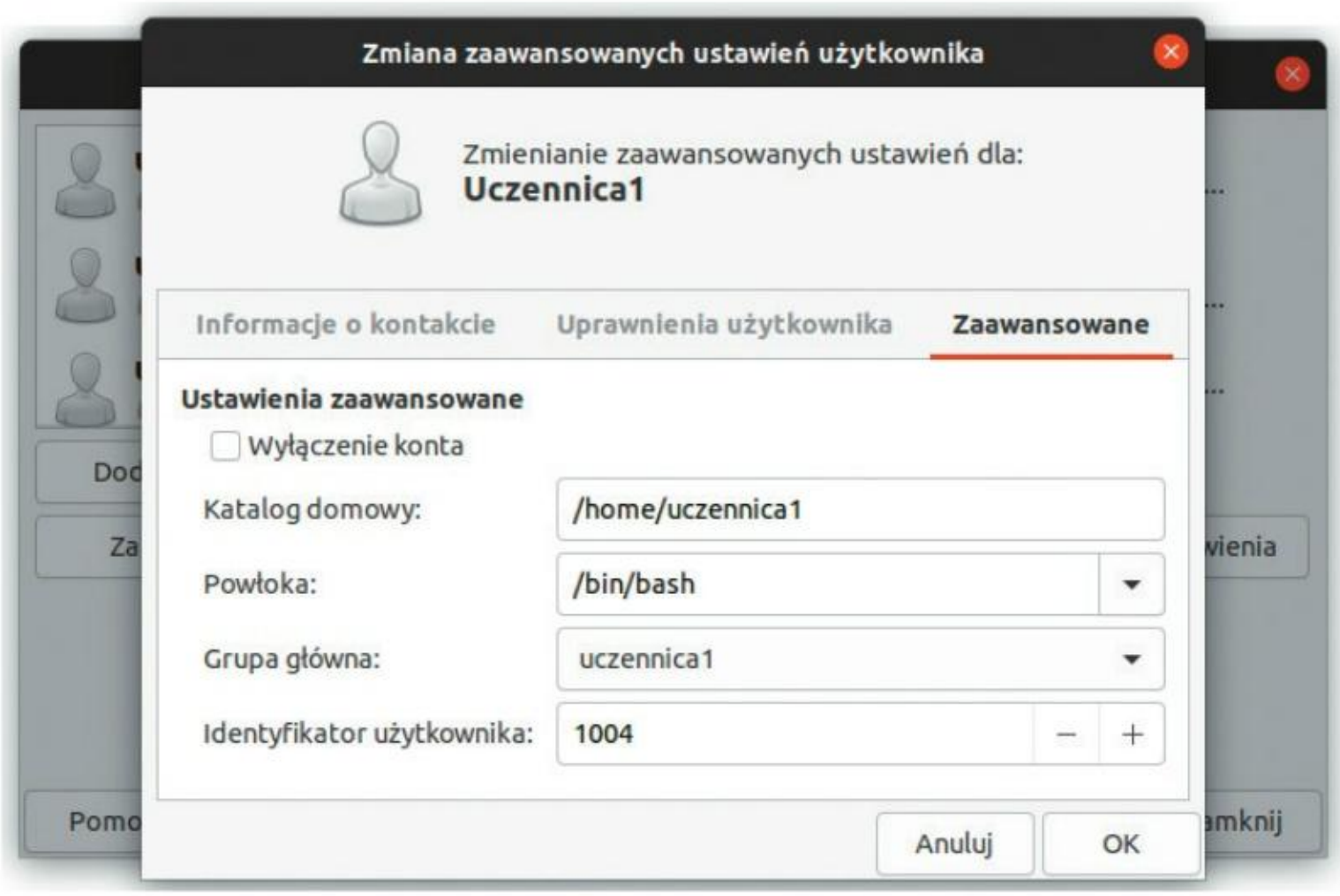


Rys. 4.8. **Informacje o nazwie dodawanego konta**



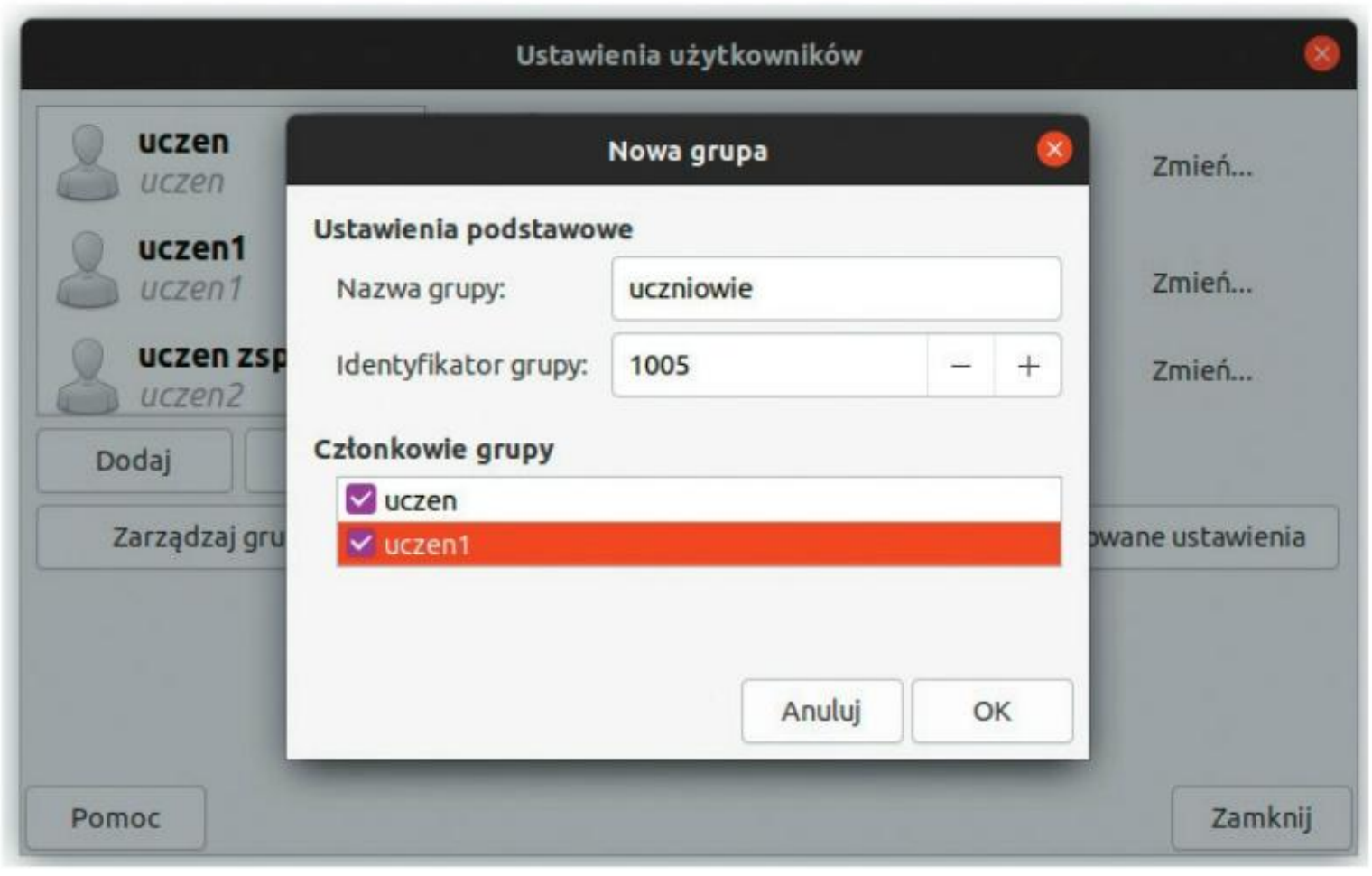
Rys. 4.9. **Wprowadzanie hasła dla dodawanego konta**

Aby uzyskać lub wprowadzić dodatkowe informacje o koncie, należy kliknąć przycisk **Zaawansowane ustawienia** (ang. *Advanced Settings*). Przykładowo, w zakładce **Zaawansowane** można odczytać lub edytować katalog domowy, powłokę logowania, grupę główną lub identyfikator użytkownika (rys. 4.10).



Rys. 4.10. **Okno edycji zaawansowanych ustawień konta użytkownika**

Aby dodać nową grupę, należy kliknąć przycisk **Zarządzaj grupami** (ang. *Manage Groups*), a następnie przycisk **Dodaj**, i określić właściwości tworzonej grupy (rys. 4.11). Można również zaznaczyć członków tej grupy.



Rys. 4.11. **Informacje o tworzonej grupie**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyświetl informacje o istniejących użytkownikach twojego komputera z systemem Linux.
2. Odszukaj identyfikator UID twojego konta.
3. Skorzystaj z konta z uprawnieniami administratora i odczytaj zawartość pliku **`/etc/shadow`**. Odszukaj swoje konto i skopiuj do notatnika zaszyfrowaną postać używanego przez ciebie hasła.
4. Tworzenie i testowanie konta nowego użytkownika:
   - Załóż konto użytkownika o nazwie *moderator*.
   - Ustal katalog domowy użytkownika: **`/home/moderator`**.
   - Ustal hasło dla nowego użytkownika (np. *zspnr1*).
   - Utwórz w trybie interaktywnym konto użytkownika *tester*.
   - Zaloguj się na konto użytkownika *moderator* i *tester*.
5. Utwórz użytkownika *Profesor* i dodaj go do grupy *root*:
   - Utwórz konto użytkownika *test* z hasłem *qwerty*. Sprawdź, czy można się na nie zalogować.
   - Dodaj użytkownika *test* do grupy *root*.
   - Za pomocą polecenia systemu Linux wyświetl listę użytkowników – członków grupy *root*.
   - Usuń konta użytkowników i grupy utworzone podczas ćwiczenia.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyświetl zawartość pliku **`/etc/group`**.
2. Jaki jest identyfikator GID grupy moderatorzy?

5 Konfigurowanie drukarki sieciowej

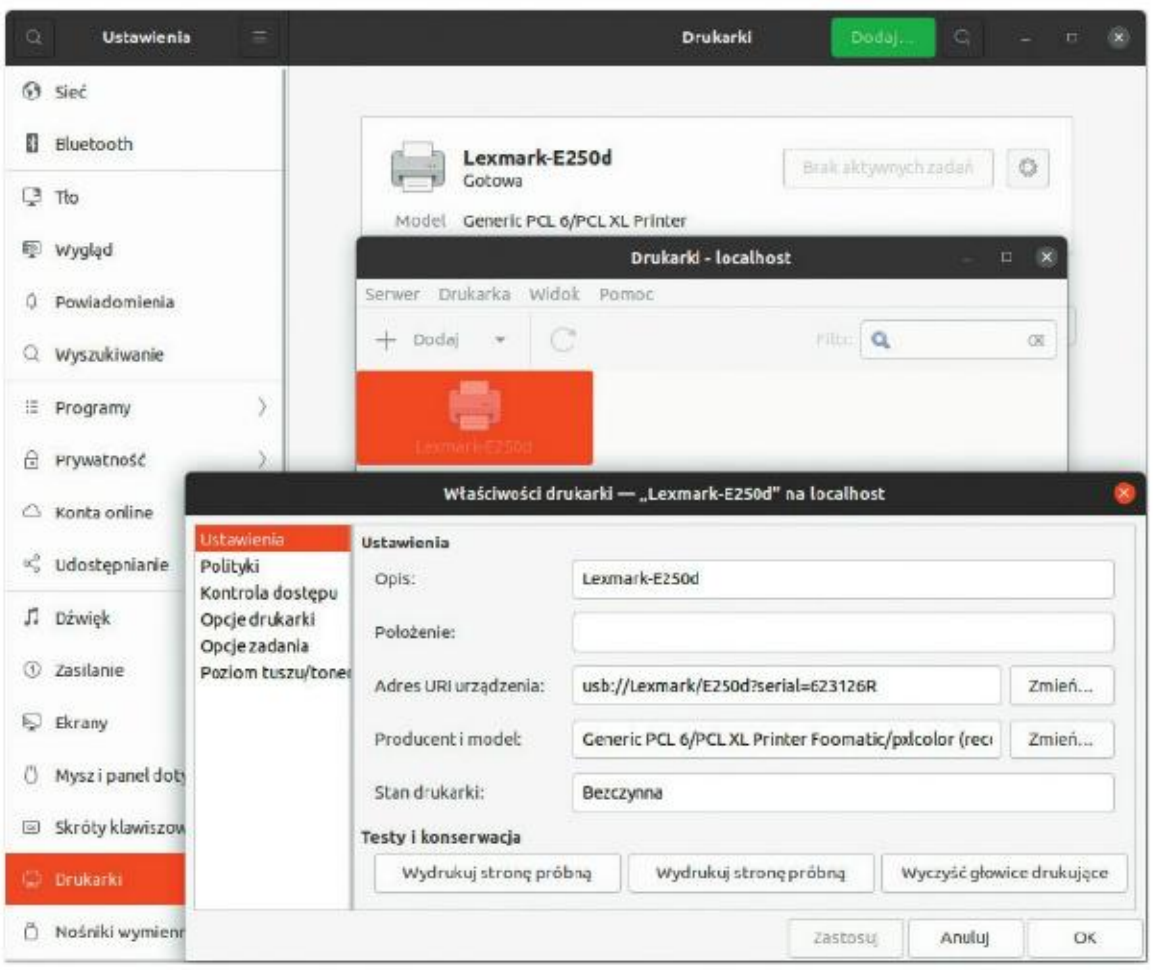
ZAGADNIENIA

Skonfigurowanie drukarki sieciowej w środowisku graficznym **Drukowanie w sieci i zarządzanie drukowaniem**

W systemie Linux drukarka może być **lokalna** – podłączona bezpośrednio do komputera lub podłączona do innego urządzenia w sieci – drukarka **sieciowa**. Konfigurację drukarki lokalnej można wykonać w środowisku graficznym za pomocą kreatora. Aby uruchomić kreatora dodawania drukarki przyłączonej bezpośrednio do komputera, należy wybrać polecenie **`Wyświetl programy/Ustawienia/Drukarki`**. Kliknięcie przycisku **`Dodaj drukarkę`**... (ang. *Add a Printer*...) uruchamia kreatora dodawania drukarki. Należy postępować zgodnie ze wskazówkami kreatora i określić dla drukarki:

- sposób podłączenia – jeżeli drukarka jest podłączona przez port USB, to może zostać automatycznie wykryta przez system;
- model drukarki i jej dodatkowe opcje, np. sterowniki;
- unikatową nazwę drukarki, opis lub położenie.

Po zainstalowaniu drukarki informacja o niej zostanie wyświetlona w oknie **`Drukarki`** (rys. 5.1). Można sprawdzić lub zmodyfikować jej działanie przez wybranie przycisku **`Dodatkowe ustawienia drukarki`**... (ang. *Additional Printer Settings*...), a następnie dwukrotne kliknięcie w ikonę drukarki. Jeżeli wydruk strony testowej przebiegnie pomyślnie, można używać polecenia drukowania z poziomu aplikacji.



Rys. 5.1. Okno konfiguracji drukarki

PRZYKŁAD 5.1

1. Zainstaluj wskazaną przez nauczyciela drukarkę lokalną.
2. Wykonaj wydruk strony testowej.

5.1. Drukowanie sieciowe i zarządzanie drukowaniem

Za drukowanie na drukarkach sieciowych jest odpowiedzialny program CUPS. Jeżeli jest aktywny, kontroluje zadania drukowania przychodzące z sieci do portu 631. Jeżeli CUPS nie jest zainstalowany, to można go zainstalować za pomocą polecenia **`sudo apt install cups`**.

uczen@uczen-VirtualBox: ~

```
uczen@uczen-VirtualBox:~$ cat /etc/cups/cupsd.conf
#
# Configuration file for the CUPS scheduler.  See "man cupsd.conf" for a
# complete description of this file.
#

# Log general information in error_log - change "warn" to "debug"
# for troubleshooting...
LogLevel warn
PageLogFormat

# Deactivate CUPS' internal logrotating, as we provide a better one, especially
# LogLevel debug2 gets usable now
MaxLogSize 0

# Only listen for connections from the local machine.
Port 631
Listen /run/cups/cups.sock

# Show shared printers on the local network.
Browsing On
BrowseLocalProtocols dnssd

# Default authentication type, when authentication is required...
DefaultAuthType Basic

# Web interface setting...
WebInterface Yes

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

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

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

# Restrict access to log files...
<Location /admin/log>
  AuthType Default
  Require user @SYSTEM
  Order allow,deny
</Location>

# Set the default printer/job policies...
<Policy default>
  # Job/subscription privacy...
  JobPrivateAccess default
  JobPrivateValues default
  SubscriptionPrivateAccess default
  SubscriptionPrivateValues default

  # Job-related operations must be done by the owner or an administrator...
  <Limit Create-Job Print-Job Print-URI Validate-Job>
    Order deny,allow
  </Limit>
```

Rys. 5.2. **Plik konfiguracyjny `/etc/cups/cupsd.conf`**

Bezpośrednio po instalacji CUPS jest skonfigurowany tylko do obsługi drukowania na drukarce lokalnej. Aby umożliwić drukowanie w sieci, należy zmodyfikować ustawienia programu. W głównym pliku konfiguracyjnym **`/etc/cups/cupsd.conf`** należy wprowadzić zmiany, tak jak na rys. 5.2:

- w sekcji **`Only listen for connections from the local machine`** – podać tylko numer portu, na którym komputer będzie nasłuchiwał przychodzące zlecenia wydruku (komputer będzie nasłuchiwał na wszystkich dostępnych adresach IP), np.:

  ```
  Port 631
  Listen /run/cups/cups.sock
  ```

- dodać możliwość przeglądania współdzielonych drukarek w sieci – w sekcji **`Show shared printers on the local network`**:

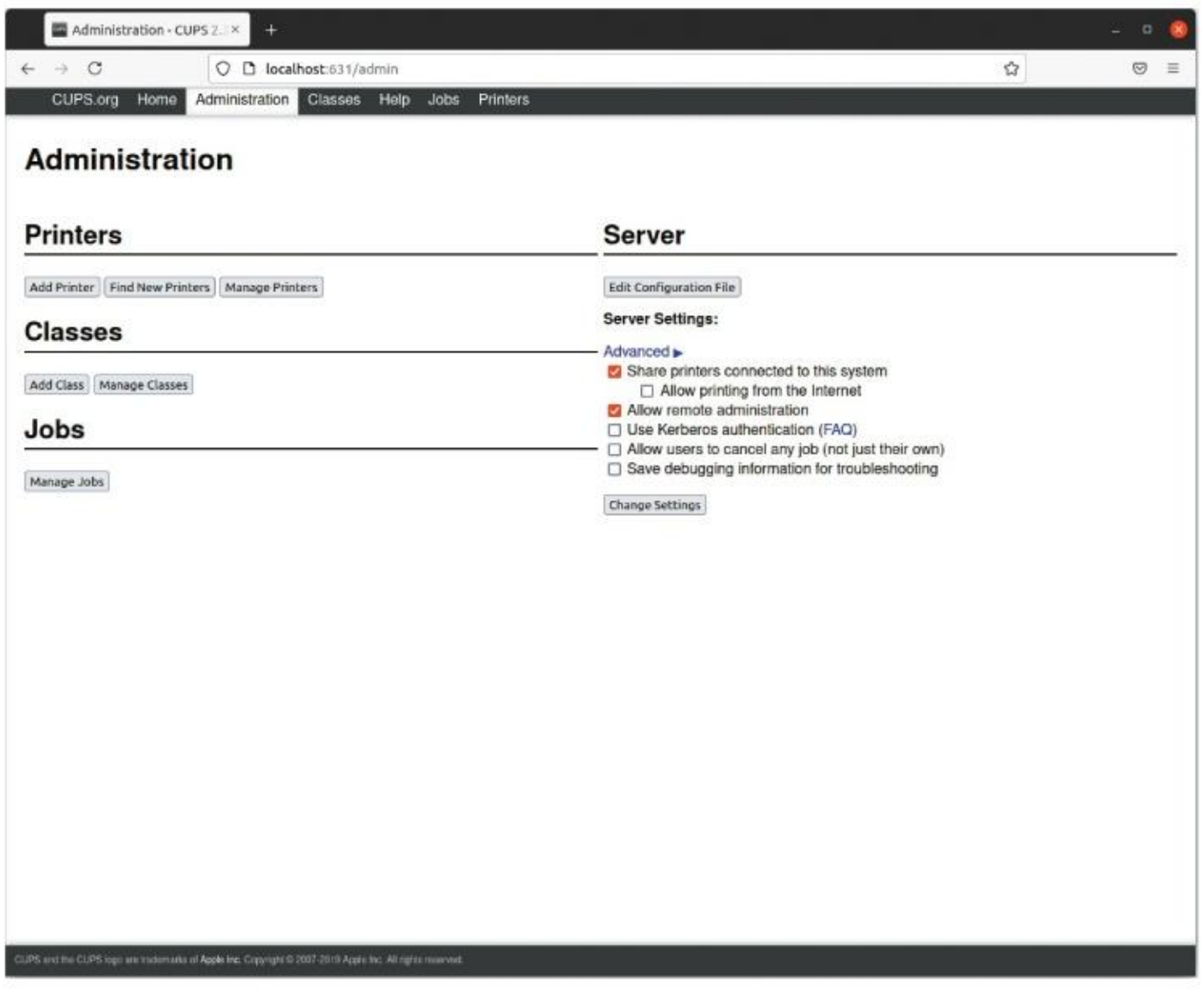
  ```
  Browsing On
  ```

- dodać możliwość dostępu z sieci lokalnej i komputera lokalnego w sekcjach **`Restrict access to the server`**, **`Restrict access to the admin pages`**, **`Restrict access to configuration files`** – dopisać opcje **`Allow localhost i Allow @LOCAL`**.

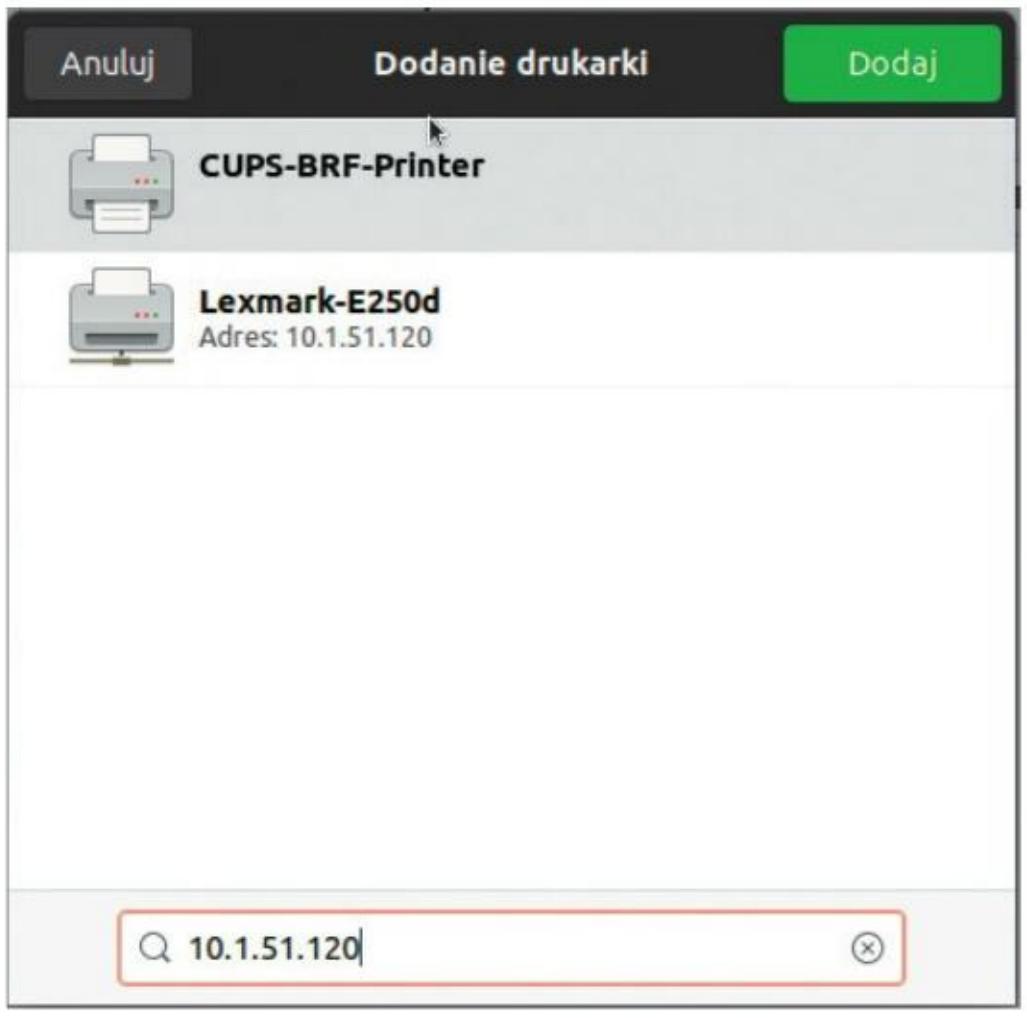
Po wprowadzeniu zmian należy ponownie uruchomić usługę, np. za pomocą polecenia:

```
sudo service cups restart
```

Do zarządzania CUPS można wykorzystać przeglądarkę internetową. W tym celu w polu adresu przeglądarki wpisuje się nazwę lub adres IP serwera wydruku i po dwukropku numer portu, np. **`localhost:631`**. W zakładce **`Administracja`** (ang. *Administration*) można udostępnić drukarkę (ang. *Share printers connected to this system*) i zezwolić na drukowanie z sieci internet (ang. *Allow printing from the Internet*) oraz na zdalne administrowanie (ang. *Allow remote administration*). Udostępniona w ten sposób drukarka będzie przyjmowała zadania od komputerów w sieci (rys. 5.3).



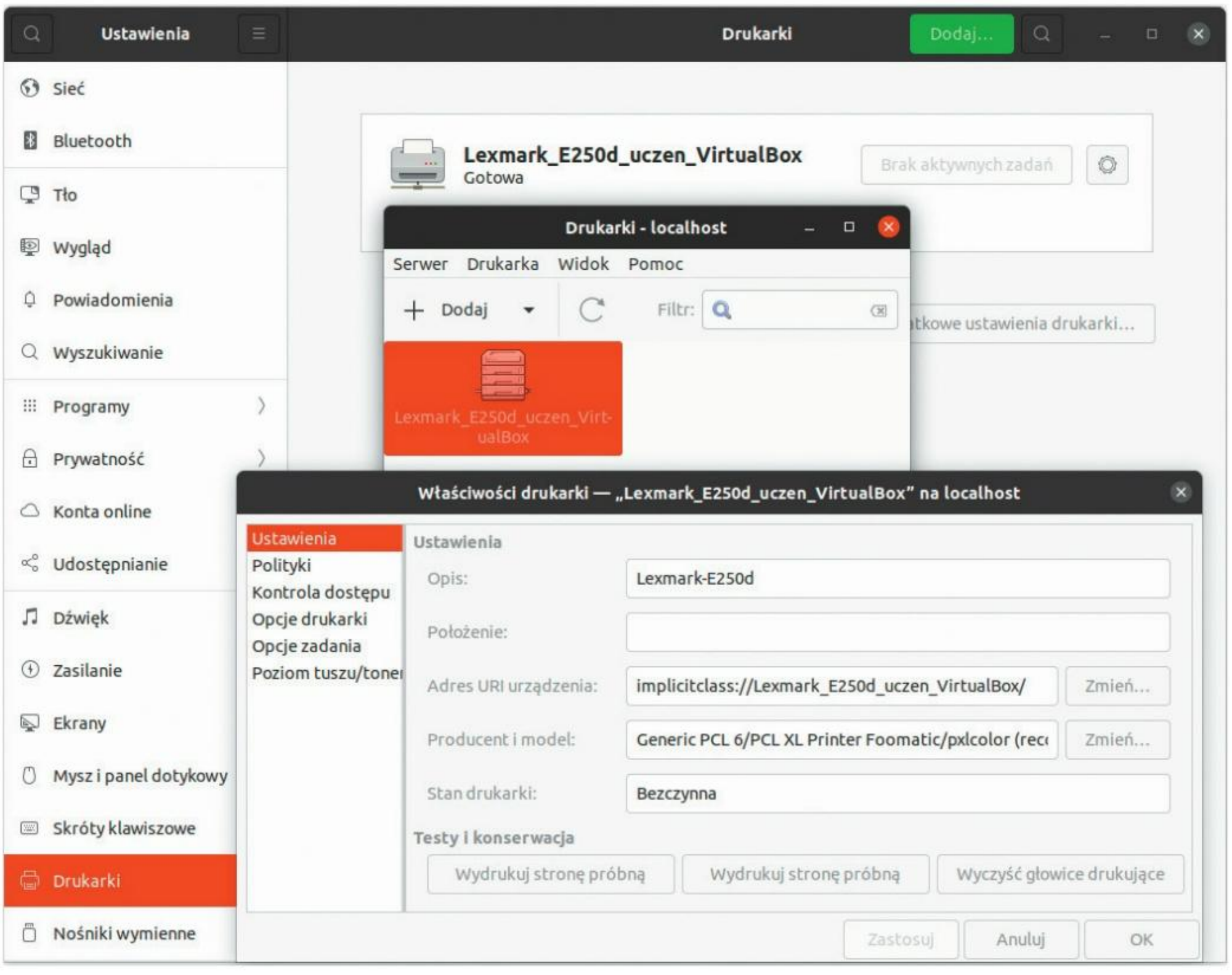
Rys. 5.3. Zarządzanie CUPS za pomocą przeglądarki internetowej



Rys. 5.4. **Dodawanie nowej drukarki sieciowej**

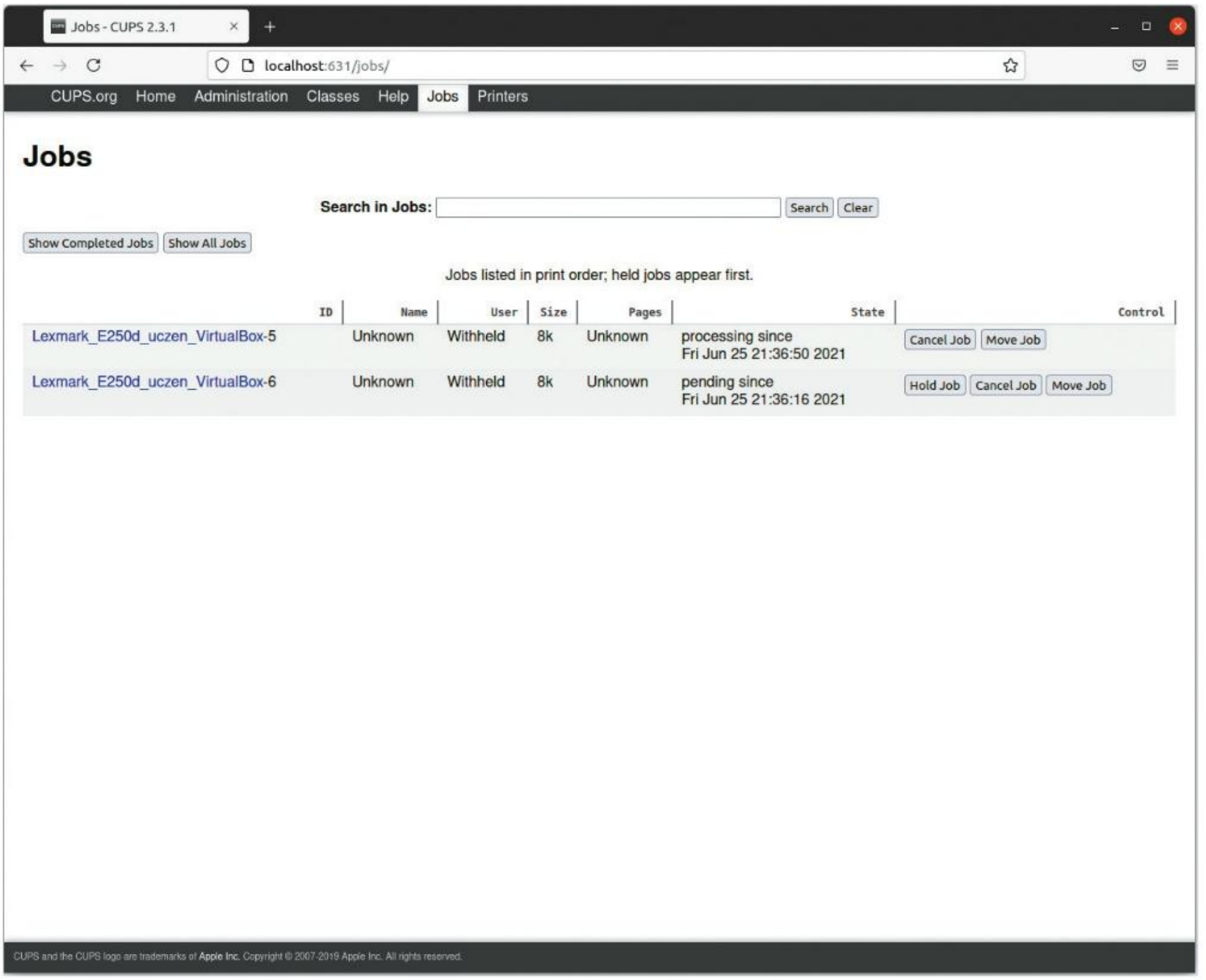
Na każdym komputerze klienckim jest konieczne skonfigurowanie **drukarki sieciowej**. System CUPS może automatycznie wykryć i zainstalować udostępnione w sieci drukarki. Aby samodzielnie rozpocząć konfigurowanie drukarki sieciowej, należy wybrać polecenie **`Wyświetl programy/Ustawienia/Drukarki`** i kliknąć przycisk **`Dodaj`** – aby uruchomić kreatora. Następnie postępować zgodnie ze wskazówkami kreatora i wskazać adres komputera, do którego jest podłączona udostępniana drukarka, np. **`10.1.51.120`** (rys. 5.4). Jeżeli drukarka zostanie wykryta, należy ją zaznaczyć i kliknąć przycisk **`Dodaj`**. Podobnie jak dla drukarki lokalnej można określić jej dodatkowe opcje, np. sterowniki, i unikatową nazwę drukarki, opis lub położenie.

Drukarka powinna zostać dodana do listy drukarek dostępnych w systemie (rys. 5.5).



Rys. 5.5. **Informacje o drukarkach zainstalowanych w systemie**

Działanie drukarki można przetestować przez wydrukowanie strony testowej. Jeżeli wydruk zakończy się powodzeniem, drukarka może być wykorzystana do drukowania z poziomu aplikacji. Jeżeli w systemie jest więcej niż jedna drukarka, warto wskazać drukarkę domyślną. Dla każdej z drukarek można dodatkowo ustawić opcje wydruku, takie jak: rozmiar papieru, skalowanie, liczba wydruków.



Rys. 5.6. Zarządzanie kolejką drukowania

Użytkownicy mający uprawnienia mogą za pośrednictwem przeglądarki internetowej przeglądać listę zadań drukowania i zarządzać drukowaniem dokumentów przez **zmianę ich kolejności** (ang. *Move Job*) lub **usuwać** (ang. *Cancel Job*) zadania druku z kolejki (rys. 5.6). Służy do tego zakładka **`Zadania`** (ang. *Jobs*) na stronie zarządzania drukarką.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Udostępnij zainstalowaną w przykładzie 5.1 drukarkę lokalną. Zainstaluj w swoim systemie drukarkę sieciową udostępnioną przez koleżankę / kolegę. Przetestuj jej działanie przez wydrukowanie strony testowej.
2. Wyłącz drukarkę. Wygeneruj trzy zadania wydruku. Za pomocą narzędzia do zarządzania wydrukami anuluj zadanie 2.
3. Zmień kolejność wykonywania zadań opisanych w punkcie 2., tak aby zadanie 3. zostało wykonane przed zadaniem 1.

6 Instalowanie pakietów

ZAGADNIENIA

Pakiety wchodzące w skład oprogramowania narzędziowego i użytkowego Zarządzanie pakietami Polecenia stosowane podczas instalacji pakietów Sposób zainstalowania pakietu za pomocą dpkg Funkcje menedżera apt Zarządzanie instalowaniem pakietów za pomocą apt Zarządzanie pakietami w środowisku graficznym

Poszczególne dystrybucje Linuksa mają różne **menedżery pakietów**, które służą do automatycznej instalacji, aktualizacji, konfiguracji i usuwania pakietów oprogramowania. Niektórych z nich można używać tylko w terminalu, inne mają interfejs graficzny. Wiele dystrybucji Linuksa jest wyposażonych w aplikację do zarządzania oprogramowaniem, np. **Ubuntu Software**. Aplikacja po uruchomieniu wymaga od użytkownika tylko wskazania pakietu, który należy zainstalować, i podania hasła administratora.

Menedżery mogą pobierać pakiety z **repozytoriów**, czyli serwerów poszczególnych dystrybucji, na których znajduje się oprogramowanie dostępne w danej dystrybucji. Dodatkową korzyścią instalowania aplikacji przez menedżer pakietów jest to, że nie trzeba sprawdzać dostępności aktualizacji poszczególnych programów – zrobi to za nas menedżer aktualizacji, który może pobrać i zainstalować wszystkie dostępne aktualizacje programów obecnych w naszym systemie.

W tabeli 6.1 przedstawiono zestawienie najpopularniejszych menedżerów pakietów.

Tabela 6.1. Zestawienie najpopularniejszych menedżerów pakietów

Nazwa	Format pakietu	System
apt, aptitude, dselect	deb	Debian, Ubuntu
yum	rpm	Fedora, SuSE, CentOS
YaST	rpm	SuSE

Ze względu na różnorodność systemów linuksowych opisanie wszystkich dystrybucji byłoby niemożliwe. Dlatego jako przykład systemu opartego na wspólnym jądrze Linuksa wybrano dystrybucję Ubuntu.

Dystrybucja Linuksa zawiera wiele różnego typu programów narzędziowych i użytkowych. Podobnie jak sam system, większość oprogramowania jest dostępna na podstawie **licencji GNU**. Istnieje jednak wiele programów dostępnych na podstawie **licencji komercyjnych**. Programy tego typu w większości przypadków zawierają fragmenty kodu chronione prawami autorskimi, w związku z tym nie mogą być rozprowadzane na podstawie licencji bezpłatnej. Aby legalnie używać takich programów, należy wykupić licencję na ich wykorzystanie.

Oprogramowanie wchodzące w skład Ubuntu i innych jego odmian podzielono na cztery kategorie zwane komponentami:

- w sekcji **main** znajdują się tylko te aplikacje, które spełniają wymagania licencyjne Ubuntu i są wspierane przez zespół projektu – to najważniejsze oprogramowanie z punktu widzenia użytkownika;
- sekcja **restricted** zawiera oprogramowanie niezbędne do pracy lub funkcjonalności systemu, opublikowane na licencji niezgodnej z wymogami Ubuntu, np. sterowniki kart graficznych;
- w sekcji **universe** znajduje się wolne oprogramowanie, tworzone przez podmioty niezależne i niewspierane przez zespół Ubuntu;
- sekcja **multiverse** zawiera oprogramowanie na licencji niezgodnej z wymogami Ubuntu i niewspierane przez zespół Ubuntu.

Celem takiego podziału jest oddzielenie od siebie aplikacji różniących się poziomem wsparcia ze strony Ubuntu i sposobem licencjonowania. Podczas instalacji systemu są instalowane tylko te programy, które wchodzą w skład jego domyślnej konfiguracji. Jeżeli podczas instalacji nie został zainstalowany program, a użytkownik chciałby z niego korzystać, można go pobrać i zainstalować w dowolnym momencie. Istnieje wiele źródeł oprogramowania, np. płyta z dystrybucją, strony WWW, witryny FTP, internetowe repozytoria (składnice) pakietów.

Dodatkowe programy mogą być instalowane w systemie Linux różnymi metodami:

- za pomocą aplikacji do zarządzania pakietami, np. Ubuntu Software;
- za pomocą poleceń w terminalu;
- ze specjalnie przygotowanych pakietów **deb**;
- z plików wykonywanych, np. **`*.run`**, **`*.sh`**.

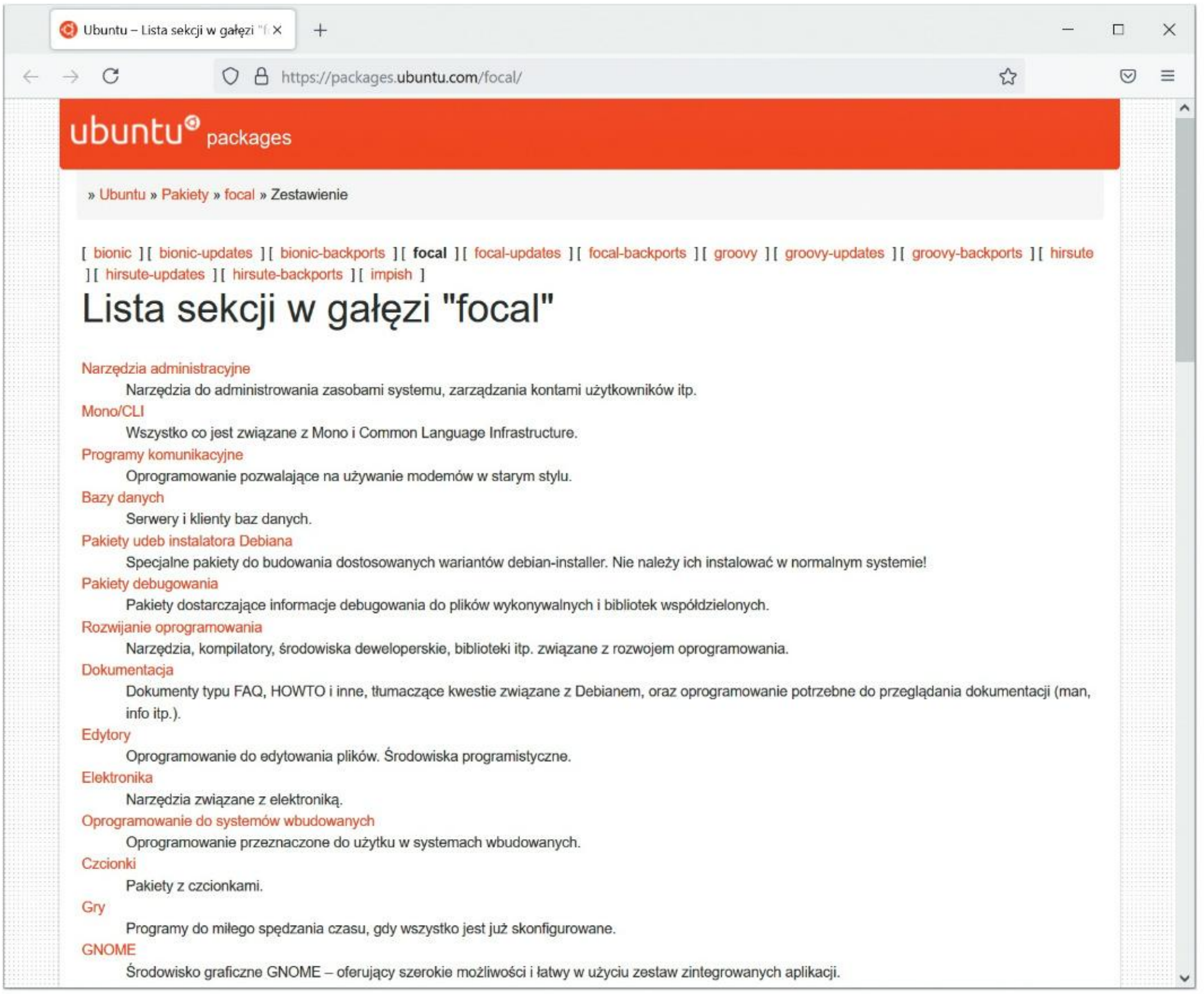
Pakiet to archiwum zawierające pliki programu i dodatkowe informacje o pakiecie oraz wymaganiach i sposobie jego instalacji. Pakiety są przygotowane w taki sposób, aby ułatwić użytkownikowi wykonanie procesu instalacji oprogramowania, a w razie potrzeby usunięcie z systemu zbędnych programów lub też ich weryfikację i naprawę. Różne dystrybucje Linuksa mają własne systemy zarządzania pakietami, np. w Fedorze i wielu innych dystrybucjach opartych na systemie RedHat jest używany menedżer pakietów **`*.rpm`**, natomiast w dystrybucjach Debian, Ubuntu i innych na nich opartych są używane pakiety w formacie **`*.deb`**.

Zarządzanie pakietami jest realizowane za pomocą programu nazywanego **Menedżerem pakietów**. Może on być przeznaczony do pracy w środowisku tekstowym, lecz istnieje wiele nakładek graficznych, które umożliwiają zarządzanie pakietami w środowisku graficznym. Oznaczenie pakietu, dla dystrybucji Debian i pochodnych, składa się z czterech elementów: nazwy pakietu, wersji pakietu, platformy sprzętowej i rozszerzenia **deb**. Przykładowo plik **`gimp_2.10.18-1_amd64.deb`** zawiera program o nazwie **`gimp`** w wersji **`2.10.18`**, przeznaczony dla komputerów z procesorem zgodnym z architekturą **`amd64`** (AMD i Intel z procesorem 64-bitowym).

6.1. Instalacja programów w środowisku tekstowym

Przed instalacją programu z pakietów **deb** należy pobrać z internetu lub innego źródła odpowiednie pakiety. Pakiety można pobierać np. ze strony https://packages.ubuntu.com/. Na stronie trzeba wybrać wersję systemu, np. **`focal`** (rys. 6.1), a następnie posłużyć się sekcjami, by odszukać i pobrać pakiet. Trzeba zwrócić szczególną uwagę na wybór wersji systemu, ponieważ pakiety przeznaczone np. dla Debiana mogą, ale nie muszą, działać poprawnie w Ubuntu lub innych dystrybucjach, mimo że wszystkie korzystają z tego samego formatu menedżera pakietów. Podobnie np. pakiet przeznaczony dla Ubuntu 20.04 może, ale nie musi, działać poprawnie w Ubuntu 18.04 lub innej wersji tej dystrybucji. Ważny jest również wybór odpowiedniej platformy sprzętowej, np. **`amd64`** dla procesorów 64-bitowych lub **`i386`** dla procesorów 32-bitowych.

> **! UWAGA**
> W Ubuntu 20.04 niektóre pakiety dostępne są tylko w wersji 64-bitowej.



Rys. 6.1. **Strona pobierania pakietów deb dla dystrybucji Ubuntu „focal"**

Większość pakietów przygotowana dla Ubuntu będzie poprawnie działała w jego różnych odmianach, np. Kubuntu, opartych na tej samej wersji. Przykładowo, do instalacji programu Gimp jest potrzebny pakiet **`gimp_2.10.18-1_amd64.deb`**. Aby pobrać ten pakiet, należy wybrać sekcję **`Grafika`** i na liście uporządkowanej alfabetycznie odszukać pakiet.

Instalacji może dokonać tylko użytkownik mający uprawnienia administratora (ang. *root*). Zarządzanie pakietami **`deb`** może być realizowane za pomocą polecenia **`dpkg`**. Najczęściej używane opcje polecenia:

- **`i`** – instalacja pakietu;
- **`r`** – usunięcie pakietu;
- **`-reconfigure`** – ponowna konfiguracja pakietu.

PRZYKŁAD 6.1

Instalowanie pakietu za pomocą dpkg

W tym przykładzie zostanie zainstalowany pakiet za pomocą menedżera **dpkg**. Menedżer jest dostępny tylko w niektórych dystrybucjach, korzystających z pakietów w formacie **deb**, np. Ubuntu. W dystrybucjach korzystających z formatu pakietów **rpm**, np. Fedora, CentOS, można zamiast niego użyć menedżera pakietów **rpm**. Jeżeli w wykorzystywanej przez ciebie dystrybucji nie jest dostępny menedżer **dpkg**, zapytaj nauczyciela, jak zainstalować pakiet.

Przed przystąpieniem do wykonania tego zadania należy sprawdzić, czy w systemie jest zainstalowany program Gimp. Jeśli tak, to należy go odinstalować lub wybrać do instalacji inny program. Aby zainstalować pakiet **deb** za pomocą polecenia **dpkg**, należy:

1. Pobrać z internetu pakiet **deb**, np. **gimp_2.10.18-1_amd64.deb**.
2. W katalogu zawierającym pakiet **deb** wydać polecenie:

   sudo dpkg -i gimp_2.8.22-1_amd64.deb

   Procedurę instalacji przedstawiono na rys. 6.2.

```
uczen@uczen-VirtualBox: ~/Pobrane
uczen@uczen-VirtualBox:~/Pobrane$ gimp

Polecenie 'gimp' nie zostało znalezione, ale można je zainstalować za pomocą:

sudo snap install gimp  # version 2.10.24, or
sudo apt  install gimp  # version 2.10.18-1

Zobacz 'snap info gimp' dla dodatkowych wersji.

uczen@uczen-VirtualBox:~/Pobrane$ ls
gimp_2.10.18-1_amd64.deb
uczen@uczen-VirtualBox:~/Pobrane$ sudo dpkg -i gimp_2.10.18-1_amd64.deb
[sudo] hasło użytkownika uczen:
Wybieranie wcześniej niewybranego pakietu gimp.
(Odczytywanie bazy danych ... 191014 plików i katalogów obecnie zainstalowanych.
)
Przygotowywanie do rozpakowania pakietu gimp_2.10.18-1_amd64.deb ...
Rozpakowywanie pakietu gimp (2.10.18-1) ...
dpkg: problemy z zależnościami uniemożliwiają skonfigurowanie pakietu gimp:
 gimp zależy od libgimp2.0 (>= 2.10.18); jednakże:
  Pakiet libgimp2.0 nie jest zainstalowany.
 gimp zależy od libgimp2.0 (<= 2.10.18-z); jednakże:
  Pakiet libgimp2.0 nie jest zainstalowany.
 gimp zależy od gimp-data (>= 2.10.18); jednakże:
  Pakiet gimp-data nie jest zainstalowany.
 gimp zależy od gimp-data (<= 2.10.18-z); jednakże:
  Pakiet gimp-data nie jest zainstalowany.
 gimp zależy od libbabl-0.1-0 (>= 0.1.10); jednakże:
  Pakiet libbabl-0.1-0 nie jest zainstalowany.
 gimp zależy od libgegl-0.4-0 (>= 0.4.22); jednakże:
  Pakiet libgegl-0.4-0 nie jest zainstalowany.
 gimp zależy od libheif1 (>= 1.4.0); jednakże:
  Pakiet libheif1 nie jest zainstalowany.
 gimp zależy od libilmbase24 (>= 2.3.0); jednakże:
  Pakiet libilmbase24 nie jest zainstalowany.
 gimp zależy od libmng2 (>= 2.0.2); jednakże:
  Pakiet libmng2 nie jest zainstalowany.
 gimp zależy od libmypaint-1.5-1 (>= 1.5.0); jednakże:
  Pakiet libmypaint-1.5-1 nie jest zainstalowany.
 gimp zależy od libopenexr24 (>= 2.3.0); jednakże:
  Pakiet libopenexr24 nie jest zainstalowany.

dpkg: błąd przetwarzania pakietu gimp (--install):
 problemy z zależnościami - pozostawianie nieskonfigurowanego
Przetwarzanie wyzwalaczy pakietu gnome-menus (3.36.0-1ubuntu1)...
Przetwarzanie wyzwalaczy pakietu desktop-file-utils (0.24-1ubuntu3)...
Przetwarzanie wyzwalaczy pakietu mime-support (3.64ubuntu1)...
Przetwarzanie wyzwalaczy pakietu man-db (2.9.1-1)...
Wystąpiły błędy podczas przetwarzania:
 gimp
uczen@uczen-VirtualBox:~/Pobrane$
```

Rys. 6.2. **Procedura instalacji programu z pakietu deb**

3. Jeżeli do poprawnego działania programu są wymagane inne składniki, np. biblioteki, to podczas sprawdzania zależności menedżer wyświetli odpowiednie komunikaty. W takim przypadku trzeba zainstalować najpierw wszystkie niezbędne składniki, a dopiero później program. Przykładowo, program Gimp wymaga do pracy dodatkowych składników. Jeżeli zależności nie zostaną spełnione, instalacja programu będzie możliwa, ale program nie będzie działał poprawnie lub się nie uruchomi.
4. Aby rozwiązać problemy z zależnościami, można użyć polecenia:

   `sudo apt install -f`

   Po wydaniu tego polecenia menedżer sprawdzi i naprawi wszystkie zależności i program będzie można uruchomić (rys. 6.3).

```
uczen@uczen-VirtualBox: ~/Pobrane
uczen@uczen-VirtualBox:~/Pobrane$ sudo apt install -f
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Naprawianie zależności... Gotowe
The following additional packages will be installed:
  gimp-data i965-va-driver intel-media-va-driver libaacs0 libamd2 libaom0
  libavcodec58 libavformat58 libavutil56 libbabl-0.1-0 libbdplus0 libblas3
  libbluray2 libcamd2 libccolamd2 libcholmod3 libchromaprint1 libcodec2-0.9
  libde265-0 libgegl-0.4-0 libgegl-common libgfortran5 libgimp2.0 libgme0
  libgsm1 libheif1 libigdgmm11 libilmbase24 liblapack3 libmetis5 libmng2
  libmypaint-1.5-1 libmypaint-common libopenexr24 libopenmpt0 libquadmath0
  libsdl2-2.0-0 libshine3 libsnappy1v5 libssh-gcrypt-4 libswresample3
  libswscale5 libumfpack5 libva-drm2 libva-x11-2 libva2 libvdpau1 libx264-155
  libx265-179 libxvidcore4 libzvbi-common libzvbi0 mesa-va-drivers
  mesa-vdpau-drivers ocl-icd-libopencl1 va-driver-all vdpau-driver-all
Sugerowane pakiety:
  i965-va-driver-shaders libbluray-bdj opencl-icd libvdpau-va-gl1
  nvidia-vdpau-driver nvidia-legacy-340xx-vdpau-driver
  nvidia-legacy-304xx-vdpau-driver
Zostaną zainstalowane następujące NOWE pakiety:
  gimp-data i965-va-driver intel-media-va-driver libaacs0 libamd2 libaom0
  libavcodec58 libavformat58 libavutil56 libbabl-0.1-0 libbdplus0 libblas3
  libbluray2 libcamd2 libccolamd2 libcholmod3 libchromaprint1 libcodec2-0.9
  libde265-0 libgegl-0.4-0 libgegl-common libgfortran5 libgimp2.0 libgme0
  libgsm1 libheif1 libigdgmm11 libilmbase24 liblapack3 libmetis5 libmng2
  libmypaint-1.5-1 libmypaint-common libopenexr24 libopenmpt0 libquadmath0
  libsdl2-2.0-0 libshine3 libsnappy1v5 libssh-gcrypt-4 libswresample3
  libswscale5 libumfpack5 libva-drm2 libva-x11-2 libva2 libvdpau1 libx264-155
  libx265-179 libxvidcore4 libzvbi-common libzvbi0 mesa-va-drivers
  mesa-vdpau-drivers ocl-icd-libopencl1 va-driver-all vdpau-driver-all
0 aktualizowanych, 57 nowo instalowanych, 0 usuwanych i 93 nieaktualizowanych.
1 nie w pełni zainstalowanych lub usuniętych.
Konieczne pobranie 42,3 MB archiwów.
Po tej operacji zostanie dodatkowo użyte 232 MB miejsca na dysku.
Kontynuować? [T/n] t
Pobieranie:1 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libbabl-0.1-0 amd64 0.1.74-1 [272 kB]
Pobieranie:2 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libaom0 amd64 1.0.0.errata1-3build1 [1 160 kB]
Pobieranie:3 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libva2 amd64 2.7.0-2 [53,5 kB]
Pobieranie:4 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libva-drm2 amd64 2.7.0-2 [7 044 B]
Pobieranie:5 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libva-x11-2 amd64 2.7.0-2 [11,9 kB]
Pobieranie:6 http://pl.archive.ubuntu.com/ubuntu focal/main amd64 libvdpau1 amd64 1.3-1ubuntu2 [25,6 kB]
Pobieranie:7 http://pl.archive.ubuntu.com/ubuntu focal/main amd64 ocl-icd-libopencl1 amd64 2.2.11-1ubuntu1 [30,3 kB]
Pobieranie:8 http://pl.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libavutil56 amd64 7:4.2.4-1ubuntu0.1 [241 kB]
Pobieranie:9 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libcodec2-0.9 amd64 0.9.2-2 [7 886 kB]
Pobieranie:10 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libgsm1 amd64 1.0.18-2 [24,4 kB]
Pobieranie:11 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libshine3 amd64 3.1.1-2 [23,2 kB]
Pobieranie:12 http://pl.archive.ubuntu.com/ubuntu focal/main amd64 libsnappy1v5 amd64 1.1.8-1build1 [16,7 kB]
Pobieranie:13 http://pl.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libswresample3 amd64 7:4.2.4-1ubuntu0.1 [57,1 kB]
Pobieranie:14 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libx264-155 amd64 2:0.155.2917+git0a84d98-2 [521 kB]
Pobieranie:15 http://pl.archive.ubuntu.com/ubuntu focal/universe amd64 libx265-179 amd64 3.2.1-1build1 [1 060 kB]
```

Rys. 6.3. **Procedura naprawy zależności między pakietami**

! UWAGA

Jeżeli w twoim systemie nie jest dostępny menedżer **`dpkg`**, skorzystaj z innego menedżera, dostępnego w twojej dystrybucji, pracującego w terminalu.

6.2. Konfiguracja menedżera apt

W dystrybucji Debian, Ubuntu i wielu innych opierających się na nich jest wykorzystywany system zarządzania pakietami i instalowania ich o nazwie **APT** (ang. *Advanced Packaging Tool*), który automatycznie zarządza zależnościami między pakietami. APT korzysta z repozytoriów pakietów zlokalizowanych w internecie. Może on automatycznie pobrać i zainstalować wszystkie pakiety niezbędne do spełnienia zależności. Do części swoich operacji APT używa pliku zawierającego listę źródeł, z których mogą być pobierane pakiety. Lista jest przechowywana w pliku **`/etc/apt/sources.list`**. Wpisy w tym pliku mają następujący format:

```
deb http://witryna.http.org/debian dystrybucja sekcja1 sekcja2
sekcja3

deb-src http://witryna.http.org/debian dystrybucja sekcja1 sekcja2
sekcja3
```

Pierwszym słowem w każdej linii jest **`deb`** lub **`deb-src`**, wskazujące typ archiwum. **`Deb`** oznacza skompilowane pakiety binarne, **`deb-src`** zawiera pakiety źródłowe, którymi są oryginalne źródła programów wraz z plikiem zawierającym opis (**`.dsc`**) i plikiem przechowującym zmiany potrzebne do zbudowania programu (**`.diff.gz`**). Przykładowy plik **`sources.list`** przedstawiono na rys. 6.4. W tym pliku można dodawać lub usuwać wpisy dotyczące poszczególnych repozytoriów, np. użytkownik może usunąć z pliku repozytoria, z których nie będzie korzystał. Po wprowadzeniu zmian w pliku **`/etc/apt/sources.list`** należy wydać polecenie **`apt update`**, aby **`APT`** pobrał listy dostępnych pakietów ze źródeł wymienionych w tym pliku.

Plik **`/etc/apt/sources.list`** może zawierać kilka typów linii. APT korzysta z archiwów typu: HTTP, FTP, file (lokalne pliki, np. katalog zawierający zamontowany system plików ISO9660) i ssh.

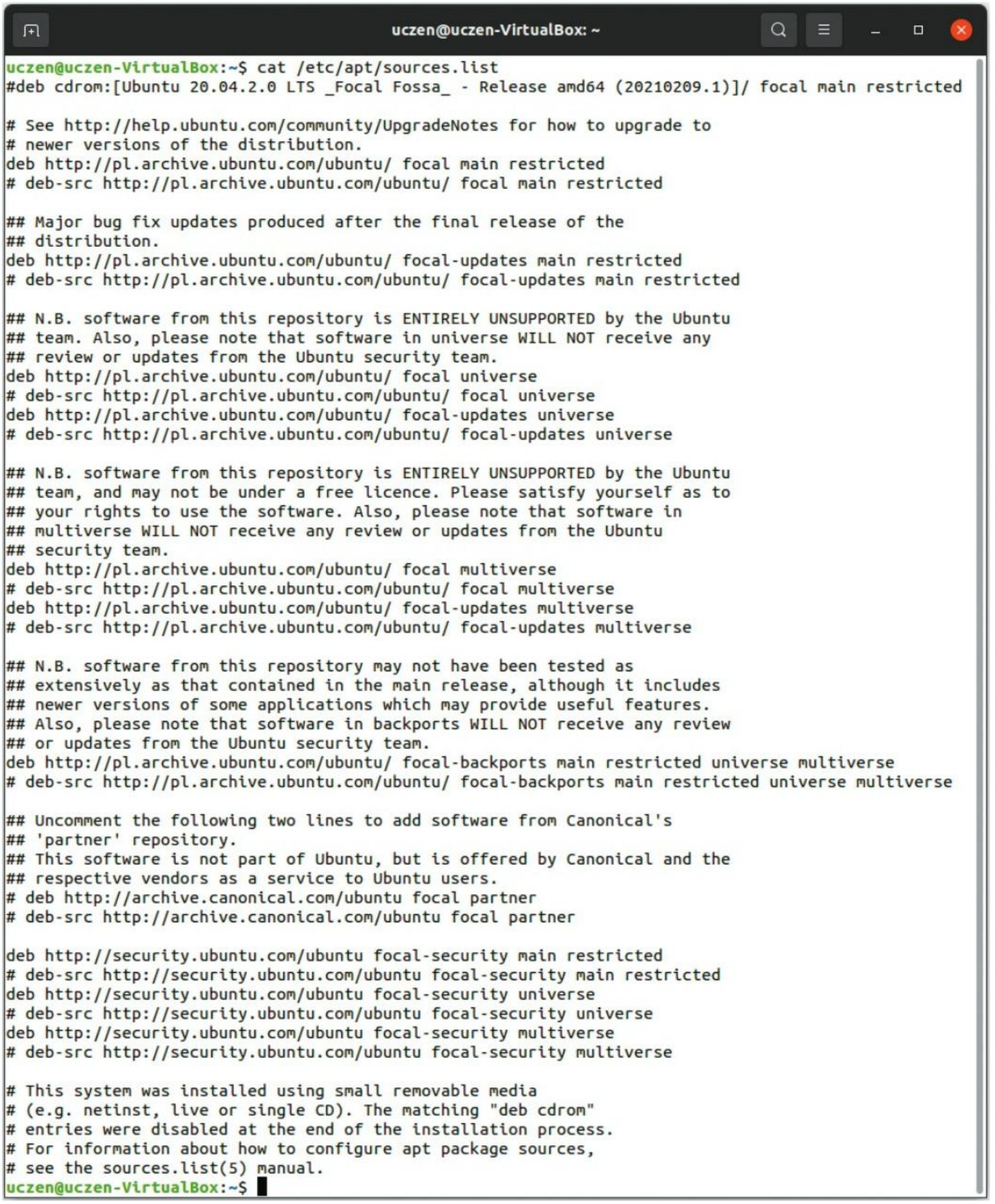
W pliku **`sources.list`** można za pomocą programu **`apt-cdrom`** umieścić repozytorium zlokalizowane na CD. W tym celu należy umieścić w napędzie CD-ROM płytę z pakietami **`deb`** i wydać polecenie: **`sudo apt-cdrom add`** (rys. 6.5).

Podane polecenie zamontuje napęd i poszuka na płycie informacji na temat pakietów. Płyta zostanie jednoznacznie zidentyfikowana i dopisana do listy repozytoriów (rys. 6.6).

Do zarządzania pakietami wykorzystuje się polecenie **`apt`**. Najczęściej używane opcje polecenia:

- **`apt update`** – pobranie najnowszych informacji o pakietach (niezbędne, by instalować najnowsze pakiety);
- **`apt upgrade`** – aktualizacja wszystkich pakietów;
- **`apt install nazwa_pakietu`** – instalacja pakietu wraz z zależnościami;
- **`apt remove nazwa_pakietu`** – usuwanie pakietu.

Za pomocą **`apt install`** można jednocześnie instalować wiele pakietów. W tym celu należy wpisać listę pakietów do instalacji (nazwy pakietów oddzielone spacją).



Rys. 6.4. Przykładowy plik `sources.list`

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ sudo apt-cdrom add
Użycie /media/uczen/Ubuntu 20.04.2.0 LTS amd64/ jako punktu montowania CD-ROM-u
Identyfikacja... [89d9609b12357e619b542fa7206b0899-2]
Skanowanie płyty w poszukiwaniu plików indeksu...
Znaleziono 4 indeksów pakietów, 0 indeksów źródłowych, 0 indeksów tłumaczeń i 1 podpisów
Płyta nosi nazwę:
"Ubuntu 20.04.2.0 LTS _Focal Fossa_ - Release amd64 (20210209.1)"
Kopiowanie list pakietów...gpgv: Podpisano w wto, 9 lut 2021, 20:06:19 CET
gpgv:                przy użyciu klucza RSA 843938DF228D22F7B3742BC0D94AA3F0EFE21092
gpgv: Poprawny podpis złożony przez ,,Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.c
om>''
Reading Package Indexes... Gotowe
Zapisywanie nowej listy źródeł
Źródła dla tej płyty to:
deb cdrom:[Ubuntu 20.04.2.0 LTS _Focal Fossa_ - Release amd64 (20210209.1)]/ focal main restricted
Należy powtórzyć ten proces dla reszty płyt.
uczen@uczen-VirtualBox:~$
```

Rys. 6.5. **Dołączanie CD do listy repozytoriów**

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/apt/sources.list
#deb cdrom:[Ubuntu 20.04.2.0 LTS _Focal Fossa_ - Release amd64 (20210209.1)]/ focal main restricted

# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb cdrom:[Ubuntu 20.04.2.0 LTS _Focal Fossa_ - Release amd64 (20210209.1)]/ focal main restricted
deb cdrom:[Linux Mint 18.3 _Sylvia_ - Release amd64 20171124]/ xenial contrib main non-free
deb http://pl.archive.ubuntu.com/ubuntu/ focal main restricted
# deb-src http://pl.archive.ubuntu.com/ubuntu/ focal main restricted

## Major bug fix updates produced after the final release of the
## distribution.
deb http://pl.archive.ubuntu.com/ubuntu/ focal-updates main restricted
# deb-src http://pl.archive.ubuntu.com/ubuntu/ focal-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://pl.archive.ubuntu.com/ubuntu/ focal universe
# deb-src http://pl.archive.ubuntu.com/ubuntu/ focal universe
deb http://pl.archive.ubuntu.com/ubuntu/ focal-updates universe
# deb-src http://pl.archive.ubuntu.com/ubuntu/ focal-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
```

Rys. 6.6. **Plik `sources.list` z dołączonym repozytorium na CD**

PRZYKŁAD 6.2

Zarządzanie pakietami za pomocą menedżera `apt`

Aby zainstalować pakiet **`nmap`** za pomocą menedżera **`apt`** i repozytorium w internecie, należy:

1. Zalogować się na konto użytkownika.
2. Sprawdzić poprawność połączenia z internetem. W przypadku braku połączenia należy je poprawnie skonfigurować.
3. Wpisać polecenie:

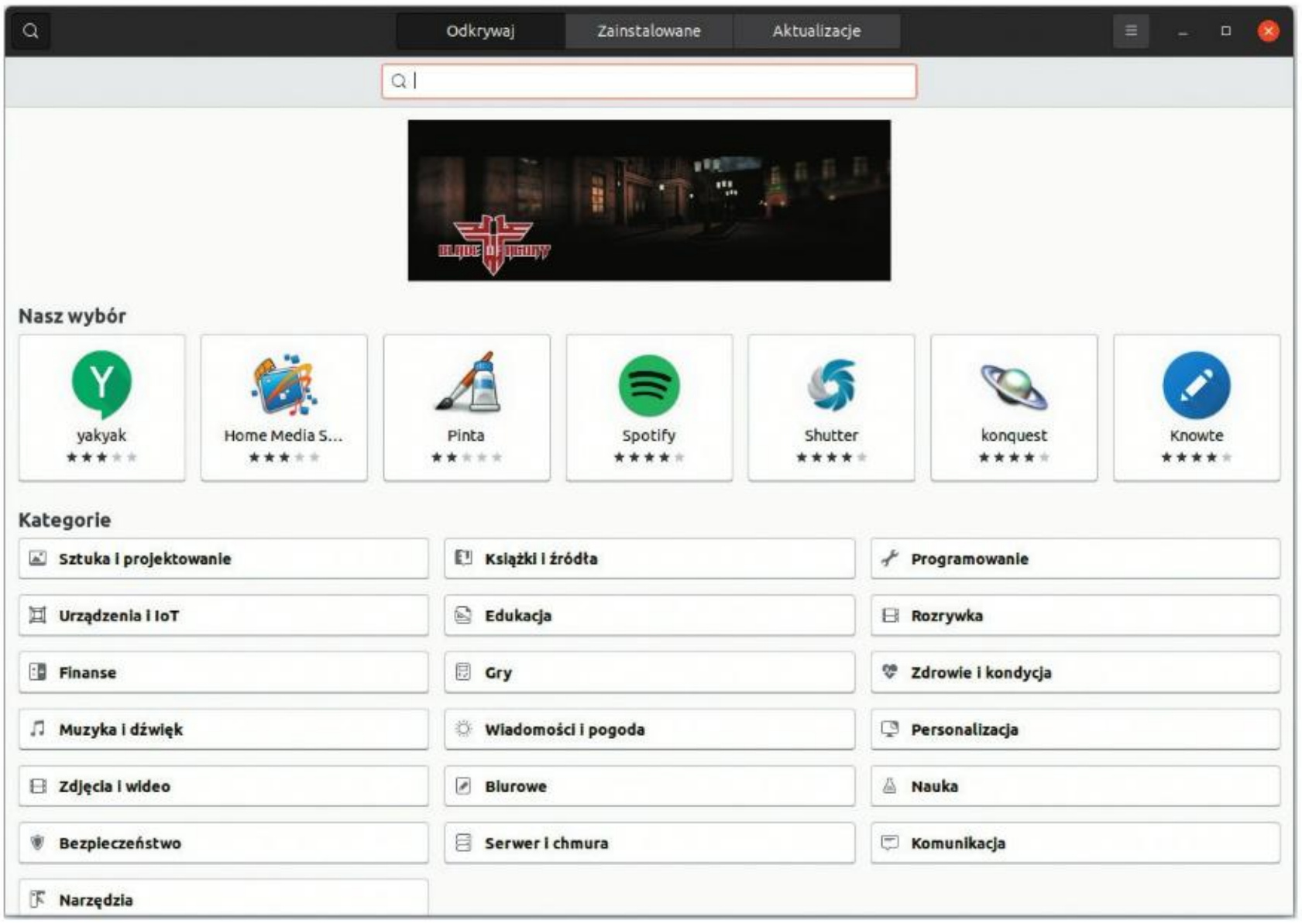
```
sudo apt install nmap
```

4. Po wykonaniu analizy instalacji i wyświetleniu podsumowania transakcji przez system potwierdzić realizację zadania.
5. Sprawdzić działanie programu za pomocą polecenia:

   `nmap localhost`
6. Odinstalować program za pomocą polecenia:

   `sudo apt remove nmap`

W środowisku graficznym można również zarządzać pakietami za pomocą aplikacji **Ubuntu Software**. Aby ją uruchomić, należy wybrać polecenie **`Wyświetl programy`** i w polu wyszukiwania wpisać **`Ubuntu Software`**, a następnie kliknąć ikonę **`Ubuntu Software`** (rys. 6.7).



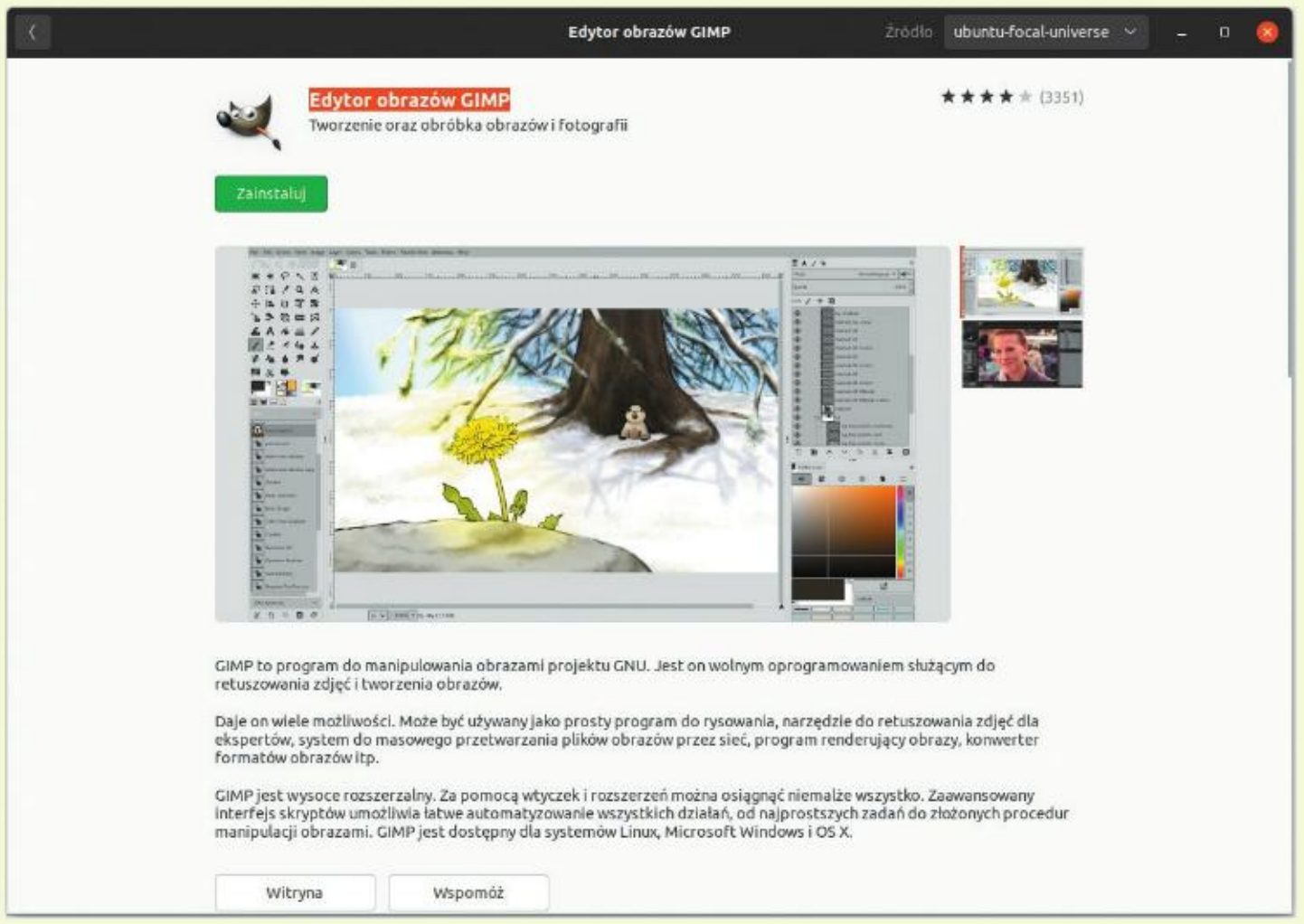
Rys. 6.7. **Menedżer pakietów w środowisku graficznym**

PRZYKŁAD 6.3

Zarządzanie pakietami za pomocą aplikacji Ubuntu Software

Aby zainstalować pakiet **`Gimp`** za pomocą z aplikacji **`Ubuntu Software`**, należy:

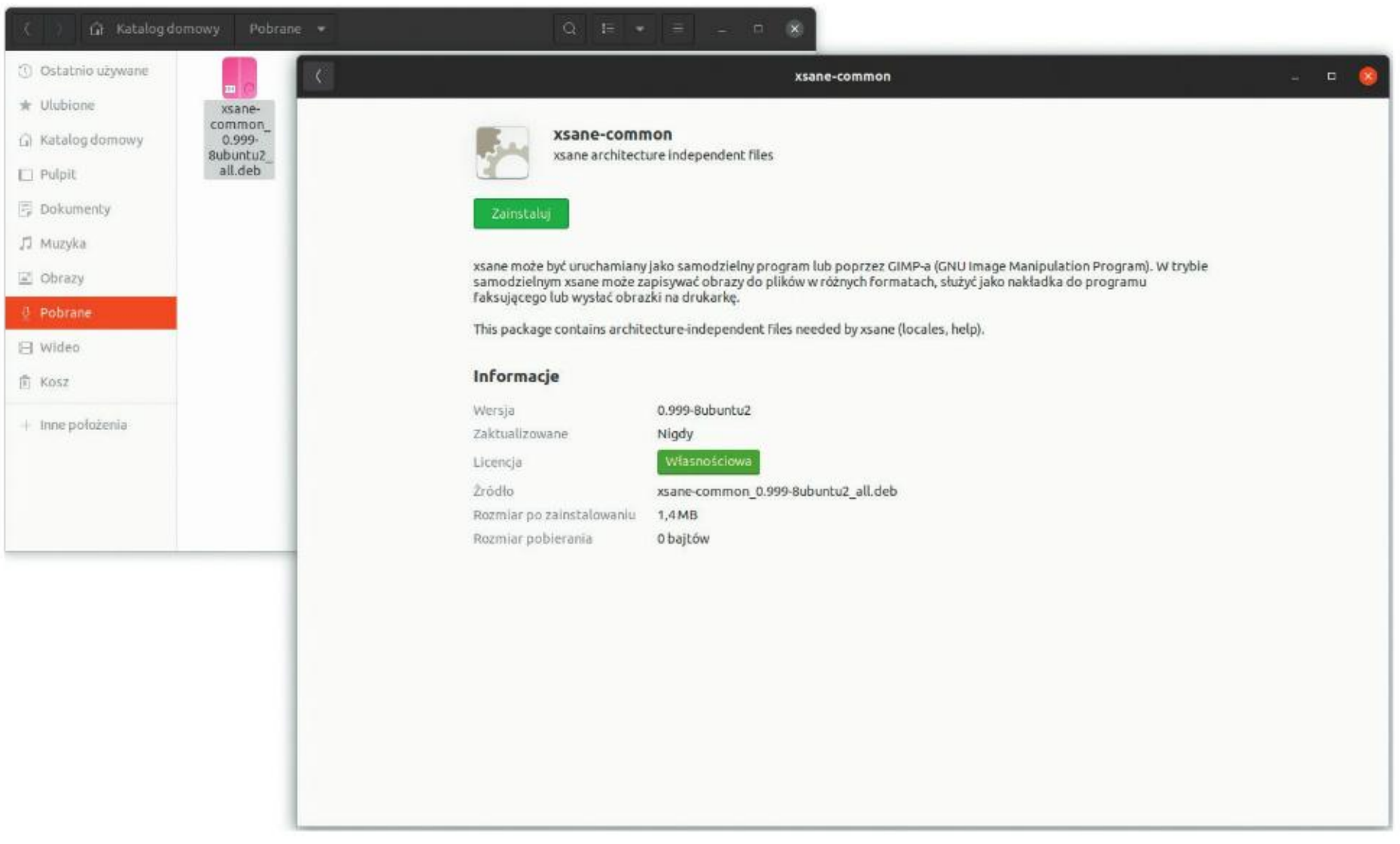
1. Zalogować się na konto użytkownika.
2. W środowisku graficznym wybrać polecenie **`Wyświetl programy`** i w polu wyszukiwania wpisać **`Ubuntu Software`**, a następnie kliknąć ikonę **`Ubuntu Software`**.
3. Odszukać pakiet **`Gimp`** lub w pole wyszukiwania wpisać nazwę pakietu.
4. Kliknąć ikonę pakietu, a następnie przycisk **`Zainstaluj`** (rys. 6.8). Wprowadzić hasło użytkownika z uprawnieniami, jeżeli system tego zażąda.
5. Uruchomić program, aby sprawdzić poprawność instalacji.
6. Odinstalować pakiet **`Gimp`**.



Rys. 6.8. **Wybór pakietu do instalacji**

7. Odszukać pakiet **Gimp**, np. w zakładce **Zainstalowane** lub w pole wyszukiwania wpisać nazwę pakietu.
8. Kliknąć ikonę pakietu, a następnie przycisk **Usuń**. Wprowadzić hasło użytkownika z uprawnieniami, jeżeli system tego zażąda.

W środowisku graficznym można również instalować pakiety **deb**. Po pobraniu wystarczy kliknąć ikonę pakietu, aby uruchomić **Instalator pakietu** (rys. 6.9). Po kliknięciu przycisku **Zainstaluj** rozpocznie się proces instalacji pakietu i w razie konieczności również pobieranie i instalacja wszystkich zależności.



Rys. 6.9. **Okno programu Instalator pakietu**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

W systemie Linux często jest używany menedżer pakietów **apt**.

1. Wyszukaj w internecie najnowsze pakiety instalacyjne programu przeznaczone dla różnych dystrybucji Linuksa, np. Fedora, CentOS (pakiety w formacie rpm), Ubuntu i Debian (pakiety w formacie deb), zarówno w wersji 32-, jak i 64-bitowej.
2. Wyszukaj w internecie pakiety zawierające kody źródłowe programu **apt**.
3. Porównaj rozmiar pakietów binarnych (w formacie **rpm** i **deb**). Który jest większy?
4. Znajdź w internecie informacje o nazwie menedżera pakietów używanego przez dystrybucję Slackware.
5. Odszukaj w internecie pakiet instalacyjny programu **nmap** przeznaczony dla używanej przez ciebie dystrybucji i wersji Linuksa. Pobierz pakiet i za pomocą menedżera **dpkg** lub innego dostępnego w twojej dystrybucji zainstaluj go. Przetestuj działanie programu, wydając polecenie **nmap localhost**.
6. Jeżeli program działa poprawnie (zostanie wyświetlona lista otwartych portów komputera), odinstaluj program.
7. Za pomocą menedżera **dpkg** zainstaluj program Gimp, korzystając z pakietu **deb**. Jeżeli podczas instalacji zostanie wyświetlony komunikat o braku biblioteki, to należy po instalacji pakietu wykonać naprawę zależności między pakietami. Uruchomić program Gimp.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Do czego służy Menedżer pakietów?
2. Co to jest repozytorium pakietów i jak uzyskać do niego dostęp?
3. Podaj zalety i wady menedżerów **apt** i **dpkg**.
4. W starszych dystrybucjach Ubuntu używano polecenia **apt-get**. Wyszukaj w internecie informacje o różnicach między **apt-get** i **apt**.
5. Czy w Ubuntu istnieje możliwość wykorzystania kilku menedżerów pakietów jednocześnie? Odpowiedź uzasadnij. Zweryfikuj odpowiedź – podejmij próbę jednoczesnego uruchomienia dwóch menedżerów pakietów.

- Uruchamianie usług sieciowych
- Przygotowanie do pracy serwera telnet
- Przygotowanie do pracy serwera SSH
- Przygotowanie do pracy serwera DHCP
- Przygotowanie do pracy serwera DNS
- Uruchomienie i korzystanie z usługi FTP
- Konfiguracja serwera poczty elektronicznej
- Uruchamianie usługi WWW
- Automatyczne uruchamianie zadań
- Zarządzanie logiczną strukturą dysku
- Przydziały dyskowe użytkowników
- Przydziały dyskowe grupy użytkowników
- Udostępnianie zasobów systemu Linux klientom MS Windows

Usługi sieciowe w systemie Linux

III

7 Uruchamianie usług sieciowych

ZAGADNIENIA

Demony i superdemony **Program Nmap** **Zainstalowanie i uruchomienie programu Nmap** **Funkcje zapory sieciowej** **Skonfigurowanie Firewall w systemie Linux** **Tworzenie i dodawanie reguł za pomocą aplikacji gufw**

Usługi, czyli serwisy systemowe, w Linuksie to programy uruchamiane w celu wykonania pewnych czynności. Programy świadczące usługi mogą być uruchomione przez cały czas pracy systemu. Programy pracujące w tle i nieprzyłączone do terminalu nazywa się demonami. **Demon** zajmuje miejsce w pamięci komputera nawet wtedy, gdy tylko oczekuje na zadania. **Superdemon**, np. **`xinetd`**, to narzędzie kontrolujące wybrane porty i uruchamiające usługi tylko w razie potrzeby. Przykładowo, demona **`sshd`** można uruchomić jako osobny proces (ang. *standalone*). Będzie on pracował jako demon i pozostanie aktywny przez cały czas, nawet gdy nie będzie prób nawiązania połączenia. Można też uruchomić **`sshd`** pod kontrolą superdemona **`xinetd`** i wówczas superdemon będzie kontrolował port 22, a gdy napłynie wywołanie – samoczynnie uruchomi nieaktywnego dotychczas demona **`sshd`**.

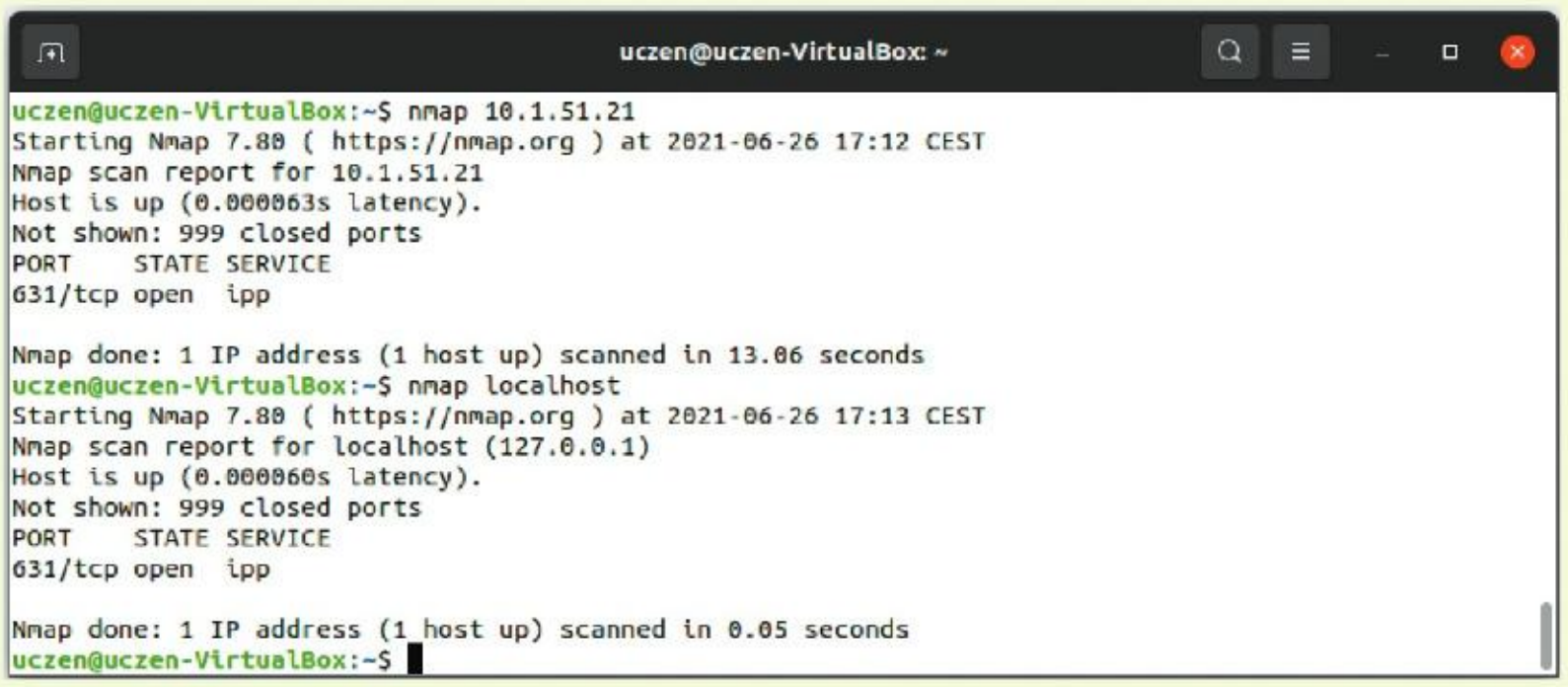
Z usługami są związane określone porty. Jeżeli port związany z daną usługą jest otwarty, może to świadczyć o tym, że usługa jest aktywna i oczekuje na klientów. Listę otwartych portów na komputerze można uzyskać za pomocą programu Nmap.

PRZYKŁAD 7.1

Instalacja i uruchomienie programu Nmap

Aby wyświetlić wykaz portów otwartych na komputerze (rys. 7.1), należy:

1. Jeżeli pakiet **`Nmap`** nie jest zainstalowany, to go zainstalować, np. za pomocą polecenia **`sudo apt install nmap`**.
2. Wpisać polecenie **`nmap nazwa/IP`**, np. **`nmap 10.1.51.21`** lub **`nmap localhost`**.



Rys. 7.1. **Lista otwartych portów komputera**

Jak widać na rys 7.1, standardowo w Linuksie jest otwarty port 631 protokołu TCP, na którym nasłuchuje usługa CUPS.

7.1. Konfigurowanie Firewall w systemie Linux

Dostęp do komputera lub sieci można ograniczyć za pomocą **zapory sieciowej** (ang. *Firewall*). Realizuje ona funkcję filtrowania krążących w sieci pakietów danych. Zależnie od sposobu konfiguracji może zabezpieczać pojedynczy komputer, serwer albo całą sieć (np. jeżeli jest skonfigurowany na routerze). Przez komputer w sieci mogą przepływać trzy typy strumieni danych: **wejściowy** (ang. INPUT), **wyjściowy** (ang. OUTPUT), **przekazywany** (ang. FORWARD). Kierunek strumienia jest określany z punktu widzenia komputera, np. strumień wejściowy to te dane, które są adresowane do komputera, strumień wyjściowy – dane, których źródłem jest komputer. Strumień przekazywany to te dane, które przepływają przez komputer, ale komputer nie jest ani ich źródłem, ani miejscem docelowym.

Większość dystrybucji Linuksa (również Ubuntu) ma zainstalowaną zaporę **iptables**. Iptables jest wyposażony w oddzielny łańcuch reguł dla każdego typu strumienia. Wykorzystując reguły, firewall podejmuje decyzję, czy pakiet **przepuścić** (ang. *allow*), **zablokować** (ang. *deny, reject*), czy też podjąć inne działanie (ang. *limit*). Blokowanie ruchu może wysyłać informację o odrzuceniu pakietu do nadawcy (ang. *reject*) lub tylko odrzucać pakiet bez powiadomienia (ang. *deny*). Reguły firewalla można edytować za pomocą klawiatury, ale wygodniej korzysta się z nakładki graficznej, ułatwiającej tworzenie reguł. Przykładem nakładki graficznej na iptables jest **gufw**. Aby ją zainstalować, należy wydać polecenie:

```
sudo apt install gufw
```

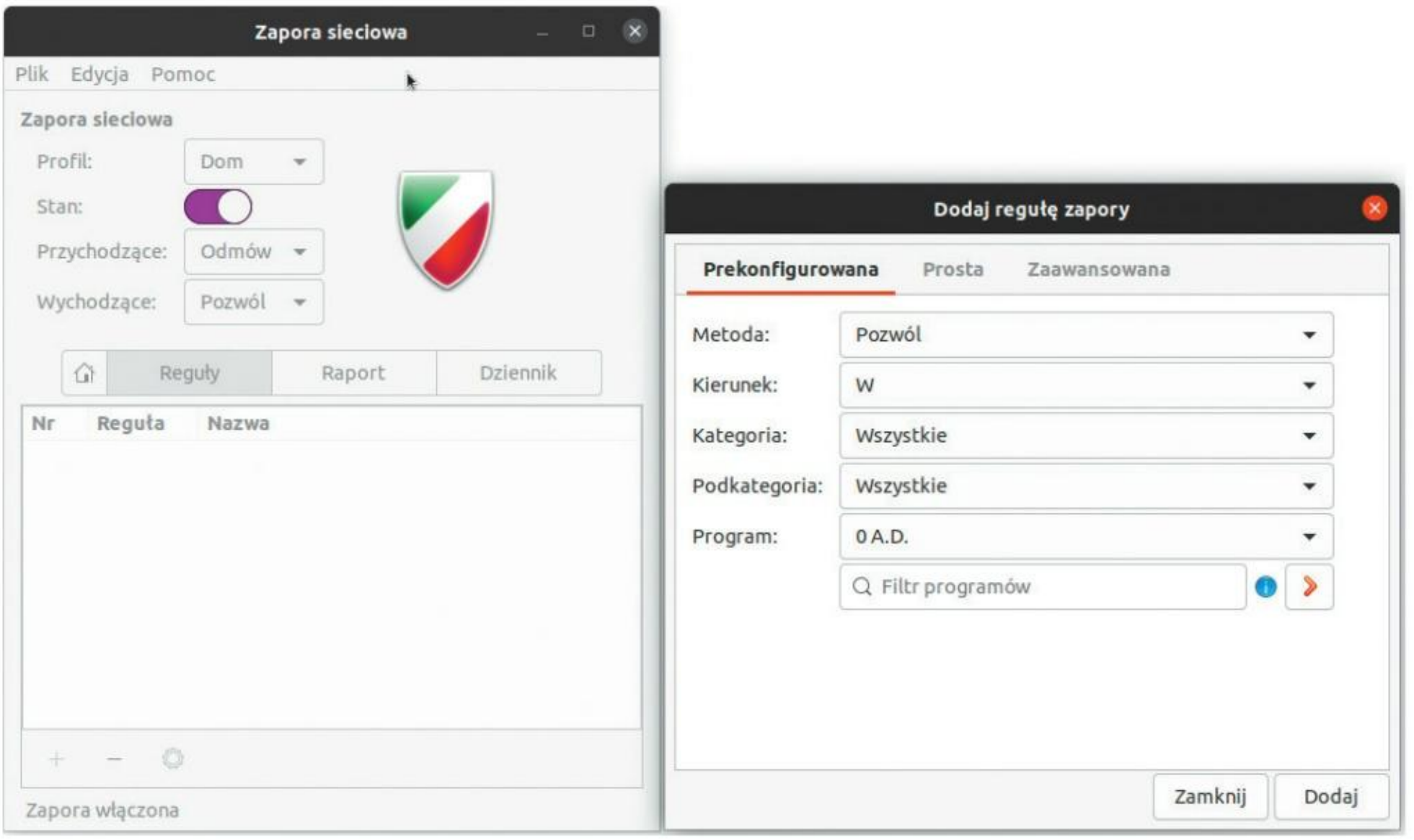
Aby uruchomić gufw, można wybrać **Wyświetl programy** i w polu wyszukiwania wpisać **gufw**, a następnie kliknąć ikonę **Konfiguracja zapory sieciowej** (ang. *Firewall Configuration*) i wprowadzić hasło użytkownika posiadającego uprawnienia do modyfikowania ustawień zapory. Po uruchomieniu aplikacji jest wyświetlany aktualny stan zapory (rys. 7.2). Aby można było wprowadzać zmiany w konfiguracji, należy odblokować aplikację, przestawiając pole wyboru **Stan**. W sekcji **Zapora sieciowa** jest zdefiniowana domyślna polityka dla strumieni **Przychodzących** i **Wychodzących**.

Rys. 7.2. **Okno główne aplikacji gufw**

Aby dodać nową regułę, należy wybrać w zakładce **Reguły** przycisk dodawania (**+**) nowej reguły (rys. 7.3). Zbędne lub źle wprowadzone reguły można usuwać za pomocą przycisku usuwania (**–**).

Użytkownik gufw może korzystać z trzech rodzajów reguł:

- **prekonfigurowanych** – pozwalają np. na filtrowanie danych na podstawie aplikacji lub usługi (nie wszystkie usługi i aplikacje mają przygotowane reguły);
- **prostych** – filtrowanie tylko na podstawie numerów portów;
- **zaawansowanych** – filtrowanie na podstawie adresów i numerów portów.



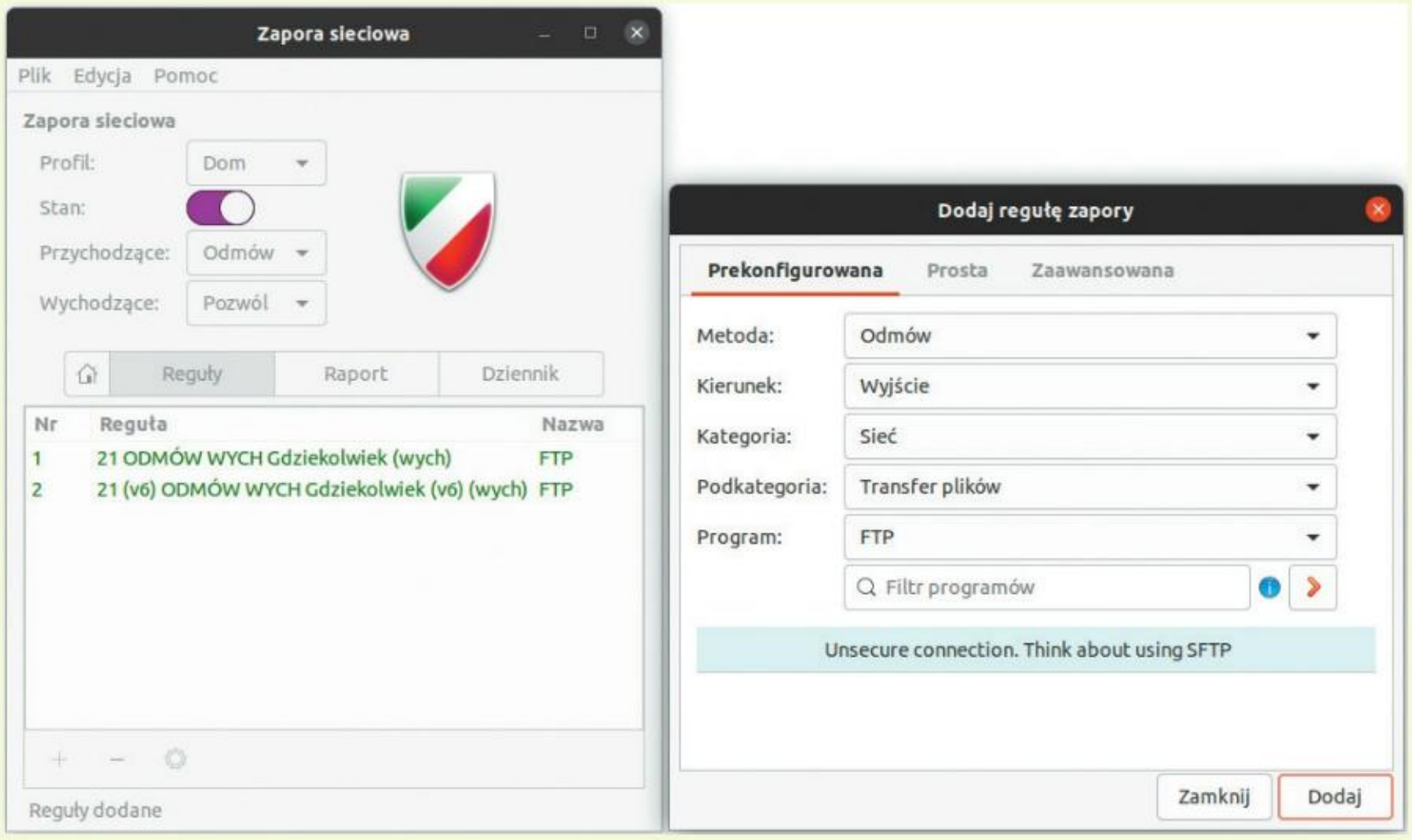
Rys. 7.3. **Dodawanie nowej reguły**

PRZYKŁAD 7.2

Dodawanie nowej reguły prekonfigurowanej

Reguła prekonfigurowana jest specjalnie przygotowana do wykonywania typowych akcji, np. blokowania usług lub aplikacji bądź ich udostępniania. Aby wprowadzić nowe reguły prekonfigurowane, należy:

1. Uruchomić aplikację **gufw** i odblokować dostęp do konfiguracji.
2. Ustawić politykę dla strumieni **Wychodzące** na **Pozwól**.
3. Wybrać tworzenie nowej reguły prekonfigurowanej (rys. 7.4).
4. Wprowadzić ustawienia blokowania (Metoda: **Odmów**) strumienia wyjściowego (Kierunek: **Wyjście**) w kategorii: **Sieć**, podkategorii: **Transfer plików** dla usługi (Program: **FTP**). Reguła uniemożliwi nawiązywanie połączenia z serwisem ftp z tego komputera. Kliknąć przycisk **Dodaj** (ang. *Add*).
5. Usunąć reguły utworzone dla protokołu IPv6. Sprawdzić, czy pozostałe reguły zostały dołączone do zbioru.
6. Przetestować działanie reguły przez próbę nawiązania połączenia z dowolnym serwerem FTP, np. **ftp.task.gda.pl**.



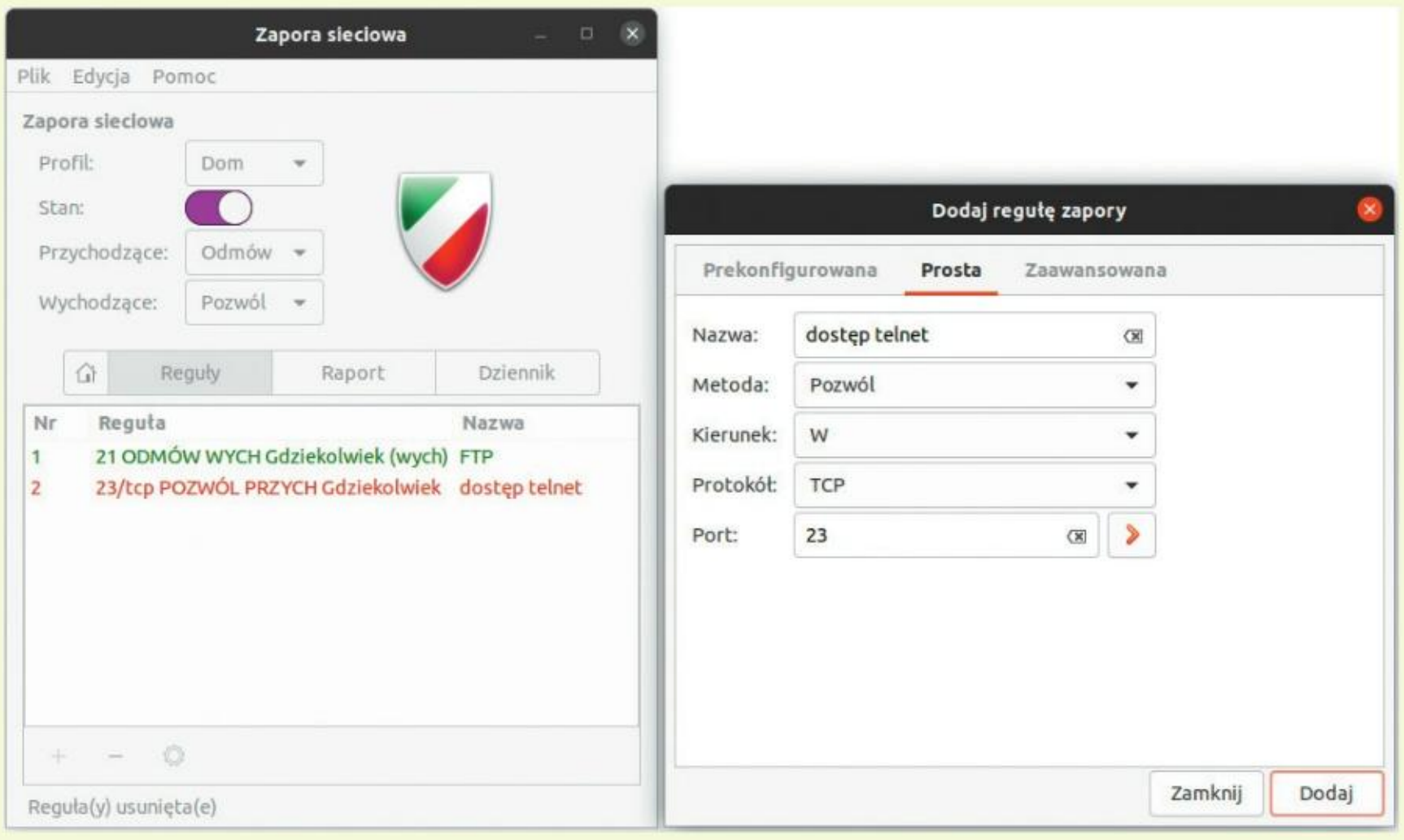
Rys. 7.4. **Tworzenie nowej reguły prekonfigurowanej**

PRZYKŁAD 7.3

Dodawanie nowej reguły prostej

Reguła prosta pozwala na filtrowanie na podstawie numerów portów (np. dla telnetu nie ma reguł prekonfigurowanych). Aby wprowadzić nową regułę prostą, należy:

1. Uruchomić aplikację **`gufw`** i odblokować dostęp do konfiguracji.
2. Ustawić politykę dla strumieni **`Przychodzących`** na **`Odmów`**.
3. Wybrać tworzenie nowej reguły prostej (rys. 7.5).



Rys. 7.5. **Tworzenie nowej reguły prostej**

4. Wprowadzić nazwę reguły, np. dostęp telnet, ustawienia zezwalania (Metoda: **Pozwól**) strumienia wejściowego (Kierunek: **W**) dla protokołu **TCP** na porcie 23. Reguła umożliwi nawiązywanie połączenia z serwisem **telnet**, standardowo działającym na porcie 23 na tym komputerze. Kliknąć przycisk **Dodaj** (ang. *Add*).
5. Usunąć reguły utworzone dla protokołu IPv6. Sprawdzić, czy reguła została dołączona do zbioru.

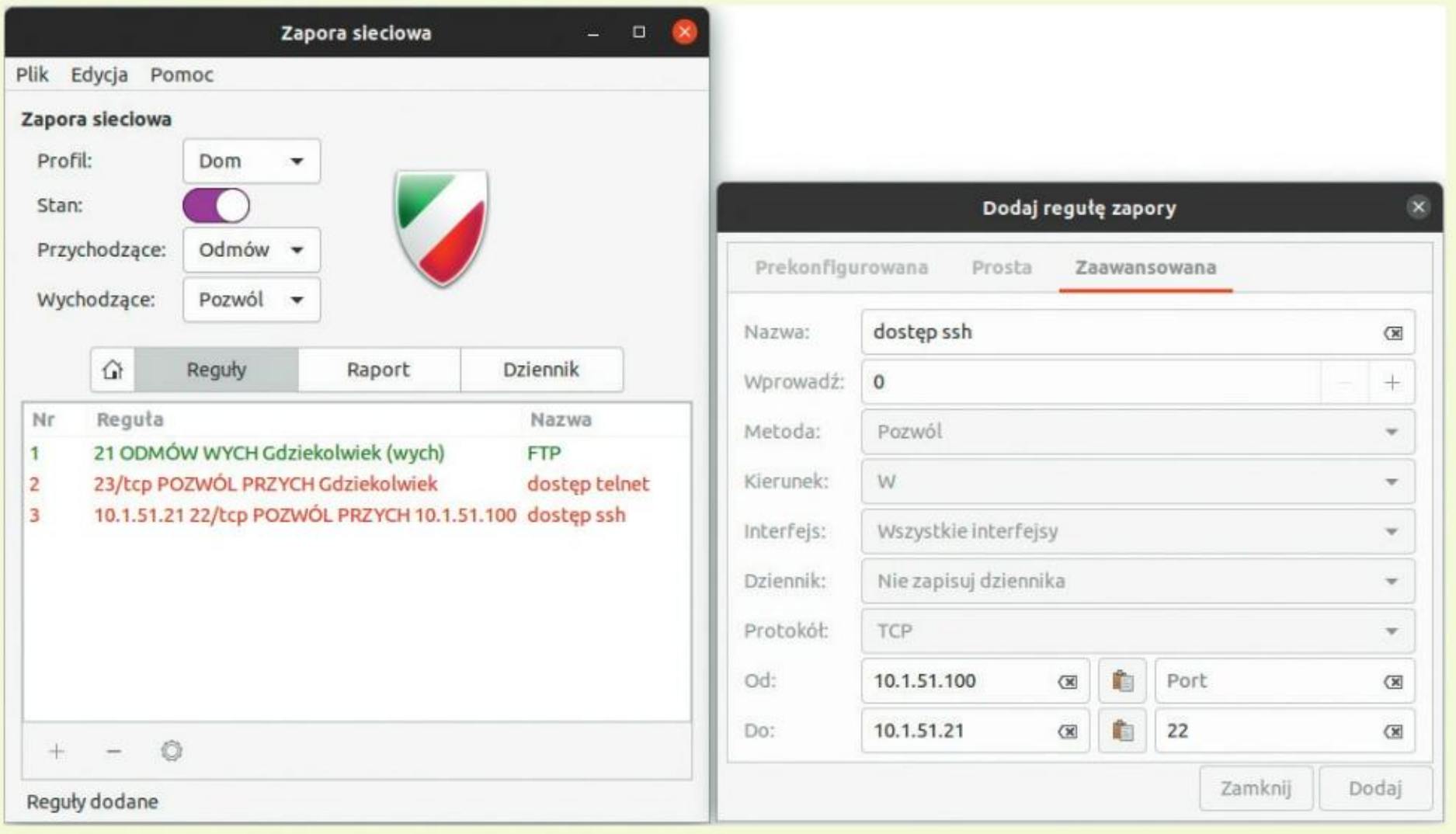
Usługa telnet nie jest jeszcze uruchomiona na komputerze, dlatego testowanie działania reguły należy odłożyć do momentu skonfigurowania usługi.

PRZYKŁAD 7.4

Dodawanie nowej reguły zaawansowanej

Reguła zaawansowana pozwala na filtrowanie danych na podstawie adresów IP i numerów portów. Aby wprowadzić nową regułę zaawansowaną, należy:

1. Uruchomić aplikację **gufw** i odblokować dostęp do konfiguracji.
2. Ustawić politykę dla strumieni **Przychodzących** na **Odmów**.
3. Wybrać tworzenie nowej reguły zaawansowanej (rys. 7.6).
4. Wprowadzić nazwę reguły, np. **dostęp ssh**, ustawienia zezwalania (Metoda: **Pozwól**) strumienia wejściowego (Kierunek: **W**) dla protokołu TCP. W regule można wskazać interfejsy lub pozostawić domyślne działanie reguły na wszystkich interfejsach. Zaawansowana reguła pozwala na określenie adresu źródłowego (np. od: **10.1.51.100**) i docelowego (np. do: **10.1.51.21**) oraz numerów portów. Pozostawienie numeru portu pustego oznacza wybór dowolnego portu. Reguła umożliwi nawiązywanie połączenia z serwisem **ssh**, standardowo działającym na porcie 22 na tym komputerze, tylko z adresu **10.1.51.100** z dowolnego portu. Kliknąć przycisk **Dodaj** (ang. *Add*).



Rys. 7.6. **Tworzenie nowej reguły zaawansowanej**

Ponieważ usługa **ssh** nie jest jeszcze uruchomiona na komputerze, testowanie działania reguły należy odłożyć do momentu skonfigurowania usługi.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sporządź listę usług, które planujesz uruchomić na swoim komputerze. Jeśli nie wiesz, jakie usługi są dostępne w sieci, zapytaj nauczyciela, które usługi będą uruchamiane.
2. Skorzystaj z informacji zawartych w internecie i ustal protokół warstwy 4 oraz standardowy numer portu dla każdej z usług.
3. Zaplanuj zbiór reguł zabezpieczających dostęp do twojego komputera.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Do czego służą zapory ogniowe?
2. Jakie inne mechanizmy mogą zwiększyć bezpieczeństwo systemu?

8 Przygotowanie do pracy serwera telnet

ZAGADNIENIA

Funkcje usługi telnet **Uruchomienie usługi telnet w systemie Linux**

Telnet pozwala zalogować się do zdalnego serwera i wykonywać na nim polecenia tak jak na komputerze lokalnym. Telnet umożliwia uzyskanie dostępu do wszystkich zasobów komputera zdalnego. Dane w sesjach telnetu są przesyłane bez szyfrowania (otwartym tekstem), co naraża użytkownika na przechwycenie i podsłuchanie transmisji. Dlatego nie należy przesyłać telnetem haseł i innych poufnych danych. Ze względu na bezpieczeństwo za pomocą telnetu nie można zalogować się na konto użytkownika *root*. Jeżeli telnet jest jedyną możliwością połączenia ze zdalnym serwerem, trzeba zalogować się na konto zwykłego użytkownika, a następnie za pomocą polecenia **`su`** uzyskać uprawnienia administratora.

Telnet jest usługą działającą w architekturze klient–serwer, kontrolowaną przez superdemona **`xinetd`**. Oprogramowanie klienta jest dołączone do każdego systemu operacyjnego. Oprogramowania serwera nie instaluje się w domyślnej konfiguracji.

PRZYKŁAD 8.1

Uruchamianie usługi telnet

Aby umożliwić nawiązywanie połączeń z komputerem za pomocą telnetu, należy:

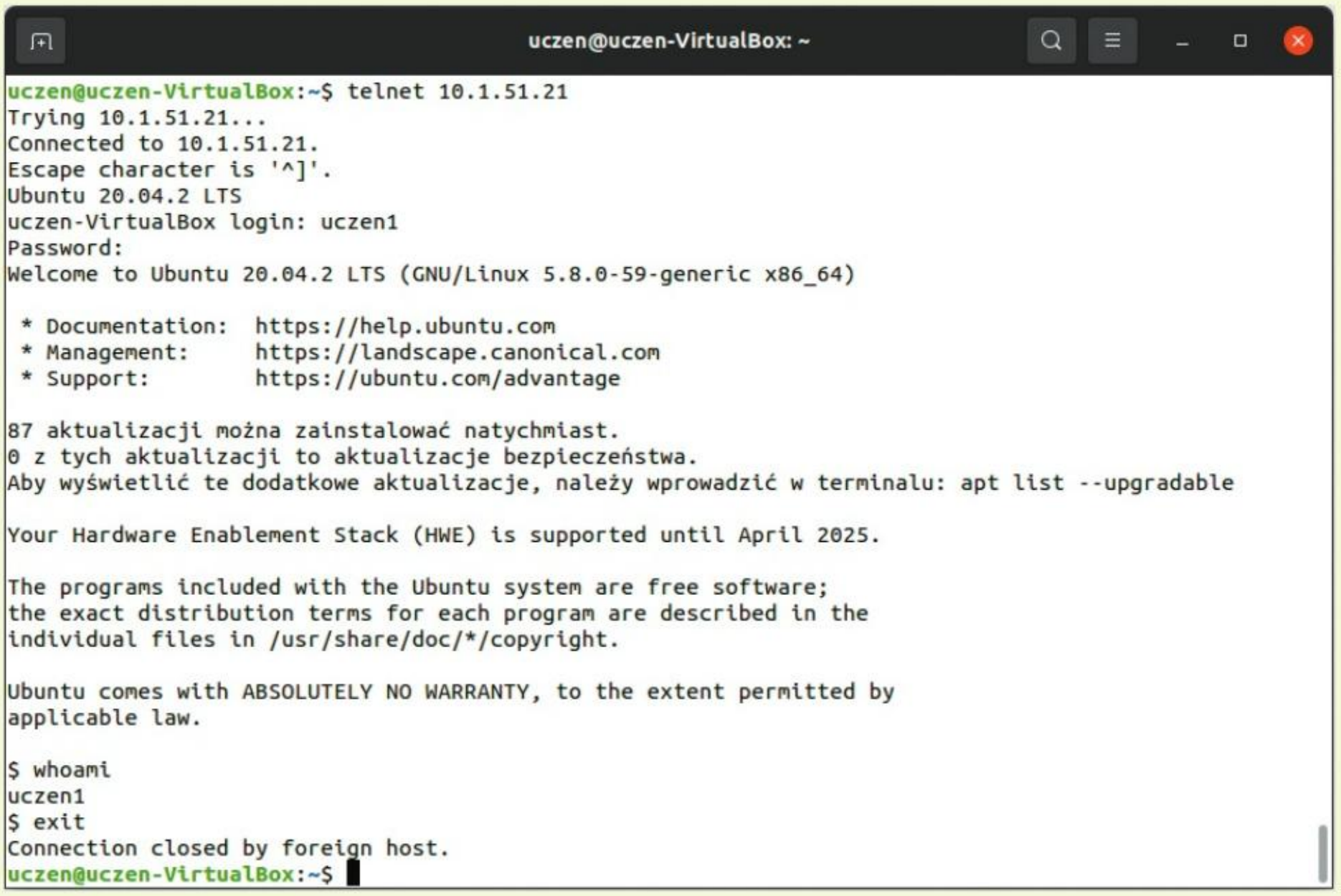
1. Zalogować się na konto użytkownika.
2. Zainstalować pakiet **`telnetd`** za pomocą polecenia:

   ```
   sudo apt install telnetd
   ```

   Serwer telnetu zostanie automatycznie dodany do listy serwisów uruchamianych podczas startu systemu.
   Ponownie uruchomić superdemona **`xinetd`** za pomocą polecenia:

   ```
   sudo /etc/init.d/openbsd-inetd restart
   ```

3. Za pomocą polecenia **`nmap`** sprawdzić, czy port 23 został otwarty.
4. Sprawdzić, czy możliwe jest nawiązanie połączenia za pomocą polecenia: **`telnet localhost`**
5. Sprawdzić możliwość połączenia z innego komputera.
   Od tego momentu można łączyć się z wybranym serwerem. Jeżeli występują problemy z nawiązaniem połączenia, należy sprawdzić, czy usługa telnet jest uruchomiona i czy firewall lub SELinux nie blokuje nawiązania połączeń. Przykładową sesję telnetu przedstawiono na rys. 8.1.
   Sesja rozpoczyna się od nawiązania połączenia, następnie jest sprawdzana nazwa konta użytkownika i sesja zostaje zakończona.



Rys. 8.1. **Sesja telnetu**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Za pomocą programu Nmap wyświetl listę otwartych portów twojego komputera.
2. Sprawdź, z którego numeru portu korzysta usługa telnet.
3. Spróbuj za pomocą telnetu nawiązać połączenie – skorzystaj z innego numeru portu otwartego na twoim komputerze. Przykładowo, aby nawiązać połączenie na porcie 22 (standardowy port dla usługi SSH), wydaj polecenie **`telnet localhost 22`**. Czego można się dowiedzieć z uzyskanej odpowiedzi serwera?
4. Spróbuj za pomocą telnetu nawiązać połączenie – skorzystaj z zamkniętego portu na twoim komputerze. Przykładowo, aby nawiązać połączenie na porcie 123, wydaj polecenie **`telnet localhost 123`**. Czego można się dowiedzieć z uzyskanej odpowiedzi serwera?

9 Przygotowanie do pracy serwera SSH

ZAGADNIENIA

Funkcje protokołu SSH **Klucze publiczne i klucze prywatne** **Nawiązywanie połączenia za pomocą SSH**

Protokół SSH (ang. *Secure Shell*) stworzono, aby wykorzystać możliwość zdalnego logowania i zachować bezpieczeństwo haseł. W Linuksie jest używana bezpłatna implementacja o nazwie OpenSSH. Protokół SSH umożliwia połączenie się użytkownika ze zdalnym systemem, tak jak w przypadku telnetu, ale sesja jest szyfrowana. Osoba używająca elektronicznego podsłuchu zobaczy zaszyfrowane informacje, których odczytanie jest możliwe tylko wtedy, gdy ma się odpowiedni klucz kryptograficzny.

Protokół SSH opiera się na kryptografii klucza publicznego. Do korzystania z **SSH** są potrzebne dwa klucze: **publiczny** i **prywatny**. Klucz publiczny jest powszechnie dostępny (może być umieszczony na stronie sieci WWW), klucz prywatny musi być dobrze chroniony. Każda kombinacja klucz prywatny / klucz publiczny jest niepowtarzalna. Klucz prywatny nie jest przesyłany przez sieć. Gdy dane są zaszyfrowane za pomocą klucza publicznego, można je odszyfrować tylko za pomocą klucza prywatnego tego użytkownika (SSH regularnie zmienia swój prywatny klucz, tak aby dane były inaczej szyfrowane co kilka minut).

Protokół SSH pracuje w architekturze klient–serwer. Klient jest instalowany domyślnie. Serwer SSH można zainstalować w dowolnym momencie poleceniem: **`sudo apt install ssh`**. Polecenie spowoduje zainstalowanie wszystkich pakietów niezbędnych do obsługi protokołu. W środowisku Windows nie ma nawet klienta SSH – jeżeli użytkownik zamierza korzystać z tego protokołu, to musi z sieci pobrać klienta, np. bezpłatny program PUTTY.

PRZYKŁAD 9.1

Uruchamianie usługi SSH

Aby umożliwić nawiązywanie połączeń za pomocą SSH z komputerem, należy:

1. Zalogować się na konto użytkownika.
2. Zainstalować pakiet SSH poleceniem:

   ```
   sudo apt install ssh
   ```

3. Serwer SSH zostanie automatycznie dodany do listy serwisów uruchamianych podczas startu systemu.
4. Ponownie uruchomić demona SSH poleceniem:

   ```
   sudo /etc/init.d/ssh restart
   ```

5. Do zatrzymania demona SSH można użyć polecenia:

   ```
   sudo /etc/init.d/ssh stop
   ```

6. Do uruchomienia demona SSH można użyć polecenia:
   `sudo /etc/init.d/ssh start`
7. Sprawdzić, czy możliwe jest nawiązanie połączenia za pomocą polecenia:
   `ssh uczen@10.1.51.21`
8. Sprawdzić możliwość połączenia z innego komputera.

Od tego momentu można łączyć się z wybranym serwerem. Jeżeli występują problemy z nawiązaniem połączenia, należy sprawdzić, czy usługa jest uruchomiona i czy firewall lub SELinux nie blokuje nawiązania połączeń. Przykładową sesję SSH przedstawiono na rys. 9.1. Sesja rozpoczyna się od nawiązania połączenia. Podczas pierwszego połączenia z serwerem jest generowana para kluczy wykorzystywanych do szyfrowania danych. Następnie zostają sprawdzone nazwa konta użytkownika i hasło. Jeżeli autoryzacja przebiegnie pomyślnie, jest ustanawiana sesja.

Rys. 9.1. Nawiązywanie połączenia za pomocą protokołu SSH

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skorzystaj z klienta PUTTY, pracującego w środowisku Windows, i nawiąż połączenie z własnym komputerem. Wyświetl nazwę konta, na którym pracujesz.
2. Za pomocą SSH połącz się z komputerem kolegi. Wprowadź polecenie:
   `sudo shutdown -h now`

Uwaga! Obowiązuje zasada: „Kto pierwszy, ten lepszy".

10 Przygotowanie do pracy serwera DHCP

ZAGADNIENIA

Protokół DHCP i jego zadania **Etapy uruchomienia serwera DHCP** **Skonfigurowanie serwera DHCP** **Uruchomienie serwera DHCP z dynamicznym i statycznym przydzielaniem adresów**

DHCP (ang. *Dynamic Host Configuration Protocol*) jest protokołem służącym do dynamicznej konfiguracji adresów dla dużych grup stacji lub komputerów przenośnych. To narzędzie składa się z oprogramowania klienta i serwera DHCP. Komputer klienta jest skonfigurowany do automatycznego uzyskiwania od serwera DHCP adresu IP i innych danych potrzebnych do jego konfiguracji.

Klient skonfigurowany do automatycznego pobierania adresu IP wysyła do sieci na adres rozgłoszeniowy **żądanie przydziału danych konfiguracyjnych** (ang. *DHCP Discover*). Serwer DHCP nasłuchuje żądań klientów. Gdy serwer odbierze żądanie, sprawdza lokalną bazę danych i wysyła odpowiedź z **ofertą danych konfiguracyjnych** (ang. *DHCP Offer*) zawierającą adres i dodatkowo adresy serwerów nazw, maskę sieciową i domyślną bramę (jeżeli te informacje zostały zdefiniowane). Oferta jest wysyłana tylko na adres klienta. Serwerów DHCP w sieci może być więcej niż jeden (nie jest to zalecane), więc klient może otrzymać kilka ofert. Klient wybiera jedną z ofert, najczęściej pierwszą, która wpłynęła, i wysyła **żądanie przydziału danych** (ang. *DHCP Request*). Żądanie jest wysyłane na adres rozgłoszeniowy – w ten sposób wszystkie serwery DHCP są informowane o tym, która oferta została zaakceptowana. Serwer, którego oferta została wybrana, wysyła do klienta **potwierdzenie** (ang. *DHCP Acknowledgement*). Klient akceptuje odpowiedź od serwera i na jej podstawie konfiguruje swoje ustawienia. Serwer DHCP przechowuje listę adresów, które może przydzielić klientom, i listę adresów już przydzielonych. Każdy adres jest przydzielany na pewien czas i nazywany **dzierżawą**. Po upływie tego czasu klient musi ponownie skontaktować się z serwerem w celu odnowienia dzierżawy. Serwer może przydzielić klientowi ponownie ten sam adres, ale może też wybrać inny z dostępnej puli adresów.

Serwer może przydzielać adresy w sposób **dynamiczny**. W takim przypadku w konfiguracji serwera jest określona pewna **pula adresów**, które przydziela klientom. Na ogół jest przydzielany pierwszy wolny adres z puli. Jeżeli klient wcześniej już korzystał z dzierżawy adresu, to może poinformować o tym serwer i uzyskać ten sam adres. Serwer zwykle przydziela ten sam adres, jeżeli jest to możliwe.

Bardzo często użytkownicy chcą, aby pewne komputery w sieci uzyskiwały zawsze ten sam adres IP. Ułatwia to odszukiwanie np. serwerów w sieci lokalnej, serwerów wydruku lub drukarek. Stały przydział klientowi adresu IP można zapewnić dzięki **wpisowi statycznemu** w konfiguracji serwera DHCP, który polega na tym, że do bazy danych serwera wprowadzamy informacje o adresach fizycznych (MAC) klientów i adresy IP, które mają im być przydzielone. Adres MAC każdego klienta jest stały i musi być unikatowy. To pozwoli serwerowi na jednoznaczne określenie i przypisywanie zawsze tego samego adresu IP. Serwer DHCP najpierw stara się przydzielić adres statyczny, a jeśli jest to niemożliwe, przydziela adres dynamicznie.

Uruchomienie serwisu DHCP składa się z trzech etapów:

1. Instalacja serwera.
2. Konfiguracja serwera.
3. Konfiguracja klientów.

Serwer DHCP nie jest instalowany domyślnie. Aby zainstalować serwer, można posłużyć się poleceniem:

```
sudo apt install isc-dhcp-server
```

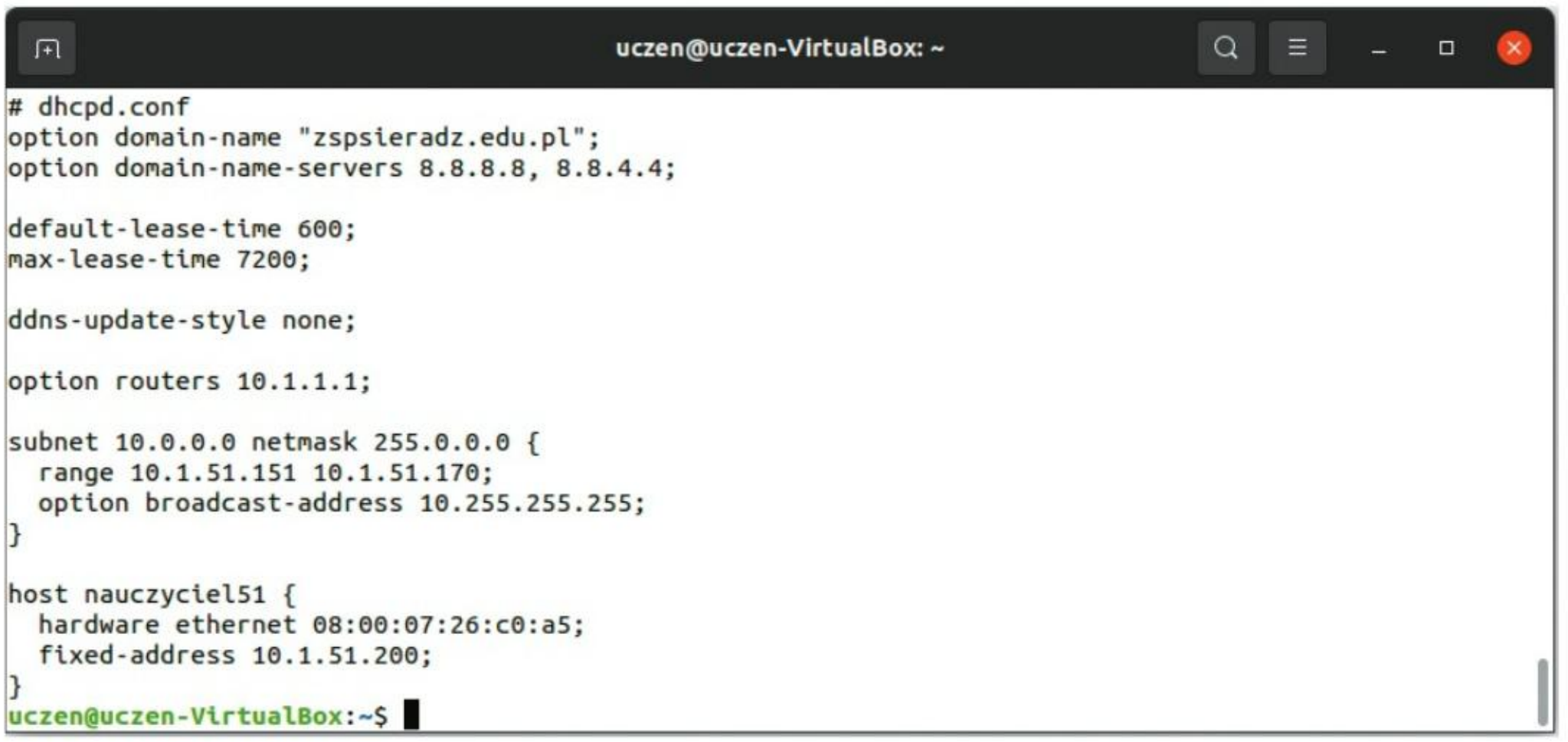
> **! UWAGA**
>
> Przed przystąpieniem do modyfikacji jakiegokolwiek pliku konfiguracyjnego należy wykonać jego kopię bezpieczeństwa. W razie problemów pozwoli ona na odtworzenie oryginalnego pliku. Kopię bezpieczeństwa pliku można wykonać za pomocą polecenia **cp**, np.:
>
> ```
> sudo cp /etc/dhcp/dhcp.conf /etc/dhcp/dhcp.conf.old
> ```

Do konfiguracji serwera DHCP wykorzystuje się dwa pliki: **/etc/default/isc-dhcp-server** i **/etc/dhcp/dhcpd.conf**. W pliku **/etc/default/isc-dhcp-server** należy określić, na którym interfejsie serwer będzie nasłuchiwał żądań od klientów. Przykładowy plik przedstawiono na rys. 10.1.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
INTERFACESv6=""
uczen@uczen-VirtualBox:~$
```

Rys. 10.1. **Przykładowy plik /etc/default/isc-dhcp-server**

W pliku konfiguracyjnym **/etc/dhcp/dhcpd.conf** są opisane parametry globalne i przydzielane adresy. Jeżeli taki plik nie istnieje, to należy go utworzyć i wpisać odpowiednie instrukcje. Przykładowy plik **dhcpd.conf** pokazano na rys. 10.2.



Rys. 10.2. **Przykładowy plik dhcpd.conf**

Plik **dhcpd.conf** może zawierać instrukcje globalne:

- **option domain-name „zspsieradz.edu.pl";** – nazwa domeny lokalnej
- **option domain-name-servers 8.8.8.8, 8.8.4.4;** – adresy serwerów DNS
- **default-lease-time 600;** – domyślny czas dzierżawy
- **max-lease-time 7200;** – maksymalny czas dzierżawy
- **option ddns-update-style none;** – obsługa DDNS (ustawienie standardowe)
- **option routers 10.1.1.1;** – adres bramy

Ustawienia dotyczące puli adresów przydzielanych dynamicznie:
subnet 10.0.0.0 netmask 255.0.0.0 { – definicja podsieci i maski
range 10.1.51.151 10.1.51.170; – pula adresów przydzielanych dynamicznie
option broadcast-address 10.255.255.255; – adres rozgłoszeniowy
}

Ustawienia dotyczące adresów przydzielanych statycznie:
host nauczyciel51 { – nazwa komputera
hardware ethernet 08:00:07:26:C0:A5; – adres MAC klienta
nauczyciel51 fixed-address 10.1.51.25; – adres IP klienta nauczyciel51
}

> **! UWAGA**
> Adres IP serwera DHCP musi należeć do podsieci zdefiniowanej za pomocą polecenia **subnet**.

Po wpisaniu instrukcji do pliku konfiguracyjnego serwer należy uruchomić za pomocą polecenia:

```
sudo service isc-dhcp-server start
```

Po każdej modyfikacji pliku konfiguracyjnego usługę trzeba uruchomić ponownie za pomocą polecenia:

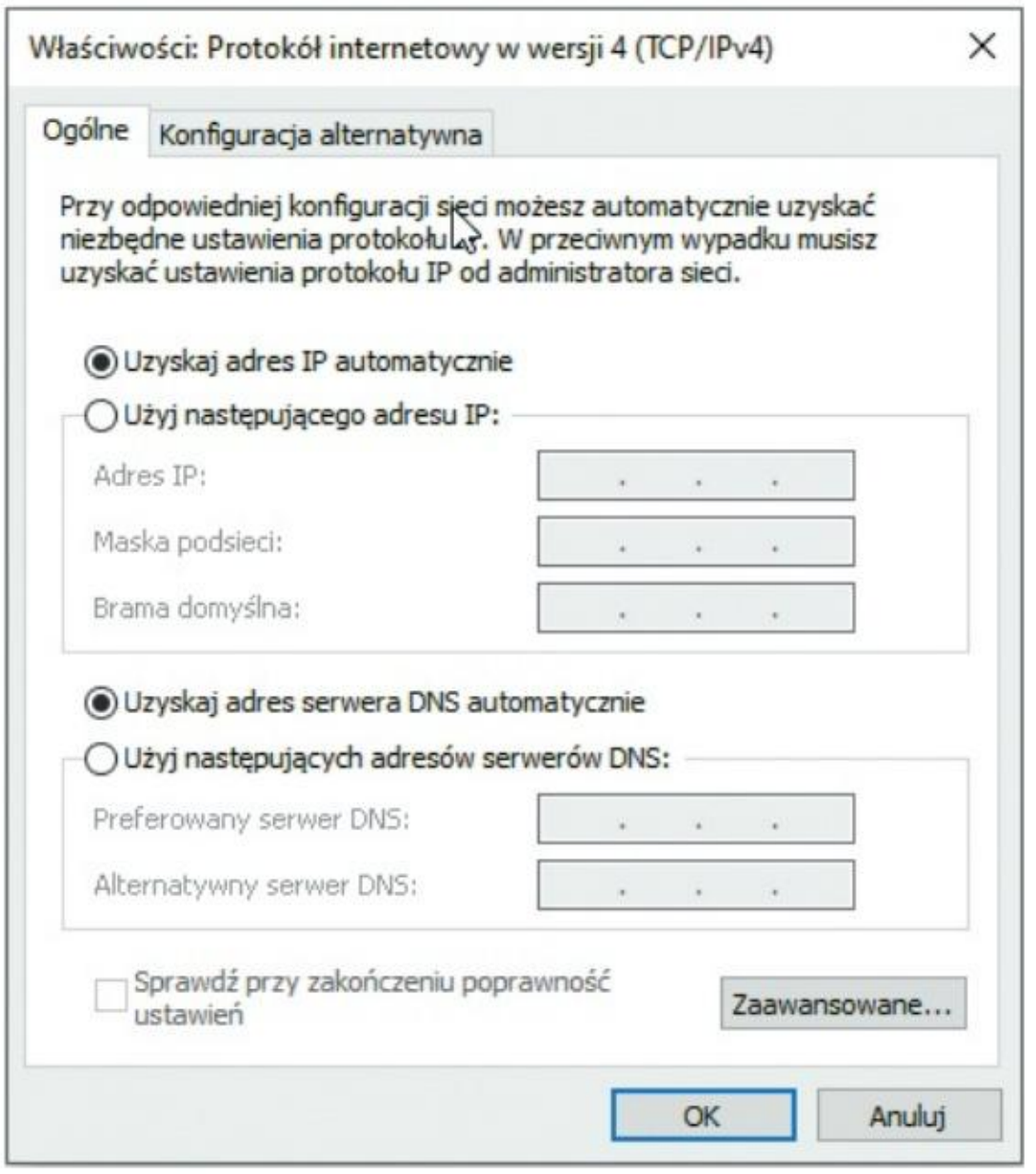
```
sudo service isc-dhcp-server restart
```

Aby zatrzymać serwer, można posłużyć się poleceniem:

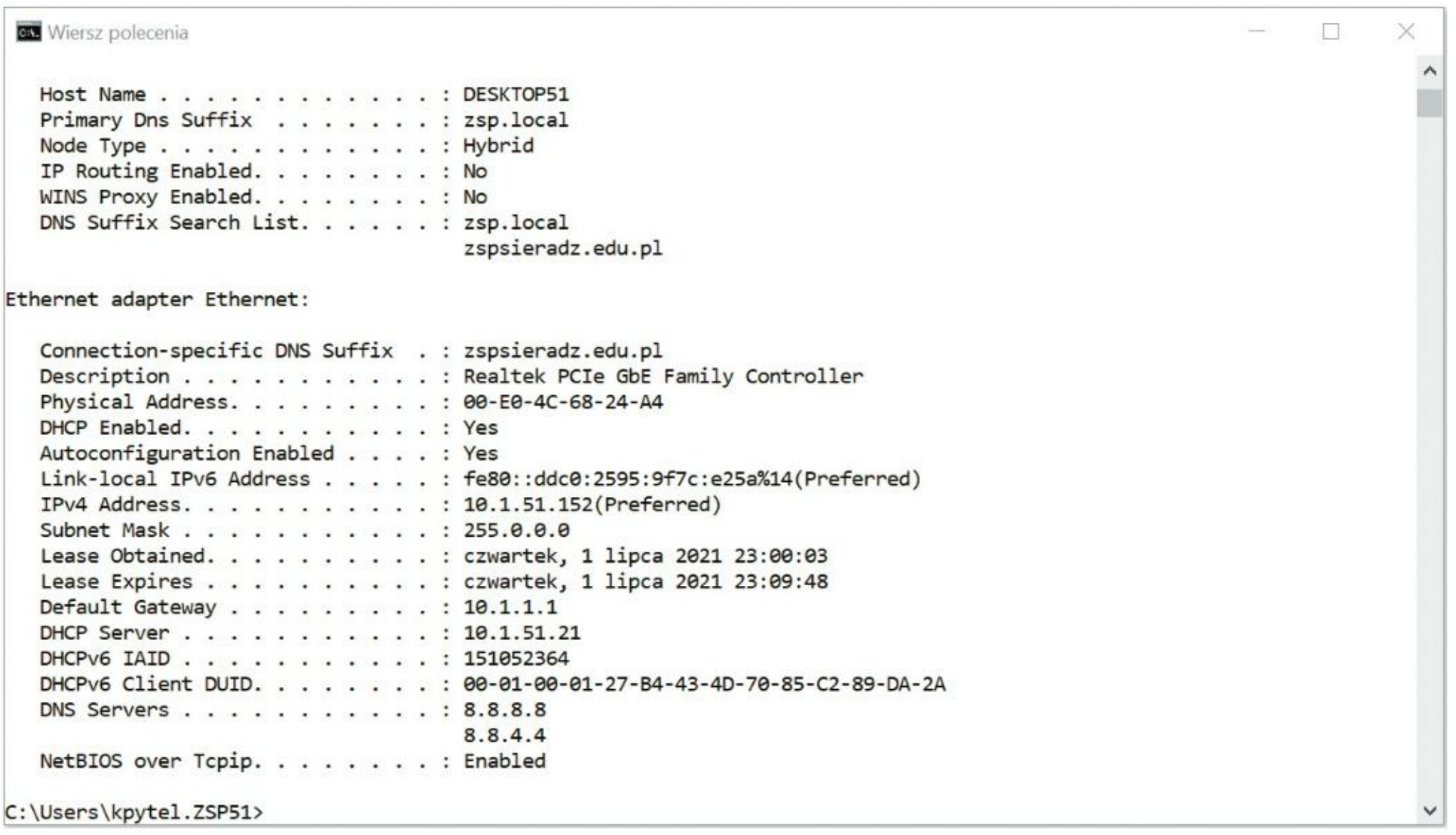
```
sudo service isc-dhcp-server stop
```

Z serwera DHCP dane konfiguracyjne mogą pobierać klienci pracujący pod dowolnym systemem operacyjnym. Konfigurację systemu Windows do współpracy z serwerem DHCP przedstawiono na rys. 10.3.

Aby sprawdzić konfigurację protokołu IP w systemie Windows, trzeba wydać polecenie: **`ipconfig /all`** (rys. 10.4).



Rys. 10.3. Ustawienie klienta do automatycznego pobierania adresu



Rys. 10.4. Weryfikacja działania protokołu DHCP

PRZYKŁAD 10.1

Uruchamianie serwera DHCP z dynamicznym przydzielaniem adresów

Aby skonfigurować serwer DHCP dynamicznie przydzielający adresy, należy:

1. Zalogować się na konto użytkownika.
2. Jeżeli serwer DHCP nie jest zainstalowany, trzeba go zainstalować.
3. Odłączyć komputery od sieci szkolnej lub połączyć po dwa komputery za pomocą kabla skrosowanego (jeden z komputerów będzie pełnił funkcję serwera DHCP, a drugi – klienta). Można również połączyć w małą sieć kilka komputerów za pomocą przełącznika i w sieci skonfigurować serwer DHCP i kilka klientów. Jeżeli komputery korzystają z innego medium transmisyjnego niż skrętka, zapytaj nauczyciela, jak je połączyć.
4. Utworzyć lub zmodyfikować pliki **`/etc/default/isc-dhcp-server`** i **`/etc/dhcp/dhcpd.conf`**. W pliku **`/etc/dhcp/dhcpd.conf`** umieścić opcje globalne i dotyczące puli adresów przydzielanych dynamicznie (opcja subnet).
5. Uruchomić usługę za pomocą polecenia:

   `sudo service isc-dhcp-server restart`
6. Skonfigurować komputer pełniący funkcję klienta DHCP.
7. Sprawdzić, czy klient otrzymuje od serwera poprawne dane. Użyć do tego polecenia: **`ipconfig /all`** w systemie Windows lub **`ifconfig`** albo **`ip addr show`** w systemie Linux.

KODY

PRZYKŁAD 10.2

Uruchamianie serwera DHCP ze statycznym przydzielaniem adresów

Aby skonfigurować serwer DHCP statycznie przydzielający adresy, należy:

1. Zalogować się na konto użytkownika.
2. Jeżeli serwer DHCP nie jest zainstalowany, to go zainstalować.
3. Odłączyć komputery od sieci szkolnej lub połączyć po dwa komputery za pomocą kabla skrosowanego (jeden z komputerów będzie odgrywał rolę serwera DHCP, a drugi – klienta). Można również połączyć w małą sieć kilka komputerów za pomocą przełącznika i w sieci skonfigurować serwer DHCP i kilka klientów. Jeżeli komputery korzystają z innego niż skrętka medium transmisyjnego, zapytaj nauczyciela, jak je połączyć.
4. Utworzyć lub zmodyfikować pliki **`/etc/default/isc-dhcp-server`** i **`/etc/dhcp/dhcpd.conf`**. W pliku **`/etc/dhcp/dhcpd.conf`** umieścić opcje globalne i dotyczące puli adresów przydzielanych statycznie (opcja host).
5. Uruchomić usługę za pomocą polecenia:

   `sudo service isc-dhcp-server restart`
6. Skonfigurować komputer odgrywający rolę klienta DHCP.
7. Sprawdzić, czy klient otrzymuje od serwera poprawne dane – użyć polecenia: **`ipconfig /all`** w systemie Windows lub **`ip addr show`** w systemie Linux.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

Połącz kablem skrosowanym komputer z systemem Windows i twój serwer. Skonfiguruj system Windows do pobierania konfiguracji z serwera DHCP. Na serwerze DHCP skonfiguruj pulę adresów dynamicznych od `10.1.51.210` do `10.1.51.220` i adres `10.1.51.200` przydzielony statycznie dla komputera z Windows.

1. Wyłącz i ponownie włącz kartę sieciową komputera z Windows. Jaki otrzymała adres IP i z jakiej klasy? Co jeszcze można powiedzieć o tym adresie?
2. Wyłącz serwer DHCP i zrestartuj kartę sieciową komputera z Windows. Jaki otrzymała adres IP i z jakiej klasy? Co jeszcze można powiedzieć o tym adresie?

11 Przygotowanie do pracy serwera DNS

ZAGADNIENIA

Funkcje protokołu DNS **Typy serwerów DNS** **Typy stref przeszukiwania i ich funkcje** **Procedura konfigurowania serwerów buforującego, podstawowego i zapasowego** **Narzędzia do testowania działania serwera DNS**

System DNS jest oparty na hierarchicznej i logicznej strukturze drzewa zwanej obszarem nazw **domen**. Każdy węzeł drzewa DNS reprezentuje nazwę DNS, np. domenę DNS. Domeny DNS mogą zawierać hosty (np. komputery, serwery) i inne domeny nazywane **poddomenami**. Węzły w drzewie domen DNS są identyfikowane przez **pełną nazwę domeny FQDN** (ang. *Fully Qualified Domain Name*) i wskazują położenie węzła względem domeny głównej.

Serwer DNS pozwala na tłumaczenie nazw w sieciach opartych na TCP/IP na adresy IP odpowiadające nazwom. Dzięki DNS użytkownik może posługiwać się nazwami domen zamiast adresami IP konkretnych serwerów. DNS może być wykorzystany do tłumaczenia nazw w sieci lokalnej lub, po zarejestrowaniu nazwy domeny, również w internecie.

Serwer DNS umożliwia dwa rodzaje przeszukiwania strefy:

- **do przodu** – na podstawie nazwy określamy adres IP;
- **wstecz** – na podstawie adresu IP szukamy odpowiadającej mu nazwy.

Do przeszukiwania stref serwer wykorzystuje rekordy zasobów:

- **A** – mapuje nazwę hosta na adres IPv4;
- **AAAA** – mapuje nazwę hosta na adres IPv6;
- **CNAME** – ustawia alias (inną nazwę) dla nazwy hosta;
- **MX** – określa serwer wymiany poczty dla domeny;
- **NS** – określa serwer nazw dla domeny (DNS);
- **PTR** – tworzy powiązanie adresu IP z nazwą w strefie przeszukiwania wstecz.

Rekord SOA (ang. *Start of Authority*) jest wymagany dla każdej strefy i określa serwer DNS, który dostarcza autorytatywne informacje dla danej strefy. Istnieją trzy główne sposoby konfigurowania usługi DNS:

- **buforujący serwer nazw** (ang. *caching name server*) – nie przechowuje bazy danych rekordów; gdy otrzyma zapytanie o nazwę, o obsłużenie żądania poprosi inny serwer nazw i umieści ją w swoim buforze, dzięki czemu będzie ona zawsze dostępna;
- **podstawowy serwer nazw** (ang. *primary name server*) – zawiera główną kopię bazy danych z nazwami wszystkich hostów w strefie i rekordy dla wszystkich poddomen;
- **zapasowy serwer nazw** (ang. *secondary name server*) – zawiera kopię bazy danych z rekordami dla domeny i poddomen; zmiany wprowadzane do podstawowego DNS są replikowane do wszystkich serwerów zapasowych.

Jednym z najpopularniejszych serwerów DNS wykorzystywanym w systemach Linux jest **BIND**. Aby zainstalować serwer w dystrybucji Ubuntu, należy wydać polecenie:

```
sudo apt install bind9
```

Pliki konfiguracyjne są przechowywane w katalogu **/etc/bind/**. Podstawowe opcje konfiguracji – w plikach **named.conf**, **named.conf.options** i **named.conf.local**. Ponadto, dodatkowe pliki wykorzystuje się do przechowywania informacji o strefach.

Dzięki buforującemu serwerowi nazw można przyspieszyć proces tłumaczenia nazw na adresy IP. Serwer umieszczony w sieci lokalnej, np. w szkole, zapisuje w swojej pamięci informacje o nazwach stron internetowych odwiedzonych przez uczniów i odpowiadających im adresach IP. Dostęp do tych informacji w sieci lokalnej jest szybszy, a ponadto można zmniejszyć liczbę zapytań wysyłanych do zewnętrznych serwerów DNS.

PRZYKŁAD 11.1

KODY

Konfigurowanie i testowanie buforującego serwera nazw

Aby skonfigurować buforujący serwer nazw, należy:

1. W pliku **named.conf.options** usunąć symbol komentarza na początku poniższych linijek i wpisać adresy serwerów DNS dostawcy usług internetowych (rys. 11.1). W tym przykładzie wpisano adresy serwerów **OpenDNS** – oferujących darmowy dostęp do DNS i dodatkowo możliwość zablokowania dostępu np. do stron pornograficznych lub zawierających sceny przemocy.

```
forwarders {
208.67.222.222;
208.67.220.220;
};
```

uczen@uczen-VirtualBox: ~

```
uczen@uczen-VirtualBox:~$ cat /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                208.67.222.222;
                208.67.220.220;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
uczen@uczen-VirtualBox:~$
```

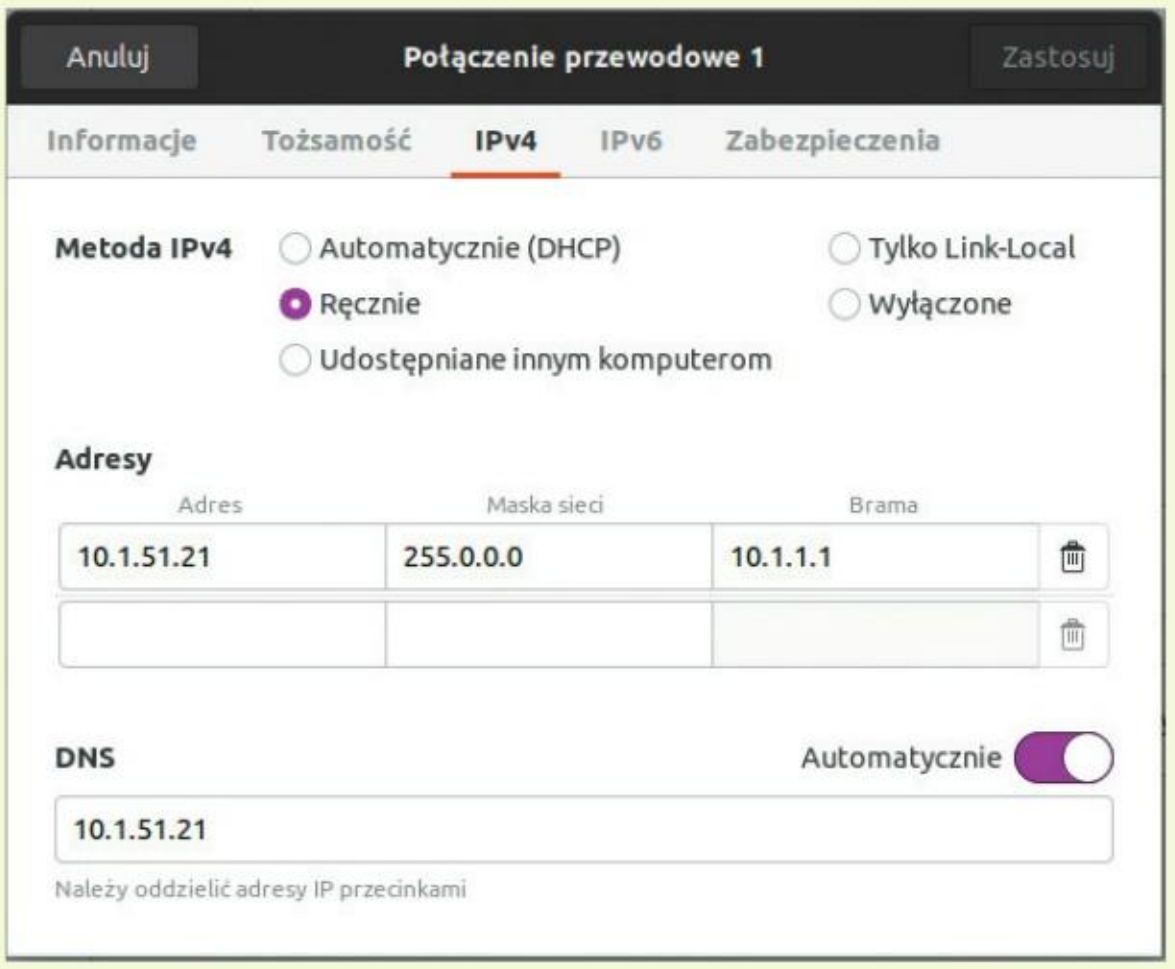
Rys. 11.1. **Przykładowy plik /etc/bind/named.conf.options**

2. Uruchomić ponownie demona BIND za pomocą polecenia:

   `sudo service bind9 restart`

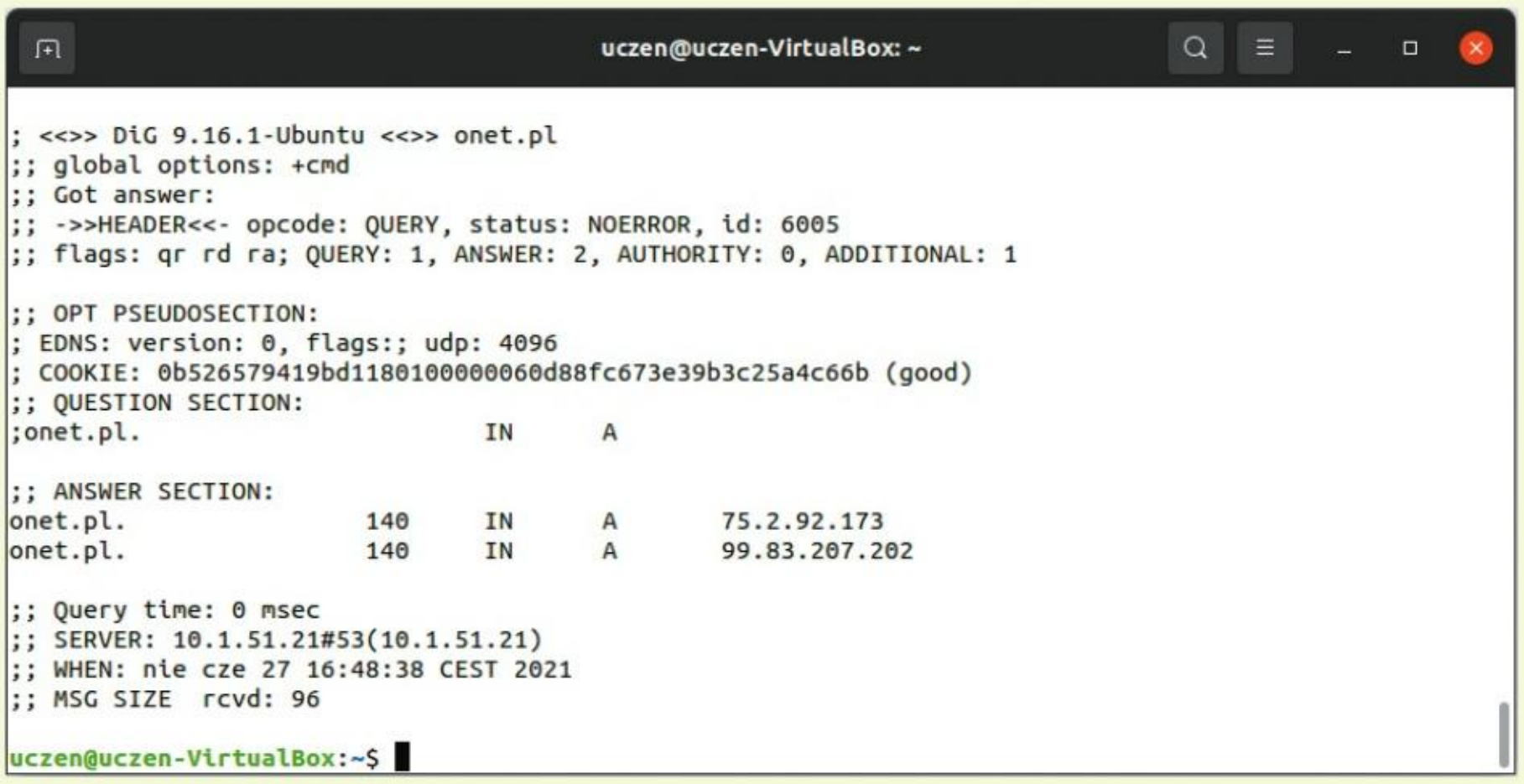
3. W oknie konfiguracji adresu IPv4 w komputerze ustawić adres serwera DNS. W polu Serwery DNS wpisać adres IP komputera, w którym jest uruchomiony buforujący serwer DNS (rys. 11.2).

KODY



Rys. 11.2. **Konfiguracja adresu serwera DNS**

4. Przetestować działanie serwera. Do testowania serwera DNS w środowisku Linux można użyć polecenia **`dig`**, np. aby sprawdzić adres IP serwera **`onet.pl`**, należy wydać polecenie: **`dig onet.pl`**.
   Przykład działania polecenia **`dig`** zaprezentowano na rys. 11.3. Adres IP **`serwera onet.pl`** jest pokazany w sekcji „ANSWER SECTION”.



Rys. 11.3. **Testowanie DNS za pomocą polecenia `dig`**

! UWAGA

Jeżeli w poleceniu **dig** jest wyświetlana informacja **;;SERVER: 127.0.0.53** (trzeci wiersz od dołu), to oznacza, że do rozwiązywania nazw jest wykorzystywany lokalny serwer DNS (uruchomiony na tym samym komputerze). W pliku resolvera **/etc/resolv.conf** można wprowadzić adres serwera nazw, np. wykomentować wiersz **nameserver 127.0.0.53** i dopisać nowy: **nameserver 10.1.51.21**.

Każdy host w domenie ma adres IP i nazwę domenową. **Rekordy odwzorowania adresów** (**A**) odwzorowują nazwę hosta na przypisany mu adres IP. Dzięki tym rekordom inne hosty w sieci mogą uzyskać od serwera DNS odpowiedź na zapytania o adres IP przypisany do określonej nazwy hosta. **Rekordy wskaźników wyszukiwania odwrotnego** (**PTR**) odwzorowują adresy IP poszczególnych hostów na przypisane im nazwy – pozwalają innym hostom w sieci uzyskać od serwera DNS informacje o nazwach odpowiadających adresowi IP. Administrator serwera DNS musi zdefiniować dane strefy DNS i utworzyć rekordy zasobów. Serwer DNS obsługuje również inne typy rekordów zasobów, np. **rekordy serwerów poczty elektronicznej** (**MX**) lub innych **serwerów nazw** (**NS**).

Każdy serwer nazw zawiera dane o pewnej części całej przestrzeni adresowej DNS. Dane z każdej domeny powinny być przechowywane na co najmniej dwóch serwerach. Jeden z nich, tzw. **podstawowy serwer nazw**, jest autorytatywnym źródłem informacji o danej domenie. Pozostałe serwery przechowują kopię zawartości serwera podstawowego. **Serwery zapasowe** zwiększają niezawodność i odporność całego systemu na awarie i są używane w przypadku awarii lub wyłączenia serwera podstawowego albo w celu rozłożenia obciążenia na kilka serwerów.

PRZYKŁAD 11.2

Konfigurowanie podstawowego serwera nazw

W tym przykładzie zostanie skonfigurowany podstawowy serwer DNS dla domeny **zsp.local**. Nazwa tej domeny nie została zarejestrowana, dlatego dostępna będzie tylko w sieci lokalnej. Aby skonfigurować podstawowy serwer nazw, należy:

1. W pliku **named.conf.local** dodać strefę przeszukiwania „w przód". W tym przykładzie dodano opis strefy **zsp.local**. W opisie strefy **type master** oznacza typ strefy podstawowej, natomiast **file** opisuje ścieżkę do pliku zawierającego bazę danych strefy:

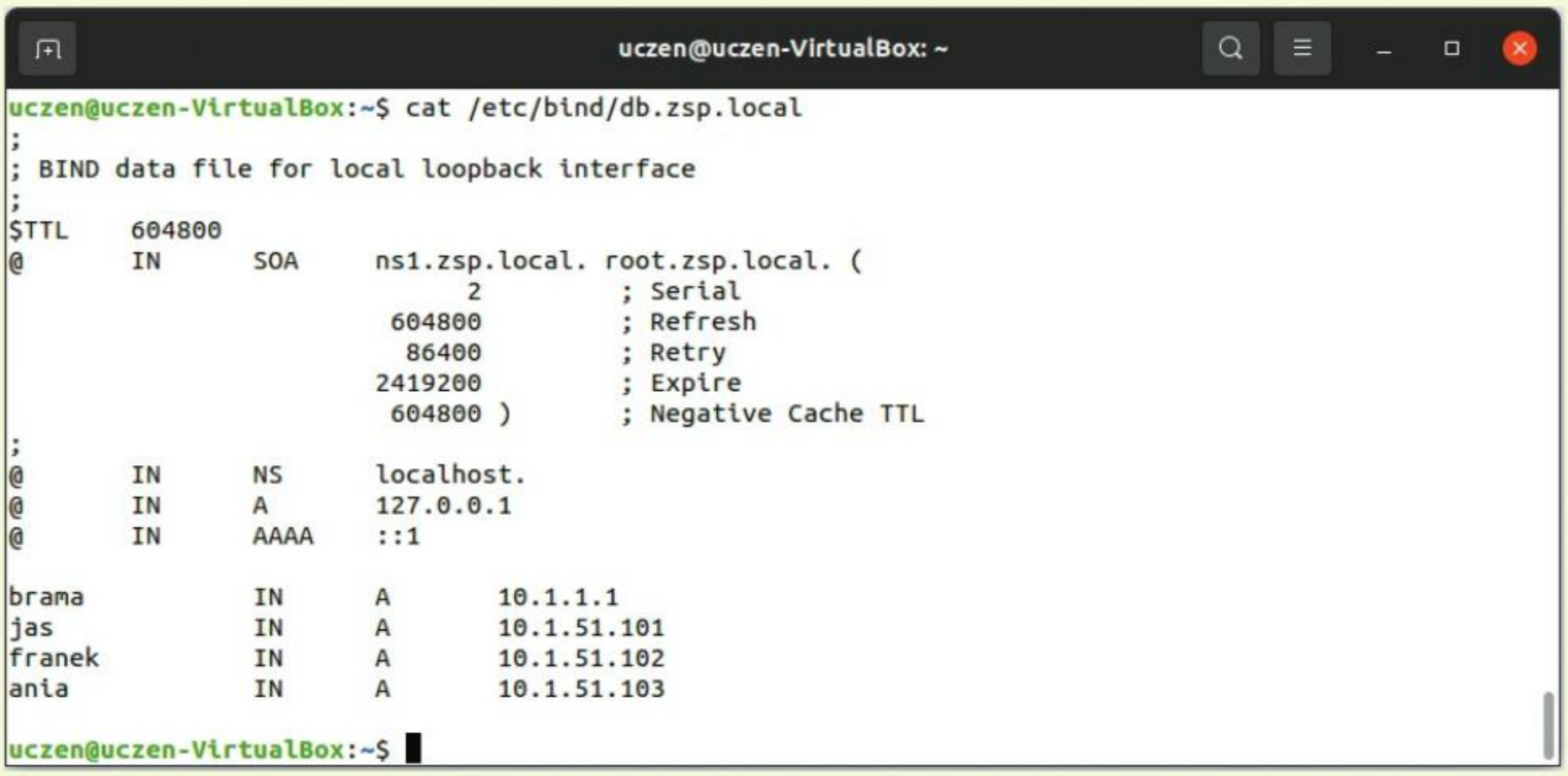
```
zone „zsp.local" IN {
type master;
file „/etc/bind/db.zsp.local";
};
```

   Przykładowy plik **named.conf.local**, zawierający strefę przeszukiwania „w przód" i „wstecz", przedstawiono na rys. 11.6.
2. Utworzyć plik konfiguracji strefy. W katalogu **/etc/bind** są umieszczone przykładowe pliki konfiguracji stref. Można skopiować plik, np. **db.local**, i poddać go modyfikacji. Na rys. 11.4 przedstawiono przykładowy plik konfiguracji strefy przeszukiwania „w przód". W pliku w obszarze SOA wprowadzono nazwę serwera DNS **ns1.zsp.local.** i **root.zsp.local**. (zwróć uwagę na kropkę na końcu nazwy). Pozostałe parametry można pozostawić bez zmian. Ponadto w pliku wprowadzono cztery rekordy typu A (*brama, jas, franek, ania*) wraz z odpowiadającymi

im adresami IP. Po każdym wprowadzeniu zmian w pliku konfiguracyjnym strefy zwiększyć wartość **numeru konfiguracji** (serial) – pozwala to na określenie, który z plików konfiguracji stref ma najbardziej aktualne dane.

3. W pliku **named.conf.local** dodać strefę przeszukiwania „wstecz". W tym przykładzie dodano opis strefy **10.in-addr.arpa**. W opisie strefy opcja **notify no** oznacza, że serwer nie będzie wysyłał powiadomień o zmianach w strefie do innych serwerów, pozostałe opcje mają takie samo znaczenie jak w strefie „w przód":

```
zone „10.in-addr.arpa" {
type master;
notify no;
file „/etc/bind/db.10.in-addr.arpa";
};
```



Rys. 11.4. **Plik konfiguracji strefy przeszukiwania „w przód"**

4. Utworzyć plik konfiguracji strefy. Można skopiować przykładowy plik, np. **db.255**, i poddać go modyfikacji. Na rys. 11.5 przedstawiono przykładowy plik konfiguracji strefy przeszukiwania „wstecz". W pliku w obszarze SOA wprowadzono nazwę serwera DNS **ns1.zsp.local.** i **root.zsp.local.** (zwróć uwagę na kropkę na końcu nazwy). Pozostałe parametry można pozostawić bez zmian. Ponadto w pliku wprowadzono cztery wskaźniki przeszukiwania wstecz dla rekordów *brama, jas, franek, ania* wraz z odpowiadającymi im adresami IP. Po każdym wprowadzeniu zmian w pliku konfiguracyjnym strefy zwiększyć wartość numeru konfiguracji (serial).
5. Uruchomić ponownie demona BIND za pomocą polecenia:

   sudo service bind9 restart.
6. Przetestować działanie serwera. Do testowania serwera DNS w środowisku Linux można użyć polecenia **nslookup**, np. aby sprawdzić adres IP komputera **franek.zsp.local**, należy wydać polecenie:

   nslookup franek.zsp.local.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/bind/db.10.in-addr.arpa
;
; BIND reverse data file for broadcast zone
;
$TTL    604800
@       IN      SOA     ns1.zsp.local. root.zsp.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.

$ORIGIN 10.in-addr.arpa.
1.1.1           IN      PTR     brama.zsp.local.
101.51.1        IN      PTR     jas.zsp.local.
102.51.1        IN      PTR     franek.zsp.local.
103.51.1        IN      PTR     ania.zsp.local.
uczen@uczen-VirtualBox:~$
```

Rys. 11.5. **Plik konfiguracji strefy przeszukiwania „wstecz”**

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "zsp.local" IN {
    type master;
    file "/etc/bind/db.zsp.local";
};

zone "10.in-addr.arpa" IN {
    type master;
    notify no;
    file "/etc/bind/db.10.in-addr.arpa";
};

uczen@uczen-VirtualBox:~$
```

Rys. 11.6. **Plik konfiguracji stref przeszukiwania**

Narzędzie **`nslookup`** może być wykorzystane do testowania strefy „w przód” – jako argument polecenia podaje się nazwę, a serwer DNS zwraca adres IP, lub do testowania strefy „wstecz” – podaje się adres IP, a otrzymuje nazwę. Przykład działania polecenia **`nslookup`** przedstawiono na rys. 11.7.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ nslookup franek.zsp.local
Server:         10.1.51.21
Address:        10.1.51.21#53

Name:   franek.zsp.local
Address: 10.1.51.102

uczen@uczen-VirtualBox:~$ nslookup 10.1.51.102
102.51.1.10.in-addr.arpa        name = franek.zsp.local.

uczen@uczen-VirtualBox:~$
```

Rys. 11.7. **Testowanie DNS za pomocą polecenia `nslookup`**

Serwery zapasowe pobierają dane strefy z **serwera autorytatywnego**. Aktualizowanie tych danych odbywa się w wyniku przesyłania strefy z serwera autorytatywnego. Podczas uruchamiania serwer zapasowy wysyła do podstawowego serwera nazw żądanie przesłania wszystkich danych dla określonej domeny. Strefa jest transferowana tylko w przypadku, gdy numer konfiguracji (serial) strefy serwera podstawowego jest wyższy niż numer konfiguracji (serial) strefy serwera zapasowego. Serwer zapasowy może zażądać zaktualizowanych danych z podstawowego serwera nazw, gdy zostanie powiadomiony o zmianach przez podstawowy serwer nazw (jeśli włączona jest opcja **`notify`**) lub gdy na podstawie zapytań kierowanych do podstawowego serwera nazw wykryje zmianę danych. Do dobrej praktyki administratora należy skonfigurowanie przynajmniej jednego serwera zapasowego dla każdej strefy.

PRZYKŁAD 11.3

KODY

Konfigurowanie zapasowego serwera nazw

W tym przykładzie zostanie skonfigurowany zapasowy serwer DNS dla domeny **`zsp.local`**. Aby skonfigurować zapasowy serwer nazw, należy:

1. Skonfigurować serwer podstawowy tak, aby zezwalał na transfer stref. W pliku **`named.conf.local`** w konfiguracji stref dodać wpis **`allow-transfer`** (rys. 11.8). Ta opcja określa adresy IP serwerów, do których będą wysyłane dane stref.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "zsp.local" IN {
    type master;
    file "/etc/bind/db.zsp.local";
    allow-transfer { 10.1.51.120; };
};

zone "10.in-addr.arpa" IN {
    type master;
    notify no;
    file "/etc/bind/db.10.in-addr.arpa";
    allow-transfer { 10.1.51.120; };
};

uczen@uczen-VirtualBox:~$
```

Rys. 11.8. **Plik konfiguracji podstawowego serwera DNS z możliwością transferu stref**

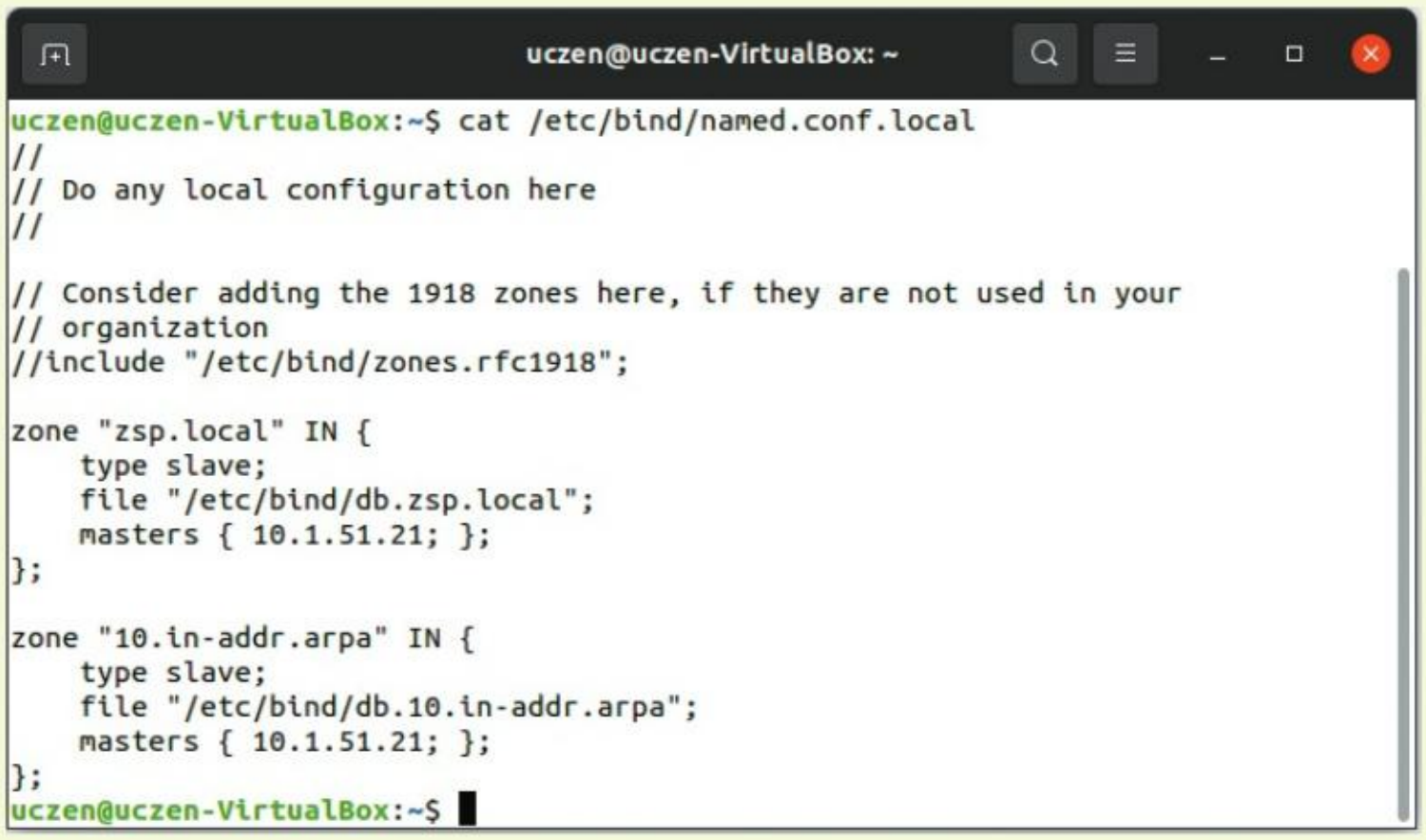
2. Skonfigurować serwer zapasowy tak, aby zezwalał na odbieranie transferu stref z serwera podstawowego. W pliku **`named.conf.local`** w konfiguracji stref dodać wpis **`masters`** (rys. 11.9). Ta opcja określa adresy IP serwerów, z których będą wysyłane dane stref. Ze względu na bezpieczeństwo systemu pliki zawierające kopie bazy danych stref są umieszczane w katalogu **`/var/cache/bind`**.
3. Na obu serwerach uruchomić ponownie demona BIND poleceniem:

   ```
   sudo /etc/init.d/bind9 restart
   ```

4. Sprawdzić w katalogu **`/var/cache/bind`**, czy zostały utworzone pliki stref i czy zawierają opisy stref.

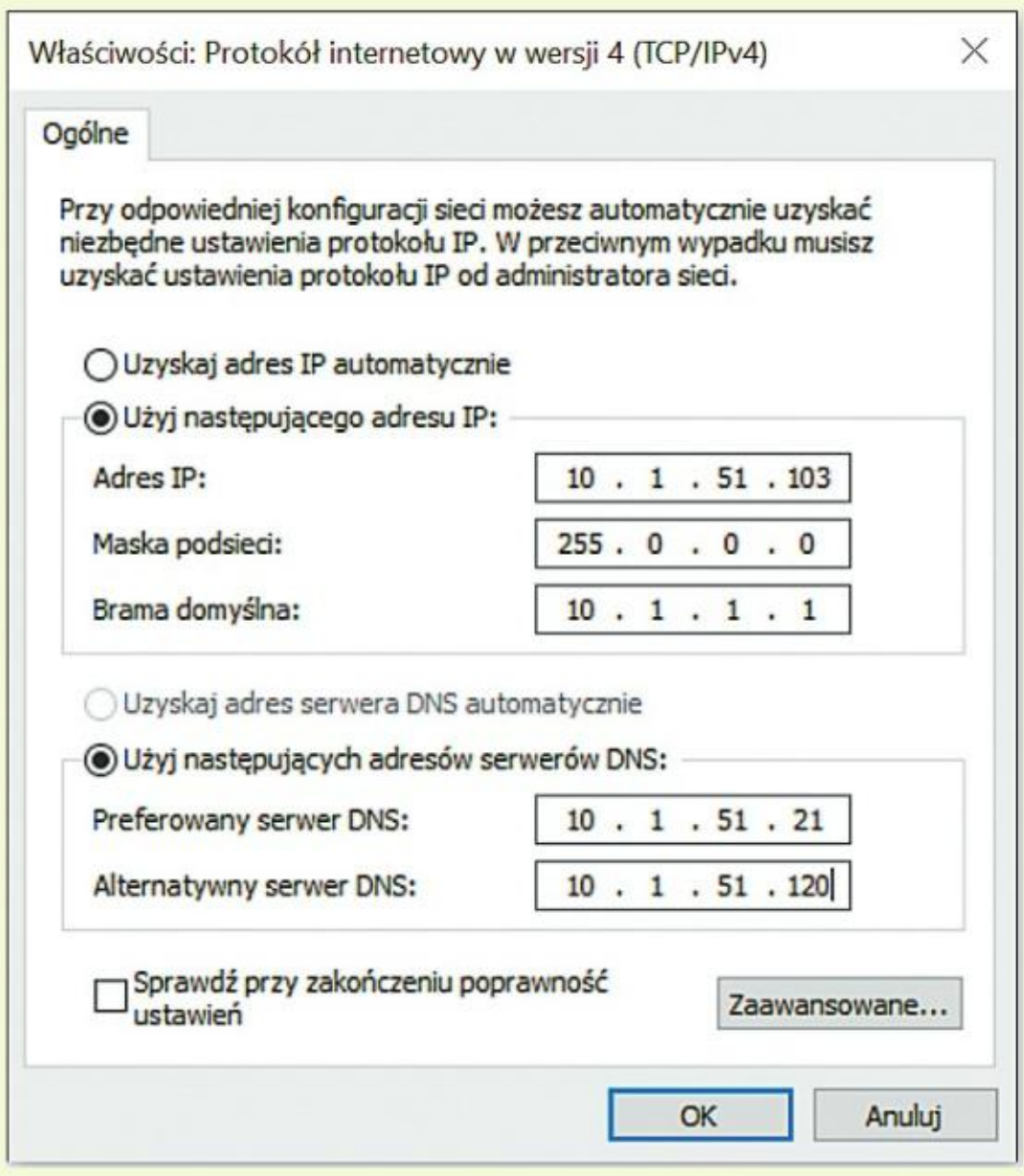
! UWAGA

Poleceniem **`rndc refresh nazwa_domeny`** wydanym na serwerze pracującym w trybie **`slave`** można wymusić transfer strefy, np. **`sudo rndc refresh zsp.local.`**



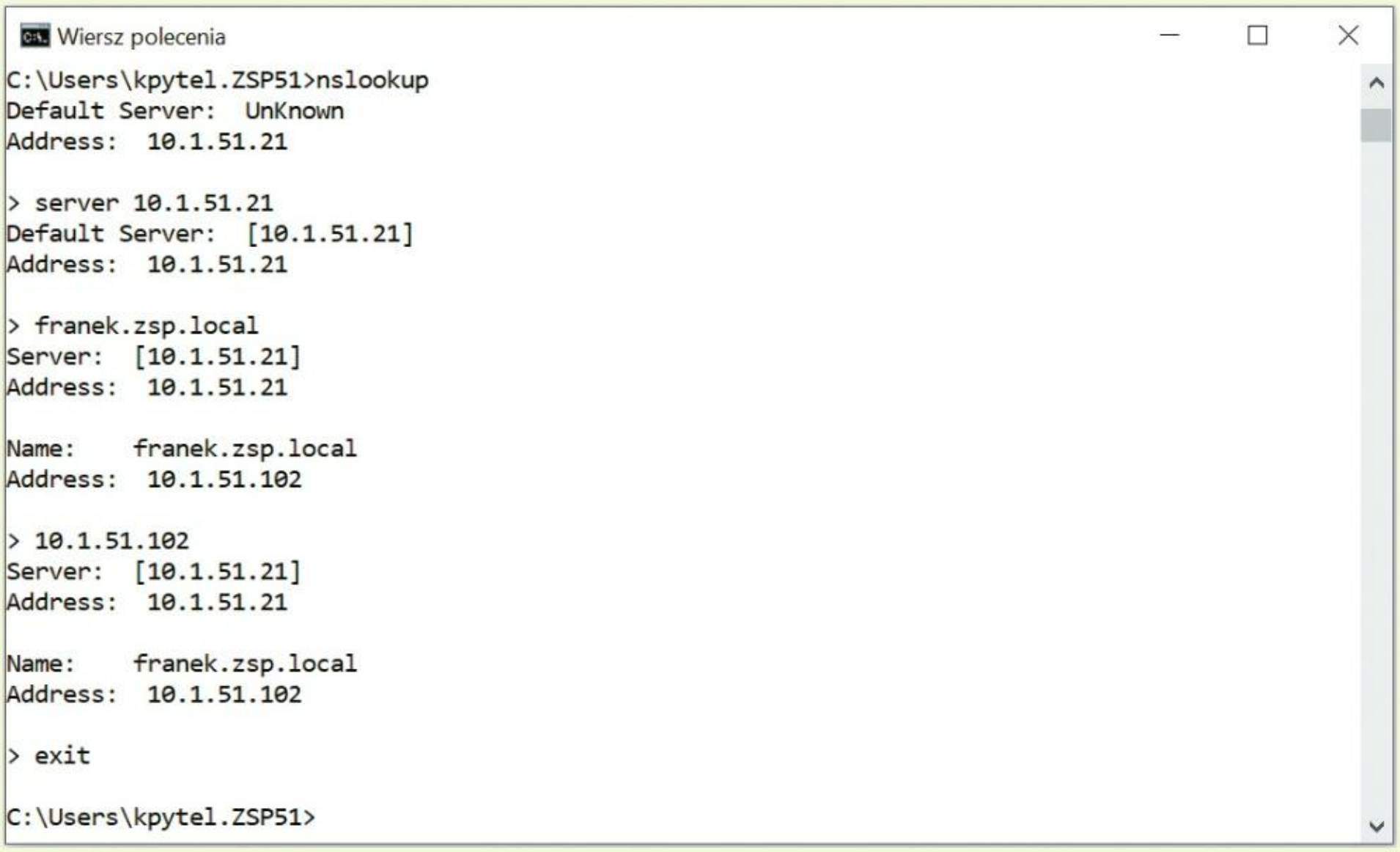
Rys. 11.9. **Plik konfiguracji zapasowego serwera DNS z możliwością odbierania transferu stref**

5. W systemie Windows w oknie konfiguracji protokołu TCP/IP ustawić adres preferowanego i alternatywnego serwera DNS, wpisać adres IP komputerów, odgrywających rolę serwerów DNS (rys. 11.10).



Rys. 11.10. **Konfiguracja adresu serwerów DNS w systemie Windows**

6. Przetestować działanie serwera. Program nslookup może pracować w trybie interaktywnym (rys. 11.11). W pierwszym poleceniu uruchomiono tryb interaktywny programu. W wierszu drugim za pomocą polecenia **`server`** wybrano preferowany serwer (do tego serwera będą wysyłane zapytania). Wprowadzenie nazwy powoduje wysłanie do serwera DNS zapytania o adres IP, natomiast wprowadzenie adresu IP wysyła zapytanie o nazwę. Poprawne wykonanie obu zapytań pozwala na przetestowanie obu stref wyszukiwania. Program zakończono poleceniem **`exit`**.



Rys. 11.11. **Testowanie serwera DNS za pomocą nslookup w trybie interaktywnym**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj serwer buforujący, który obsługuje sieć szkolną.
2. Wykonaj konfigurację i testowanie działania podstawowego i zapasowego serwera DNS dla sieci w twojej szkole.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyjaśnij, jakie typy rekordów są używane do opisywania zasobów w systemie DNS.
2. Wyjaśnij, jaka jest różnica między serwerami DNS buforującym a podstawowym.
3. Wyjaśnij, dlaczego w sieci powinien się znajdować więcej niż jeden serwer DNS.

12 Uruchamianie i korzystanie z usługi FTP

ZAGADNIENIA

Funkcje protokołu FTP **Korzystanie z konta anonimowego na serwerze FTP** **Instalowanie serwera FTP na przykładzie vsftpd** **Podstawowe opcje konfiguracyjne serwera vsftpd** **Nawiązanie i zakończenie połączenia z serwerem FTP** **Użytkownicy lokalni** **Skonfigurowanie serwera vsftpd dla użytkowników lokalnych** **Użytkownik anonimowy** **Skonfigurowanie serwera vsftpd dla użytkowników anonimowych** **Umożliwienie użytkownikom anonimowym zapisywanie danych w wybranym katalogu na serwerze** **Przykładowe opcje konfiguracyjne, w jakie jest wyposażony serwer vsftpd, i sposób korzystania z nich**

FTP (ang. *File Transfer Protocol*) to protokół służący do transmisji plików tekstowych i binarnych w internecie. Działa na podstawie protokołów TCP/IP i wykorzystuje zazwyczaj do transmisji danych port 20, a do kontroli transmisji – port 21.

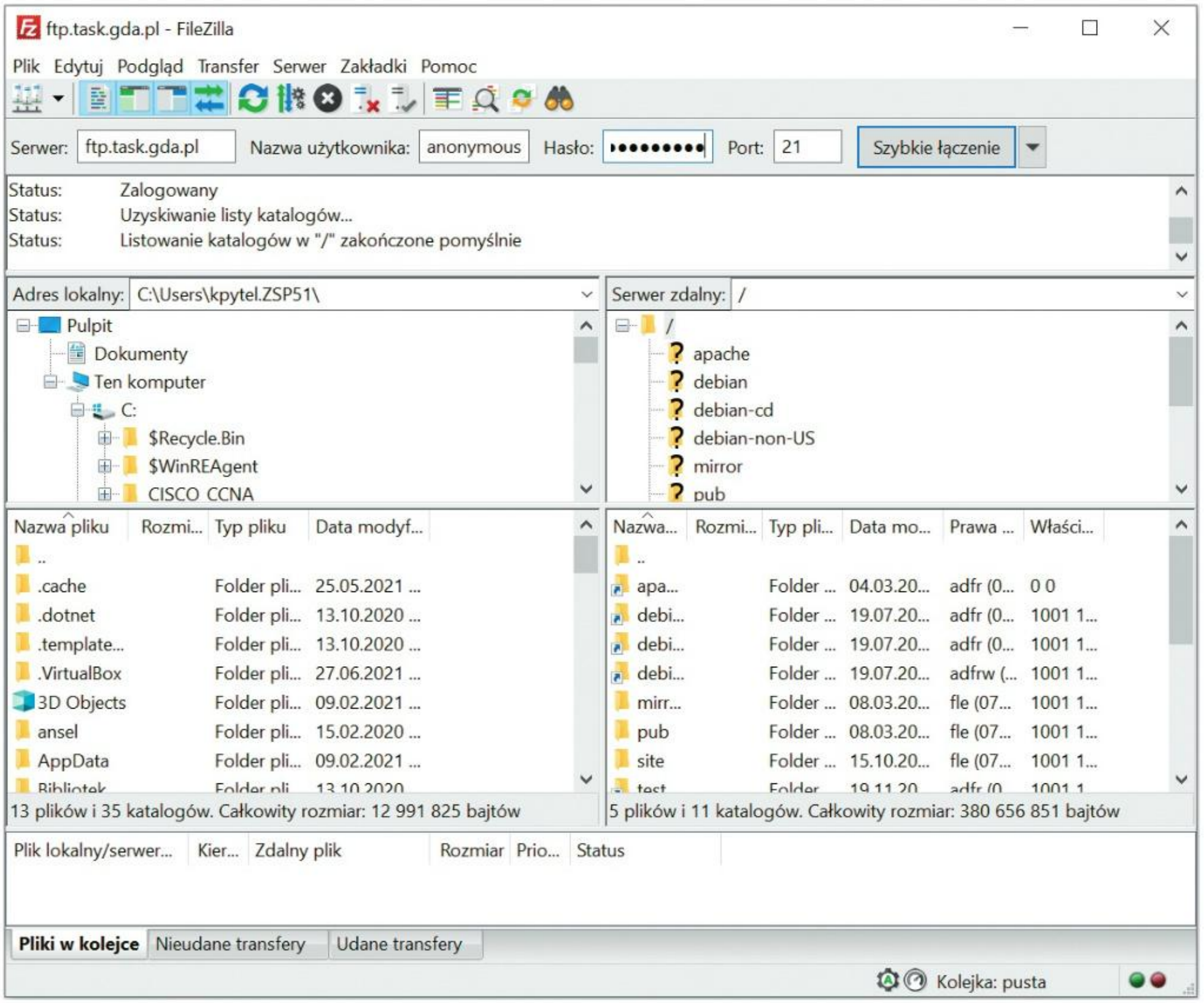
Podstawową zaletą FTP jest to, że rozpoczęty, ale niezakończony pomyślnie, transfer danych może zostać wznowiony aż do uzupełnienia brakujących części pliku. Należy jednak pamiętać, że nie wszystkie serwery oferują tę usługę i nie każdy klient FTP potrafi z niej skorzystać.

Główne wady protokołu to brak możliwości szyfrowania transmisji oraz to, że kanał kontrolny powoduje problemy z implementacją filtrów pakietów na routerach. Pomimo tych wad FTP jest nadal jednym z najpopularniejszych w internecie protokołów przesyłania danych. Działa on na podstawie architektury **klient–serwer**.

Użytkownik łączy się z serwerem FTP za pomocą specjalnego programu, nazywanego **klientem FTP**. W większości systemów operacyjnych jest wbudowany klient FTP pracujący w trybie tekstowym, operacje wykonuje się przez wpisanie odpowiednich poleceń.

Klienta FTP zawierają także przeglądarki internetowe, choć ich możliwości nie dorównują dedykowanym klientom FTP, np. **gFTP** pod Linuksa lub **Filezilla** pod Windows. Klient FTP jest wbudowany także w wiele programów typu menedżer plików, np. **Midnight Commander**.

Współczesne wersje klientów FTP (rys. 12.1) mają okno podzielone na dwie części: po jednej stronie są widoczne katalogi lokalnego komputera (klienta), a po drugiej – katalogi serwera FTP. Kopiowanie plików przez internet sprowadza się wówczas do przeciągnięcia myszą ikony pliku.



Rys. 12.1. **Przykładowy klient FTP**

12.1. Konta użytkowników FTP

Dostęp do zasobów serwera można otrzymać, jeżeli użytkownik ma na tym serwerze **konto lokalne**. Konta są tworzone i zarządzane przez administratora serwera. Administrator decyduje o zakresie uprawnień przyznanych konkretnemu użytkownikowi. Większość serwerów FTP oferuje również **dostęp publiczny** – tzw. anonimowy; identyfikatorem użytkownika jest zazwyczaj „anonymous", a hasłem adres poczty elektronicznej nawiązującego połączenie klienta. Podczas korzystania z konta anonimowego dysponuje się na ogół bardzo ograniczonymi uprawnieniami umożliwiającymi jedynie pobieranie zbiorów z serwera. Tylko niektóre systemy mają oddzielne katalogi przeznaczone na pliki z zewnątrz – są to najczęściej pojedyncze katalogi o nazwie **`upload`** lub **`incoming`**. W tych katalogach można umieścić ciekawy program lub dokument, ale taki plik nie powinien być dostępny dla osób odwiedzających serwer bez sprawdzenia przez administratora serwera i udostępnienia go dla innych użytkowników. Po zalogowaniu się na konto anonimowe użytkownik jest przenoszony do katalogu głównego usługi FTP.

Wspomniany katalog w Ubuntu jest zlokalizowany w **`/srv/ftp`**. Użytkownik zwykle dysponuje w nim tylko uprawnieniami do pobierania plików. Po zalogowaniu się na konto lokalne na serwerze użytkownik jest przenoszony do katalogu domowego. Standardowo w Linuksie jest to katalog **`/home/uzytkownik`**, w którym właściciel dysponuje pełnymi uprawnieniami (pliki można pobierać z serwera, przenosić na serwer, kasować i zarządzać katalogami).

12.2. Instalacja serwera FTP na przykładzie vsftpd w dystrybucji Ubuntu

Zaletami serwera **vsftpd** (ang. *very secure FTP server*) są łatwa konfiguracja (bardzo szybko można postawić wydajny i bezpieczny serwer FTP) i szybkość (transfer jest o wiele większy niż w przypadku innych serwerów FTP). Używa go wiele serwisów FTP.

Aby zainstalować serwer vsftpd za pomocą **apt**, należy wpisać z konta użytkownika polecenie:

```
sudo apt install vsftpd.
```

Po sprawdzeniu zależności między pakietami system wyświetli informacje o pakietach, które należy pobrać i zainstalować. Jeżeli serwer zostanie poprawnie zainstalowany, można przystąpić do jego uruchomienia za pomocą polecenia:

```
sudo service vsftpd start.
```

Aby zatrzymać usługę, należy wpisać polecenie:

```
sudo service vsftpd stop.
```

Jeżeli usługa była wcześniej uruchomiona i dokonamy zmian w konfiguracji, to trzeba ponownie uruchomić usługę. Można to zrobić, wpisując polecenie:

```
sudo service vsftpd restart.
```

Jeżeli podczas uruchamiania usługi nie pojawią się komunikaty o błędach, oznacza to, że serwer działa poprawnie. Konfiguracja dostarczona przez dystrybucję pozwala na wykorzystanie serwera przez większość użytkowników bez konieczności wprowadzania jakichkolwiek zmian w konfiguracji. Jeżeli konfiguracja nie odpowiada użytkownikowi, to można dokonać zmian.

Zanim przystąpi się do konfiguracji serwera, należy sprawdzić, czy usługa jest dostępna. W tym celu można użyć narzędzia **Nmap**.

PRZYKŁAD 12.1

Instalowanie serwera vsftpd

Aby zainstalować serwer vsftpd, należy:

1. Zalogować się na konto użytkownika.
2. Zainstalować serwer za pomocą polecenia:
   ```
   sudo apt install vsftpd.
   ```
3. Uruchomić usługę za pomocą polecenia:
   ```
   sudo service vsftpd start.
   ```
4. Sprawdzić, czy usługa jest uruchomiona – wydać polecenie:
   ```
   nmap localhost.
   ```

12.3. Konfiguracja serwera vsftpd

Głównym plikiem konfiguracyjnym serwera vsftpd jest **/etc/vsftpd.conf**. Opcje konfiguracyjne są zapisywane w formacie **opcja=wartość**. Między nazwą opcji a znakiem = oraz wartością opcji nie umieszczamy spacji. W pliku konfiguracyjnym istotna jest również wielkość liter. Wszystkie linie rozpoczynające się od znaku # są komentarzami, które nie mają wpływu na działanie serwera, a jedynie wyjaśniają, do czego służą poszczególne opcje. Podstawowe opcje konfiguracyjne serwera umożliwiające dostosowanie jego działania do potrzeb użytkownika:

```
# Zezwolenie na logowanie anonimowych użytkowników:
anonymous_enable=YES
# Zezwolenie logowania dla lokalnych użytkowników:
local_enable=YES
# Pozwolenie na zapis we własnym katalogu:
write_enable=YES
# Banner, który będzie wyświetlany podczas każdego połączenia z serwerem:
ftpd_banner=Prywatny serwer FTP - Powered by: vsftpd
```

Po uruchomieniu serwera możemy wykonać próbę nawiązania połączenia (rys. 12.2).

Rys. 12.2. **Logowanie na konto lokalne serwera FTP**

12.4. Konfiguracja serwera FTP do obsługi użytkowników lokalnych

Przed rozpoczęciem konfiguracji serwera zaleca się skopiowanie oryginalnego pliku konfiguracyjnego. Gdyby po dokonaniu zmian w konfiguracji serwer nie mógł się uruchomić, będzie można przywrócić jego wcześniejsze ustawienia.

Użytkownicy lokalni to ci, którzy mają na serwerze swoje konta. Aby otrzymać takie konto, należy zwrócić się do administratora z prośbą o jego założenie. Użytkownicy lokalni na ogół mają uprawnienia do zapisywania danych w swoich katalogach lokalnych (usługa niedostępna dla użytkowników anonimowych). W konfiguracji dostarczanej z dystrybucją opcja korzystania z kont lokalnych jest standardowo włączona. Jeżeli serwer ma być dostępny dla użytkowników lokalnych, należy upewnić się, że jest włączona opcja zezwalająca na logowanie się użytkowników lokalnych. W tym celu trzeba ustawić wartość opcji **`local_enable=YES`**.

Po wprowadzeniu zmian w konfiguracji trzeba zapisać plik konfiguracyjny i ponownie uruchomić serwer za pomocą polecenia: **`sudo service vsftpd restart`**.

PRZYKŁAD 12.2

Konfigurowanie serwera vsftpd tylko dla użytkowników lokalnych

Aby umożliwić logowanie do serwera vsftpd tylko użytkownikom lokalnym, należy:

1. Zalogować się na konto użytkownika.
2. Sporządzić kopię zapasową pliku konfiguracyjnego za pomocą polecenia:

   `sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.old.`

3. Zmodyfikować plik konfiguracyjny **`/etc/vsftpd.conf`** (ustawić wartość opcji **`anonymous_enable=NO`** i **`local_enable=YES`**).
4. Zapisać zmiany w pliku i ponownie uruchomić usługę za pomocą polecenia:

   `sudo service vsftpd restart`.

5. Sprawdzić poprawność konfiguracji przez wykonanie próby logowania – skorzystać z konta anonimowego i lokalnego.

12.5. Konfiguracja serwera FTP do obsługi użytkowników anonimowych

Z konta anonimowego może korzystać każdy, ale standardowo uprawnienia na ogół są ograniczone tylko do pobierania danych. Hasłem do konta anonimowego jest adres e-mail użytkownika. Niektóre serwery sprawdzają, czy wpisane hasło jest poprawnym adresem poczty elektronicznej. W konfiguracji dostarczanej z dystrybucją opcja korzystania z konta anonimowego jest standardowo wyłączona. Jeżeli serwer ma być dostępny tylko dla użytkowników anonimowych, należy wyłączyć opcję zezwalającą na logowanie się użytkowników lokalnych. W tym celu trzeba ustawić wartość opcji **`local_enable=NO`** i **`anonymous_enable=YES`**.

Po wprowadzeniu zmian w konfiguracji trzeba zapisać plik konfiguracyjny i ponownie uruchomić serwer za pomocą polecenia:

`sudo service vsftpd restart.`

PRZYKŁAD 12.3

Konfigurowanie serwera vsftpd tylko dla użytkowników anonimowych

Aby umożliwić logowanie do serwera vsftpd tylko użytkownikom anonimowym, należy:

1. Zalogować się na konto użytkownika.
2. Zmodyfikować plik konfiguracyjny **`/etc/vsftpd.conf`** (ustawić wartość opcji **`local_enable=NO`**).
3. Zmodyfikować plik konfiguracyjny **`/etc/vsftpd.conf`** (ustawić wartość opcji **`anonymous_enable=YES`**).
4. Zapisać zmiany w pliku i ponownie uruchomić usługę za pomocą polecenia:

   `sudo service vsftpd restart`

5. Sprawdzić poprawność konfiguracji przez wykonanie próby logowania – skorzystać z konta anonimowego i lokalnego.

12.6. Zapisywanie danych na serwerze przez użytkowników anonimowych

Standardowo użytkownicy anonimowi mają uprawnienia ograniczone tylko do pobierania danych. W szczególnych okolicznościach można im umożliwić zapisywanie danych na serwerze, ale tylko w wybranym przez administratora katalogu, przeznaczonym do tego celu. Programy i dokumenty umieszczone na serwerze przez użytkowników anonimowych mogą stanowić poważne **zagrożenie dla bezpieczeństwa** (wirusy, konie trojańskie itp.).

Trzeba zadbać również o to, aby administrowany serwer nie stał się punktem dystrybucji **nielegalnego oprogramowania** lub innych **niedozwolonych treści**. Jeżeli anonimowy użytkownik skopiuje na serwer dowolny plik, to nie może mieć prawa do jego ponownego pobrania, skasowania lub modyfikacji. Najlepiej, aby w ogóle nie mógł przeglądać zawartości tego katalogu. Każdy z takich plików powinien zostać sprawdzony przez administratora pod kątem legalności i zawartych w nim treści. Jeśli administrator uzna plik za bezpieczny, może udostępnić go wszystkim użytkownikom, przenosząc go do katalogu, z którego będzie go można pobierać.

Aby umożliwić użytkownikom anonimowym zapisywanie danych w wybranym katalogu, należy taki katalog utworzyć w miejscu, do którego anonimowi użytkownicy usługi FTP będą mogli uzyskać dostęp. Dobrym miejscem może być katalog domowy użytkownika FTP (konto jest tworzone podczas instalacji serwera vsftpd i wykorzystywane przez serwer do uzyskiwania dostępu do systemu). Katalog domowy tego użytkownika można utworzyć w **`/srv/ftp`**.

PRZYKŁAD 12.4

Udostępnianie prawa zapisu użytkownikom anonimowym

Aby udostępnić prawa zapisu katalogu użytkownikom anonimowym, należy dokonać następującej modyfikacji:

1. Zalogować się na konto użytkownika.
2. Utworzyć katalog **`/srv/ftp/upload`** za pomocą polecenia:
   `sudo mkdir /srv/ftp/upload.`
3. Zmienić katalog na **`/srv/ftp`** za pomocą polecenia:
   `sudo cd /var/ftp.`
4. Zmienić właściciela katalogu na FTP i grupę FTP za pomocą polecenia:
   `sudo chown ftp:ftp upload.`
5. Nadać uprawnienia do katalogu za pomocą polecenia:
   `sudo chmod 300 upload.`
6. W pliku konfiguracyjnym **`vsftpd.conf`** zmodyfikować lub dodać następujące opcje:
   # Pozwolenie na zapis w domowym folderze:
   `write_enable=YES`
   # Zezwolenie na upload plików:
   `anon_upload_enable=YES`
   # Pozwolenie anonimowemu użytkownikowi na tworzenie nowych katalogów:
   `anon_mkdir_write_enable=YES`
   # Pozwolenie na modyfikację plików / katalogów (nadpisywanie / kasowanie / zmiana nazwy):
   `anon_other_write_enable=YES`
   Po restarcie serwera FTP anonimowi użytkownicy będą mogli zapisywać pliki i tworzyć katalogi w katalogu **`upload`**, ale nie będą widzieli zawartości tego katalogu.

12.7. Inne opcje konfiguracyjne serwera FTP

W serwerze vsftpd występuje bardzo wiele opcji konfiguracyjnych pozwalających dostosować go do potrzeb użytkownika i administratora. Poniżej przedstawiono wybrane opcje (rys. 12.3).

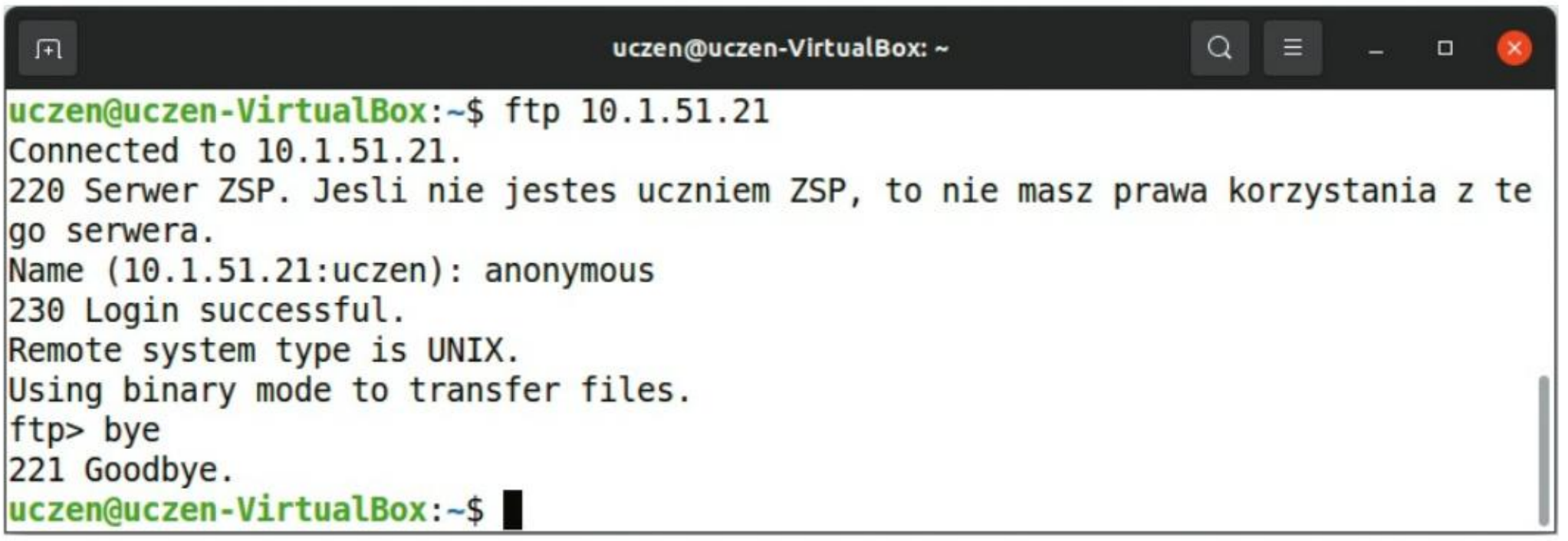
Zezwolenie na logowanie anonimowych użytkowników bez podawania hasła:

```
no_anon_password=YES
```

Komunikat wyświetlany przed zalogowaniem się na konto:

```
ftpd_banner=Serwer ZSP. Jesli nie jestes uczniem ZSP, to nie masz
prawa korzystania z tego serwera.
```

KODY



Rys. 12.3. **Logowanie bez podawania hasła**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Jako administrator serwera FTP umieść w katalogu **pub** plik przeznaczony do pobierania przez użytkowników anonimowych.
2. Jako użytkownik anonimowy pobierz plik z katalogu **pub** za pomocą klienta z wiersza polecenia, przeglądarki internetowej, programu Midnight Commander i specjalnego klienta FTP (np. gFTP). Jeżeli program gFTP nie jest jeszcze zainstalowany, można to zrobić za pomocą polecenia **sudo apt install gftp**.
3. Skorzystaj z konta użytkownika anonimowego i skopiuj plik **nazwisko.txt** do udostępnionego na serwerze katalogu **upload**. Wykonaj kopiowanie – skorzystaj z wiersza polecenia, przeglądarki internetowej, programu Midnight Commander i specjalnego klienta FTP (np. gFTP).
4. Jako administrator serwera sprawdź zawartość skopiowanych plików pod kątem legalności oraz zawartości i przenieś je do katalogu **pub** zawierającego pliki udostępniane klientom anonimowym.
5. Zmodyfikuj plik konfiguracyjny tak, aby umożliwić logowanie tylko użytkownikom anonimowym.

6. Zmodyfikuj plik konfiguracyjny tak, aby umożliwić logowanie tylko użytkownikom lokalnym.
7. Zmodyfikuj plik konfiguracyjny tak, aby umożliwić zapisywanie plików na serwerze użytkownikom anonimowym.
8. Skonfiguruj serwer tak, aby wyświetlał komunikat powitalny.
9. Skonfiguruj serwer tak, aby użytkownicy anonimowi nie musieli podawać hasła podczas logowania.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Co jest standardowym hasłem używanym do zalogowania się na serwer FTP przez użytkownika anonimowego (anonymous)?
2. Podaj powody, dla których warto używać klienta FTP zamiast klienta z wiersza poleceń.
3. Jakie zagrożenia może powodować udostępnianie zapisu na serwerze FTP dla użytkowników anonimowych?
4. Jakie rozwiązania można zastosować, aby zmniejszyć zagrożenie związane z udostępnianiem zapisu na serwerze FTP dla użytkowników anonimowych?

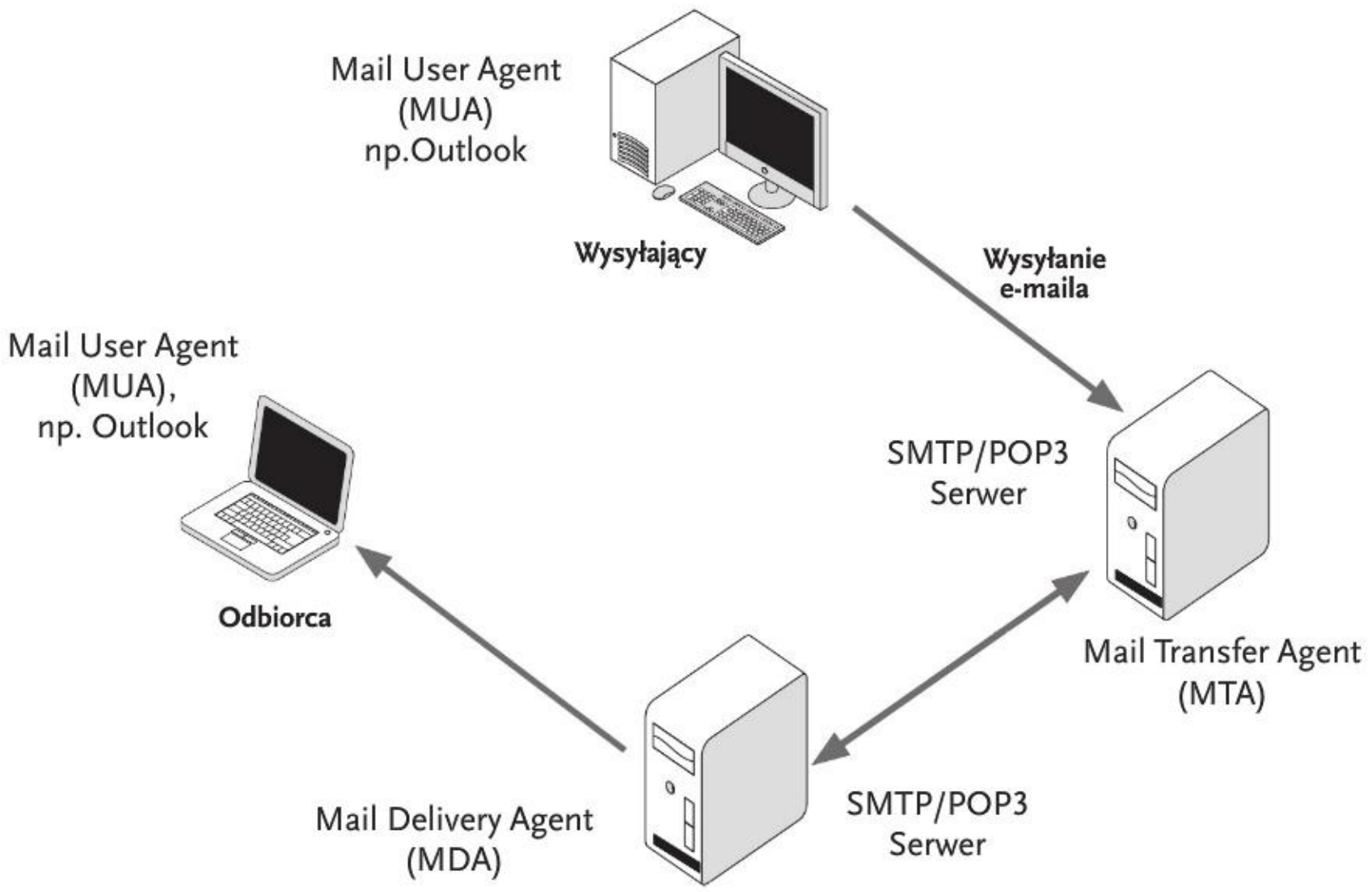
13 Konfiguracja serwera poczty elektronicznej

ZAGADNIENIA

Zainstalowanie i skonfigurowanie serwera pocztowego **Wysyłanie i odbieranie wiadomości e-mail**

Poczta elektroniczna (ang. *e-mail*) opiera się na przekazywaniu informacji w postaci tekstów między użytkownikami sieci. Działanie poczty elektronicznej polega na przesyłaniu korespondencji między serwerami pocztowymi i klientami. Sposób komunikacji przedstawiono na rys. 13.1. Na stacji roboczej wysyłającego jest uruchomiony **Mail User Agent** (MUA) – program przeznaczony do wysyłania i odbierania wiadomości pocztowych. Przykładami programów typu MUA są **Outlook**, **Thunderbird** i wiele innych. Wiadomość za pomocą protokołu **SMTP** (ang. *Simple Mail Transfer Protocol*) jest przesyłana do serwera skonfigurowanego jako **serwer poczty wychodzącej**. Na serwerze jest uruchomione oprogramowanie **Mail Transfer Agent** (MTA).

MTA na podstawie adresu wiadomości i własnej listy odbiorców podejmuje decyzję, czy wiadomość powinna być przekazana do skrzynki odbiorcy (jeżeli adresat ma skrzynkę na tym serwerze). Jeżeli odbiorca nie ma skrzynki na tym serwerze, MTA przesyła wiadomość do innego serwera. Za pomocą protokołu SMTP wiadomość dociera do serwera, na którym jest skonfigurowana skrzynka adresata.



Rys. 13.1. Dostarczanie poczty elektronicznej

Mail Delivery Agent (MDA) uruchomiony na tym serwerze dostarcza wiadomość do skrzynki pocztowej adresata. Adresat za pomocą programu pocztowego (MUA) uruchomionego na swoim komputerze może w dowolnym momencie połączyć się z serwerem za pomocą protokołu **POP3** (ang. *Post Office Protocol*) lub **IMAP** (ang. *Internet Messages Access Protocol*) i pobrać wiadomości ze skrzynki.

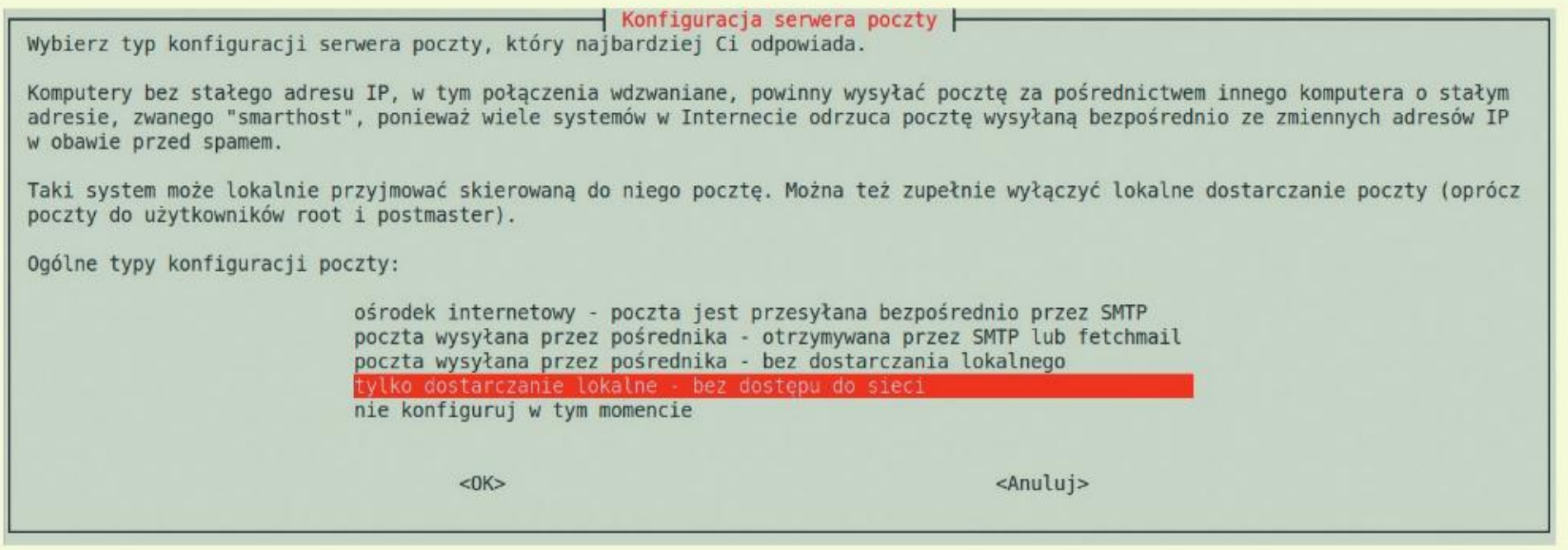
PRZYKŁAD 13.1

Instalacja serwera pocztowego na przykładzie Exim

W tym ćwiczeniu zostanie zainstalowany serwer poczty elektronicznej obsługujący sieć lokalną. Skonfigurowane będą tylko podstawowe funkcje serwera bez szyfrowania i uwierzytelniania.

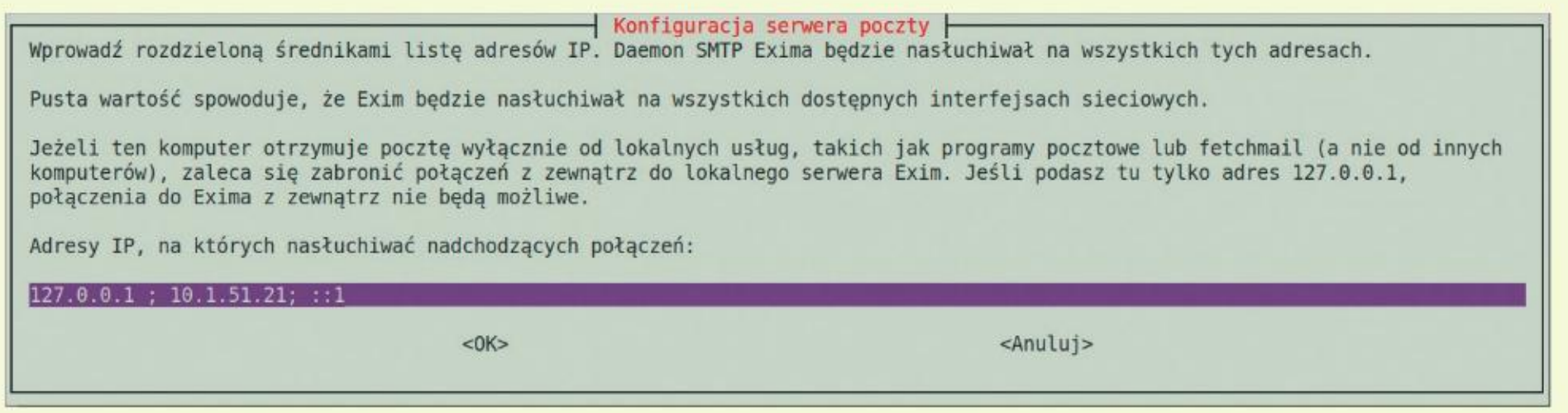
Aby zainstalować i skonfigurować serwer, należy:

1. Zalogować się na konto użytkownika.
2. Zainstalować oprogramowanie serwera – wydać polecenie:
   `sudo apt install exim4.`
3. Uruchomić kreatora konfiguracji serwera za pomocą polecenia:
   `sudo dpkg-reconfigure exim4-config.`
4. Wybrać typ konfiguracji serwera – **tylko dostarczanie lokalne - bez dostępu do sieci** (rys. 13.2.) Klawiszem [Tab] wybrać opcję **OK**.



Rys. 13.2. **Wybór typu konfiguracji serwera**

5. Wprowadzić nazwę domeny, w której pracuje serwer, i wybrać **OK** (można wpisać **`zsp.local`**).
6. Wprowadzić adres IP, na którym serwer będzie nasłuchiwał nadchodzących połączeń (rys. 13.3), i wybrać **OK**.



Rys. 13.3. **Wprowadzanie adresu IP, na którym nasłuchuje serwer**

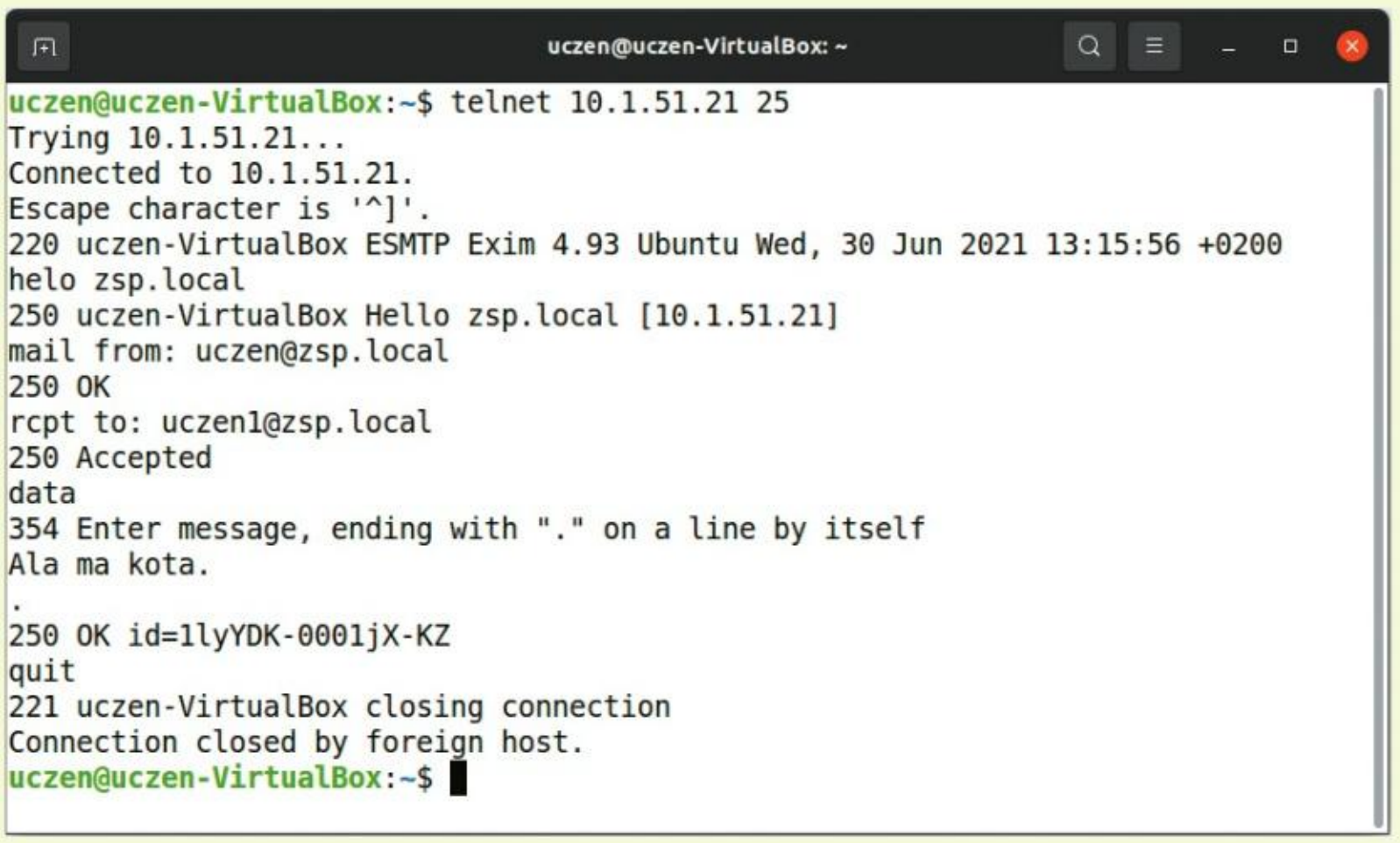
7. Wprowadzić listę domen, dla których serwer jest miejscem docelowym (można wpisać **`zsp.local`**).
8. Dla opcji **`Utrzymywać ilość zapytań DNS na minimalnym poziomie`** wybrać opcję **`Nie`**.
9. Format dostarczania poczty lokalnie – wybrać **`mbox w /var/mail`**.
10. Nie dzielić konfiguracji na małe pliki – wybrać **`Nie`**.
11. W polu **`Odbiorca poczty dla kont root i postmaster`** wprowadzić nazwę własnego konta na serwerze, np. **`uczen`**.
12. Po zakończeniu działania kreatora uruchomić ponownie serwer za pomocą polecenia: **`sudo service exim4 restart`**.

PRZYKŁAD 13.2

Wysyłanie wiadomości tekstowej

Podczas normalnej pracy oprogramowanie klienta poczty elektronicznej wykonuje wszystkie procedury związane z obsługą wysyłania i pobierania wiadomości e-mailowych. W ćwiczeniu zostanie wysłany e-mail z wykorzystaniem wiersza poleceń i protokołu telnet. W tym celu należy:

1. Zalogować się na konto dowolnego użytkownika.
2. Za pomocą telnetu połączyć się z serwerem na porcie 25.
3. Rozpocząć komunikację za pomocą polecenia:
   `helo zsp.local`
4. Wprowadzić nazwę nadawcy wiadomości, np.:
   `mail from: uczen@zsp.local`
5. Wprowadzić nazwę odbiorcy wiadomości, np.:
   `rcpt to: uczen1@zsp.local`
6. Wprowadzić polecenie **`data`** i przejść do trybu pisania wiadomości. Pisanie wiadomości zakończyć kropką (**`.`**) w oddzielnej linii.
7. Zakończyć sesję – wydać polecenie **`quit`**. Przebieg ćwiczenia przedstawiono na rys. 13.4.



Rys. 13.4. **Procedura wysyłania e-maila**

PRZYKŁAD 13.3

Odbieranie wiadomości e-mail

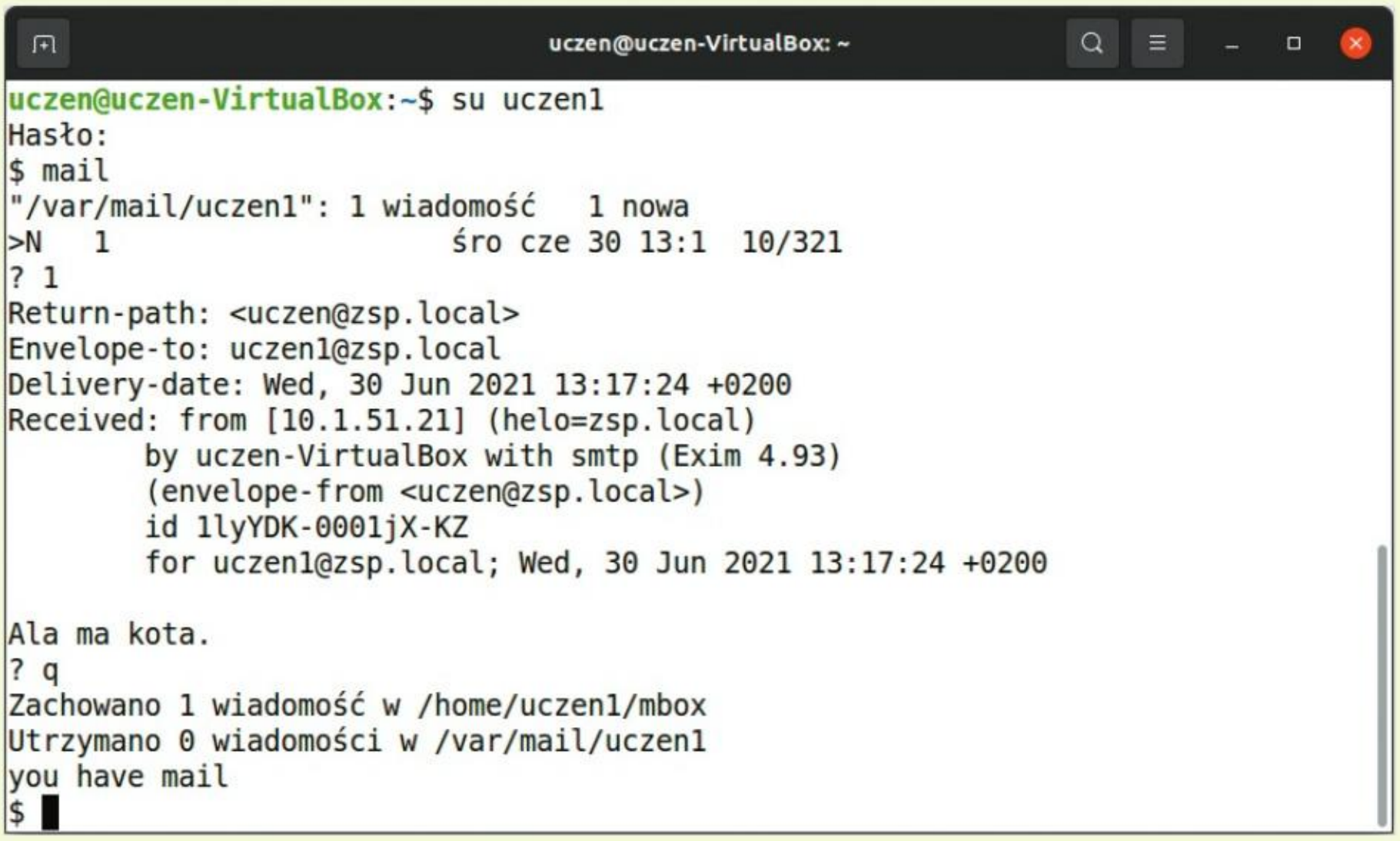
Wiadomości e-mail można również odczytać za pomocą telnetu, ale wygodniej to robić za pomocą programu **mail**.

Aby odczytać wiadomość, należy:

1. Zainstalować program za pomocą polecenia:

   ```
   sudo apt install mailutils
   ```

2. Zalogować się na konto odbiorcy wiadomości lub zmienić konto – wydać polecenie **su**, np. **su uczen1**.
3. Wywołać polecenie **mail**.
4. Na liście wiadomości sprawdzić numer wiadomości, która ma być odczytana.
5. Wpisać numer wiadomości i nacisnąć [Enter].
6. Po przeczytaniu wiadomości zakończyć pracę programu – wydać polecenie **q** (rys. 13.5).



Rys. 13.5. **Odbieranie wiadomości e-mail**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj na swoim serwerze skrzynkę pocztową dla koleżanki / kolegi. Przetestuj możliwość wysyłania i odbierania wiadomości.
2. Wyszukaj w internecie, np. na stronie https://www.wikihow.com/Check-Email-with-Telnet, informacje o sposobie odbierania wiadomości e-mail za pomocą telnetu. Sprawdź możliwość odbierania wiadomości z serwera pocztowego za pomocą telnetu.

14 Uruchamianie usługi WWW

ZAGADNIENIA

Funkcja usługi WWW **Udostępnianie katalogów na serwerze WWW** **Instalowanie i uruchamianie serwera WWW** **Najważniejsze pliki konfiguracyjne serwera httpd** **Zainstalowanie i uruchomienie serwera Apache2** **Umieszczanie stron WWW w katalogu głównym serwera** **Systemy operacyjne rozróżniające wielkości liter w nazwach plików i folderów** **Włączenie udostępniania katalogów domowych użytkowników** **Konfigurowanie serwera Apache2 do udostępniania stron domowych użytkowników** **Wirtualne serwery WWW i korzyści z ich konfigurowania** **Przebieg procedury konfigurowania wirtualnych serwerów WWW** **Konfigurowanie serwera Apache2 do blokowania listowania zawartości katalogu zawierającego strony domowe użytkowników** **Wprowadzenie ochrony dostępu do udostępnianego katalogu za pomocą hasła** **Doinstalowanie modułu PHP5** **Skonfigurowanie serwera Apache2 do obsługi języka PHP** **Logi serwera** **Funkcje zmiennych ErrorLog i LogLevel** **Przeglądanie logów serwera**

Usługa WWW (ang. *World Wide Web*) jest hipertekstowym, multimedialnym, sieciowym systemem informacyjnym opartym na publicznie dostępnych, otwartych standardach. Podstawowym zadaniem WWW jest publikowanie informacji. Aby uzyskać dostęp do tak udostępnianej informacji, trzeba posłużyć się **przeglądarką internetową**. Przeglądarka łączy się z **serwerem WWW**, skąd pobiera pewien zbiór informacji, określany jako **strona internetowa**. Strona internetowa może zostać wyświetlona, zapisana w lokalnym systemie plików lub wydrukowana. Usługa działa na podstawie architektury klient–serwer.

14.1 Udostępniane katalogi

Serwer WWW może udostępniać pojedynczą witrynę internetową. Pobieranie danych z takiej witryny polega na wpisaniu w pole adresu przeglądarki internetowej nazwy serwera lub jego adresu IP. W serwerach z zainstalowanym systemem Linux, katalogiem głównym, w którym domyślnie są przechowywane witryny, jest **`/var/www`**. Przeglądanie stron internetowych rozpoczyna się od pliku **`index.html`** (w niektórych systemach może to być: **`index.htm`**, **`default.html`**, **`default.htm`**, **`index.php`**). Jeżeli w katalogu głównym witryny znajduje się plik **`index.html`**, to po wpisaniu adresu witryny zostanie pobrany (wraz z innymi zależnymi plikami).

Przeglądarka **interpretuje** treść pobranych plików, **scala** i **wyświetla** jako dokument hipertekstowy. Jeżeli nazwa pliku jest inna, to należy w adresie podać nazwę pliku, który ma być wyświetlony. Inne witryny internetowe mogą być umieszczane w podkatalogach katalogu głównego. W takim przypadku, aby wyświetlić odpowiednią witrynę w polu adresu, trzeba podać nazwę komputera i ścieżkę dostępu (należy rozpocząć od katalogu głównego witryny WWW).

Serwer WWW może udostępniać również wiele witryn internetowych, wykorzystując „wirtualne serwery". Każdy z takich **wirtualnych serwerów** może być identyfikowany za pomocą innej nazwy, adresu IP lub numeru portu. Położenie katalogu głównego takiej witryny jest określane przez administratora serwera WWW. Na serwerze WWW mogą być udostępniane również witryny użytkowników mających konta w systemie. W serwerach z zainstalowanym systemem Linux każdy z użytkowników może udostępniać swoje witryny w specjalnie do tego celu przeznaczonym katalogu **public_html** (jeżeli konfiguracja serwera na to zezwala). Katalog **public_html** jest umieszczany w katalogu domowym użytkownika **/home/nazwa_uzytkownika**.

14.2. Instalacja serwera WWW

Większość dystrybucji Linuksa standardowo zawiera oprogramowanie umożliwiające uruchomienie serwera WWW. Podczas instalacji Linuksa ten serwer może być zainstalowany domyślnie. Jeżeli podczas instalacji serwer WWW nie został zainstalowany, można go doinstalować w dowolnym momencie. Do instalacji pakietów serwera należy wykorzystać menedżer pakietów **apt**. Polecenie:

```
sudo apt install apache2
```

spowoduje zainstalowanie serwera i dodatków niezbędnych do jego pracy.

14.3. Uruchamianie serwera WWW

Serwer WWW można uruchomić za pomocą polecenia **service**, np. aby uruchomić serwer, należy wpisać polecenie:

```
sudo service apache2 start.
```

W celu zatrzymania usługi należy wydać polecenie:

```
sudo service apache2 stop.
```

Jeżeli usługa była wcześniej uruchomiona i dokonamy zmian w konfiguracji, należy uruchomić usługę ponownie. Można to zrobić dzięki poleceniu:

```
sudo service apache2 restart.
```

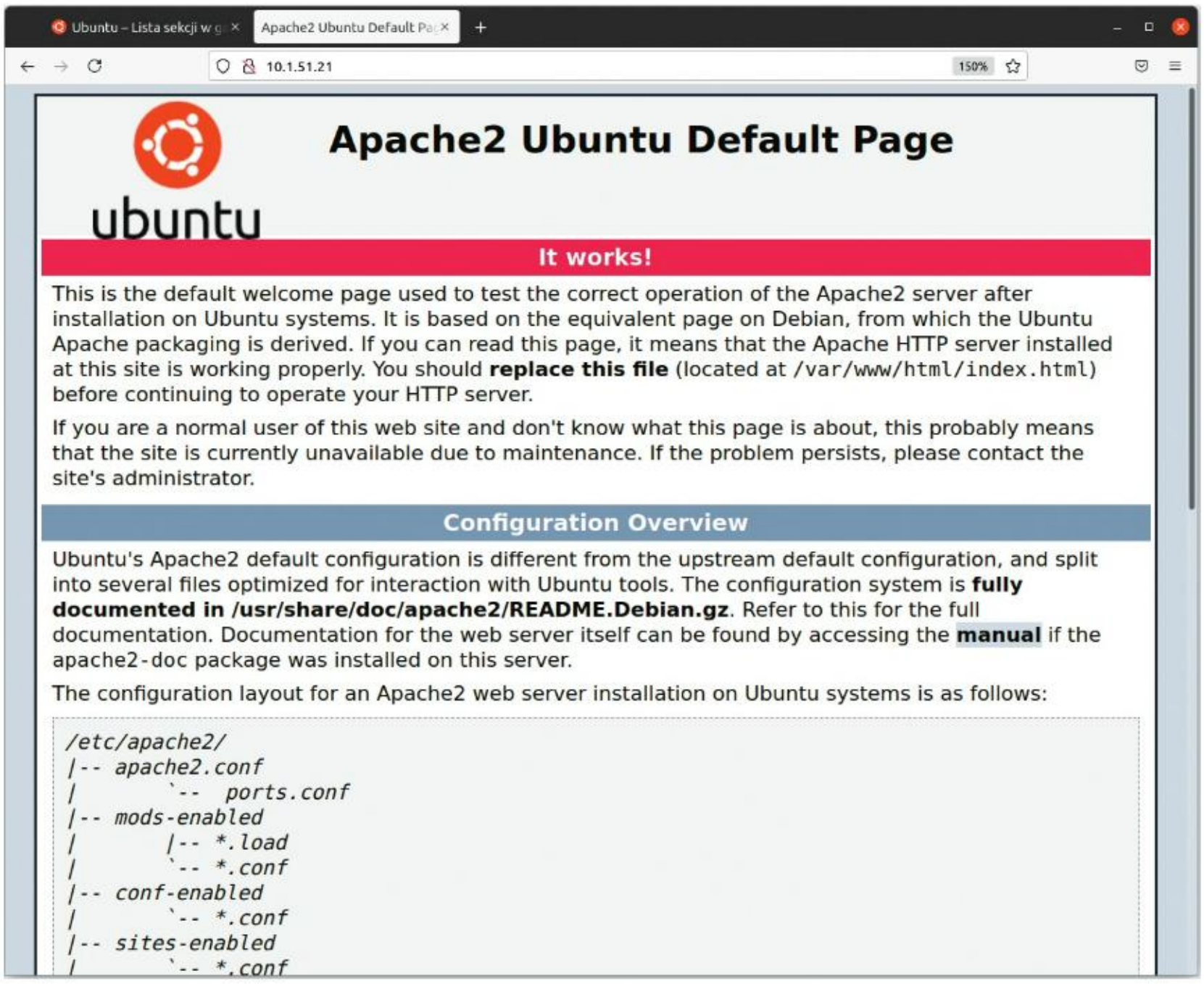
Konfiguracja dostarczona przez dystrybucję pozwala na wykorzystanie serwera przez większość użytkowników bez konieczności dokonywania jakichkolwiek zmian w konfiguracji. Jeżeli ta konfiguracja nie jest odpowiednia, można ją zmienić.

14.4. Konfiguracja serwera Apache

Pliki konfiguracyjne serwera są zlokalizowane w katalogu **/etc/apache2**. Głównym plikiem konfiguracyjnym jest **apache2.conf**, w którym oprócz opcji konfiguracyjnych znajdują się odnośniki do innych plików konfiguracyjnych, np. **httpd.conf**, **ports.conf**. W pliku **httpd.conf** będą umieszczane wpisy użytkownika, plik **ports.conf** pozwala na zdefiniowanie wirtualnych serwerów. Wszystkie linie rozpoczynające się od znaku **#** są komentarzami, które nie mają wpływu na działanie serwera, a tylko wyjaśniają, do czego służą poszczególne opcje. W opcjach plików konfiguracyjnych litery duże i małe są rozróżniane. W niektórych przypadkach konieczne będzie nadanie nazwy serwerowi. W tym celu w pliku konfiguracyjnym **/etc/apache2/sites-available/000-default.conf** należy w opcji **ServerName** wprowadzić nazwę serwera, np.:

```
ServerName zspsieradz.edu.pl
```

Po ponownym uruchomieniu serwera można wykonać próbę nawiązania połączenia: w okno adresu przeglądarki wpisujemy adres IP lub nazwę komputera (rys. 14.1).



Rys. 14.1. Strona startowa serwera Apache

PRZYKŁAD 14.1

Instalowanie i uruchomienie serwera Apache2

Aby zainstalować i uruchomić serwer Apache2, należy:

1. Zalogować się na konto użytkownika.
2. Zainstalować serwer. W tym celu trzeba posłużyć się poleceniem:

   `sudo apt install apache2.`
3. Sporządzić kopie zapasowe plików konfiguracyjnych, np. **`/etc/apache2/apache2.conf`**, **`/etc/apache2/sites-available/000-default.conf`**, i innych przed ich modyfikacją za pomocą poleceń:

   `sudo cp /etc/apache2/apache2.conf /etc/apache2/apache2.conf.old`
   `sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/000-default.conf.old`
4. Zmodyfikować plik konfiguracyjny przez dopisanie nazwy serwera (podać nazwę własnego serwera).
5. Uruchomić ponownie usługę za pomocą polecenia:

   `sudo service apache2 restart.`
6. Sprawdzić, czy usługa jest uruchomiona za pomocą polecenia:

   `nmap localhost.`

KODY

7. Uruchomić przeglądarkę internetową i w pole adresu wpisać adres IP serwera WWW. Jeżeli konfiguracja jest poprawna, zostanie wyświetlona strona testowa serwera Apache2.

14.5. Umieszczanie stron na serwerze WWW

Położenie głównego katalogu zawierającego strony udostępniane użytkownikom jest określone w pliku konfiguracyjnym **`/etc/apache2/sites-available/default`** za pomocą zmiennej **`DocumentRoot`**, np.:

```
DocumentRoot /var/www/html
```

Jeżeli w tym katalogu umieści się plik **`index.html`** lub inny znajdujący się na liście domyślnie uruchamianych, to zostanie on wczytany i wyświetlony w oknie przeglądarki.

PRZYKŁAD 14.2

Umieszczanie stron WWW w katalogu głównym usługi

Aby umieścić stronę WWW w katalogu głównym usługi, należy:

1. Zalogować się na konto użytkownika.
2. W pliku konfiguracyjnym zlokalizować położenie katalogu głównego zawierającego strony WWW (opcja **`DocumentRoot`**).
3. Przygotować plik **`index.html`**, zawierający dokument w języku HTML.
4. Za pomocą usługi FTP skopiować plik do katalogu głównego usługi WWW.
5. Uruchomić przeglądarkę internetową i w pole adresu wpisać adres IP serwera WWW. Jeżeli konfiguracja jest poprawna, zostanie wyświetlona strona zawierająca przygotowany wcześniej dokument (rys. 14.2).

Rys. 14.2. **Zmodyfikowana strona testowa serwera Apache**

14.6. Wielkość liter, nazwy plików

Systemy operacyjne z rodziny Windows nie rozróżniają wielkości liter w nazwach plików i folderów. Ponadto te systemy nie zachowują konsekwencji w wyświetlaniu nazw (np. zamieniają pierwszą literę małą na dużą, ukrywają rozszerzenia nazw plików). Może to powodować pewne utrudnienia w korzystaniu z usług internetowych. Większość serwerów w internecie pracuje na podstawie systemów Unix/Linux. W tych systemach w nazwach plików i folderów są rozróżniane małe i duże litery (np. plik **`index.html`** i **`INDEX.HTML`** to zupełnie różne pliki). Nie możemy

przewidzieć, czy nasza witryna zostanie umieszczona na serwerze z systemem Windows bądź Linux, dlatego aby uniknąć niespodzianek, należy ściśle przestrzegać reguł dotyczących wielkości liter w nazwach.

14.7. Konfiguracja serwera Apache do obsługi stron użytkowników

Użytkownicy lokalni mają na serwerze konta założone przez administratora i posiadają uprawnienia do zapisywania danych w swoich katalogach domowych. W katalogu domowym użytkownika może być utworzony podkatalog **`public_html`**, który będzie udostępniany za pośrednictwem usługi WWW. Za obsługę stron użytkowników odpowiada zmienna **UserDir**. Gotowe skrypty zawierające ustawienia konfiguracyjne są umieszczone w katalogu **`mods-available`**, w którym znajduje się wiele gotowych skryptów, możliwych do wykorzystania (ale nie wszystkie z nich są wykorzystywane).

Aktywowanie skryptu odbywa się przez dołączenie go do listy. W tym celu w katalogu **`mods-enabled`** należy utworzyć linki do odpowiednich skryptów. W ten sposób spośród dużej liczby przygotowanych skryptów można wybrać tylko te, które są potrzebne i mają być aktywowane. Włączyć udostępnianie katalogów domowych użytkowników można za pomocą poleceń:

```
cd /etc/apache2/mods-enabled
sudo ln -s ../mods-available/userdir.conf userdir.conf
sudo ln -s ../mods-available/userdir.load userdir.load
```

W pierwszym poleceniu zmieniamy katalog na **`/etc/apache2/mods-enabled`**. Drugie polecenie tworzy w katalogu bieżącym (**`mods-enabled`**) link symboliczny (**`ln -s`**) o nazwie **`userdir.conf`** do pliku **`../mods-available/userdir.conf`** (zapis **`../mods-available/userdir.conf`** oznacza, że należy wyjść o jeden poziom wyżej w strukturze katalogów i wejść do katalogu **`mods-available`**). Link aktywuje zmienne odpowiedzialne za udostępnianie katalogów domowych użytkowników. W ostatnim poleceniu jest tworzony link symboliczny do skryptu odpowiedzialnego za załadowanie modułu programu Apache2, zawierającego obsługę wymaganych funkcji.

PRZYKŁAD 14.3

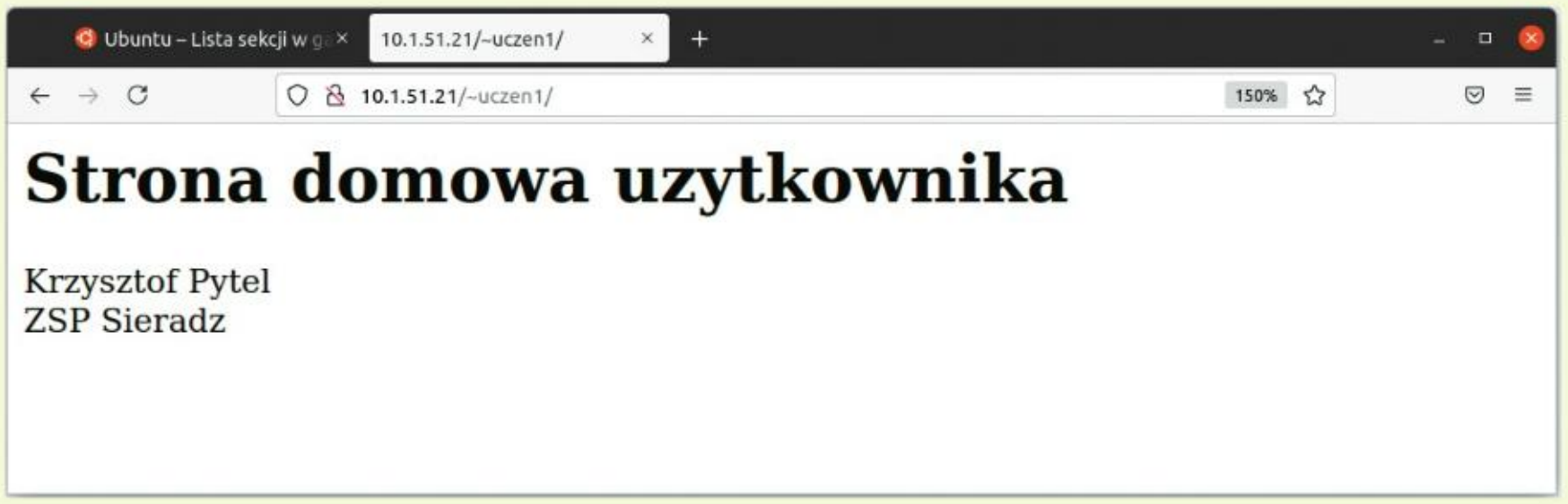
Konfiguracja serwera Apache2 do udostępniania stron domowych użytkowników

Użytkownicy lokalni mogą udostępniać własne strony po wykonaniu poniższej procedury.

1. Zalogować się na konto użytkownika.
2. Utworzyć w katalogu domowym użytkownika podkatalog **`public_html`** za pomocą polecenia:

   `mkdir ~/public_html.`
3. Powtórzyć tę operację dla każdego użytkownika, który będzie miał prawo udostępniania swojego katalogu.
4. Utworzyć w katalogu **`mods-enabled`** linki do plików konfiguracyjnych **`userdir.conf`** i **`userdir.load`**.
5. Utworzyć plik **`index.html`** w katalogu **`public_html`**.
6. Uruchomić ponownie serwer za pomocą polecenia:

   `sudo service apache2 restart.`
7. Przetestować działanie usługi (rys. 14.3).



Rys. 14.3. **Strona udostępniana przez użytkownika**

8. Aby wyświetlić zawartość strony użytkownika, w pole adresu przeglądarki należy za adresem serwera wpisać **`/~nazwa_uzytkownika`**, np. **`10.1.51.21/~uczen1`**.

14.8. Konfigurowanie wirtualnych serwerów WWW

Mechanizm **wirtualnych serwerów** umożliwia uruchomienie więcej niż jednej witryny internetowej na pojedynczym komputerze, np. można uruchomić stronę szkoły i samorządu uczniowskiego. Wirtualne serwery mogą być rozróżniane za pomocą **adresów IP** (ang. *IP-based*), oznacza to, że dla każdej witryny jest przydzielany inny adres IP, za pomocą **portów** (ang. *port-based*), co z kolei znaczy, że dla każdej witryny jest przydzielany inny numer portu lub za pomocą **nazw** (ang. *name-based*) – pojedynczy adres IP jest wykorzystywany przez wiele witryn. Udostępnianie dużej liczby witryn na pojedynczym serwerze umożliwia obniżenie kosztów instalacji i administracji (zamiast kupować, instalować i administrować odrębnym serwerem dla każdej witryny, wystarczy jeden serwer obsługujący wszystkie witryny).

PRZYKŁAD 14.4

KODY

Konfigurowanie i testowanie wirtualnych serwerów opierających się na adresach IP

W tym rozwiązaniu konieczne jest skonfigurowanie innego adresu IP dla każdej udostępnianej witryny. W tym przykładzie serwer zostanie skonfigurowany do obsługi witryny szkoły (**`10.1.51.101`**), samorządu szkolnego (**`10.1.51.121`**) i szkolnego koła sportowego (**`10.1.51.141`**).

Aby skonfigurować wirtualne serwery, należy:

1. Skonfigurować interfejs sieciowy tak, aby obsługiwał wiele adresów IP (aliasy adresów IP). W tym celu dla każdego dodawanego adresu wydać polecenie:

   `sudo ip addr add 10.1.51.121 dev enp0s3.`

   W tym poleceniu do interfejsu **`enp0s3`** jest przypisywany dodatkowy adres **`10.1.51.121`**. Aby sprawdzić, czy adresy zostały poprawnie dodane, można wyświetlić listę adresów za pomocą polecenia:

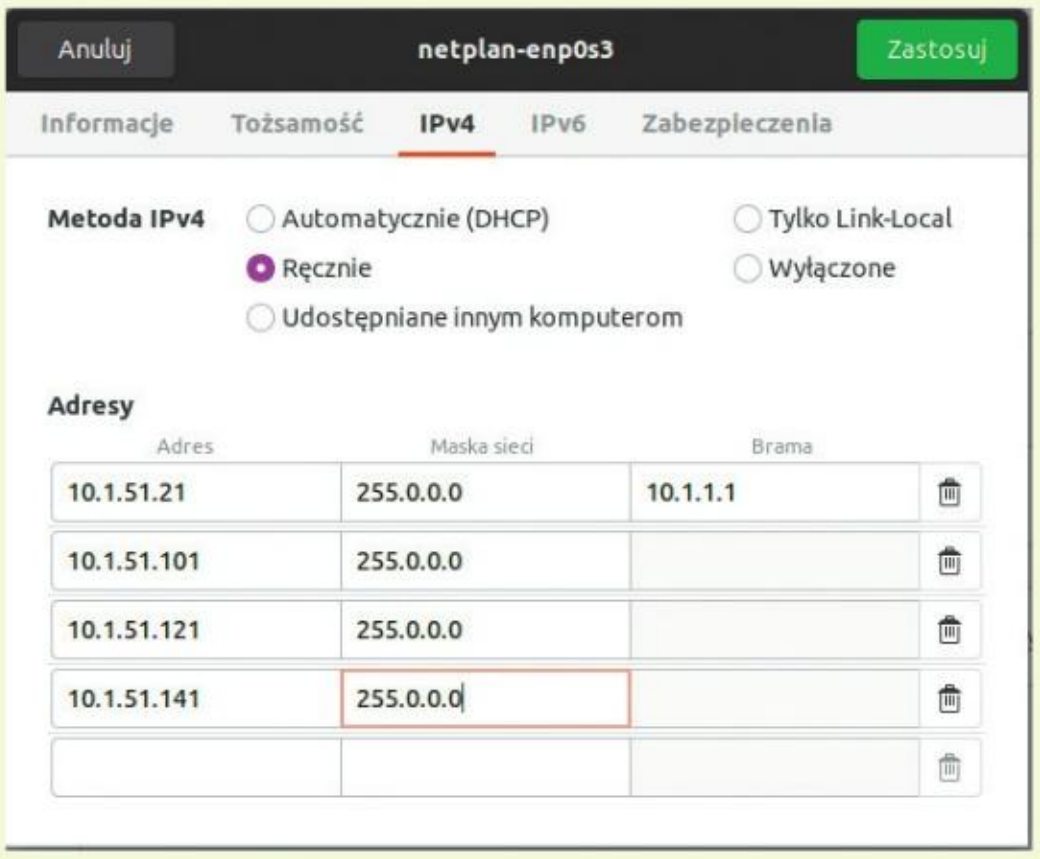
   `sudo ip addr show.`

   i przetestować adres za pomocą polecenia **`ping`**. Sposób wykonania tych operacji przedstawiono na rys. 14.4.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ sudo ip addr add 10.1.51.101 dev enp0s3
[sudo] hasło użytkownika uczen:
uczen@uczen-VirtualBox:~$ sudo ip addr add 10.1.51.121 dev enp0s3
uczen@uczen-VirtualBox:~$ sudo ip addr add 10.1.51.141 dev enp0s3
uczen@uczen-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:ce:97:41 brd ff:ff:ff:ff:ff:ff
    inet 10.1.51.21/8 brd 10.255.255.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet 10.1.51.101/32 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet 10.1.51.121/32 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet 10.1.51.141/32 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fece:9741/64 scope link
       valid_lft forever preferred_lft forever
uczen@uczen-VirtualBox:~$ ping 10.1.51.101
PING 10.1.51.101 (10.1.51.101) 56(84) bytes of data.
64 bytes from 10.1.51.101: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 10.1.51.101: icmp_seq=2 ttl=64 time=0.018 ms
^C
--- 10.1.51.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1020ms
rtt min/avg/max/mdev = 0.018/0.018/0.018/0.000 ms
uczen@uczen-VirtualBox:~$ ping 10.1.51.121
PING 10.1.51.121 (10.1.51.121) 56(84) bytes of data.
64 bytes from 10.1.51.121: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 10.1.51.121: icmp_seq=2 ttl=64 time=0.021 ms
^C
--- 10.1.51.121 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.018/0.019/0.021/0.001 ms
uczen@uczen-VirtualBox:~$ ping 10.1.51.141
PING 10.1.51.141 (10.1.51.141) 56(84) bytes of data.
64 bytes from 10.1.51.141: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 10.1.51.141: icmp_seq=2 ttl=64 time=0.021 ms
^C64 bytes from 10.1.51.141: icmp_seq=3 ttl=64 time=0.020 ms
64 bytes from 10.1.51.141: icmp_seq=4 ttl=64 time=0.021 ms
64 bytes from 10.1.51.141: icmp_seq=5 ttl=64 time=0.023 ms
^C
--- 10.1.51.141 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4098ms
rtt min/avg/max/mdev = 0.018/0.020/0.023/0.001 ms
uczen@uczen-VirtualBox:~$
```

Rys. 14.4. **Dodawanie i testowanie aliasów IP**

Wprowadzone adresy będą aktywne do czasu ponownego uruchomienia systemu. Aby dodać je w sposób trwały, można skorzystać z narzędzia do konfiguracji sieci w środowisku graficznym, uruchamianego przez **Wyświetl programy/Ustawienia/Sieć**. W oknie **Sieć** w sekcji **Przewodowe** należy wybrać tryb konfiguracji połączenia (kliknąć ikonę koła zębatego). W zakładce IPv4 ustawić sposób konfiguracji na **Ręcznie** i dodać adresy. Po wprowadzeniu dodatkowych adresów (rys. 14.5) kliknąć przycisk **Zastosuj** i w razie konieczności wprowadzić hasło administratora.



Rys. 14.5. **Wprowadzanie dodatkowych adresów IP**

2. Utworzyć katalogi, w których będą przechowywane pliki stron. Można to zrobić za pomocą poleceń:

```
sudo mkdir /var/www/samorzad
sudo mkdir /var/www/sks
```

3. Przydzielić uprawnienia do katalogów i zmienić ich właściciela, np. za pomocą poleceń:

```
sudo chown -R uczen:uczen /var/www/samorzad
sudo chown -R uczen:uczen /var/www/sks
sudo chmod -R 755 /var/www/samorząd
sudo chmod -R 755 /var/www/sks
```

4. Utworzyć przykładowe strony dla samorządu i SKS, np. dla witryny samorządu utworzyć plik **index.html** za pomocą polecenia:

```
sudo vi /var/www/samorzad/index.html
```

i wpisać zawartość:

```
<html>
<head>
<title>Samorzad ZSP</title>
</head>
<body>
<h1>Strona Samorzadu Szkolnego</h1>
</body>
</html>
```

5. Utworzyć pliki konfiguracyjne wirtualnych serwerów. Można skopiować przykładowy plik konfiguracyjny wirtualnego serwera, a następnie go zmodyfikować:

   `sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/samorzad.conf`

   `sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/sks.conf`

6. Wykonać konfigurację wirtualnych serwerów. Otworzyć plik konfiguracyjny witryny samorządu za pomocą polecenia:

   `sudo vi /etc/apache2/sites-available/samorzad.`

   Wprowadzić w pliku następujące zmiany:
   - w wierszu **`<VirtualHost *:80>`** **`symbol`** „*” zamienić na adres IP wirtualnego serwera, np. **`<VirtualHost 10.1.51.121:80>`**
   - określić położenie katalogu zawierającego witrynę **`DocumentRoot /var/www/samorzad`**

Przykładowy plik z wprowadzonymi zmianami przedstawiono na rys. 14.6.
W analogiczny sposób zmodyfikować plik konfiguracyjny witryny SKS i szkoły.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$
uczen@uczen-VirtualBox:~$ cat /etc/apache2/sites-available/samorzad.conf
<VirtualHost 10.1.51.121:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com
        ServerName zspsieradz.edu.pl

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/samorzad

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
uczen@uczen-VirtualBox:~$
```

Rys. 14.6. **Plik konfiguracji wirtualnego serwera opartego na adresach IP**

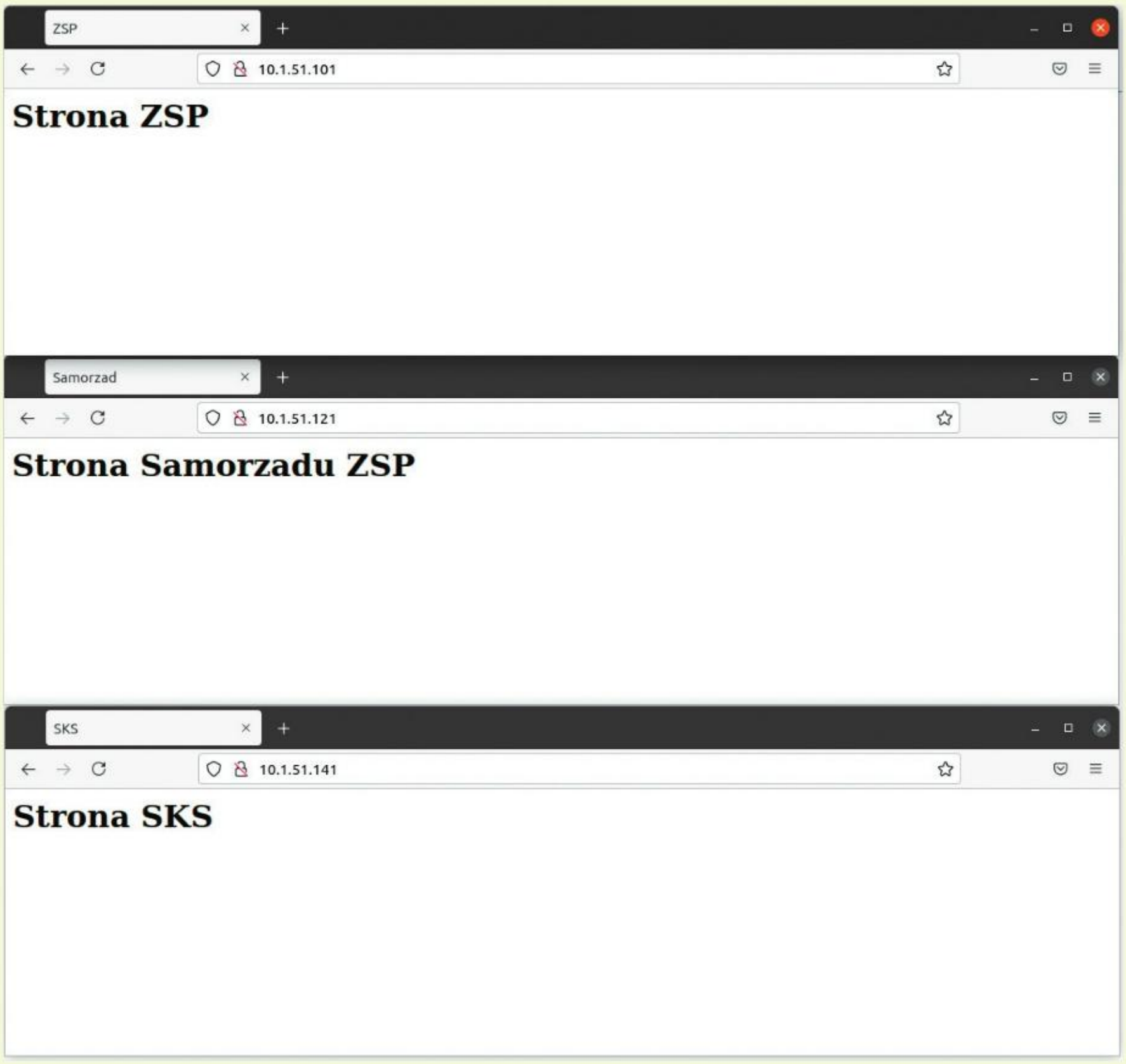
7. Aktywować witrynę przez utworzenie odpowiednich skrótów, wykonując polecenia:

```
sudo a2ensite samorzad
sudo a2ensite sks.
```

8. Uruchomić ponownie serwer Apache2 poleceniem:

```
sudo service apache2 restart.
```

9. Przetestować działanie wirtualnych serwerów przez uruchomienie udostępnianych stron za pomocą adresów IP wirtualnych serwerów (rys. 14.7).



Rys. 14.7. **Testowanie działania wirtualnych serwerów rozróżnianych przez adresy IP**

PRZYKŁAD 14.5

KODY

Konfigurowanie i testowanie wirtualnych serwerów opierających się na nazwach (name-based)

W tym rozwiązaniu konieczne jest skonfigurowanie innej nazwy dla każdej udostępnianej witryny. W tym przykładzie serwer zostanie skonfigurowany do obsługi witryny szkoły (**`szkola.zsp.local`**), samorządu szkolnego (**`samorzad.zsp.local`**) i szkolnego koła sportowego (**`sks.zsp.local`**).

Aby strony mogły być uruchamiane z wszystkich komputerów w sieci lokalnej, trzeba w konfiguracji serwera DNS dodać wpisy (rekordy A lub aliasy) łączące nazwy **`szkola.zsp.local`**, **`sks.zsp.local`** i **`samorzad.zsp.local`** z adresem serwera, np. **`10.1.51.21`**.

Aby skonfigurować wirtualne serwery, należy tak jak w poprzednim ćwiczeniu:

1. Utworzyć katalogi, w których będą przechowywane pliki stron.
2. Przydzielić uprawnienia do katalogów.
3. Utworzyć przykładowe strony dla samorządu i SKS.
4. Utworzyć pliki konfiguracyjne wirtualnych serwerów.
5. Wykonać konfigurację wirtualnych serwerów. Otworzyć plik konfiguracyjny witryny samorządu za pomocą polecenia:

   `sudo vi /etc/apache2/sites-available/samorzad.`

6. Wprowadzić w pliku następujące zmiany:
   - określić dla wirtualnego serwera nazwę (ang. *ServerName*) i alias nazwy (ang. *ServerAlias*), w opcjach wprowadzić:

     `ServerName samorzad.zsp.local`
     `ServerAlias www.samorzad.zsp.local`

   - określić położenie katalogu zawierającego witrynę:

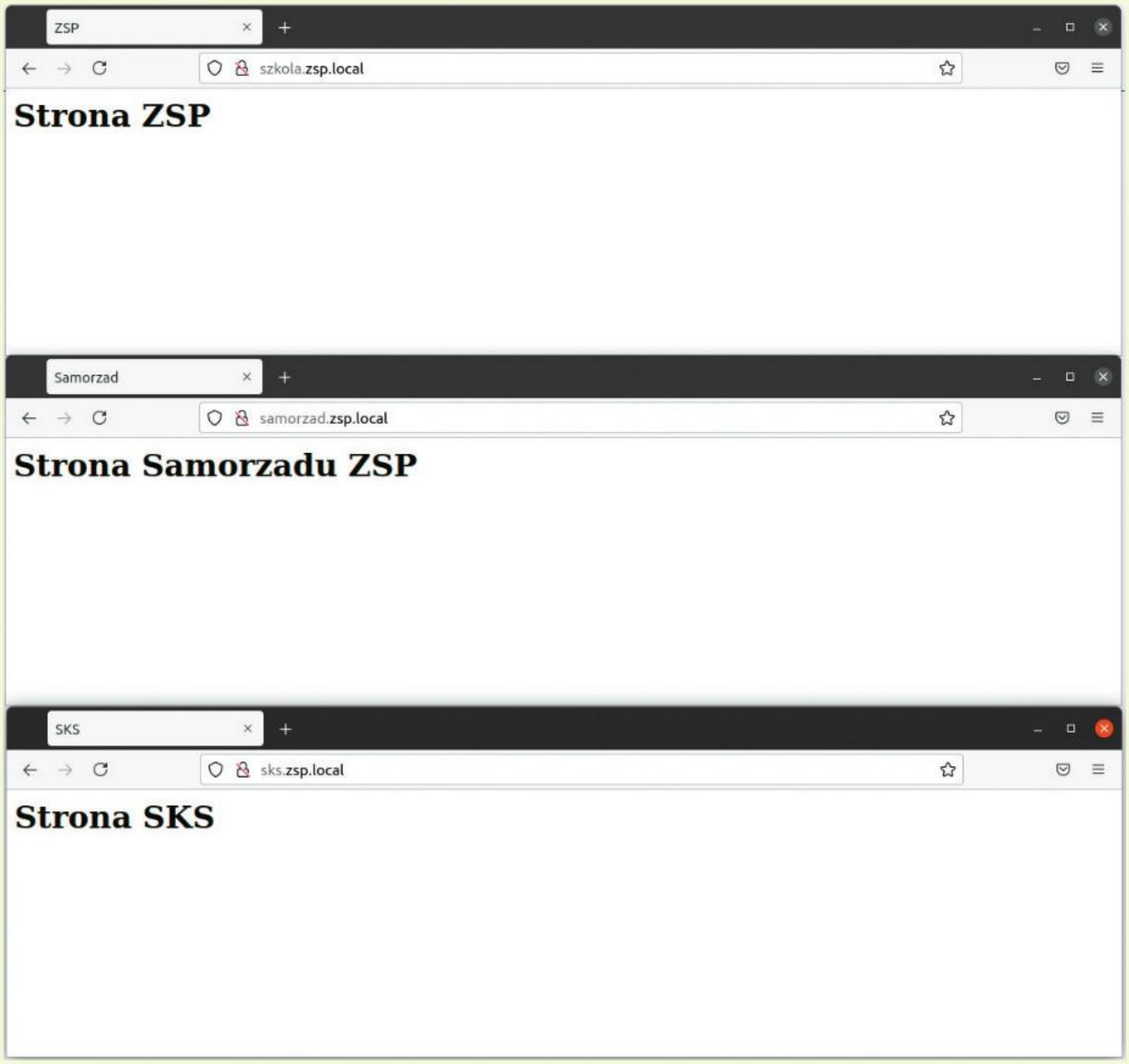
     `DocumentRoot /var/www/samorzad`

Przykładowy plik z wprowadzonymi zmianami przedstawiono na rys. 14.8.

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/apache2/sites-available/samorzad.conf
<VirtualHost 10.1.51.21:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com
        ServerName samorzad.zsp.local
        ServerAlias www.samorzad.zsp.local

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/samorzad

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
uczen@uczen-VirtualBox:~$
```

Rys. 14.8. **Plik konfiguracji wirtualnego serwera opartego na nazwach**

7. W analogiczny sposób zmodyfikować plik konfiguracyjny witryny SKS.
8. Aktywować witrynę przez utworzenie odpowiednich skrótów i uruchomić ponownie serwer Apache2 (patrz: punkty 7. i 8. w poprzednim ćwiczeniu).
9. Skonfigurować serwer DNS, aby nazwy udostępnianych wirtualnych serwerów były skojarzone z adresem IP serwera (nazwa wirtualnego serwera musi być taka sama jak nazwa w rekordzie DNS). Do celów testowych można również przypisać nazwy wirtualnych serwerów do adresu IP w pliku **`/etc/hosts`**.
10. Przetestować działanie wirtualnych serwerów przez uruchomienie udostępnianych stron za pomocą nazw wirtualnych serwerów (rys. 14.9).



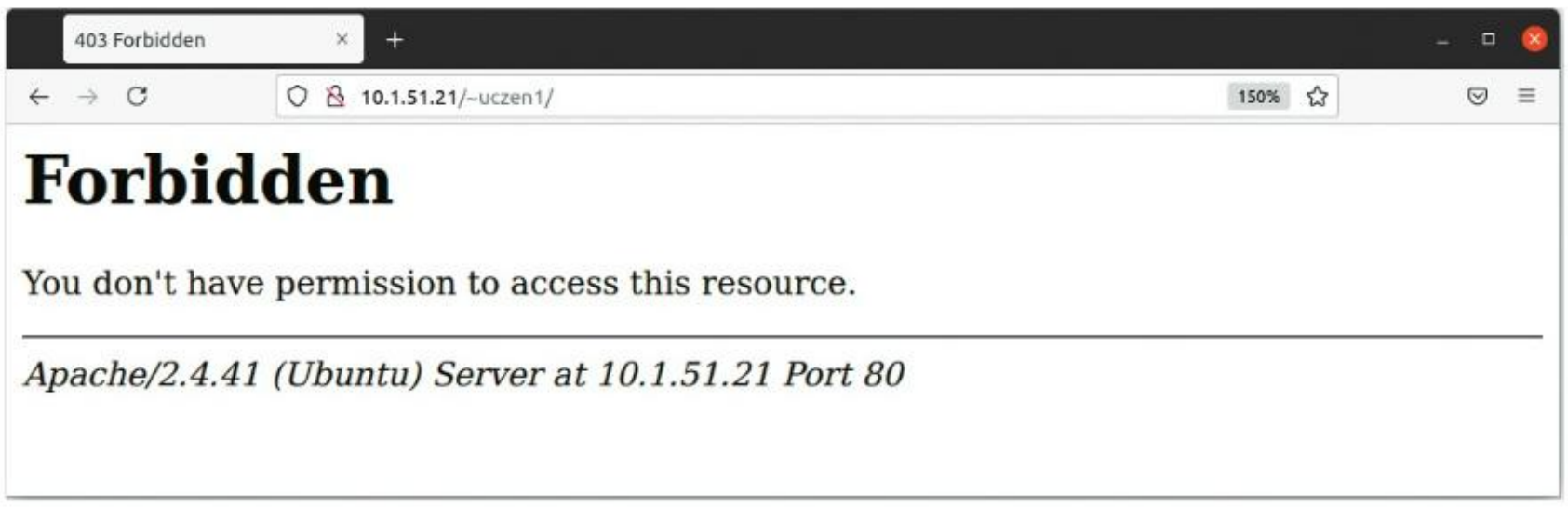
Rys. 14.9. **Testowanie działania wirtualnych serwerów rozróżnianych przez nazwy**

14.9. Blokowanie przeglądania zawartości katalogu

W serwerze Apache2 standardowo jest włączone wyświetlanie zawartości katalogów domowych użytkownika. Dla użytkownika oznacza to, że jeżeli w pole adresu przeglądarki wpisze on nazwę pliku, to zostanie wyświetlony wskazany plik. Jeżeli wpisze się ścieżkę do katalogu, zostanie wyświetlona zawartość pliku startowego (np. **`index.html`**). Jeżeli nie istnieje plik o nazwie domyślnej lub wskazanej przez użytkownika, jest wyświetlana zawartość katalogu (rys. 14.10).

Rys. 14.10. **Odblokowane wyświetlanie zawartości katalogu**

Taka opcja może być przydatna, gdy użytkownik chce udostępnić pliki za pomocą WWW i aby inni użytkownicy mogli sprawdzić nazwy plików. Wyświetlanie zawartości katalogów może stanowić jednak zagrożenie bezpieczeństwa. Przez zmianę konfiguracji serwera zmienia się jego funkcjonalność tak, aby w takim przypadku wyświetlał komunikat o błędzie (rys. 14.11).



Rys. 14.11. **Zablokowane wyświetlanie zawartości katalogu**

W tym celu w pliku **`/etc/apache2/mods-available/userdir.conf`** należy odszukać fragment:

```
<Directory /home/*/public_html>
AllowOverride FileInfo AuthConfig Limit Indexes Options MultiViews
Indexes SymLinksIfOwnerMatch IncludesNoExec
Require method GET POST OPTIONS
</Directory>
```

W pliku konfiguracyjnym trzeba postawić znak **#** na początku każdej linii między znacznikami:

`<Directory/home/*/public_html> i </Directory>`

PRZYKŁAD 14.6

Konfigurowanie serwera Apache2 do blokowania listowania zawartości katalogu zawierającego strony domowe użytkowników

KODY

Aby umożliwić blokowanie listowania zawartości katalogu zawierającego strony domowe użytkowników, należy:

1. Zalogować się na konto użytkownika.
2. Zmodyfikować plik konfiguracyjny **`/etc/apache2/mods-available/userdir.conf`** zgodnie z opisem.

3. Usunąć plik **index.html** (lub zmienić jego nazwę, np. na **index.txt**) z katalogu **public_html**.
4. Uruchomić ponownie serwer za pomocą polecenia:

   sudo service apache restart.
5. Przetestować działanie usługi.

Dostęp do katalogu lub całej witryny udostępnianej przez WWW można ograniczyć przez pliki **.htaccess** i **.htpasswd**. Ta metoda pozwala na zawężenie dostępu do katalogu tylko dla osób znających login i hasło. Ta możliwość jest ważna w przypadku, gdy część opublikowanych informacji powinna być dostępna tylko dla uprawnionych użytkowników (np. oprogramowanie tylko dla klientów, dokumenty dla pracowników).

PRZYKŁAD 14.7

KODY

Konfigurowanie funkcji kontroli dostępu do udostępnianego katalogu
W tym przykładzie zostanie ograniczony dostęp do katalogu **dokumenty**. Tylko osoby znające nazwę konta i hasło będą mogły przeglądać jego zawartość. Aby skonfigurować konto i hasło niezbędne do uzyskania dostępu do katalogu, należy:

1. W katalogu, w którym są przechowywane pliki witryny szkoły, utworzyć podkatalog **dokumenty**, np. za pomocą polecenia:

   sudo mkdir /var/www/html/dokumenty.
2. W katalogu **dokumenty** utworzyć plik **.htaccess** zawierający:

   ```
   AuthName „Katalog z ograniczonym dostepem”
   AuthType Basic
   AuthUserFile /hasla/.htpasswd
   Require valid-user
   ```

   W tym pliku, w opcji **AuthName**, można wpisać dowolny tekst (np. informacje o ograniczeniu dostępu). W linii **AuthUserFile** należy podać pełną ścieżkę do pliku **.htpasswd**, w którym są przechowywane nazwy kont i hasła dostępu. Plik powinien zostać umieszczony w miejscu, do którego zwykły użytkownik nie będzie miał dostępu.
3. Utworzyć plik **.htpasswd** w miejscu wskazanym w pliku **.htacces**. Plik **.htpasswd** będzie zawierał nazwy użytkowników i ich hasła dostępu. Zawartość pliku **.htpasswd** tworzy się według schematu:

   nazwa_uzytkownika:hasło_dostępu

   Hasło dostępu jest odpowiednio zakodowane funkcjami **crypt()**, **MD5** lub **SHA-1**. Przykładowo, użytkownik *uczen1* może mieć hasło *Qwerty123*. W każdej linijce pliku wprowadza się informacje dotyczące jednego konta. Przykładowy plik zawierający konta użytkowników *uczen1*, *uczen2* i *uczen3* z hasłem *Qwerty123* zakodowanym odpowiednio funkcjami **MD5**, **SHA-1** i **crypt()**:

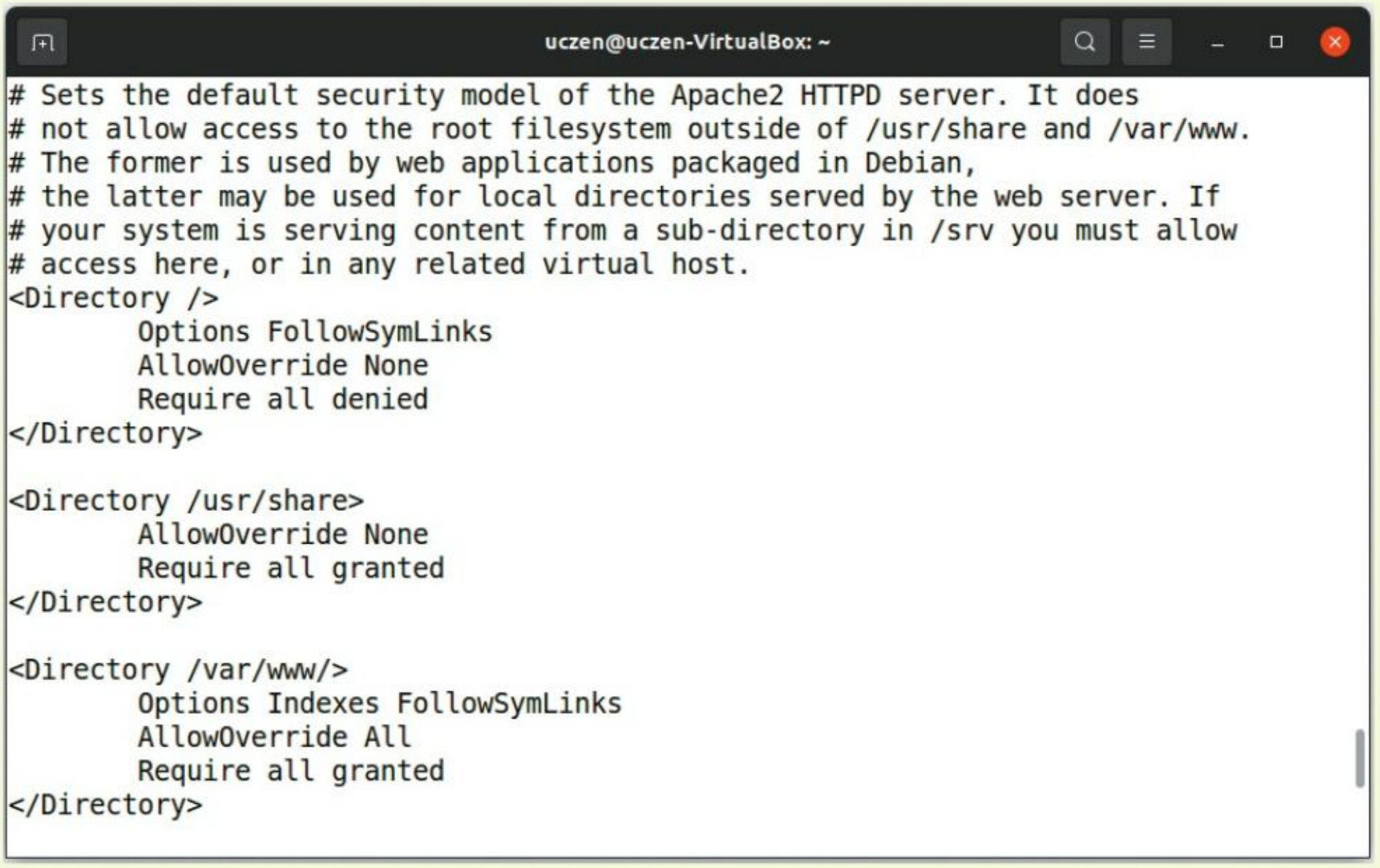
   ```
   uczen1:$apr1$.c/vGOHV$C/QQGFwte0rW1DUGlyW3L1
   uczen2:{SHA}zJ+BakJDHPhSzcej+tQqb2X/ziQ=
   uczen3:9NE3e1mWz/eSc
   ```

Plik z hasłami można utworzyć za pomocą polecenia:

`sudo htpasswd -c /hasla/.htpasswd uczen1.`

Hasła do pliku **`.htpasswd`** dla kont użytkowników można zakodować również za pomocą generatora haseł działającego pod adresem http://aspirine.org/htpasswd_en.html.

4. Zezwolić na nadpisywanie ustawień w pliku konfiguracyjnym witryny. Jeżeli zabezpieczany katalog jest częścią witryny głównej, należy zmodyfikować plik **`/etc/apache2/apache2.conf`**. Jeżeli katalog jest częścią wirtualnego hosta, to trzeba zmodyfikować plik konfiguracyjny tego hosta. W pliku konfiguracyjnym trzeba odszukać sekcję opisującą reguły dostępu do katalogu **`/var/www`** i zamienić opcję **`AllowOverride None`** na **`AllowOverride All`**.
   Na rys. 14.12 przedstawiono plik konfiguracyjny i zaznaczono właściwy fragment. W konfiguracji zezwolono na nadpisywanie ustawień w katalogu **`/var/www`** i wszystkich katalogach podrzędnych.

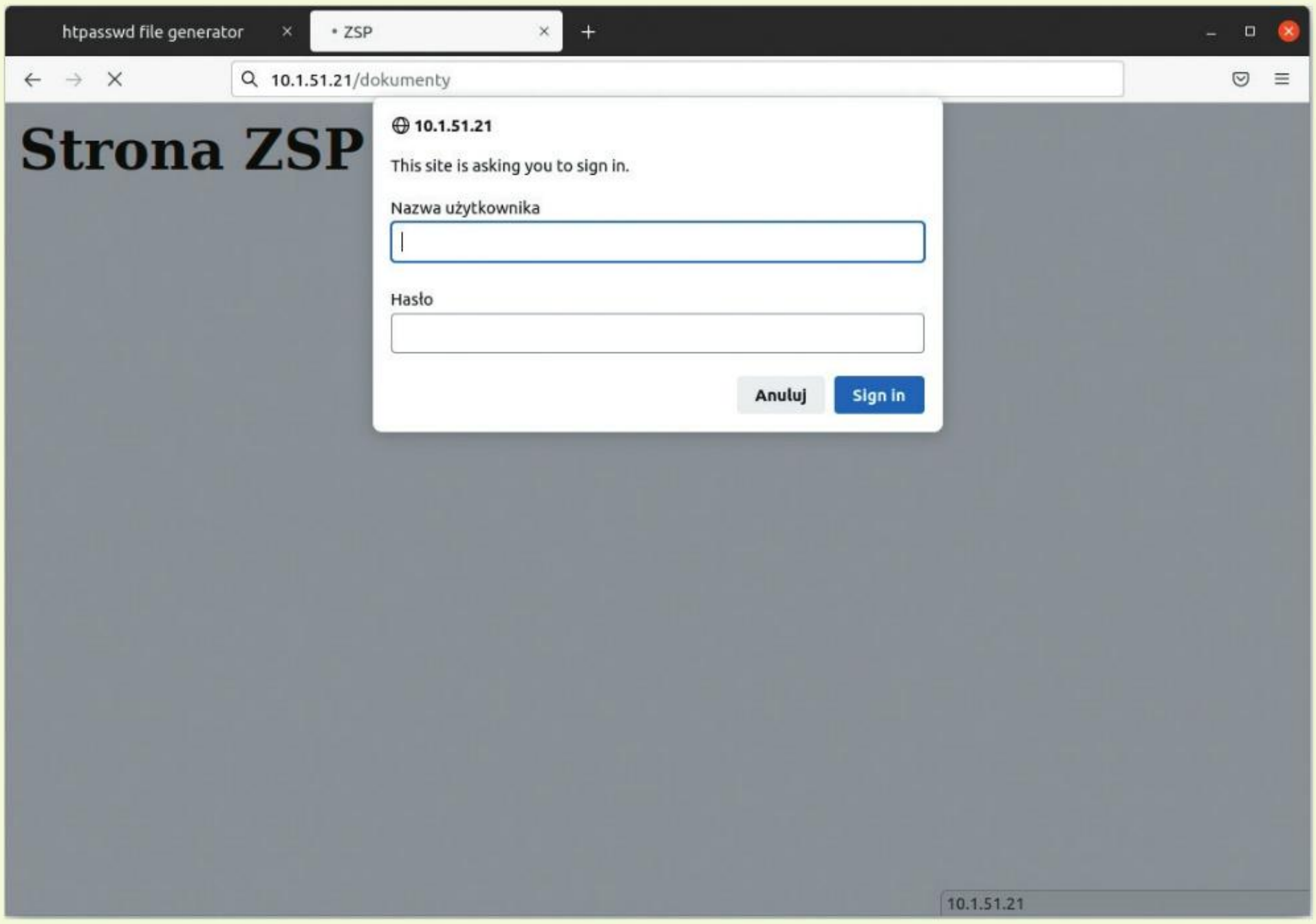


Rys. 14.12. **Zezwolenie na nadpisywanie ustawień w katalogu**

5. Uruchomić ponownie serwer Apache, np. za pomocą polecenia:

   `sudo /etc/init.d/apache2 restart.`

6. Przetestować działanie wprowadzonych zabezpieczeń. Jeżeli konfiguracja przebiegła poprawnie, to podczas próby uzyskania dostępu do zabezpieczonego katalogu pojawi się okno z żądaniem podania nazwy konta i hasła (rys. 14.13).



Rys. 14.13. **Testowanie systemu ochrony katalogu za pomocą hasła**

14.10. Zmiana domyślnie uruchamianego pliku

Jeżeli w pole adresu przeglądarki zostanie wpisana ścieżka katalogu, to we wskazanym katalogu będzie poszukiwany plik o domyślnej nazwie **`index.html`**. Za nazwę domyślnego pliku odpowiada zmienna **DirectoryIndex** w pliku **`/etc/apache2/mods-available/dir.conf`**, np.:

```
DirectoryIndex index.php index.html default.html.
```

Po nazwie tej zmiennej można podać listę plików (oddzielonych spacjami wraz z rozszerzeniami), które mają być domyślnie uruchamiane przez przeglądarkę (ważna jest kolejność). Jeżeli zamierza się korzystać np. ze skryptów języka PHP, to warto dodać do tej listy nazwę **`index.php`**.

Jeżeli domyślna konfiguracja serwera WWW nie umożliwia obsługi stron zawierających skrypty PHP, można doinstalować moduł PHP5 za pomocą polecenia:

```
sudo apt install php php-cgi libapache2-mod-php php-common php-pear
php-mbstring.
```

Polecenie zainstaluje obsługę języka PHP5 i dodatkowe moduły.

PRZYKŁAD 14.8

KODY

Konfigurowanie serwera Apache2 do obsługi języka PHP

Aby umożliwić wykonywanie skryptów języka PHP na serwerze, należy:

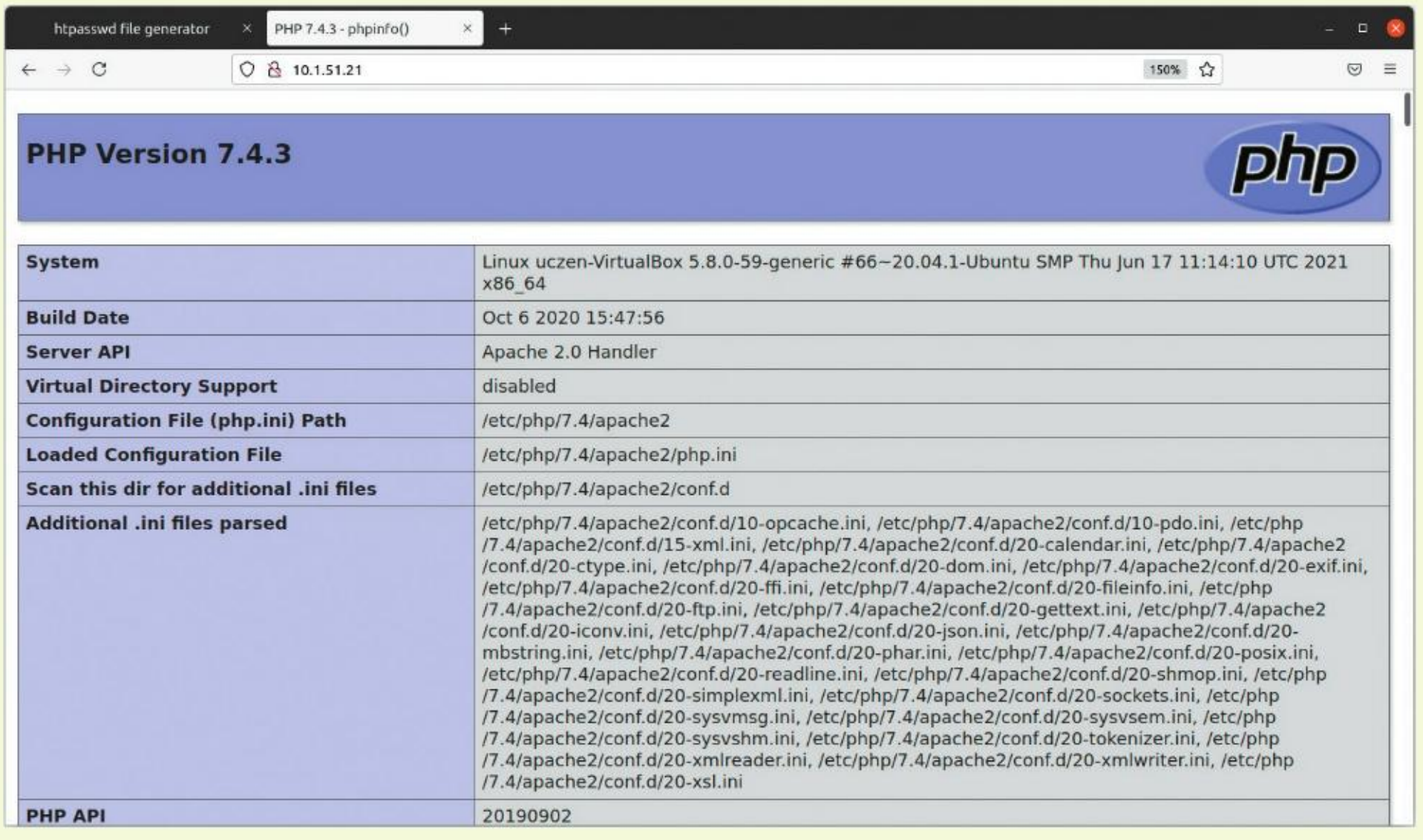
1. Zalogować się na konto użytkownika.
2. Zainstalować moduł PHP5 za pomocą polecenia:

   `sudo apt install php php-cgi libapache2-mod-php php-common php-pear php-mbstring.`
3. Utworzyć plik **`index.php`** w katalogu **`/var/www/html`**.
   Przykładowa zawartość pliku **`index.php`**:

```
<html>
<body>
<?php phpinfo()
?>
</body>
</html>
```

4. Zmodyfikować plik konfiguracyjny **`/etc/apache2/mods-available/dir.conf`** zgodnie z opisem.
5. Uruchomić ponownie serwer za pomocą polecenia:

   `sudo service apache2 restart.`
6. Przetestować działanie usługi. Jeżeli usługa działa właściwie, to po wczytaniu strony powinna się pojawić informacja o PHP, jak na rys. 14.14.



System	Linux uczen-VirtualBox 5.8.0-59-generic #66~20.04.1-Ubuntu SMP Thu Jun 17 11:14:10 UTC 2021 x86_64
Build Date	Oct 6 2020 15:47:56
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xmlreader.ini, /etc/php/7.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini
PHP API	20190902

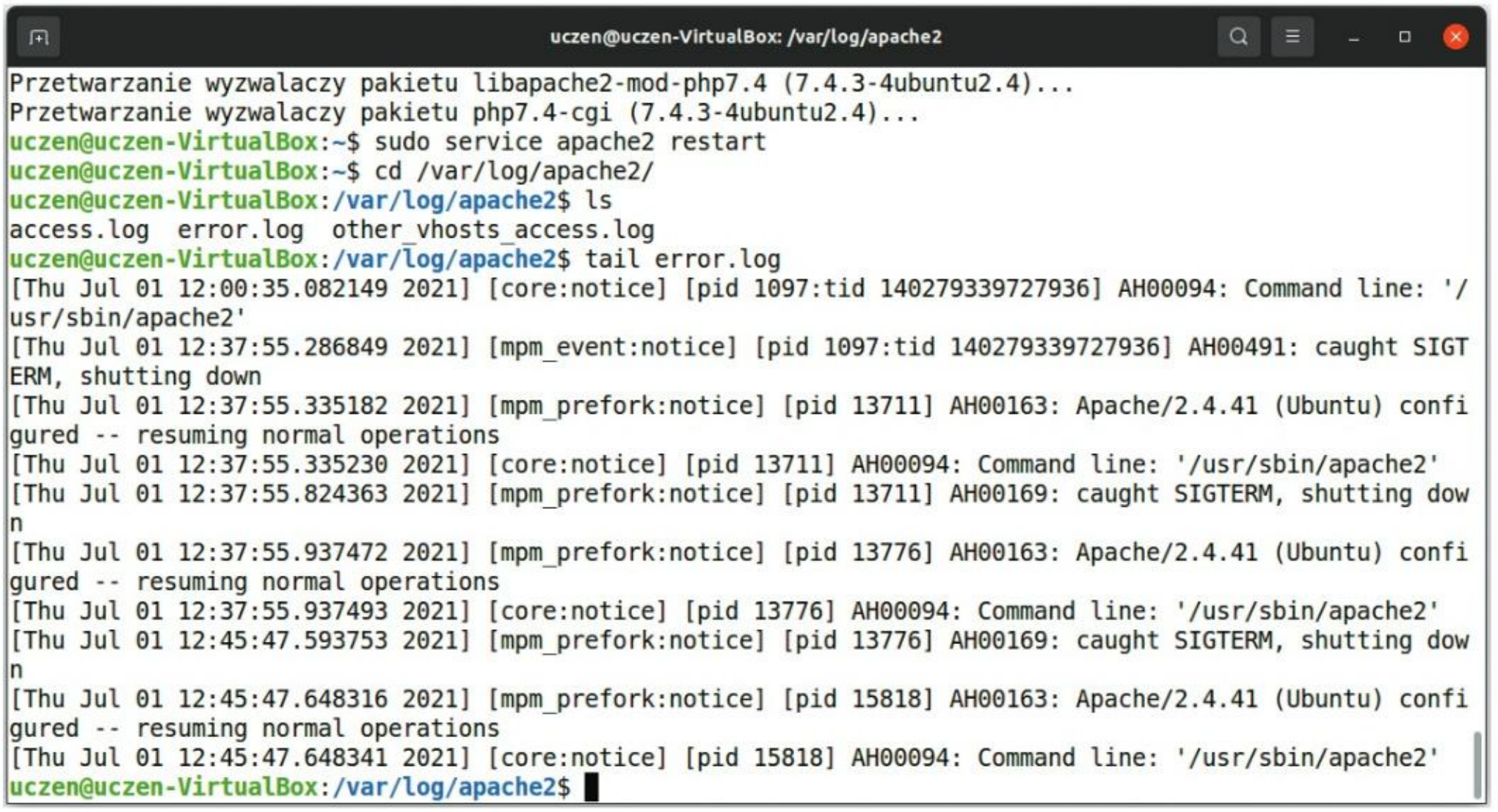
Rys. 14.14. **Testowanie działania PHP na serwerze**

14.11. Przeglądanie logów serwera

Serwer może być tak skonfigurowany, aby zapisywał wszystkie przypadki **uzyskania dostępu** do jego zasobów (ang. *access.log*) i wszystkie **przypadki błędów** (ang. *error.log*), np. gdy użytkownik wpisze nazwę pliku, który nie istnieje na serwerze. Ścieżki dostępu do plików zawierających logi błędów opisują zmienne **ErrorLog** i **LogLevel** w pliku **`/etc/apache2/apache2.conf`**. Zmienna ErrorLog wskazuje położenie plików logów, np. **`ErrorLog ${APACHE_LOG_DIR}/error.log`**.

Zmienna LogLevel kontroluje liczbę logowanych komunikatów. Może zawierać wartości (według malejącej liczby logowanych komunikatów): **`debug`**, **`info`**, **`notice`**, **`warn`**, **`error`**, **`crit`**, **`alert`**, **`emerg`**, np. **`LogLevel warn`**.

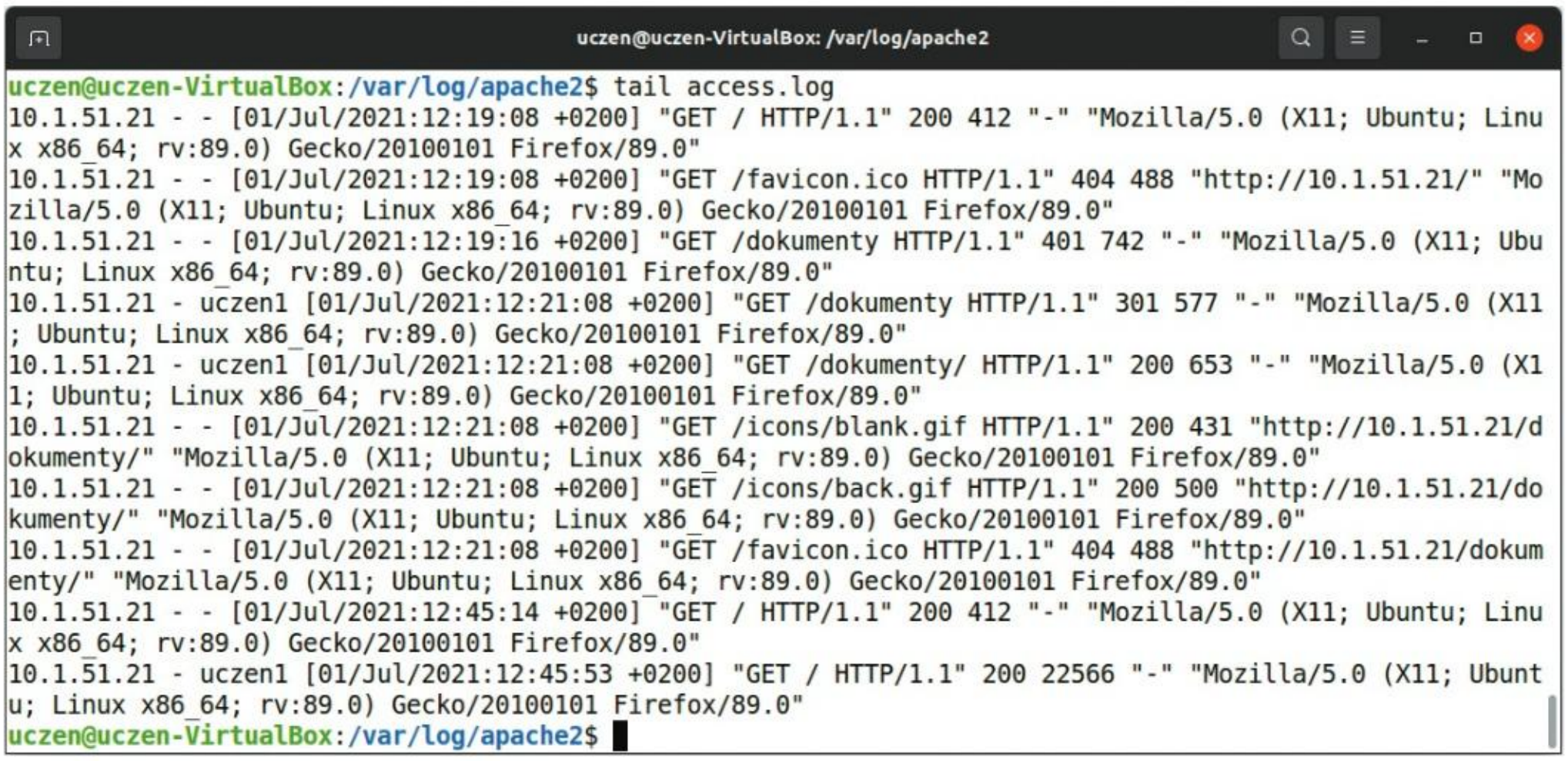
Przykłady plików logów z pliku **`/var/log/apache2/error.log`** przedstawiono na rys. 14.15.



Rys. 14.15. Przykładowy log z pliku `error.log`

Przykłady plików logów z pliku **`/var/log/apache2/access.log`** przedstawiono na rys. 14.16.

Jednym z podstawowych obowiązków administratora jest przeglądanie logów serwera. Z plików można dowiedzieć się o błędach występujących w kodach stron internetowych, np. o brakujących lub uszkodzonych plikach. Można również przeanalizować, które strony i pliki są pobierane i z jaką częstotliwością oraz jacy klienci i kiedy odwiedzali serwer.



Rys. 14.16. **Przykładowy log z pliku `access.log`**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź w internecie, czy istnieje inny niż Apache serwer WWW przeznaczony do pracy w systemie Linux.
2. Wyszukaj w internecie informacje dotyczące procentowego udziału w rynku różnych serwerów WWW.
3. Zainstaluj serwer WWW. Otwórz stronę testową serwera – w pole adresu przeglądarki internetowej wpisz adres IP lub nazwę serwera, np. **`localhost`**. Odczytaj tekst ze strony startowej.
4. Wyświetl zawartość pliku **`apache2.conf`** i sprawdź wartość zmiennej **`Timeout`**. Na podstawie opisu umieszczonego w pliku wyjaśnij, do czego służy ta zmienna.
5. Wyświetl zawartość pliku **`ports.conf`** i sprawdź wartość zmiennej **`Listen`**. Wyjaśnij, do czego służy ta zmienna.
6. Utwórz przykładową stronę w języku HTML zawierającą twoje imię i nazwisko.
7. Za pomocą protokołu FTP skopiuj stronę do katalogu **`public_html`** w swoim katalogu domowym.
8. Przetestuj działanie strony. Skorzystaj z własnego komputera (podaj nazwę komputera – localhost) i komputera koleżanki / kolegi (podaj adres IP komputera).
9. Zaplanuj liczbę i nazwy dla wirtualnych serwerów w twojej szkole.
10. Utwórz system wirtualnych serwerów dla twojej szkoły i przetestuj ich działanie.
11. Zainstaluj moduł PHP w serwerze. Za pomocą skryptu języka PHP wyświetl informacje o zainstalowanej wersji PHP i położeniu pliku konfiguracyjnego **`php.ini`**.
12. Wyszukaj w internecie informacje o innych niż PHP językach skryptowych używanych do tworzenia stron internetowych.
13. Skonfiguruj serwer WWW, umieść na nim przynajmniej jedną stronę i przetestuj działanie usługi.
14. Włącz udostępnianie stron WWW użytkowników i przetestuj działanie serwera.
15. Zablokuj możliwość przeglądania zawartości katalogów zawierających strony użytkowników i przetestuj działanie serwera.

16. Przetestuj obsługę skryptów PHP na twoim serwerze, dołącz plik **`index.php`** do listy przeszukiwanych plików.
17. Przeanalizuj logi serwera powstałe podczas testowania serwera. Na ich podstawie określ, które pliki były najczęściej pobierane i czy w czasie pracy serwera pojawiły się błędy. Jeśli tak, to czym były spowodowane.
18. Skorzystają z pomocy systemu Linux lub internetu i znajdź informacje, do czego służy polecenie **`tail`** i jak ono działa.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Do czego służy usługa WWW?
2. Opisz procedurę instalacji serwera WWW.
3. Jakim poleceniem można uruchomić serwer WWW?
4. Jaka zmienna wskazuje nazwę katalogu zawierającego strony domowe użytkowników?
5. Opisz procedurę konfiguracji serwera Apache2 do udostępniania stron domowych użytkowników.
6. Wyjaśnij, jaka jest różnica między działaniem wirtualnych serwerów opartych na adresach IP a opartych na nazwach.
7. Gdybyś była / był administratorem szkolnego serwera WWW, to czy utworzyłabyś / utworzyłbyś wirtualne serwery? Jeśli tak, to jakie? Uzasadnij decyzję.
8. Wyjaśnij, na czym polega zagrożenie bezpieczeństwa spowodowane możliwością listowania katalogów.
9. W jakich sytuacjach, jako administratorka / administrator serwera WWW, wprowadziłabyś / wprowadziłbyś kontrolę dostępu do zawartości katalogu? Podaj przykłady.
10. Do czego służy moduł PHP i jakie są jego zadania?
11. W jaki sposób doinstalować moduł PHP?
12. Opisz procedurę konfiguracji serwera Apache2 do obsługi języka PHP.

15 Automatyczne uruchamianie zadań

ZAGADNIENIA

Polecenia służące do automatycznego uruchamiania zadań **Zarządzanie zleceniami jednokrotnymi** **Program cron** **Zarządzanie zleceniami wielokrotnymi**

Wszystkie dotychczas poznane polecenia system wykonywał natychmiast po ich wydaniu. Czasem jednak administrator chciałby, aby polecenie było zrealizowane **w określonym momencie w przyszłości**. Istnieją również w systemie zdarzenia, które powinny być **uruchamiane cyklicznie**, np. uaktualnianie bazy wirusów, sporządzanie kopii zapasowych. Do obsługi tego typu zdarzeń można wykorzystać demony **atd** i **cron**.

Polecenie **at** wykorzystuje demona **atd** do **jednokrotnego** wykonania polecenia w zadanym czasie – czyta ze standardowego wejścia (klawiatury) lub podanego pliku polecenia, które mają zostać wykonane przy użyciu powłoki. **Superużytkownik** (ang. *root*) może zawsze posługiwać się opisywanym poleceniem. O prawie do używania **at** decydują pliki **/etc/at.allow** i **/etc/at.deny**. Plik **/etc/at.allow** zawiera listę użytkowników, którzy mają prawo uruchamiania **at**. Jeśli ten plik nie istnieje, to jest sprawdzany plik **/etc/at.deny**, zawierający listę użytkowników, którzy nie mają prawa uruchamiania **at**. Jeśli nie istnieje żaden z plików kontrolujących dostęp do polecenia **at**, może się nim posługiwać wyłącznie superużytkownik. Pusty plik **/etc/at.deny** oznacza, że pozwala się na używanie opisywanego polecenia wszystkim użytkownikom.

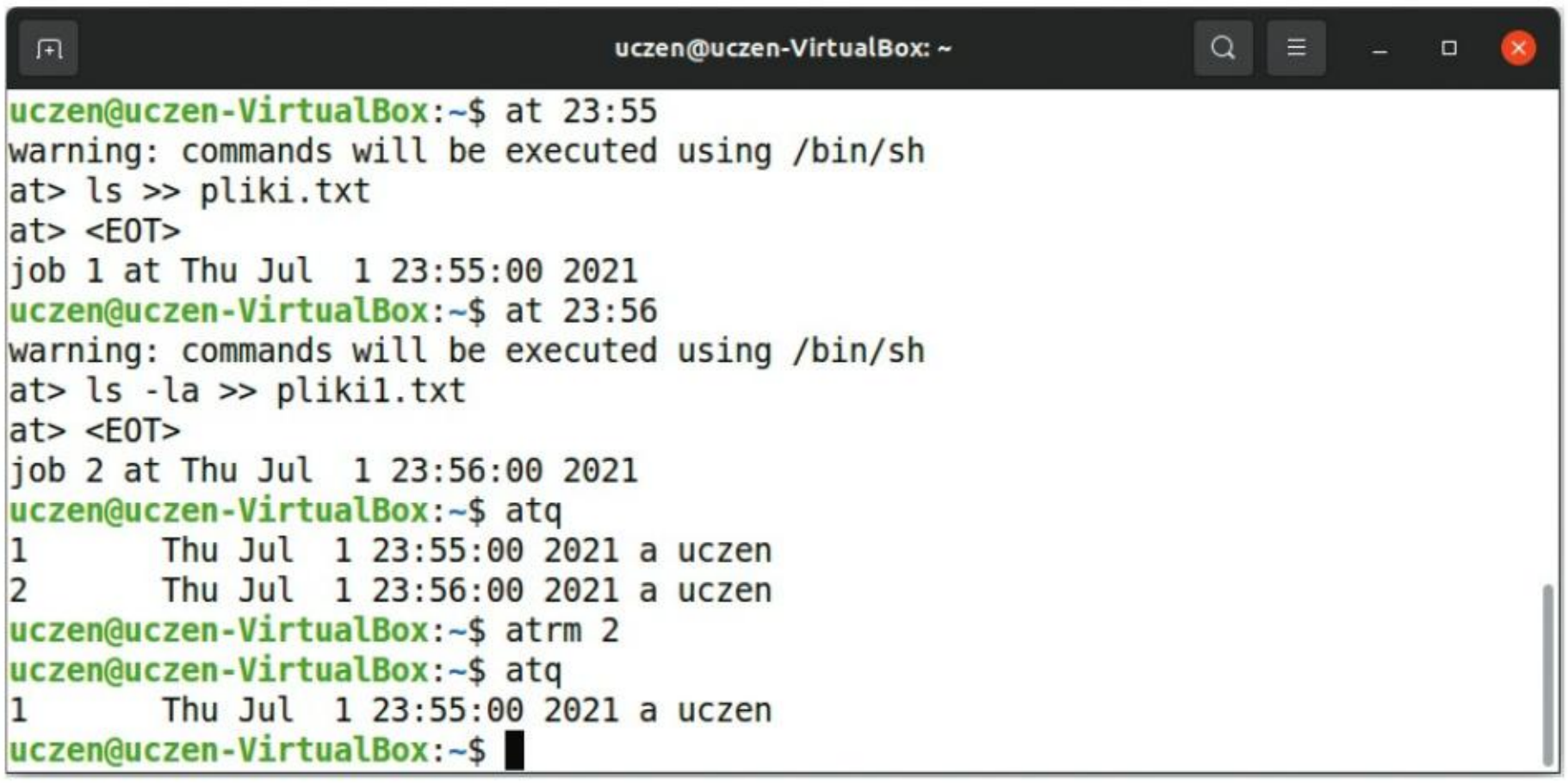
Nowe zlecenie realizowane za pomocą **at** musi zawierać informację o czasie jego wykonania. Czas w **at** można podawać na wiele sposobów, np.:

- **at 18:21** – podawać godzinę wykonania zadania;
- **at 18:23 07.01.19** – podawać godzinę i konkretny dzień (w formacie DD/ MM/YY) wykonania zadania;
- **at 4pm + 3 days** – stosować znak + jako informację, że czas (data) wykonania to suma dwóch czasów (dat), np. za trzy dni o czwartej;
- **at 10am Jul 31 04** – daty i czas mogą być mieszane.

Jeżeli polecenie **at** nie jest dostępne, to można zainstalować odpowiedni pakiet poleceniem:

```
sudo apt install at
```

Na rys. 15.1 przedstawiono przykład zarządzania zleceniami. Zlecenia dotyczą wylistowania zawartości aktualnego katalogu o godz. 23.55 i o 23.56 dzisiaj. Składanie zlecenia należy zakończyć kombinacją klawiszy [Ctrl] + [D]. Zostanie wyświetlone potwierdzenie wraz z podanym terminem uruchomienia polecenia. Jeśli z jakiegoś powodu administrator chce zrezygnować z wykonywania zleconego polecenia, można je usunąć za pomocą polecenia **atrm** z podanym numerem zadania przeznaczonego do skasowania. Numer odczytuje się w pierwszej kolumnie wyniku polecenia **atq** wyświetlającego kolejkę zadań do wykonania.



Rys. 15.1. **Zarządzanie zleceniami jednokrotnymi**

PRZYKŁAD 15.1

Zarządzanie zleceniami jednokrotnymi

Aby utworzyć zlecenie wykonywane jednokrotnie, należy:

1. Zalogować się na konto użytkownika.
2. Wprowadzić zlecenie uruchamiane za 5 minut od teraz (**`at now +5 min`**).
3. Wpisać polecenie listowania zawartości aktualnego katalogu do pliku **`plik.txt`** (**`ls >> plik.txt`**).
4. Wprowadzić zlecenie uruchamiane za 10 minut od teraz (**`at now +10 min`**).
5. Wpisać polecenie listowania zawartości katalogu **`/etc`** do pliku **`plik.txt`** (**`ls /etc >> plik.txt`**).
6. Wyświetlić kolejkę zadań do wykonania poleceniem **`atq`**.
7. Usunąć z kolejki zadanie, które miało być uruchomione za 10 minut, np. jeżeli 2 jest numerem zadania do usunięcia, to można wpisać polecenie **`atrm 2`**.
8. Ponownie sprawdzić zawartość kolejki.
9. Po upływie 5 minut sprawdzić, czy został utworzony **`plik.txt`**, zawierający listę zbiorów katalogu aktualnego.

Program **cron** jest demonem systemowym odpowiedzialnym za uruchamianie zadań (programów) **cyklicznie** lub o określonej porze (działa w systemach pracujących 24 godz. na dobę). W większości dystrybucji **`cron`** jest uruchomiony domyślnie – można nim jednak zarządzać za pomocą polecenia:

```
sudo service cron stop|start|restart.
```

Standardowo z programu **`cron`** może korzystać *root*, natomiast jeżeli występuje potrzeba, aby inni użytkownicy mogli również z niego korzystać, trzeba im na to zezwolić. Służą do tego pliki **`cron.allow`** i **`cron.deny`** w katalogu **`/etc`**. Najbezpieczniej w pliku **`/etc/cron.deny`** wpisać **`all`**, zabroni to korzystania z programu **`cron`** wszystkim, a następnie w **`/etc/cron.allow`** dopisać użytkowników, którym pozwoli się na jego używanie.

Cron co minutę przegląda katalog **/var/spool/cron** w poszukiwaniu plików-tabel (ang. *crontab*) nazywanych według kont, np. dla użytkownika *uczen* jest tworzony plik **uczen**. Do zakładania, usuwania lub przeglądania zawartości tabel używanych przez **cron** służy program **crontab**. Demona **cron** nie trzeba restartować po każdej wprowadzonej zmianie, ponieważ sprawdzi on czasy modyfikacji tabel i przeładuje wszystkie te, które były ostatnio zmienione.

Do edycji tabel crontab używamy następujących poleceń:

- **crontab -e** – edycja listy zadań;
- **crontab -l** – wyświetlanie listy zadań;
- **crontab -r** – usuwanie listy zadań.

Domyślnie edycję tabel wykonuje się za pomocą domyślnego edytora, np. **vi**. Wpisy w plikach **crontab** są zbudowane z sześciu pól (tabela 15.1). Pierwsze pięć pól określa czas wykonania, natomiast szóste pole – czynność.

Tabela 15.1. Pola tabeli w plikach crontab

Minuty	Godziny	Dni miesiąca	Miesiące	Dni tygodnia	Zadanie
*	*	*	*	*	echo „co 1 min" >> /home/uczen/min.txt
01	12	*	*	mon	/home/uczen/skrypt_poniedzialek.sh

Wpis w pierwszej pozycji spowoduje wykonanie co minutę polecenia **echo** i dopisanie do istniejącego pliku tekstu „co 1 min". Wpis w drugiej pozycji spowoduje uruchomienie w każdy poniedziałek o godz. 12.01 skryptu **skrypt_poniedzialek.sh**.

Dopuszczalne wartości w polach:

- minuta – zakres 0–59;
- godzina – zakres 0–23;
- dni miesiąca – zakres 0–31;
- miesiąc – zakres 0–12 lub nazwa (pierwsze trzy litery nazwy angielskiej);
- dni tygodnia – zakres 0–7 (0 i 7 to niedziela) lub nazwa (pierwsze trzy litery nazwy angielskiej);
- polecenie – polecenie lub skrypt do wykonania.

Pole może mieć gwiazdkę, co oznacza wykonanie zawsze. Dozwolone są zakresy liczb oddzielonych przecinkami lub myślnikiem. Zakres jest domknięty, np. 3–6 dla godzin oznacza wywoływanie w godzinach 3, 4, 5, 6. Dozwolone są też listy liczb oddzielonych przecinkami, np. 1,2,3,5. Można również określić czas za pomocą wskazania, co które odmierzenie opatrzonej nim jednostki czasu ma wykonać się operacja, np. */5 – oznacza „co 5 jednostek czasu".

PRZYKŁAD 15.2

Zarządzanie zleceniami wielokrotnymi

Aby utworzyć zlecenie wykonywane wielokrotnie, należy:

1. Zalogować się na konto użytkownika *root* lub mającego uprawnienia do korzystania z **cron**.
2. Uruchomić edycję tabel za pomocą polecenia:

   crontab -e.

3. Wprowadzić zlecenia:
   - uruchamiane co 1 minutę

     (* * * * * echo „co 1 min" >> ~/cron.txt)

   - uruchamiane co 2 minuty

     (*/2 * * * * echo „co 2 min" >> ~/cron.txt).

   Za ostatnim zleceniem należy wprowadzić pustą linię.
4. Wyświetlić listę zadań do wykonania za pomocą polecenia: **crontab -l**.
5. Sprawdzić, czy został utworzony plik **cron.txt** zawierający wpisy.
6. Usunąć wszystkie zadania za pomocą polecenia:

   crontab -r.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj system tak, aby o 00.05 jednokrotnie wykonał wyszukiwanie plików, których jesteś właścicielem. Lista plików powinna być zapisana w pliku **zbiory.txt** w twoim katalogu domowym.
2. Skonfiguruj system tak, aby to samo zadanie wykonał jednokrotnie o tej samej godzinie za tydzień. Lista plików powinna być zapisana w pliku **zbiory_za_tydzien.txt** w twoim katalogu domowym.
3. Utwórz katalog **/kopie** i nadaj uprawnienia umożliwiające dostęp tylko tobie. 3. Skonfiguruj system tak, aby o 1.05 codziennie wykonywał kopiowanie zbiorów z twojego katalogu domowego do katalogu /kopie.
4. Utwórz katalog **/kopie_inne** i nadaj uprawnienia umożliwiające dostęp tylko użytkownikowi root. Skonfiguruj system tak, aby o 2.05 w każdy piątek wykonywał kopiowanie zbiorów z katalogów domowych wszystkich użytkowników do katalogu **/kopie_inne**.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyjaśnij różnicę w zastosowaniu **cron** i **at**.
2. Wyjaśnij w zeszycie przedmiotowym, jak zapisać czas w systemie zgodnym z formatem **at**:
   - za miesiąc od teraz;
   - za 3 godziny od teraz;
   - za 30 minut od teraz.
3. Wyjaśnij w zeszycie przedmiotowym, jak zapisać czas w systemie zgodnym z formatem **cron**:
   - pierwszego dnia miesiąca o 2.15 w nocy;
   - co dwa dni;
   - co 6 godzin w środy.

16 Zarządzanie logiczną strukturą dysku

ZAGADNIENIA

Katalogi domowe użytkowników **Funkcje przydziałów dyskowych** **Zarządzanie przydziałami dyskowymi** **Narzędzie w systemie Linux służące do zarządzania partycjami** **Utworzenie w systemie nowej partycji** **Formatowanie i montowanie partycji** **Przygotowanie nowej partycji do pracy**

Z zasobów udostępnianych przez serwery jednocześnie korzysta wielu użytkowników. Każdy z nich powinien oprócz swojego konta mieć określone zasoby, umożliwiające wykonywanie zadań. Przykładem takiego zasobu jest miejsce na dysku serwera, w którym są przechowywane dane użytkownika. Użytkownicy mają specjalne katalogi przeznaczone do przechowywania prywatnych danych. Nazywa się je **katalogami domowymi** (w systemie Linux standardowo są umieszczane w **/home**).

Podczas instalacji systemu Linux przeznaczonego na serwer katalogi domowe użytkowników zostają na ogół zlokalizowane na odrębnej partycji. Nawet jeżeli użytkownicy zapełnią danymi całą partycję z katalogami domowymi, nie spowoduje to awarii głównego systemu plików, znajdującego się na innej partycji. Innym możliwym zabezpieczeniem jest **przydział dyskowy** (ang. *quota*). Umożliwia on określenie maksymalnego rozmiaru danych, jakie użytkownicy i grupy użytkowników mogą przechowywać na poszczególnych partycjach dysku. Temu ograniczeniu nie podlega użytkownik *root*.

Zwykle zakłada się, że nie wszyscy użytkownicy będą w pełni wykorzystywali przydzieloną im przestrzeń dyskową, dlatego suma limitów wszystkich użytkowników może być większa niż fizyczny rozmiar partycji. Przydziały dyskowe są definiowane dla każdej partycji oddzielnie. Aby zdefiniować przydziały dyskowe, można stworzyć w systemie nową partycję przeznaczoną na dane użytkowników.

16.1. Tworzenie nowej partycji w systemie

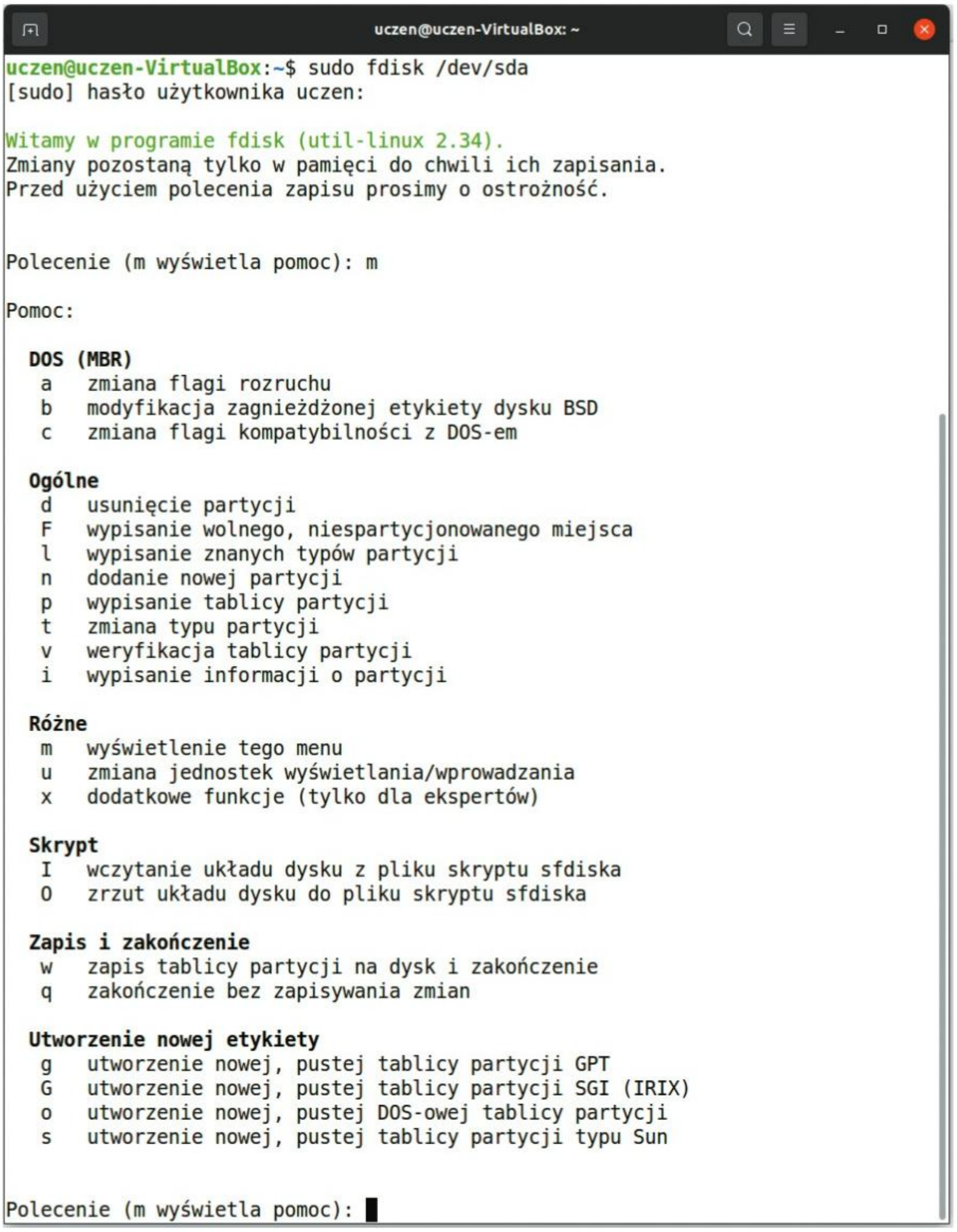
Nowa partycja zostanie utworzona w obszarze dysku nieprzydzielonym wcześniej żadnej innej partycji. Jeżeli na dysku nie ma wolnego obszaru, to należy zmodyfikować układ partycji tak, aby możliwe było utworzenie nowej partycji. Do zarządzania partycjami w systemie Linux można wykorzystać narzędzie **fdisk**. Prawo do jego uruchomienia ma tylko użytkownik *root*.

Narzędzie jest uruchamiane za pomocą polecenia:

```
sudo fdisk /dev/sdba,
```

gdzie **/dev/sdba** oznacza identyfikator dysku w systemie.

Po uruchomieniu narzędzia (rys. 16.1) należy wpisać polecenie **m**, aby uzyskać wykaz dostępnych zadań.

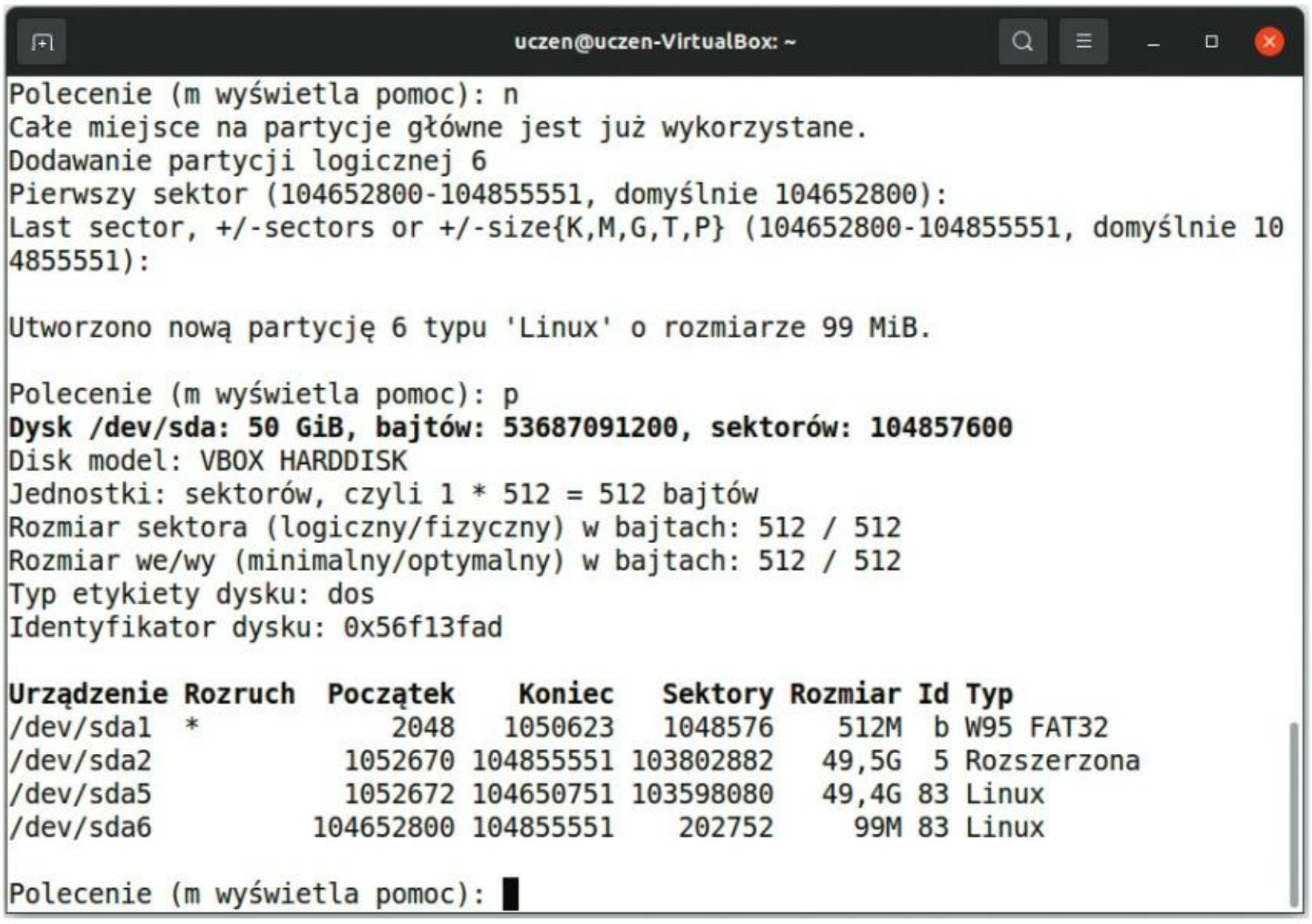


Rys. 16.1. **Uruchomienie narzędzia `fdisk`**

Aby dodać nową partycję w nieprzydzielonym wcześniej obszarze dysku, trzeba wybrać polecenie **`n`**. Następnie można wybrać typ partycji (podstawowa lub rozszerzona) i jej numer. Jeżeli w systemie istniały tylko jedna partycja podstawowa (**`/dev/sda1`**) i partycja wymiany (**`/dev/sda2`**), to nowo tworzona partycja podstawowa powinna otrzymać numer 3.

Jeżeli planujemy pozostawienie na dysku wolnego obszaru do późniejszego wykorzystania, można określić rozmiar tworzonej partycji przez wskazanie cylindrów na dysku lub zajmowanego przez nią rozmiaru. Jeżeli nowa partycja ma zająć cały wolny obszar na dysku, można zaakceptować wartości zaproponowane przez kreatora. Wyświetlenie wykazu partycji na dysku można uzyskać po wpisaniu polecenia **`p`** (rys. 16.2).

Po sprawdzeniu, czy układ partycji jest zgodny z oczekiwaniami użytkownika, można go zapisać na dysku za pomocą polecenia **w**. Wprowadzone zmiany wymagają ponownego uruchomienia komputera. Przygotowana nowa partycja wymaga jeszcze **sformatowania** i **zamontowania** do systemu plików.



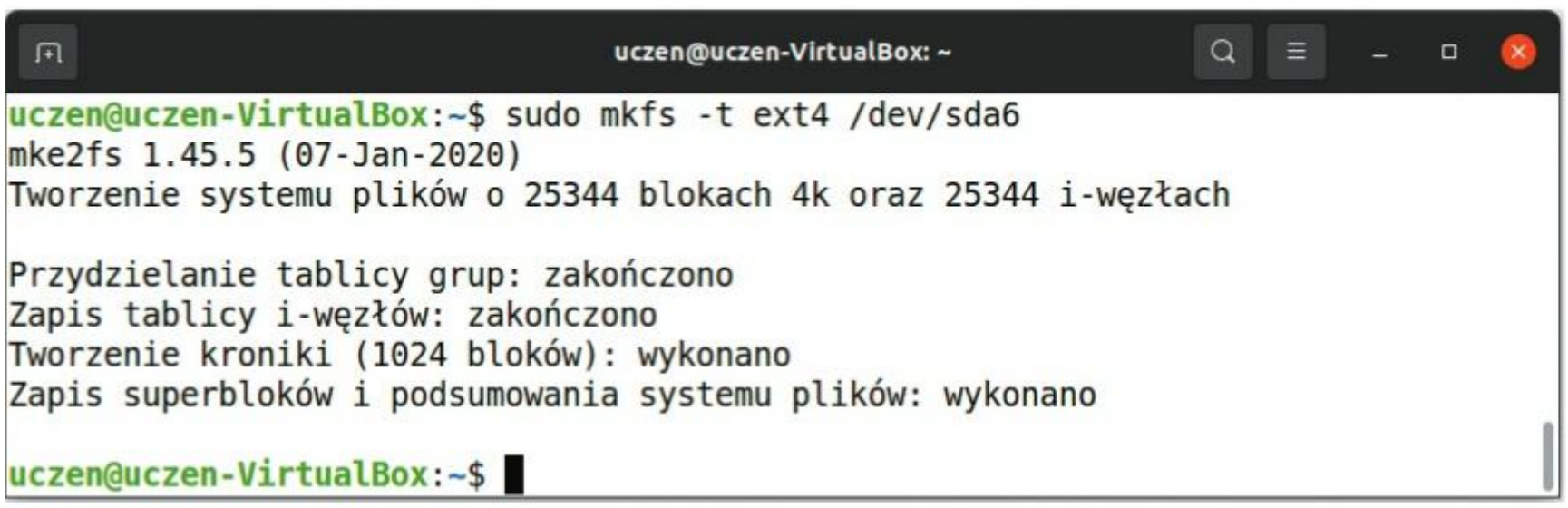
Rys. 16.2. **Tworzenie partycji za pomocą narzędzia `fdisk`**

16.2. Formatowanie i montowanie partycji

Formatowanie jest procesem przygotowania partycji do zapisu danych. Podczas formatowania jest tworzony system plików. Dla nowej partycji można wybrać system **`ext4`**. Jest on najczęściej używanym systemem plików w systemie Linux. Umożliwia również wprowadzenie przydziałów dyskowych. Do formatowania partycji można wykorzystać konto z uprawnieniami użytkownika *root* i polecenie:

`sudo mkfs -t ext4 /dev/sda6`,

gdzie opcja **`-t ext4`** wskazuje typ systemu plików, natomiast **`/dev/sda6`** – partycję do formatowania. Przebieg formatowania przedstawiono na rys. 16.3.



Rys. 16.3. **Formatowanie partycji**

Każda partycja w systemie Linux musi zostać **zamontowana** do głównego systemu plików. **Punkt montowania** to katalog uważany przez system za miejsce, od którego zaczyna się partycja. Wszystkie dane zapisane na partycji będą traktowane tak, jakby znajdowały się w katalogu stanowiącym punkt montowania.

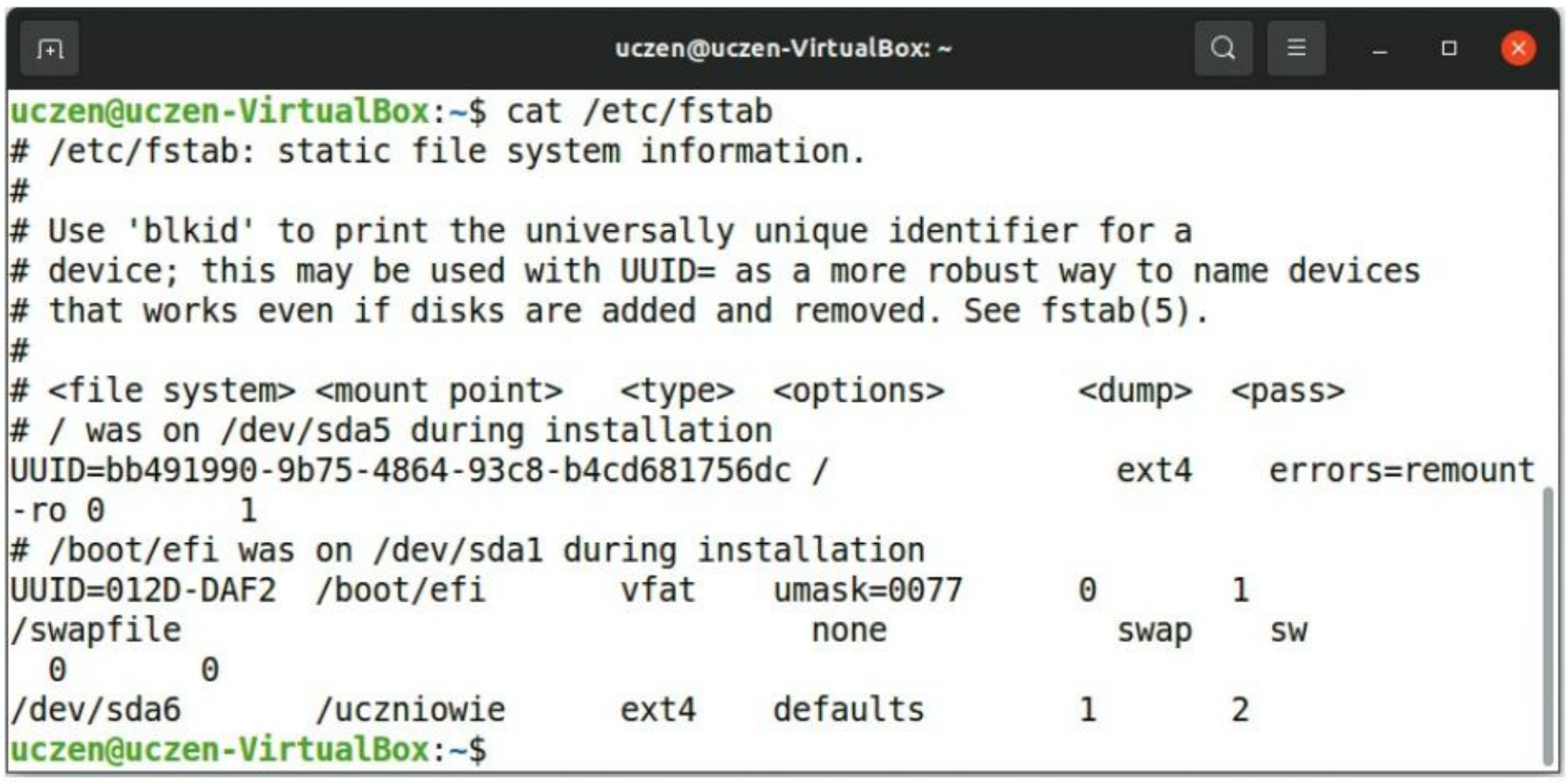
Jako punkt montowania można wybrać dowolny katalog (najlepiej pusty) lub utworzyć nowy, np. za pomocą polecenia:

```
sudo mkdir /uczniowie
```

Utworzony katalog powinien mieć nadane odpowiednie uprawnienia. Można to zrobić za pomocą polecenia:

```
sudo chmod 777 /uczniowie
```

Partycja może być montowana do głównego systemu plików podczas uruchamiania komputera. W pliku **/etc/fstab** jest umieszczony opis wszystkich systemów plików montowanych podczas uruchamiania komputera. Każdy system jest opisany w oddzielnej linii (rys. 16.4).

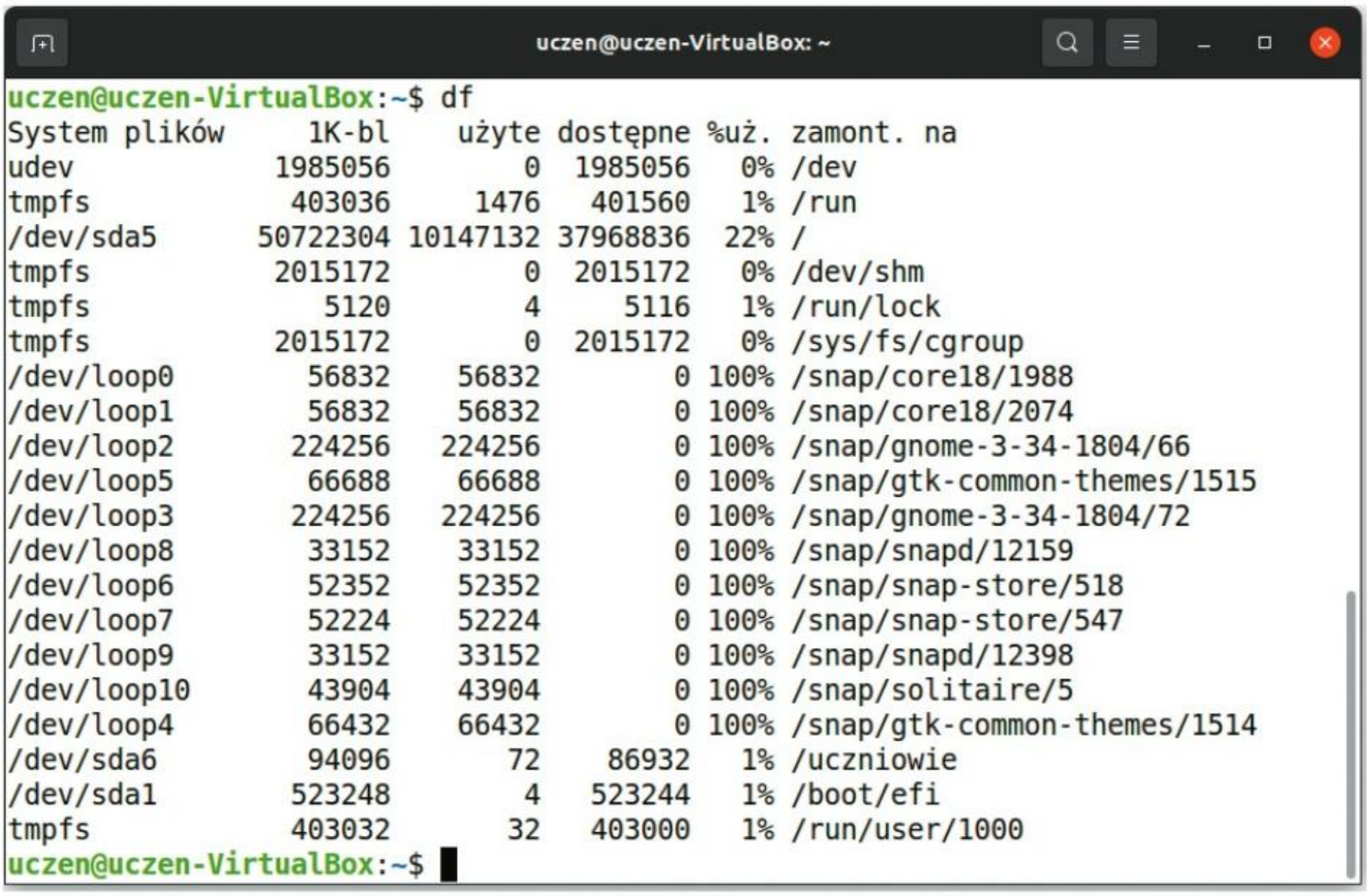


Rys. 16.4. **Zawartość pliku /etc/fstab**

Ostatnia linia opisuje sposób montowania nowo utworzonej partycji. Poszczególne wpisy oznaczają:

- **/dev/sda6** – oznaczenie partycji;
- **/uczniowie** – punkt montowania (katalog musi istnieć w systemie);
- **ext4** – typ systemu plików;
- **defaults** – dodatkowe opcje (domyślne ustawienia);
- **pierwsza cyfra** – wartość używana przez program **dump**, aby wykryć, który system plików ma być odłączony;
- **druga cyfra** – wartość używana przez program fsck, aby zdecydować o kolejności sprawdzania dysku; główny system plików powinien mieć wartość równą 1, a inne systemy plików – równą 2.

Systemy plików w obrębie dysku będą sprawdzane sekwencyjnie, ale systemy plików na innych dyskach – w tym samym czasie. Podczas ponownego uruchomienia komputera partycja zostanie zamontowana zgodnie z opisem w pliku **/etc/fstab**. Do wyświetlenia informacji o wszystkich zamontowanych systemach plików można użyć polecenia **df** (rys. 16.5).



Rys. 16.5. **Lista plików zamontowanych w systemie**

PRZYKŁAD 16.1

Przygotowanie nowej partycji do pracy

Aby utworzyć i przygotować nową partycję do pracy w systemie Linux, należy:

1. Zalogować się na konto użytkownika z uprawnieniami *root*.
2. Uruchomić program fdisk, podając jako argument identyfikator dysku (np. polecenie: **`fdisk /dev/sda`**).
3. Utworzyć nową partycję zgodnie z opisem.
4. Zapisać zmiany w układzie partycji (w programie fdisk opcja **`w`**).
5. Sformatować nowo utworzoną partycję za pomocą polecenia:

   ```
   sudo mkfs -t ext4 /dev/sda6
   ```

6. Utworzyć w katalogu głównym podkatalog uczniowie za pomocą polecenia:

   ```
   sudo mkdir /uczniowie
   ```

7. Nadać uprawnienia do korzystania z tego katalogu wszystkim użytkownikom za pomocą polecenia:

   ```
   sudo chmod 777 /uczniowie
   ```

8. Utworzyć kopię zapasową pliku **`/etc/fstab`** za pomocą polecenia:

   ```
   sudo cp /etc/fstab /etc/fstab.old
   ```

9. Dodać wpis w pliku **`/etc/fstab`** opisujący sposób montowania nowej partycji (można wprowadzić opcje tak jak na rys. 16.4).
10. Uruchomić ponownie komputer za pomocą polecenia:

    ```
    sudo reboot
    ```

11. Sprawdzić za pomocą polecenia **`sudo df`**, czy partycja jest zamontowana.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skorzystaj z protokołu ssh i sprawdź stopień wykorzystania dysku w komputerze koleżanki / kolegi. Z jakiego systemu plików korzysta partycja zawierająca pliki systemowe?
2. Skorzystaj z protokołu telnet i wyświetl za pomocą programu fdisk informacje o partycjach w komputerze koleżanki / kolegi. Z ilu bloków składa się partycja wymiany?

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakie jest przeznaczenie katalogów domowych użytkowników?
2. Do czego służą przydziały dyskowe i jaki jest cel ich stosowania?
3. Do czego służy punkt montowania partycji?
4. Jakie narzędzie w systemie Linux służy do zarządzania partycjami?
5. Opisz proces tworzenia w systemie Linux nowej partycji.
6. W jakim celu wykonuje się formatowanie partycji?
7. Jak zamontować partycję w systemie Linux?
8. Opisz proces przygotowywania nowej partycji do pracy.

17 Przydziały dyskowe użytkowników

ZAGADNIENIA

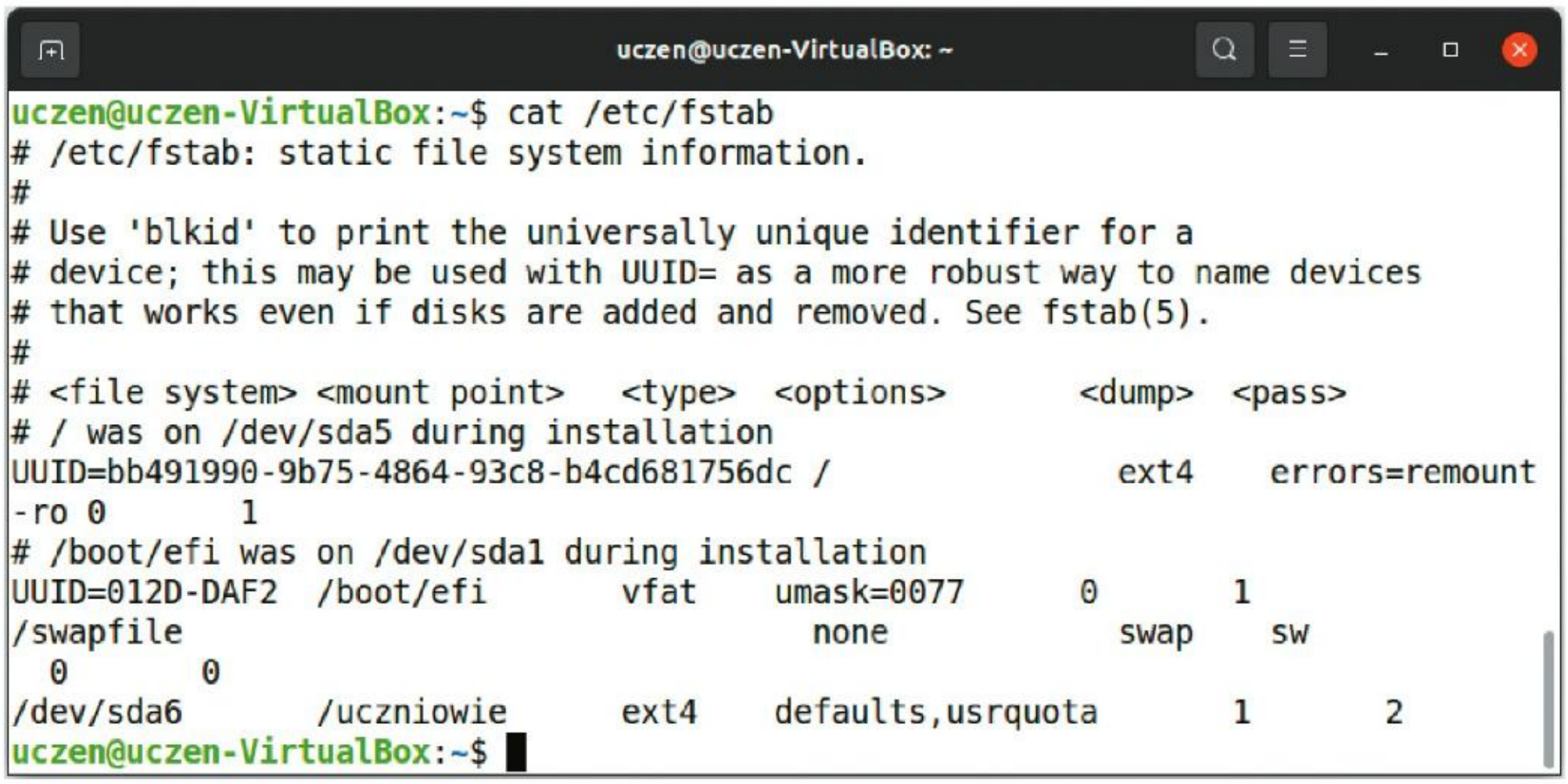
Funkcje pakietu quota **Przebieg procesu przydzielania przestrzeni dyskowej użytkownikom** **Polecenie pozwalające kontrolować rozmiar wykorzystanej przestrzeni dyskowej** **Przydziały dyskowe dla użytkowników indywidualnych**

Przydziały dyskowe użytkownika (ang. *Quota*) pozwalają na określenie maksymalnego obszaru dysku, zajmowanego przez zbiory poszczególnych użytkowników. Są one przyznawane dla każdej partycji niezależnie. Przydziały dyskowe nie dotyczą użytkownika *root*. Aby tworzenie przydziałów było możliwe, należy zainstalować pakiet **quota**, np. za pomocą polecenia:

```
sudo apt install quotatool
```

Aby wprowadzić przydziały dyskowe na poziomie użytkownika, należy:

1. Zmodyfikować plik **/etc/fstab** – w opcjach opisu wariantów montowania partycji trzeba dodać wpis **usrquota** (rys. 17.1). Poszczególne opcje są oddzielone tylko przecinkiem.



Rys. 17.1. **Wprowadzenie mechanizmu quota dla użytkowników na partycji /dev/sda6**

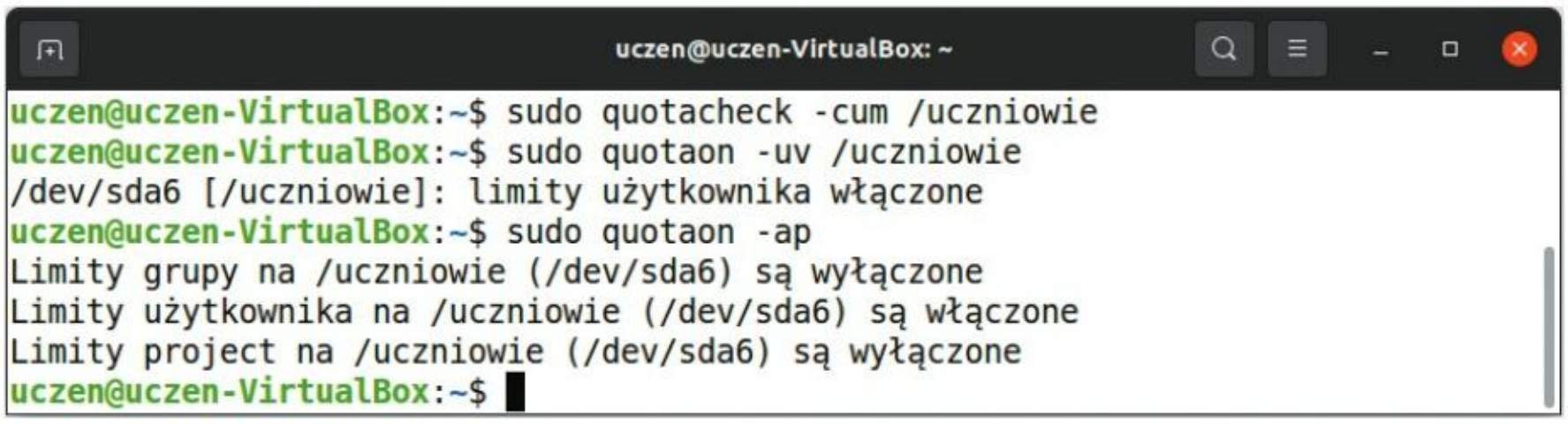
2. Ponownie zamontować system plików – aby zmiany dokonane w pliku **/etc/fstab** były wprowadzone do systemu, można też jeszcze raz uruchomić komputer lub wpisać polecenie:

```
sudo mount -o remount /uczniowie
```

3. Utworzyć plik zawierający opis przydziałów – informacje o przydziałach dyskowych poszczególnych użytkowników są przechowywane w pliku **aquota.user**. Można utworzyć go za pomocą polecenia:

   sudo quotacheck -cum /uczniowie

   Plik ten musi znajdować się w katalogu stanowiącym punkt montowania (w opisywanym przypadku jest to katalog **/uczniowie**). Polecenie powoduje skanowanie systemu plików i umieszcza w pliku informacje o aktualnym stopniu wykorzystania systemu plików. Polecenie **sudo quotaon -uv /uczniowie** powoduje włączenie mechanizmu quoty. Polecenie **sudo quotaon -ap** pozwala na weryfikację działania quoty (rys. 17.2).



Rys. 17.2. **Sprawdzanie, czy quota jest włączona**

> **! UWAGA**
>
> Po wykonaniu polecenia **sudo quotacheck -cum /uczniowie** trzeba sprawdzić, czy nie zostały zmienione uprawnienia do katalogu **/uczniowie**. W razie konieczności ponownie ustawić uprawnienia na 777.

4. Przydzielić przestrzeń dyskową użytkownikom – przydziały są ustalane indywidualnie dla każdego użytkownika. Do edycji przydziałów można wykorzystać polecenie **edquota**, np.:

   sudo edquota -u uczen1

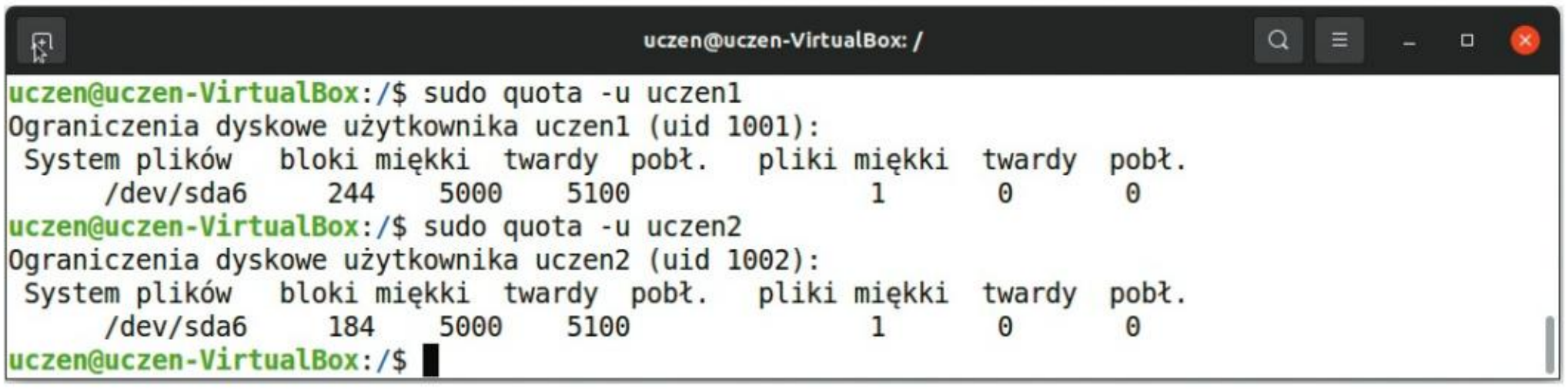
   Umożliwia ono edycję przydziałów w domyślnym edytorze (rys. 17.3). W kolumnach „bloki" oraz „i-węzły" jest wyświetlana liczba aktualnie używanych jednostek. Przestrzeń dyskowa przeznaczona dla użytkownika może być określana za pomocą liczby bloków (o rozmiarze 1 kB) lub i-węzłów. **Limit miękki** (ang. *soft*) może być przekroczony, ale tylko w określonych warunkach. **Limitu twardego** (ang. *hard*) nie można przekroczyć.

Rys. 17.3. **Edycja przydziałów dyskowych użytkownika**

17.1. Testowanie przydziałów dyskowych użytkownika

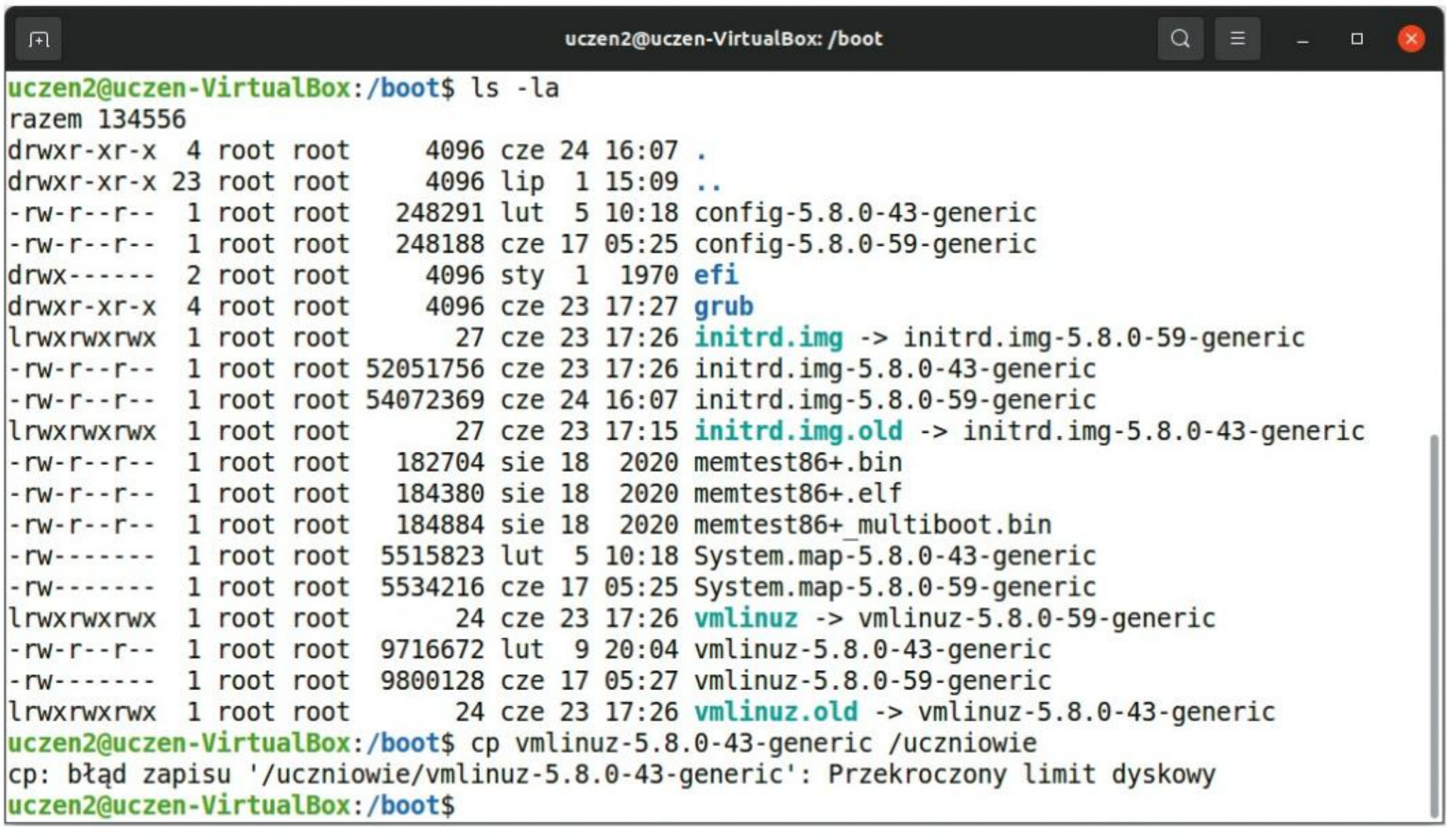
Przydziały dyskowe użytkownika umożliwiają ograniczenie przestrzeni dyskowej zajmowanej przez zbiory użytkownika. Każdy z użytkowników może na bieżąco kontrolować rozmiar aktualnie wykorzystanej przestrzeni i przyznane mu limity. Do wyświetlenia tych informacji (rys. 17.4) można wykorzystać polecenie **`sudo quota -u uczen1`**.

> **! UWAGA**
>
> Należy wcześniej utworzyć lub skopiować plik do katalogu **`/uczniowie`**, korzystając z konta użytkowników *uczen1* i *uczen2*.

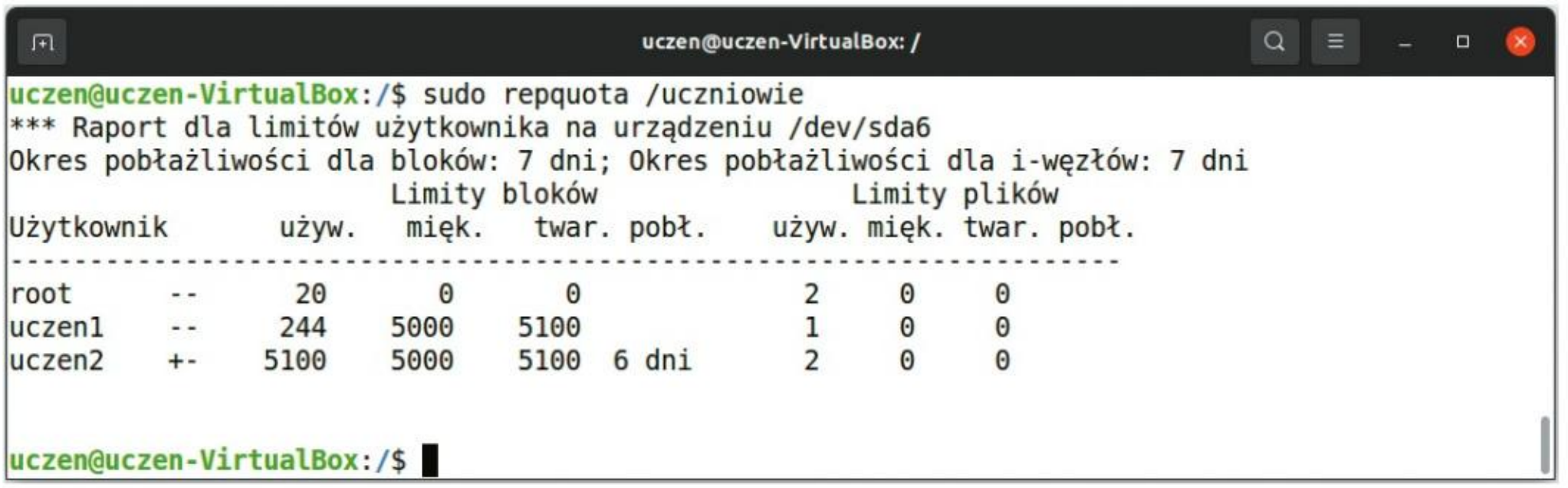


Rys. 17.4. **Sprawdzanie przyznanych przydziałów dyskowych**

Gwiazdka przy liczbie używanych bloków oznacza przekroczenie limitu przez użytkownika. Jeżeli użytkownik przekroczy limit przyznanych przydziałów dyskowych, to system nie dopuści do wykonania polecenia, które powoduje naruszenie limitu (rys. 17.5).



Rys. 17.5. **Informacja o przekroczeniu przydziału dyskowego**



Rys. 17.6. Raport z wykorzystania przydziałów dyskowych

Użytkownik z uprawnieniami *root* może kontrolować przydziały wszystkich użytkowników (rys. 17.6) za pomocą narzędzia **repquota**, np. **sudo repquota /uczniowie**.

PRZYKŁAD 17.1

Tworzenie przydziałów dyskowych dla użytkowników indywidualnych

Aby wprowadzić przydziały dyskowe dla użytkownika, należy:

1. Zalogować się na konto użytkownika z uprawnieniami *root*.
2. Zmodyfikować plik **/etc/fstab** – w opcjach opisu opcji montowania partycji dodać wpis **usrquota**.
3. Ponownie zamontować system plików za pomocą polecenia:

   ```
   sudo mount -o remount /uczniowie
   ```

4. Utworzyć plik **aquota.user** zawierający opis przydziałów. W pliku **aquota.user** umieścić tabelę zawierającą informacje o aktualnym stopniu wykorzystania systemu plików za pomocą polecenia:

   ```
   sudo quotacheck -cum /uczniowie
   ```

5. Włączyć przydziały dyskowe za pomocą polecenia:

   ```
   sudo quotaon -uv /uczniowie
   ```

6. Poleceniem **sudo quotaon -ap** zweryfikować działanie quoty.
7. Przydzielić przestrzeń dyskową dla użytkownika *uczen1*. Do edycji przydziałów można wykorzystać polecenie **edquota**, np.:

   ```
   sudo edquota -u uczen1
   ```

8. Wartości limitu miękkiego i twardego można ustawić odpowiednio na **5000** i **5100** bloków.
9. Wyświetlić informację o przydziale za pomocą polecenia:

   ```
   sudo quota -u uczen1
   ```

10. Uruchomić ponownie komputer i zalogować się na konto użytkownika *uczen1*.
11. Przetestować działanie przydziałów – kopiować zbiory do katalogu **/uczniowie** aż do przekroczenia przyznanego limitu.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Utwórz partycję przeznaczoną do przechowywania stron internetowych użytkowników. Za pomocą quoty ogranicz liczbę danych użytkowników do 50 MB.
2. Utwórz partycję przeznaczoną na katalogi domowe użytkowników. Za pomocą quoty ogranicz liczbę danych w katalogach domowych użytkowników do 100 MB.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyjaśnij, do czego służą przydziały dyskowe.
2. Uzasadnij, dlaczego katalogi domowe użytkowników powinny być zlokalizowane na oddzielnej partycji. Które inne zbiory powinny być, twoim zdaniem, umieszczone na oddzielnej partycji?
3. Wyjaśnij różnicę między limitem miękkim i limitem twardym w przydziałach dyskowych.

18 Przydziały dyskowe grupy użytkowników

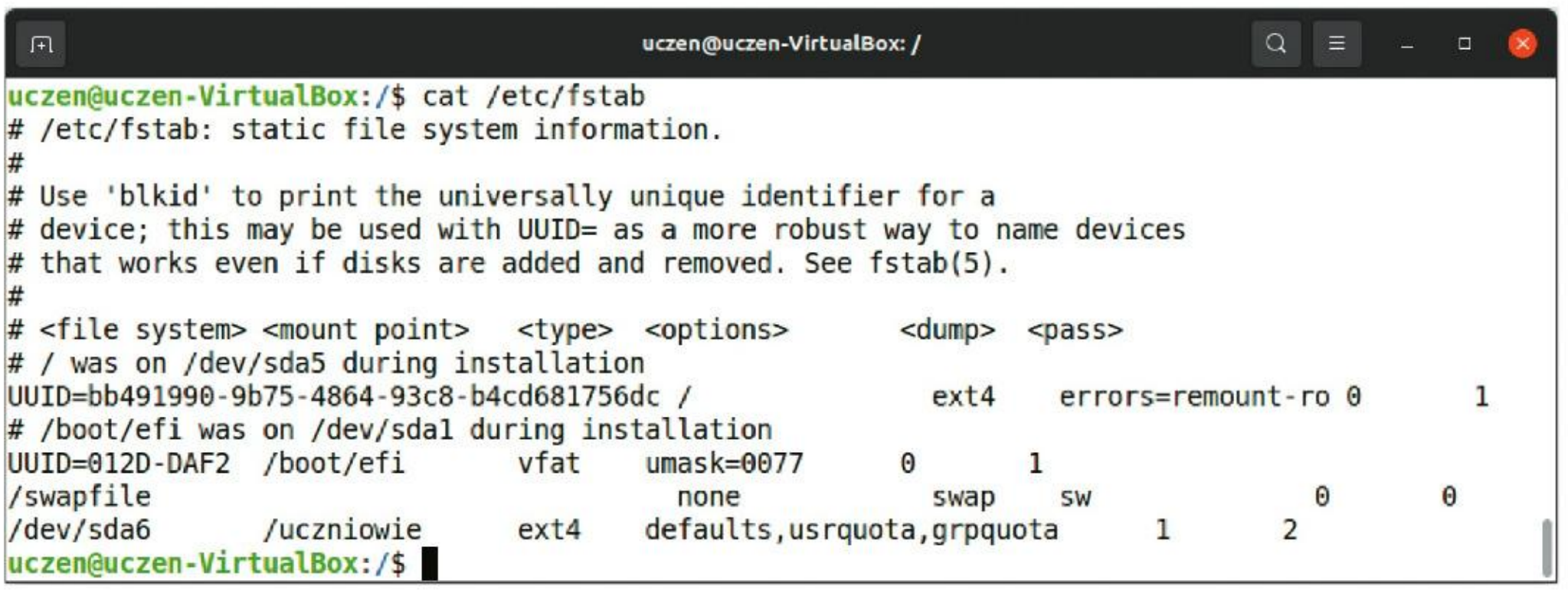
ZAGADNIENIA

- **Przebieg procesu przydzielania przestrzeni dyskowej na poziomie grupy użytkowników**
- **Przydziały dyskowe dla grup użytkowników**

Przydziały dyskowe grupy użytkowników pozwalają na określenie maksymalnego obszaru dysku zajmowanego przez zbiory wszystkich członków danej grupy. Podobnie jak przydziały użytkowników, przydziały dyskowe są przyznawane dla każdej partycji niezależnie. Aby wprowadzić przydziały dyskowe na poziomie grupy użytkowników, należy:

1. Zmodyfikować plik **/etc/fstab** – w opcjach opisu wariantów montowania partycji dodać wpis **grpquota** (rys. 18.1). Jeżeli przydziały dyskowe są przyznawane zarówno na poziomie użytkowników, jak i grup, to dodać również opcję **usrquota**.
2. Ponownie zmontować system plików – można ponownie uruchomić komputer lub wpisać polecenie:

   ```
   sudo mount -o remount /uczniowie
   ```



Rys. 18.1. **Wprowadzenie mechanizmu quota dla grup na partycji /dev/sda6**

3. Utworzyć plik zawierający opis przydziałów – informacje o przydziałach dyskowych poszczególnych grup użytkowników są przechowywane w pliku **aquota.group**. Musi on znajdować się w katalogu stanowiącym punkt montowania (w opisywanym przypadku jest to katalog **/uczniowie**). W pliku należy umieścić tabelę zawierającą informacje o aktualnym stopniu wykorzystania systemu plików za pomocą polecenia:

   ```
   sudo quotacheck -cgumf /uczniowie
   ```

4. Włączyć przydziały dyskowe dla grupy poleceniem:

   sudo quotaon -gv /uczniowie

5. Zweryfikować działanie quoty poleceniem:

   sudo quotaon -ap

   Przydzielić przestrzeń dyskową dla grup użytkowników – przydziały są ustalane indywidualnie dla każdej grupy. Grupa musi wcześniej istnieć w systemie. Do edycji przydziałów można wykorzystać polecenie **edquota**, np.:

   sudo edquota -g uczniowie

Znaczenie poszczególnych wpisów jest takie samo jak w przydziałach dla użytkowników. Użytkownik *root* może wykorzystać do zarządzania przydziałami grup następujące polecenia:

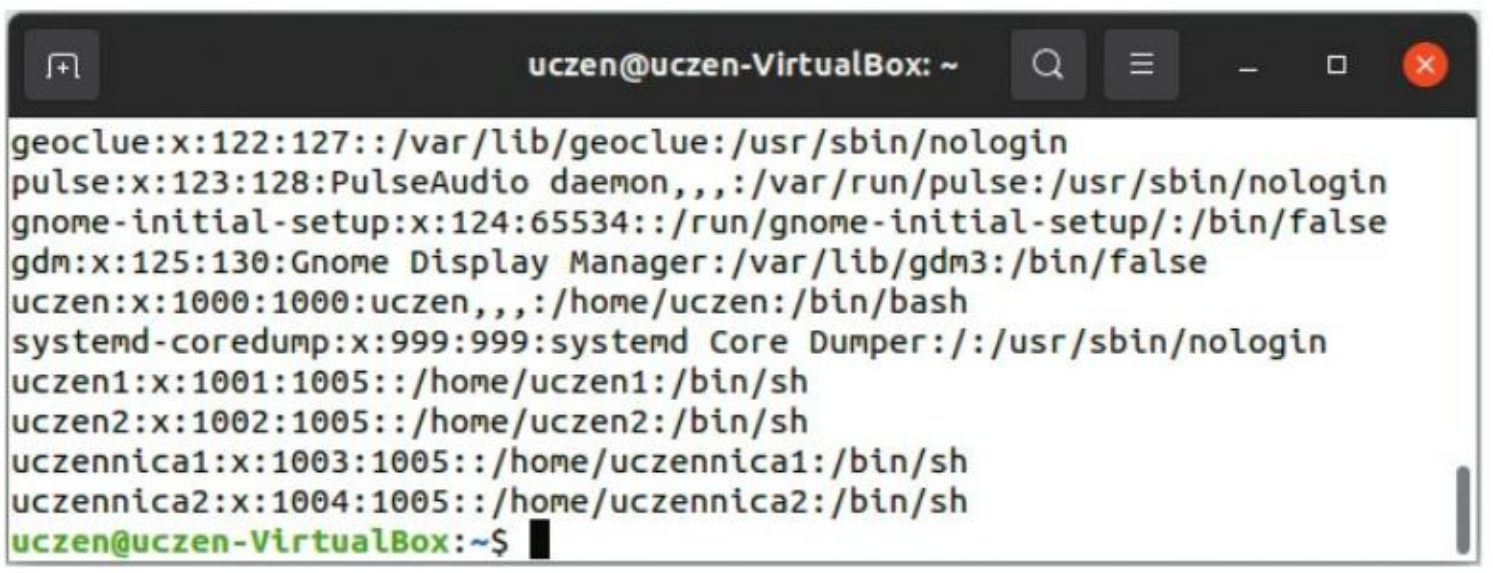
- wyświetlić informacje o przydziałach dyskowych grupy za pomocą polecenia:

  sudo quota -g uczniowie

- wyświetlić raport limitów dla grup w określonym systemie plików za pomocą polecenia:

  sudo repquota -g /uczniowie

Aby przetestować działanie przydziałów dyskowych grupy, należy dodać użytkowników do grupy, której przyznano przydziały. W pliku **/etc/passwd** dla każdego konta w miejscu na identyfikator grupy trzeba wpisać identyfikator tej grupy, dla której przyznano przydziały (rys. 18.2). Jeżeli grupa *uczniowie* ma przypisany identyfikator **1005** (można to sprawdzić w pliku **/etc/group**), to dla wszystkich członków grupy *uczniowie* należy ustawić identyfikator grupy **1005**.



Rys. 18.2. **Zmiana przynależności użytkownika do grupy**

PRZYKŁAD 18.1

Tworzenie przydziałów dyskowych dla grup użytkowników

Aby wprowadzić przydziały dyskowe dla grup użytkowników, należy:

1. Zalogować się na konto z uprawnieniami użytkownika *root*.
2. Utworzyć grupę *uczniowie* i przypisać do niej użytkowników *uczen1*, *uczen2*.
3. Zmodyfikować plik **/etc/fstab** – w opcjach opisu opcji montowania partycji dodać wpis **grpquota**.
4. Ponownie zamontować system plików za pomocą polecenia:

   sudo mount -o remount /uczniowie

5. Włączyć przydziały dyskowe dla grupy poleceniem:

   `sudo quotaon -gv /uczniowie`

6. Zweryfikować działanie quoty poleceniem:

   `sudo quotaon -ap`

7. Utworzyć plik **`aquota.group`** zawierający opis przydziałów. W pliku **`aquota.group`** umieścić tabelę zawierającą informacje o aktualnym stopniu wykorzystania systemu plików poleceniem:

   `sudo quotacheck -cgumf /uczniowie`

8. Przydzielić przestrzeń dyskową dla grupy *uczniowie*. Do edycji przydziałów można wykorzystać polecenie **`edquota`**, np.:

   `sudo edquota -g uczniowie`

9. Wyświetlić informację o przydziale za pomocą polecenia:

   `sudo quota -g uczniowie`

10. Uruchomić ponownie komputer i zalogować się na konto użytkownika *uczen2*.
11. Przetestować działanie przydziałów – kopiować zbiory do katalogu **`/uczniowie`** aż do przekroczenia przyznanego limitu.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Na serwerze z systemem Linux mają być udostępniane strony WWW użytkowników. Maksymalny rozmiar strony nie może przekroczyć 25 MB dla użytkownika indywidualnego (strona domowa wraz z katalogiem domowym). Ponadto na serwerze mogą być udostępniane strony użytkowników komercyjnych. Maksymalny rozmiar takiej strony to 100 MB. Zaplanuj mechanizmy wymuszające na użytkownikach przestrzeganie tych zasad.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyjaśnij, dlaczego warto zakładać quotę dla użytkowników.
2. Opisz proces przydzielania przestrzeni dyskowej na poziomie grupy użytkowników w systemie Linux.

19 Udostępnianie zasobów systemu Linux klientom MS Windows

ZAGADNIENIA

Oprogramowanie Samba **Przebieg procesu instalowania oprogramowania Samba** **Konfigurowanie serwera Samba** **Plik konfiguracyjny serwera Samba** **Narzędzia do konfiguracji serwera Samba w środowisku graficznym** **Zasoby udostępnione przez serwer Samba w systemie Windows**

Przez większość użytkowników Linux jest postrzegany jako wydajny system operacyjny przeznaczony do instalowania na serwerach. W typowych zastosowaniach domowych lub biurowych na stacjach roboczych klientów są instalowane różne wersje Windows. Konieczne w takiej sytuacji jest tworzenie mieszanego środowiska, w którym komputery z systemem operacyjnym Linux i Windows mogą wzajemnie korzystać ze swoich zasobów, takich jak pliki i drukarki.

Najwygodniej z punktu widzenia klienta byłoby, gdyby serwer z systemem Linux świadczył usługi za pomocą protokołu **SMB** (ang. *Server Message Block*), wykorzystywanego w środowisku Windows. Świadczenie usług klientom pracującym w środowisku Windows w taki sposób, jak robią to serwery Windows, zapewnia w systemie Linux oprogramowanie **Samba**.

Oprogramowanie Samba składa się z dwóch demonów:

- **`smbd`** – demon umożliwiający współdzielenie plików i drukarek w sieci SMB, zapewnia uwierzytelnianie klientów SMB;
- **`nmbd`** – demon odpowiedzialny za obsługę żądań serwera nazw NetBIOS, świadczy usługi WINS (ang. *Windows Internet Name Service*) i wspomaga przeglądanie zasobów sieci.

Uruchomienie serwera **`Samba`** następuje w kilku etapach:

- instalacja oprogramowania;
- włączenie uruchamiania demonów **`nmdb`** i **`smbd`** podczas startu systemu – dzięki temu usługi będą dostępne natychmiast po uruchomieniu komputera;
- konfiguracja serwera **`Samba`**;
- utworzenie kont użytkowników;
- utworzenie udostępnianych udziałów i przydzielenie uprawnień;
- testowanie serwera.

Oprogramowanie Samba może oferować wybrane usługi charakterystyczne dla systemów serwerowych z rodziny Windows i świadczone innym stacjom roboczym.

PRZYKŁAD 19.1

Instalowanie oprogramowania Samba

Aby umożliwić użytkownikowi systemu Linux udostępnianie zasobów klientom Windows, należy:

1. Zainstalować oprogramowanie Samba – wpisać polecenie:

```
sudo apt install samba
```

2. Po dokonaniu zmian w konfiguracji serwera ponownie uruchomić usługi, np. wpisać polecenia:

```
sudo service nmbd restart
```

i

```
sudo service smbd restart
```

Serwer **Samba** umożliwia zapewnienie klientom pracującym w systemie Windows dostępu do drukarek i katalogów. Drukarka, która ma być udostępniana, musi zostać wcześniej zainstalowana w systemie Linux. Klienci Windows muszą mieć sterowniki przeznaczone dla ich systemu operacyjnego. Katalog, który ma być udostępniany, musi istnieć w systemie, a użytkownicy muszą posiadać odpowiednie uprawnienia w systemie plików.

PRZYKŁAD 19.2

Konfigurowanie serwera Samba

W tym ćwiczeniu zostanie skonfigurowany serwer **Samba**, który udostępnia zasoby w grupie roboczej Windows. Aby utworzyć nowy katalog o nazwie **samba**, przeznaczony dla klientów Windows, i nadać uprawnienia wszystkim użytkownikom, należy:

1. Utworzyć katalog i nadać mu odpowiednie uprawnienia, np. za pomocą poleceń:

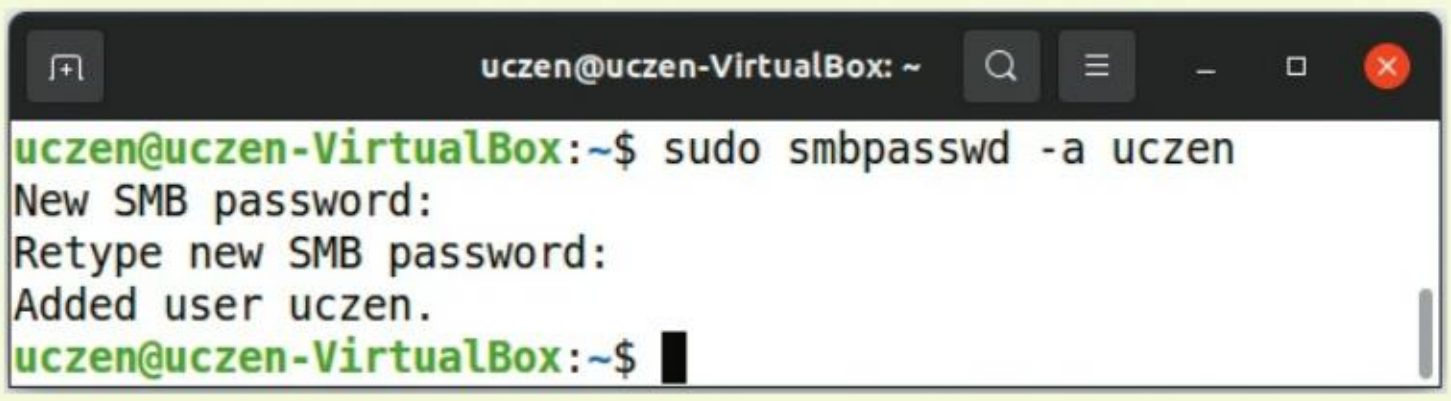
```
sudo mkdir /samba
```

i

```
sudo chmod 777 /samba
```

2. **Samba** ma własną bazę danych użytkowników i system haseł. Dla Samby trzeba utworzyć użytkownika, np. *uczen*, i hasło, np. *Qwerty123* (rys. 19.1):

```
sudo smbpasswd -a uczen
```



Rys. 19.1. **Tworzenie użytkownika w serwerze Samba**

3. Zmodyfikować plik konfiguracyjny **/etc/samba/smb.conf** (rys. 19.2):
   - w linii 29. ustawić nazwę grupy roboczej, np.:

     ```
     workgroup = ZSP51
     ```

   - w linii 39. wprowadzić informacje o interfejsach wykorzystywanych do świadczenia usługi, np.:

     ```
     interfaces = 127.0.0.0/8 10.0.0.0/8 eth0
     ```

   - usunąć komentarz w linii 46.:

     ```
     bind interfaces only = yes
     ```

```
uczen@uczen-VirtualBox: ~
uczen@uczen-VirtualBox:~$ cat /etc/samba/smb.conf
#
# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Some options that are often worth tuning have been included as
# commented-out examples in this file.
#  - When such options are commented with ";", the proposed setting
#    differs from the default Samba behaviour
#  - When commented with "#", the proposed setting is the default
#    behaviour of Samba but the option is considered important
#    enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

#======================= Global Settings =======================

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = ZSP51

# server string is the equivalent of the NT Description field
   server string = %h server (Samba, Ubuntu)

#### Networking ####

# The specific set of interfaces / networks to bind to
# This can be either the interface name or an IP address/netmask;
# interface names are normally preferred
   interfaces = 127.0.0.0/8 10.0.0.0 eth0

# Only bind to the named interfaces and/or networks; you must use the
# 'interfaces' option above to use this.
# It is recommended that you enable this feature if your Samba machine is
# not protected by a firewall or is a firewall itself.  However, this
# option cannot handle dynamic or non-broadcast interfaces correctly.
   bind interfaces only = yes
```

Rys. 19.2. **Konfiguracja sekcji globalnej pliku `/etc/samba/smb.conf`**

4. Wprowadzić na końcu sekcji **Zasobów współdzielonych** (ang. *Share Definitions*) informacje o zasobach współdzielonych, np. jak na rys. 19.3:

```
[Samba]
path = /samba
```

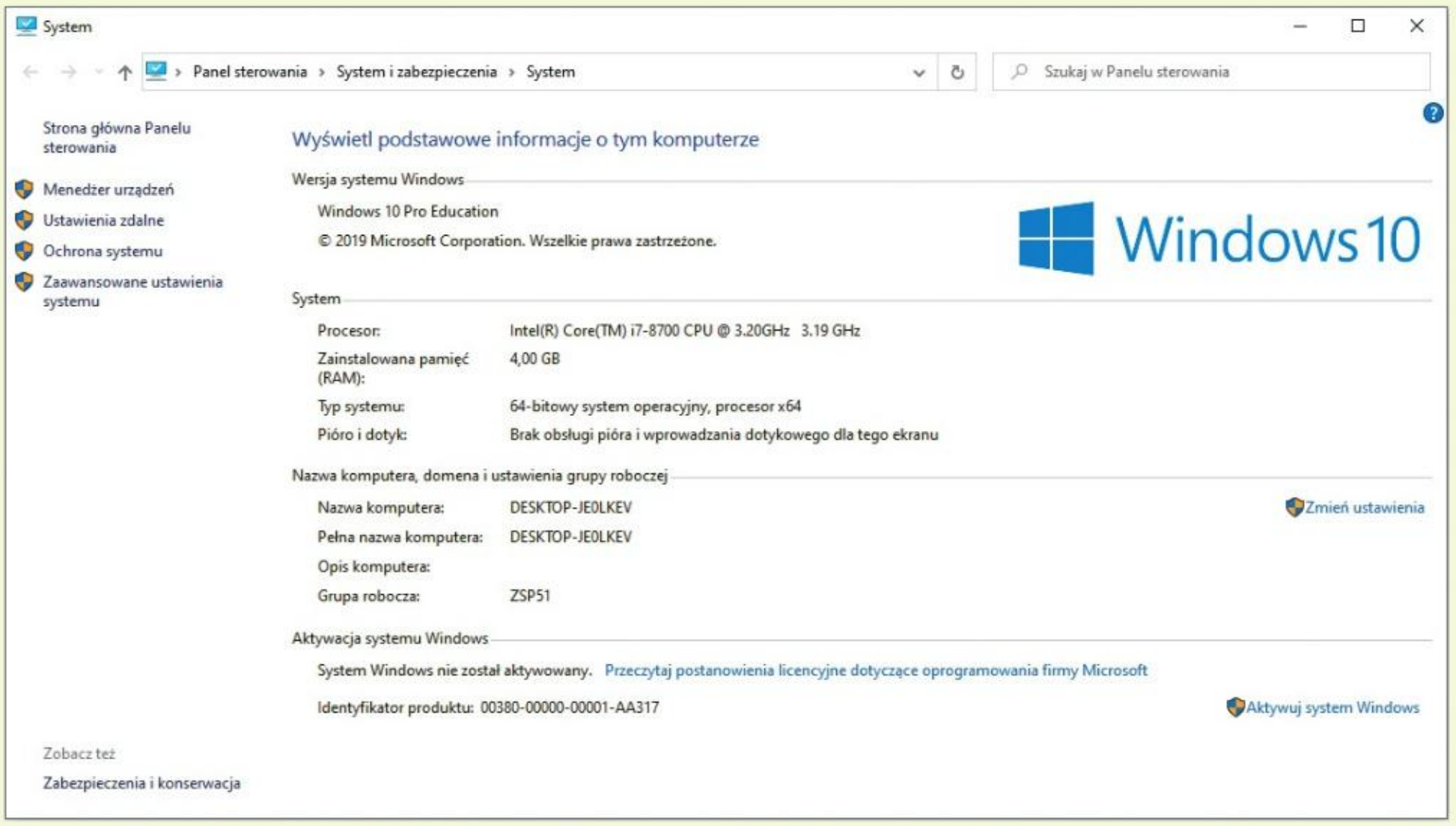
```
writable = yes
guest ok = yes
guest only = yes
create mode = 777
directory mode = 0777
```

uczen@uczen-VirtualBox: ~

```
#====================== Share Definitions ======================

# Un-comment the following (and tweak the other settings below to suit)
# to enable the default home directory shares. This will share each
# user's home directory as \\server\username
;[homes]
;   comment = Home Directories
;   browseable = no

# By default, the home directories are exported read-only. Change the
# next parameter to 'no' if you want to be able to write to them.
;   read only = yes

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
;   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
;   directory mask = 0700

# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# Un-comment the following parameter to make sure that only "username"
# can connect to \\server\username
# This might need tweaking when using external authentication schemes
;   valid users = %S

[printers]
   comment = All Printers
   browseable = no
   path = /var/spool/samba
   printable = yes
   guest ok = no
   read only = yes
   create mask = 0700

[Samba]
path = /samba
writable = yes
guest ok = yes
guest only = yes
create mode = 777
directory mode = 0777
```

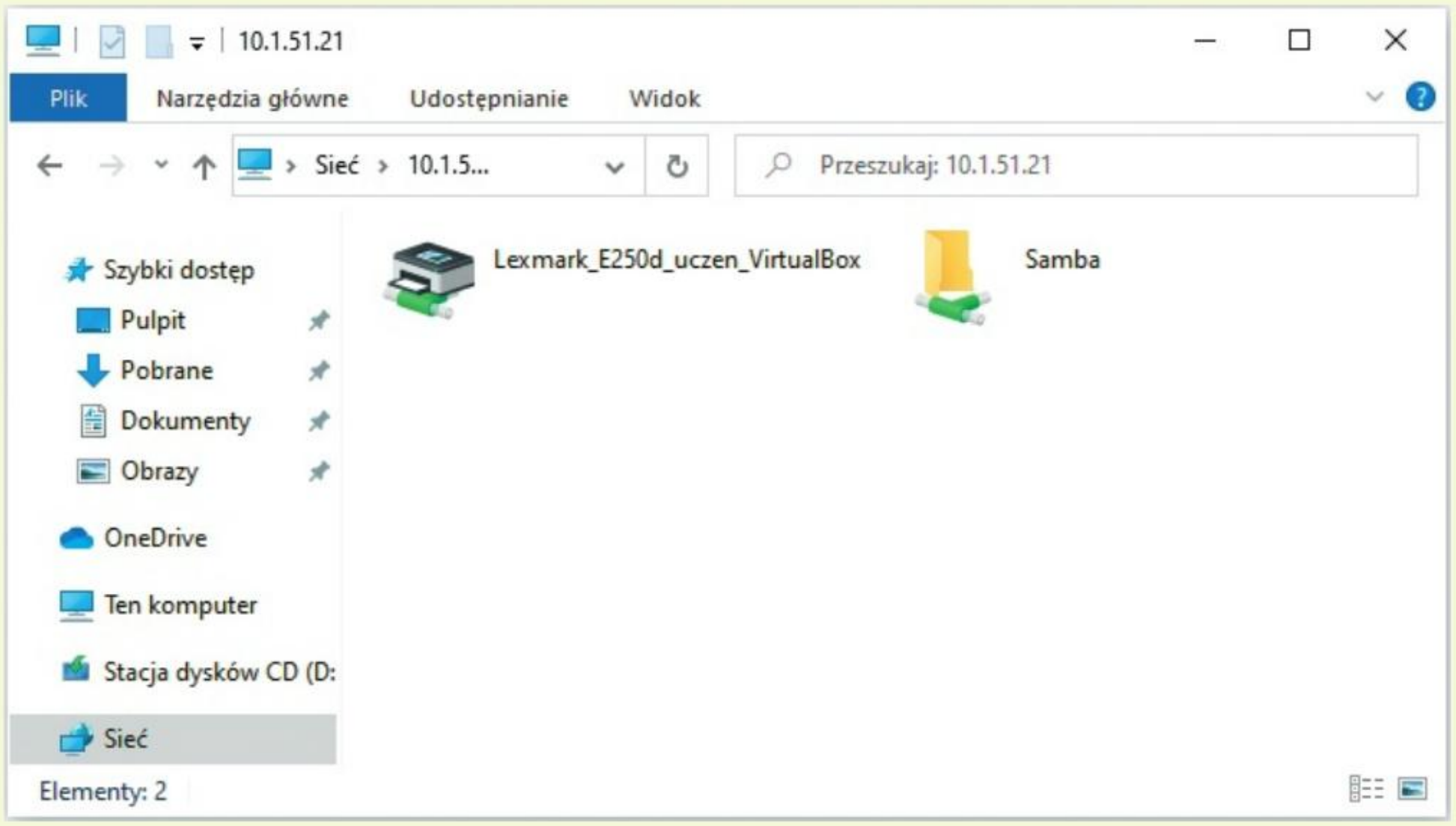
Rys. 19.3. **Konfiguracja sekcji zasobów współdzielonych pliku `/etc/samba/smb.conf`**

5. Skonfigurować komputer z systemem Windows 10 do pracy w grupie roboczej ZSP51 (rys. 19.4).



Rys. 19.4. **Konfiguracja komputera z systemem Windows 10 do pracy w grupie roboczej ZSP51**

6. Wyszukać w grupie roboczej komputer z uruchomionym serwerem **`Samba`** (rys. 19.5).



Rys. 19.5. **Przeglądanie zasobów udostępnionych przez serwer `Samba`**

19.1. Plik konfiguracyjny serwera Samba

Serwer **Samby** jest konfigurowany przez plik **/etc/samba/smb.conf**. Plik **smb.conf** jest podzielony na:

- **sekcję globalną** (ang. *global*) – definiuje parametry konfiguracyjne dla całego serwera;
- **sekcje** – definiują udostępniane zasoby.

Sekcja globalna (ang. *global*) definiuje parametry, które wpływają na cały system, np.:

- **workgroup** – określa grupę roboczą, której członkiem jest serwer;
- **server string** – to opisowy komentarz dla serwera;
- **log file** – ustala położenie pliku dziennika zawierającego informacje o zdarzeniach;
- **max log size** – wyznacza w kilobajtach maksymalny rozmiar pliku dziennika; domyślną wartością jest 5 MB, czyli 5000 kB. Jeśli maksymalny rozmiar pliku zostanie przekroczony, **smbd** zamyka dziennik, zmienia jego nazwę i dopisuje rozszerzenie **.old**.

Sekcję globalną z przykładowego pliku konfiguracyjnego serwera udostępniającego zasoby w grupie roboczej przedstawiono na rys. 19.6.

uczen@uczen-VirtualBox: ~

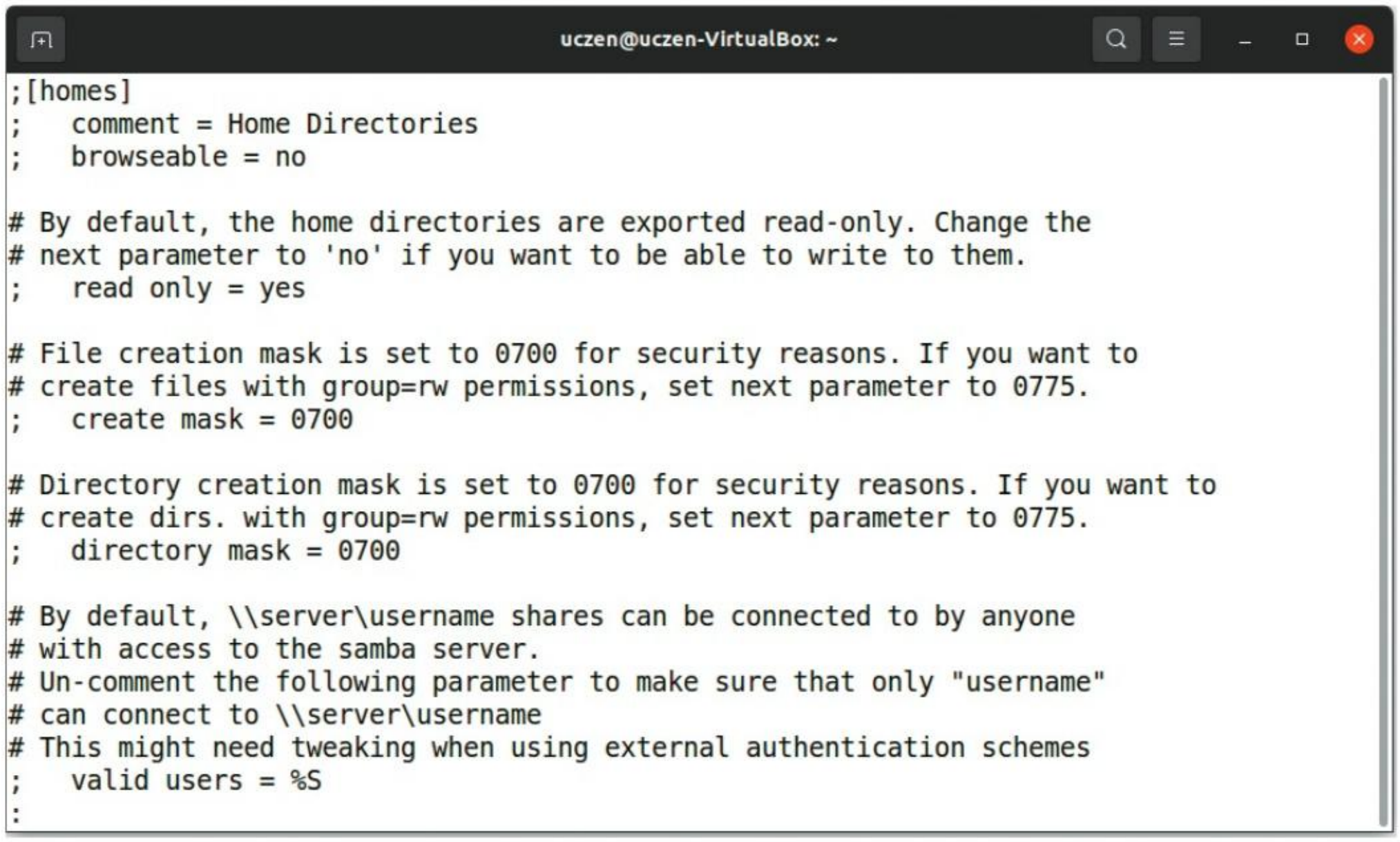
```
#====================== Global Settings =====================

[global]
        bind interfaces only = yes
        interfaces = 127.0.0.0/8 10.0.0.0/8 eth0
        max log size = 1000
        usershare allow guests = yes
        workgroup = ZSP51
        unix password sync = yes
        path = /windows
        passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully* .
        log file = /var/log/samba/log.%m
        passwd program = /usr/bin/passwd %u
        map to guest = bad user
        panic action = /usr/share/samba/panic-action %d
        server role = standalone server
        server string = %h server (Samba, Ubuntu)
        pam password change = yes
        logging = file
        comment = Windows
        obey pam restrictions = yes
```

Rys. 19.6. **Sekcja globalna z przykładowego pliku konfiguracyjnego**

Sekcja katalogów domowych (ang. *homes*) jest specjalną sekcją odnoszącą się do udziałów (zezwala użytkownikom na dostęp do ich katalogów domowych). Nie podaje określonej ścieżki do współdzielonego katalogu, lecz używa katalogu domowego z pliku **/etc/passwd** na podstawie nazwy użytkownika żądającego zasobu (rys. 19.7).

W sekcji można definiować m.in.:

- **comment** – to opis współdzielonego zasobu (komentarz);
- **browsable** – określa, czy wszyscy użytkownicy mogą przeglądać zawartość danego zasobu:
  - **no** – oznacza, że tylko użytkownicy z określonymi zezwoleniami, tzn. prawidłowym identyfikatorem, mogą przeglądać zasób;
  - **yes** – oznacza, że wszyscy użytkownicy mogą przeglądać zasób;
- **read only** – określa, czy do danego zasobu mogą być zapisywane pliki:
  - **no** – oznacza, że pliki mogą być zapisywane;
  - **yes** – oznacza, że zasób jest tylko do odczytu.



Rys. 19.7. **Sekcja katalogów domowych z przykładowego pliku konfiguracyjnego**

Sekcja drukarek (ang. *printers*) zawiera opcje związane z udostępnianiem drukarek. Lista drukarek jest pobierana z pliku **/etc/printcap**, w którym znajduje się opis wszystkich drukarek zainstalowanych w systemie. Dla każdej drukarki zdefiniowanej w pliku **/etc/printcap** zostaje utworzony specjalny udział umożliwiający drukowanie (rys. 19.8).

Sekcje katalogów współdzielonych przez Sambę – każda sekcja ma nazwę (wyświetlaną jako katalog w oknie **Sieć klienta**), a ponadto może zawierać opcje, np.:

- **path** – definiuje ścieżkę do katalogu oferowanego przez dany współdzielony zasób;
- **valid users** – pozwala określić listę użytkowników uprawnionych do korzystania z udziału.

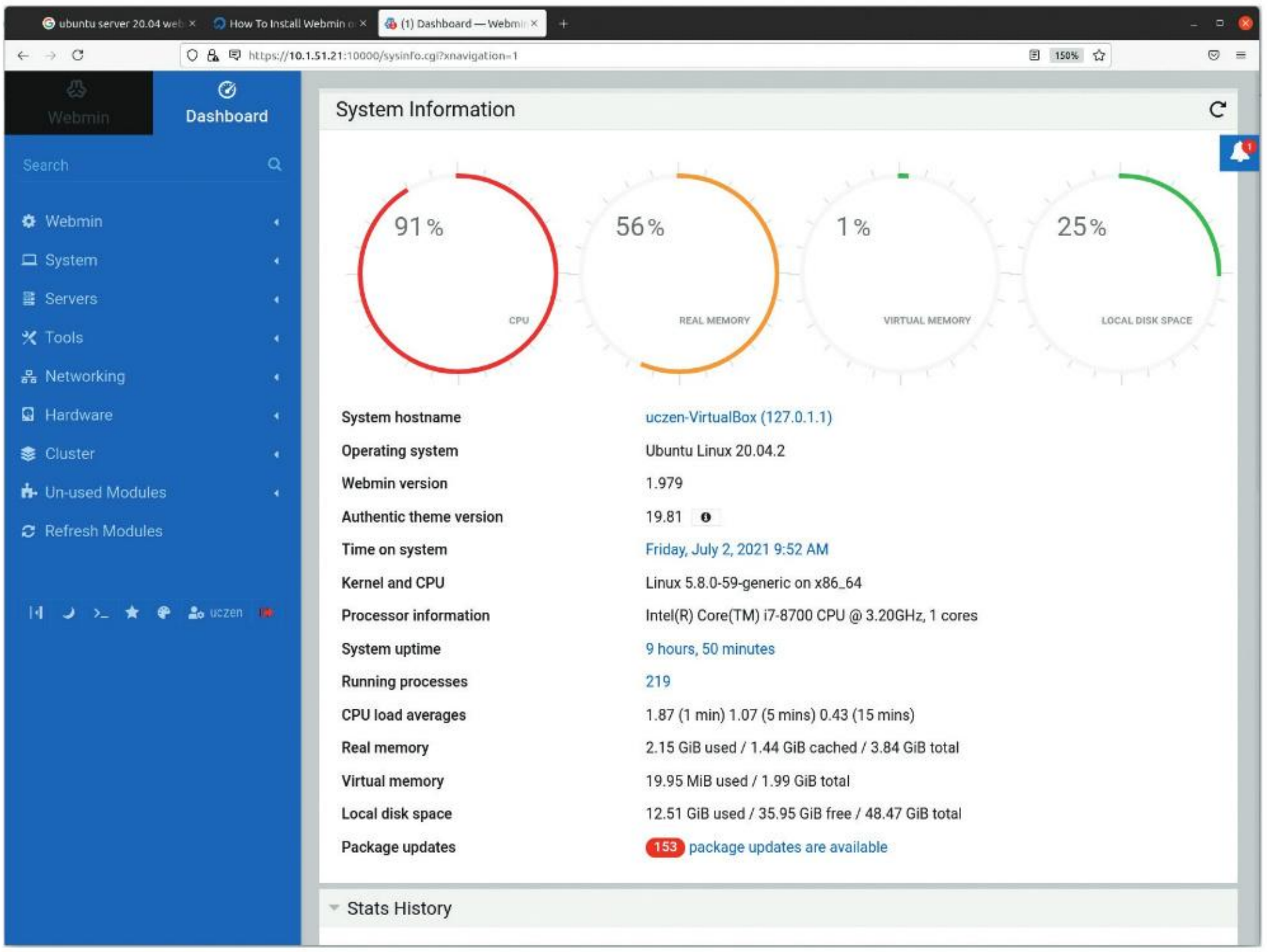
Ustawianie praw dostępu dla plików i katalogów uzyskuje się za pomocą opcji:

- **create mask** – kontroluje prawa dostępu używane podczas zapisywania przez klienta plików do katalogu współdzielonego; np. 750 oznacza, że pliki będą tworzone z uprawnieniami odczytu / zapisu / wykonywania dla właściciela, odczytu / wykonywania dla grupy i bez uprawnień dla reszty użytkowników;
- **directory mode** – definiuje prawa dostępu użyte podczas tworzenia przez klienta katalogu wewnątrz współdzielonego zasobu, np. directory mode 744.

Rys. 19.8. **Sekcje drukarek i katalogów współdzielonych z przykładowego pliku konfiguracyjnego**

19.2. Konfiguracja serwera Samba w środowisku graficznym

Jeżeli użytkownik chce włączyć możliwość pracy Samby jako kontroler domeny Windows lub zarządzać serwerem przez przeglądarkę internetową, powinien skorzystać z bardziej zaawansowanych programów, np. **SWAT**, **Webmin**, bądź przeprowadzić konfigurację za pomocą edycji pliku konfiguracyjnego. Okno programu Webmin przedstawiono na rys. 19.9.



Rys. 19.9. **Okno programu Webmin**

PRZYKŁAD 19.3

Instalowanie i uruchomienie programu Webmin

W tym ćwiczeniu zostanie skonfigurowany i uruchomiony program **Webmin**, umożliwiający zarządzanie Linuksem w środowisku graficznym. Aby go zainstalować, należy:

1. Zaktualizować bazę repozytoriów oprogramowania, np. za pomocą polecenia:
   `sudo apt update;`
2. Otworzyć plik `/etc/apt/sources.list` za pomocą dowolnego edytora tekstu, np.:
   `sudo nano /etc/apt/sources.list;`
3. Dodać w pliku `/etc/apt/sources.list` repozytorium programu Webmin.
   Na końcu pliku dopisać wiersz:
   `deb http://download.webmin.com/download/repository sarge contrib`
   Zapisać zmiany w pliku, wybierając kolejno [Ctrl] + [o] i [Ctrl] + [x];
4. Pobrać klucz Webmin PGP, który spowoduje, że komputer będzie ufał nowo dodanemu repozytorium. Klucz musi zostać dodany do listy kluczy. Wykonać polecenie:
   `wget -q -O- http://www.webmin.com/jcameron-key.asc | sudo apt-key add`
5. Zaktualizować bazę repozytoriów oprogramowania, np. za pomocą polecenia:
   `sudo apt update;`
6. Zainstalować program Webmin za pomocą polecenia:
   `sudo apt install webmin`
7. Po zainstalowaniu Webmin nasłuchuje na porcie 10000. Aby połączyć się z nim, w oknie przeglądarki internetowej wpisać: `https://twoj_serwer:10000`, np. `https://10.1.51.21:10000`, a następnie zalogować się na konto użytkownika z uprawnieniami administratora, np. *uczen*.

Webmin pozwala na zdalną konfigurację systemu za pomocą przeglądarki internetowej. Dysponuje modułami do konfiguracji serwerów, np. Apache, DHCP, DNS, poczty elektronicznej i współdzielenia plików i drukarek przy użyciu Samby, oraz wieloma innymi funkcjami i narzędziami.

PRZYKŁAD 19.4

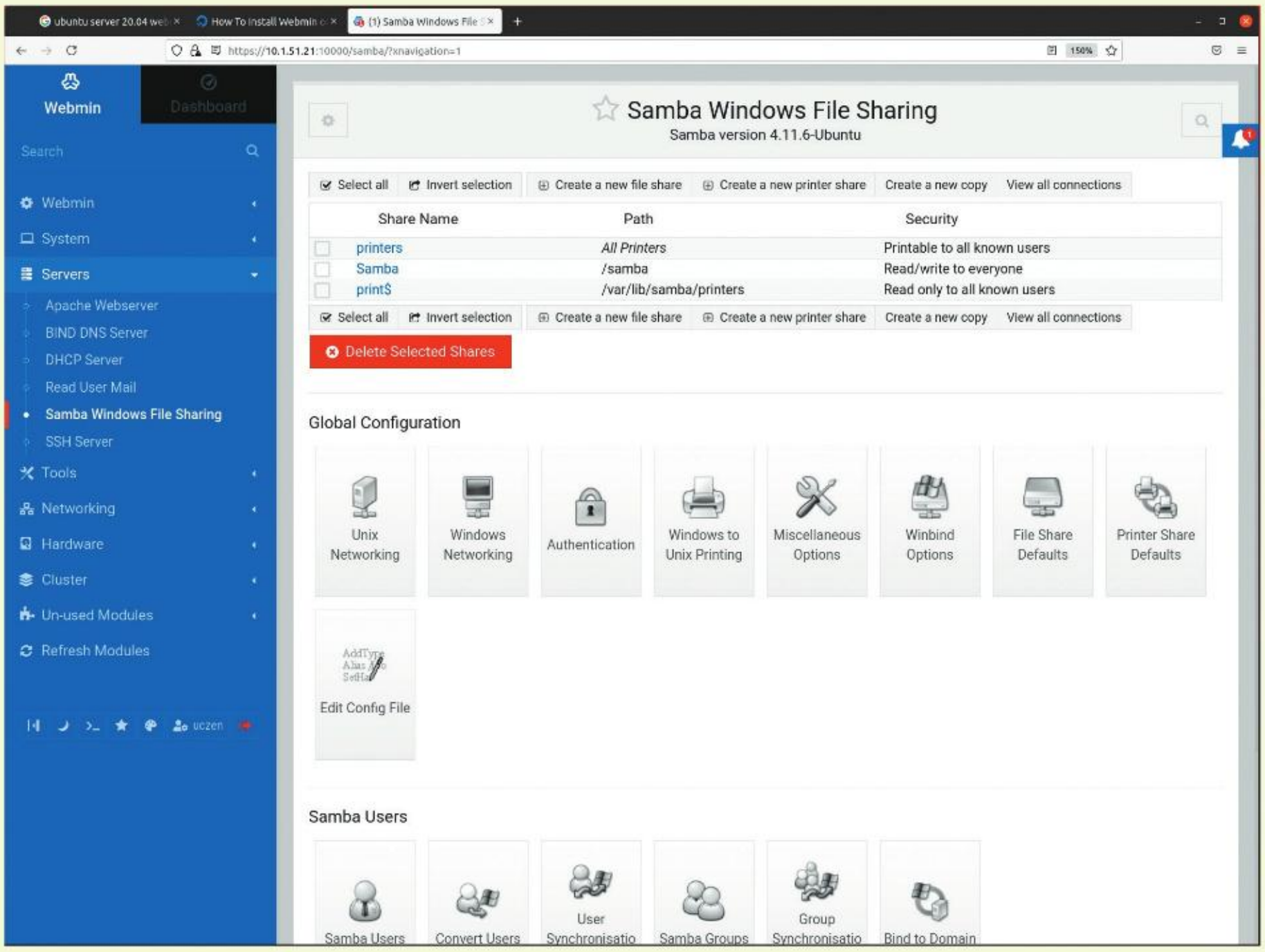
Zarządzanie serwerem Samba za pomocą programu Webmin

W tym ćwiczeniu zostanie udostępniony folder dla użytkowników Windows za pomocą programu Webmin.

Aby udostępnić zasób za pomocą Webmin, należy:

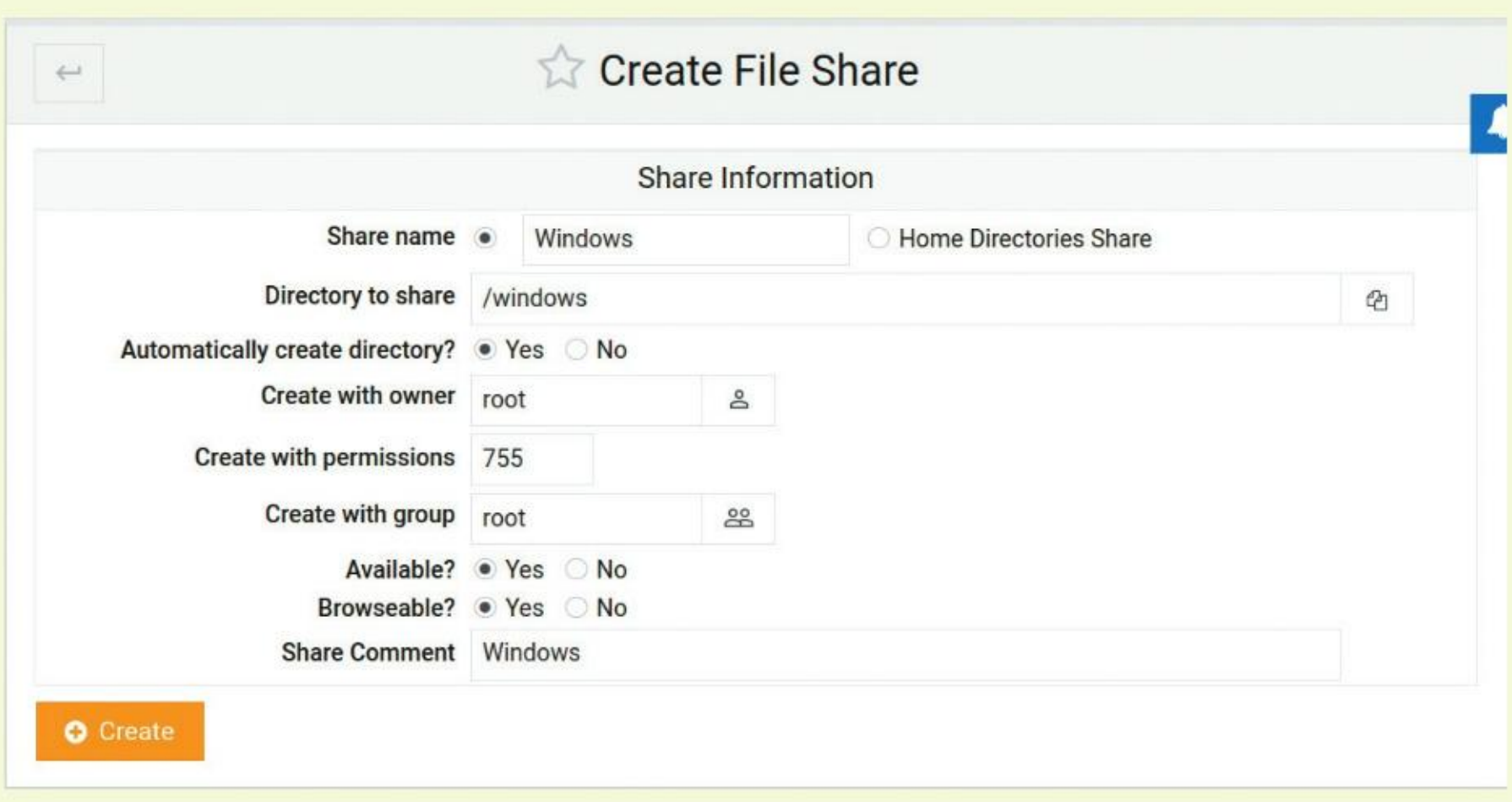
1. Utworzyć katalog i nadać mu odpowiednie uprawnienia, np. za pomocą poleceń:
   `sudo mkdir /windows`
   i
   `sudo chmod 777 /windows`
2. Uruchomić przeglądarkę internetową i nawiązać połączenie z serwerem. W polu adres przeglądarki wpisać `https://twoj_serwer:10000`, np. `https://10.1.51.21:10000`, i zalogować się na konto użytkownika z uprawnieniami administratora, np. *uczen*.

3. W lewym panelu wybrać sekcje **`Servers/Samba Windows File Sharing`** (rys. 19.10).



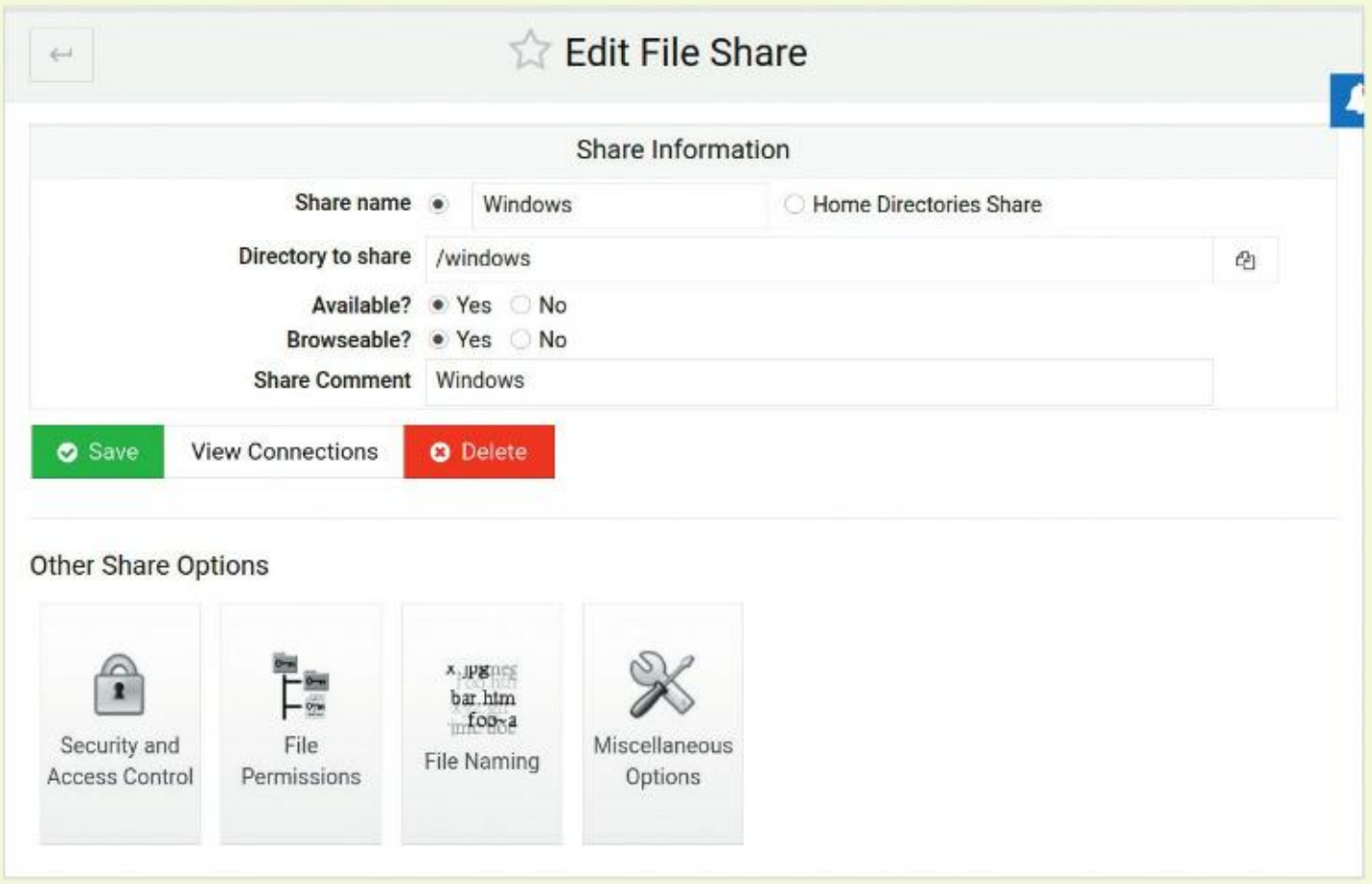
Rys. 19.10. **Zarządzanie serwerem Samba za pomocą Webmin**

4. Kliknąć ikonę **`Create a new file share`** (rys. 19.11). Wskazać udostępniany zasób, np. **`/Windows`**. Kliknąć przycisk **`Create`**.



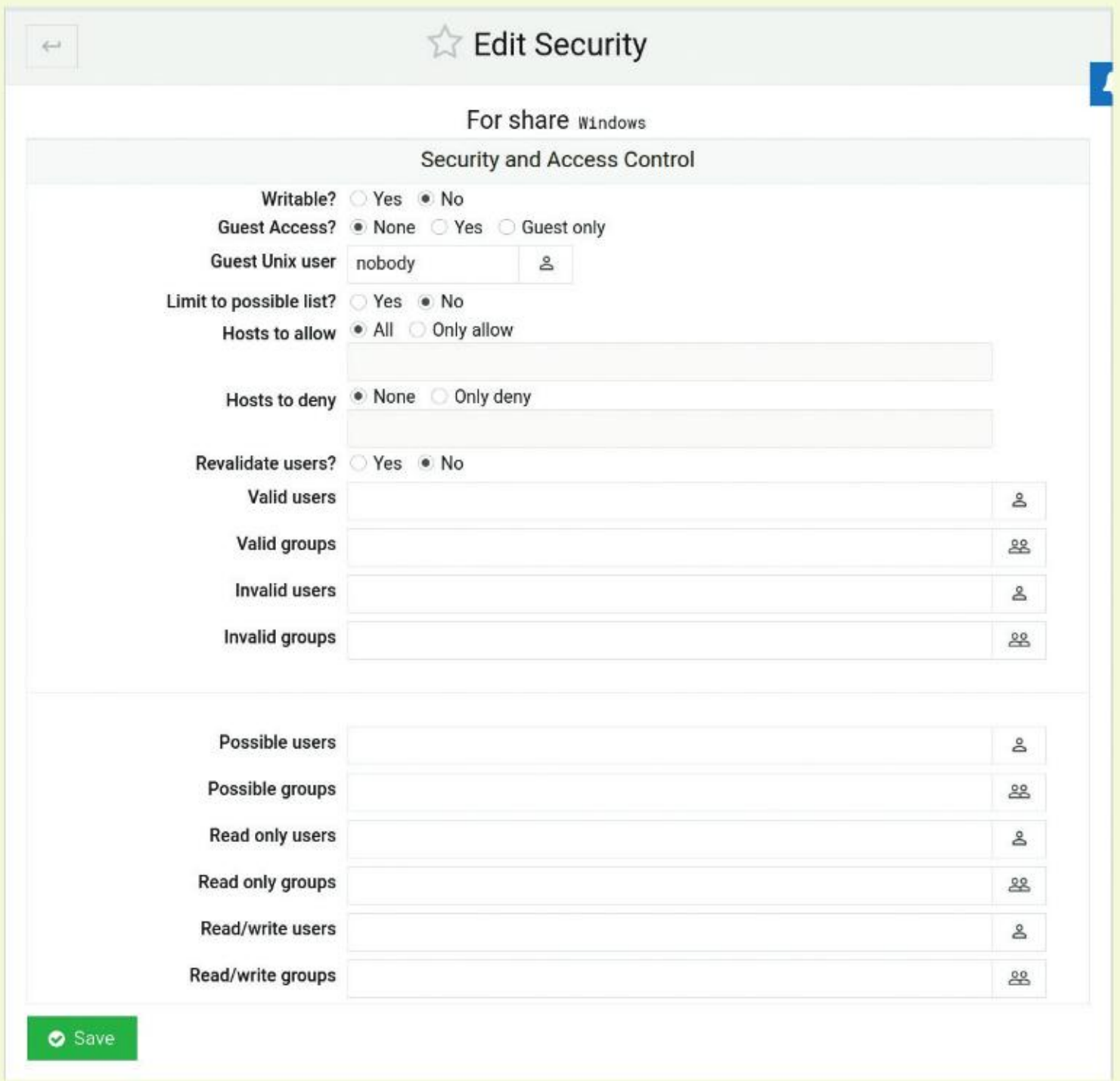
Rys. 19.11. **Tworzenie udostępnionego zasobu**

5. Wskazać udostępniany zasób, np. **`/Windows`** (rys. 19.12).



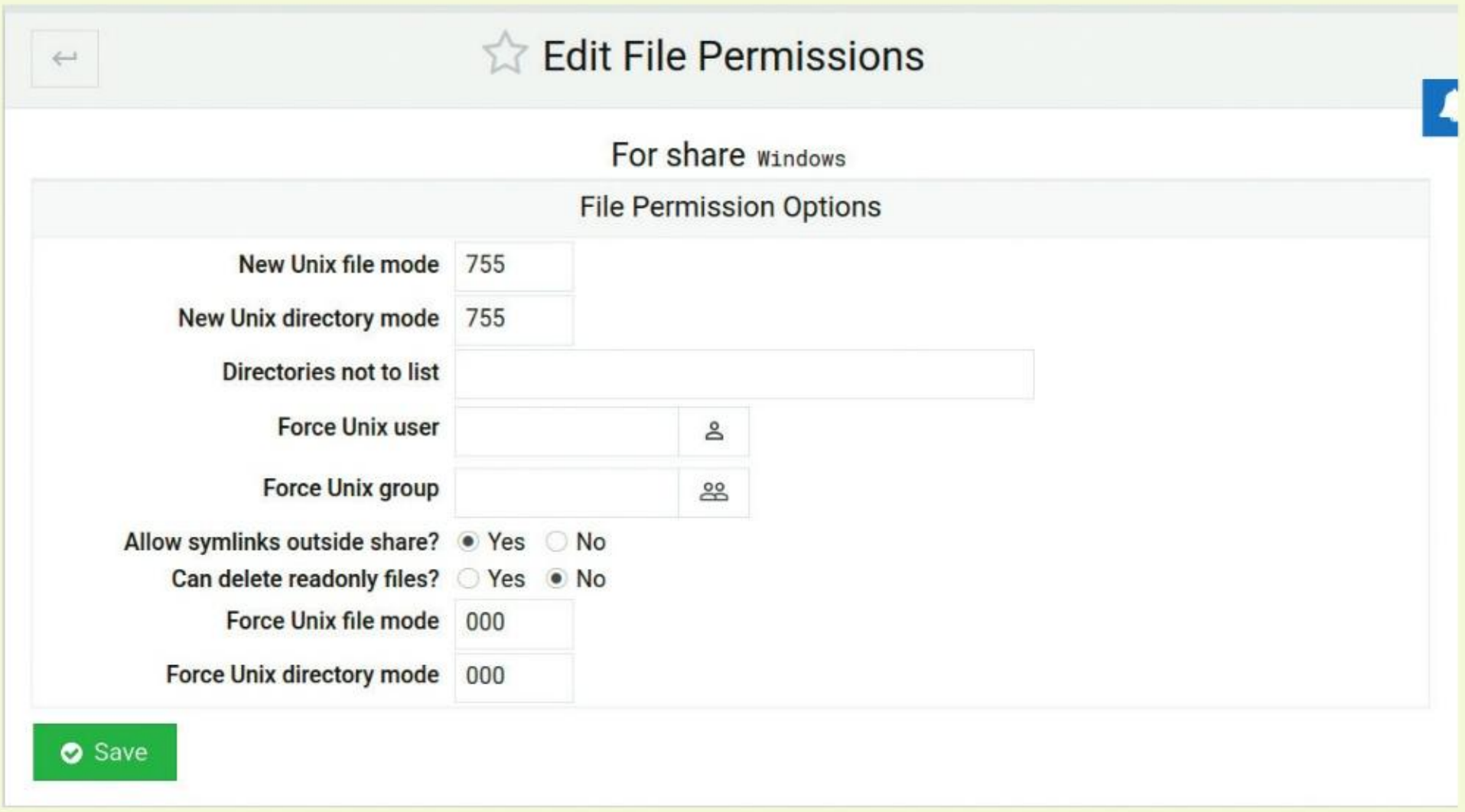
Rys. 19.12. **Edycja udostępnionego zasobu**

6. Kliknąć ikonę **`Security and Access Control`**. Określić uprawnienia w oknie **`Edit Security`** (rys. 19.13).



Rys. 19.13. **Edycja zasad bezpieczeństwa udostępnionego zasobu**

7. Kliknąć ikonę **File Permissions**. Określić uprawnienia w oknie **Edit File Permissions** (rys. 19.14).



Rys. 19.14. **Edycja uprawnień udostępnionego zasobu**

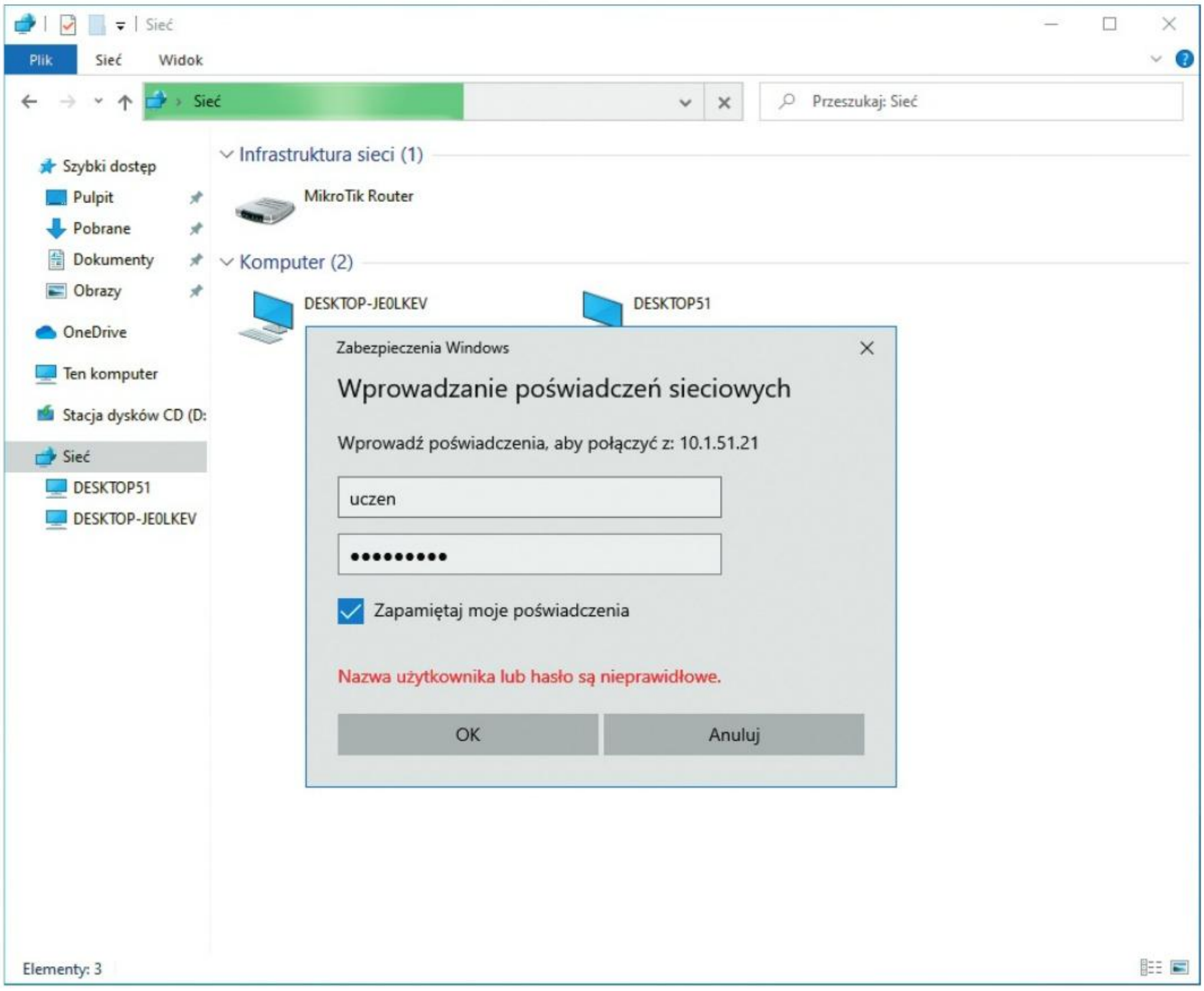
8. Pozostałe opcje można pozostawić jako wartości domyślne.
9. Sprawdzić, czy zasób jest dostępny dla użytkowników Windows.

19.3. Przeglądanie zasobów udostępnianych za pomocą serwera Samba

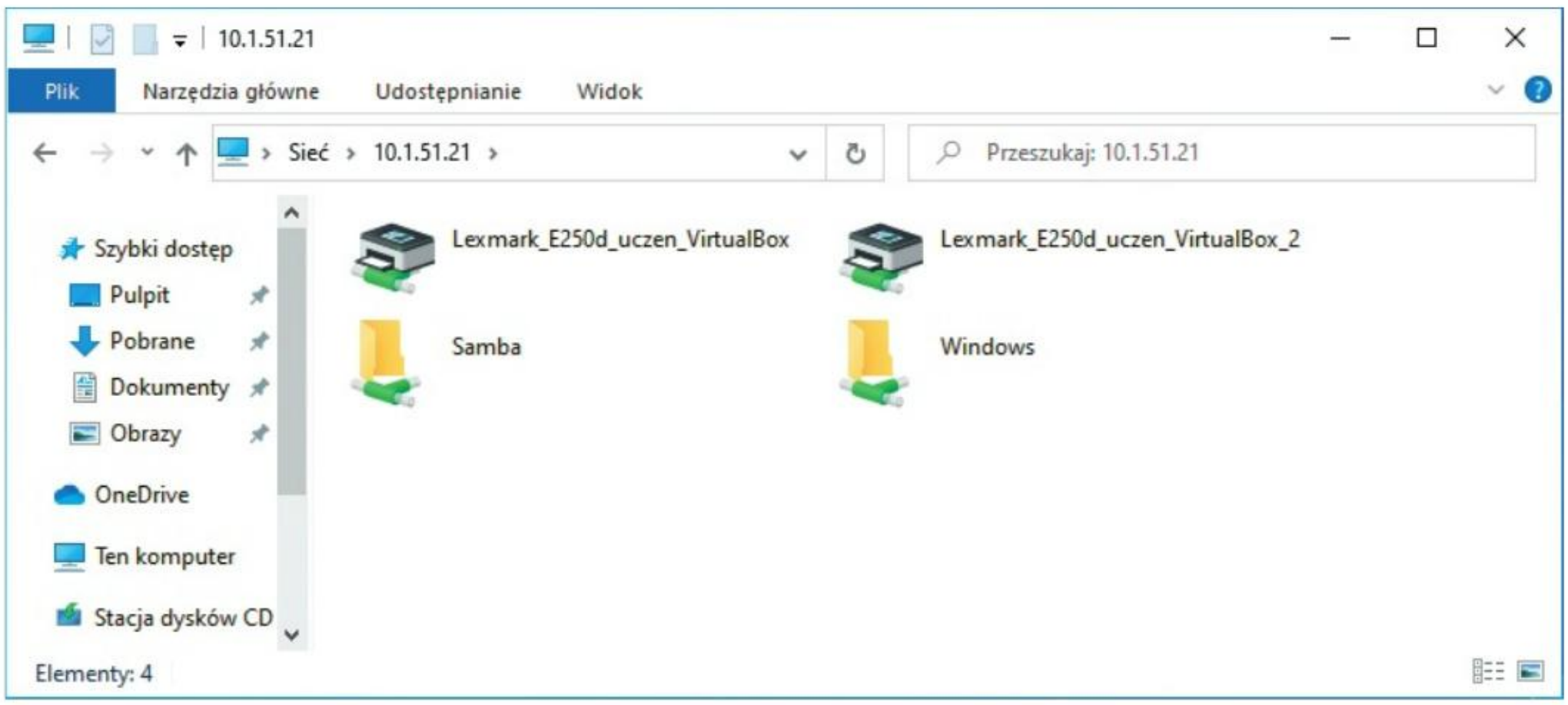
W większości przypadków z zasobów udostępnianych przez serwer **Samba** korzystają klienci z zainstalowanym systemem Windows. Zasoby serwera **Samba** są dostępne za pośrednictwem aplikacji **Sieć** lub jej odpowiednika w innych wersjach systemu Windows. Po wybraniu opcji **Sieć** są wyświetlane nazwy komputerów udostępniających zasoby w grupie roboczej. Dla aplikacji nie ma znaczenia, czy są to komputery z zainstalowanym Windowsem czy z Sambą. Podczas próby dotarcia do udostępnionego zasobu system zażąda podania nazwy konta i odpowiadającego mu hasła (rys. 19.15). Jeżeli użytkownik zamierza korzystać w przyszłości z zasobu, to jest zalecane zaznaczenie opcji **Zapamiętaj moje hasło**. Podczas ponownej próby korzystania z zasobu system Windows sprawdzi zapisane wcześniej hasło i nie będzie wymagał ponownej identyfikacji.

Jeżeli użytkownik ma uprawnienia do zasobu i zostanie pozytywnie zweryfikowany, to w oknie aplikacji zostaną wyświetlone zasoby udostępniane na serwerze (rys. 19.16).

Linux, oprócz serwera **Samba**, oferuje również oprogramowanie klienta. Umożliwia korzystanie z zasobów udostępnianych przez inne komputery z systemem Windows lub serwerem **Samba**.



Rys. 19.15. **Identyfikacja użytkownika Samby**



Rys. 19.16. **Zasoby udostępnione przez serwer**

PRZYKŁAD 19.5

Przeglądanie zasobów udostępnionych przez serwer Samba

Aby przeglądać zasoby udostępnione przez serwer **Samba**, należy:

1. Uruchomić system Windows 10.
2. Uruchomić aplikację **Sieć** (**Start/Ten komputer/Sieć**).
3. Wskazać serwer **Samba** (w celu przyspieszenia wyszukiwania można wpisać adres IP serwera w pole **adres**).
4. Wprowadzić nazwę użytkownika uprawnionego do korzystania z zasobów i poprawne hasło.
5. Udostępniane zasoby serwera zostaną wyświetlone w oknie aplikacji – można z nich korzystać tak jak w systemie Windows.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Za pomocą dowolnego edytora tekstu zmodyfikuj plik konfiguracyjny **Samby**:
   - Zmień grupę roboczą na „samba".
   - Udostępnij do odczytu wszystkim użytkownikom katalog **/studenci**.
   - Udostępnij do zapisu i odczytu wszystkim użytkownikom katalog **/uczniowie**.
   - Sprawdź poprawność konfiguracji.
2. Uruchom serwer telnet. Sprawdź, czy koleżanki / koledzy mogą się z nim połączyć z innych komputerów.
3. Uruchom serwer ssh. Sprawdź, czy koleżanki / koledzy mogą się z nim połączyć z innych komputerów.
4. Uruchom serwer DHCP. Połącz swój komputer z komputerem koleżanki / kolegi za pomocą kabla skrosowanego. Sprawdź, czy komputer koleżanki / kolegi otrzymał poprawny adres. Dodaj wpis statyczny zawierający adres MAC komputera koleżanki / kolegi.
5. Utwórz skrypt uruchamiający program Midnight Commander. Skonfiguruj system tak, aby program był uruchamiany o każdej pełnej godzinie w poniedziałek.
6. Skorzystaj z komputera z systemem Windows, wyświetl informację o zasobach udostępnianych przez twój serwer **Samba**.
7. Wykonaj w systemie Windows mapowanie katalogu udostępnianego przez twój serwer **Samba**.
8. Skorzystaj z komputera z systemem Windows i wyświetl informację o zasobach udostępnianych przez serwer **Samba** koleżanki / kolegi.
9. Wykonaj w systemie Windows mapowanie katalogu udostępnianego przez serwer **Samba** koleżanki / kolegi.
10. Sprawdź możliwość wykonywania operacji zapisu i odczytu w katalogu udostępnionym przez twój serwer **Samba**.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jaka jest różnica w przydzielaniu przez serwer DHCP adresów statycznych i dynamicznych?
2. Podaj zalety i wady korzystania z anonimowego konta FTP.
3. Jakie zasady dotyczą nazw plików i katalogów udostępnianych przez WWW?
4. Podaj przykłady zadań wykonywanych okresowo, które można realizować przez uruchamianie automatyczne.
5. Jakie kryteria powinny decydować o ograniczeniu przestrzeni dyskowej użytkowników?

- Podstawowe pojęcia związane z Active Directory
- Przygotowanie do instalacji Windows Server 2016
- Konfiguracja Windows Server po instalacji
- Instalacja kontrolera domeny
- Zarządzanie kontami komputerów. Dodawanie komputerów do domeny
- Zarządzanie kontami użytkowników
- Uprawnienia w systemie Windows
- Udostępnianie zasobów i przypisywanie uprawnień do udostępnianych zasobów
- Foldery macierzyste użytkowników
- Profile użytkowników Windows
- Konfigurowanie roli serwera wydruku
- Instalowanie i zarządzanie serwerem DHCP
- Konfigurowanie serwera DNS
- Internetowe usługi informacyjne
- Konfigurowanie usługi RRAS
- Zarządzanie serwerem za pomocą pulpitu zdalnego
- Usługi terminalowe
- Konfigurowanie usługi WDS
- Usługi serwera aktualizacji Windows
- Usługi zasad sieciowych i dostępu sieciowego
- Zabezpieczenie kontrolera domeny przed atakami

Sieciowy system operacyjny – Windows Server

IV

20 Podstawowe pojęcia związane z Active Directory

ZAGADNIENIA

- **Funkcja usługi Active Directory w systemie Windows Server**
- **Zastosowanie DNS**

Systemy operacyjne z rodziny Windows Server są przeznaczone do instalowania na komputerach odgrywających rolę serwerów w sieci. W systemach Windows Server można podzielić użytkowników i grupy na:

- **użytkowników lokalnych i grupy lokalne** – konta są tworzone na lokalnym komputerze i umożliwiają korzystanie z jego zasobów. Przechowywuje się je tylko na komputerach, na których zostały stworzone. Miejscem przechowywania kont jest baza **SAM** (ang. *Security Accounts Manager*), zapisana lokalnie na komputerze. Konta użytkowników lokalnych są inne na każdym komputerze, nawet gdy nazwy użytkowników są takie same;
- **użytkowników domenowych i grupy domenowe** – konta mają na celu logowanie się użytkowników do domeny, co umożliwia korzystanie z zasobów z dowolnego komputera przyłączonego do domeny. Konta użytkowników domenowych są przechowywane w **usługach katalogowych** (ang. *Active Directory*) na **kontrolerach domeny**, a następnie replikowane między wszystkimi kontrolerami w domenie.

Active Directory (AD) to usługa katalogowa dla systemów Windows. Od systemu Windows 2008 otrzymała nazwę **Active Directory Domain Services** (AD DS), aby identyfikować usługę katalogową jako zapewniającą uwierzytelnianie zasobów w obrębie organizacji, w której usługi sieciowe kontroluje wewnętrzna domena, i zarządzanie nimi. Opisuje ona strukturę sieci i jej składników. Może pracować w trybie **natywnym** (ang. *native*) lub w **trybie zgodności** ze starszymi wersjami Windows. W trybie natywnym w sieci są obsługiwane tylko systemy Windows 2000 i nowsze. Jeżeli w sieci znajdują się komputery z systemami Windows Millenium i starszymi, to konieczny jest tryb zgodności, aby mogły one łączyć się do domeny. Domyślnie jest wybierany tryb natywny, a włączenie trybu zgodności jest możliwe w konfiguracji niestandardowej.

Active Directory jest przestrzenią nazw. **Przestrzeń nazw** (ang. *namespace*) to ograniczony obszar, w którego obrębie nazwa może być odnaleziona i wykorzystana do uzyskania dostępu do obiektu i jego atrybutów lub usług. Przykładem przestrzeni nazw może być system plików w systemie operacyjnym, w którym na podstawie nazwy plików i ścieżki dostępu można zlokalizować plik. Przestrzeń nazw w AD może być ciągła lub nieciągła. Przestrzeń jest **ciągła**, jeśli w całej strukturze istnieją dokładnie jeden obiekt typu **korzeń** (ang. *root*) i nazwa **obiektu podrzędnego** (ang. *child*), która powstaje przez dodanie prefiksu do nazwy obiektu **nadrzędnego** (ang. *parent*). Gdy nie ma jednego korzenia, przestrzeń jest **nieciągła**.

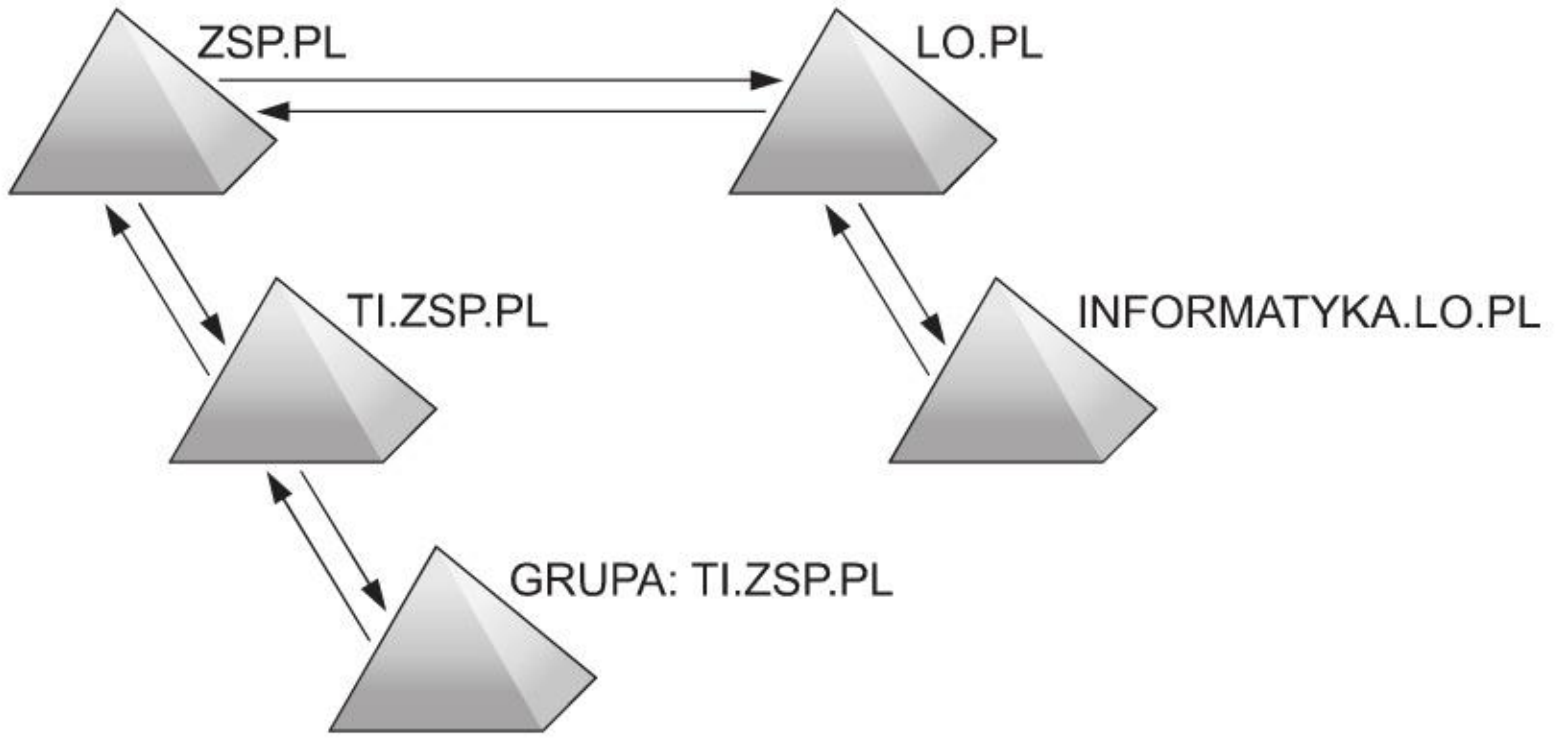
Obiekt to wyróżniony, nazwany zbiór atrybutów reprezentujący np. użytkownika, drukarkę lub komputer. Zbiór wszystkich możliwych rodzajów obiektów występujących w Active Directory i związanych z nimi atrybutów stanowi **schemat** (ang. *schema*).

W Active Directory podstawowym elementem konstrukcji jest **domena** (ang. *domain*). Domena to grupa komputerów połączonych w sieć, składająca się z serwera odgrywającego rolę

kontrolera domeny i **stacji roboczych** – klientów współdzielących bazę katalogową. **Kontroler domeny** (ang. *domain controller*) przechowuje informacje o użytkownikach sieci i ich uprawnieniach. Dzięki temu informacje są gromadzone w jednym miejscu i dostępne dla wszystkich klientów, co ułatwia zarządzanie siecią. W dużych sieciach może być więcej kontrolerów domeny, ale w takim przypadku wymieniają się między sobą przechowywanymi informacjami o sieci. Kontrolery domeny są równoprawne – każdy ma zapisywalną replikę tej samej bazy danych.

Domena jest częścią **drzewa** (ang. *tree*), czyli związku wielu domen mających ten sam schemat, konfigurację i tworzących ciągłą hierarchiczną przestrzeń nazw. Przyłączenie domeny do drzewa jest określone w momencie instalacji jej pierwszego kontrolera.

Las (ang. *forest*) to struktura złożona z wielu drzew, także o wspólnym schemacie i konfiguracji, ale niemająca ciągłej przestrzeni nazw. Las może składać się z jednego drzewa lub wielu drzew. Przynależność do lasu jest określana w momencie instalacji pierwszego kontrolera domeny – przed określeniem przynależności do drzewa. Przykładowy las przedstawiono na rys. 20.1.



Rys. 20.1. Schemat lasu AD

Przestrzeń nazw w Active Directory została zorganizowana hierarchicznie. Obiekty typu **kontenery** mogą przechowywać inne obiekty. Nazwa obiektu w Active Directory opisuje jego położenie w strukturze hierarchicznej. Taką nazwę określa się mianem **pełnej nazwy DN** (ang. *Distinguished Name*).

Podstawowe składniki DN to:

- **DC** – komponent domenowy (ang. *domain component*);
- **CN** – nazwa (ang. *common name*);
- **OU** – jednostka organizacyjna (ang. *organizational unit*);
- **O** – organizacja (ang. *organization*).

Przykładowo, zapis **O=Internet/DC=PL/OU=ZSP/CN=uczen** oznacza, że obiekt **uczen** jest zlokalizowany w jednostce organizacyjnej **ZSP** domeny **PL** w organizacji **internet**.

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

Domena AD jest zorganizowana hierarchicznie, a jej podstawowy składnik to **jednostka organizacyjna** (ang. *Organizational Unit*). Jest ona kontenerem, dzięki czemu może zawierać w sobie inne obiekty, co pozwala grupować zasoby i użytkowników oraz delegować prawa administracyjne. Jednostki organizacyjne mogą być uporządkowane hierarchicznie, np. w modelu geograficznym jednostki są tworzone zgodnie z lokalizacjami oddziałów firmy, natomiast w modelu organizacyjnym struktura jednostek powinna odpowiadać strukturze organizacyjnej firmy.

Oprócz jednostek organizacyjnych w Active Directory można tworzyć obiekty reprezentujące:

- użytkowników;
- komputery;
- drukarki;
- grupy;
- udostępnione foldery;
- kontakty.

Obiekty tworzone w Active Directory są reprezentantami rzeczywistych zasobów sieci.
W Active Directory istnieją dwie kategorie grup:

- **grupa dystrybucyjna** (ang. *distribution*) – używana jedynie do dystrybuowania wiadomości e-mail; nie jest związana z zabezpieczeniami, tzn. nie można jej przypisać uprawnień;
- **grupa zabezpieczeń** (ang. *security*) – przeznaczona do przyznawania uprawnień do obiektów (jest wyposażona w możliwości grup dystrybucyjnych).

Występują trzy rodzaje grup zabezpieczeń:

- **grupa globalna** – mogą do niej należeć konta użytkowników, komputerów i grupy globalne wchodzące tylko w skład tej samej domeny co grupa globalna. Można jej przypisywać uprawnienia do obiektów z dowolnej domeny. Wykorzystuje się ją do grupowania użytkowników zależnie od ich uprawnień;
- **grupa lokalna w domenie** – mogą do niej należeć konta użytkowników, komputerów i grupy globalne z dowolnej domeny i grupy uniwersalne. Można jej przypisać jedynie uprawnienia do obiektów z tej samej domeny. Wykorzystuje się ją do skupiania grup globalnych z różnych domen, którym zostaną przydzielone takie same uprawnienia do obiektu (np. drukarki) znajdującego się w tej samej domenie co grupa lokalna;
- **grupa uniwersalna** – występuje jedynie w trybie natywnym. Mogą do niej należeć konta użytkowników, komputerów oraz grupy uniwersalne i globalne z dowolnej domeny. Można jej przypisać uprawnienia do obiektów z różnych domen.

Tworząc strukturę grup, należy przydzielić użytkowników do grup globalnych i grupy globalne do grup lokalnych, a następnie nadać prawa grupom lokalnym.

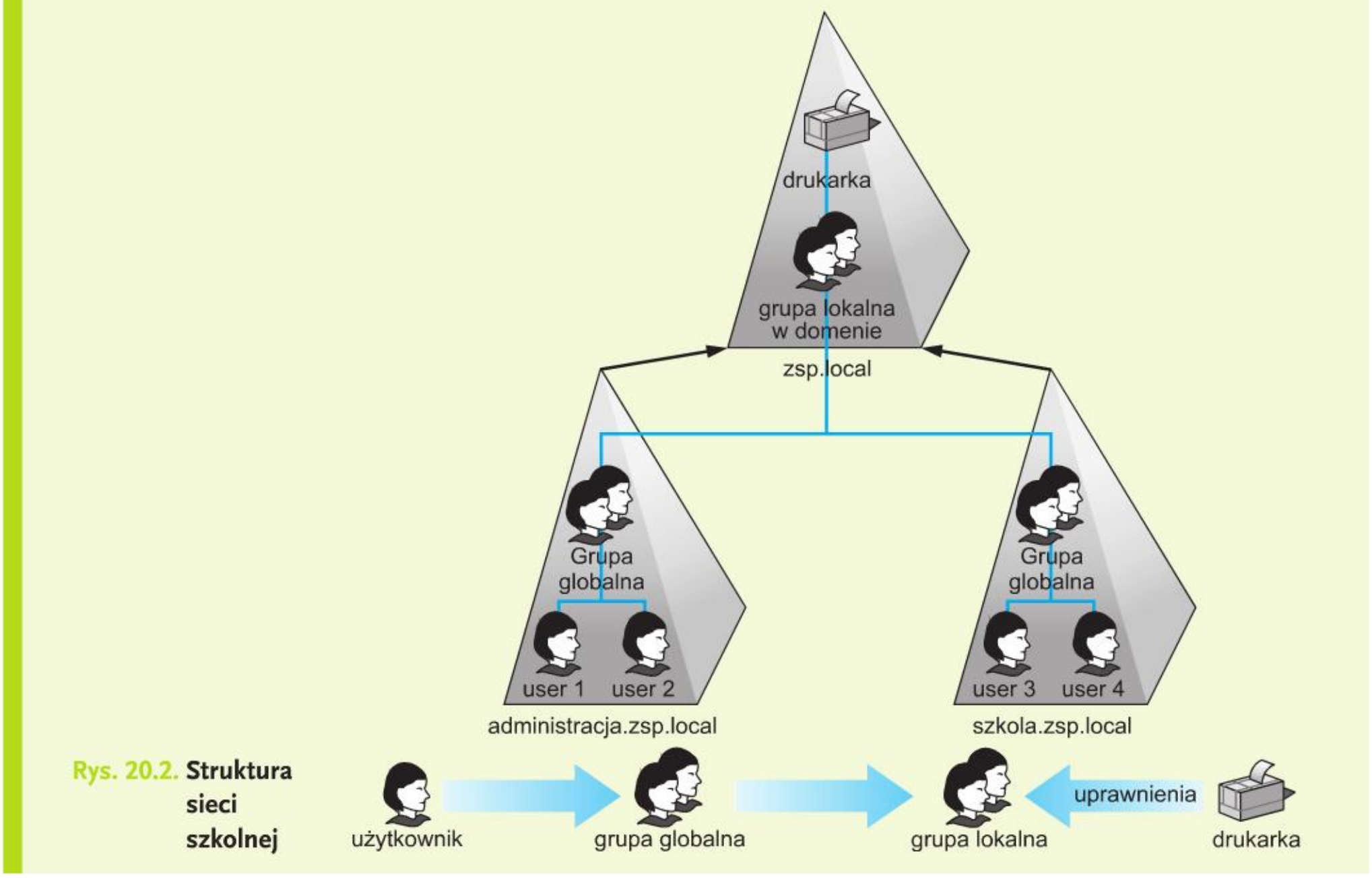
PRZYKŁAD 20.1

Projektowanie struktury domen i grup w szkole

Szkolna sieć jest zbudowana z trzech domen. Domena główna o nazwie **`zsp.local`** ma dwie poddomeny: **`administracja.zsp.local`** i **`szkola.zsp.local`**. W domenie **`zsp.local`** znajduje się drukarka, z której mają korzystać użytkownicy z wszystkich domen.

1. Należy utworzyć grupy, które umożliwią spełnienie powyższych wymagań. W każdej z domen trzeba zgrupować użytkowników mających prawo do drukowania i przypisać ich do grupy globalnej.
2. Grupy globalne z domen **`administracja.zsp.local`** i **`szkola.zsp.local`** należy przypisać do grupy lokalnej w domenie **`zsp.local`**.
3. Trzeba też przypisać odpowiednie uprawnienia do drukarki grupie lokalnej w domenie.

Na rys. 20.2 przedstawiono strukturę sieci szkolnej, w której zrealizowano powyższe wymagania.



Rys. 20.2. **Struktura sieci szkolnej**

Active Directory zapewnia kontrolę dostępu do zasobów i informacji o obiektach przechowywanych w strukturze katalogowej przez weryfikację uprawnień. Administrator lub właściciel obiektu musi nadać prawa dostępu do niego, zanim ktokolwiek będzie korzystać z obiektu. Lista uprawnień jest przechowywana w AD i zawiera informację o tym, kto może wykonać operację i jaki jej rodzaj. Uprawnienia można **nadawać** (ang. *allow*) lub ich **zabronić** (ang. *deny*), przy czym zabranianie zawsze ma priorytet w stosunku do zezwolenia.

Jest pięć podstawowych uprawnień do obiektów AD:

- **pełna kontrola** (ang. *full control*) – zmiana uprawnień, przejmowanie na własność i wszelkie pozostałe działania;
- **odczyt** (ang. *read*) – prawo odczytania listy uprawnień i wszystkich atrybutów każdego z obiektów;
- **zapis** (ang. *write*) – prawo zmiany wszystkich atrybutów obiektów;
- **tworzenie wszystkich obiektów podrzędnych** (ang. *create all child objects*) – prawo tworzenia obiektów dowolnego typu wewnątrz OU;
- **usuwanie wszystkich obiektów podrzędnych** (ang. *delete all child objects*) – prawo usuwania obiektów dowolnego typu z OU.

Głównym mechanizmem wykorzystywanym przez Active Directory do identyfikacji obiektów jest system **DNS** (ang. *Domain Name System*). DNS służy do kojarzenia nazw i adresów IP. Domeny DNS są budowane w sposób hierarchiczny. Na różnych poziomach hierarchii występują domeny główne, podrzędne, a także komputery, np. **`www.zsp.pl`**, gdzie **`www`** jest nazwą komputera, a **`zsp`** – nazwą domeny szkoły w domenie **`pl`**. Nie można zainstalować Active Directory bez uprzednio zainstalowanego serwera DNS obsługującego tę domenę.

Nazwy domen muszą być unikatowe w całej sieci. Można jednak tworzyć poddomeny, np. **`ti.zsp.pl`** jest poddomeną domeny **`zsp.pl`**. Aby zagwarantować unikatowość nazwy, każdą domenę nadrzędną należy zarejestrować przed jej założeniem.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zaplanuj strukturę domen w twojej szkole. Narysuj schemat domen.
2. Konta uczniów każdej klasy technikum informatycznego w twojej szkole powinny być zlokalizowane w oddzielnej jednostce organizacyjnej. Narysuj schemat jednostek organizacyjnych w twojej szkole. W schemacie uwzględnij jednostkę organizacyjną dla kont nauczycieli.
3. Zapisz pełną nazwę DN (ang. *Distinguished Name*) do kontenera zawierającego twoje konto.
4. Zaplanuj system grup użytkowników w twojej szkole, zakładając podział na klasy i grupy ćwiczeniowe.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Jakie są zadania usługi Active Directory?
2. Wyjaśnij pojęcie domeny.
3. Jakie są podstawowe uprawnienia w usłudze Active Directory?
4. Wyjaśnij, jaką funkcję pełni system DNS.

21 Przygotowanie do instalacji Windows Server 2016

ZAGADNIENIA

Przygotowanie instalacji sieciowego systemu operacyjnego Windows Server 2016 Jak przygotować pendrive z obrazem do instalacji Windows Server? Wymagania sprzętowe Windows Server 2016 Aktualizowanie i ponowne instalowanie Windows Server 2016 Proces instalacji systemu Windows Server 2016

Rodzina systemów operacyjnych Windows Server jest przeznaczona do instalowania na serwerach. Szczególny nacisk położono w tych systemach na wydajność i niezawodność. W kolejnych rozdziałach tego podręcznika mówi się o wersji systemu Windows Server 2016, jako przykład systemów z rodziny Windows. Istnieje jednak możliwość korzystania także z innych wersji, np. 2003, 2008, 2012 lub 2019, dlatego poszczególne opcje mogą się różnić. W takim przypadku podczas ćwiczeń poproś nauczyciela o pomoc.

Windows Server jest oprogramowaniem komercyjnym i aby z niego legalnie korzystać, należy wykupić licencję. Producent oprogramowania udostępnia na stronie https://www.microsoft.com/pl-pl/cloud-platform/windows-server-trial specjalną wersję próbną. Oprogramowanie umożliwia zapoznanie się z możliwościami systemu bez konieczności ponoszenia dodatkowych kosztów związanych z jego zakupem.

System Windows Server 2016 jest dostępny tylko w wersji 64-bitowej. Istnieje kilka wersji systemu Windows Server 2016 różniących się możliwościami i zastosowaniem:

- **Windows Server 2016 Essentials** – wersja przeznaczona dla organizacji z nie więcej niż 25 użytkownikami i 50 urządzeniami;
- **Windows Server 2016 Standard** – podstawowa wersja systemu;
- **Windows Server 2016 Datacenter** – wersja najbardziej rozbudowana, przeznaczona dla centrów przetwarzania danych.

System może być instalowany w wersji **pełnej** (serwer ze środowiskiem pulpitu) lub w trybie instalacji **Core**, w którym nie instaluje się powłoki graficznej ani innych programów mających interfejs graficzny, z wyjątkiem notatnika, edytora rejestru i menedżera zadań. Zarządzanie odbywa się przez **Wiersz poleceń** `cmd.exe` albo **PowerShell** lub zdalnie, przez połączenie z użyciem **Microsoft Management Console**.

Nowością jest tryb instalacji **Nano Server**, który oferuje minimalną wersję systemu Windows Server bez interfejsu graficznego. Wersja jest zoptymalizowana pod kątem chmur prywatnych i centrów danych. Nie ma funkcji logowania lokalnego i obsługuje tylko 64-bitowe wersje aplikacji, narzędzi i agentów. Zajmuje o wiele mniej miejsca na dysku, zapewnia skrócony czas konfiguracji i wymaga znacznie mniejszej liczby aktualizacji i ponownych uruchomień niż system Windows Server. Nano Server nie może pełnić funkcji kontrolera domeny usługi Active Directory.

Poprawna instalacja sieciowego systemu operacyjnego jest czynnością bardzo ważną, bo warunkuje dalsze właściwe działanie wszystkich usług umieszczonych na serwerze i poprawne zaimplementowanie zasad zabezpieczeń. Przed przystąpieniem do instalacji należy przygotować odpowiedzi na następujące pytania:

- Czy sprzęt komputerowy spełnia minimalne wymagania producenta sieciowego systemu operacyjnego (CPU, HDD, RAM)?
- Czy sprzęt komputerowy jest kompatybilny z listą obsługiwanych urządzeń lub czy są dostępne dla niego sterowniki?
- Czy zachodzi potrzeba uaktualniania systemu?
- Czy wykonano kopię bezpieczeństwa (w przypadku aktualizacji systemu)?
- Czy zdefiniowano położenie i wielkości partycji?
- Czy zebrano dane dotyczące ustawień interfejsów sieciowych (adresy IP, maska podsieci, domyślna brama, adresy serwerów DNS itp.)?
- Jaką główną rolę będzie odgrywał serwer?
- Czy wybrano usługi sieciowe i aplikacje użytkowe?

PRZYKŁAD 21.1

Przygotowanie pendrive'a do instalacji systemu Windows Server 2016

Obraz do instalacji systemu można pobrać ze strony producenta, ale jest on zbyt duży, aby można było przygotować płytę DVD. Do instalacji można wykorzystać pendrive o pojemności co najmniej 8 GB. Procedura przygotowania pendrive'a składa się z następujących kroków:

1. Ze strony producenta pobrać obraz systemu (plik **`.iso`**) na dysk komputera z Windows 10.
2. Kliknąć dwukrotnie plik z obrazem lub otworzyć za pomocą aplikacji **`Eksplorator Windows`**. Zanotować literę przypisaną do dysku.
3. Podłączyć pendrive do komputera i zanotować literę przypisaną do dysku.
4. Uruchomić okno **`Wiersz poleceń`** w trybie administratora: **`Start`**, wpisać w pole wyszukiwania **`cmd`**, kliknąć prawym klawiszem myszy ikonę konsoli i wybrać **`Uruchom jako Administrator`**.
5. Uruchomić aplikację **`Diskpart`** do przygotowania pendrive'a (polecenie **`diskpart`**).
6. Wyświetlić informacje o dyskach poleceniem **`list disk`**.
7. Wybrać dysk, np. poleceniem **`select disk 2`**.
8. Sprawdzić poleceniem **`list disk`**, czy został wybrany właściwy dysk (dysk zostanie zaznaczony symbolem gwiazdki (*)). Wynik działania poleceń pokazano na rys. 21.1.
9. Wyczyścić zawartość dysku poleceniem **`clean`**.
10. Utworzyć na dysku nową partycję podstawową poleceniem **`create partition primary`**.
11. Aktywować partycję poleceniem **`active`**.
12. Sformatować partycję poleceniem **`format fs=ntfs quick`**.
13. Zakończyć pracę aplikacji **`Diskpart`** poleceniem **`exit`** (rys. 21.2).
14. Skopiować wszystkie dane z obrazu do folderu głównego dysku pendrive.

```
Administrator: Wiersz polecenia
Microsoft Windows [Version 10.0.17134.472]
(c) 2018 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.17134.1

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-Q8BAF78

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          232 GB  1024 KB
  Disk 1    Online           14 GB  3072 KB
  Disk 2    Online           14 GB      0 B

DISKPART> select disk 2

Disk 2 is now the selected disk.

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          232 GB  1024 KB
  Disk 1    Online           14 GB  3072 KB
* Disk 2    Online           14 GB      0 B
```

Rys. 21.1. **Polecenia do przygotowania instalacyjnego dysku pendrive**

```
Administrator: Wiersz polecenia

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART> create partition primary

DiskPart succeeded in creating the specified partition.

DISKPART> select partition 1

Partition 1 is now the selected partition.

DISKPART> active

DiskPart marked the current partition as active.

DISKPART> format fs=ntfs quick

  100 percent completed

DiskPart successfully formatted the volume.

DISKPART> exit

Leaving DiskPart...

C:\WINDOWS\system32>
```

Rys. 22.2. **Tworzenie i formatowanie partycji na dysku pendrive**

21.1. Wymagania sprzętowe Windows Server

Zależnie od wersji instalowanego systemu Windows Server 2016 wymagania sprzętowe są różne. Przedstawiono je w tabeli 21.1.

Tabela 21.1. **Wymagania systemu Windows Server 2016**

	Wymagania minimalne	Wymagania zalecane
Procesor	1,4 GHz (x64)	3,1 GHz
Pamięć RAM	2 GB 512 MB dla wersji bez GUI	16 GB
Miejsce na dysku	32 GB	60 GB
Karta sieciowa 1 Gb lub szybsza	tak	tak
Monitor Super VGA (1024 × 768) lub lepszy	tak	tak
Dostęp do internetu	tak	tak

Wymagania podzielono na dwie kategorie:

- **minimalne** – sprzęt nie może mieć gorszych parametrów (instalator przerwie instalację);
- **zalecane** – sprzęt może mieć gorsze parametry, ale nie powinien (w czasie instalacji będą pojawiać się ostrzeżenia, mimo to będzie ona kontynuowana).

Serwery mogą być zbudowane z podzespołów pochodzących od różnych producentów. Na ogół są to komponenty charakteryzujące się wyższą szybkością i niezawodnością w stosunku do podzespołów stosowanych w zwykłych komputerach (i zwykle również wyższą ceną). Firma Microsoft – producent Windows – bada podzespoły różnych producentów pod kątem ich zgodności z systemem operacyjnym i wyniki tych badań publikuje jako **listy zgodności sprzętu HCL** (ang. *Hardware Compatibility List*) – listy urządzeń, które pomyślnie przeszły testy zgodności sprzętowej. Jeżeli urządzenia nie znajdują się na liście HCL, instalacja może być przeprowadzona, ale firma Microsoft nie gwarantuje poprawnego działania systemu i tych urządzeń. Zgodność sprzętu można sprawdzić przez porównanie z listą HCL umieszczoną na stronie https://www.windowsservercatalog.com/.

Instalację Windows Server można przeprowadzić jako **nową instalację** (ang. *new installation*). Wykonuje się ją w przypadku, gdy:

- zmienia się wielkość partycji instalacyjnej;
- zachodzi konieczność sformatowania dysku;
- jest wymagana pełna rekonfiguracja systemu;
- brak możliwości uaktualnienia zainstalowanego systemu do Windows Server.

Jeżeli na dysku była zainstalowana wcześniejsza wersja systemu, to można dokonać **aktualizacji** (ang. *upgrade*). Aktualizację systemu wykonuje się w przypadku, gdy:

- chce się zachować istniejące konta użytkowników i grup;
- chce się zachować istniejące uprawnienia;
- chce się zachować zainstalowane aplikacje;
- wykonuje się uaktualnienie do nowszej wersji kontrolera domeny.

Przed rozpoczęciem uaktualnienia należy wykonać kopie zapasowe systemu i danych użytkowników. Uaktualnienie jest możliwe tylko dla serwerowych wersji Windows.

Windows Server może być instalowany tylko na partycjach z systemem plików NTFS, który zapewnia:

- możliwość nadawania uprawnień do obiektów (np. plików, folderów, drukarek);
- możliwość nadawania atrybutu kompresji;
- możliwość nadawania atrybutu szyfrowania danych EFS (ang. *Encryption File System*);
- możliwość ograniczania miejsca na dysku poszczególnym użytkownikom – Quota;
- większą niezawodność i skalowalność.

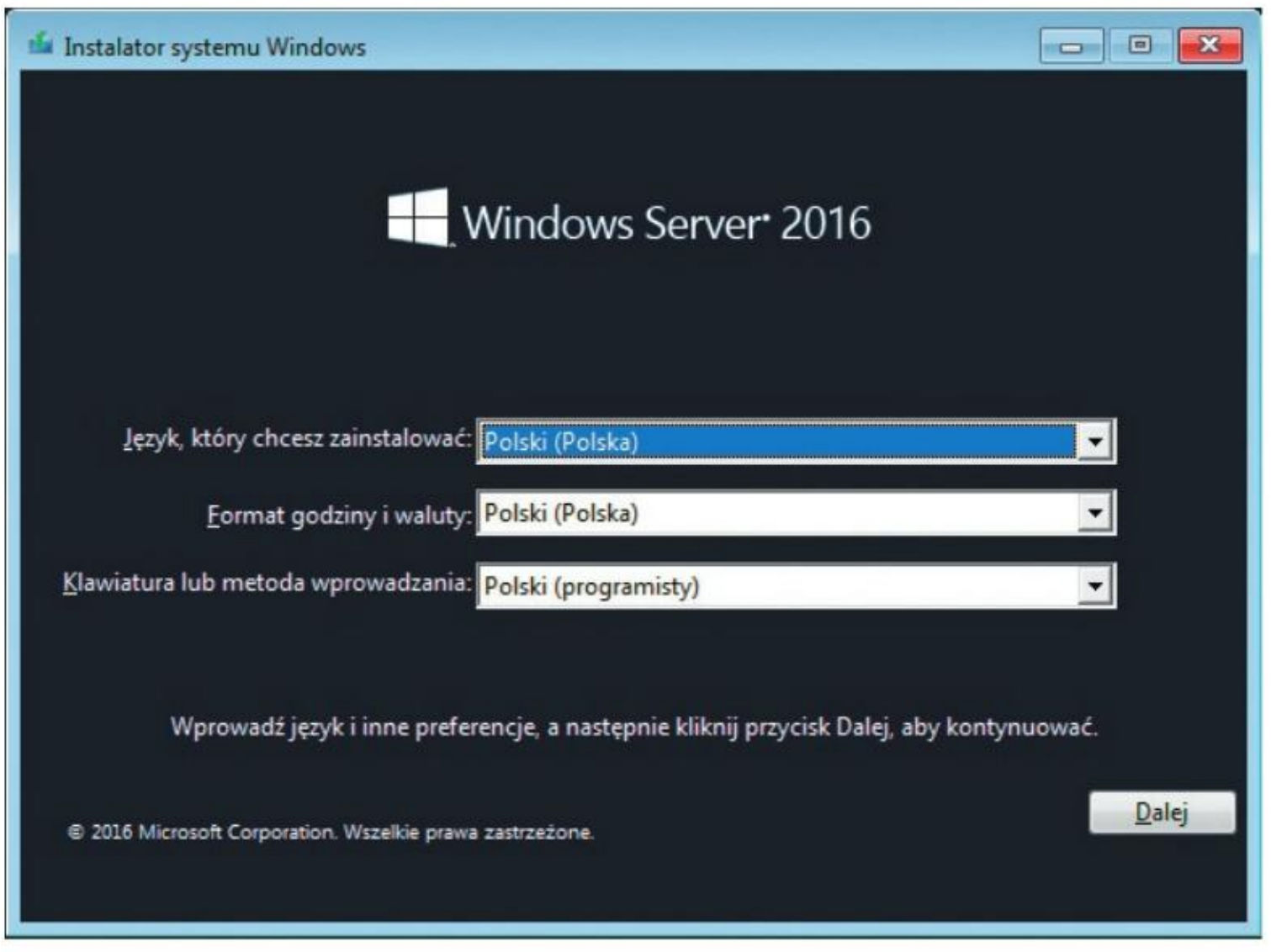
Serwery Windows mogą pracować w jednym z trzech trybów:

- **serwer samodzielny** (ang. *standalone server*) – klienci należący tylko do grupy roboczej;
- **serwer członkowski** (ang. *member server*) – serwer jest członkiem domeny Windows;
- **kontroler domeny** (ang. *domain controler*) – serwer jest kontrolerem domeny Windows.

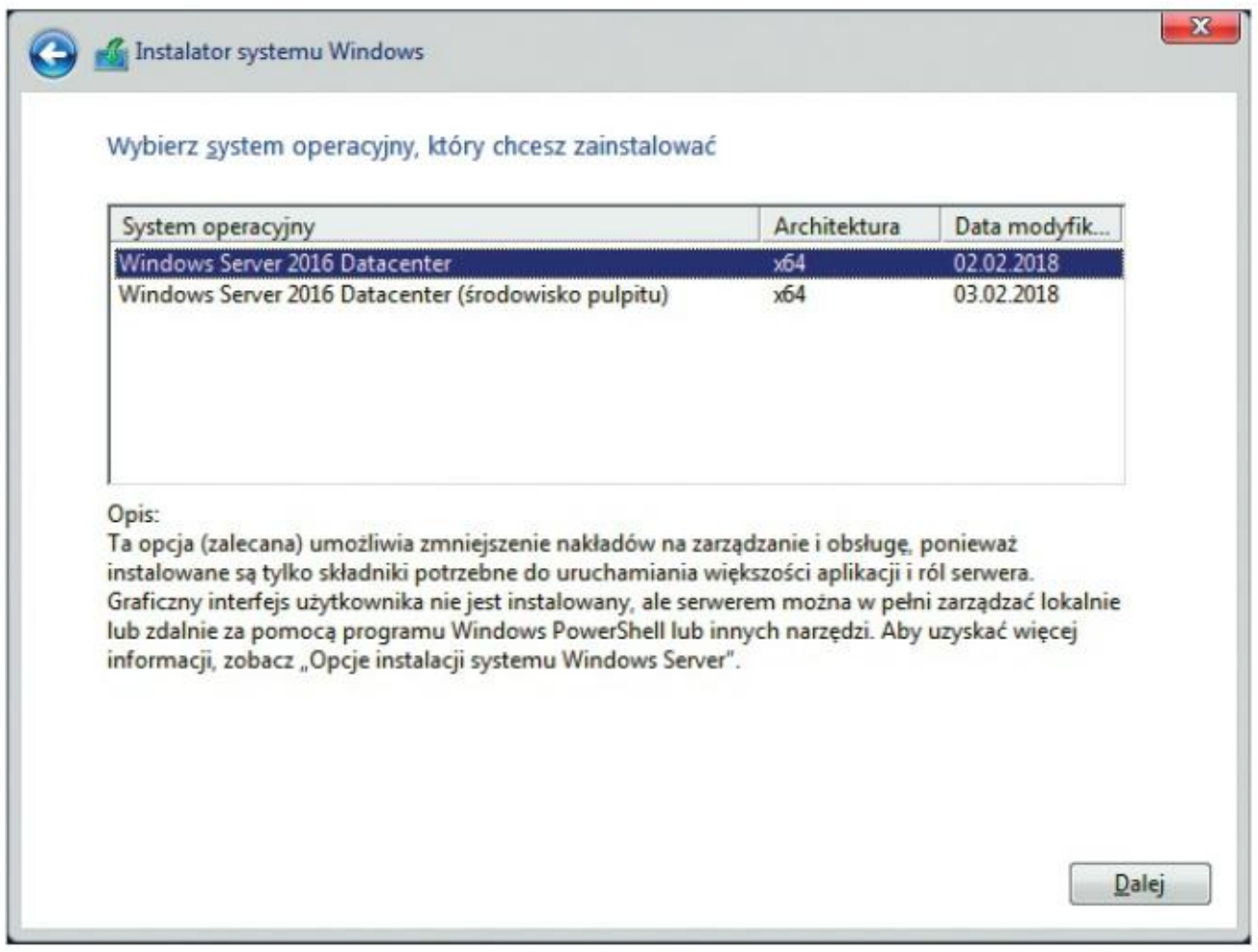
Instalacja Windows Server jest wykonywana przez **Kreatora instalacji**. Uruchomienie kreatora następuje po włożeniu do napędu DVD płyty instalacyjnej lub podłączeniu pendrive'a z wersją instalacyjną systemu i po uruchomieniu komputera z tego nośnika. Pozostały proces instalacji systemu jest nadzorowany przez kreatora i wymaga od użytkownika wprowadzania informacji dotyczących instalowanego systemu.

Instalacja składa się z następujących czynności:

1. Wyboru języka i preferencji dotyczących klawiatury i ustawień regionalnych (rys. 21.3).
2. Wprowadzenia klucza produktu.
3. Wyboru wersji instalowanego systemu (rys. 21.4). Wybór opcji ze środowiskiem pulpitu pozwoli na zainstalowanie graficznego interfejsu użytkownika.
4. Zapoznania się z warunkami licencji – musi być potwierdzone zaznaczeniem odpowiedniego pola, w którym użytkownik akceptuje postanowienia licencyjne.

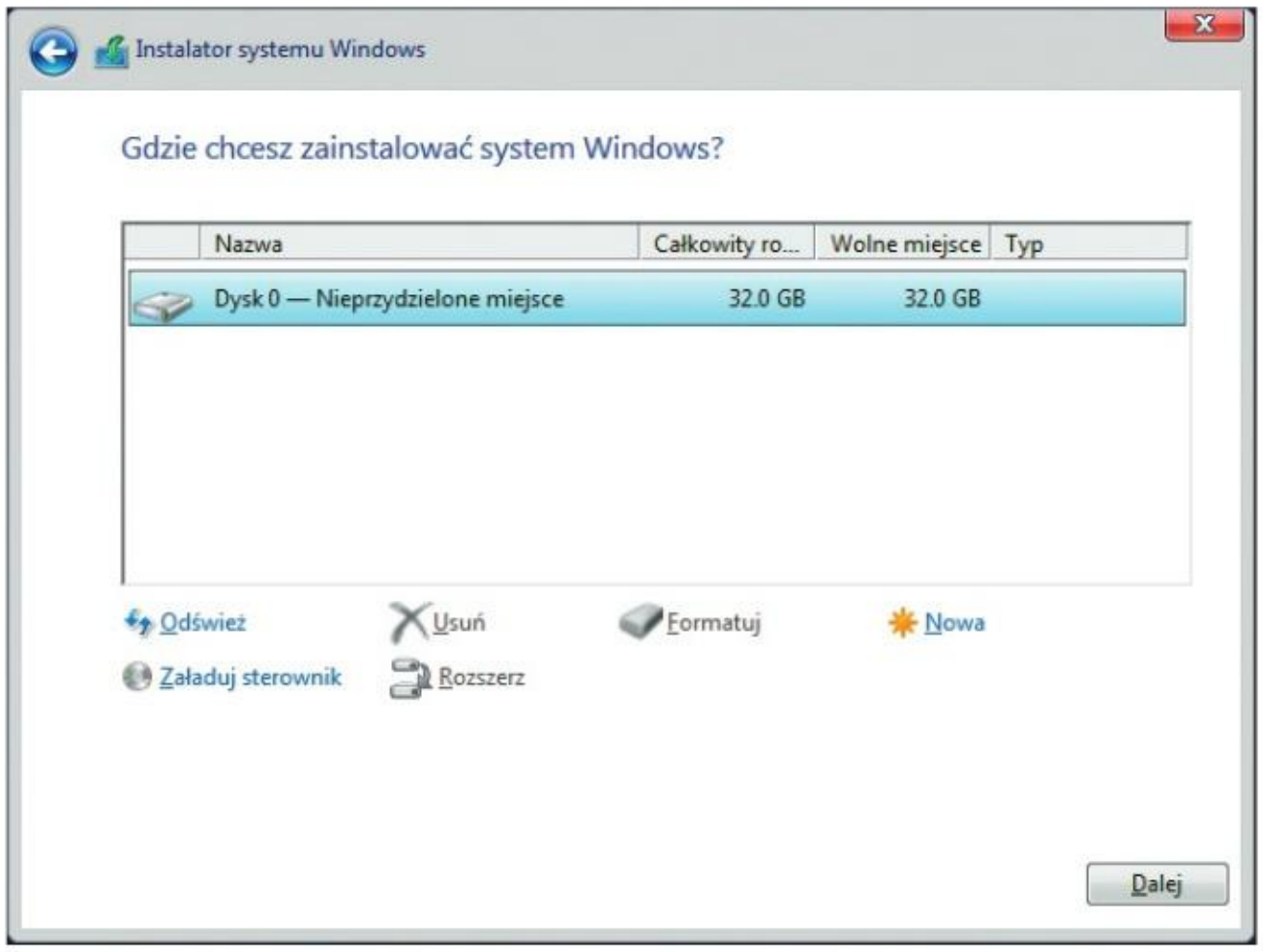


Rys. 21.3. Wybór języka i ustawień regionalnych



Rys. 21.4. Wybór wersji instalowanego systemu

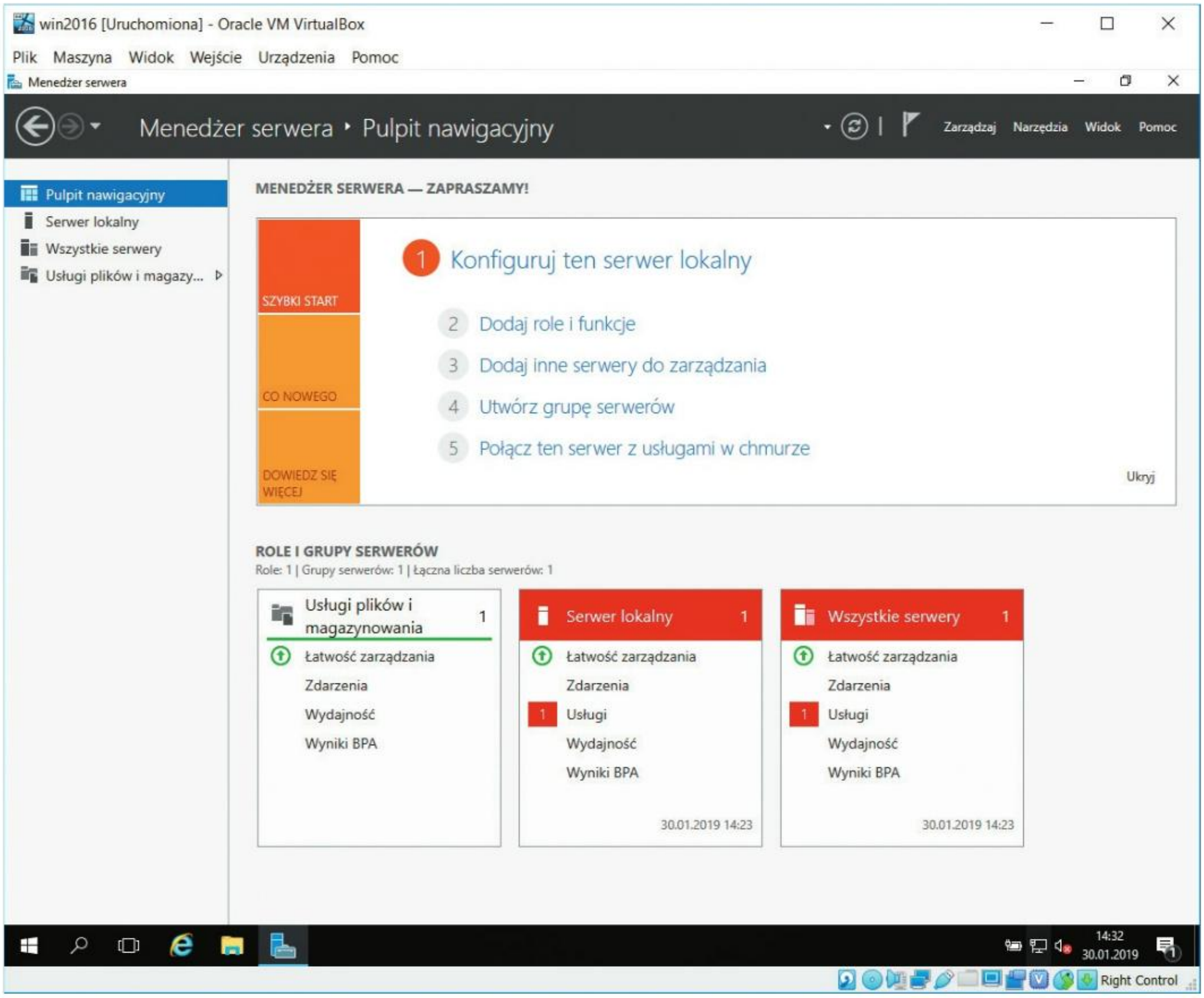
5. Wyboru sposobu instalacji – wybór opcji instalacji niestandardowej pozwala na włączenie zaawansowanych opcji i ich samodzielne określenie.
6. Podziału dysku na partycje – najczęściej system jest instalowany na wydzielonej, przeznaczonej wyłącznie dla niego partycji (rys. 21.5).
7. Zależnie od liczby, rodzaju i rozmiaru instalowanych aplikacji partycja powinna mieć co najmniej 32 GB. Instalator systemu umożliwia tworzenie, usuwanie, a także określanie rozmiaru partycji dysków serwera. Operacja usuwania partycji powoduje również usunięcie wszystkich danych zapisanych na tej partycji. Dobrym rozwiązaniem jest przeznaczenie oddzielnej partycji na zbiory użytkowników.



Rys. 21.5. Wybór partycji do instalacji systemu

8. Po wykonaniu formatowania na przygotowaną partycję są kopiowane pliki systemu i wykonywane operacje ich rozpakowania, instalowania funkcji i aktualizacji. Kontynuacja instalacji wymaga restartu komputera, a następnie zmiany hasła administratora w środowisku graficznym.

9. Po zalogowaniu się na konto administratora należy określić, czy inne komputery i urządzenia w tej sieci będą mogły znajdować ten komputer (wybrać **Tak** – zalecane).



Rys. 21.6. Okno Menedżera serwera

Po instalacji systemu, zanim udostępni się go użytkownikom, należy jeszcze wykonać wiele czynności związanych z przygotowaniem serwera do eksploatacji. Serwer wymaga weryfikacji, czy instalacja została wykonana poprawnie, czy wszystkie urządzenia zostały właściwie rozpoznane i czy zainstalowano odpowiednie sterowniki. Trzeba również wykonać podstawową konfigurację systemu:

- konfigurację strefy czasowej;
- konfigurację karty sieciowej;
- określenie nazwy i domeny komputera;
- przeprowadzenie i włączenie aktualizacji systemu;
- konfigurację zapory sieciowej.

W Windows Server jest wymagane uaktywnienie systemu, np. przez internet. Czynność powinno się jednak odłożyć do czasu, aż upewni się, że system i wszystkie urządzenia zostały zainstalowane i skonfigurowane poprawnie.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Przygotuj odpowiedzi na pytania zadawane przed instalacją systemu.
2. Sporządź listę czynności, które należy wykonać w celu zainstalowania systemu Windows Server na twoim komputerze. Ustaw je w kolejności wykonywania.
3. Na jakie elementy należy zwrócić uwagę przed rozpoczęciem procesu instalacji systemu Windows Server?
4. Przygotuj płytę CD/DVD lub zestaw płyt zawierający wszystkie sterowniki dla systemu Windows Server urządzeń zainstalowanych w twoim komputerze.
5. Przygotuj pendrive umożliwiający instalację systemu Windows Server.
6. Wyszukaj w internecie informacje o programach do tworzenia pendrive'ów z możliwością bootowania systemu. Za pomocą wybranego programu przygotuj pendrive do instalacji systemu Windows Server.
7. Sprawdź, czy karta graficzna i karta sieciowa zainstalowane w twoim komputerze są na liście zgodności sprzętu z systemem Windows Server.
8. Z jakimi innymi systemami z rodziny Windows są zgodne karta graficzna i karta sieciowa zainstalowane w twoim komputerze?

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyjaśnij, do czego służy lista zgodności sprzętu HCL.
2. Kiedy należy zaktualizować, a kiedy ponownie zainstalować Windows Server?
3. Opisz proces instalacji systemu Windows Server.

22 Konfiguracja Windows Server po instalacji

ZAGADNIENIA

Skonfigurowanie serwera po instalacji **Wyłączenie wymogu posiadania cyfrowego podpisu przez sterowniki** **Skonfigurowanie kart sieciowych** **Skonfigurowanie karty grafiki i pliku wymiany** **Skonfigurowanie dysków i partycji** **Skonfigurowanie zarządzania rolami serwera**

Po instalacji systemu należy sprawdzić i – jeżeli jest to konieczne – zainstalować sterowniki urządzeń nierozpoznanych podczas instalacji. System ma duży zbiór sterowników różnych urządzeń, ale warto sprawdzić na stronach producentów, czy nie pojawiły się ich nowsze wersje. W przypadku niektórych urządzeń, np. kart graficznych, sterowniki mogą mieć duży wpływ na wydajność i stabilność systemu oraz szybkość działania.

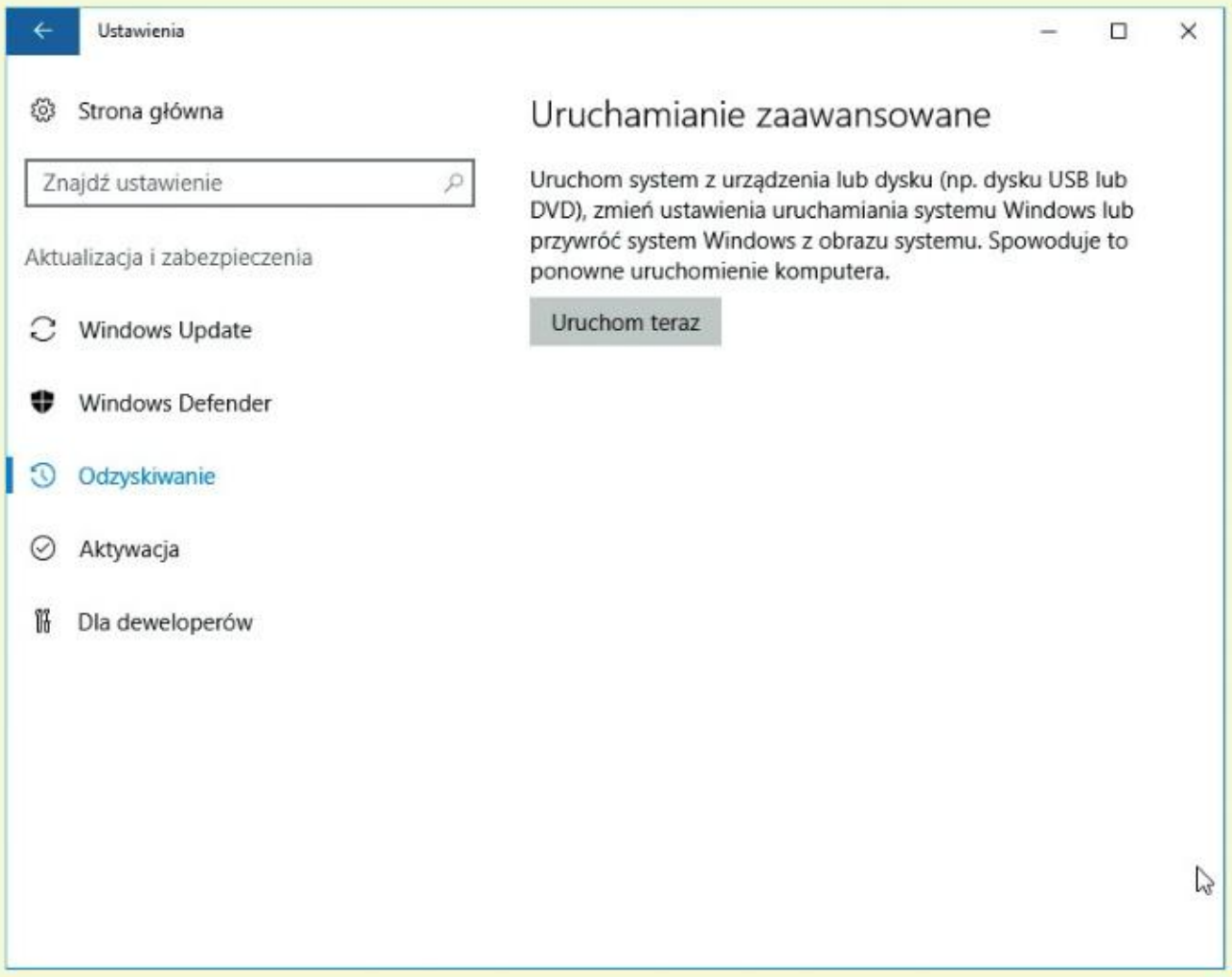
Sterowniki **urządzeń Plug&Play** do systemu Windows Server powinny mieć certyfikat zgodności z systemem. Aby zapewnić stabilność systemu, powinno się instalować tylko sterowniki podpisane cyfrowo. Jeżeli sterownik niepodpisany cyfrowo uniemożliwia uruchomienie systemu, to należy wyłączyć wymóg posiadania podpisu. W tym celu trzeba włączyć komputer w trybie zaawansowanych opcji rozruchu.

Zaawansowane opcje rozruchu można uruchomić w ustawieniach komputera (gdy możliwe jest uruchomienie komputera) lub w środowisku odzyskiwania systemu Windows (gdy nie jest możliwe uruchomienie komputera w trybie normalnym).

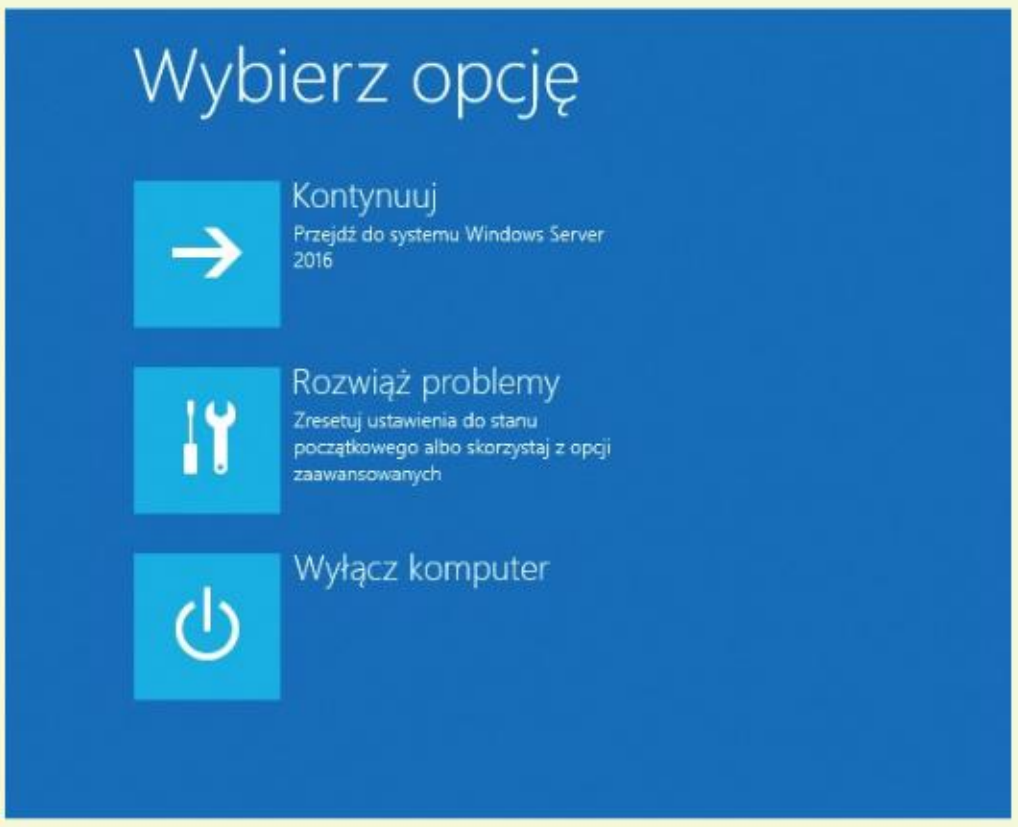
PRZYKŁAD 22.1

Przechodzenie do ekranu zaawansowanych opcji rozruchu w ustawieniach komputera

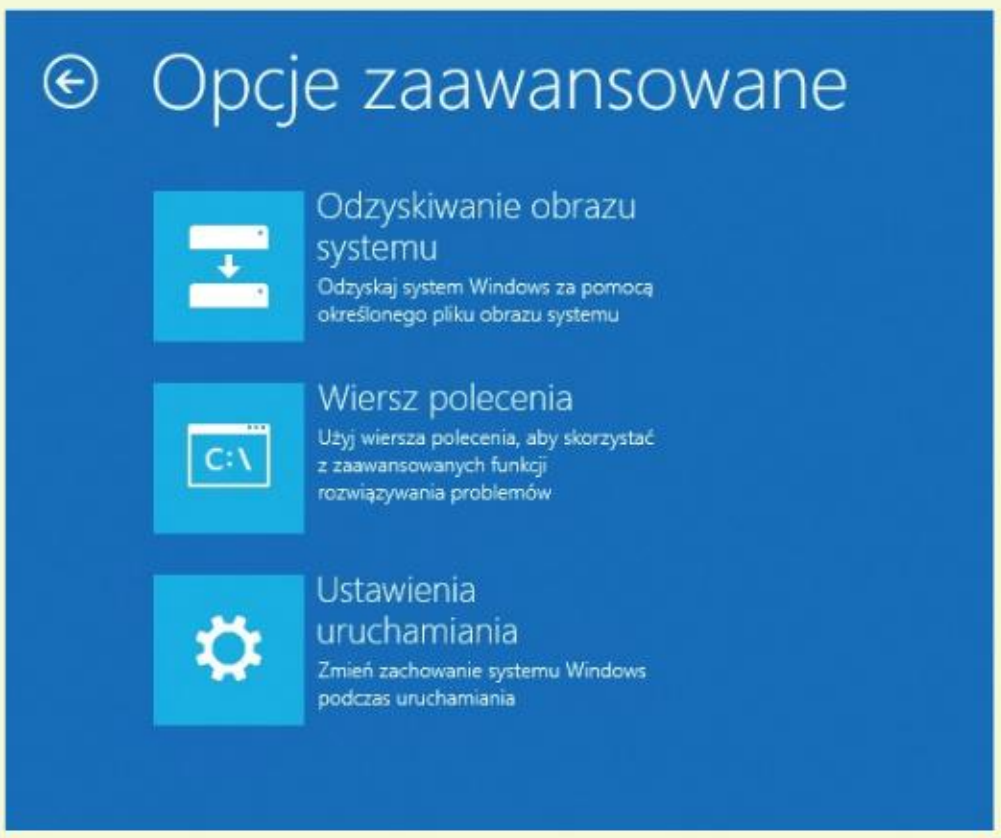
1. W ustawieniach systemu (**`Start/Ustawienia`**) wybrać opcję **`Aktualizacja i zabezpieczenia`**. W lewym panelu zaznaczyć opcję **`Odzyskiwanie`** i kliknąć przycisk **`Uruchom teraz`** (rys. 22.1).
2. Wskazać przyczynę ponownego uruchomienia systemu i kliknąć przycisk **`Kontynuuj`**.
3. Wybrać opcję **`Rozwiąż problemy`** (rys. 22.2).
4. Wybrać opcję **`Ustawienia uruchamiania`** (rys. 22.3).
5. W oknie **`Ustawienia uruchamiania`** kliknąć przycisk **`Uruchom ponownie`** (rys. 22.4).
6. Po ponownym uruchomieniu komputera w oknie **`Zaawansowane opcje rozruchu`** (rys. 22.5) można wskazać sposób uruchomienia komputera.



Rys. 22.1. **Okno odzyskiwania systemu**



Rys. 22.2. **Wybór opcji `Rozwiąż problemy`**



Rys. 22.3. **Wybór opcji `Ustawienia uruchamiania`**

Rys. 22.4. **Okno `Ustawienia uruchamiania`**

```
                    Zaawansowane opcje rozruchu

Wybierz opcje zaawansowane: Windows Server 2016
(Użyj klawiszy strzałek, aby wyróżnić wybraną opcję).

    Napraw komputer

    Tryb awaryjny
    Tryb awaryjny z obsługą sieci
    Tryb awaryjny z wierszem polecenia

    Włącz rejestrowanie rozruchu
    Włącz wideo o niskiej rozdzielczości
    Ostatnia znana dobra konfiguracja (zaawansowane)
    Tryb debugowania
    Wyłącz automatyczne ponowne uruchamianie komputera po błędzie systemu
    Wyłącz wymuszanie podpisów sterowników
    Wyłącz sterownik usługi wczesnej ochrony przed złośliwym kodem

    Uruchom system Windows normalnie

Opis: Wyświetl listę narzędzi do odzyskiwania systemu, których można użyć
      do naprawiania problemów z uruchamianiem, przeprowadzania
      diagnostyki i przywracania systemu.
ENTER=Wybierz                                          ESC=Anuluj
```

Rys. 22.5. **Okno wyboru zaawansowanych opcji rozruchu**

Inną możliwością uruchomienia trybu awaryjnego jest, przy wciśniętym klawiszu [Shift], wybranie polecenia **`Start/Uruchom ponownie`**.

PRZYKŁAD 22.2

Przechodzenie do ekranu zaawansowanych opcji rozruchu w środowisku odzyskiwania systemu Windows

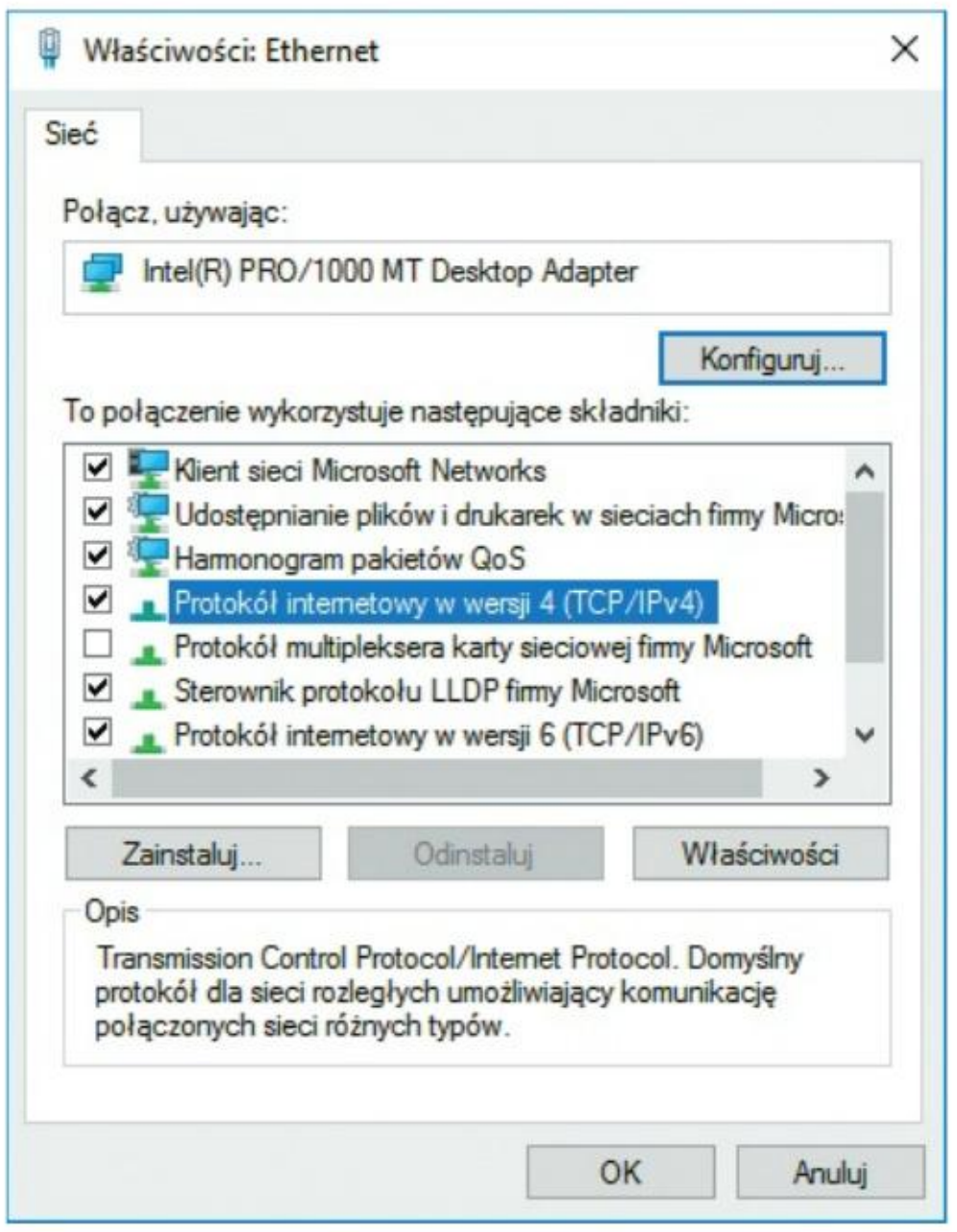
1. Podczas uruchomiania komputera, gdy pojawią się krążące punkty, zresetować system za pomocą przycisku wyłącznika. Powtórzyć operację kilkakrotnie, aż w miejsce krążących punktów pojawi się komunikat o przygotowywaniu naprawy automatycznej.
2. Po uruchomieniu w oknie **`Odzyskiwanie`** wskazać **`Zobacz zawansowane opcje naprawy`**.
3. Postępować dalej tak, jak we wcześniejszym ćwiczeniu i wybrać opcję **`Rozwiąż problemy/Ustawienia uruchamiania/Uruchom ponownie`**.

PRZYKŁAD 22.3

Wyłączenie wymogu posiadania cyfrowego podpisu przez sterowniki i odinstalowanie niezgodnego sterownika

Wyłączenie wymogu posiadania cyfrowego podpisu dotyczy tylko bieżącego uruchomienia systemu i powinno być wykonywane w wyjątkowych okolicznościach. Jeżeli zainstalowany sterownik jest niezgodny z systemem i uniemożliwia uruchomienie systemu, to można wyłączyć wymóg posiadania cyfrowego podpisu. Aby wyłączyć wymóg posiadania cyfrowego podpisu przez sterowniki, należy uruchomić komputer w trybie edycji zaawansowanych opcji rozruchu:

1. W oknie **`Zaawansowane opcje rozruchu`** (rys. 22.5) wybrać pozycję **`Wyłącz wymuszanie podpisów sterowników`**.
2. Uruchomić system i odinstalować niepodpisany sterownik.



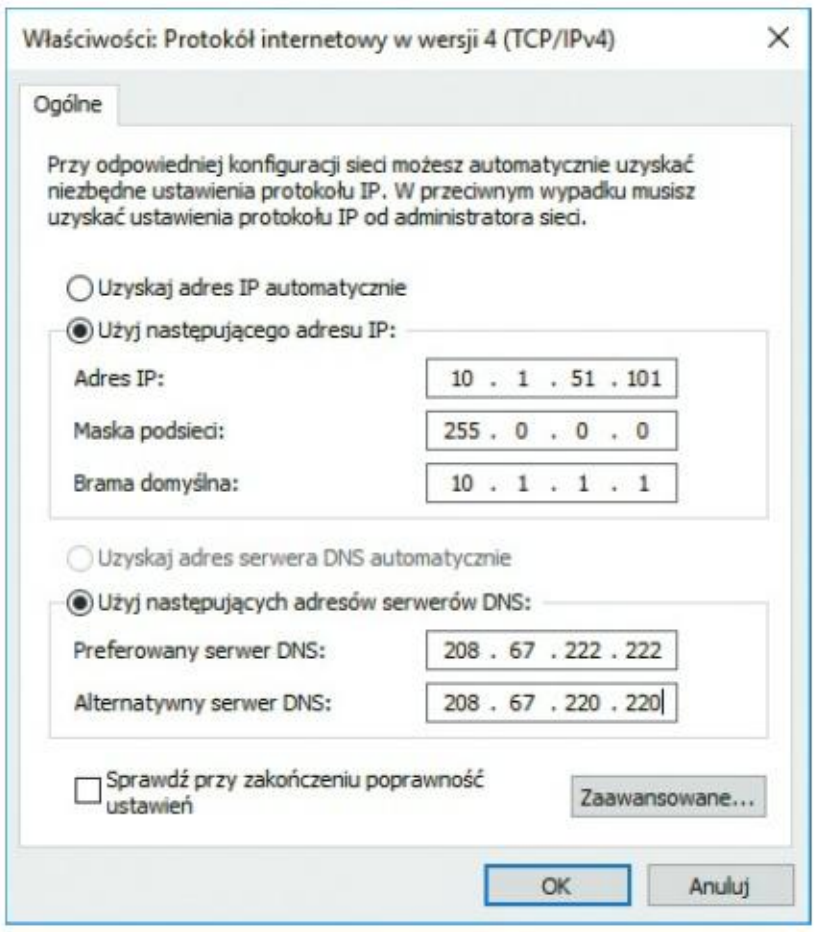
Rys. 22.6. **Okno właściwości połączenia lokalnego**

Jednym z pierwszych urządzeń, które należy skonfigurować, jest karta sieciowa. Przyłączenie komputera do sieci umożliwi pobranie uaktualnień i nowszych wersji sterowników. Konfiguracja karty sieciowej może być wykonana podczas instalacji systemu pod warunkiem, że karta zostanie poprawnie rozpoznana przez system i będą dostępne odpowiednie sterowniki. Jeżeli podczas instalacji karta sieciowa nie została prawidłowo rozpoznana, to należy w dokumentacji komputera sprawdzić typ i model karty oraz zainstalować jej sterowniki za pomocą oprogramowania dostarczonego przez producenta na płycie dołączonej do karty. Jeśli sterownik nie został dołączony przez producenta, trzeba go pobrać z internetu za pomocą innego komputera.

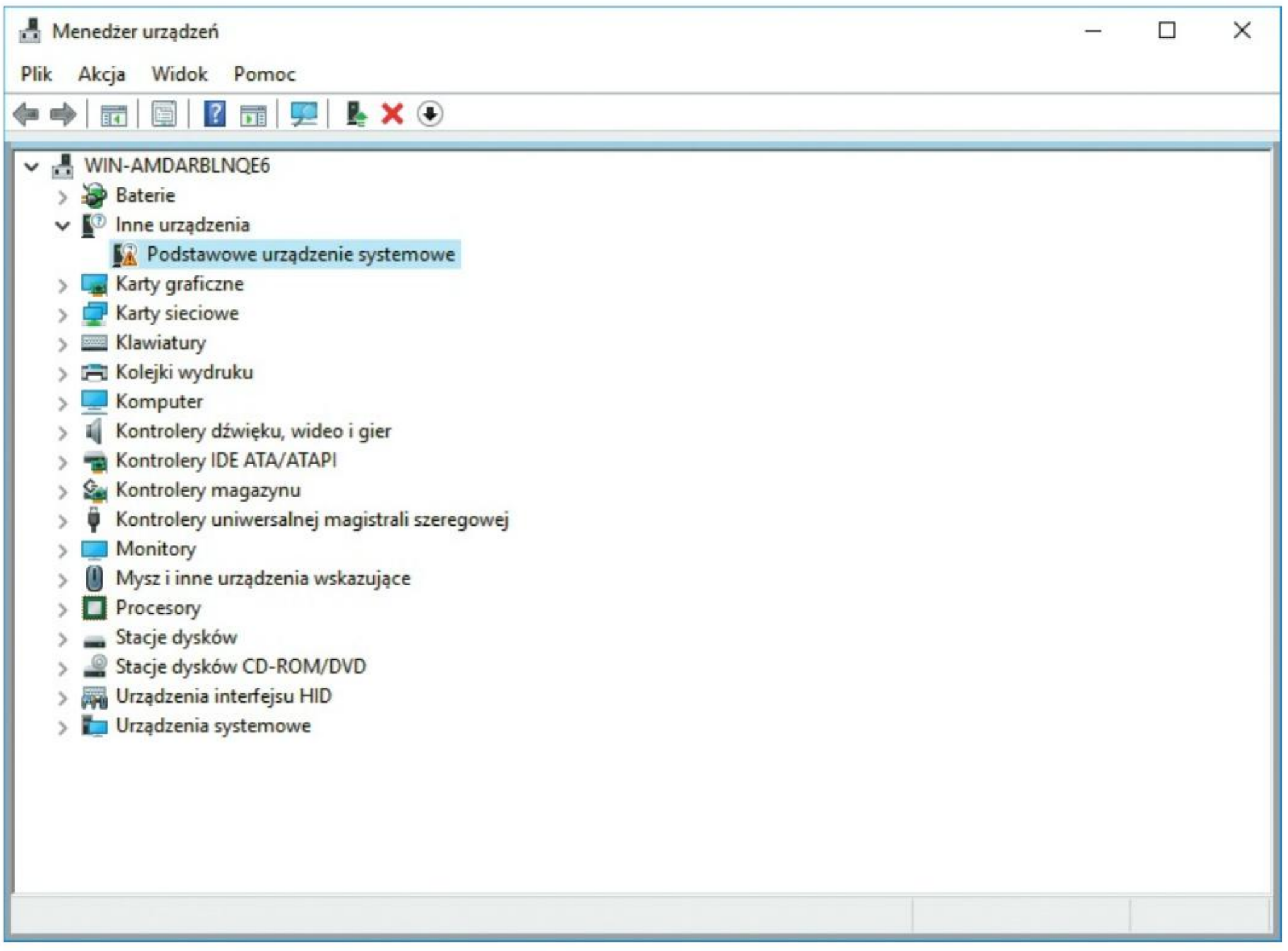
Po zainstalowaniu karty sieciowej trzeba skonfigurować usługi niezbędne do jej pracy i protokoły. Podstawowym protokołem używanym w większości sieci komputerowych jest TCP/IP. Okno konfiguracji protokołu TCP/IP otwiera się za pomocą polecenia **`Start/Panel sterowania/Sieć i internet/Centrum sieci i udostępniania/Zmień ustawienia karty sieciowej`**. Następnie prawym klawiszem myszy wskazuje się kartę sieciową i wybiera opcję **`Właściwości`** (rys. 22.6).

Aby serwer w sieci można było łatwo odszukać, powinien on używać zawsze tego samego adresu IP. Z tego powodu adres IP dla serwera na ogół przypisuje się ręcznie w oknie konfiguracji, w sposób analogiczny do tego stosowanego w Windows 10. Po wskazaniu protokołu TCP/IPv4 wybiera się przycisk **`Właściwości`**, aby otworzyć okno konfiguracji protokołu (rys. 22.7).

W celu sprawdzenia wykazu zainstalowanych urządzeń trzeba wybrać **Start/Panel sterowania/System i zabezpieczenia/System/Menedżer urządzeń**. Okno menedżera (rys. 22.8) przypomina okno znane z systemu Windows 10. Urządzenia, do których nie odnaleziono właściwych sterowników, są widoczne w grupie ikon ze znakiem zapytania, a przy niektórych jest wyświetlany wykrzyknik. Aby zainstalować sterownik, należy kliknąć ikonę prawym przyciskiem i z menu podręcznego wybrać **Aktualizuj oprogramowanie sterownika**. Dalej postępuje się zgodnie z instrukcjami **Kreatora aktualizacji sterowników**. Jeśli po instalacji urządzeń zostaniemy poproszeni o restart serwera, trzeba go wykonać.



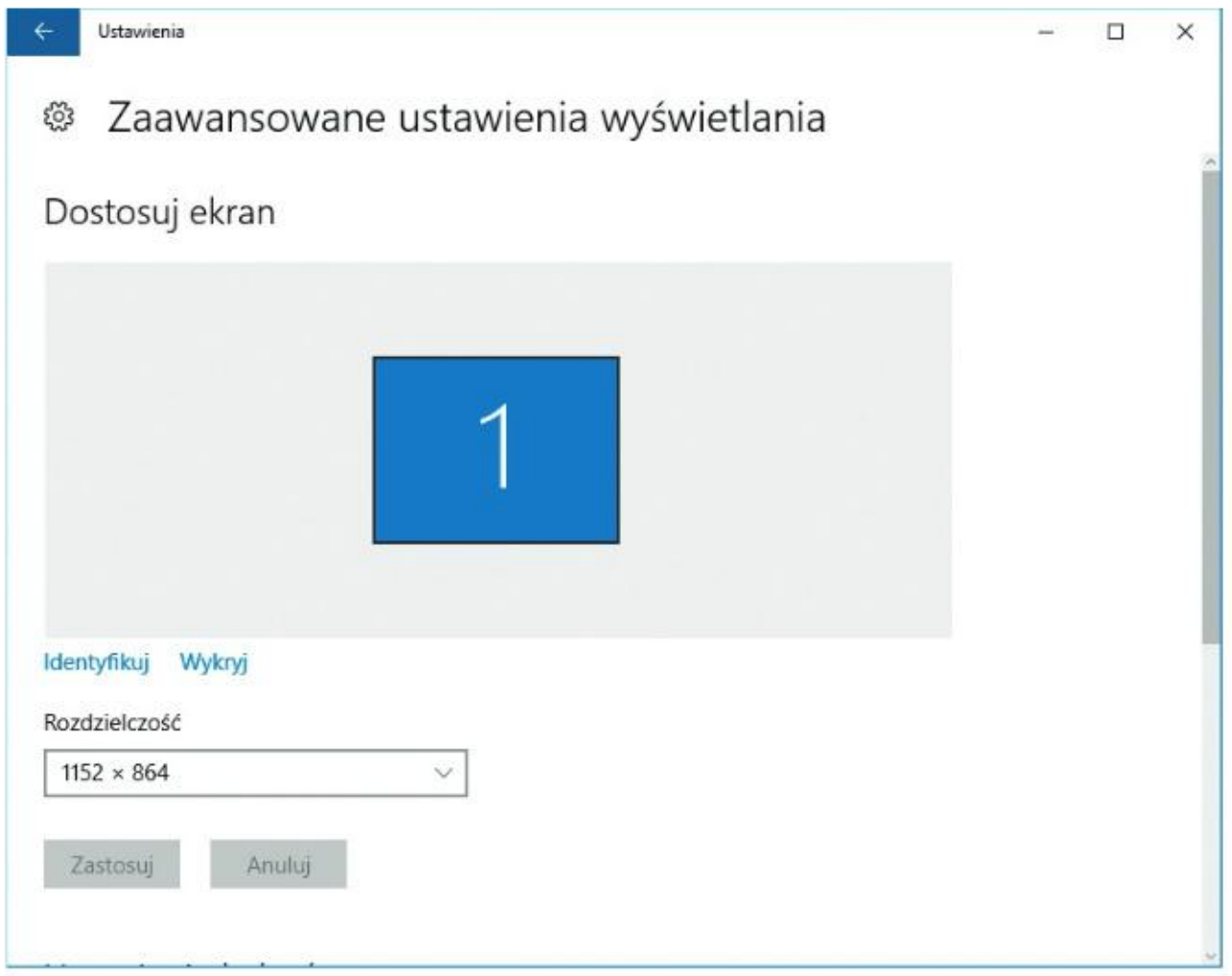
Rys. 22.7. Okno konfiguracji protokołu TCP/IP



Rys. 22.8. Okno `Menedżera urządzeń`

Jeśli karta graficzna została właściwie rozpoznana, to sterowniki powinny być już zainstalowane. Przed zainstalowaniem sterowników należy sprawdzić, czy nie pojawiła się ich nowsza wersja. Sterowniki, zwłaszcza dla nowych modeli kart graficznych, są często aktualizowane

i ich najnowsze wersje można pobrać ze strony producenta karty graficznej. Po zainstalowaniu sterowników powinniśmy dostosować rozdzielczość i liczbę wyświetlanych kolorów do monitora i naszych potrzeb. Zalecane ustawienia minimalne to rozdzielczość 1024 × 768. Zmiany ustawień dokonujemy w oknie **Start/Panel sterowania/Wygląd i personalizacja /Ekran/Zmień ustawienia ekranu**. W oknie **Dostosuj ekran** trzeba wybrać odnośnik **Zaawansowane ustawienia wyświetlania** (rys. 22.9) i ustawić wybraną rozdzielczość.

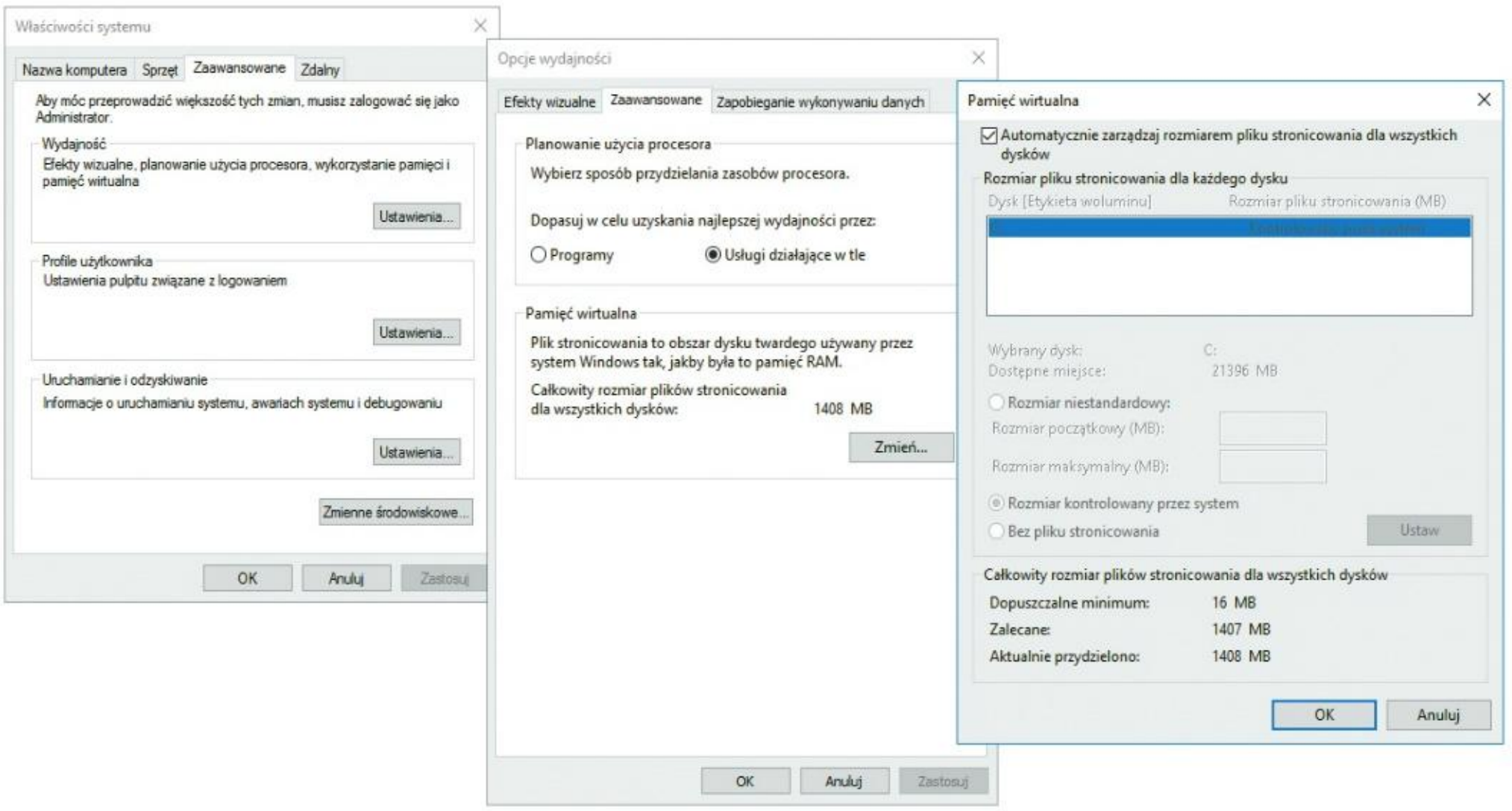


Rys. 22.9. Okno konfiguracji rozdzielczości ekranu

Windows Server pozwala na jednoczesne uruchamianie wielu aplikacji. Każdy z programów wymaga odpowiednich **zasobów sprzętowych**, np. pamięci RAM. System przydziela aplikacjom odpowiednią ilość pamięci, a jednocześnie dba o to, żeby nie doszło do konfliktu między aplikacjami. Jeśli aplikacje uruchomione w systemie wymagają więcej pamięci RAM, niż jest zainstalowane w komputerze, wykorzystuje się **pamięć wirtualną**. Menedżer pamięci przenosi na dysk do pliku wymiany obszar pamięci zajęty przez niewykorzystywaną aplikację. Plik wymiany **pagefile.sys** jest umieszczony domyślnie w folderze głównym dysku systemowego.

Dla wydajności systemu duże znaczenie ma zarówno położenie tego pliku, jak i jego rozmiar. Najlepszym rozwiązaniem jest przeniesienie pliku wymiany z partycji systemowej na inny dysk, aby zapobiec zapełnieniu partycji systemowej. Zalecany rozmiar pliku to 150 procent pamięci RAM, np. gdy system ma 4 GB RAM-u, podczas instalacji będzie utworzony plik o rozmiarze początkowym 6 GB. Rozmiar pliku może być **stały** (zalecane), dzięki czemu w trakcie startu system przeznaczy dla niego ciągłą przestrzeń, co zapobiega rozproszeniu danych na dysku. W przypadku **pliku o zmiennym rozmiarze** system automatycznie będzie dostosowywał go do potrzeb, to znaczy, że jeżeli wzrośnie zapotrzebowanie na pamięć wirtualną, plik zostanie powiększony.

Rozmiarem i położeniem pliku **pagefile.sys** zarządza się za pomocą okna **Pamięć wirtualna**. Aby uruchomić okno, należy wybrać polecenia **Start/Panel sterowania/System i zabezpieczenia/System/Zaawansowane ustawienia systemu**. W oknie **Właściwości** systemu trzeba wybrać zakładkę **Zaawansowane**, a następnie kliknąć przycisk **Ustawienia** w sekcji **Wydajność**. W oknie **Opcje wydajności** wybrać zakładkę **Zaawansowane** i kliknąć przycisk **Zmień** (rys. 22.10).

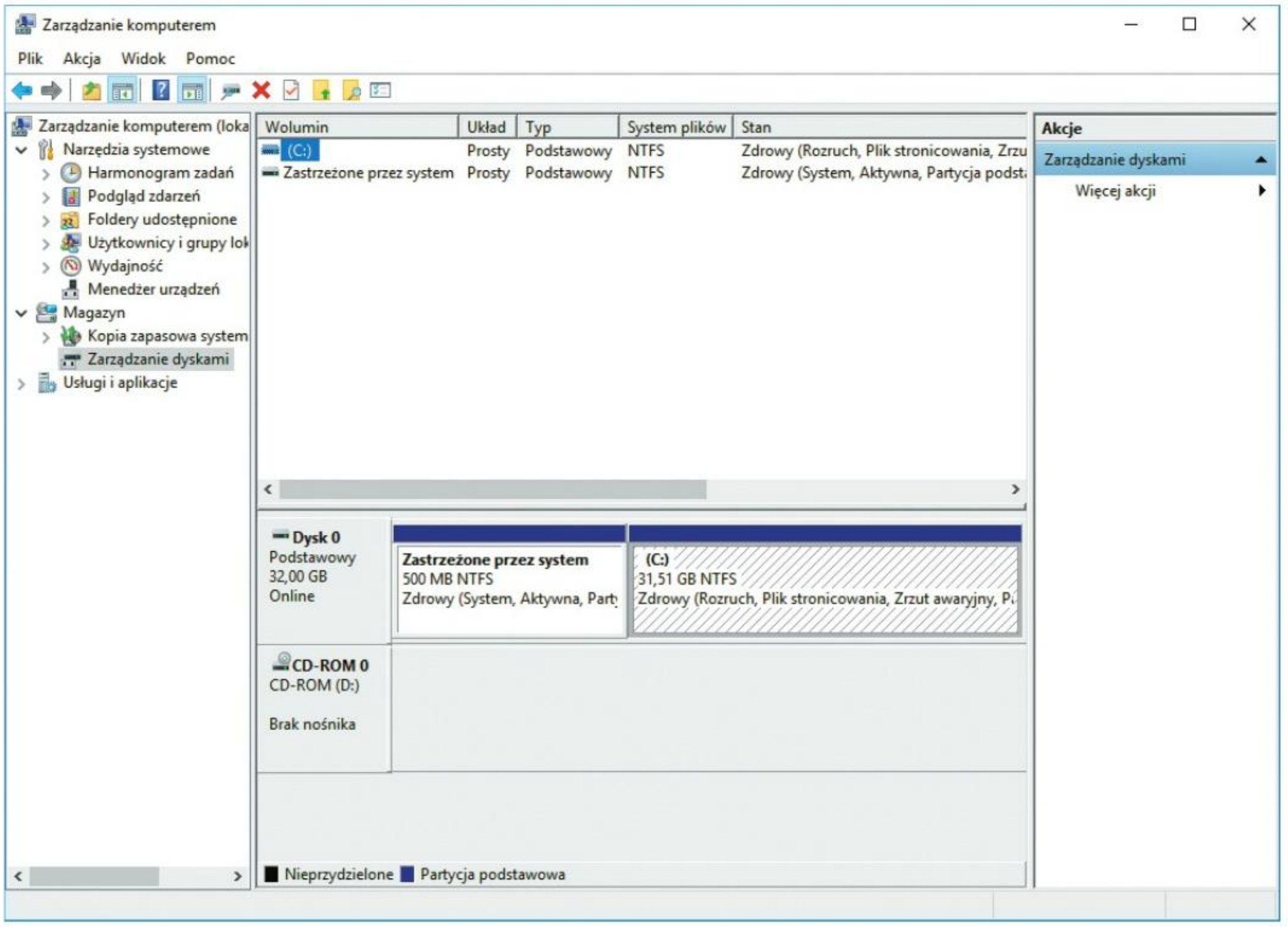


Rys. 22.10. Okno konfiguracji pamięci wirtualnej

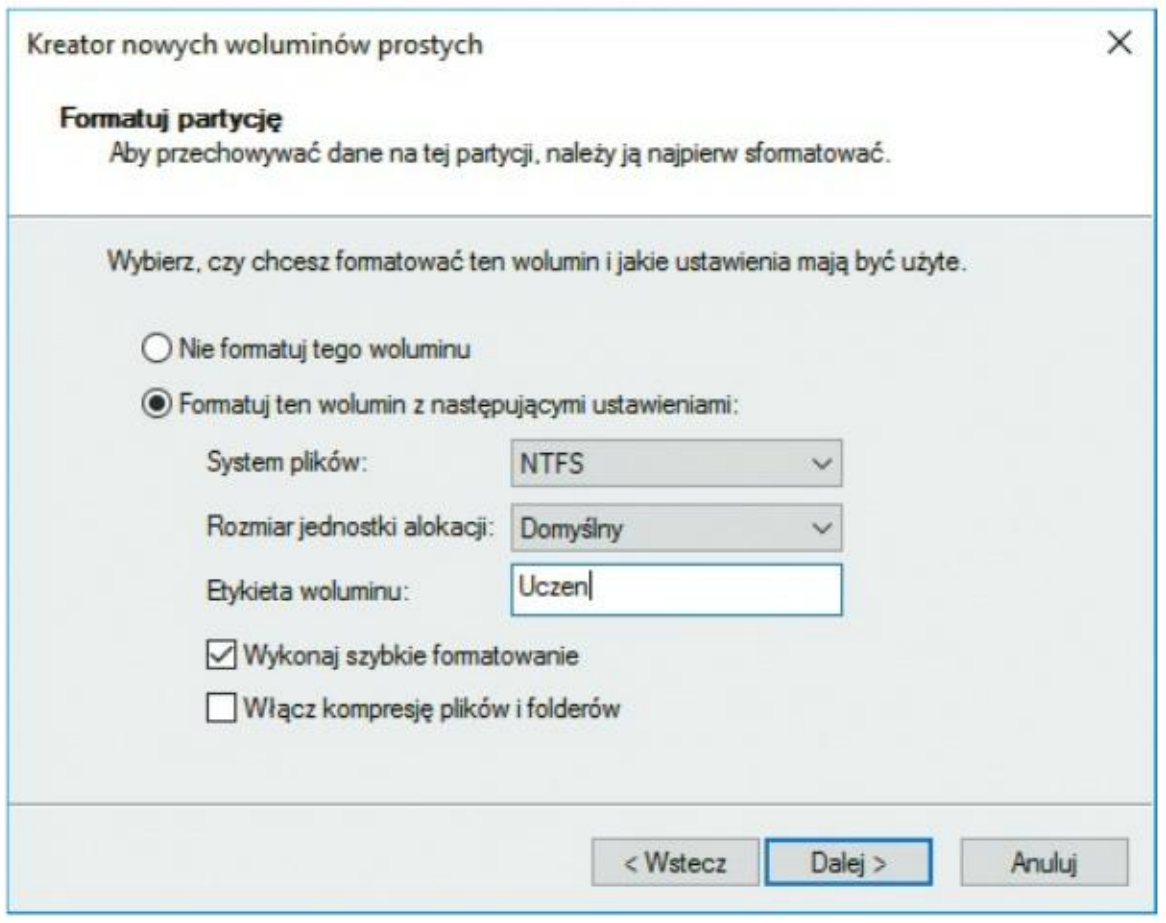
Następnie należy usunąć zaznaczenie opcji **Automatycznie zarządzaj rozmiarem pliku stronicowania dla wszystkich dysków**. Po wprowadzeniu zmian trzeba kliknąć przycisk **Ustaw**, a potem – **OK**. Aby zmiany zostały wprowadzone, trzeba ponownie uruchomić komputer.

Windows Server może korzystać z wielu partycji. Do dobrych praktyk należy przeznaczenie oddzielnej partycji na przechowywanie danych użytkowników. Do konfiguracji dysków i partycji służy przystawka **Zarządzanie dyskami** dostępna w oknie **Zarządzanie komputerem**. Zarządzanie komputerem uruchamia się przez wybranie polecenia **Start/Zarządzanie komputerem**. W oknie **Zarządzanie komputerem** należy rozwinąć opcję **Magazyn/Zarządzanie dyskami**. W oknie **Zarządzania dyskami** (rys. 22.11) uzyskuje się informacje o dyskach zainstalowanych w systemie i woluminach.

Można modyfikować rozmiar woluminów bez utraty danych, np. zmniejszyć rozmiar w celu uzyskania wolnego miejsca na dysku. Jeżeli na dysku jest wolne miejsce, to można zwiększyć rozmiar woluminu lub utworzyć nowy. Aby utworzyć nowy wolumin, należy kliknąć prawym przyciskiem myszy obszar dysku oznaczony etykietą **Nieprzydzielone** i z menu podręcznego wybrać opcję **Nowy wolumin prosty**. W kreatorze nowych woluminów prostych wprowadzamy rozmiar woluminu i przypisujemy mu literę dysku. W oknie formatowania partycji (rys. 22.12) można zaznaczyć system plików (zalecane NTFS), rozmiar jednostki alokacji i etykietę dysku. Aby przyspieszyć proces formatowania, zaznacza się opcję **Wykonaj szybkie formatowanie**. Podczas formatowania dysku zostanie pominięte skanowanie powierzchni dysku w poszukiwaniu uszkodzonych sektorów. W przypadku dysku serwera, w którym zależy nam na niezawodności działania, pominięcie skanowania nie jest zalecane (nie zaznaczać opcji). Proces formatowania będzie trwał dłużej, ale wykrycie uszkodzonych sektorów może mieć wpływ na bezpieczeństwo systemu.



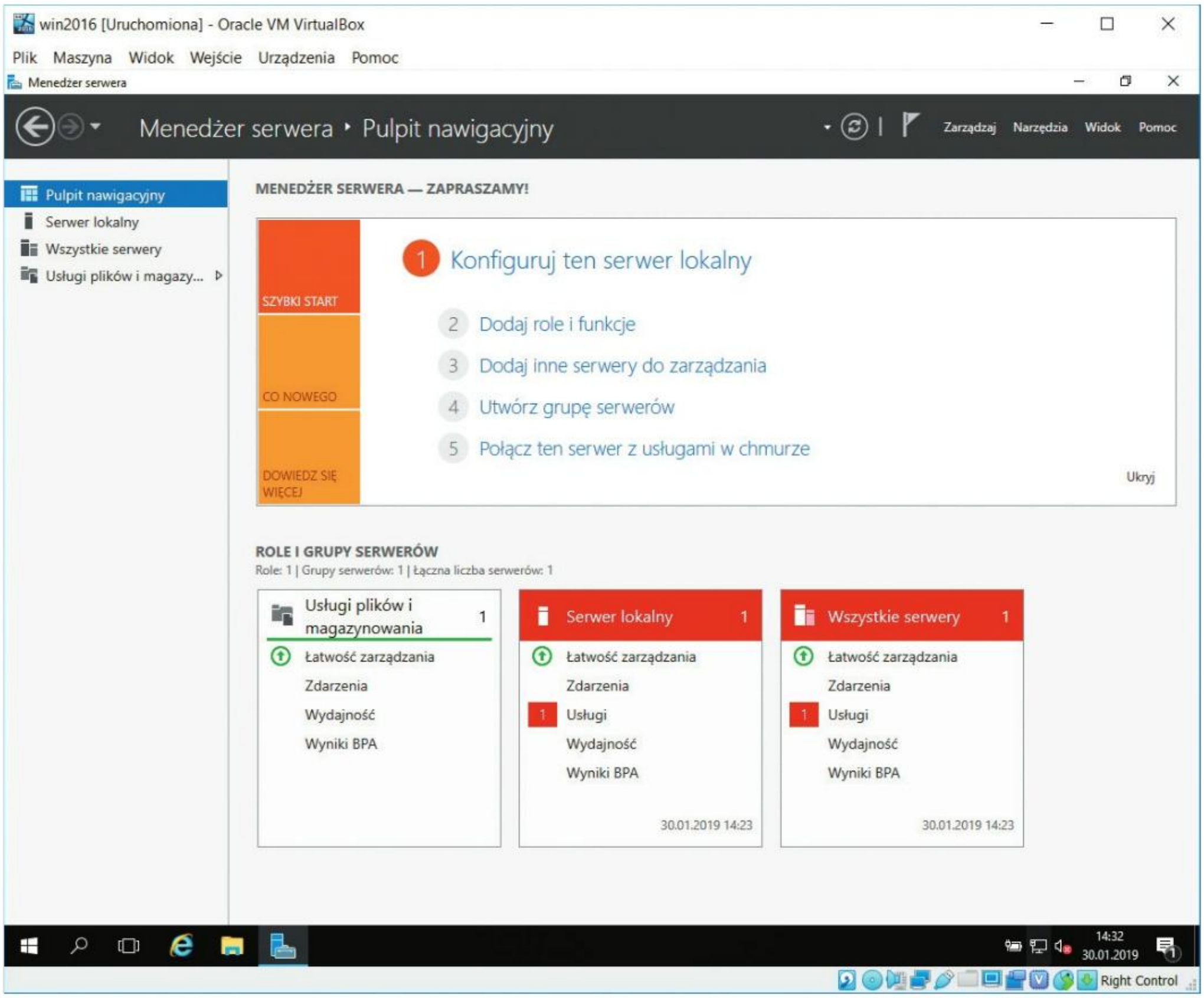
Rys. 22.11. **Okno zarządzania dyskami**



Rys. 22.12. **Okno formatowania partycji**

Bezpośrednio po uruchomieniu systemu jest wyświetlane okno **Menedżer serwera** (rys. 22.13). Umożliwia on szybkie przygotowanie systemu do wypełniania określonych zadań. Możliwe jest zarządzanie pojedynczym serwerem lub grupą serwerów. Po rozwinięciu gałęzi drzewa w lewym panelu okna można wybrać uruchomienie kreatorów konfiguracji ról i funkcji serwera lub wykonywanie innych typowych zadań administratora.

Po zainstalowaniu jednej lub kilku ról okno będzie zawierać listę wybranych funkcji wraz z odnośnikami do narzędzi pozwalających na konfigurację systemu.



Rys. 22.13. Okno zarządzania rolami komputera

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wymień zadania, które należy wykonać przed instalacją systemu i po niej.
2. Co to jest tryb awaryjny i czym różni się od trybu normalnego?
3. Wyjaśnij, jak działa pamięć wirtualna.
4. Jakie są zasady dobierania rozmiaru pamięci wirtualnej?

23 Instalacja kontrolera domeny

ZAGADNIENIA

Funkcja w sieci pełniona przez kontroler domeny **Zainstalowanie kontrolera domeny** **Skonfigurowanie kontrolera domeny** **Zainstalowanie kontrolera domeny tylko do odczytu** **Dodanie przystawki do konsoli mmc i zarządzanie nią**

Kontroler domeny to komputer, na którym uruchomiono usługę **Active Directory**, zarządzającą dostępem użytkowników do sieci i jej zasobów. W małej sieci wystarczy jeden kontroler w domenie (ze względu na nadmiarowość lepszym rozwiązaniem są co najmniej dwa kontrolery zawierające kopie bazy danych Active Directory). W dużych sieciach, ze względu na możliwość rozłożenia ruchu, zwykle konfiguruje się kilka kontrolerów domeny.

Kontrolery, dzięki usłudze **replikacji danych**, mają jednakowe bazy danych o obiektach w sieci, co pozwala klientom na uzyskanie informacji od dowolnego z nich. Modyfikowanie danych można wykonać na dowolnym z kontrolerów, a proces replikacji zapewni dystrybucję zmienionych danych do pozostałych kontrolerów.

W systemie Windows Server od wersji 2008 wprowadzono nowy typ: **kontroler tylko do odczytu** (ang. *Read-Only Domain Controller*). Kontroler RODC jest zwykle stosowany w oddziałach firmy, w których niewielka prędkość łączy WAN wymusza instalację kontrolera w oddziale (uwierzytelnianie na odległym kontrolerze przez łącza WAN byłoby zbyt wolne). Jeżeli oddział jest zbyt mały, aby zatrudniać administratora z prawami do zarządzania, to ze względu na bezpieczeństwo nie zezwala się na wprowadzanie zmian w Active Directory na tym serwerze.

Zainstalowanie usługi Active Directory (promocja serwera do roli kontrolera domeny) spowoduje zablokowanie wszystkich kont lokalnych, dlatego najlepiej przeprowadzić ją zaraz po instalacji systemu. Podczas instalacji zostaną utworzone nowe konta w domenie oraz zainstalowane serwer DNS, obsługujący domenę, i serwer DHCP, jeśli jest wymagany.

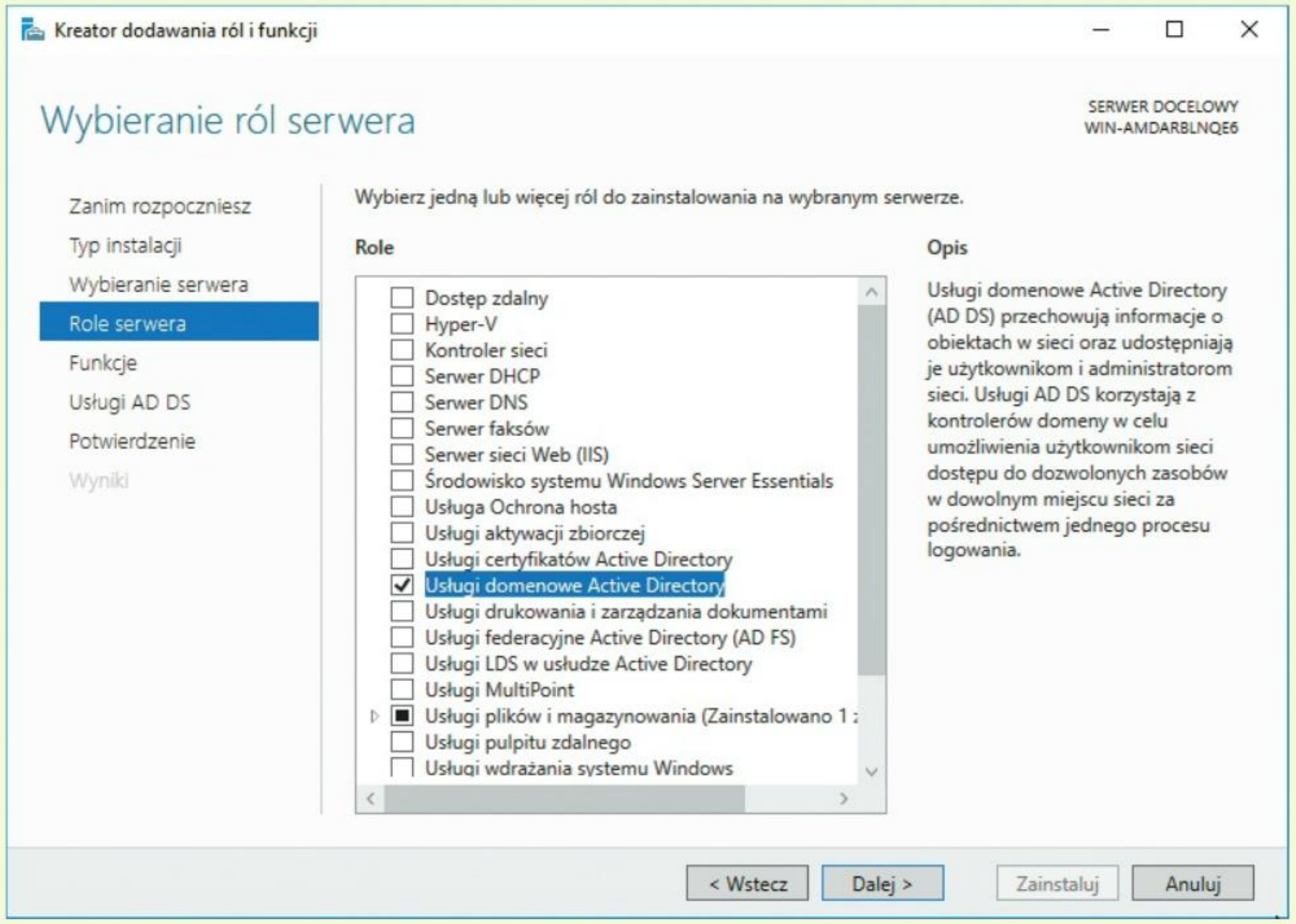
PRZYKŁAD 23.1

Instalowanie kontrolera domeny

W tym ćwiczeniu zostanie utworzona nowa domena i zainstalowany kontroler domeny nią zarządzający. Instalacja kontrolera składa się z dwóch etapów: instalacji roli kontrolera i jego konfiguracji. Aby rozpocząć proces instalacji kontrolera domeny, należy uruchomić kreatora instalacji, który poprowadzi użytkownika przez proces instalacji i konfiguracji:

1. W oknie **`Menedżer serwera`** rozwinąć opcję menu **`Zarządzaj`** i wybrać opcję **`Dodaj role i funkcje`**. Można również w lewym panelu zaznaczyć **`Pulpit nawigacyjny`** i wybrać opcję **`Dodaj role i funkcje`** w prawym panelu.
2. W oknie **`Zanim rozpoczniesz`** zapoznać się z zasadami instalacji kontrolera. Kliknąć przycisk **`Dalej`**.

3. W oknie **Wybieranie typu instalacji** wybrać **Instalacja oparta na rolach lub oparta na funkcjach**, a następnie kliknąć przycisk **Dalej**.
4. W oknie **Wybieranie serwera docelowego** wybrać opcję **Wybierz serwer z puli serwerów** i wskazać nazwę serwera, na którym ma zostać zainstalowana usługa AD DS, a następnie kliknąć przycisk **Dalej**.
5. W oknie **Wybieranie ról serwera** (rys. 23.1) zaznaczyć **Usługi domenowe Active Directory**, a następnie zezwolić kreatorowi na doinstalowanie wszystkich funkcji niezbędnych do prawidłowej pracy kontrolera. Kliknąć przycisk **Dalej**.



Rys. 23.1. **Wybór instalacji roli kontrolera domeny**

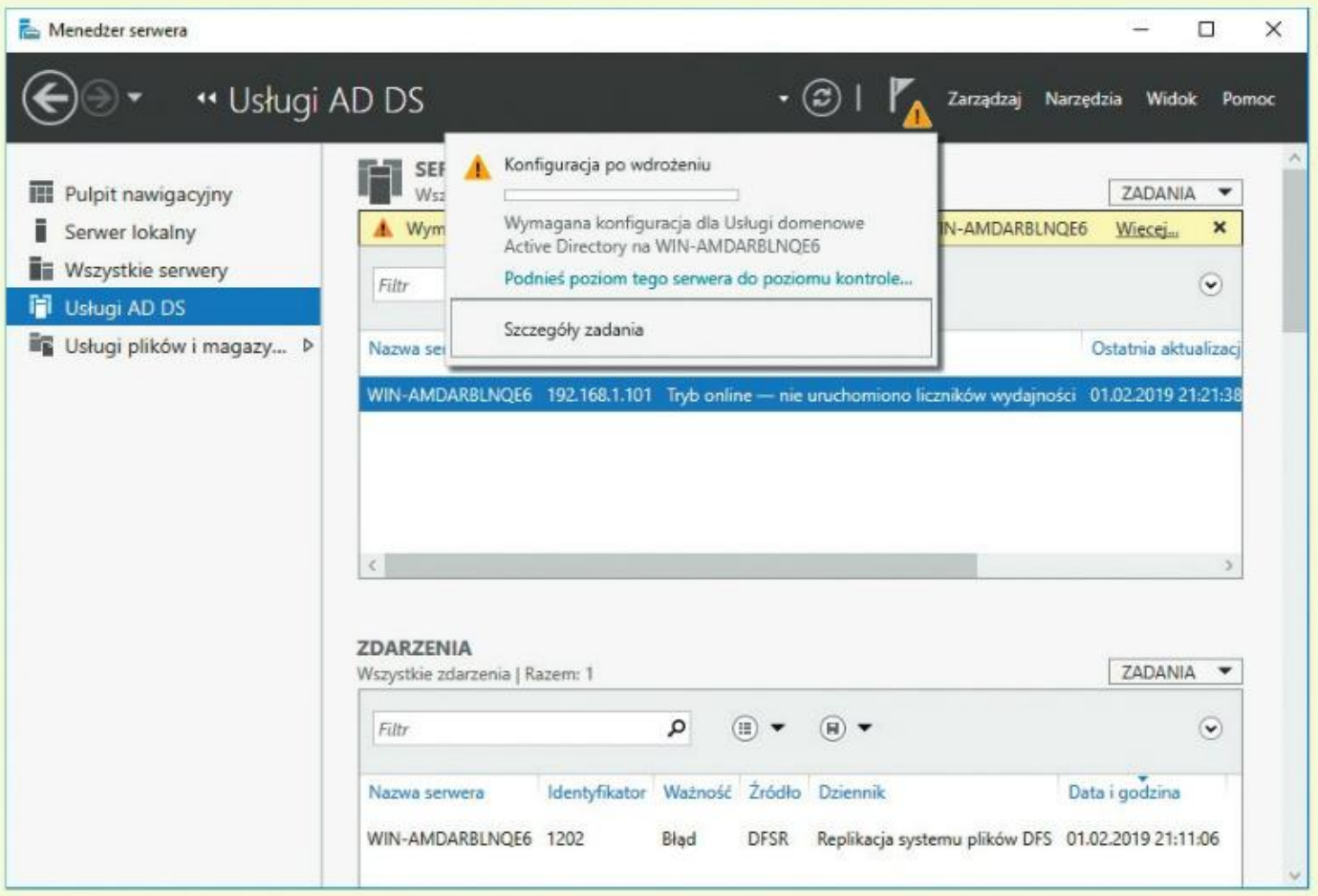
6. W oknie **Wybieranie funkcji** wybrać dodatkowe funkcje, które trzeba zainstalować (w tym ćwiczeniu nie wprowadzamy żadnych zmian), a następnie kliknąć przycisk **Dalej**.
7. W oknie **Usługi domenowe Active Directory** zweryfikować wprowadzone informacje, a następnie kliknąć przycisk **Dalej**.
8. W oknie **Potwierdzenie opcji instalacji** można zaznaczyć opcję **Automatycznie uruchom ponownie serwer docelowy, jeśli będzie to potrzebne**. Kliknąć przycisk **Zainstaluj**.
9. Po wyświetleniu informacji o pomyślnym zakończeniu instalacji kliknąć przycisk **Zamknij**.
   Oprogramowanie niezbędne do działania usługi Active Directory zostało pomyślnie zainstalowane. Należy jeszcze skonfigurować usługę.

PRZYKŁAD 23.2

Promowanie serwera do roli kontrolera domeny

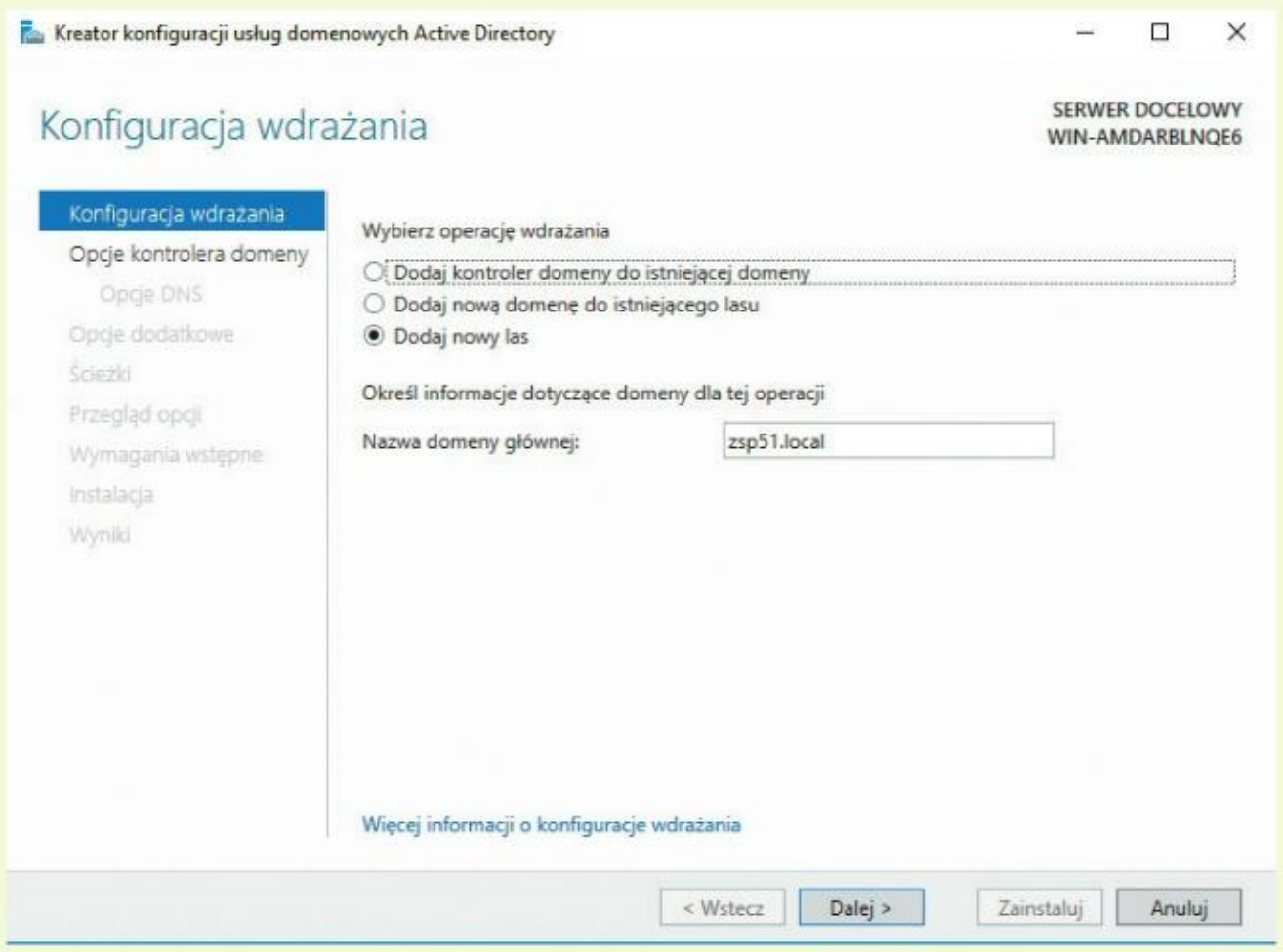
Aby rozpocząć proces konfiguracji kontrolera domeny, należy:

1. W oknie **Menedżer serwera** kliknąć ikonę powiadomień (rys. 23.2) i z rozwijanego menu wybrać polecenie **Podnieś poziom tego serwera do poziomu kontrolera domeny**.



Rys. 23.2. **Uruchamianie kreatora promowania serwera do poziomu kontrolera domeny**

2. Wskazać opcję **Dodaj nowy las** i wprowadzić nazwę nowej domeny, np. **zsp51.local** (local wskazuje, że będzie to domena lokalna, niedostępna w internecie). Kliknąć przycisk **Dalej** (rys. 23.3). Zostaną utworzone nowa domena, drzewo i las.



Rys. 23.3. **Wybór operacji wdrażania AD**

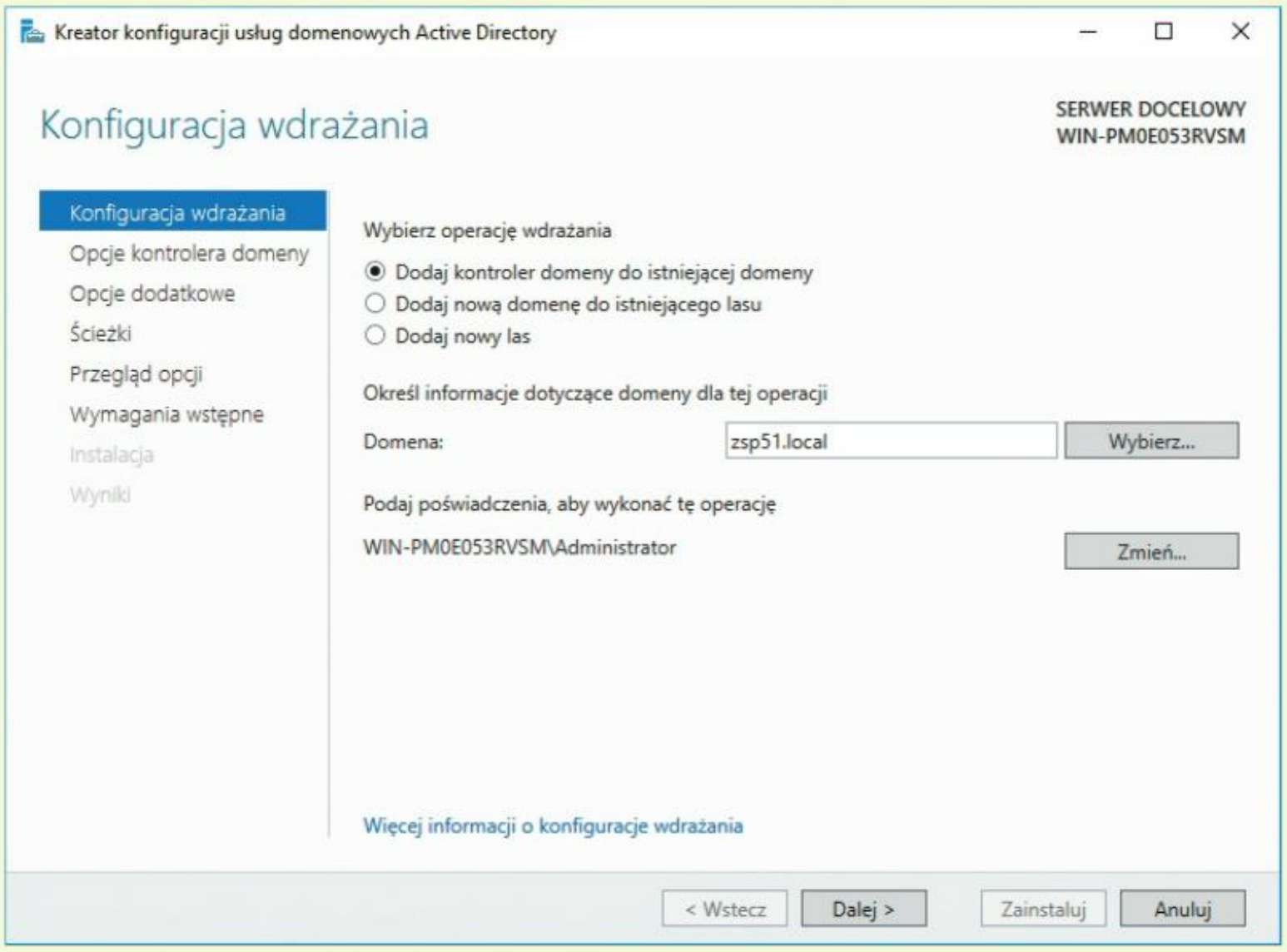
3. Wybrać poziom funkcjonalności lasu **Windows Server 2016** (rys. 23.4), jeżeli wszystkie kontrolery w domenie będą działały w tym poziomie (lub niższym, jeśli w domenie będą starsze wersje kontrolerów, np. Windows Server 2008). Zaznaczyć instalację serwera **DNS**. Usługa DNS jest wymagana – zwykle instaluje się ją na pierwszym kontrolerze w domenie. Na pierwszym kontrolerze w domenie musi być zainstalowany **Wykaz globalny**. Wszystkie obiekty w obrębie drzewa mają odnośniki w wykazie globalnym, co pozwala na wyszukiwanie obiektów w innych domenach (w całym lesie). W wykazie globalnym znajdują się tylko atrybuty wykorzystywane do wyszukiwania obiektów, np. *imię, nazwisko*. W każdym lesie musi być przynajmniej jeden wykaz globalny.
4. Wprowadzić dwukrotnie hasło administratora. Kliknąć przycisk **Dalej**.
5. Domena nie jest zarejestrowana w internecie, dlatego pojawia się błąd systemu DNS. Kontynuować pracę kreatora – kliknąć przycisk **Dalej**.
6. Zweryfikować nazwę NetBIOS domeny – pozostawić bez zmian. Kliknąć przycisk **Dalej**.
7. Zatwierdzić ścieżki do katalogów przechowujących dane Active Directory. Kliknąć przycisk **Dalej**.
8. Zapoznać się z podsumowaniem. Kliknąć przycisk **Dalej**, a następnie **Zainstaluj**.
9. Po zakończeniu instalacji ponownie uruchomić komputer.

PRZYKŁAD 23.3

Instalowanie kontrolera domeny tylko do odczytu

W utworzonej w poprzednim ćwiczeniu domenie zostanie zainstalowany kontroler domeny tylko do odczytu. Przed rozpoczęciem instalacji trzeba upewnić się o możliwości komunikacji między serwerami (polecenie **ping**) i na komputerze z RODC ustawić jako adres serwera DNS adres IP pierwszego kontrolera domeny. Aby skonfigurować kontroler domeny tylko do odczytu, należy:

1. Zainstalować rolę **Usługi domenowe Active Directory** i uruchomić kreatora promowania serwera do poziomu kontrolera domeny.
2. W oknie **Konfiguracja wdrażania** zaznaczyć opcję **Dodaj kontroler domeny do istniejącej domeny** i wprowadzić nazwę domeny, np. **zsp51.local**, do której jest dodawany kontroler RODC (rys. 23.4). Podać poświadczenia, np. konto **zsp51.local\Administrator** i hasło. Kliknąć przycisk **Dalej**.
3. Wybrać opcje kontrolera domeny. Dla kontrolera RODC można nie instalować funkcji serwera DNS i wykazu globalnego. Zaznaczyć opcję **Kontroler domeny tylko do odczytu (RODC)**. Wpisać hasło trybu przywracania usług katalogowych (DSRM), np. *Qwerty123*. Kliknąć przycisk **Dalej**.
4. Wybrać opcje kontrolera RODC (można pozostawić wartości domyślne). Kliknąć przycisk **Dalej**.
5. Wybrać opcje dodatkowe (można pozostawić wartości domyślne). Kliknąć przycisk **Dalej**.
6. Zatwierdzić ścieżki do katalogów przechowujących dane Active Directory. Kliknąć przycisk **Dalej**.
7. Zapoznać się z podsumowaniem. Kliknąć przycisk **Dalej**, a następnie **Zainstaluj**.
8. Po zakończeniu instalacji ponownie uruchomić komputer.



Rys. 23.4. **Wybór operacji wdrażania kontrolera RODC**

W systemie Windows Server do zarządzania domeną można wykorzystać przystawki konsoli mmc:

- **Użytkownicy i komputery usługi Active Directory** – służy do zarządzania komputerami, użytkownikami i grupami (w warunkach szkolnych do zarządzania siecią z jedną domeną wystarczy tylko ta przystawka);
- **Domeny i relacje zaufania Active Directory** – umożliwia pracę z domenami, drzewami domen;
- **Lokacje i usługi Active Directory** – zarządza lokacjami i podsieciami, czyli strukturą fizyczną;
- **Wynikowy zestaw zasad** – pozwala na planowanie zmian i przeglądanie zasad dla użytkowników.

PRZYKŁAD 23.4

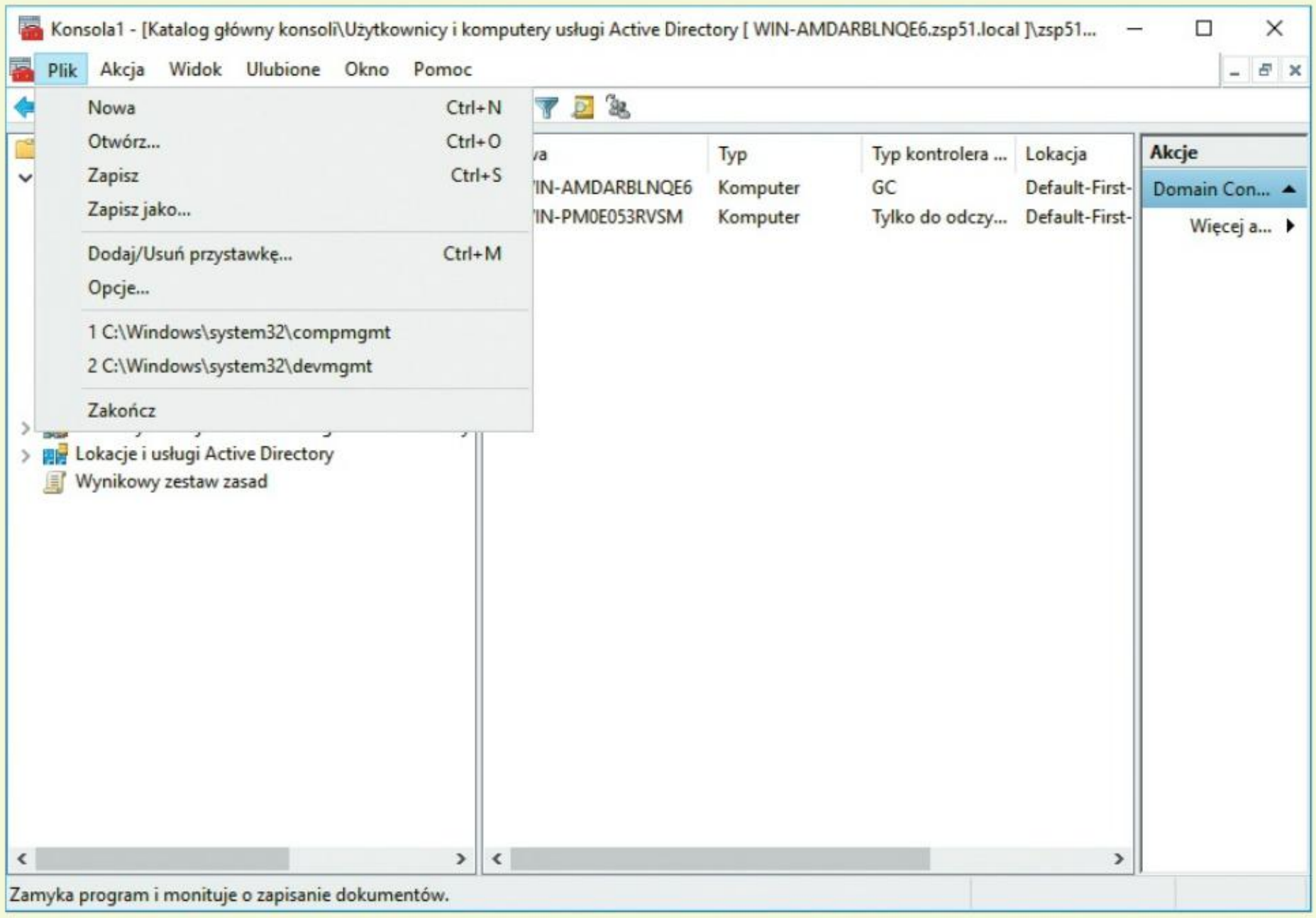
Dodawanie przystawki do konsoli mmc

Przystawki możemy dodać do konsoli mmc, a następnie zapisać ustawienia, co ułatwi zarządzanie usługami w przyszłości.

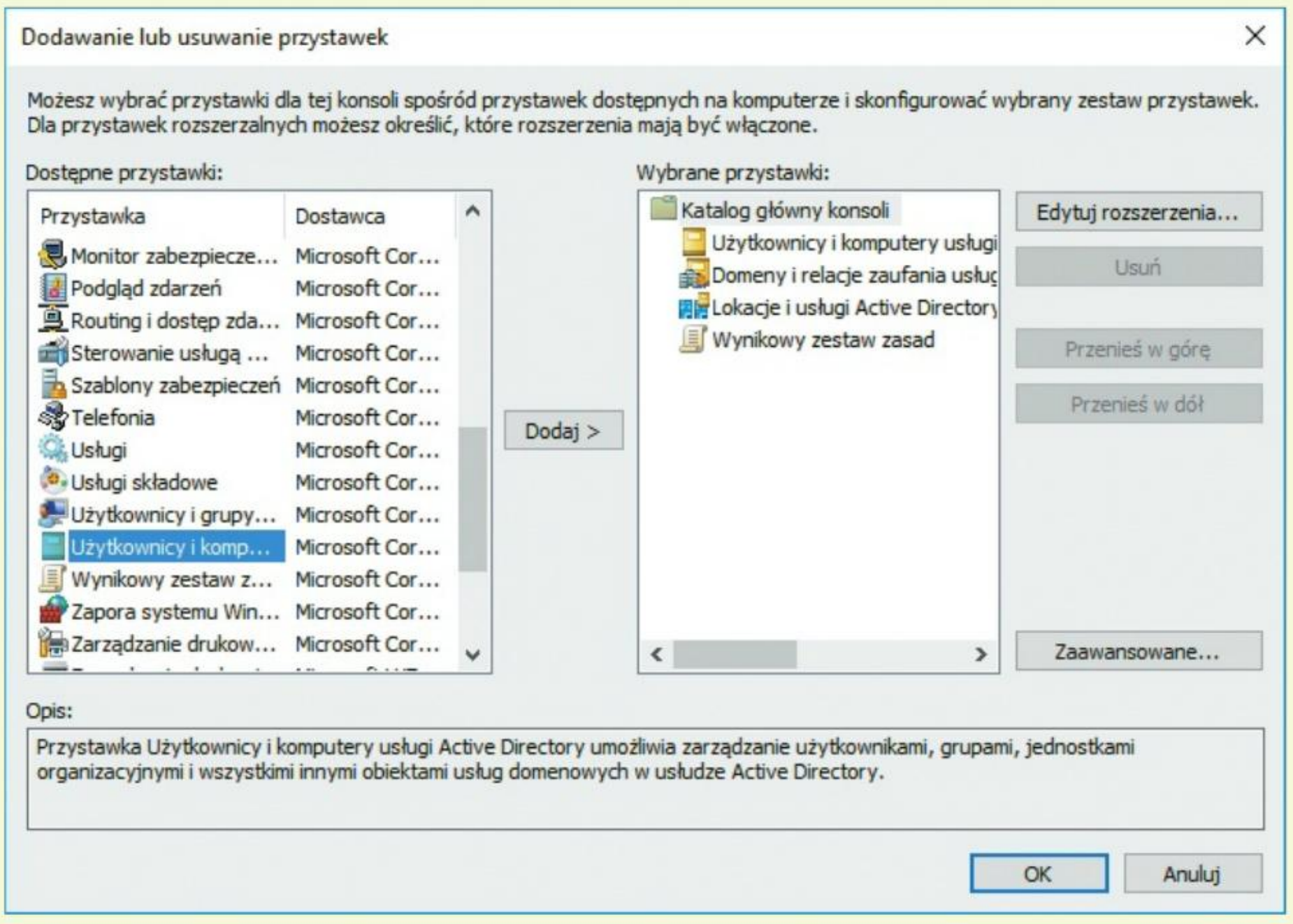
Aby dodać przystawkę do konsoli mmc, należy:

1. Uruchomić konsolę. Kliknąć przycisk wyszukiwania, a następnie w pole **`Wyszukaj w systemie Windows`** wpisać **`mmc`** i nacisnąć [Enter].
2. W oknie konsoli (rys. 23.5) z menu głównego wybrać **`Plik/Dodaj/Usuń przystawkę`**.
3. Przeciągnąć z lewego panelu do prawego te przystawki, które mają się znaleźć w oknie konsoli (rys. 23.6). Kliknąć przycisk **`OK`**.

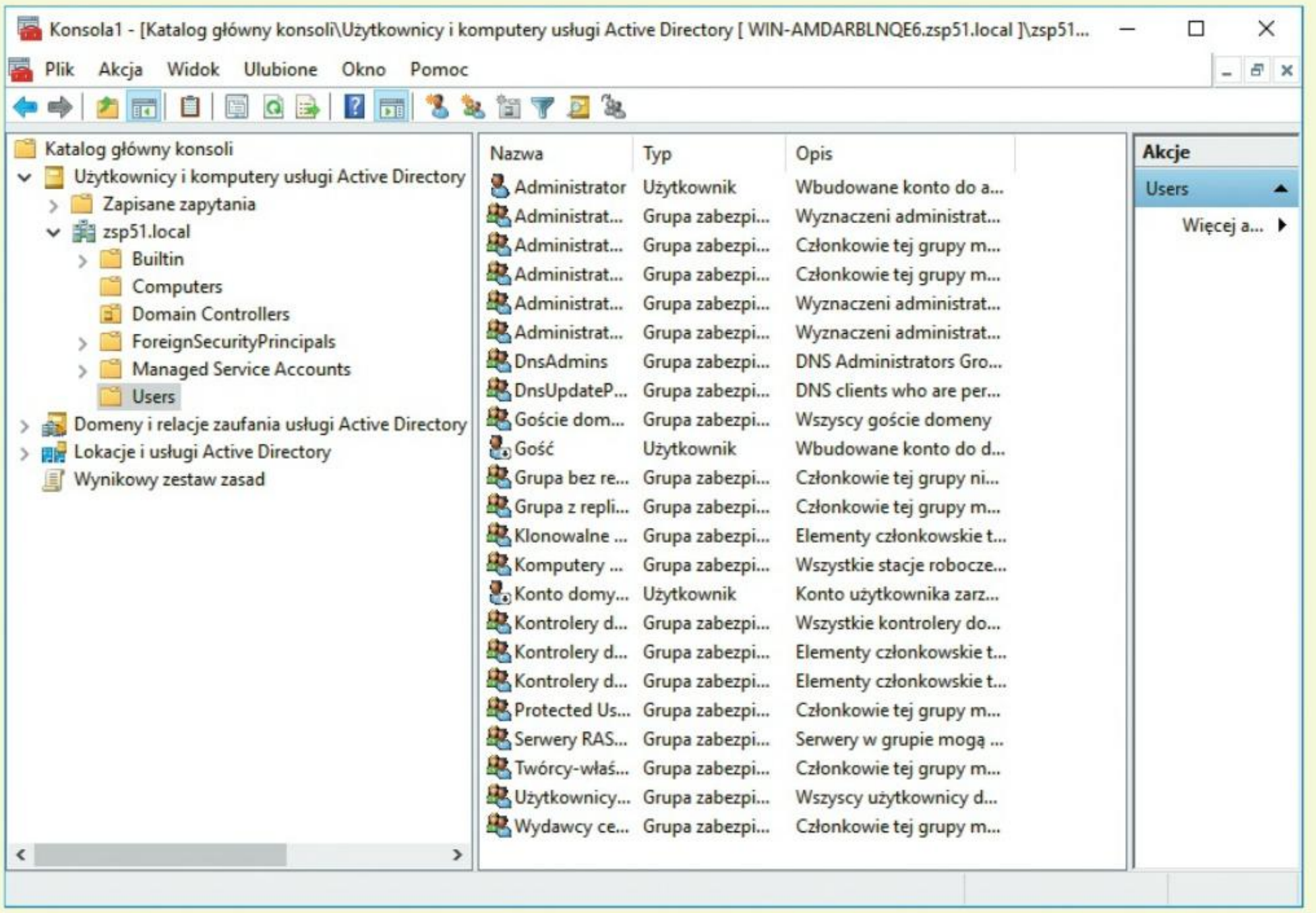
W konsoli na rys. 23.7 pokazano wszystkie przystawki służące do zarządzania domeną i listę użytkowników domeny utworzonych podczas instalacji. Należy zapisać ustawienia konsoli – z menu głównego wybrać **`Plik/Zapisz jako`** oraz wskazać nazwę pliku i miejsce do zapisu.



Rys. 23.5. **Dodawanie przystawki**



Rys. 23.6. **Zaznaczanie przystawek do dodania do konsoli**

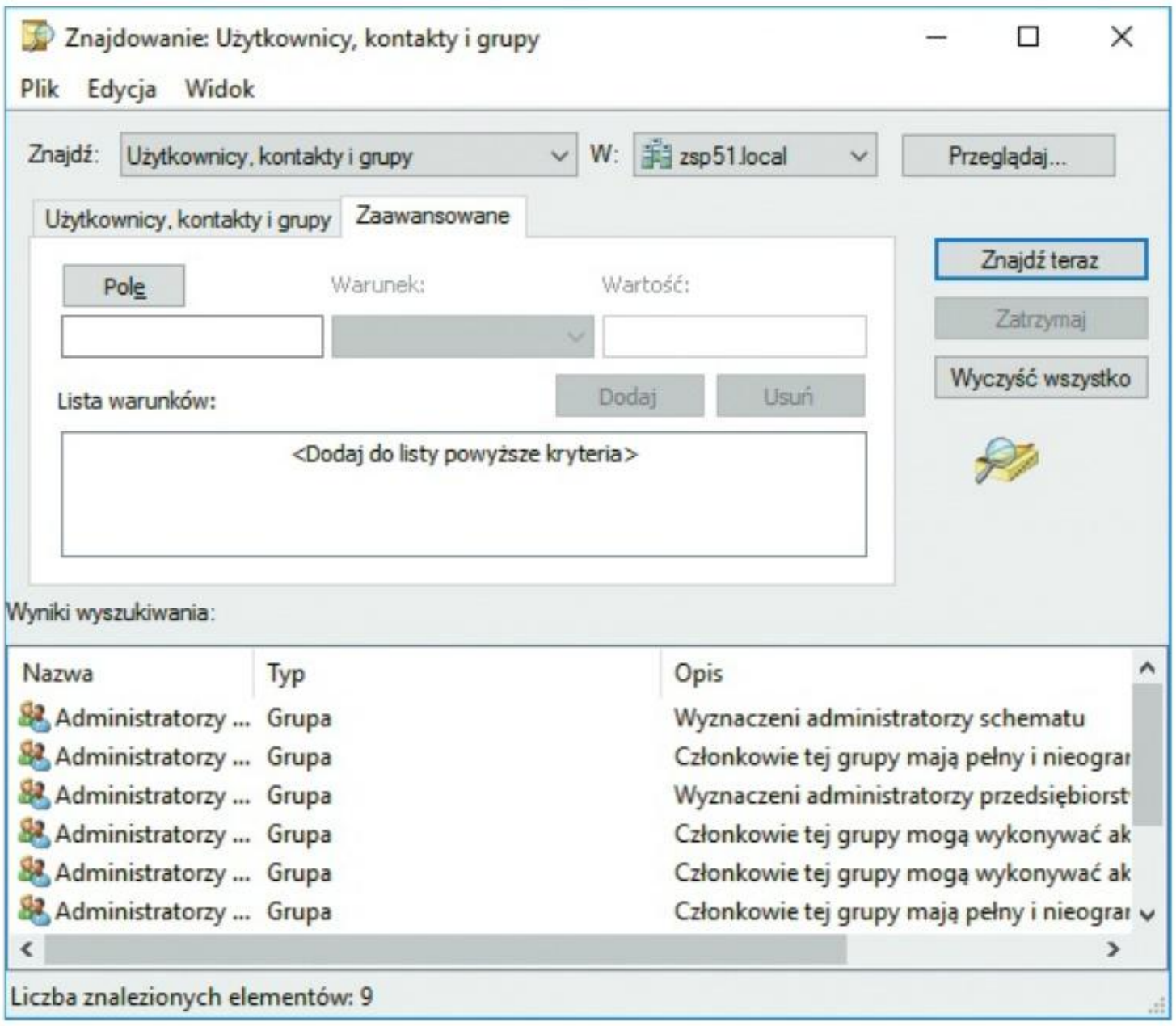


Rys. 23.7. **Przystawki do zarządzania domeną**

Za pomocą przystawki **Użytkownicy i komputery Active Directory** można wykonywać wszystkie zadania związane z użytkownikami, grupami i komputerami. Po jej uruchomieniu zobaczymy drzewo przedstawiające obiekty użytkowników i komputerów aktualnej domeny. Aby zarządzać użytkownikami innej domeny, należy kliknąć prawym przyciskiem myszy gałąź **Użytkownicy i komputery usługi Active Directory** i wybrać **Zmień kontroler domeny** lub **Wybierz domenę**. W tym narzędziu po lewej stronie występują foldery:

- **Zapisane zapytania** – zapisane kryteria wyszukiwania;
- **Builtin** – lista wbudowanych kont użytkowników;
- **Computers** – kontener dla kont komputerów;
- **Domain Controllers** – kontener dla kontrolerów domeny;
- **ForeignSecurityPrincipals** – zawiera informacje o obiektach należących do zaufanych domen zewnętrznych;
- **Users** – kontener dla kont użytkowników.

W przystawce można wyszukiwać obiekty w katalogu, np. użytkowników, grupy, komputery, drukarki, foldery udostępnione, jednostki organizacyjne. Interesująca jest opcja, która umożliwia szybkie wyszukiwanie kont na podstawie takich cech, jak nielogowanie się w określonym czasie, wygasanie haseł czy wyłączenie. Aby otworzyć okno wyszukiwania, klikamy wybraną domenę lub inny kontener prawym klawiszem myszy i z menu kontekstowego wybieramy **Znajdź** (rys. 23.8).



Rys. 23.8. **Wyszukiwanie obiektów**

Wyszukanym obiektem można bezpośrednio zarządzać, np. gdy w wyniku wyszukiwania zobaczymy kilku użytkowników, to po kliknięciu prawym przyciskiem myszy wybranego użytkownika możemy zmienić jego nazwę, przenieść go lub usunąć, dodać go do grupy, wyłączyć konto lub zresetować jego hasło.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

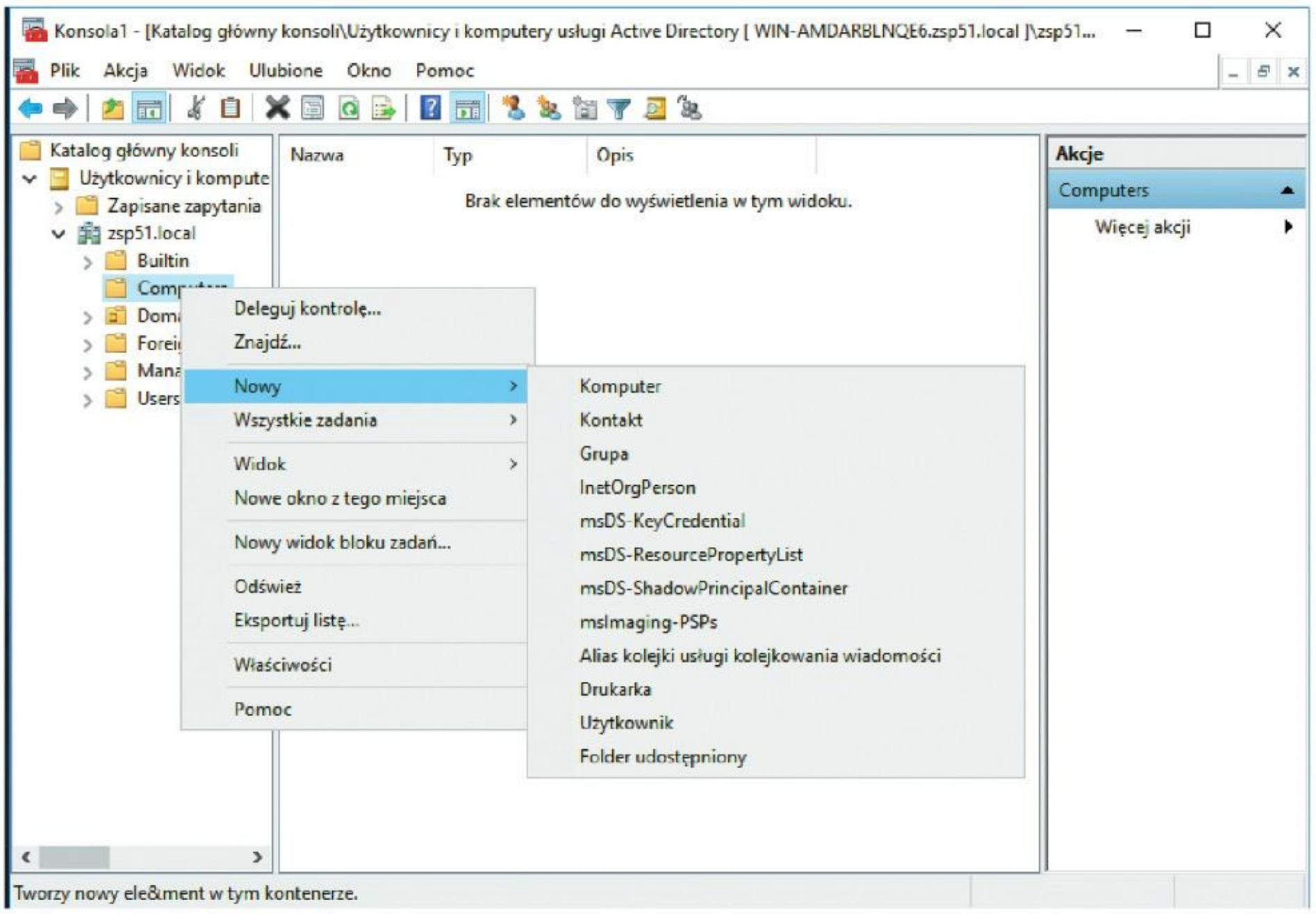
1. Zainstaluj drugi kontroler w domenie.
2. Skonfiguruj poddomenę domeny głównej, np. domena **`zsp51.local`** i poddomena **`klasa2.zsp51.local`**.

24 Zarządzanie kontami komputerów. Dodawanie komputerów do domeny

ZAGADNIENIA

- **Zarządzanie kontami komputerów**
- **Dodawanie komputerów do domeny**
- **Zalogowanie się do domeny**

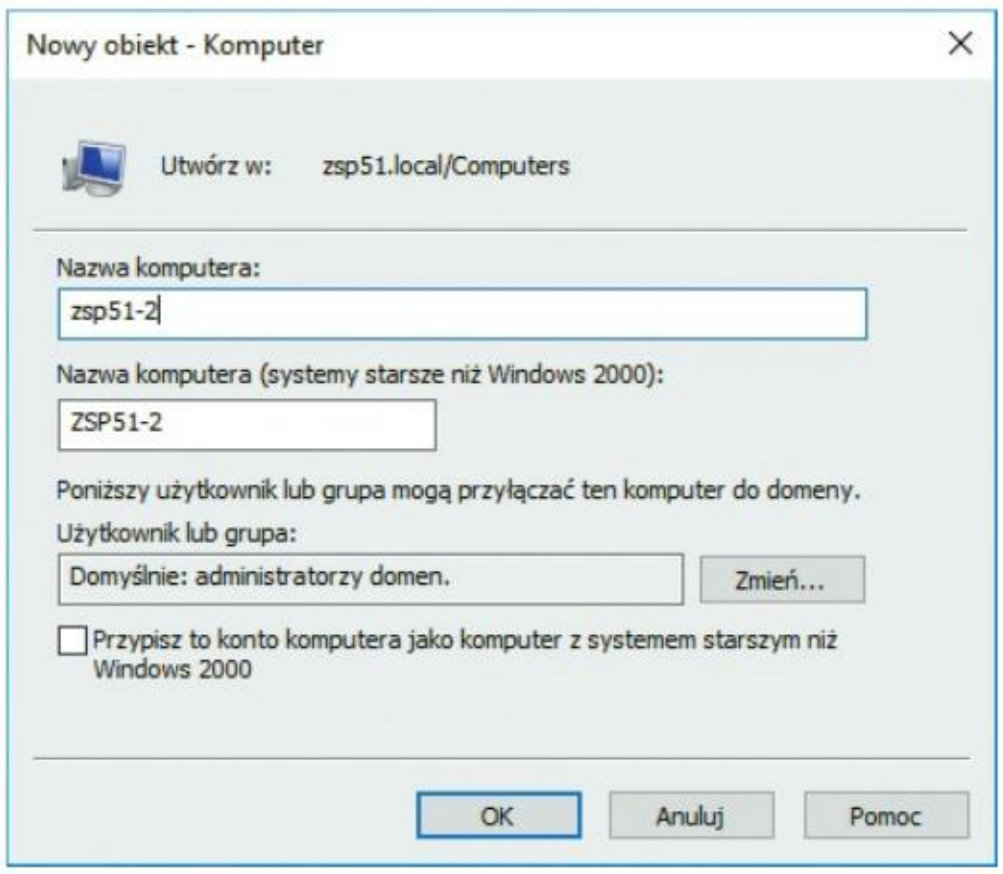
Każdy komputer, który łączy się z domeną, musi mieć swoje **konto**. Kontami komputerów zarządza się za pomocą przystawki **`Użytkownicy i komputery usługi Active Directory`** w konsoli mmc. Konta komputerów są domyślnie zlokalizowane w kontenerze **`Computers`**. Powinno się je utworzyć przed przyłączeniem komputera do domeny. Pozwala to na umieszczenie ich w wybranym kontenerze i w konsekwencji łatwe zarządzanie nimi. Aby utworzyć nowe konto komputera, należy kliknąć prawym klawiszem myszy wybrany kontener, np. **`Computers`**, i z menu kontekstowego wybrać **`Nowy/Komputer`** (rys. 24.1).



Rys. 24.1. Tworzenie konta komputera

Zostanie uruchomiony **`Kreator tworzenia konta nowego komputera`**. Najpierw należy podać nazwę nowego komputera i nazwę komputera dla systemów starszych niż Windows 2000 (rys. 24.2).

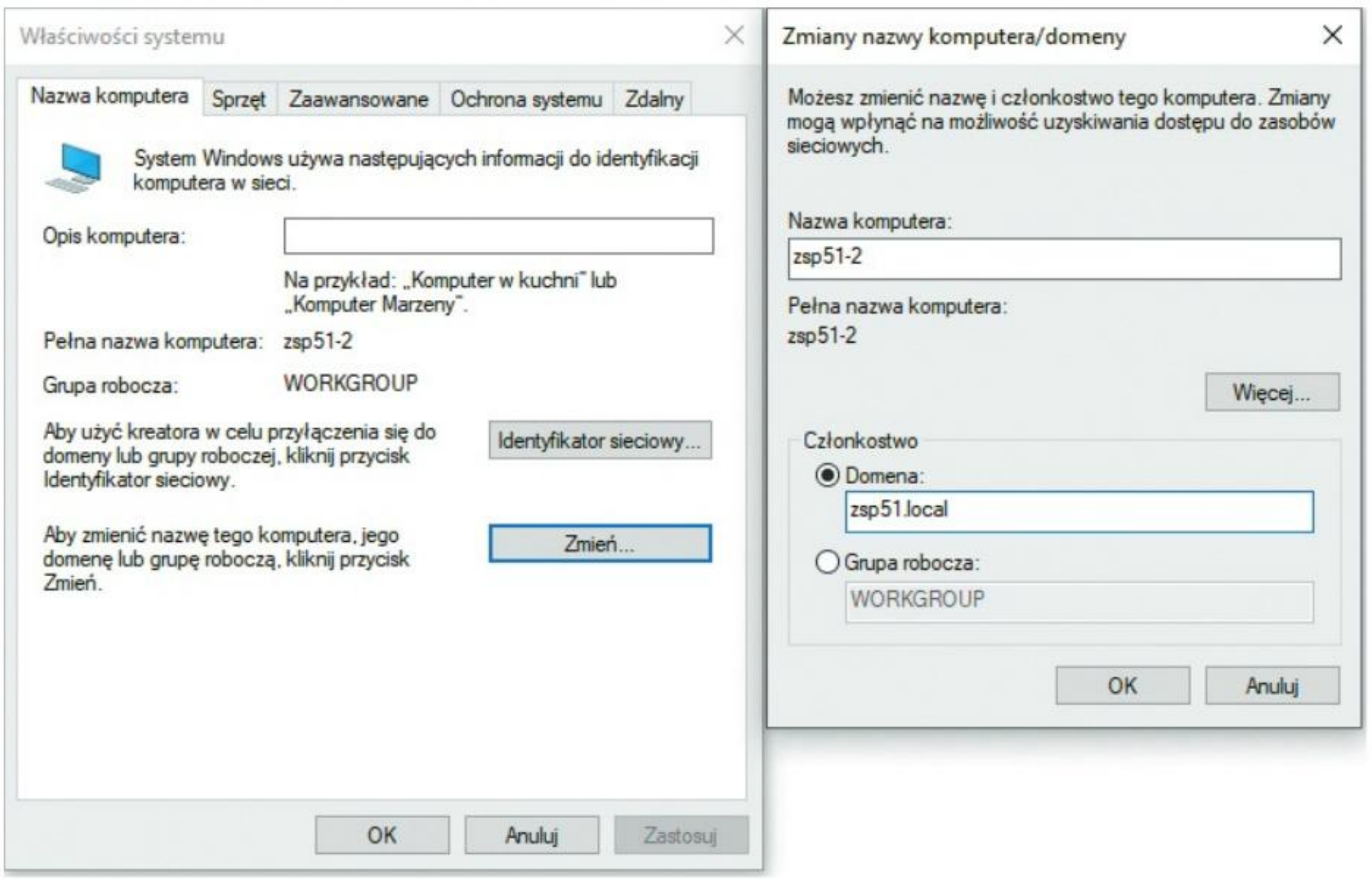
Domyślnie konto komputera może utworzyć grupa *Administratorzy domen*. Możemy delegować to uprawnienie dla użytkownika, jeśli klikniemy przycisk **Zmień**. Jeżeli na przyłączanym komputerze jest starszy system niż Windows 2000, należy wówczas zaznaczyć pole **Przypisz to konto komputera jako komputer z systemem starszym niż Windows 2000**. Nieużywane konta komputerów możemy wyłączyć lub usunąć. W tym celu otwieramy kontener, w którym jest zapisane konto, następnie klikamy prawym klawiszem myszy niepotrzebne konto, po czym z menu wybieramy **Usuń** lub **Wyłącz konto**. Można wyłączyć tylko konta aktualnie nieużywane. Wyłączone konto, po kliknięciu prawym klawiszem myszy, będzie miało opcję **Włącz konto**.



Rys. 24.2. **Tworzenie konta komputera**

Aby dołączyć komputer z Windows 10 do domeny, należy najpierw zalogować się na tym komputerze do konta z uprawnieniami administratora lokalnego. Przed przyłączeniem komputera do domeny trzeba się upewnić, czy jest możliwość komunikacji między komputerem i kontrolerem domeny (polecenie **ping**) i w konfiguracji protokołu TCP/ IP komputera przypisać adres kontrolera domeny jako adres serwera DNS.

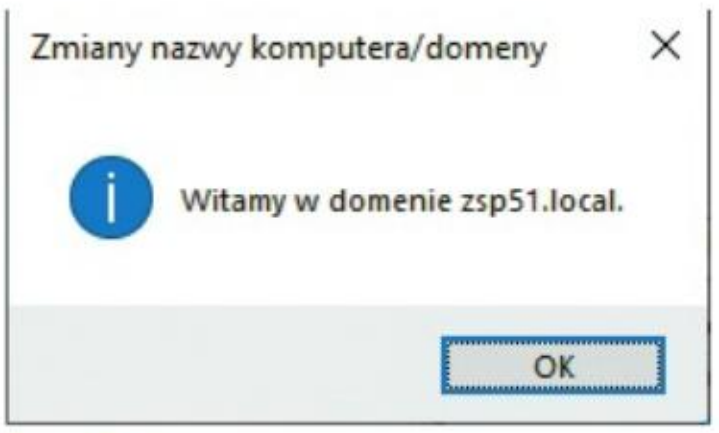
W oknie **System** (**Start/Panel sterowania/System**), w sekcji **Nazwa komputera** kliknąć przycisk **Zmień ustawienia**. W oknie **Właściwości systemu** kliknąć przycisk **Zmień** i w oknie **Zmiany nazwy komputera** (rys. 24.3) zmienić opcję **Grupa robocza** na **Domena**, a następnie wpisać nazwę domeny, np. **zsp51.local**.



Rys. 24.3. **Konfigurowanie Windows 10 do logowania w domenie**

Po wprowadzeniu nazwy konta administratora na kontrolerze domeny i pomyślnym zweryfikowaniu hasła pojawia się okno potwierdzające przyłączenie komputera do domeny (rys. 24.4).

Aby wprowadzone zmiany odniosły skutek, musimy uruchomić ponownie klienta (komputer z Windows 10). W oknie logowania powinna pojawić się opcja logowania do domeny (rys. 24.5).



Rys. 24.4. **Okno potwierdzające przyłączenie do domeny**

Rys. 24.5. **Opcja logowania do domeny**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Utwórz konto dla komputera koleżanki / kolegi. Nazwij konto imieniem koleżanki / kolegi.
2. Przyłącz swój komputer do domeny zarządzanej przez koleżankę / kolegę.
3. Na komputerze przyłączonym do domeny sprawdź możliwość logowania się na konto lokalne. Zapisz w zeszycie login i hasło do logowania lokalnego.

25 Zarządzanie kontami użytkowników

ZAGADNIENIA

Tworzenie kont użytkowników **Modyfikowanie właściwości użytkowników** **Tworzenie grup użytkowników i sposoby zarządzania nimi** **Polecenie do zarządzania użytkownikami w konsoli tekstowej** **Jak zarządzać użytkownikami w konsoli tekstowej** **Co to jest konsola PowerShell** **Jak uruchomić konsolę PowerShell** **Jak zarządzać użytkownikami w konsoli PowerShell**

Wszystkie konta użytkowników są identyfikowane przez system za pomocą identyfikatora **SID** (ang. *Security Identifier*). Identyfikator SID jest automatycznie tworzony wraz z ustanawianiem nowych kont użytkowników (zarówno lokalnych, jak i domenowych). Gdy usuwa się konto użytkownika, usuwa się również jego identyfikator. Utworzenie konta o tej samej nazwie co usunięty użytkownik powoduje utworzenie nowego identyfikatora SID (dla systemu będzie to inny użytkownik – inny identyfikator SID).

Jednym z głównych zadań administratora jest zarządzanie kontami użytkowników i grup. Konta użytkowników pozwalają na logowanie się indywidualnych użytkowników do zasobów sieciowych, a konta grupowe – na zarządzanie wieloma użytkownikami jednocześnie. Uprawnienia nadawane użytkownikom mają zapewnić bezpieczeństwo w systemie, ale jednocześnie umożliwić wykonanie zadań, dlatego należy nadawać użytkownikom tylko niezbędne uprawnienia.

Podstawowymi składnikami systemu bezpieczeństwa w Windows Server są: **uwierzytelnianie użytkowników** i **kontrola dostępu**. Uwierzytelnianie użytkowników składa się z dwóch faz:

- **interaktywnego logowania** – podczas logowania na lokalnym komputerze sprawdza tożsamość i nadaje dostęp lub odmawia dostępu do usługi Active Directory;
- **uwierzytelniania sieciowego** – uprawnienia użytkownika są sprawdzane podczas każdej próby skorzystania z zasobu sieciowego. W Windows Server do uwierzytelniania sieciowego jest wykorzystywany **protokół Kerberos**, który zapewnia odpowiedni poziom bezpieczeństwa. Sprawdzanie uprawnień do zasobów sieciowych realizuje się przez usługę Active Directory, dzięki czemu użytkownik może być uwierzytelniony na dowolnym kontrolerze domeny.

Podczas logowania na komputerze przyłączonym do domeny użytkownik wybiera sposób logowania. Może zalogować się lokalnie – korzysta wtedy z konta istniejącego na komputerze – w takim przypadku będzie miał uprawnienia do korzystania tylko z komputera lokalnego. Jeżeli wskaże nazwę domeny i poprawną nazwę konta wraz z odpowiadającym mu hasłem, to zaloguje się do domeny i po uwierzytelnieniu uzyska dostęp do zasobów zdefiniowanych w Active Directory.

Podczas instalacji systemu jest tworzonych wiele kont specjalnych, wykorzystywanych w systemie. Na rys. 25.1 przedstawiono listę użytkowników domeny bezpośrednio po instalacji. Tylko konto administratora umożliwia korzystanie z usług. Dla pozostałych użytkowników należy

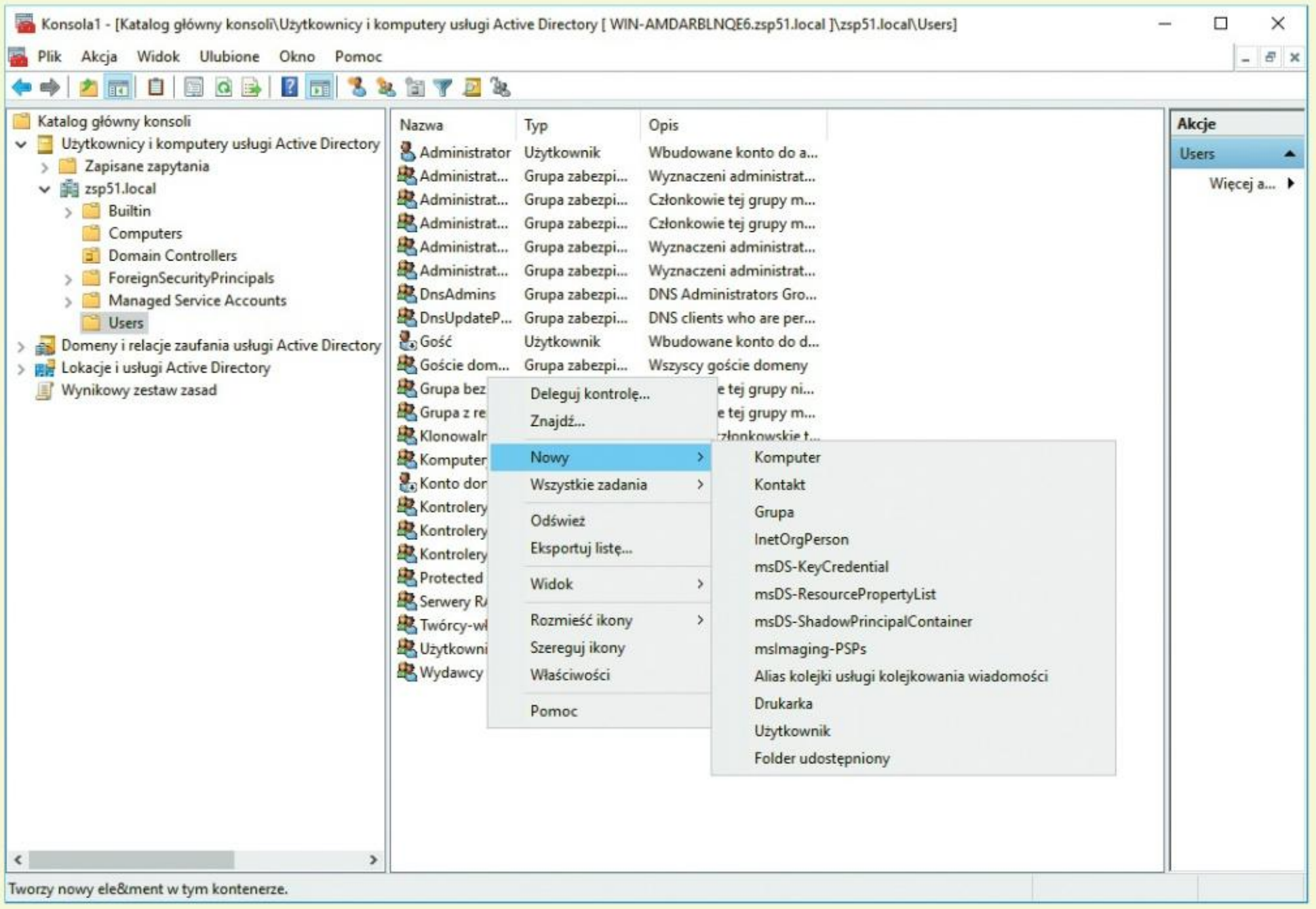
takie konta utworzyć. Jest to zadanie odpowiedzialne i wymaga wcześniejszego opracowania systemu nazw dla kont. Najczęściej stosuje się nazwę konta zawierającą pierwszą literę imienia i nazwisko lub imię i nazwisko użytkownika pisane razem, np. Jan Kowalski może mieć konto o nazwie *jkowalski*, *jankowalski* lub *jan.kowalski*. Konta użytkowników domyślnie znajdują się w kontenerze **`Users`**.

PRZYKŁAD 25.1

Tworzenie konta użytkownika

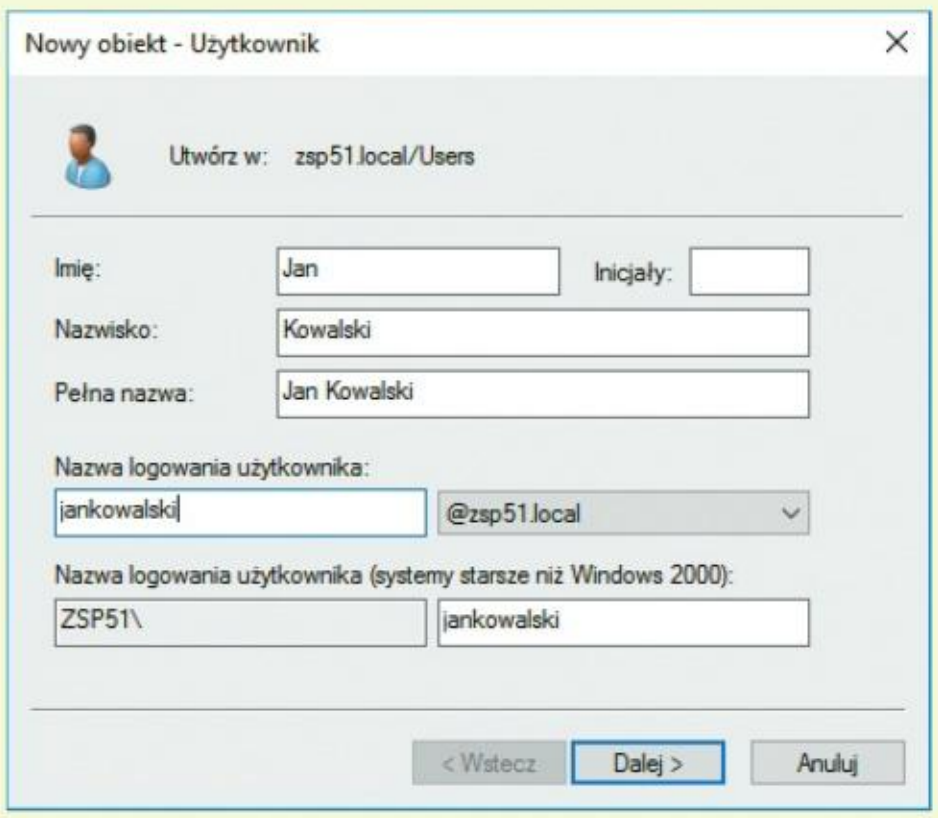
Aby utworzyć nowe konto użytkownika w konsoli mmc, należy:

1. Otworzyć konsolę mmc i przystawkę **`Użytkownicy i komputery usługi Active Directory`**. Odszukać kontener, w którym ma być utworzone konto.
2. Kliknąć prawym przyciskiem myszy obszar roboczy okna i wybrać z menu kontekstowego opcję **`Nowy/Użytkownik`** (rys. 25.1).

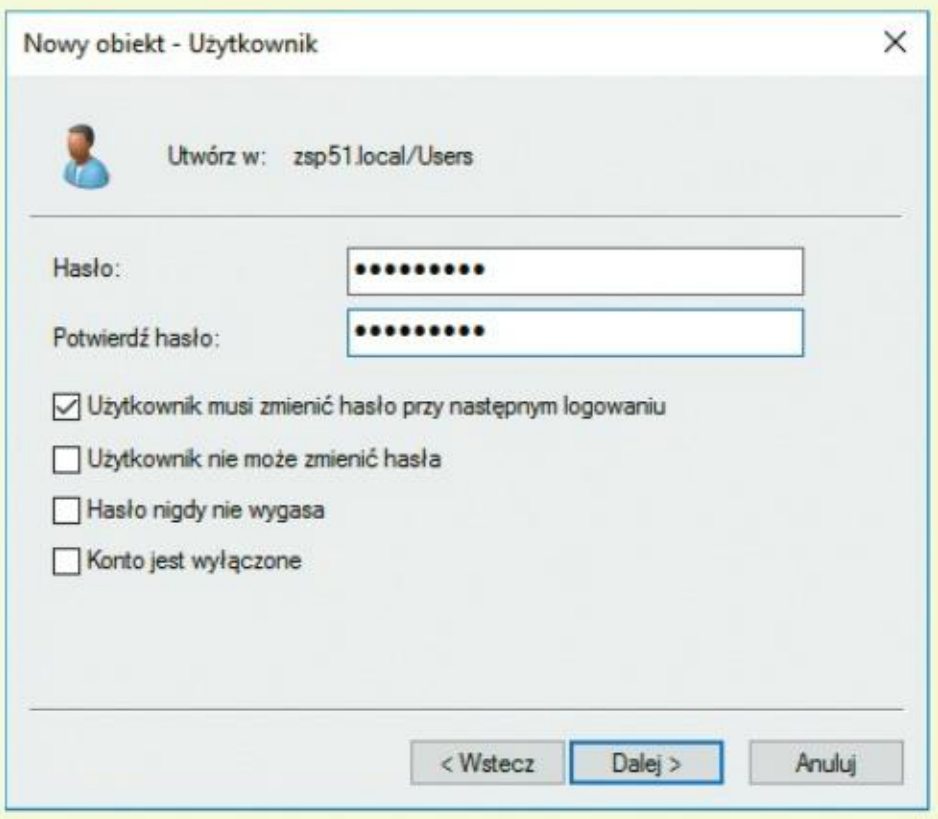


Rys. 25.1. **Otwieranie okna tworzenia nowego użytkownika**

3. W pierwszym oknie (rys. 25.2) kreatora tworzenia użytkownika wpisać informacje o użytkowniku (nazwa logowania oraz imię i nazwisko), a w drugim (rys. 25.3) – wybrać hasło i ustawienia konta.
4. Sprawdzić, czy utworzony w ten sposób użytkownik pojawił się na liście w zakładce.



Rys. 25.2. **Informacje o użytkowniku**



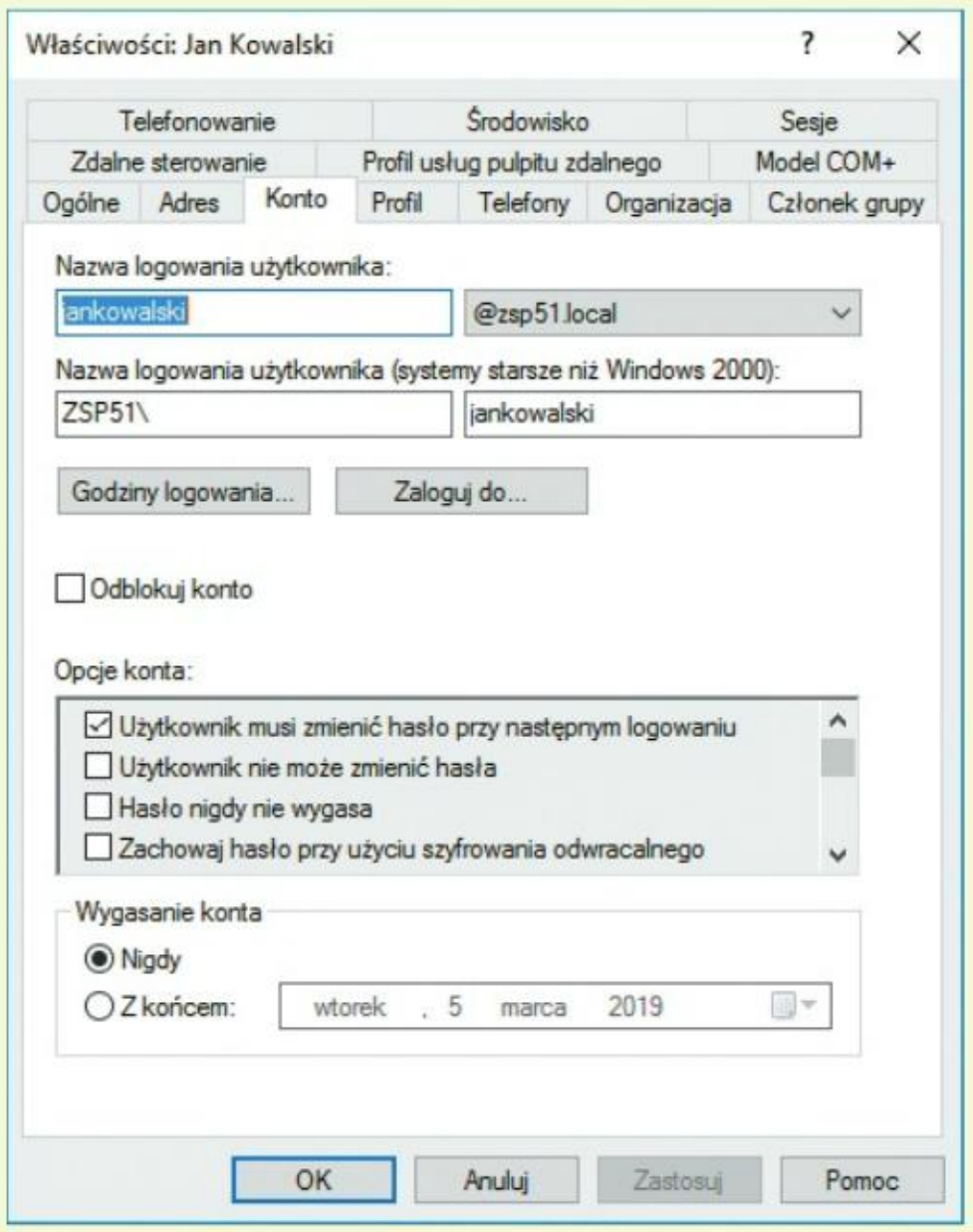
Rys. 25.3. **Hasło i ustawienia konta**

PRZYKŁAD 25.2

Modyfikacja właściwości użytkownika

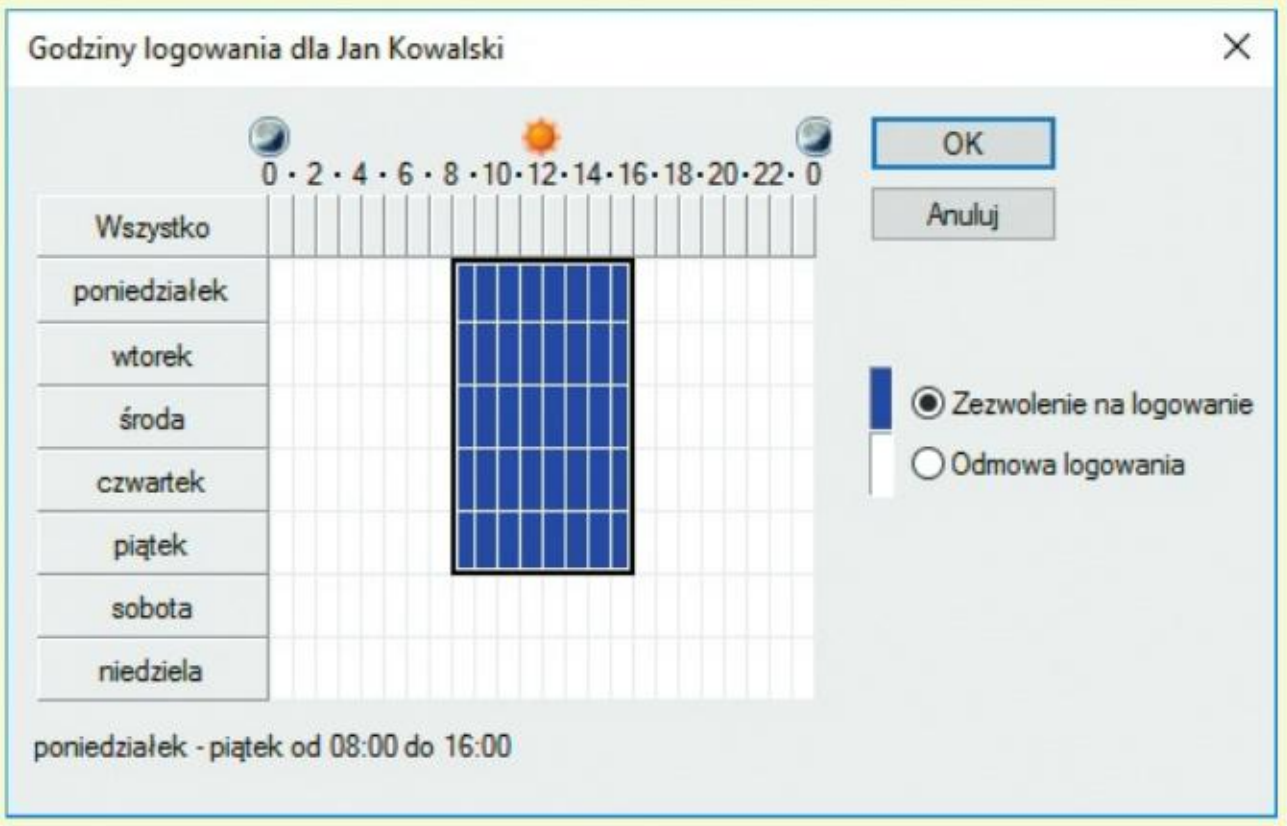
W dowolnym momencie można obejrzeć lub zmodyfikować właściwości użytkownika w przystawce **`Użytkownicy i komputery usługi Active Directory`**. W tym celu należy:

1. Kliknąć prawym klawiszem myszy użytkownika i z menu kontekstowego wybrać polecenie **`Właściwości`** (rys. 25.4) i zakładkę **`Konto`**.

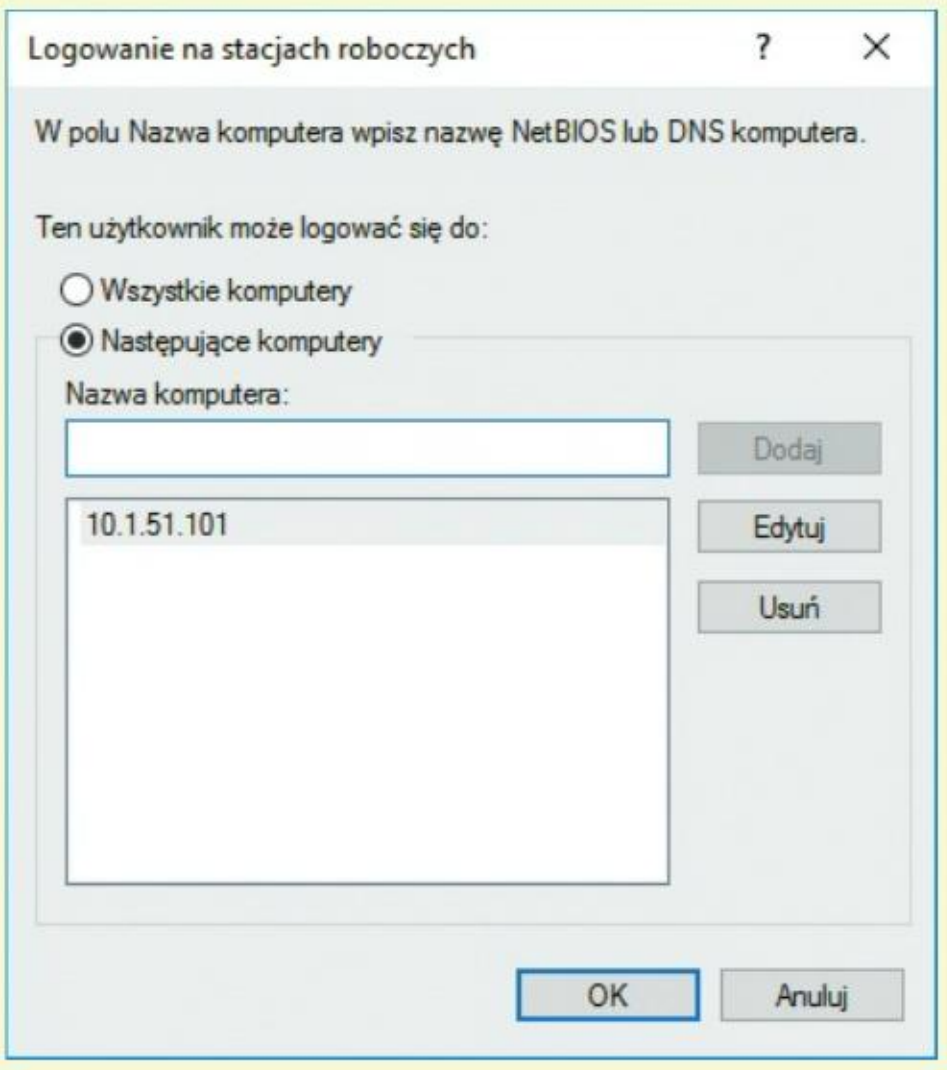


Rys. 25.4. **Właściwości użytkownika**

2. Zmodyfikować czas logowania użytkownika. Użytkownicy będą mogli logować się do domeny tylko w wyznaczonych godzinach, np. w czasie lekcji, co może zwiększyć bezpieczeństwo w systemie. Po kliknięciu przycisku **Godziny logowania** jest otwierane okno pozwalające na wskazanie czasu logowania (rys. 25.5).
3. Ograniczyć możliwość logowania tylko do wyznaczonych stacji roboczych. Użytkownik będzie mógł logować się do domeny tylko z wyznaczonych stacji roboczych, umieszczonych na liście. Po kliknięciu przycisku **Zaloguj do** jest otwierane okno pozwalające na wskazanie nazw lub adresów IP stacji roboczych (rys. 25.6).



Rys. 25.5. **Okno ustawień czasu logowania**



Rys. 25.6. **Okno ustawień miejsca logowania**

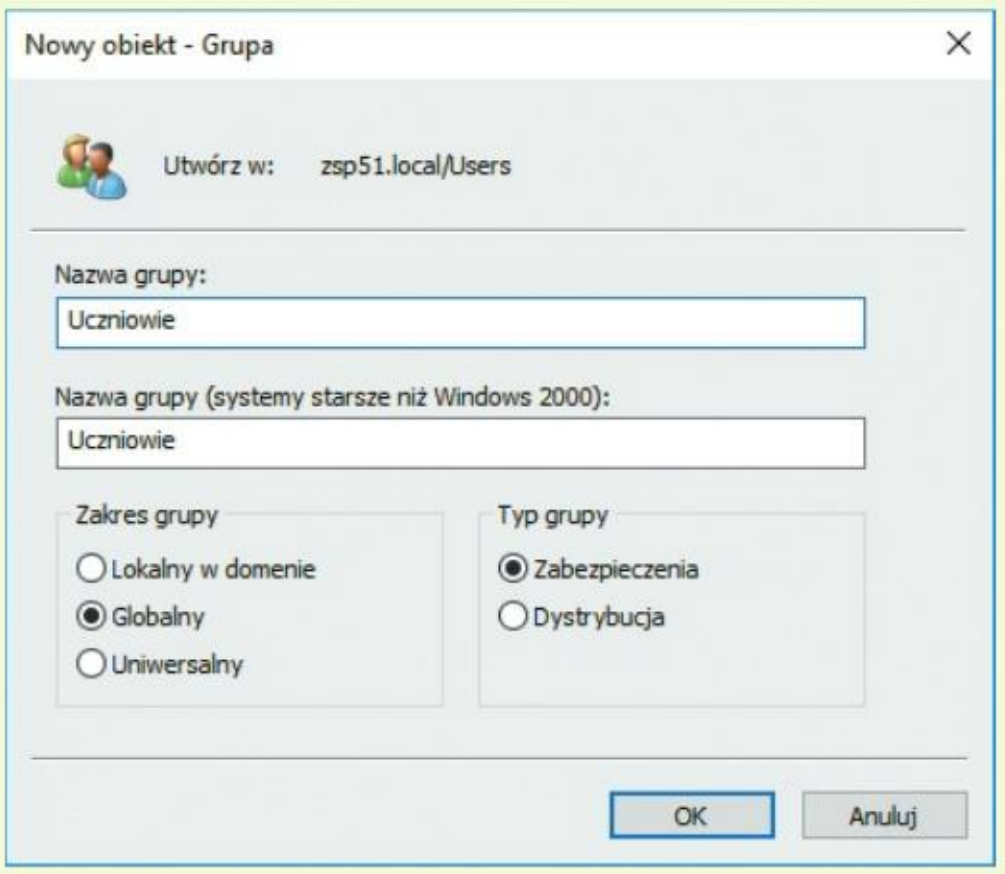
Oprócz kont użytkowników indywidualnych można również tworzyć **grupy użytkowników**. Grupy ułatwią zarządzanie uprawnieniami przyznawanymi użytkownikom.

PRZYKŁAD 25.3

Tworzenie grupy użytkowników

Aby utworzyć nowe konto grupy, należy:

1. Otworzyć konsolę mmc i przystawkę **Użytkownicy i komputery usługi Active Directory**. Odszukać kontener, w którym ma być utworzone konto.
2. Kliknąć prawym przyciskiem myszy obszar roboczy okna i wybrać z menu kontekstowego opcję **Nowy/Grupa** (rys. 25.7). W oknie **Nowy obiekt** podać nazwę tworzonej grupy oraz jej zakres i typ, a następnie kliknąć przycisk **OK**.
3. Sprawdzić, czy utworzona w ten sposób grupa pojawiła się na liście w zakładce.



Rys. 25.7. **Tworzenie grupy**

PRZYKŁAD 25.4

Zarządzanie członkostwem w grupach

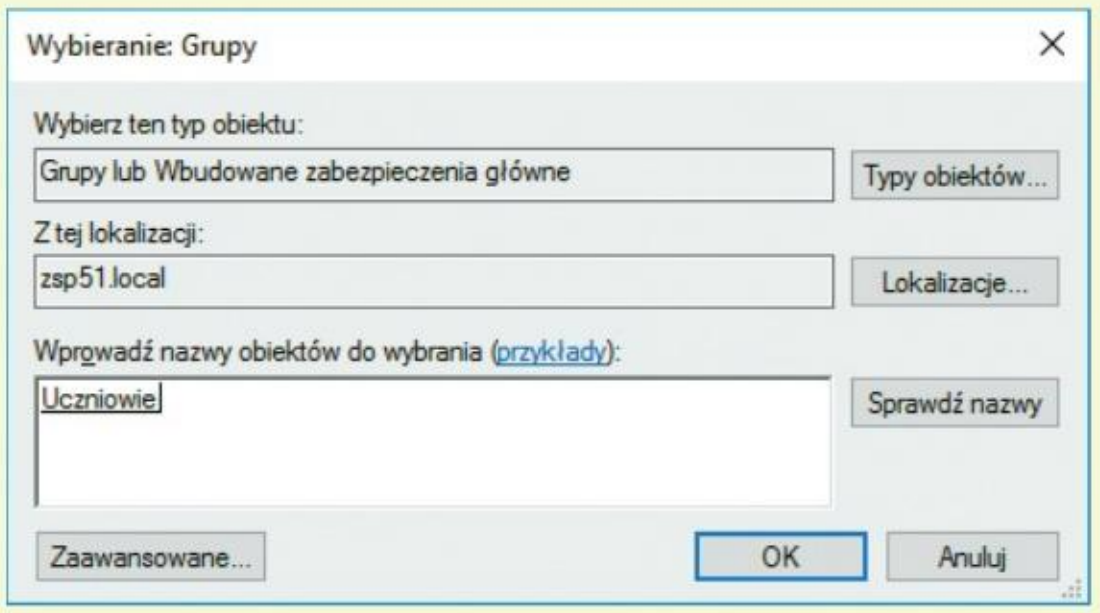
Po utworzeniu kont należy dołączyć użytkowników do grup. Członkami grup mogą być użytkownicy indywidualni lub inne grupy.

Użytkownika można przyłączyć do grupy w następujący sposób:

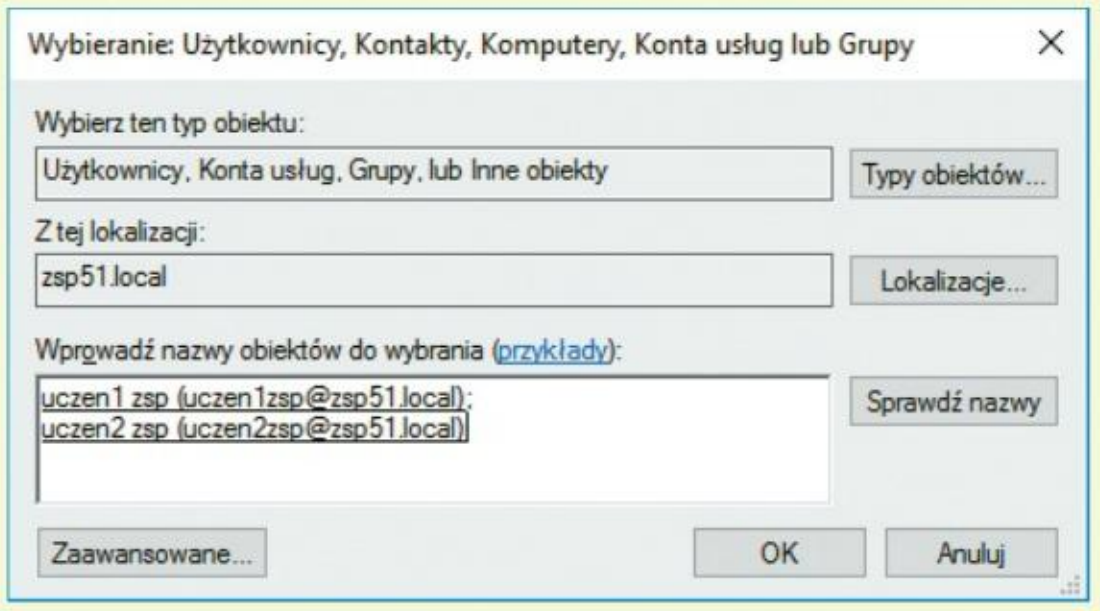
1. Otworzyć konsolę mmc i przystawkę **Użytkownicy i komputery usługi Active Directory**.
2. Kliknąć prawym przyciskiem myszy nazwę użytkownika i z menu kontekstowego wybrać polecenie **Dodaj do grupy** (rys. 25.8). Po wskazaniu nazwy użytkownika i kliknięciu przycisku **OK** użytkownik zostanie członkiem grupy.
3. Sprawdzić, czy użytkownik pojawił się na liście członków grupy.

Dołączenie użytkownika do grupy jest również możliwe za pomocą zakładki **Członkowie** we właściwościach grupy. Można to wykonać w następujący sposób:

1. Kliknąć prawym przyciskiem myszy nazwę grupy i z menu kontekstowego wybrać polecenie **Właściwości**.
2. W oknie **Właściwości** wybrać zakładkę **Członkowie**, a następnie przycisk **Dodaj** (rys. 25.9). Po wskazaniu nazwy użytkownika i kliknięciu przycisku **OK** użytkownik zostanie członkiem grupy.
3. Sprawdzić, czy użytkownik pojawił się na liście członków grupy.



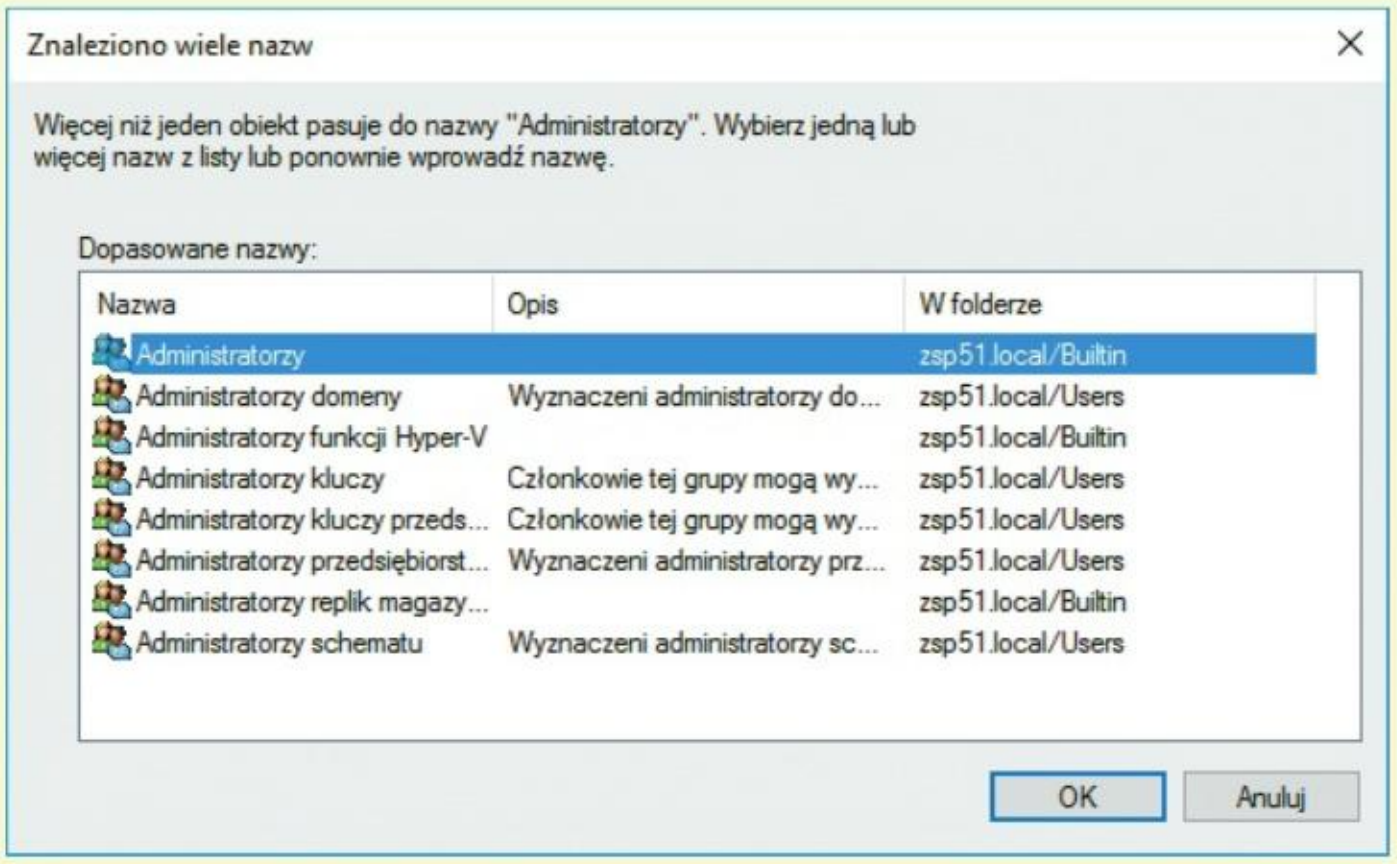
Rys. 25.8. **Dołączanie użytkownika do grupy**



Rys. 25.9. **Dodawanie użytkownika do grupy**

Członkiem grupy może być również inna grupa. Dodawanie grupy *Uczniowie* do grupy *Administratorzy* może przebiegać następująco:

1. Kliknąć prawym przyciskiem myszy na grupę *Uczniowie* i z menu kontekstowego wybrać polecenie **`Dodaj do grupy`**.
2. Po wpisaniu nazwy *Administratorzy* kliknąć przycisk **`Sprawdź nazwy`**. Ponieważ istnieje więcej grup, których nazwy zaczynają się od *Administratorzy*, zostanie wyświetlone okno z listą tych nazw (rys. 25.10). Należy wskazać właściwą nazwę grupy i kliknąć przycisk **`OK`**.
3. Kliknąć przycisk **`OK`**, aby zakończyć dodawanie członka do grupy.
4. Sprawdzić, czy grupa *Uczniowie* pojawiła się na liście członków grupy *Administratorzy*.



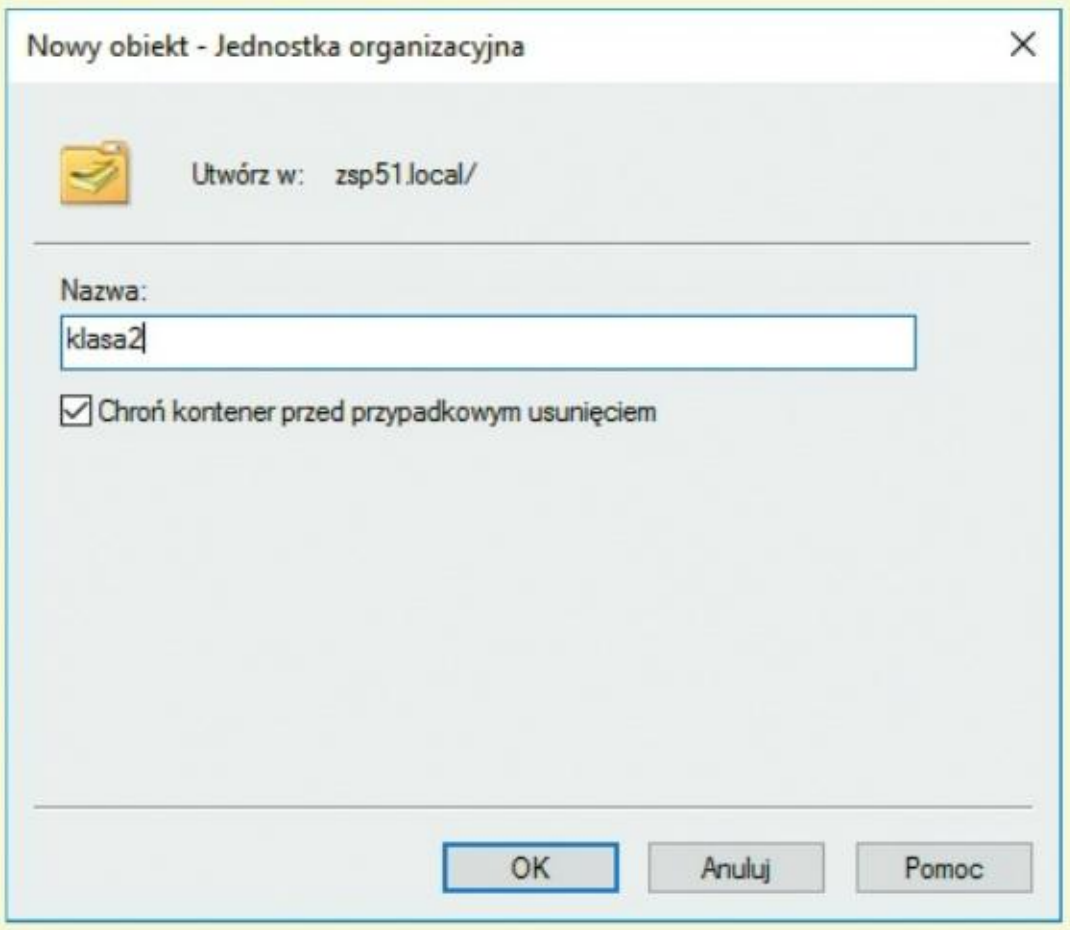
Rys. 25.10. **Wybór grupy z listy**

PRZYKŁAD 25.5

Tworzenie jednostki organizacyjnej

Jednostka organizacyjna jest kontenerem, w którym mogą być przechowywane inne obiekty, np. użytkownicy lub inne jednostki organizacyjne. Jednostki organizacyjne pozwalają na grupowanie obiektów Active Directory, np. w celu przydzielania uprawnień. Jednostkę organizacyjną można utworzyć w następujący sposób:

1. Otworzyć konsolę mmc i przystawkę **`Użytkownicy i komputery usługi Active Directory`**.
2. Kliknąć prawym przyciskiem myszy nazwę kontenera, w którym ma być utworzona jednostka, np. nazwę domeny **`zsp51.local`**.
3. Z menu kontekstowego wybrać polecenie **`Nowy/Jednostka organizacyjna`** (rys. 25.11).



Rys. 25.11. **Tworzenie jednostki organizacyjnej**

4. Usunąć zaznaczenie opcji **`Chroń kontener przed przypadkowym usunięciem`**. Ta opcja wprowadza dodatkowe zabezpieczenie kontenera. Taki kontener można usunąć, ale wymaga to dodatkowych zabiegów.
5. Po wskazaniu nazwy jednostki i kliknięciu przycisku **`OK`** zostanie ona utworzona.

25.1. Zarządzanie kontami użytkowników w konsoli tekstowej

Tworzenie i zarządzanie kontami użytkowników jest możliwe również za pomocą polecenia **`net user`** w konsoli tekstowej **`cmd.exe`**. Za jego pomocą można wyświetlać informacje o istniejących kontach, aktywować konta, tworzyć lub usuwać konta bądź resetować ich hasła. To polecenie jest bardzo często wykorzystywane w skryptach, np. w celu utworzenia kont dla wszystkich uczniów w szkole. Wykonanie takiego zadania za pomocą przystawki **`Użytkownicy i komputery usługi Active Directory`** byłoby bardzo pracochłonne i podatne na błędy.

Polecenie **`net user`** ma wiele opcji i przełączników, z których najczęściej używane to:

- **`net user`** – lista kont użytkowników w systemie;
- **`net localgroup`** – lista grup użytkowników w systemie;
- **`net user`** *`nazwa_użytkownika`* **`/add`** – tworzenie konta użytkownika;

- **net user** *nazwa_użytkownika hasło_użytkownika* – ustawienie hasła użytkownika;
- **net user** *nazwa_użytkownika* **/logonpasswordchg:yes** – wymuszenie zmiany hasła użytkownika po zalogowaniu;
- **net user** *nazwa_użytkownika* **/passwordchg:no** – zablokowanie możliwości zmiany hasła użytkownika;
- **net user** *nazwa_użytkownika* **/times:{czas}** – ograniczenie czasu pracy użytkownika;
- **net user** *nazwa_użytkownika* – wyświetlenie ustawień konta użytkownika;
- **net user** *nazwa_użytkownika* **/expires:{data}** – ustawienie daty wygaśnięcia konta użytkownika;
- **net user** *nazwa_użytkownika* **/comment:"treść_komentarza"** – ustawienie komentarza dla konta użytkownika;
- **net user** *nazwa_użytkownika* **/fullname:"Pełna nazwa"** – dodanie pełnej nazwy konta użytkownika;
- **net user** *nazwa_konta* **/active:no** – dezaktywacja konta użytkownika;
- **net localgroup** *nazwa_grupy nazwa_konta* **/add** – dodanie konta użytkownika do grupy lokalnej;
- **net user** *nazwa_konta* **/del** – usunięcie konta użytkownika.

! UWAGA

Opcja **/domain** powoduje użycie polecenia na kontrolerze bieżącej domeny.

Do zarządzania grupami globalnymi można wykorzystać polecenie **net group**. Użyte bez parametrów, wyświetla nazwy grup na serwerze. Inne opcje polecenia:

- **net group** *nazwa_grupy* – lista użytkowników w grupie;
- **net group** *nazwa_grupy* **/add** – dodaje grupę;
- **net group** *nazwa_grupy nazwa_użytkownika* **/add** – dodaje użytkownika do grupy;
- **net group** *nazwa_grupy* **/delete** – usuwa grupę;
- **net group** *nazwa_grupy nazwa_użytkownika* **/delete** – usuwa użytkownika z grupy.

PRZYKŁAD 25.6

Zarządzanie użytkownikami za pomocą polecenia net user

W tym ćwiczeniu zostaną zaprezentowane wybrane polecenia do zarządzania kontami użytkownika za pomocą polecenia **net user**. Należy:

1. Uruchomić konsolę tekstową z uprawnieniami administratora. Wybrać polecenie **Start**, w pole wyszukiwania wpisać **cmd**, a następnie kliknąć prawym klawiszem myszy **Wiersz polecenia** i wybrać **Uruchom jako administrator** (rys. 25.12).
2. Wyświetlić listę użytkowników poleceniem **net user**.
3. Utworzyć konto użytkownika *uczen11*, z hasłem *Qwerty123* za pomocą polecenia:
   net user uczen11 Qwerty123 /add /domain.
4. Wymusić zmianę hasła użytkownika po zalogowaniu za pomocą polecenia:
   net user uczen11 /logonpasswordchg:yes /domain;
5. Ustawić datę wygaśnięcia konta za pomocą polecenia:
   net user uczen11 /expires:31/12/21 /domain;

6. Ustawić czas logowania od poniedziałku (Pn) do piątku (Pt) od 8.00 do 16.00 i w soboty (So) od 8.00 do 12.00 za pomocą polecenia:

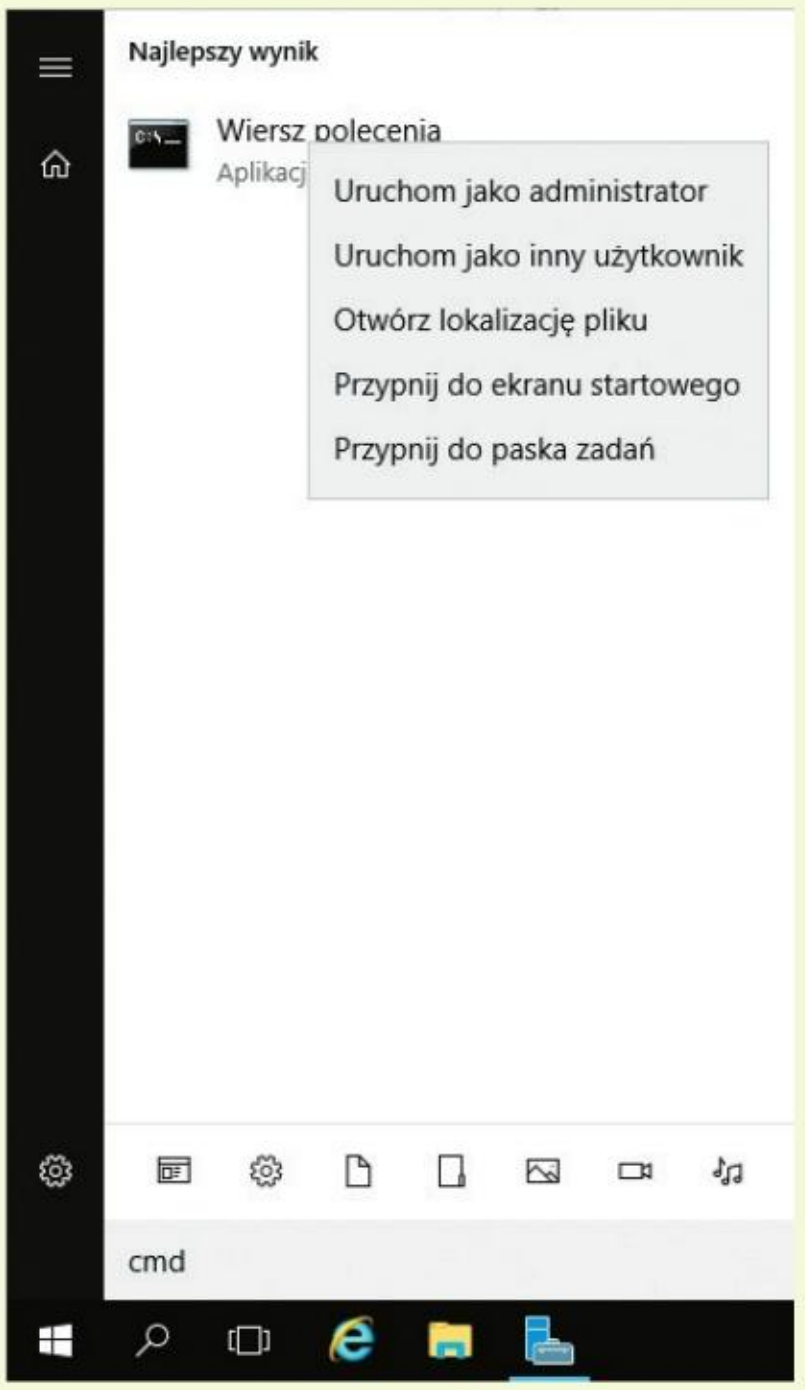
   `net user uczen11 /times: Pn-Pt,08:00-16:00;So,08:00-12:00 /domain`;

7. Dodać użytkownika *uczen11* do grupy *Administratorzy* za pomocą polecenia:

   `net localgroup Administratorzy uczen11 /add /domain`

8. Sprawdzić wprowadzone ustawienia poleceniem **`net user uczen11`** (rys. 25.13).
9. Skasować konto użytkownika *uczen11* za pomocą polecenia:

   `net user uczen11 /del`.



Rys. 25.12. Uruchomienie konsoli tekstowej z uprawnieniami administratora

```
Administrator: Wiersz polecenia

C:\Users\Administrator>net user uczen11
Nazwa użytkownika                    uczen11
Pełna nazwa
Komentarz
Komentarz użytkownika
Kod kraju/regionu                    000 (Domyślne ustawienia systemu)
Konto jest aktywne                   Tak
Wygasanie konta                      31.12.2022 00:00:00

Hasło ostatnio ustawiano             03.07.2021 15:11:18
Ważność hasła wygasa                 14.08.2021 15:11:18
Hasło może być zmieniane             04.07.2021 15:11:18
Wymagane jest hasło                  Tak
Użytkownik może zmieniać hasło       Tak

Dozwolone stacje robocze             Wszystkie
Skrypt logowania
Profil użytkownika
Katalog macierzysty
Ostatnie logowanie                   Nigdy

Dozwolone godziny logowania          Poniedzialek 08:00:00 - 16:00:00
                                     Wtorek 08:00:00 - 16:00:00
                                     Sroda 08:00:00 - 16:00:00
                                     Czwartek 08:00:00 - 16:00:00
                                     Piatek 08:00:00 - 16:00:00
                                     Sobota 08:00:00 - 12:00:00

Członkostwa grup lokalnych           *Administratorzy
Członkostwa grup globalnych          *Użytkownicy domeny
Polecenie zostało wykonane pomyślnie.


C:\Users\Administrator>
```

Rys. 25.13. Ustawienia konta użytkownika

PRZYKŁAD 25.7

KODY

Zarządzanie użytkownikami za pomocą plików wsadowych

W tym ćwiczeniu zostanie zaprezentowany plik wsadowy, który tworzy określoną liczbę kont użytkowników.

1. Utwórz plik, np. plik **konta.bat**, zawierający polecenia:

```
@echo off
echo Tworzenie kont w domenie
set /p ile="Podaj liczbe kont do utworzenia „
for /L %%X IN (1,1,%ile%) do net user uczen%X%
Qwerty123 /add /domain
net user
pause
```

Pierwsze polecenie wyłącza wyświetlanie poleceń na ekranie. W drugim poleceniu na ekranie jest wyświetlany komunikat dla użytkownika. W trzecim poleceniu użytkownik wprowadza za pomocą klawiatury liczbę kont do utworzenia. Liczba jest przechowywana w zmiennej **ile**. W pętli **for** są tworzone konta użytkowników *uczen*, począwszy od numeru 1, np. *uczen1*, *uczen2*, ..., z hasłem *Qwerty123*. Polecenie **net user** pozwala sprawdzić, czy konta zostały utworzone. Polecenie **Pause** zatrzymuje skrypt do czasu wciśnięcia dowolnego klawisza.

2. Uruchom plik. W oknie **Wiersz poleceń** (uruchomionym z uprawnieniami administratora) wybierz odpowiedni folder i wywołaj nazwę pliku. Sprawdź, czy nie pojawiły się komunikaty o błędzie.
3. Sprawdź w oknie **Użytkownicy i komputery usługi Active Directory**, czy konta zostały utworzone.

25.2. Zarządzanie kontami użytkowników w konsoli PowerShell

PowerShell jest interpretatorem poleceń podobnym do **cmd.exe**. Umożliwia wykonywanie zadań administracyjnych zarówno w lokalnych, jak i zdalnych systemach Windows. Składa się z powłoki wiersza poleceń, języka skryptów i struktury zarządzania konfiguracją. **Powłoka PowerShell** akceptuje i zwraca obiekty .NET. Zawiera następujące funkcje:

- historia wiersza poleceń;
- uzupełnianie po tabulatorach i przewidywanie poleceń;
- aliasy poleceń i parametrów;
- potok dla poleceń łańcucha;
- system pomocy podobny do stron man systemu Linux.

Język skryptowy może być używany do automatyzacji zarządzania systemami. **Skrypt PowerShell** jest zbudowany na podstawie środowiska uruchomieniowego **.NET Common Language Runtime** (CLR). Wszystkie dane wejściowe i wyjściowe są obiektami .NET.

Zarządzanie konfiguracją **PowerShell Desired State Configuration** (DSC) jest platformą zarządzania, która umożliwia zarządzanie infrastrukturą przedsiębiorstwa za pomocą konfiguracji jako kodu.

PowerShell dysponuje środowiskiem do pisania skryptów **PowerShell ISE**, w którym są dostępne narzędzia ułatwiające tworzenie skryptów, takie jak lista wszystkich **komend**, **cmdletów** (cmdlet wykonuje akcję i zwykle zwraca obiekt Microsoft .NET do następnego polecenia w potoku) wraz ze składnią.

PRZYKŁAD 25.8

Uruchomienie środowiska PowerShell

W tym ćwiczeniu zostanie zaprezentowany sposób uruchomienia i wykorzystania pomocy środowiska PowerShell. Aby uruchomić środowisko PowerShell, należy:

1. Wybrać polecenie **`Start`**, w pole wyszukiwania wpisać **`powershell`**, a następnie kliknąć prawym klawiszem myszy **`Windows PowerShell`**.
2. Aby uzyskać pomoc, można wprowadzić polecenie **`get-help <warunki poszukiwania>`**, np. **`get-help user`** wyświetli pomoc dotyczącą użytkowników (rys. 25.14).

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> get-help user

Name                                Category  Module                    Synopsis
----                                --------  ------                    --------
New-ADUser                          Cmdlet    ActiveDirectory           New-ADUser...
Get-ADUser                          Cmdlet    ActiveDirectory           Get-ADUser...
Remove-ADUser                       Cmdlet    ActiveDirectory           Remove-ADUser...
Get-ADUserResultantPasswordPolicy   Cmdlet    ActiveDirectory           Get-ADUserResultantPasswordPolicy...
Set-ADUser                          Cmdlet    ActiveDirectory           Set-ADUser...
Set-WinUserLanguageList             Cmdlet    International             Set-WinUserLanguageList...
New-WinUserLanguageList             Cmdlet    International             New-WinUserLanguageList...
Get-WinUserLanguageList             Cmdlet    International             Get-WinUserLanguageList...
New-LocalUser                       Cmdlet    Microsoft.PowerShell.L... New-LocalUser...
Rename-LocalUser                    Cmdlet    Microsoft.PowerShell.L... Rename-LocalUser...
Enable-LocalUser                    Cmdlet    Microsoft.PowerShell.L... Enable-LocalUser...
Remove-LocalUser                    Cmdlet    Microsoft.PowerShell.L... Remove-LocalUser...
Set-LocalUser                       Cmdlet    Microsoft.PowerShell.L... Set-LocalUser...
Disable-LocalUser                   Cmdlet    Microsoft.PowerShell.L... Disable-LocalUser...
Get-LocalUser                       Cmdlet    Microsoft.PowerShell.L... Get-LocalUser...
Set-PcsvDeviceUserPassword          Function  PcsvDevice                 ...
Invoke-RDUserLogoff                 Function  RemoteDesktop              ...
Disconnect-RDUser                   Function  RemoteDesktop              ...
Send-RDUserMessage                  Function  RemoteDesktop              ...
Get-RDUserSession                   Function  RemoteDesktop              ...
Enable-ServerManagerStandardUs...   Function  ServerManager              ...
Disable-ServerManagerStandardU...   Function  ServerManager              ...
Restore-UevUserSetting              Cmdlet    UEV                       Restore-UevUserSetting...
Get-UalUserAccess                   Function  UserAccessLogging          ...
Get-UalServerUser                   Function  UserAccessLogging          ...
Get-UalDailyUserAccess              Function  UserAccessLogging          ...

PS C:\Users\Administrator> _
```

Rys. 25.14. **Uzyskiwanie pomocy w PowerShell**

3. Aby uzyskać pomoc dotyczącą polecenia **`New-ADUser`** wraz z przykładami zastosowania, można wprowadzić polecenie **`get-help New-ADUser -examples`** (rys. 25.15).

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> get-help new-aduser -examples

NAME
    New-ADUser

SYNOPSIS
    Creates a new Active Directory user.


    -------------------------- EXAMPLE 1 --------------------------

    C:\PS>New-ADUser GlenJohn -Certificate (new-object System.Security.Cryptography.X509Certificates.X509Certificate -A
    rgumentList "export.cer")

    Description

    -----------

    Create a new user named 'GlenJohn' with a certicate imported from the file "export.cer".
    -------------------------- EXAMPLE 2 --------------------------

    C:\PS>New-ADUser GlenJohn -OtherAttributes @{title="director";mail="glenjohn@fabrikam.com"}

    Description

    -----------

    Create a new user named 'GlenJohn' and set the title and mail properties on the new object.
    -------------------------- EXAMPLE 3 --------------------------

    C:\PS>New-ADUser GlenJohn -Type iNetOrgPerson -Path "DC=AppNC" -server lds.Fabrikam.com:50000

    Description

    -----------

    Create a new inetOrgPerson named 'GlenJohn' on an AD LDS instance.


PS C:\Users\Administrator>
```

Rys. 25.15. **Pomoc w PowerShell z przykładami użycia polecenia**

PRZYKŁAD 25.9

Uruchomienie skryptu w środowisku PowerShell ISE

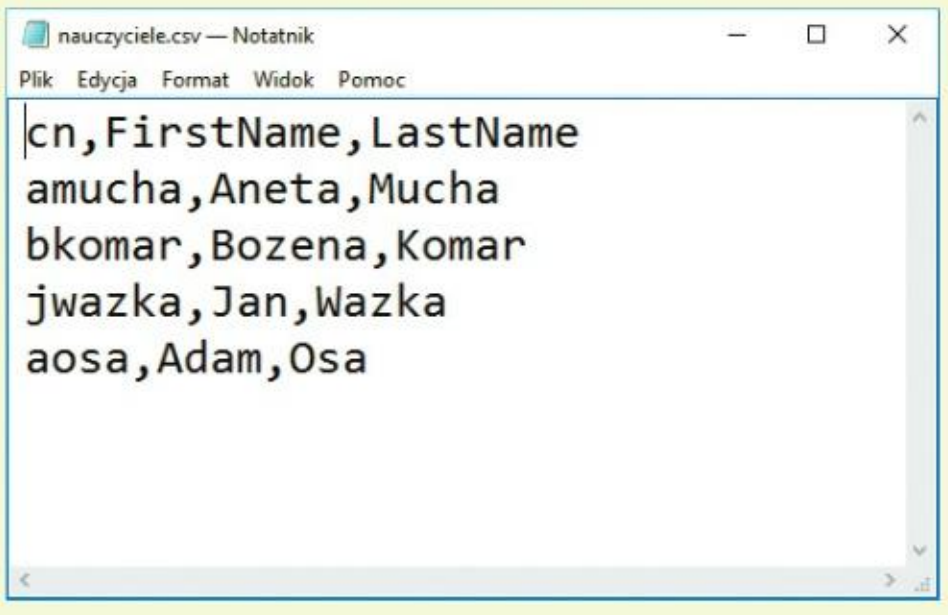
W tym ćwiczeniu zostanie zaprezentowany sposób uruchomienia skryptu w środowisku PowerShell ISE. Aby uruchomić środowisko PowerShell ISE, należy:

1. Wybrać polecenie **Start**, w pole wyszukiwania wpisać **powershell**, a następnie kliknąć prawym klawiszem myszy **Windows PowerShell ISE**.
2. W oknie edycji utworzyć skrypt tworzący konta użytkowników na podstawie danych pobieranych z pliku. W skrypcie są: określona ścieżka do jednostki organizacyjnej, w której będą tworzone obiekty, i nazwa pliku zawierającego dane tworzonych kont. Dla każdego wiersza z pliku zostaje utworzone nowe konto z hasłem *Qwerty123*.

```
$objOU=[ADSI]"LDAP://OU=ZSP,DC=zsp51,DC=local"
$dataSource=import-csv "nauczyciele.csv"
foreach($dataRecord in $dataSource){
  $cn=$dataRecord.cn
  $sAMAccountName=$dataRecord.cn
  $givenName=$dataRecord.FirstName
  $sn=$dataRecord.LastName
  $displayName=$sn + ", " + $givenName
  $userPrincipalName=$cn + "@zsp51.local"
#-----------------------------------------
$objUser=$objOU.Create("user","CN="+$cn)
$objUser.Put("sAMAccountName",$sAMAccountName)
$objUser.Put("userPrincipalName",$userPrincipalName)
$objUser.Put("displayName",$displayName)
$objUser.Put("givenName",$givenName)
$objUser.Put("sn",$sn)
#-----------------------------------------
$objUser.SetInfo()
$objUser.SetPassword("Qwerty123")
$objUser.psbase.InvokeSet("AccountDisabled",$false)
$objUser.Put("pwdLastSet",0)
$objUser.SetInfo()
}
```

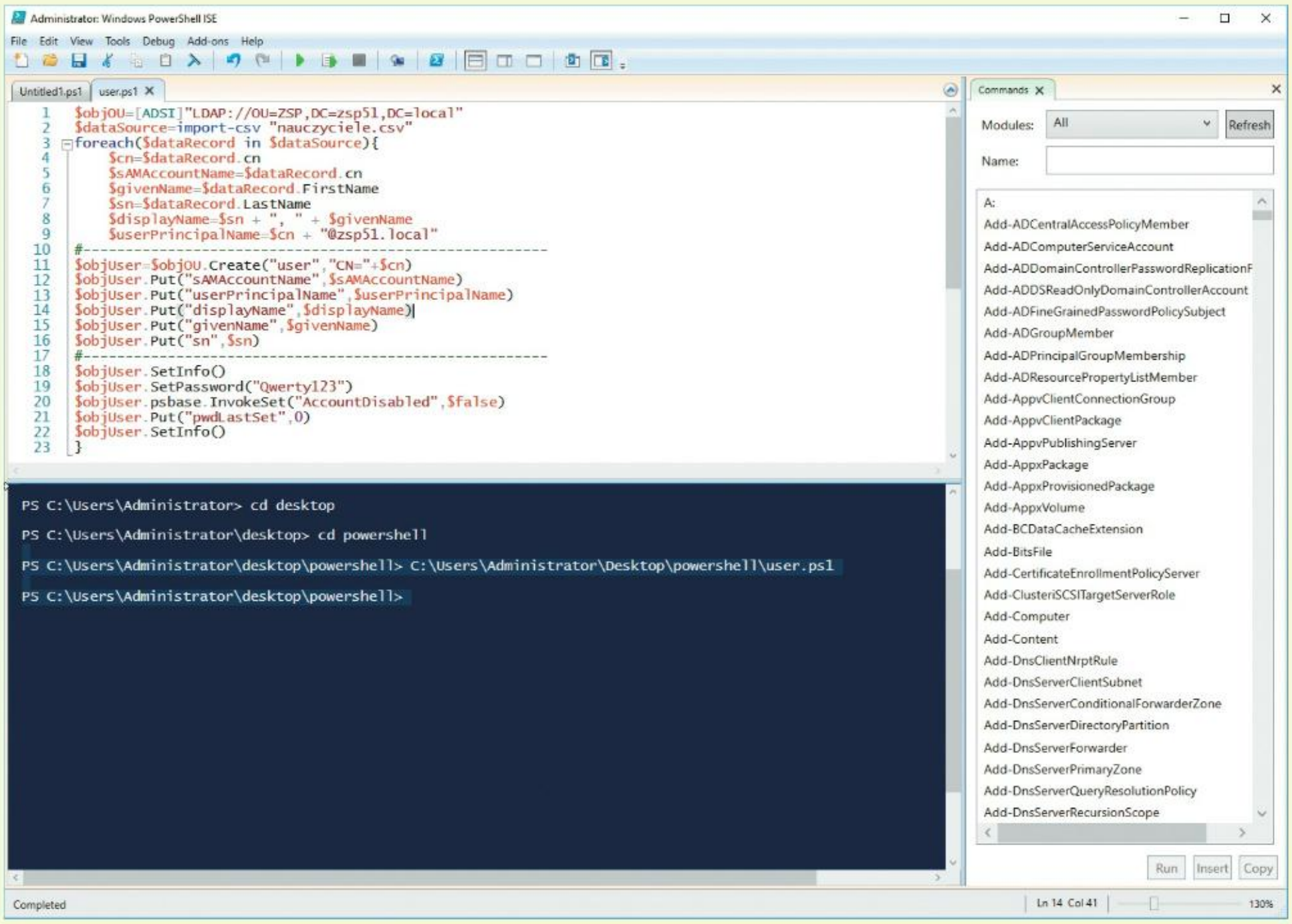
3. Utworzyć plik z danymi tworzonych kont (rys. 25.16).

KODY



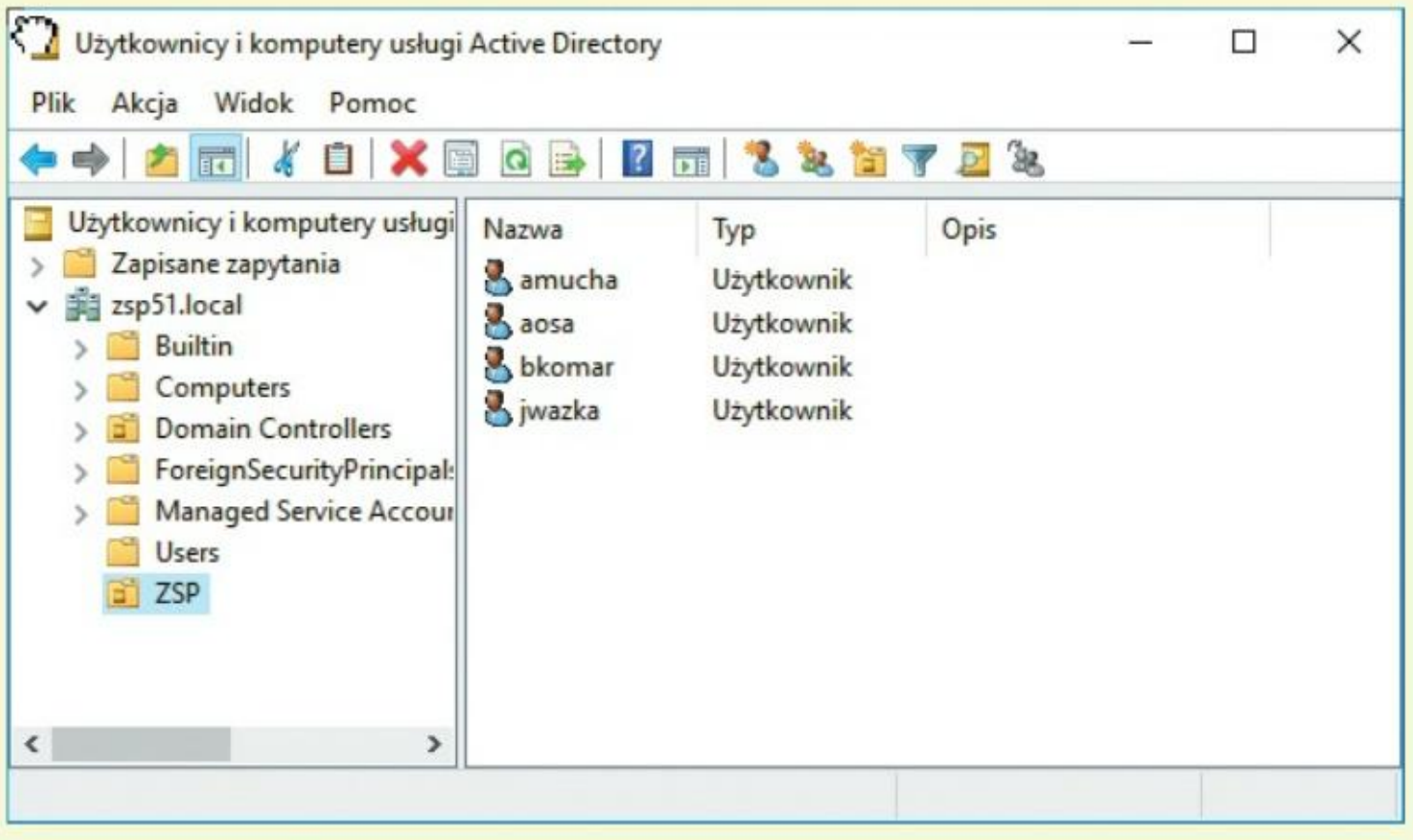
Rys. 25.16. **Plik z danymi tworzonych kont**

4. W oknie konsoli ustawić ścieżkę dostępu do folderu zawierającego skrypt, np. za pomocą polecenia **`cd Desktop\powershell`**.
5. Uruchomić skrypt przyciskiem **`Run Script`** lub nacisnąć klawisz [F5] (rys. 25.17).



Rys. 25.17. **Uruchomienie skryptu w PowerShell ISE**

6. Sprawdzić w oknie **`Użytkownicy i komputery usługi Active Directory`**, czy konta zostały utworzone (rys. 25.18).



Rys. 25.18. **Sprawdzanie, czy konta zostały utworzone**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Klasy 2 i 3 technikum informatycznego zostaną podzielone na dwie grupy: *grupa1* i *grupa2*. Do każdej z grup powinno należeć co najmniej pięciu uczniów. Konta uczniów z każdej grupy trzeba umieścić w oddzielnych jednostkach organizacyjnych. Nauczyciele muszą mieć własne grupę i jednostkę organizacyjną.
   - Zaplanuj system nazw używany w domenie.
   - Utwórz odpowiednie jednostki organizacyjne.
   - Utwórz grupy globalne i konta użytkowników oraz przypisz do nich uczniów i nauczycieli.
   - Ogranicz możliwość logowania dla uczniów tylko do czasu, kiedy odbywają się zajęcia w szkole.
   - Przydziel nauczycielom prawo logowania się tylko z własnego komputera (na podstawie adresu IP).
2. Zmodyfikuj plik z przykładu 25.7 tak, aby użytkownicy musieli zmienić hasło podczas pierwszego logowania.
3. Napisz plik wsadowy, który skasuje konta utworzone w przykładzie 25.7.
4. Klasy 2 i 3 technikum informatycznego zostaną podzielone na dwie grupy: *grupa1* i *grupa2*. Nauczyciele muszą mieć własną grupę. Do każdej z grup powinno należeć co najmniej dziesięciu uczniów lub nauczycieli. Utwórz plik wsadowy tworzący strukturę kont.
5. Przeanalizuj skrypt z przykładu 25.9 i wyjaśnij, korzystając z pomocy PowerShell, znaczenie poszczególnych komend.

26 Uprawnienia w systemie Windows

ZAGADNIENIA

Rodzaje uprawnień występujące w systemie Windows **Zarządzanie uprawnieniami do folderu** **Zarządzanie uprawnieniami specjalnymi do folderu** **Dziedziczenie uprawnień**

Z każdym kontem są związane pewne **prawa** i **przywileje**, na których podstawie system podejmuje decyzję, czy zezwolić na wykonanie czynności, czy też zabronić jej wykonywania. Każdy użytkownik ma swój unikatowy **identyfikator** (SID), który jest tworzony w momencie zakładania konta. Na podstawie **SID** (a nie nazwy logowania) są identyfikowani użytkownik i jego prawa.

Ogólnie możliwości związane z kontem można podzielić na:

- **przywileje** – uprawnienia pozwalające na wykonanie określonych zadań administracyjnych, np. dodawanie stacji roboczych do domeny;
- **prawa logowania** – pozwalają użytkownikowi na zalogowanie się do systemu, np. prawo do logowania lokalnego;
- **uprawnienia wbudowane** – wstępnie zdefiniowane uprawnienia, przypisane grupom. Nie można ich zmieniać, można przekazać innym użytkownikom, dołączając ich do grupy mającej uprawnienie, np. prawo do tworzenia nowych kont;
- **prawa dostępu** – definiują operacje, które mogą być wykonane na zasobach sieciowych, np. prawo do tworzenia plików.

W warunkach szkolnych problem przyznania przywilejów i praw logowania będzie rozwiązany przez dołączenie wybranych użytkowników do grup wbudowanych, mających odpowiednie uprawnienia wbudowane. Przykładowo, jeżeli użytkownik *jankowalski* powinien mieć prawo do tworzenia nowych kont sieciowych, to możemy dołączyć go do grupy *Administratorzy domeny*. W dużych sieciach, np. w firmach o skomplikowanej strukturze, mogą być tworzone nowe grupy i przyznawane bardziej szczegółowe przywileje i prawa.

W systemach z rodziny Windows Server uprawnienia zarówno na poziomie udostępniania zasobów, jak i na poziomie systemu plików NTFS opierają się na **listach kontroli dostępu** (ang. *Access Control List*, ACL). Pozwalają one na bardzo szczegółowe zdefiniowanie uprawnień do poszczególnych obiektów (np. plików, folderów, udostępnień). Na poziomie systemu plików NTFS istnieje dużo bardzo szczegółowych uprawnień, które można przypisać. Poszczególne uprawnienia będą nazywane **uprawnieniami specjalnymi** lub **zaawansowanymi**. Aby ułatwić zarządzanie uprawnieniami specjalnymi, są one łączone w grupy, które tworzą **uprawnienia**. Innymi słowy, uprawnienie składa się z wielu uprawnień specjalnych. Wykaz tych uprawnień przedstawiono w tabeli 26.1. Uprawnienia specjalne (lewa kolumna) zostają przypisane do konkretnych grup uprawnień (górny wiersz).

Tabela 26.1. Tabela uprawnień NTFS

Uprawnienia specjalne	Pełna kontrola	Modyfikacja	Odczyt i wykonanie	Wyświetlanie zawartości folderu (tylko foldery)	Odczyt	Zapis
Przechodzenie przez folder / Wykonywanie pliku	X	X	X	X		
Wyświetlanie zawartości folderu / Odczyt danych	X	X	X	X	X	
Odczyt atrybutów	X	X	X	X	X	
Odczyt atrybutów rozszerzonych	X	X	X	X	X	
Tworzenie plików / Zapis danych	X	X	X			X
Tworzenie folderów / Dołączanie danych	X	X	X			X
Zapis atrybutów	X	X	X			X
Zapis atrybutów rozszerzonych	X	X	X			X
Usuwanie podfolderów i plików	X					
Usuwanie	X	X				
Odczyt uprawnień	X	X	X	X	X	X
Zmiana uprawnień	X					
Przejęcie na własność	X					

Uprawnienia można **nadawać** – **Zezwalaj** (ang. *Allow*) lub **odbierać** – **Odmów** (ang. *Deny*). Zaznaczenie pola **Zezwalaj** nadaje użytkownikowi (grupie) dane uprawnienia (rys. 26.1). Uprawnienia każdego użytkownika do danego obiektu są sumą uprawnień wynikających z praw, jakie ma dany użytkownik, i wynikających z praw, jakie mają grupy, do których on przynależy. Zaznaczenie **Odmawiaj** ma zastosowanie wtedy, gdy chcemy zabrać użytkownikowi prawo do danego obiektu, mimo posiadania przez niego praw wynikających z jego przynależności do danej grupy użytkowników. Odmowa uprawnienia jest ważniejsza niż zezwolenie. Stosujemy ją, gdy chcemy stworzyć wyjątek. Załóżmy, że *jankowalski* jest członkiem grupy *uczniowie*. Jeżeli nadamy uprawnienie (Zezwalaj) do folderu grupie *uczniowie*, to z powodu przynależności do

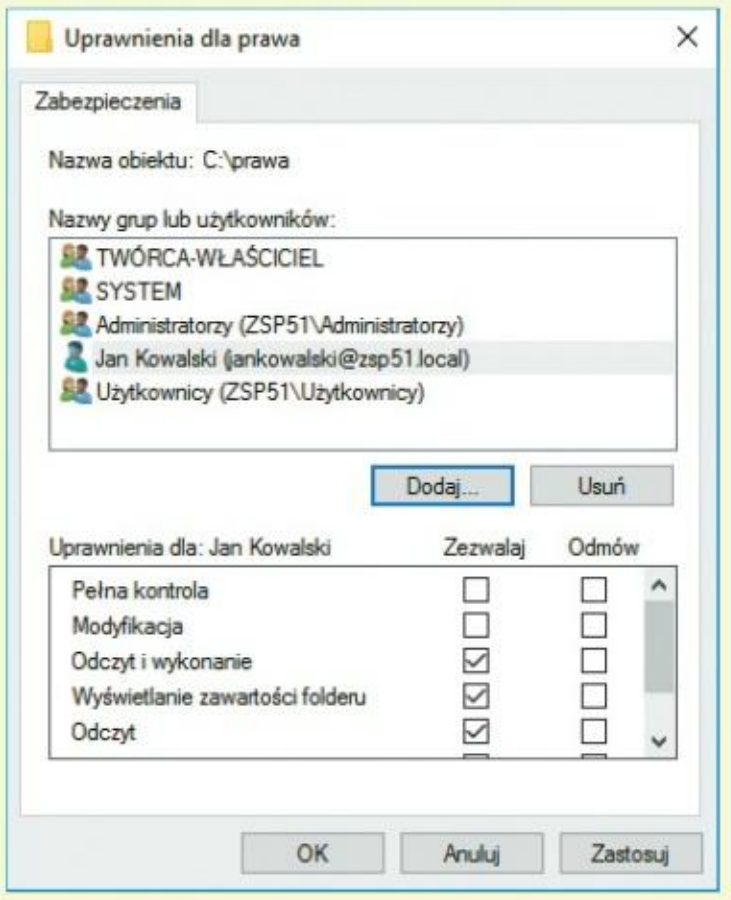
niej otrzyma uprawnienie również *jankowalski*. Jeżeli odmówimy uprawnienia (Odmów) użytkownikowi *jankowalski*, to nie będzie on miał uprawnienia, mimo że powinien je mieć z racji przynależności do grupy *uczniowie*.

PRZYKŁAD 26.1

Zarządzanie uprawnieniami do folderu

Aby zmieniać lub przeglądać uprawnienia do folderu, należy:

1. Kliknąć prawym przyciskiem myszy folder, którego uprawnienia będą modyfikowane, i z menu kontekstowego wybrać **Właściwości**, a następnie zakładkę **Zabezpieczenia**.
2. Kliknąć przycisk **Edytuj**, a następnie przycisk **Dodaj**, aby dodać użytkownika lub grupę do listy uprawnionych (jeżeli użytkownik jest na liście, wystarczy go wskazać i przejść do piątego punktu).
3. Wprowadzić nazwę użytkownika, który ma być dodany do listy uprawnionych.
4. Wskazać kursorem użytkownika, którego uprawnienia będą modyfikowane.
5. Zaznaczyć uprawnienia (**Zezwalaj** lub **Odmów**), które mają być zmodyfikowane, i kliknąć przycisk **Zastosuj**.



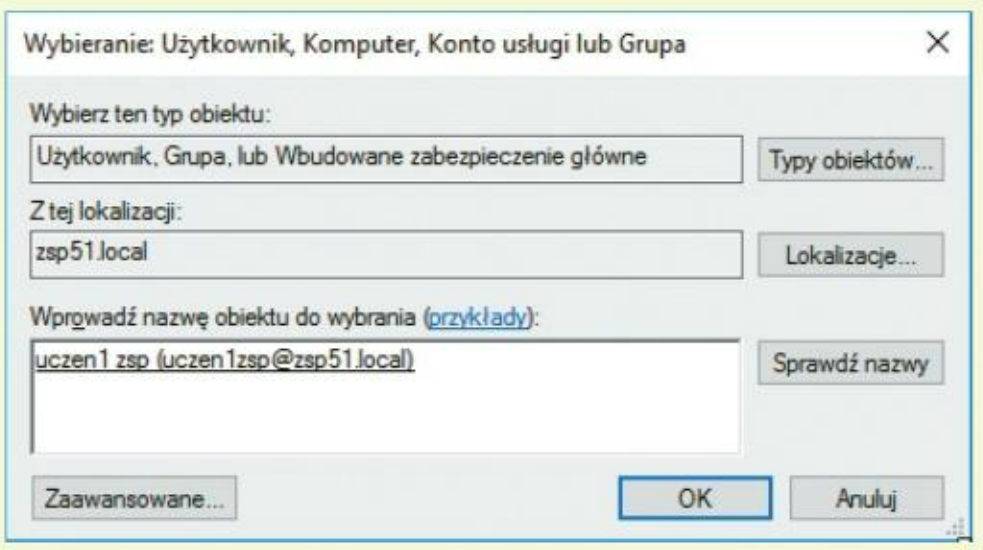
Rys. 26.1. **Uprawnienia użytkownika do folderu**

PRZYKŁAD 26.2

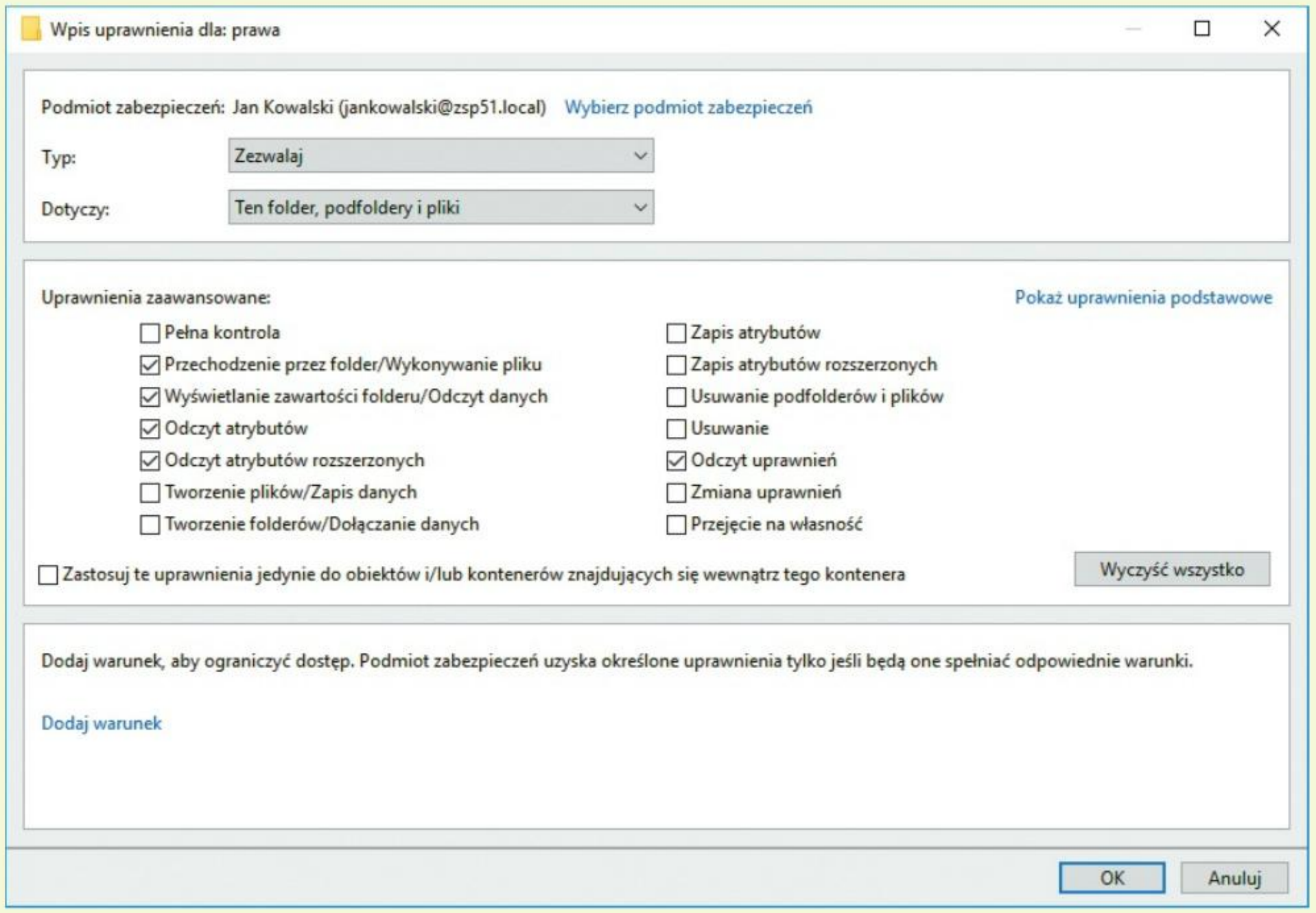
Zarządzanie uprawnieniami specjalnymi do folderu

Aby zmienić lub przeglądać uprawnienia specjalne do folderu, należy:

1. Kliknąć prawym przyciskiem myszy folder, którego uprawnienia będą modyfikowane, i z menu kontekstowego wybrać **Właściwości**, a następnie zakładkę **Zabezpieczenia**.
2. Kliknąć przycisk **Zaawansowane**.
3. W zakładce **Uprawnienia**, jeżeli użytkownik jest na liście, to wystarczy go wskazać i przejść do punktu 5.
4. Kliknąć przycisk **Dodaj**. Kliknąć odnośnik **Wybierz podmiot zabezpieczeń** i wprowadzić nazwę użytkownika, który ma być dodany do listy uprawnionych (rys. 26.2). Kliknąć przycisk **OK**.
5. Wskazać myszą użytkownika, którego uprawnienia będą modyfikowane, i kliknąć przycisk **Edytuj**.
6. Kliknąć odnośnik **Pokaż uprawnienia zaawansowane**.
7. W polu **Typ** wskazać typ uprawnień (**Zezwalaj** lub **Odmów**), które mają być zmodyfikowane, i kliknąć przycisk **OK** (rys. 26.3).



Rys. 26.2. **Wybór podmiotu zabezpieczeń**

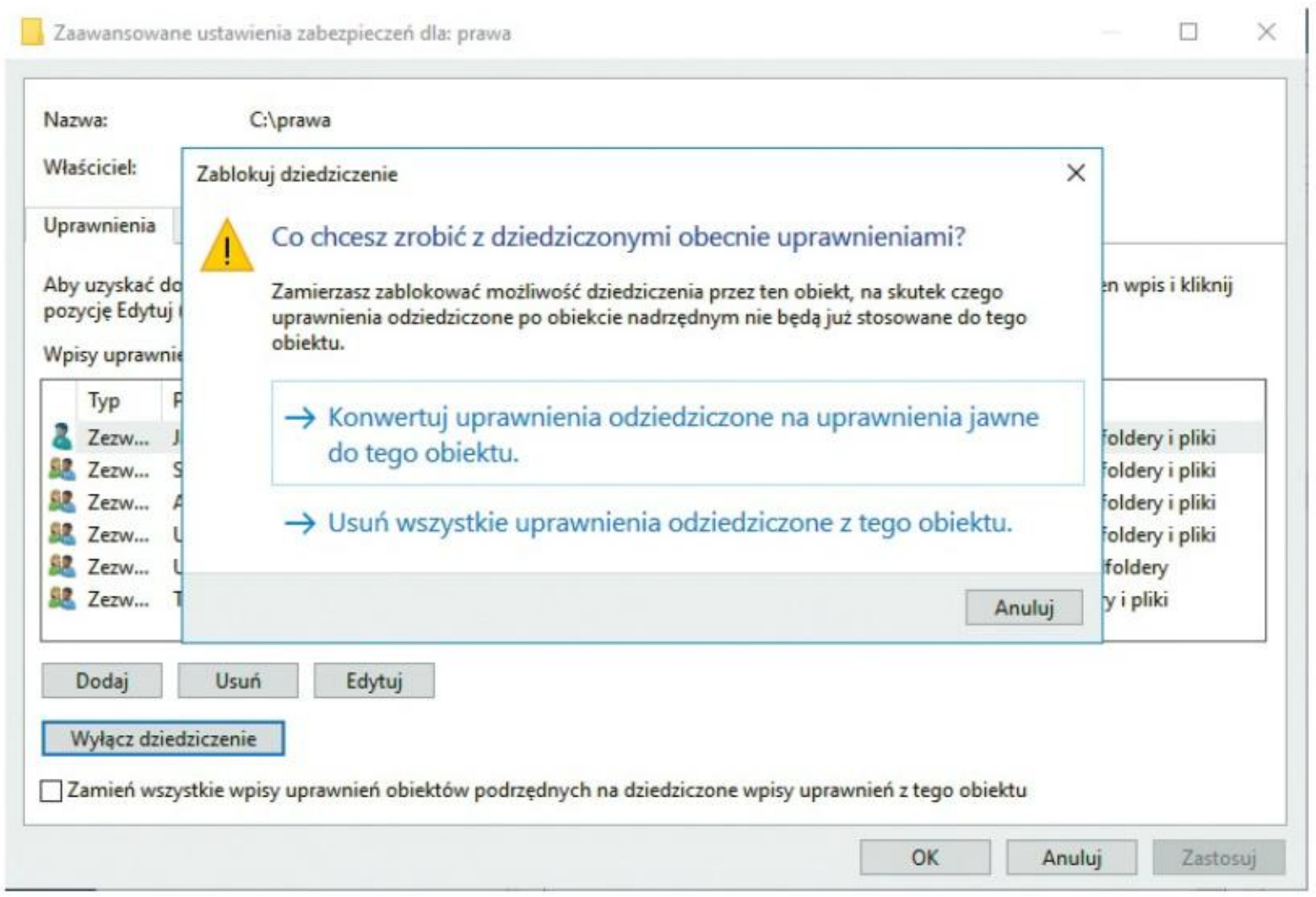


Rys. 26.3. **Uprawnienia zaawansowane użytkownika do folderu**

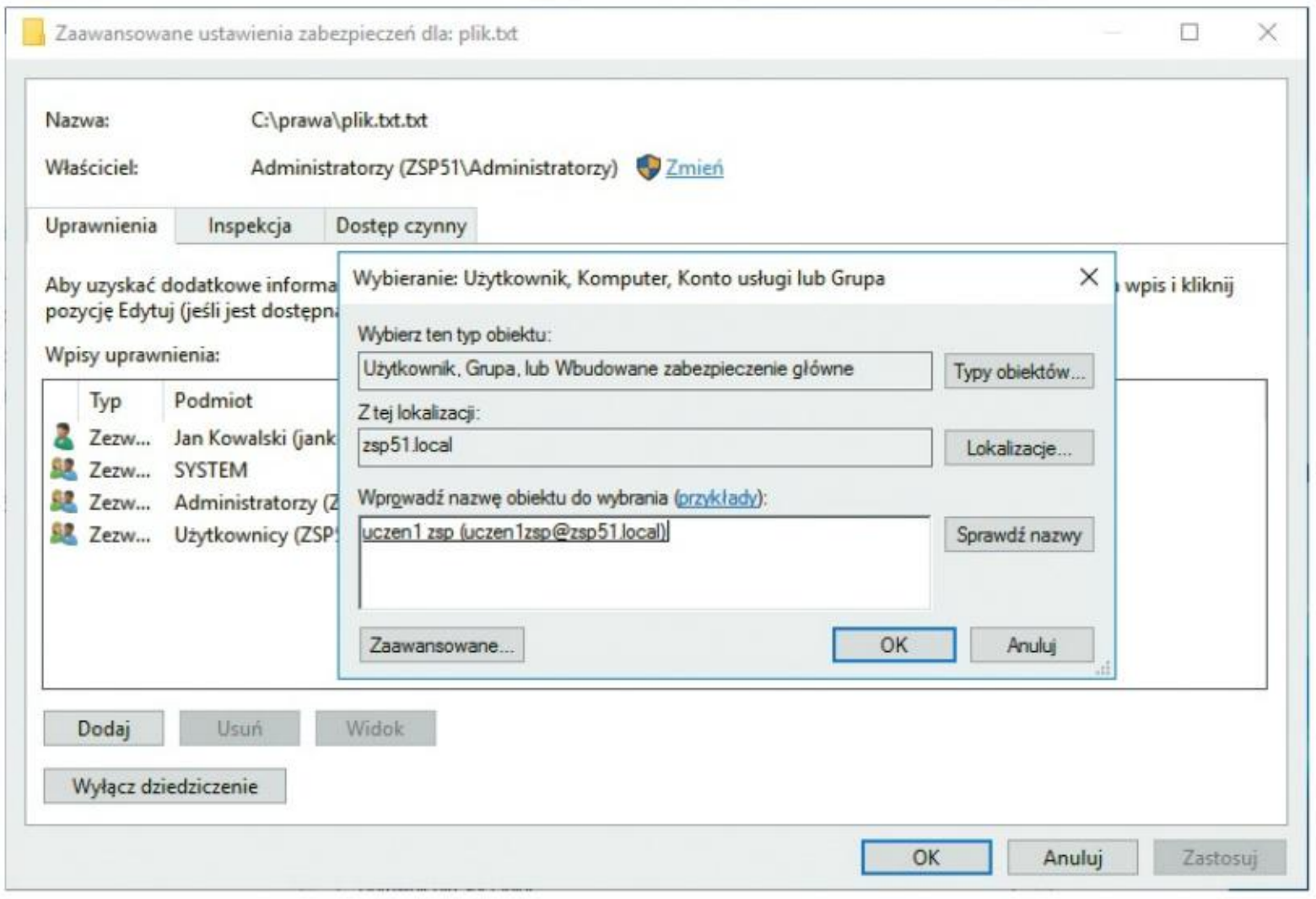
Jedną z ważniejszych zalet mechanizmu uprawnień jest możliwość dziedziczenia uprawnień. **Dziedziczenie** uprawnień pozwala na to, aby np. wszystkie pliki bądź podfoldery dziedziczyły uprawnienia z folderu nadrzędnego. Jeśli podczas przeglądania uprawnień dla obiektu pola wyboru uprawnień **Zezwalaj** i **Odmów** są zacieniowane, oznacza to, że obiekt odziedziczył uprawnienia z obiektu nadrzędnego. Istnieją trzy sposoby wprowadzania zmian w uprawnieniach dziedziczonych:

- **jawne wprowadzenie zmian w obiekcie nadrzędnym** – obiekt podrzędny odziedziczy zmienione uprawnienia;
- **jawne wprowadzenie zmian w obiekcie**, np. zaznaczenie uprawnienia **Zezwalaj**, aby zastąpić dziedziczone uprawnienie **Odmów**;
- **wyłączenie dziedziczenia** – kliknąć przycisk **Wyłącz dziedziczenie** i wybrać sposób postępowania z dziedziczonymi obecnie uprawnieniami (rys. 26.4). Następnie wprowadzić zmiany w uprawnieniach – obiekt nie będzie już dziedziczyć uprawnień po obiekcie nadrzędnym. Kliknąć przycisk **OK**.

Każdy obiekt, np. plik, ma swojego **właściciela**. Domyślnie jest nim ten, kto obiekt stworzył. Bez względu na uprawnienia właściciel zawsze może zmienić prawa ustawione dla swojego obiektu, a w szczególności zabrać sobie samemu prawa do niego. Wtedy nie ma możliwości np. odczytania danego pliku, jeżeli wcześniej nie przywróci sobie praw. Zmiany właściciela pliku można dokonać w oknie **Zaawansowane ustawienia zabezpieczeń** (rys. 26.5). Należy kliknąć odnośnik **Zmień** i wskazać nowego właściciela.



Rys. 26.4. Wyłączanie dziedziczenia uprawnień



Rys. 26.5. Zmiana właściciela pliku

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wymień rodzaje uprawnień występujących w systemie Windows.
2. Co to są uprawnienia specjalne do folderu? Jak nimi zarządzać?
3. Wypisz uprawnienia specjalne, które składają się na prawo zapisywania w folderze.
4. Na czym polega mechanizm dziedziczenia uprawnień? Podaj przykłady.
5. Do czego służy odmowa uprawnienia (**Odmów**)? Podaj przykłady wykorzystania.

27 Udostępnianie zasobów i przypisywanie uprawnień do udostępnianych zasobów

ZAGADNIENIA

Uprawnienia nadawane do udostępnianych zasobów **Udostępnianie folderów i przypisywanie do nich uprawnień**

Jeśli udostępniamy zasób w sieci, możemy każdemu użytkownikowi lub grupie przydzielić uprawnienia:

- **pełna kontrola** – użytkownik ma pełne prawa; może tworzyć nowe pliki, odczytywać, modyfikować, zapisywać i usuwać już istniejące oraz zmieniać uprawnienia i przejmować je na własność;
- **zmiana** – użytkownik ma te same uprawnienia co pełna kontrola poza prawem do zmiany uprawnień i przejmowania na własność, czyli może tworzyć nowe pliki, odczytywać, modyfikować, zapisywać i usuwać już istniejące;
- **odczyt** – użytkownik ma prawo do odczytywania plików (w tym ich uruchamiania), nie może tworzyć nowych plików i usuwać ani modyfikować już istniejących.

Uprawnienia do udostępnionego zasobu sieciowego, np. folderu, są wypadkową wynikającą z uprawnień nadanych na poziomie udostępniania udziału i na poziomie systemu plików NTFS. Oznacza to, że zawsze zostaną zastosowane bardziej rygorystyczne uprawnienia.

PRZYKŁAD 27.1

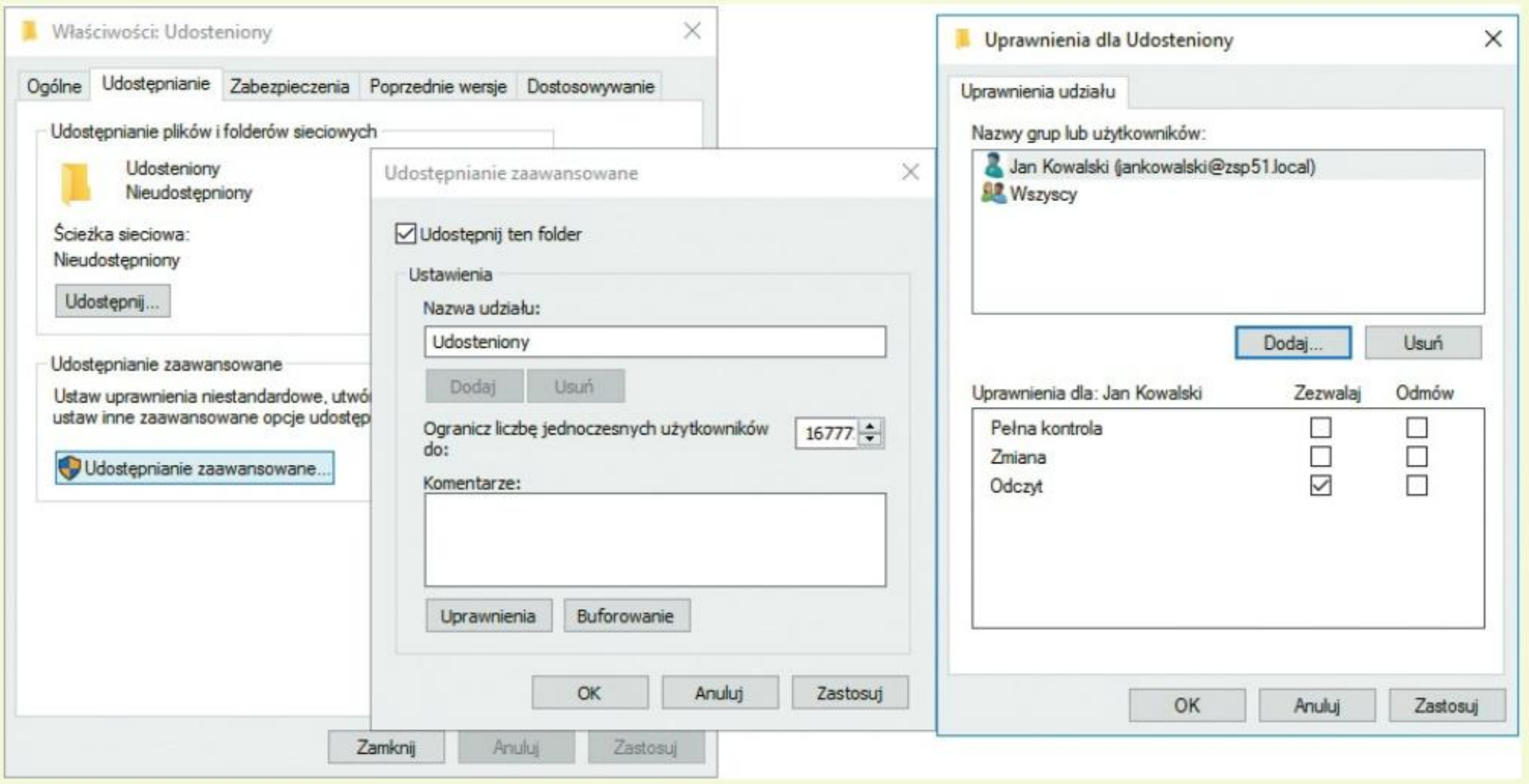
Udostępnianie folderu

Aby udostępnić folder w sieci, należy:

1. Kliknąć prawym przyciskiem myszy folder i wybrać **Właściwości**.
2. Wybrać zakładkę **Udostępnianie** i kliknąć przycisk **Udostępnianie zaawansowane**.
3. Zaznaczyć opcję **Udostępnij ten folder** i kliknąć przycisk **Uprawnienia**.
4. W oknie **Uprawnienia dla** (rys. 27.1) wskazać użytkownika (jeżeli nie ma go na liście – kliknąć przycisk **Dodaj** i dodać użytkownika do listy).
5. Zaznaczyć uprawnienia (**Zezwalaj** lub **Odmów**), które mają być zmodyfikowane, i kliknąć przycisk **OK** (rys. 27.1).

UWAGA

Nie zapomnij o nadaniu uprawnień w systemie NTFS. Jeżeli użytkownik nie otrzyma uprawnień do pliku, to pomimo udostępnienia zasobów będzie on niedostępny.



Rys. 27.1. **Uprawnienia do udostępnianego zasobu**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Utwórz folder **`Pliki`**. Udostępnij go w sieci. Przydziel uprawnienia:
   - uczniom wszystkich klas i grup – tylko możliwość odczytywania plików;
   - nauczycielom – możliwość odczytywania i zapisywania;
   - kontu nauczyciel1 – pełne prawa do folderu.

   W folderze **`Pliki`** każdy z pięciu nauczycieli ma folder prywatny, np. *nauczyciel1* – nikt poza nim nie może mieć żadnych uprawnień do tego folderu.

28 Foldery macierzyste użytkowników

ZAGADNIENIA

Funkcje folderów macierzystych użytkowników **Skonfigurowanie folderu macierzystego dla użytkownika**

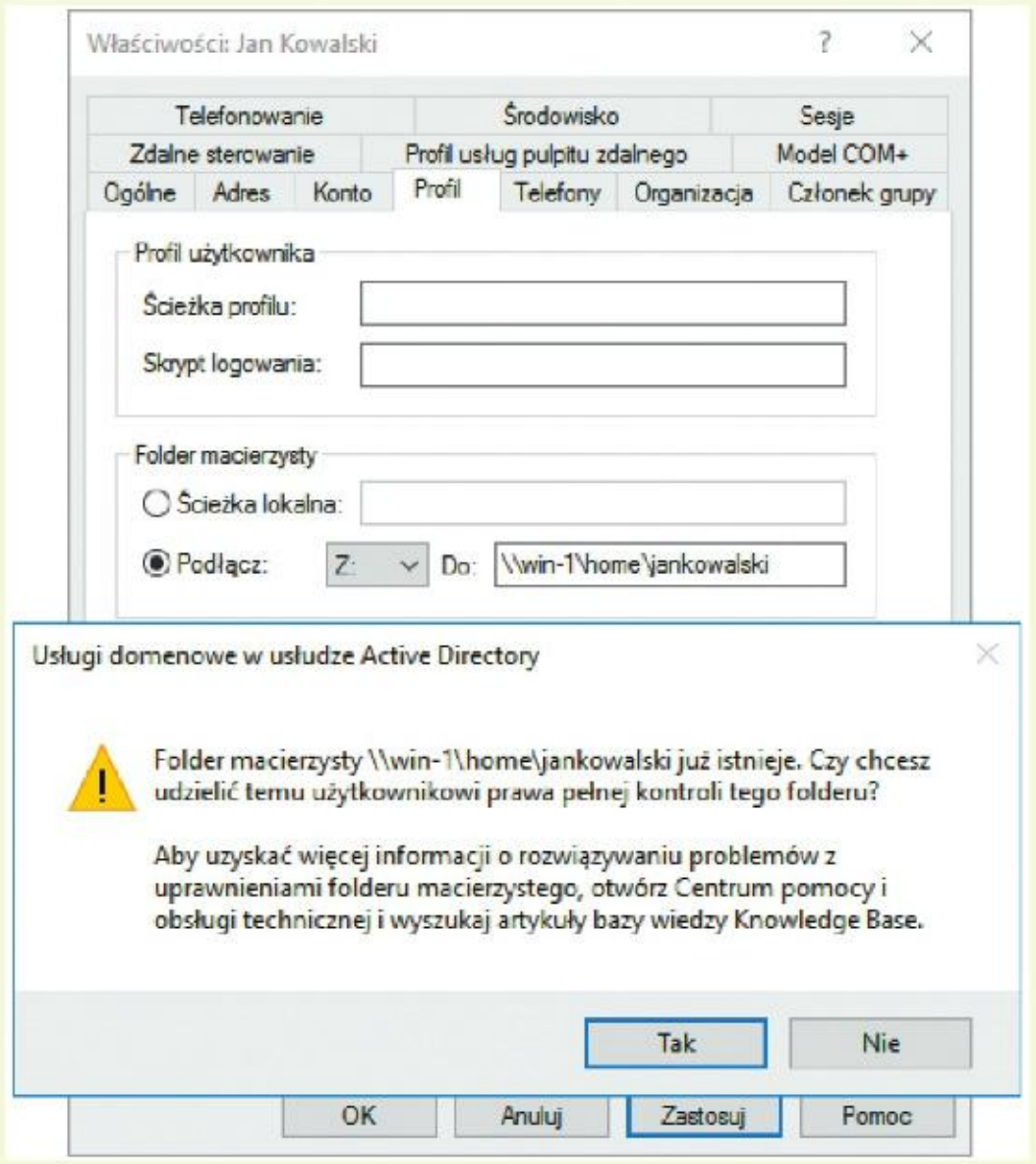
Domena umożliwia przypisywanie **folderów macierzystych** użytkownikom. Dzięki temu użytkownicy mogą korzystać z własnych dokumentów przechowywanych na serwerze z dowolnego komputera przyłączonego do domeny. Po zalogowaniu zostanie on zmapowany jako dysk sieciowy. Foldery macierzyste ułatwiają administratorowi tworzenie kopii zapasowych plików użytkowników przez zbieranie ich w jednym miejscu na serwerze.

PRZYKŁAD 28.1

Konfigurowanie folderu macierzystego użytkownika

Aby przydzielić użytkownikowi folder macierzysty, należy:

1. Na dysku serwera utworzyć folder, np. **`home`**, z przeznaczeniem na foldery macierzyste użytkowników i udostępnić go w sieci dla grupy *Wszyscy*.
2. W folderze utworzyć podfoldery o takich samych nazwach, jak użytkownicy, np. *jankowalski*.



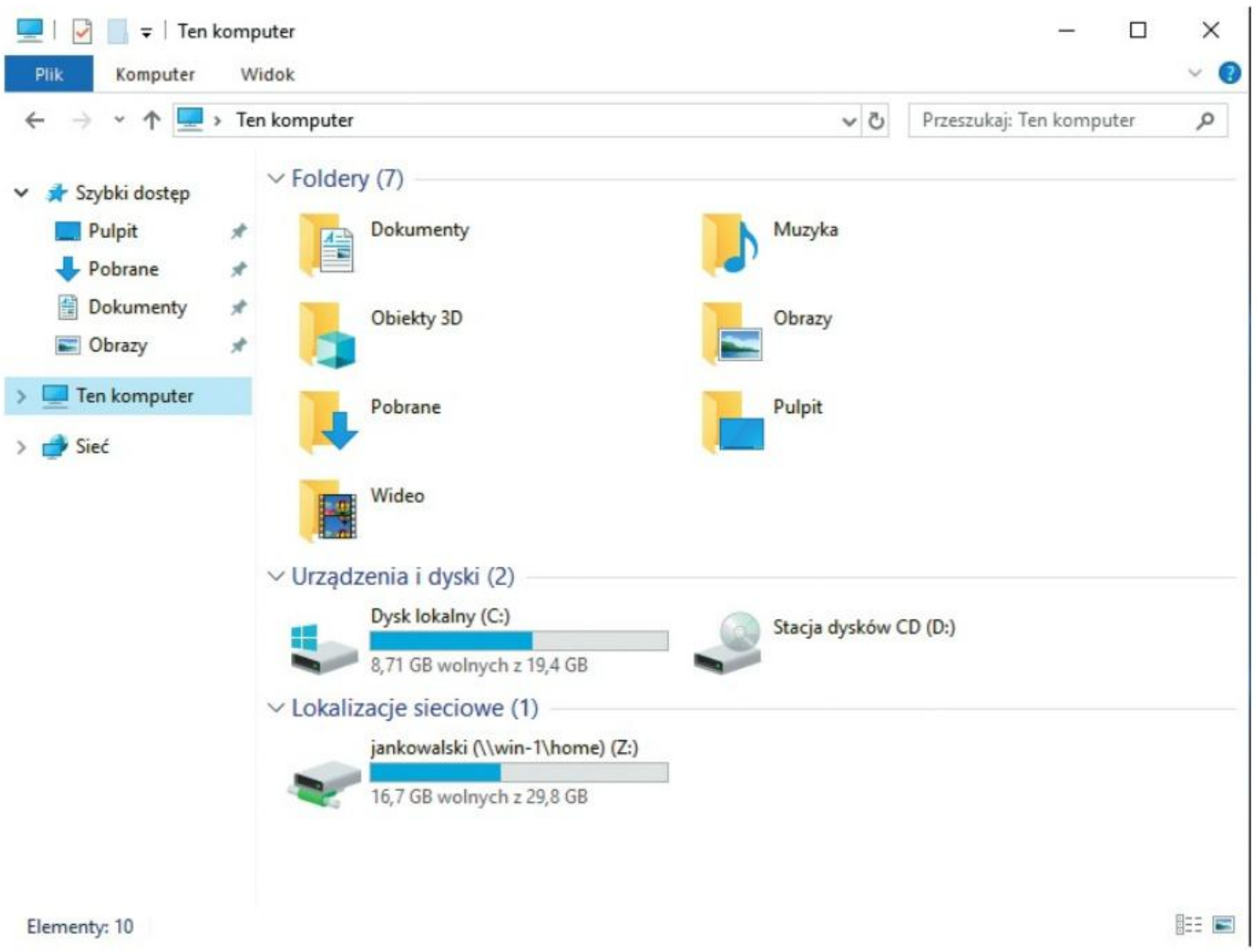
Rys. 28.1. Konfigurowanie folderu macierzystego użytkownika

3. W przystawce konsoli **Użytkownicy i komputery usługi Active Directory** kliknąć prawym przyciskiem myszy użytkownika, np. *jankowalski*, i wybrać **Właściwości**.
4. W zakładce **Profil** w polu **Podłącz** wybrać literę dysku, która posłuży do reprezentowania folderu, a w polu **Do** wpisać sieciową ścieżkę do zasobu, np. **\\WIN-1\home\%UserName%** (rys. 28.1). System zamieni parametr **%UserName%** na nazwę logowania użytkownika.

! UWAGA

Aby zapewnić bezpieczeństwo plikom użytkowników w folderze domowym, należy za pomocą uprawnień systemu plików (NTFS) ograniczyć dostęp użytkowników tylko do własnego podfolderu. W ten sposób można zabezpieczyć folder domowy przed dostępem nieupoważnionych użytkowników.

Po zalogowaniu się do domeny z dowolnego komputera użytkownik *jankowalski* będzie miał do dyspozycji dysk Z, który jest jego katalogiem macierzystym (rys. 28.2).



Rys. 28.2. Folder macierzysty użytkownika

SPRAWDŹ SWOJĄ WIEDZĘ

1. Co to jest folder macierzysty?
2. Jaka jest różnica między folderem domowym z systemu Linux a folderem macierzystym w Windows Server?

29 Profile użytkowników Windows

ZAGADNIENIA

Definicja profilu użytkownika **Funkcje profilu użytkownika** **Rodzaje profili użytkowników**

Profil użytkownika to zbiór ustawień środowiska pracy. W profilu są przechowywane informacje:

- preferencje pulpitu;
- kolory ekranu;
- menu Start;
- ustawienia programów, połączenia sieciowe, połączenia drukarek, ustawienia myszy, rozmiary i położenie okien;
- folder **`Moje dokumenty`**;
- pliki cookies.

Profil zostaje utworzony po pierwszym zalogowaniu użytkownika na komputerze. System tworzy profil użytkownika przez skopiowanie **profilu użytkownika domyślnego** (ang. *Default User*) do nowego folderu, którego nazwa jest tworzona w oparciu na nazwie logowania. Środowisko użytkownika powstaje przez połączenie informacji z **profilu ogólnego** (ang. *All Users*) z profilem użytkownika. Dzięki profilowi użytkownik może korzystać z ustawień zdefiniowanych w profilu na komputerze użytkowanym przez różne osoby lub uzyskać identyczne środowisko pracy na każdym komputerze, z którego korzysta.

Rozróżnia się następujące typy profili użytkowników:

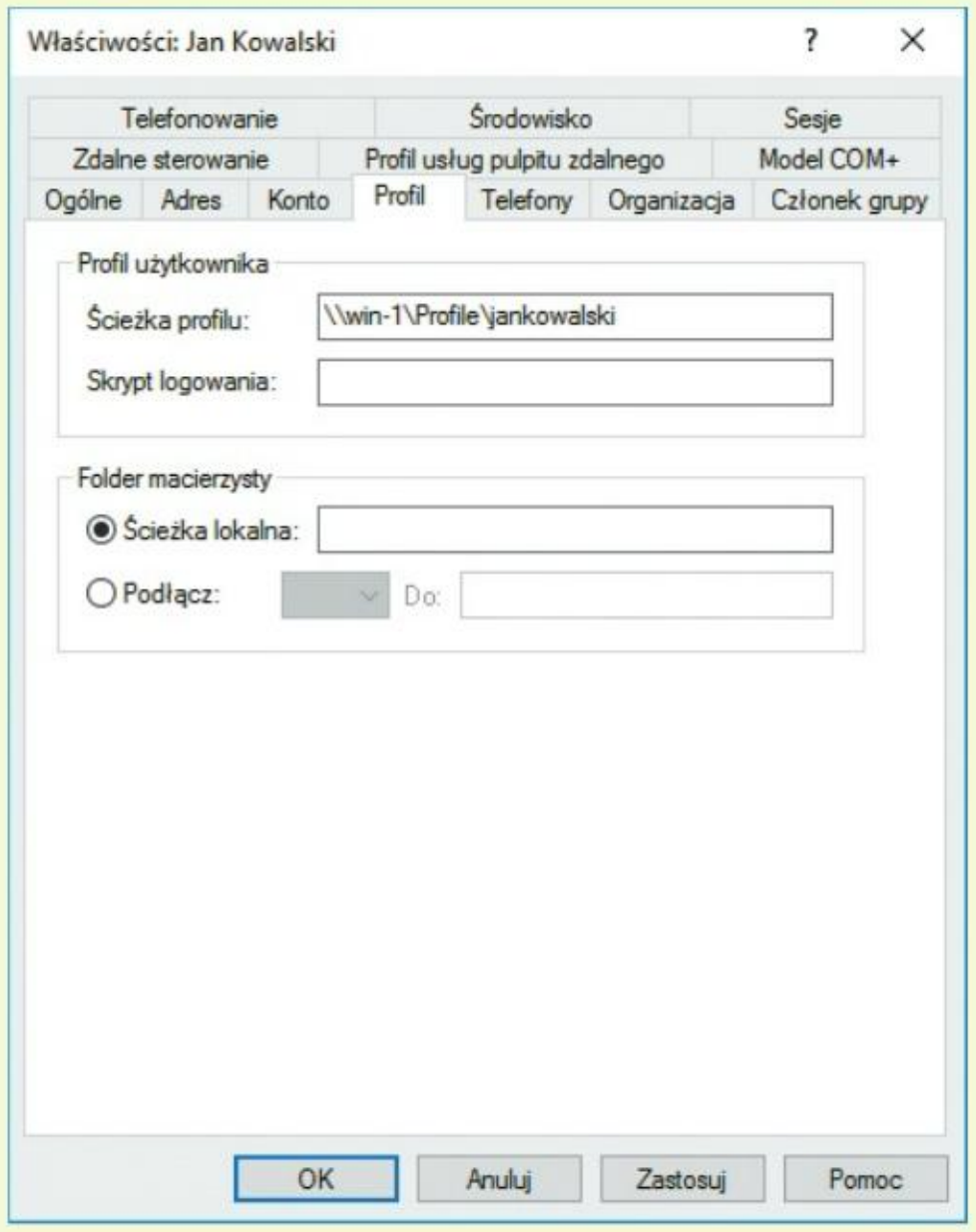
- **lokalny** – przechowywany na lokalnym dysku twardym komputera; zmiany lokalnego profilu użytkownika dotyczą tylko tego komputera;
- **mobilny** – tworzony przez administratora systemu i przechowywany na serwerze. Dostępny podczas każdego logowania na dowolnym komputerze w sieci. Gdy użytkownik loguje się do komputera na konto, dla którego został określony profil mobilny, jest on pobierany z serwera i wykorzystywany podczas pracy. W trakcie wylogowania się z komputera wszelkie zmiany w profilu zostają zapisane na serwerze w udostępnionym folderze, w którym jest przechowywany profil;
- **obowiązkowy** – profil mobilny, który może określać ustawienia dla pojedynczych użytkowników i całych grup. Zezwala na modyfikowanie środowiska profilu przez użytkownika, ale zmiany nie są zapisywane i po następnym logowaniu środowisko pracy użytkownika jest przywracane do stanu początkowego. Jest przydatny, kiedy zmiany wprowadzone przez jednego użytkownika nie powinny mieć wpływu na środowisko innych użytkowników, np. w szkole, gdy nie chcemy, aby uczniowie zmieniali pulpit;
- **tymczasowy** – używany, jeśli błąd uniemożliwia załadowanie profilu użytkownika. Te profile są usuwane, a ustawienia tracone po wylogowaniu się użytkownika.

PRZYKŁAD 29.1

Tworzenie profilu mobilnego

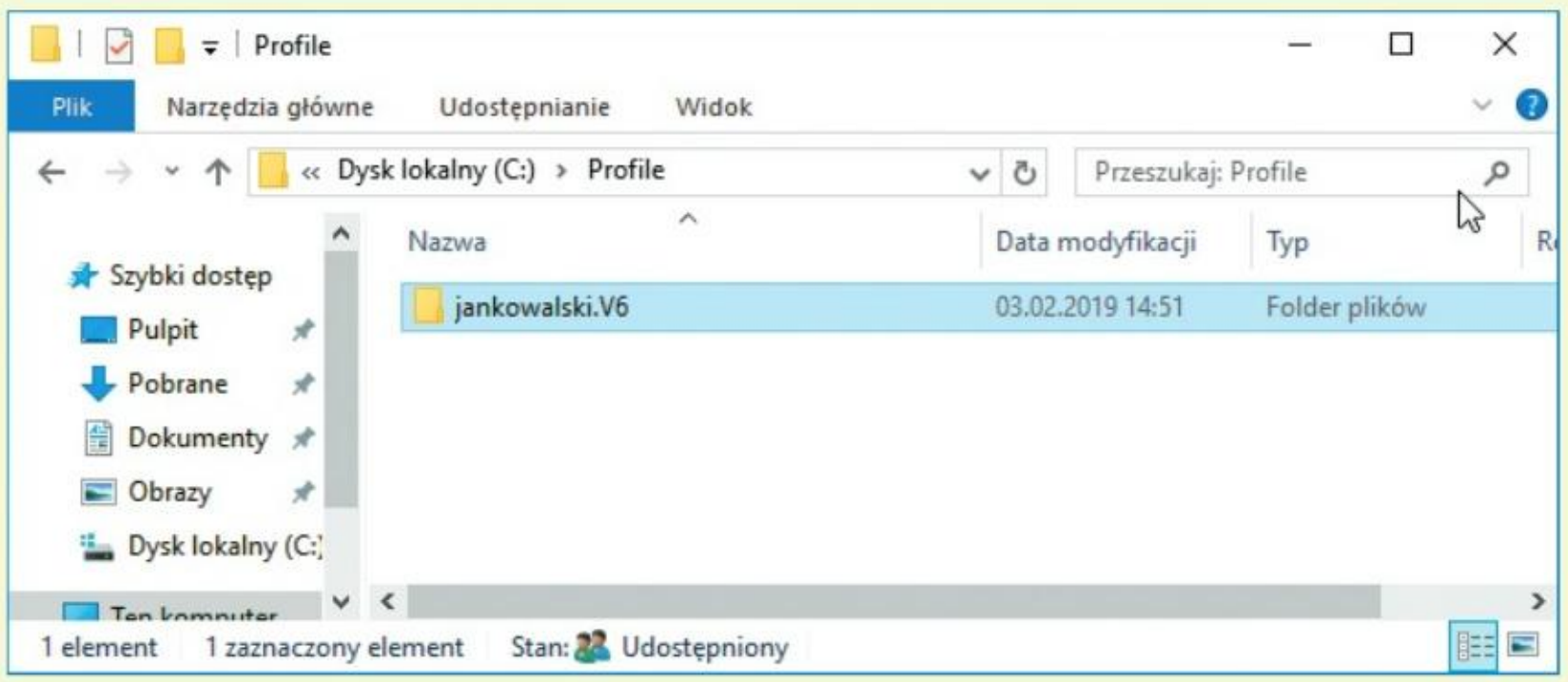
W tym ćwiczeniu zostanie skonfigurowany profil mobilny użytkownika. Profil mobilny jest przechowywany na serwerze w folderze udostępnionym dla wszystkich użytkowników. Będzie to folder najwyższego poziomu, zawierający wszystkie profile poszczególnych użytkowników. Aby utworzyć profil mobilny użytkownika, należy:

1. Utworzyć na serwerze folder, np. **`Profile`**, w którym będą przechowywane profile użytkowników.
2. Udostępnić ten folder i nadać wszystkim użytkownikom uprawnienia **`Pełna kontrola`**.
3. Otworzyć przystawkę **`Użytkownicy i komputery usługi Active Directory`**, a następnie kliknąć prawym klawiszem myszy obiekt określonego użytkownika, np. *jankowalski*, i wybrać **`Właściwości`**.
4. W zakładce **`Profil`** (rys. 29.1), w polu Ścieżka profilu wpisać ścieżkę sieciową do folderu udostępnionego, w którym będzie przechowywany profil użytkownika, np. **`\\win-1\Profile\%UserName%`**.
5. Zmienna **`%UserName%`** zostanie automatycznie zamieniona na nazwę użytkownika. We wskazanym folderze zostanie utworzony folder zawierający profil użytkownika.



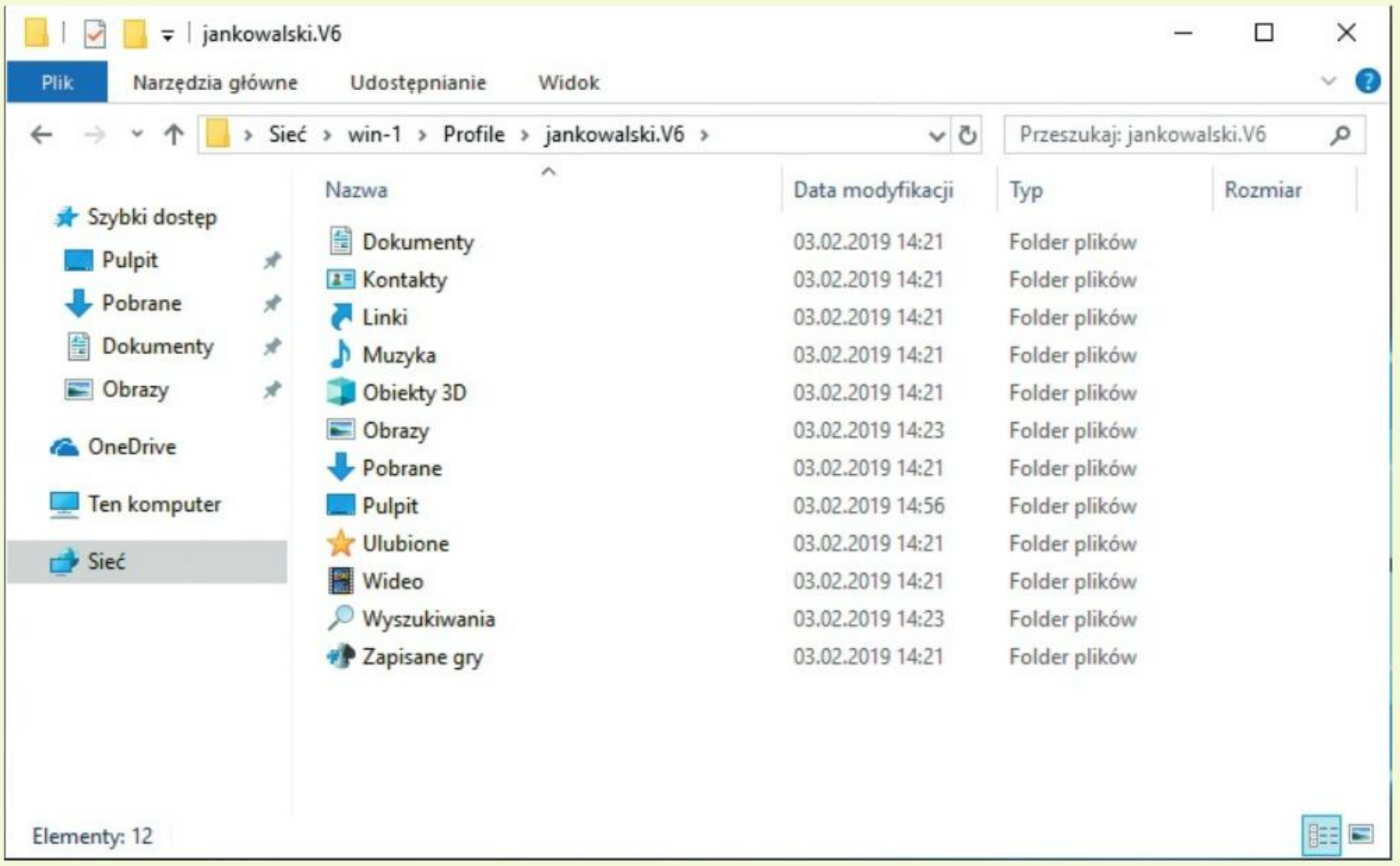
Rys. 29.1. **Konfiguracja profilu mobilnego użytkownika**

6. Po ponownym zalogowaniu użytkownika w folderze z profilami zostanie utworzony folder o nazwie takiej jak zalogowany użytkownik (rys. 29.2). Będą w nim przechowywane wszystkie informacje z profilu.



Rys. 29.2. **Folder z profilami użytkowników**

Użytkownik może podejrzeć zawartość swojego folderu z profilem (rys. 29.3).



Rys. 29.3. **Zawartość folderu z profilem użytkownika**

! UWAGA

Aby zapewnić bezpieczeństwo plikom użytkowników w folderze z profilami, należy za pomocą uprawnień systemu plików (NTFS) ograniczyć dostęp użytkowników tylko do własnego podfolderu. W ten sposób można zabezpieczyć foldery z profilami przed dostępem nieupoważnionych użytkowników.

PRZYKŁAD 29.2

Tworzenie profilu obowiązkowego

W tym ćwiczeniu zostanie skonfigurowany profil obowiązkowy dla użytkownika. Aby wykonać to zadanie, należy:

1. Utworzyć profil mobilny dla użytkownika.
2. Zalogować się na konto użytkownika i dostosować środowisko do wymagań.
3. Na serwerze zlokalizować folder z profilem.
4. Wyświetlić ukryte pliki folderu. Wybrać z menu polecenie **`Widok/Opcje/Zmień opcje folderów i wyszukiwania`**. W zakładce **`Widok`** zaznaczyć opcję **`Pokaż ukryte pliki, foldery i dyski`** i usunąć zaznaczenie opcji **`Ukryj rozszerzenia znanych typów plików`**. Kliknąć przyciski **`Zastosuj`** i **`OK`**, aby zastosować zmiany i zamknąć okno dialogowe.
5. Odszukać i kliknąć prawym przyciskiem myszy plik **`NTUSER.DAT`**, a następnie zmienić jego nazwę na **`NTUSER.MAN`**.

6. Zweryfikować działanie profilu. Zalogować się na konto, zmodyfikować wygląd pulpitu. Wylogować się i zalogować ponownie. Sprawdzić, czy wygląd pulpitu uległ zmianie.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Utwórz profile dla użytkowników *uczen1*, *uczen2* i *uczen3*.
2. Utwórz profil obowiązkowy użytkownika dla *uczen2*. Zaloguj się na konto użytkownika *uczen2*. Zmień wygląd pulpitu. Zaloguj się ponownie na konto. Czy wprowadzone zmiany są widoczne?
3. Sprawdź, jaki jest rozmiar folderu zawierającego profil użytkownika *uczen2*.

SPRAWDŹ SWOJĄ WIEDZĘ

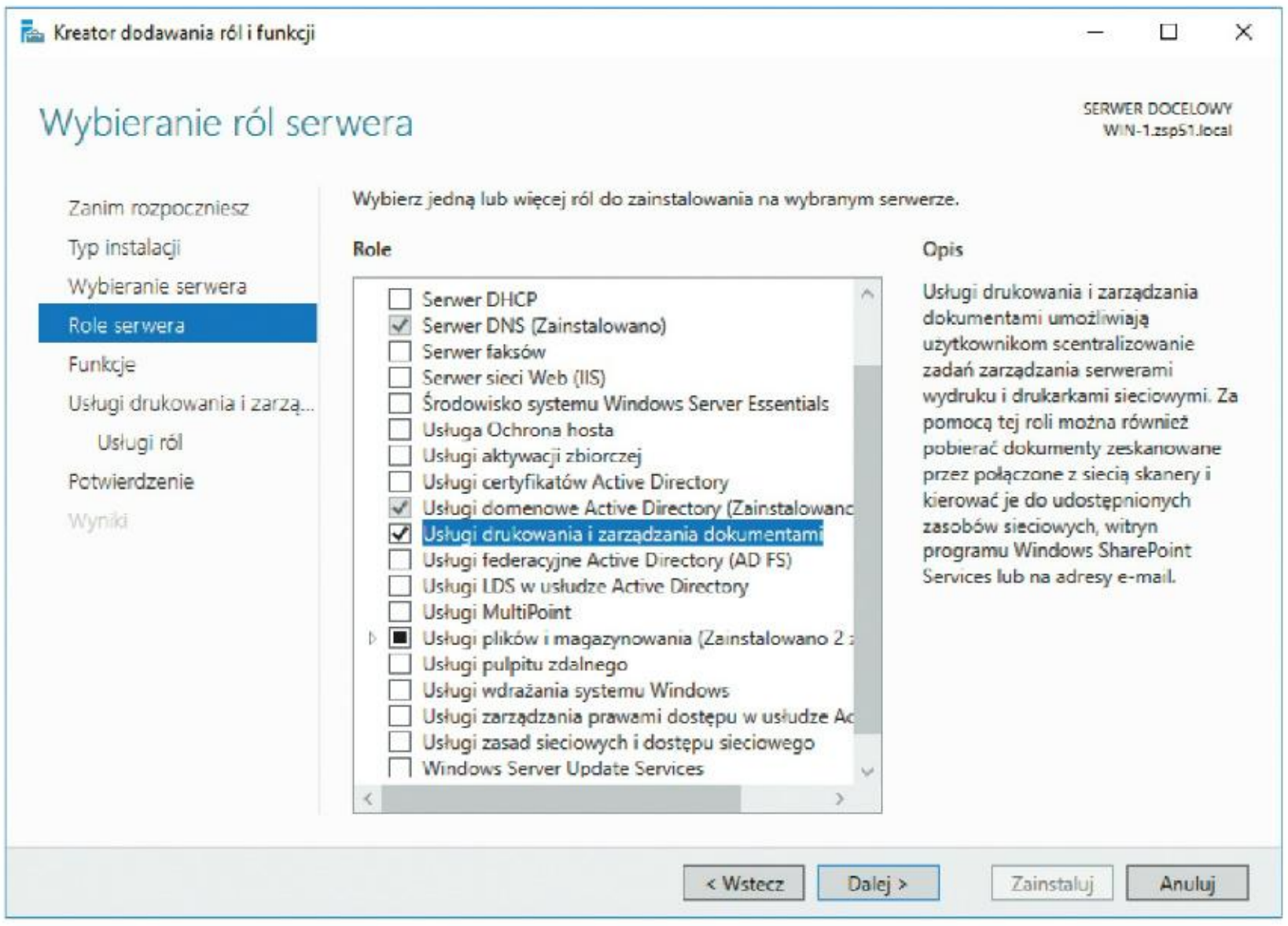
1. Jakie informacje są zapisywane w profilu?
2. Czym charakteryzuje się profil mobilny?
3. Czym różni się profil mobilny od profilu obowiązkowego?

30 Konfigurowanie roli serwera wydruku

ZAGADNIENIA

- **Funkcja pełniona przez serwer wydruku**
- **Skonfigurowanie serwera wydruku**
- **Udostępnianie użytkownikom możliwości drukowania na drukarce przyłączonej do serwera**

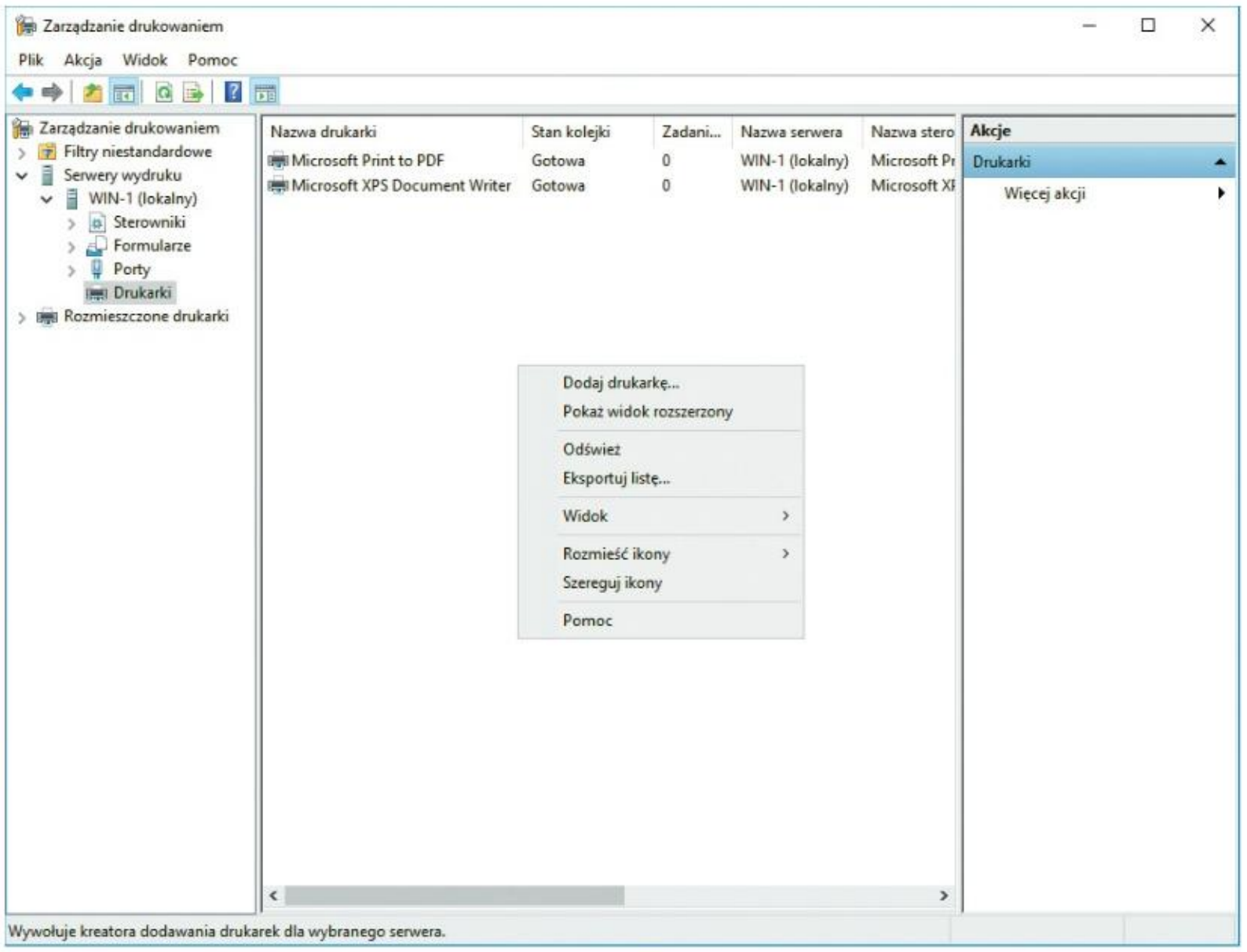
W sieci Windows można skonfigurować **drukarkę lokalną** (przyłączoną do komputera) lub **sieciową** (przyłączoną do zdalnego komputera). Drukarka sieciowa musi być udostępniona na komputerze, do którego jest przyłączona. Do zarządzania usługami drukowania na serwerze można skonfigurować rolę **serwera wydruku**. Kreatora roli serwera wydruku uruchamia się za pomocą aplikacji **Menedżer serwera**. W oknie należy wybrać odnośnik **Dodaj role i funkcje** i postępować zgodnie ze wskazówkami kreatora. Wybrać instalację opartą na rolach lub funkcjach i wskazać serwer, na którym będzie przeprowadzana instalacja. W oknie **Wybieranie ról serwera** (rys. 30.1) zaznaczyć opcję **Usługi drukowania i zarządzania dokumentami** i dodać wszystkie funkcje niezbędne do prawidłowego funkcjonowania usługi.



Rys. 30.1. Wybieranie ról serwera

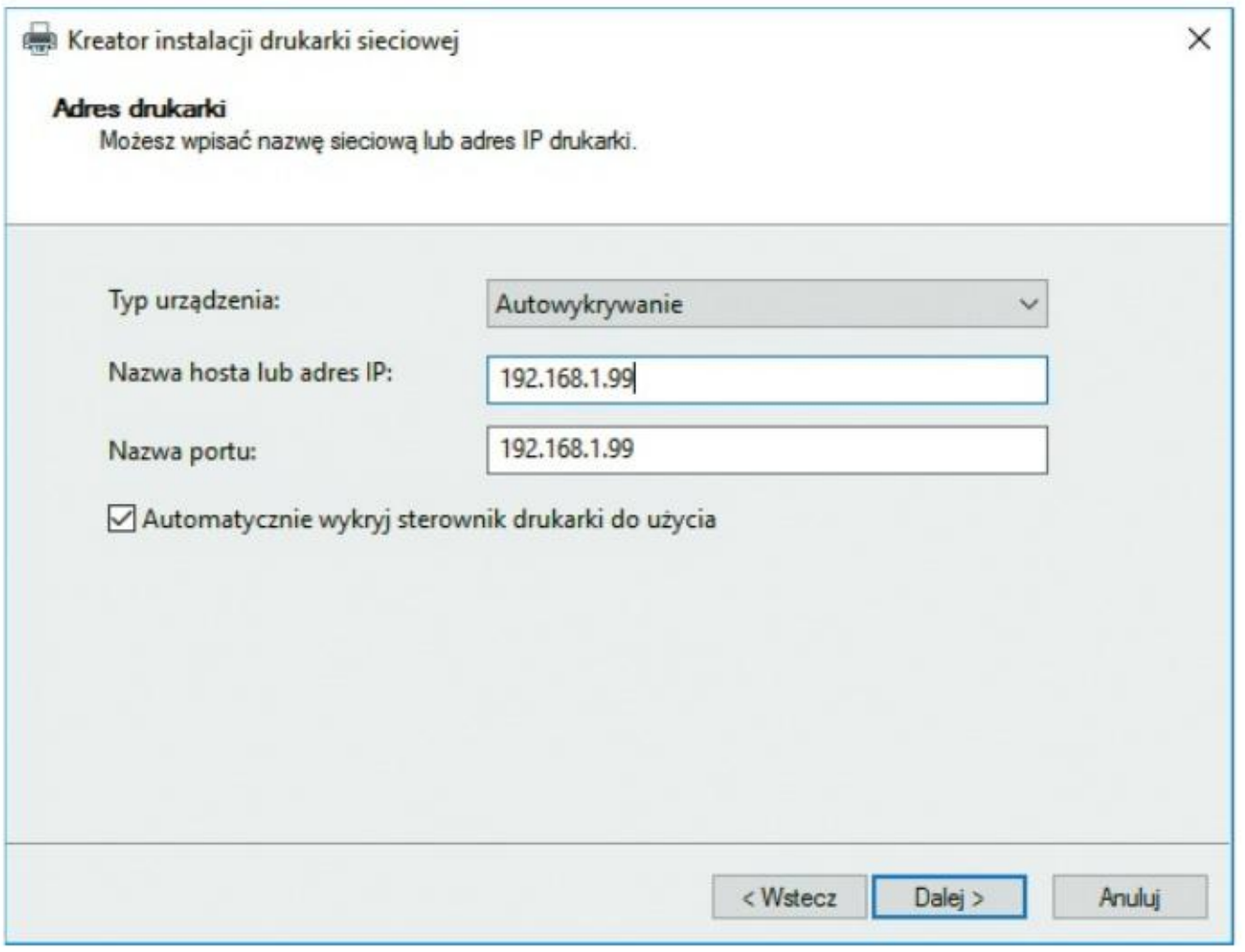
W oknie **Wybieranie usług ról** można pozostawić zaznaczoną tylko opcję **Serwer wydruku**. Jeżeli to konieczne, po instalacji należy ponownie uruchomić komputer.

Po zainstalowaniu roli serwera wydruku można zarządzać usługami drukowania za pomocą okna programu **Menedżer serwera**. W tym celu w menu należy wybrać polecenie **Narzędzia/Zarządzanie drukowaniem**. W lewym panelu rozwinąć gałęzie **Serwery wydruku/Drukarki**, a następnie kliknąć prawym przyciskiem myszy w prawym panelu i wybrać opcję **Dodaj drukarkę** (rys. 30.2).



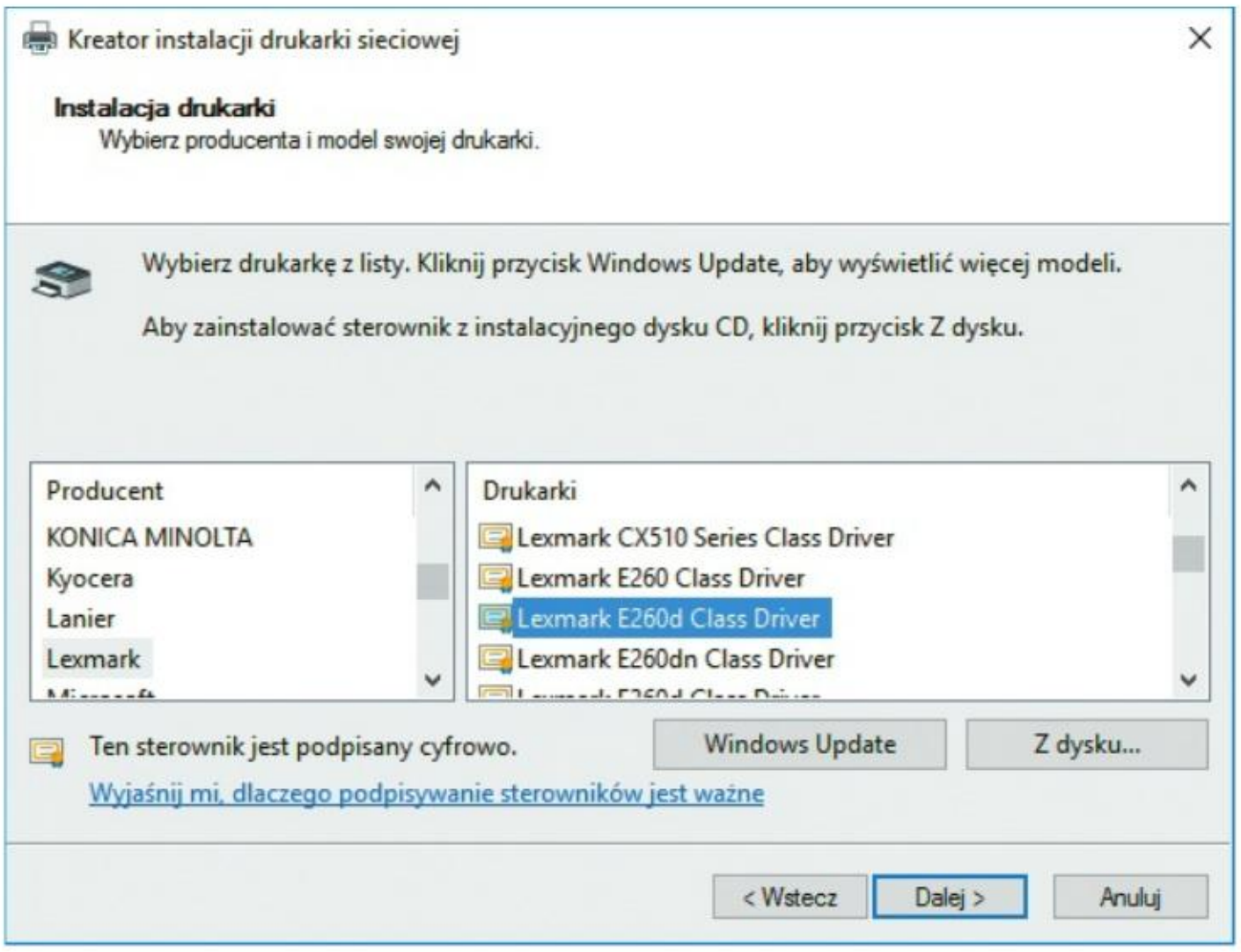
Rys. 30.2. Uruchamianie kreatora dodawania drukarki

Drukarka wyposażona w port USB powinna być rozpoznana i zainstalowana automatycznie. Jeżeli drukarka ma interfejs sieciowy, to można wybrać opcję dodawania drukarki sieciowej – **Dodaj drukarkę TCP/IP lub drukarkę usług sieci Web, używając adresu IP lub nazwy hosta**. W oknie **Adres drukarki** (rys. 30.3) trzeba wprowadzić adres IP lub nazwę hosta.



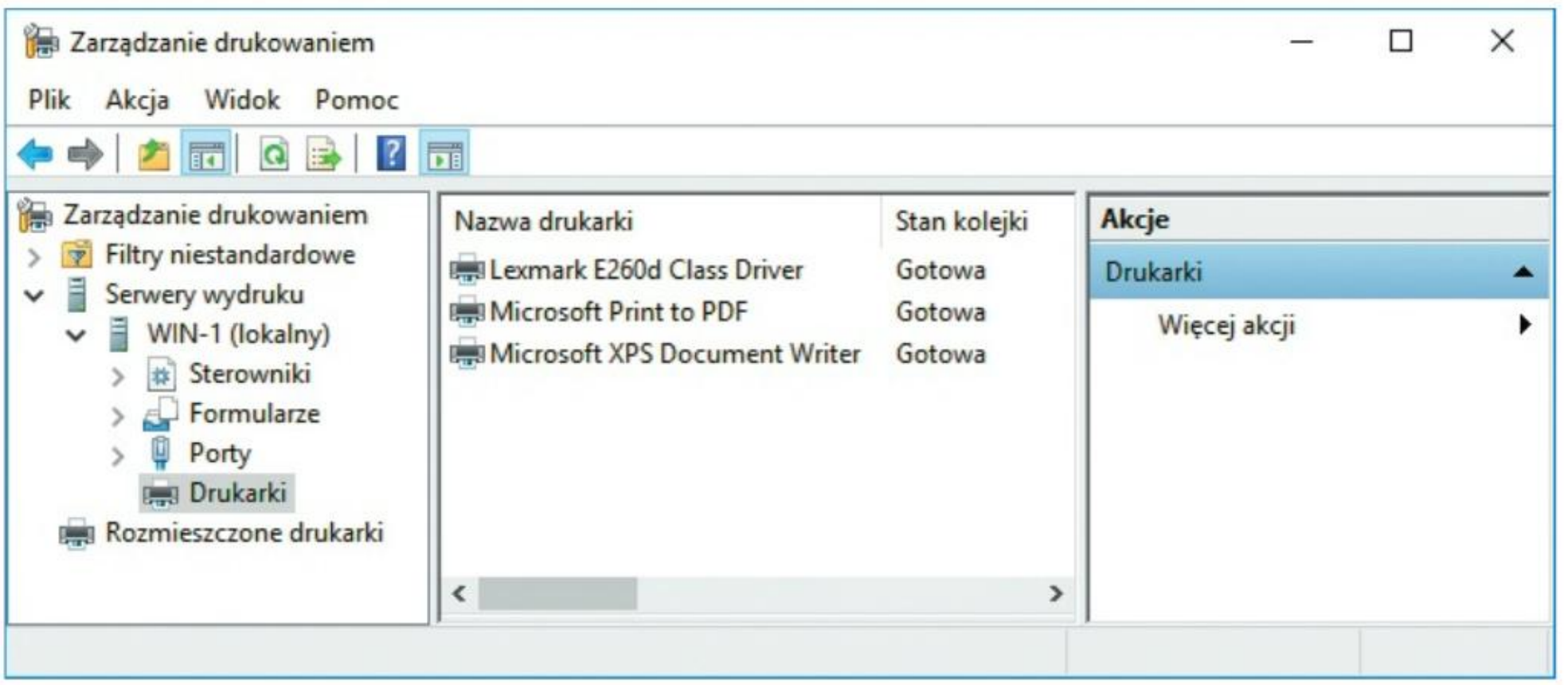
Rys. 30.3. Wprowadzanie adresu IP drukarki

Po wykryciu drukarki pod wskazanym adresem komputer wyświetli informacje o znalezionej drukarce i poprosi o wprowadzenie informacji o sterowniku drukarki. Jeżeli drukarki nie ma na liście, sterownik można pobrać lub zainstalować, korzystając z dysku lub innego nośnika (rys. 30.4).



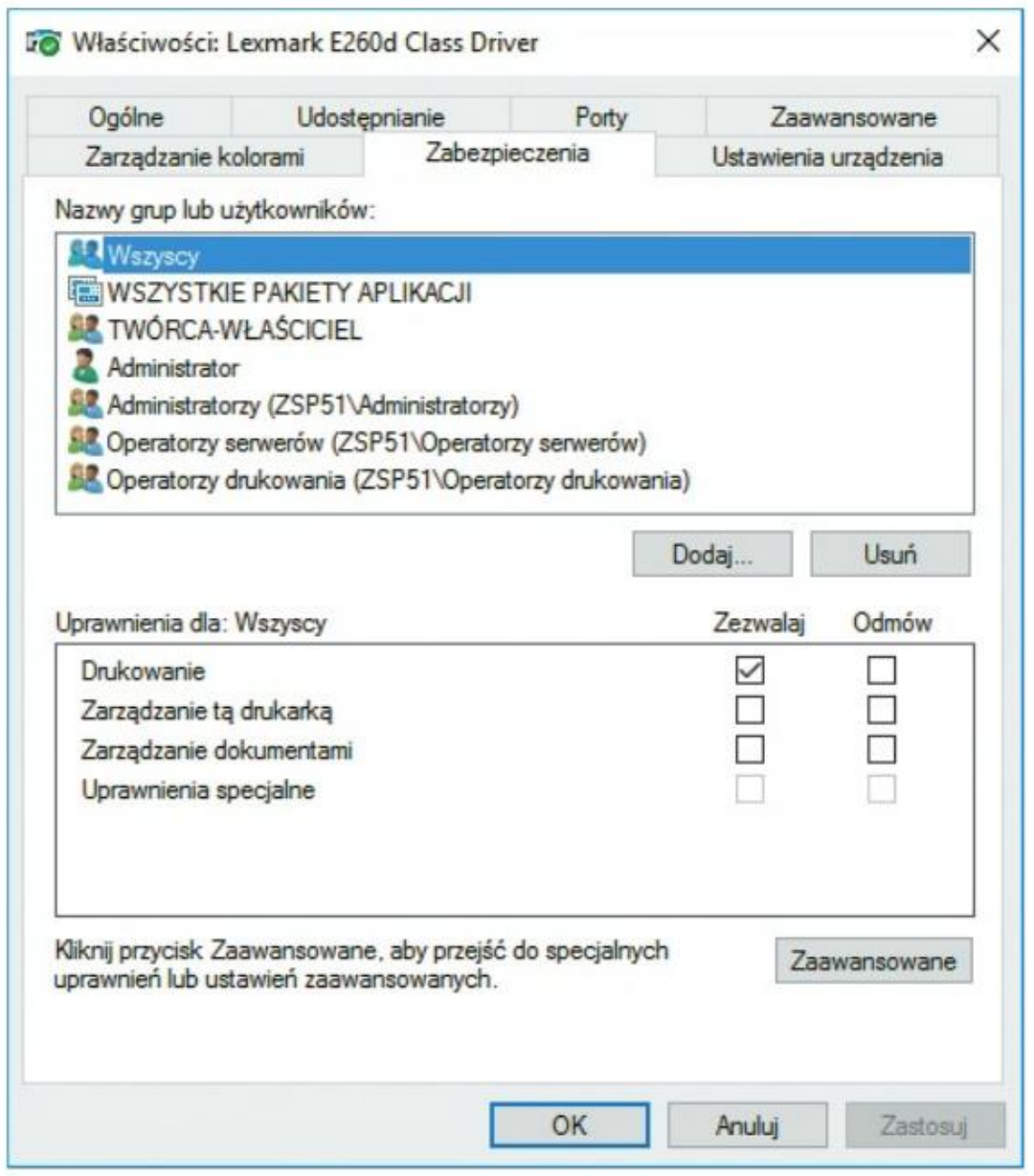
Rys. 30.4. Wybór sterownika dla drukarki

Na zakończenie procesu instalacji kreator pozwala na wprowadzenie opisu i lokalizacji drukarki. Jeżeli proces przebiegnie poprawnie, drukarka zostanie dołączona do listy drukarek dostępnych w systemie (rys. 30.5).



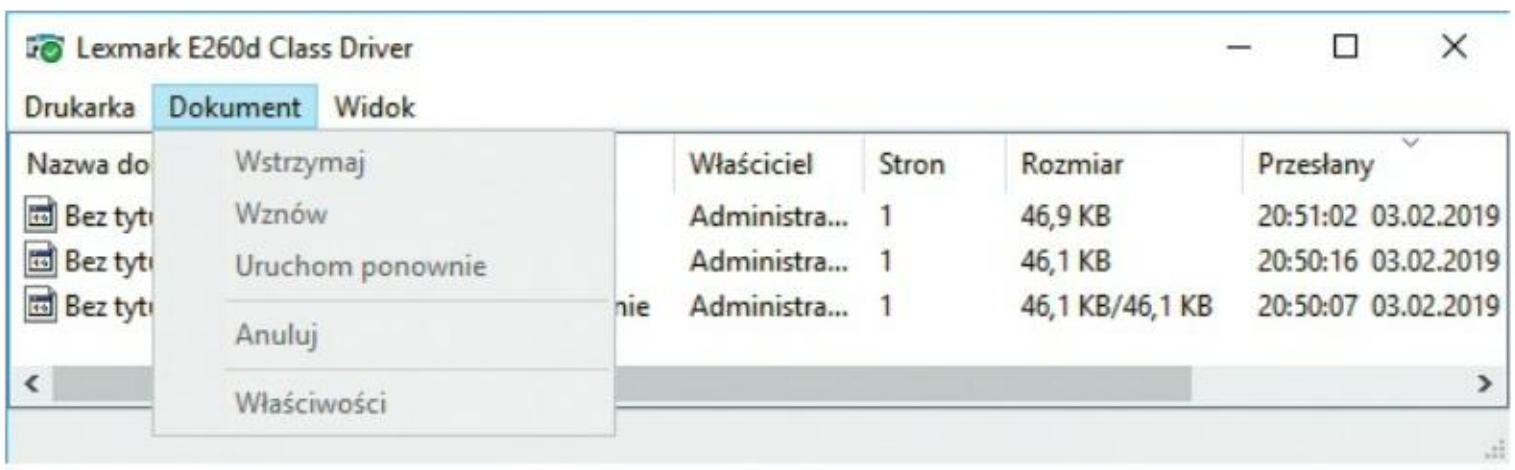
Rys. 30.5. Lista zainstalowanych drukarek

Aby przypisać użytkownikom uprawnienia do korzystania z drukarki, należy kliknąć prawym klawiszem ikonę drukarki i z menu kontekstowego wybrać opcję **`Właściwości`**, a następnie w zakładce **`Zabezpieczenia`** przypisać uprawnienia związane z drukowaniem dla poszczególnych użytkowników (rys. 30.6).



Rys. 30.6. Uprawnienia do drukarki

Okno zarządzania kolejką wydruku można otworzyć, klikając ikonę drukarki w prawym dolnym rogu ekranu.



Rys. 30.7. Okno zarządzania kolejką wydruku

Aby zarządzać zadaniami w kolejce, należy zaznaczyć zadanie i z menu wybrać polecenie **`Dokument`** (rys. 30.7).

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zainstaluj drukarkę sieciową na swoim serwerze. Nadaj prawa do drukowania wszystkim koleżankom / kolegom z klasy, a uprawnienia do zarządzania drukarką i dokumentami tylko jednemu z kolegów. Przetestuj działanie systemu drukowania. Usuń papier z drukarki lub odłącz drukarkę od zasilania. Za pomocą dowolnej aplikacji wygeneruj trzy zadania drukowania.
2. Otwórz aplikację do zarządzania kolejką wydruku (konieczne będą uprawnienia do zarządzania dokumentami).
3. Wstrzymaj drukowanie pierwszego i anuluj wykonanie drugiego zadania.
4. Aby kontynuować wykonanie trzeciego zadania, usuń przyczynę niesprawności drukarki, zaznacz zadanie i wybierz z menu **`Dokument/Uruchom ponownie`**.

31 Instalowanie i zarządzanie serwerem DHCP

ZAGADNIENIA

- **Zainstalowanie serwera DHCP**
- **Skonfigurowanie puli adresów serwera DHCP**

Klient DHCP pobiera dane konfiguracyjne od pierwszego **serwera DHCP**, od którego może je uzyskać. Aby uniknąć problemów, w sieci powinien być jeden serwer DHCP lub inne rozwiązania gwarantujące przydzielanie odpowiednich danych. Przed przystąpieniem do instalacji serwera DHCP należy odłączyć pracownię od reszty sieci lub połączyć po dwa komputery za pomocą **kabla skrosowanego** (ang. *crossover*). Jeden z komputerów będzie serwerem, a drugi – klientem DHCP.

Podczas dodawania roli kontrolera domeny powinna zostać również dodana rola serwera DHCP. Jeżeli z jakiegoś powodu ta rola nie została dodana, to można ją dodać w dowolnym momencie. W tym celu w oknie **Menedżer serwera** należy kliknąć odnośnik **Dodaj role i funkcje**, a następnie wskazać serwer, na którym ma być zainstalowana usługa, zaznaczyć serwer DHCP i dodać funkcje wymagane do poprawnej pracy serwera. **Kreator roli serwera DHCP** zainstaluje wszystkie niezbędne składniki i funkcje. Po zakończeniu instalacji można przejść do konfiguracji po wdrożeniu. Obejmuje ona wprowadzenie opisu serwera i jego **autoryzację**. W systemie Windows 2003 Server i nowszych serwery DHCP należące do środowiska domeny opartego na usłudze Active Directory muszą być autoryzowane, aby zapobiec włączaniu się do sieci obcych serwerów DHCP.

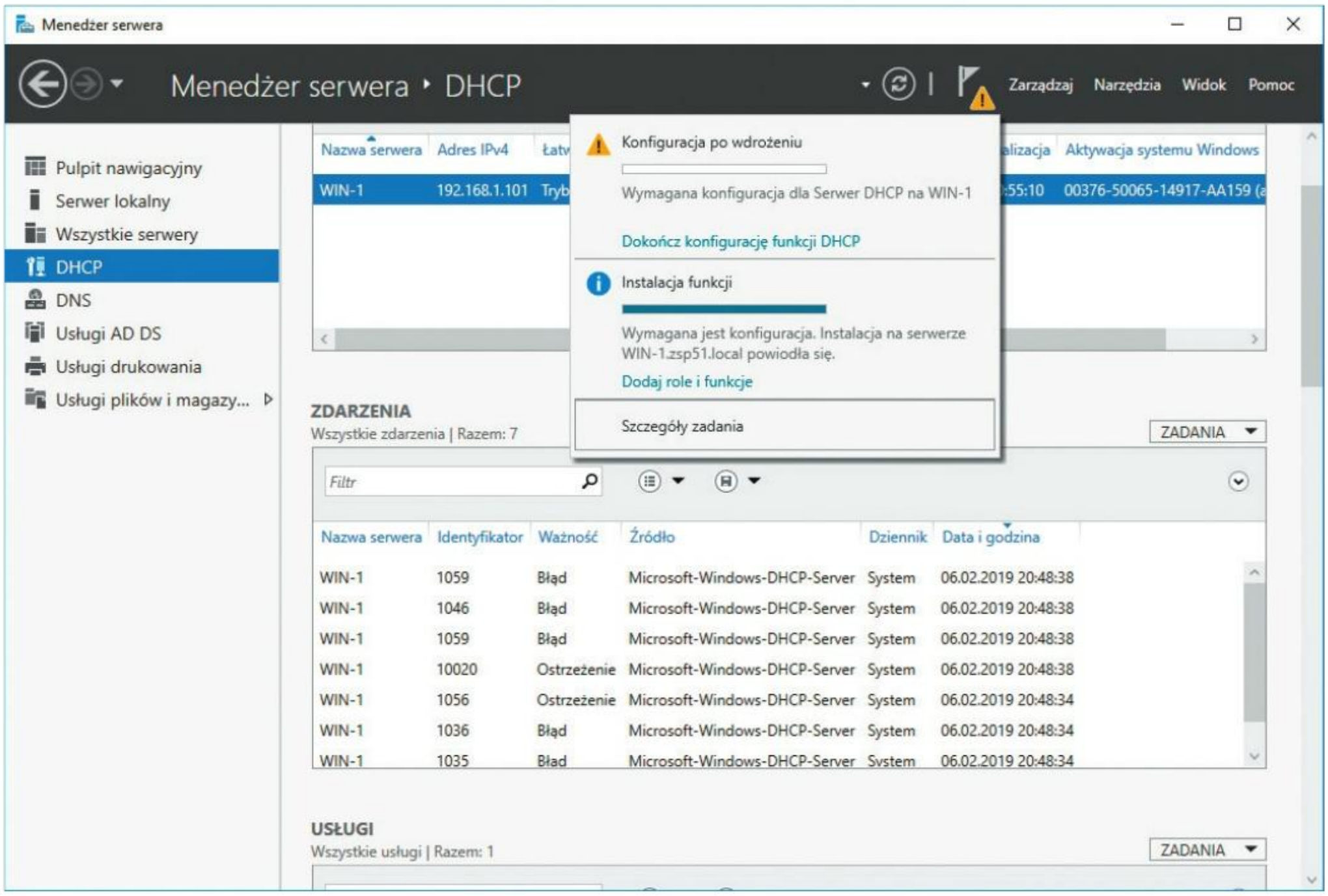
Po zakończeniu instalacji należy przeprowadzić konfigurację usługi, np. zdefiniować zakresy adresów udostępnianych klientom, opcje i rezerwacje adresów. Aby rozpocząć proces konfiguracji, trzeba w oknie **Menedżera serwera** wybrać polecenie **Narzędzia/DHCP/Dokończ konfigurację funkcji DHCP** (rys. 31.1).

Do zarządzania serwerem służy specjalna aplikacja uruchamiana w oknie **Menedżera serwera** za pomocą polecenia **Narzędzia/DHCP**. Przykład skonfigurowanego zakresu przedstawiono na rys. 31.2.

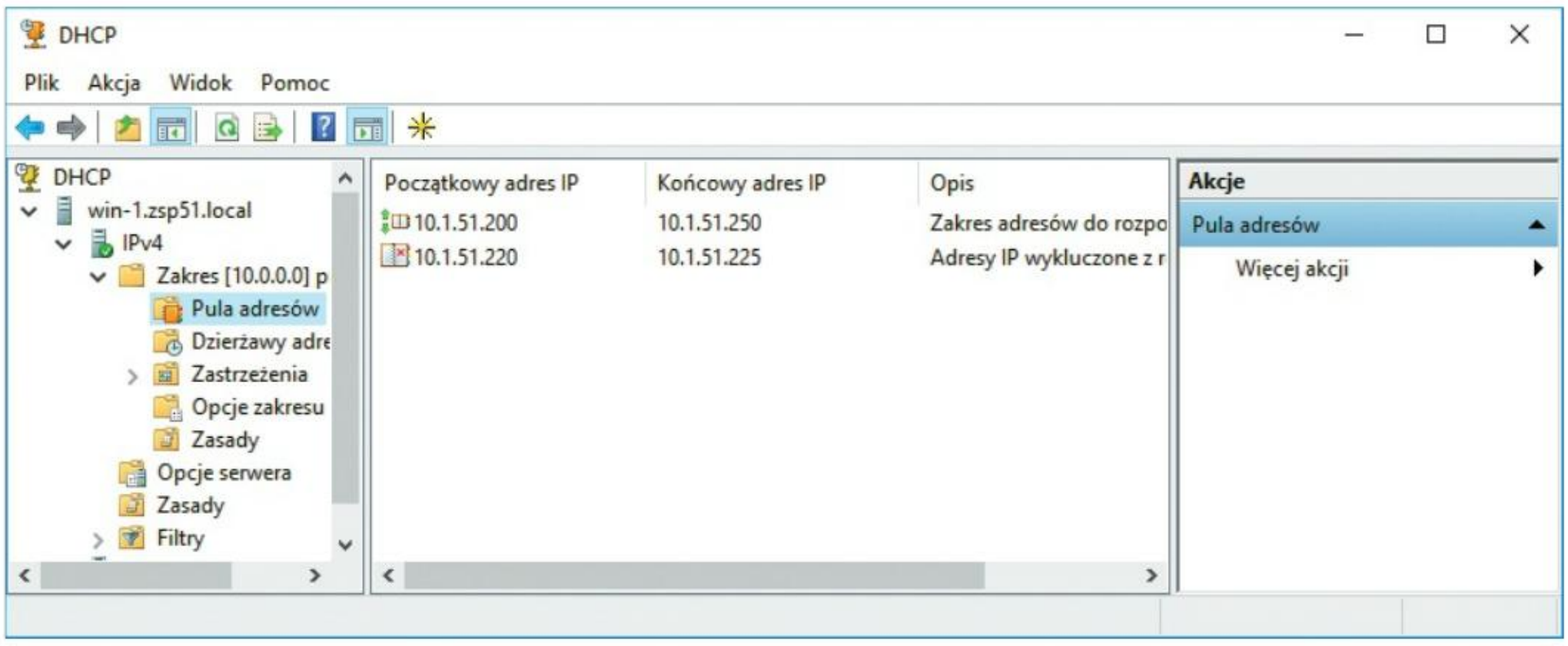
Adresy IP i inne dane potrzebne do konfiguracji komputera korzystającego z DHCP mogą być uzyskiwane w sposób dynamiczny (z puli adresów). W takim wypadku jest definiowana pula adresów, z której serwer DHCP zwykle przydziela pierwszy wolny adres. Komputer może uzyskać adres wcześniej używany lub uzyskać inny wolny adres z puli. Niektóre hosty, np. serwery, punkty dostępowe sieci Wi-Fi, telefony VoIP, drukarki lub inne urządzenia sieciowe powinny być osiągalne w sieci zawsze pod tym samym adresem.

Z puli można wykluczyć adresy przeznaczone dla tych urządzeń i przydzielić im adresy IP ręcznie lub w sposób statyczny. Zastrzeżenie w konfiguracji strefy pozwala na zdefiniowanie adresu MAC hosta i określenie odpowiadającego mu adresu IP. Serwer DHCP w pierwszej kolejności sprawdzi, czy dla danego hosta (adresu MAC) utworzono zastrzeżenie. Jeśli tak, to przydzieli adres IP zdefiniowany w zastrzeżeniu. Jeśli nie, to przydzieli adres z puli. Planując przydział adresów w sieci, należy zwrócić uwagę, aby adresy przydzielane ręcznie, z puli i na podstawie zastrzeżeń nie powodowały konfliktów i stanowiły odrębne zbiory.

W zakresie do przydzielania dynamicznego wybrano adresy od **10.1.51.200** do **10.1.51.250**. Ponadto z podanego zakresu wykluczono adresy od **10.1.51.220** do **10.1.51.225**. Adresy wykluczone mogą być przydzielane w inny sposób, np. dla serwerów lub innych urządzeń, które wymagają zawsze tego samego adresu.



Rys. 31.1. **Konfigurowanie funkcji serwera DHCP**



Rys. 31.2. **Pula adresów zakresu**

PRZYKŁAD 31.1

Konfiguracja puli adresów serwera DHCP

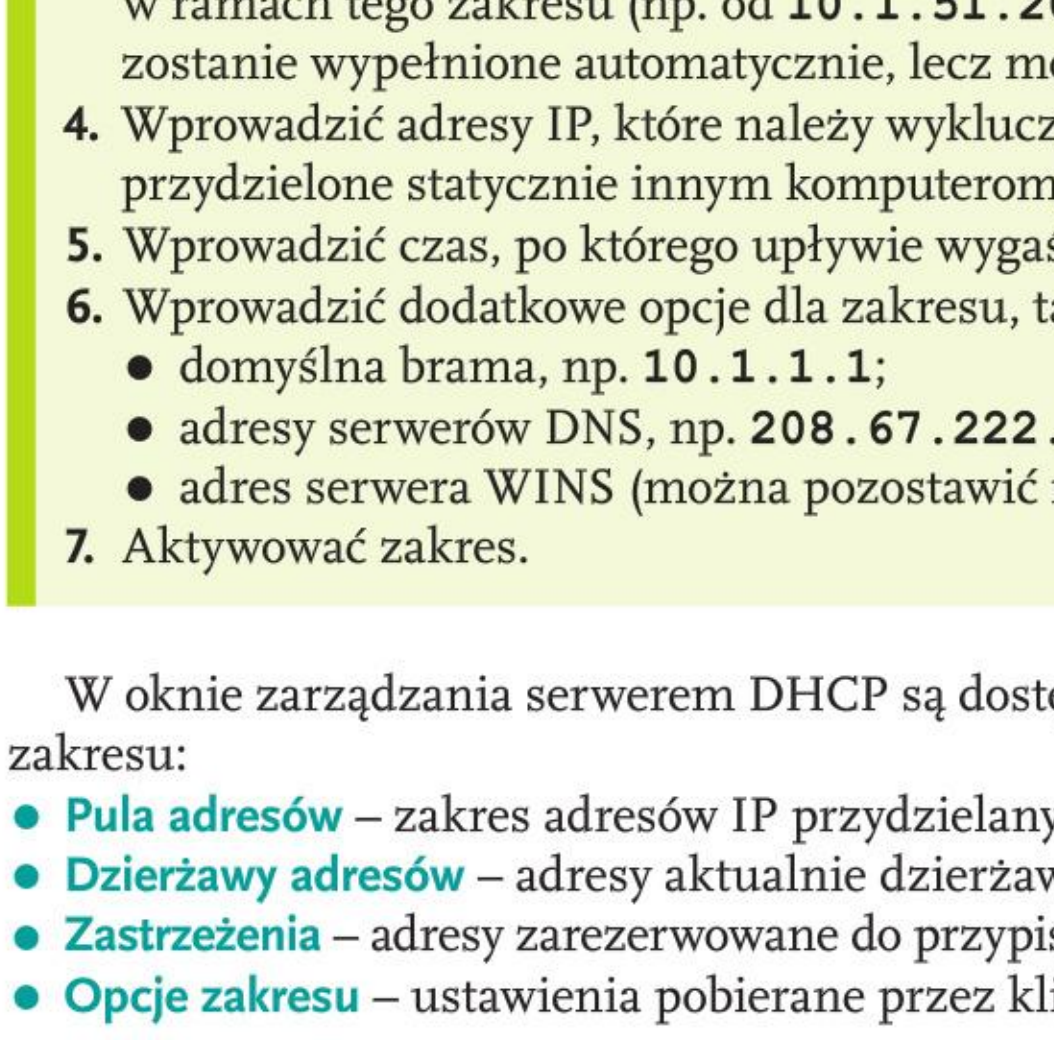
W serwerze może być utworzonych wiele zakresów. Procedura tworzenia nowego zakresu składa się z następujących czynności:

1. W drzewie serwera DHCP należy kliknąć prawym przyciskiem myszy w miejscu, w którym trzeba utworzyć nowy zakres DHCP, np. rozwinąć gałąź **win-1.zsp51.local/IPv4**, a następnie z menu kontekstowego wybrać **Nowy zakres**. Po zapoznaniu się z informacjami w oknie kreatora nowych zakresów kliknąć przycisk **Dalej**.
2. Wprowadzić nazwę zakresu, np. *pracownia51*, i opis zakresu, np. *pracownia komputerowa 51*.
3. Wprowadzić adres początkowy i końcowy, które można wydzierżawiać klientom w ramach tego zakresu (np. od **10.1.51.200** do **10.1.51.250**). Pole maski podsieci zostanie wypełnione automatycznie, lecz można je zmienić w razie potrzeby.
4. Wprowadzić adresy IP, które należy wykluczyć z wprowadzonego zakresu, np. już przydzielone statycznie innym komputerom, np. od **10.1.51.220** do **10.1.51.225**.
5. Wprowadzić czas, po którego upływie wygaśnie dzierżawa adresu IP, np. *1 dzień*.
6. Wprowadzić dodatkowe opcje dla zakresu, takie jak:
   - domyślna brama, np. **10.1.1.1**;
   - adresy serwerów DNS, np. **208.67.222.222** i **208.67.220.220**;
   - adres serwera WINS (można pozostawić niewypełnione).
7. Aktywować zakres.

W oknie zarządzania serwerem DHCP są dostępne zakładki zawierające informacje o użyciu zakresu:

- **Pula adresów** – zakres adresów IP przydzielanych klientom i adresy wykluczone;
- **Dzierżawy adresów** – adresy aktualnie dzierżawione przez klientów;
- **Zastrzeżenia** – adresy zarezerwowane do przypisywania adresów IP na podstawie adresu MAC;
- **Opcje zakresu** – ustawienia pobierane przez klientów, np. adres bramy, serwery DNS.

Niektóre urządzenia w sieci, np. drukarki, powinny uzyskiwać zawsze ten sam adres IP, co ułatwia ich odszukanie w sieci. Dla takich urządzeń można zarezerwować adresy IP, przydzielane na podstawie adresu MAC. Aby zarezerwować nowy adres, należy kliknąć prawym przyciskiem myszki **Zastrzeżenia**, a następnie z menu kontekstowego wybrać **Nowe zastrzeżenie**. W otwartym oknie (rys. 31.3) wpisać nazwę, rezerwowany adres IP i adres MAC urządzenia, dla którego ma być zachowany adres IP.



Rys. 31.3. **Okno nowego zastrzeżenia**

Jeżeli w interfejsie nie ustawiono statycznego adresu IP, a stacja nie mogła pobrać adresu z serwera DHCP, system Windows ustawia adres automatyczny z puli **APIPA** (ang. *Automatic Private IP Addressing*). Pula obejmuje adresy **`169.254.x.x`** z maską sieci **`255.255.0.0`**. Gdy serwer DHCP znów stanie się osiągalny, komputer automatycznie uzyska adres IP z serwera.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj serwer DHCP do obsługi zakresu 30 adresów. Dziesięć adresów ze środka zakresu należy wykluczyć i przeznaczyć na urządzenia sieciowe. Stwórz zastrzeżenie dla drukarki sieciowej.

32 Konfigurowanie serwera DNS

ZAGADNIENIA

Funkcje serwera DNS **Zainstalowanie serwera DNS i skonfigurowanie strefy przeszukiwania** **Dodawanie rekordów do konfiguracji serwera DNS** **Dodawanie aliasów do konfiguracji serwera DNS** **Dodawanie wskaźnika przeszukiwania wstecz do konfiguracji serwera DNS** **Dodawanie rekordu serwera pocztowego do konfiguracji serwera DNS**

Serwer DNS może być wykorzystany do tłumaczenia nazw w sieci lokalnej na adresy IP (strefa przeszukiwania „w przód") i adresów IP na nazwy (strefa przeszukiwania „wstecz"). Serwer może być zintegrowany z usługą Active Directory z dynamiczną aktualizacją danych klientów. **Aktualizacje dynamiczne** umożliwiają komputerom klientów rejestrowanie i aktualizowanie ich rekordów zasobów w strefach przeszukiwania DNS po wystąpieniu każdej zmiany. Pozwala to ograniczyć konieczność ręcznego modyfikowania rekordów przez administratora, szczególnie w przypadku klientów, którzy często zmieniają lokalizację, a do uzyskiwania adresu IP wykorzystują usługę DHCP.

Aktualizacje dynamiczne mogą być wykonywane z powodów:

- dodania, usunięcia lub modyfikacji adresu IP podczas konfigurowania protokołu TCP/IP;
- zmiany lub odnowienia dzierżawy adresu IP z serwera DHCP;
- użycia polecenia **`ipconfig /registerdns`** służącego do wymuszenia odświeżenia rejestracji nazwy klienta w systemie DNS;
- podczas uruchamiania komputera;
- gdy komputer ma pełnić funkcję kontrolera domeny.

Możliwość dynamicznego dołączania komputerów jest obsługiwana tylko przez systemy Windows 2000 i nowsze. W przypadku starszych wersji administrator musi aktualizować bazę stref. Serwer DNS powinien być skonfigurowany w każdej domenie i poddomenie. W małej sieci szkolnej wystarczy tylko serwer podstawowy, chociaż ze względów bezpieczeństwa byłoby dobrze skonfigurować zarówno serwer **podstawowy**, jak i **zapasowy**. Na tym serwerze zostaną zapisane informacje o wszystkich komputerach w szkole (domenie). Jeżeli na serwerze jest skonfigurowana rola kontrolera domeny (Active Directory), serwer DNS powinien być również zainstalowany. W innym przypadku należy dodać rolę serwera DNS dla naszego komputera.

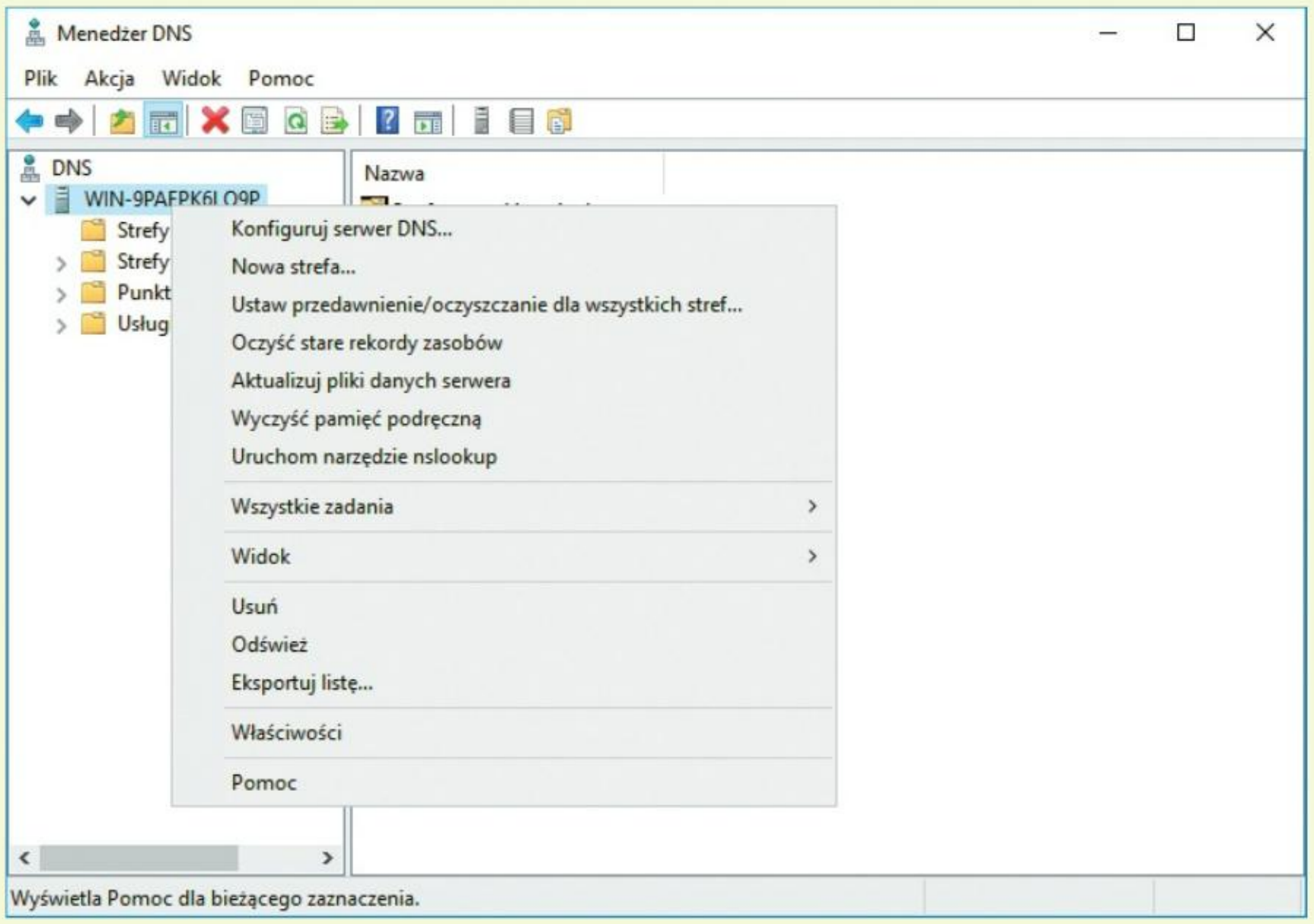
PRZYKŁAD 32.1

Instalacja serwera DNS i konfiguracja stref przeszukiwania

Aby zainstalować serwer DNS, możemy skorzystać z kreatora w oknie **`Menedżer serwera`**. Należy kliknąć odnośnik **`Dodaj role i funkcje`** i wskazać serwer DNS do zainstalowania. Po zakończeniu instalacji trzeba wykonać konfigurację roli serwera DNS.

W tym celu należy:

1. W oknie aplikacji **Menedżer serwera** wybrać polecenia **Narzędzia/DNS**.
2. W lewym panelu rozwinąć gałąź DNS, kliknąć prawym przyciskiem myszy nazwę serwera i z menu kontekstowego wybrać **Konfiguruj serwer DNS**... (rys. 32.1).



Rys. 32.1. **Uruchomienie kreatora konfiguracji serwera DNS**

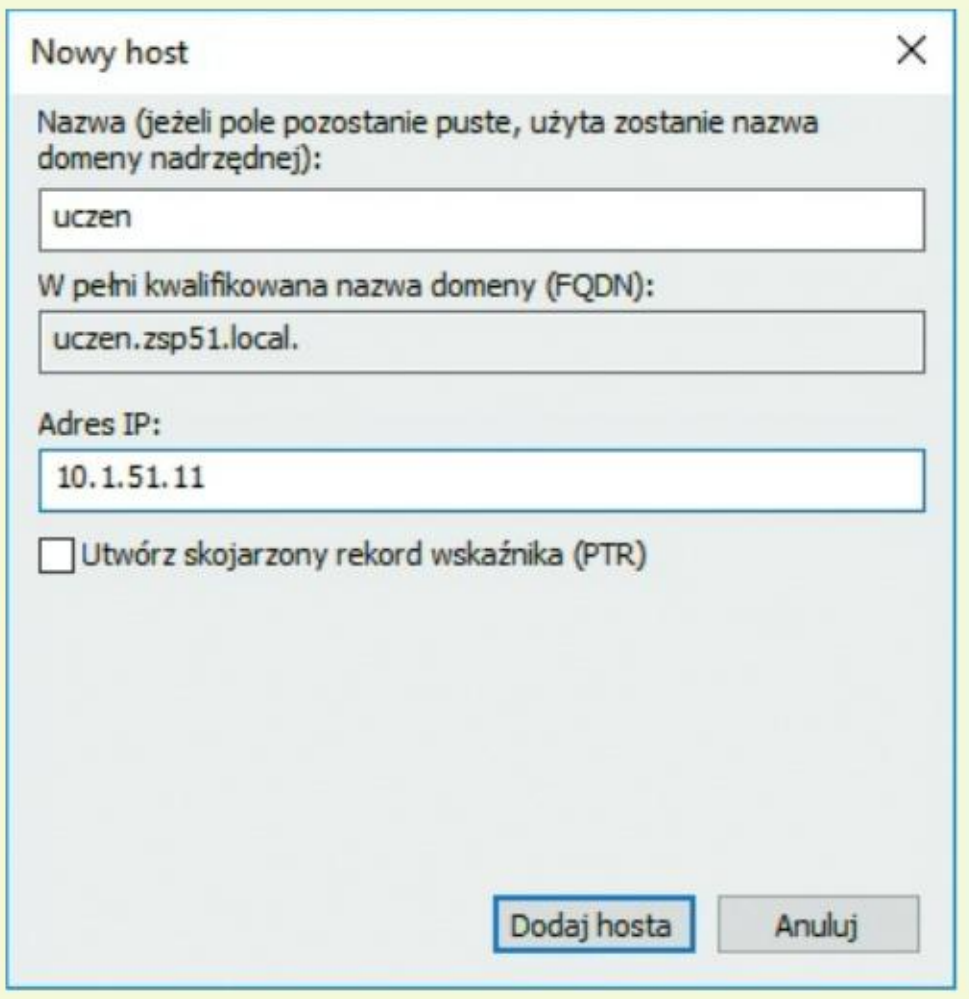
3. Wybrać rodzaj strefy, która ma być zainstalowana. Dla małych sieci jest zalecane zainstalowanie tylko strefy przeszukiwania „do przodu", dla dużych – tworzenie obu stref. Tu należy wybrać utworzenie obu stref.
4. Wprowadzić dane dotyczące konfiguracji strefy przeszukiwania „do przodu":
   - typ przechowywanej strefy – wybrać **strefę podstawową**;
   - nazwę strefy, np. **zsp51.local**;
   - zatwierdzić nazwę tworzonego pliku strefy;
   - informacje o aktualizacjach dynamicznych – nie zezwalaj na aktualizacje dynamiczne, wszystkie dane będą wprowadzane przez administratora.
5. Wprowadzić dane dotyczące konfiguracji strefy przeszukiwania „wstecz":
   - typ przechowywanej strefy – wybrać **strefę podstawową**;
   - wybrać wersję protokołu **IPv4**;
   - identyfikator (adres IP) sieci, np. **10.1.51**;
   - zatwierdzić nazwę tworzonego pliku strefy;
   - informacje o aktualizacjach dynamicznych – nie zezwalaj na aktualizacje dynamiczne, wszystkie dane będą wprowadzane przez administratora.
6. Zaznaczyć opcję, że serwer nie powinien przesyłać kwerend dalej, aby nie zakłócać pracy serwerów DNS w internecie.
7. Funkcja aktualizacji dynamicznych nie została włączona, dlatego trzeba umieścić wpisy dotyczące obsługiwanych w sieci nazw.

PRZYKŁAD 32.2

Dodawanie rekordów do konfiguracji serwera DNS

Aby dodać nowy wpis hosta (rekord typu A), należy:

1. Kliknąć prawym przyciskiem myszy na wybranej strefie (np. wyszukiwania do przodu **`zsp51.local`**).
2. Z menu kontekstowego wybrać opcję **`Nowy host`** (A lub AAAA).
3. W oknie tworzenia nowego hosta (rys. 32.2) wpisać nazwę hosta, np. *uczen*, i adres IP komputera, do którego ma się odwoływać nazwa, np. **`10.1.51.11`**. Zaznaczenie opcji **`Utwórz skojarzony rekord wskaźnika PTR`** spowodowałoby utworzenie odpowiedniego wskaźnika w strefie przeszukiwania „wstecz".



Rys. 32.2. **Tworzenie wpisu rekordu typu A**

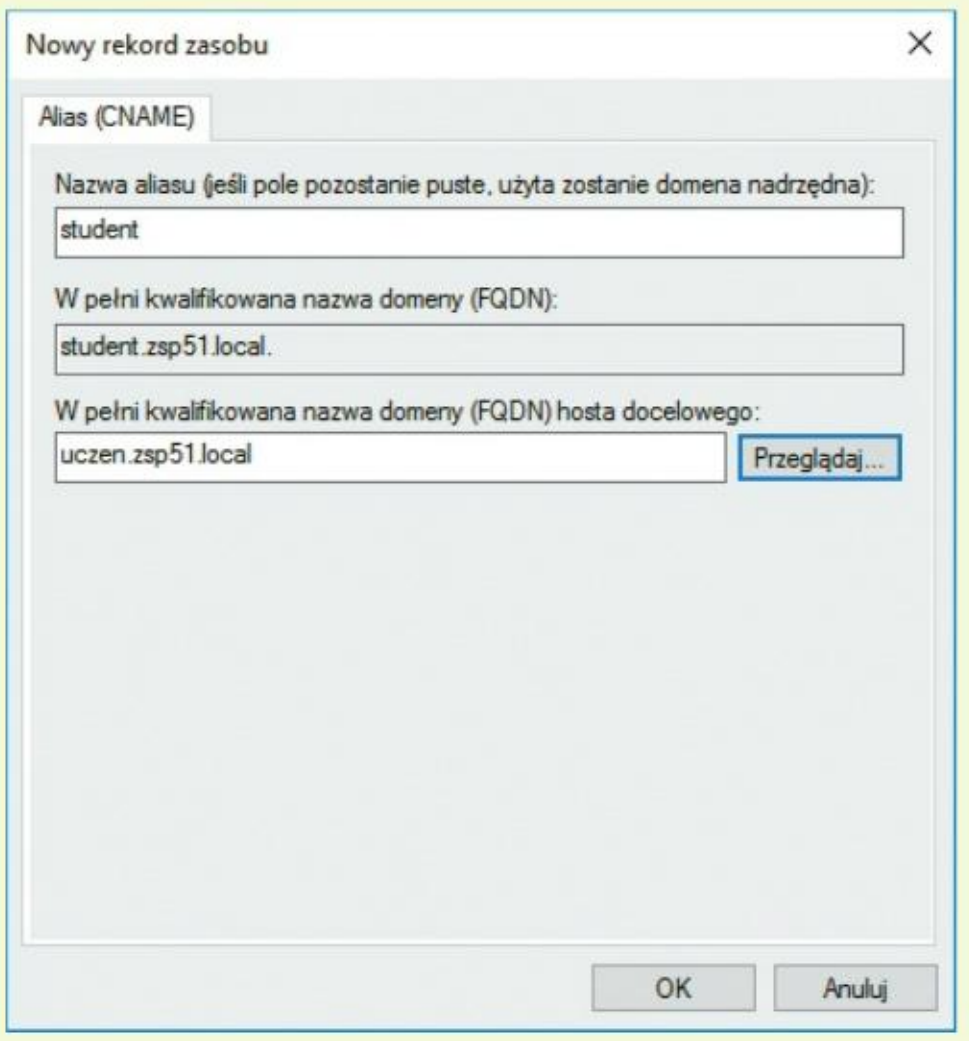
System DNS zezwala, aby do jednego adresu IP można było odwoływać się za pomocą różnych nazw. Możemy to uzyskać, jeśli utworzymy aliasy do nazw.

PRZYKŁAD 32.3

Dodawanie aliasu do konfiguracji serwera DNS

Aby dodać nowy alias (rekord typu CNAME), należy:

1. Kliknąć prawym przyciskiem myszy na wybranej strefie (np. **`zsp51.local`**).
2. Z menu kontekstowego wybrać opcję **`Nowy alias`** (CNAME).
3. W oknie tworzenia nowego aliasu (rys. 32.3) wpisać nazwę aliasu, np. *student*, i nazwę rekordu typu A, do którego ma się odwoływać alias, np. **`uczen.zsp51.local`**.
4. Po wprowadzeniu danych do DNS nazwa **`student.zsp51.local`** będzie wskazywać na ten sam adres IP co nazwa **`uczen.zsp51.local`**.



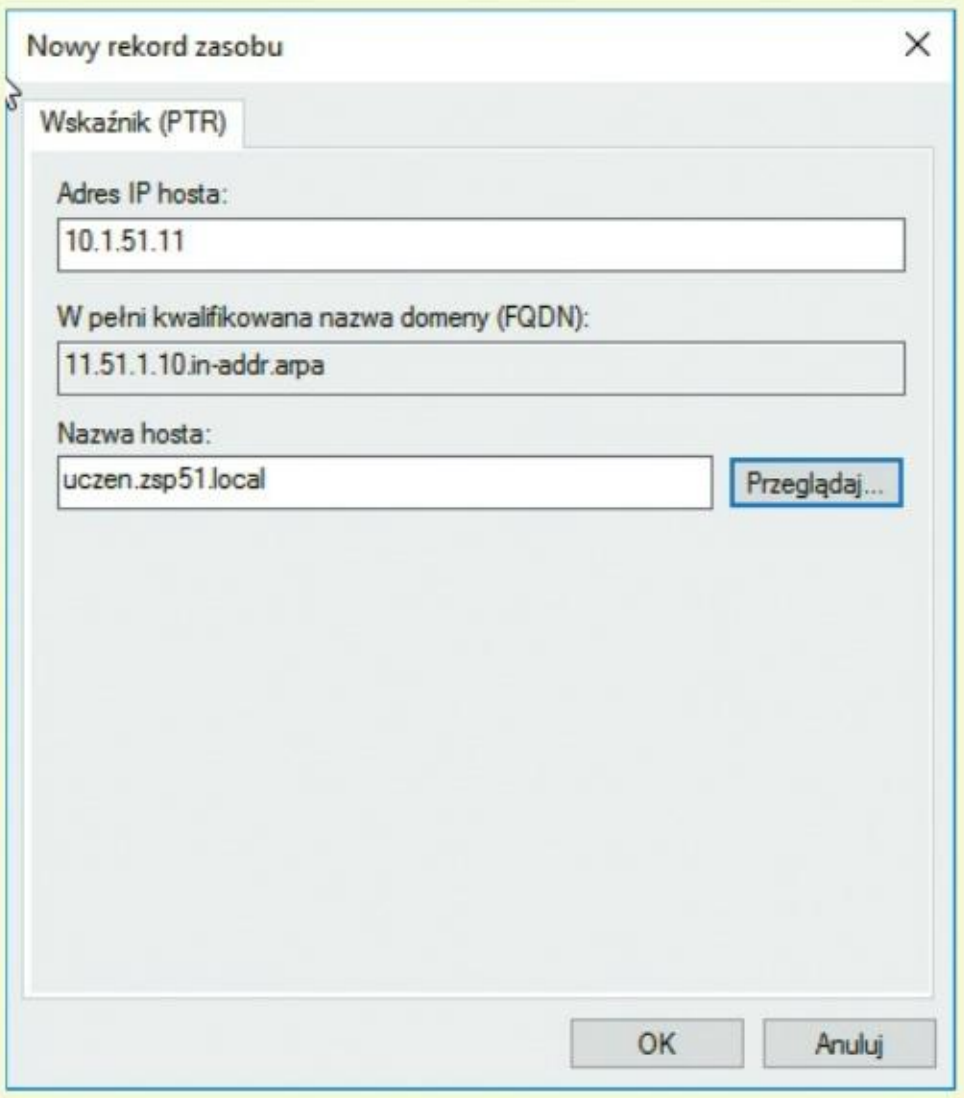
Rys. 32.3. **Tworzenie aliasu**

PRZYKŁAD 32.4

Dodawanie wskaźnika przeszukiwania wstecz do konfiguracji serwera DNS

Aby dodać nowy wskaźnik przeszukiwania wstecz (rekord typu PTR), należy:

1. Kliknąć prawym przyciskiem myszy wybraną strefę przeszukiwania „wstecz” (np. **`51.1.10.in-addr.arpa`**).
2. Z menu kontekstowego wybrać opcję **`Nowy wskaźnik`** (PTR).
3. W oknie tworzenia nowego wskaźnika (rys. 32.4) wpisać adres IP i nazwę rekordu typu A, do którego ma się odwoływać wskaźnik, np. **`uczen.zsp51.local`**.



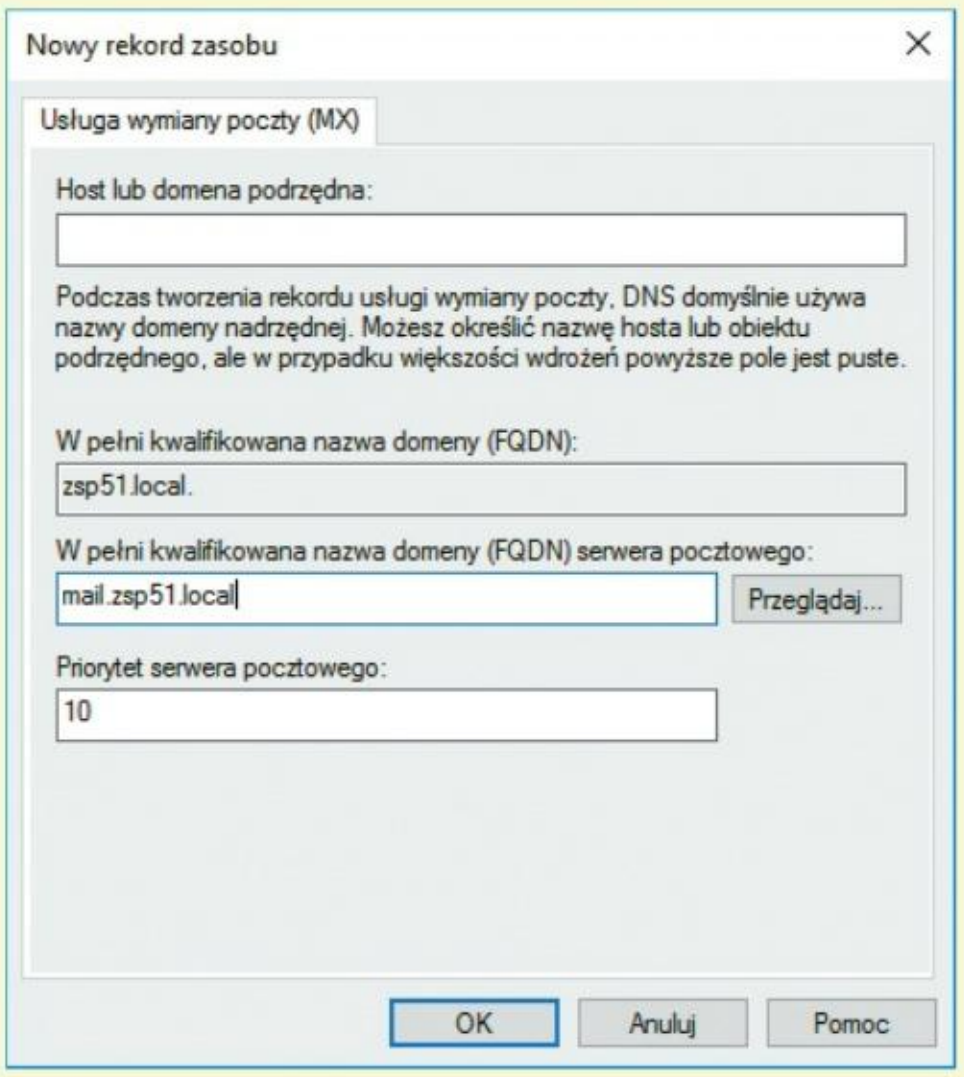
Rys. 32.4. **Tworzenie wskaźnika dla strefy przeszukiwania wstecz**

PRZYKŁAD 32.5

Dodawanie rekordu serwera pocztowego do konfiguracji serwera DNS

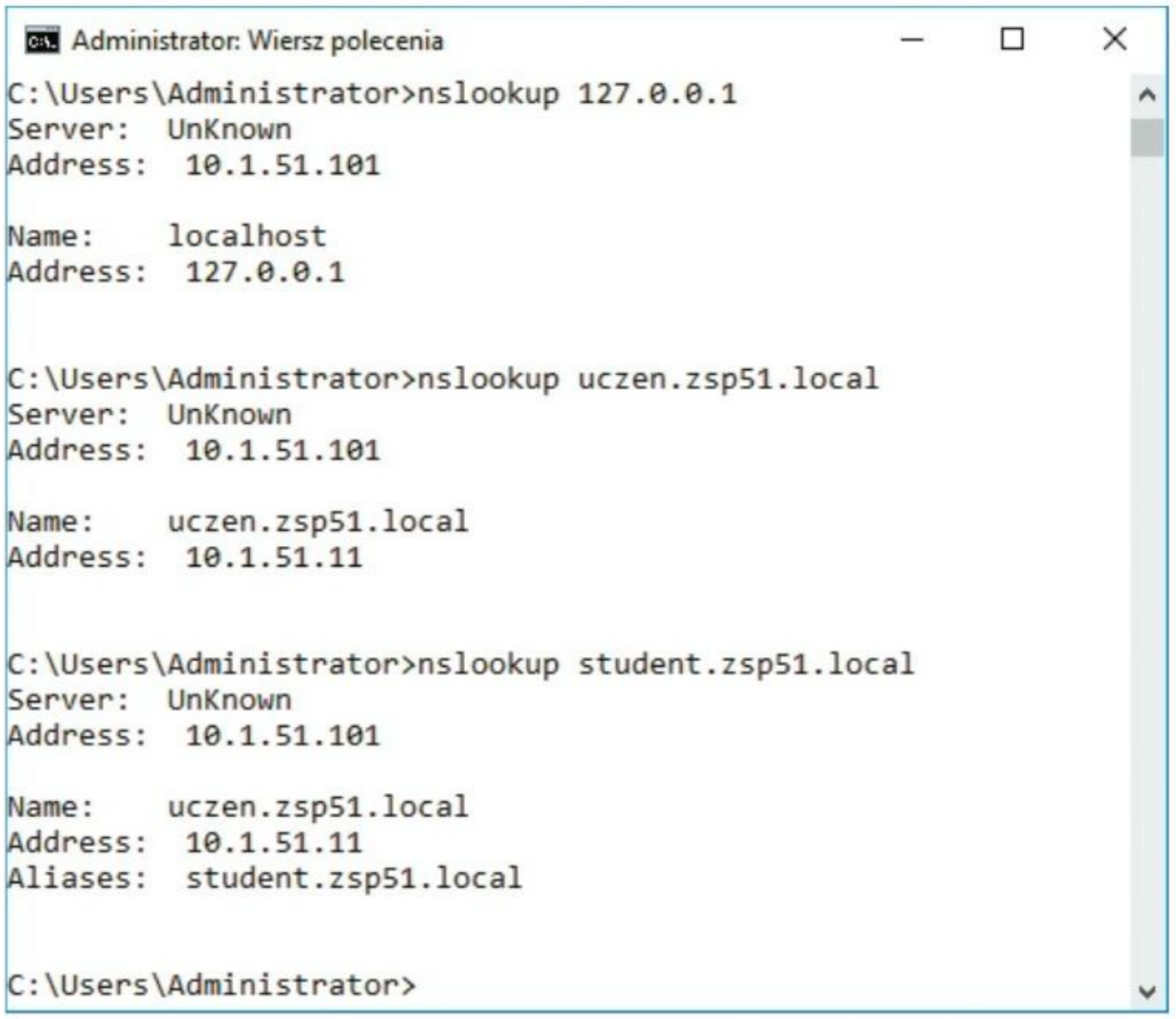
Aby dodać nowy rekord serwera pocztowego (rekord typu MX), należy:

1. Kliknąć prawym przyciskiem myszy wybraną strefę przeszukiwania.
2. Z menu kontekstowego wybrać opcję **`Nowa usługa wymiany poczty`** (MX).
3. W oknie tworzenia nowego wpisu (rys. 32.5) wpisać nazwę serwera poczty, np. **`mail.zsp51.local`**, i priorytet tego serwera. Pole **`Host lub domena podrzędna`** na ogół pozostawia się puste, wtedy serwer będzie obsługiwał całą domenę.



Rys. 32.5. **Tworzenie wpisu serwera pocztowego**

Do przetestowania działania serwera DNS można wykorzystać narzędzie **Nslookup**. Wysyła ono zapytanie do serwera i zwraca dokładne informacje pozwalające zlokalizować i diagnozować problemy. **`Nslookup`** jest narzędziem linii poleceń. Jako argument dla polecenia można użyć nazwy komputera (testowanie strefy przeszukiwania „do przodu") lub adresu IP (testowanie strefy przeszukiwania wstecz). Przykład działania polecenia przedstawiono na rys. 32.6. Aby móc testować działanie wprowadzonych wpisów do serwera DNS, należy ustawić w opcjach połączenia sieciowego adres lokalnego komputera jako adres serwera DNS.



Rys. 32.6. Testowanie DNS za pomocą narzędzia nslookup

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj serwer DNS obsługujący twoją szkołę. Serwer powinien zawierać rekordy:
   - hostów – co najmniej 5;
   - serwera WWW;
   - serwera poczty elektronicznej;
   - wskaźniki strefy przeszukiwania wstecz.
2. Sprawdź, jakie serwery DNS są wykorzystywane w twojej szkole.
3. Wypisz w zeszycie przedmiotowym adresy przynajmniej pięciu ogólnodostępnych serwerów DNS działających w internecie.

SPRAWDŹ SWOJĄ WIEDZĘ

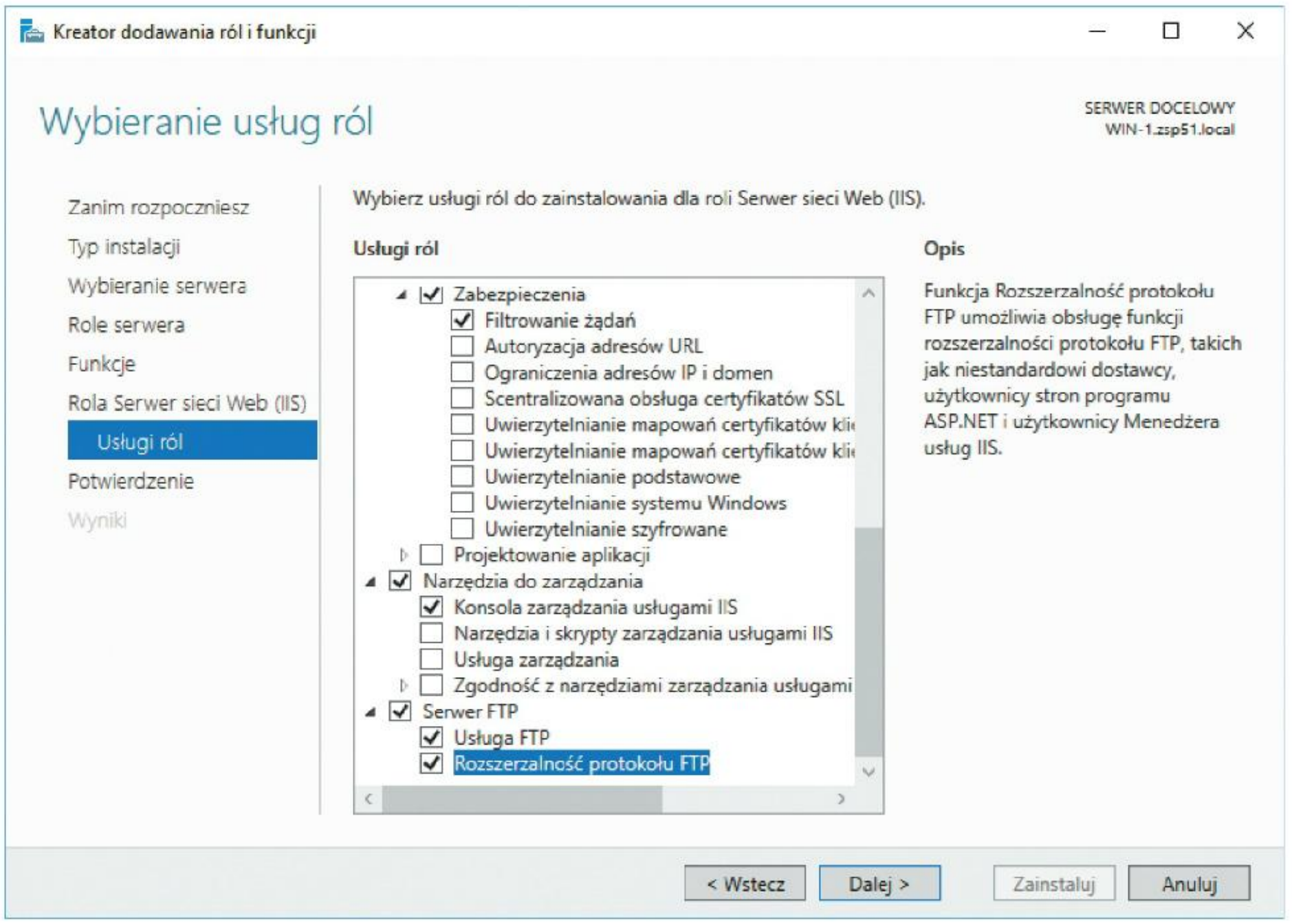
1. Wyjaśnij, do czego można wykorzystać rekord CNAME.
2. Wyjaśnij, dlaczego w sieci powinny być serwery DNS podstawowy i zapasowy.
3. Na czym polega różnica między rekordem A i rekordem AAAA.

33 Internetowe usługi informacyjne

ZAGADNIENIA

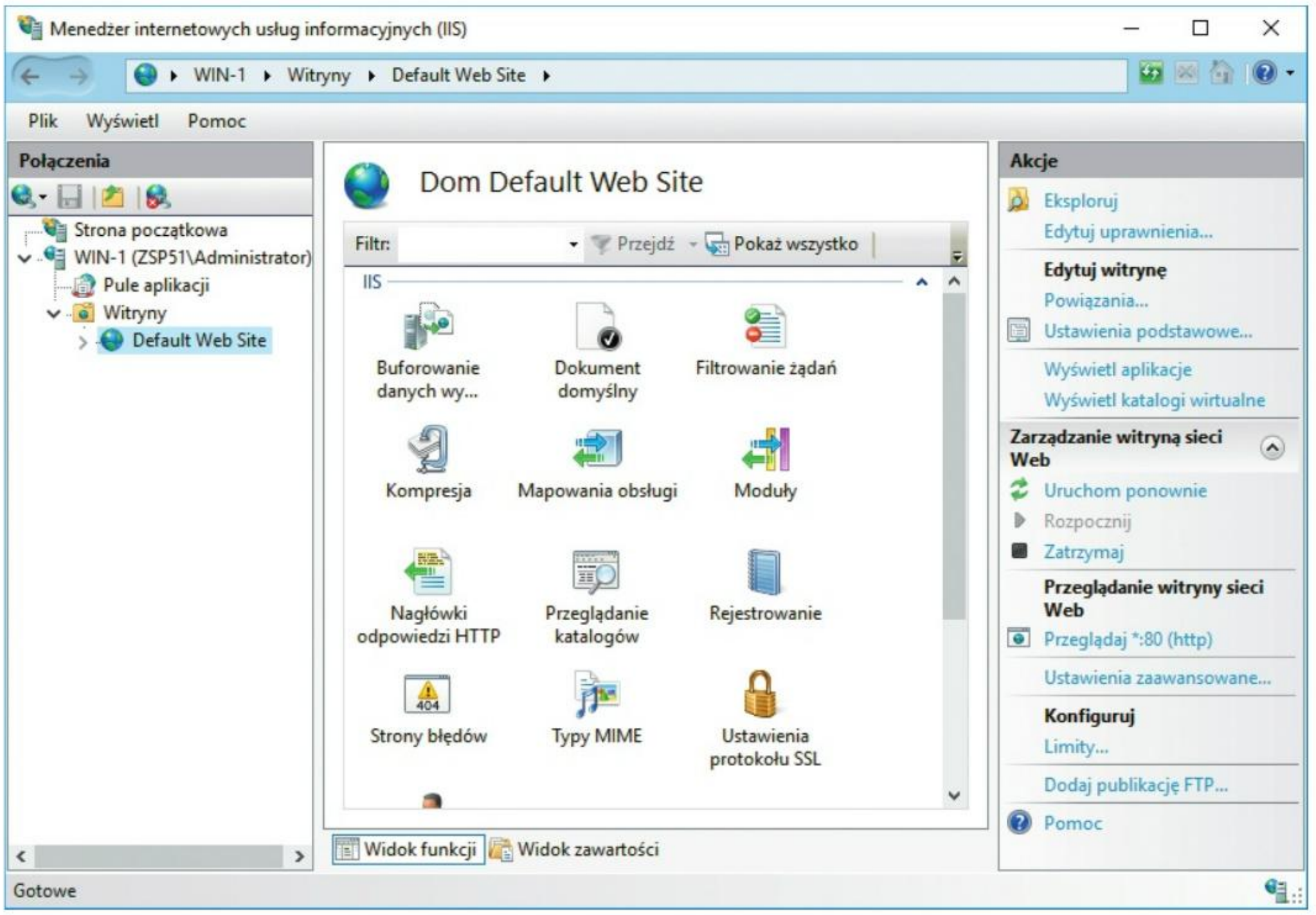
Funkcje Menedżera internetowych usług informacyjnych **Utworzenie nowej witryny FTP** **Skonfigurowanie komunikatów wyświetlanych w czasie pracy serwera** **Utworzenie i skonfigurowanie nowej witryny WWW** **Konfigurowanie ustawień witryny zależnie od potrzeb użytkownika**

Internet Information Services (IIS) to zbiór usług internetowych dla systemów rodziny Microsoft Windows. Usługi umożliwiają użytkownikowi obsługę własnej witryny sieci WWW i FTP w internecie lub intranecie. Wspomniane usługi są składnikiem opcjonalnym systemu i należy je zainstalować dodatkowo po instalacji systemu. Jeśli usługa IIS nie jest zainstalowana, należy zainstalować odpowiednie komponenty. W tym celu można posłużyć się kreatorem dostępnym w oknie **`Menedżer serwera`** i dodać rolę **`Serwer sieci Web (IIS)`**. Podczas instalacji trzeba wykonywać polecenia kreatora, a w celu zapewnienia obsługi witryn FTP w oknie **`Wybieranie usług ról`** zaznaczyć opcje **`Serwer FTP`** (rys. 33.1).



Rys. 33.1. Wybieranie usług ról IIS

Po zainstalowaniu IIS można zarządzać usługą za pomocą aplikacji **Menedżer internetowych usług informacyjnych (IIS)**. Aby uruchomić **Menedżera IIS**, należy w oknie **Menedżer serwera** z menu wybrać polecenie **Narzędzia**, a następnie polecenie **Menedżer internetowych usług informacyjnych (IIS)**. Menedżera IIS można uruchomić również za pomocą okna dialogowego **Uruchamianie**. W tym celu należy wybrać **Start/Uruchom**, wpisać polecenie **inetmgr** i kliknąć przycisk polecenia. Na rys. 33.2 przedstawiono okno **Menedżera IIS**.



Rys. 33.2. Okno **Menedżera IIS**

33.1. Konfigurowanie serwera FTP

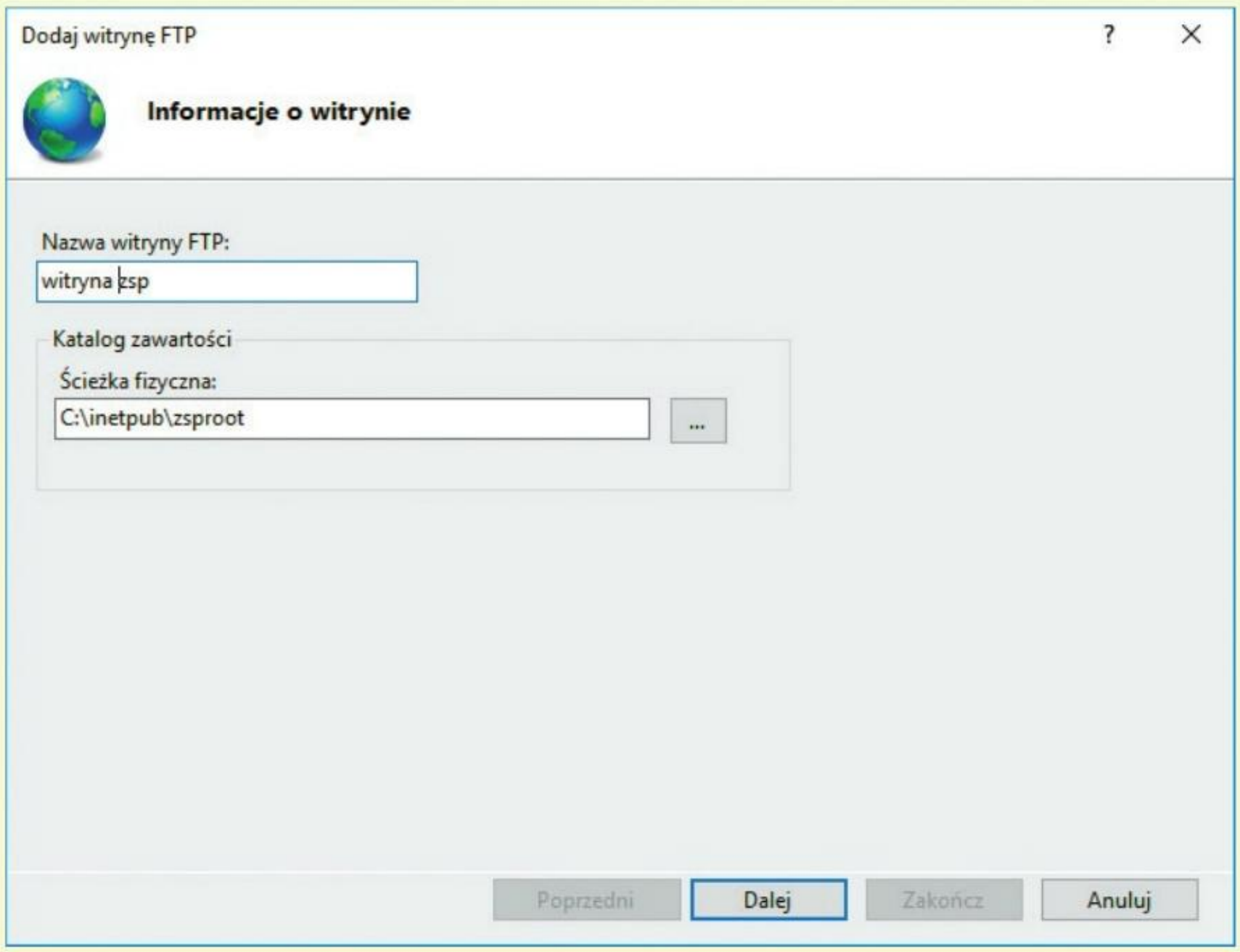
Usługa FTP jest jedną z najstarszych usług oferowanych w sieciach komputerowych. Pomimo tego powszechnie się z niej korzysta do transferu plików między komputerami i serwerami oferującymi pliki do pobrania, a także do umieszczania witryn internetowych na serwerach. Aby zarządzać usługą FTP, należy uruchomić aplikację **Menedżer internetowych usług informacyjnych (IIS)**. W gałęzi **Witryny** (rys. 33.3) można utworzyć nową witrynę FTP. W tym celu trzeba kliknąć prawym przyciskiem myszy obiekt **Witryny** i wybrać polecenie **Dodaj witrynę FTP**. Serwer musi mieć możliwość identyfikacji poszczególnych witryn, dlatego nowo tworzonej witrynie trzeba przypisać unikatowy adres IP lub unikatowy numer portu, na którym będzie nasłuchiwać na zlecenia klientów. Skonfigurowanie witryn z tymi samymi adresami i numerami portów spowoduje, że tylko jedna z nich zostanie w danym momencie uruchomiona.

PRZYKŁAD 33.1

Tworzenie nowej witryny FTP

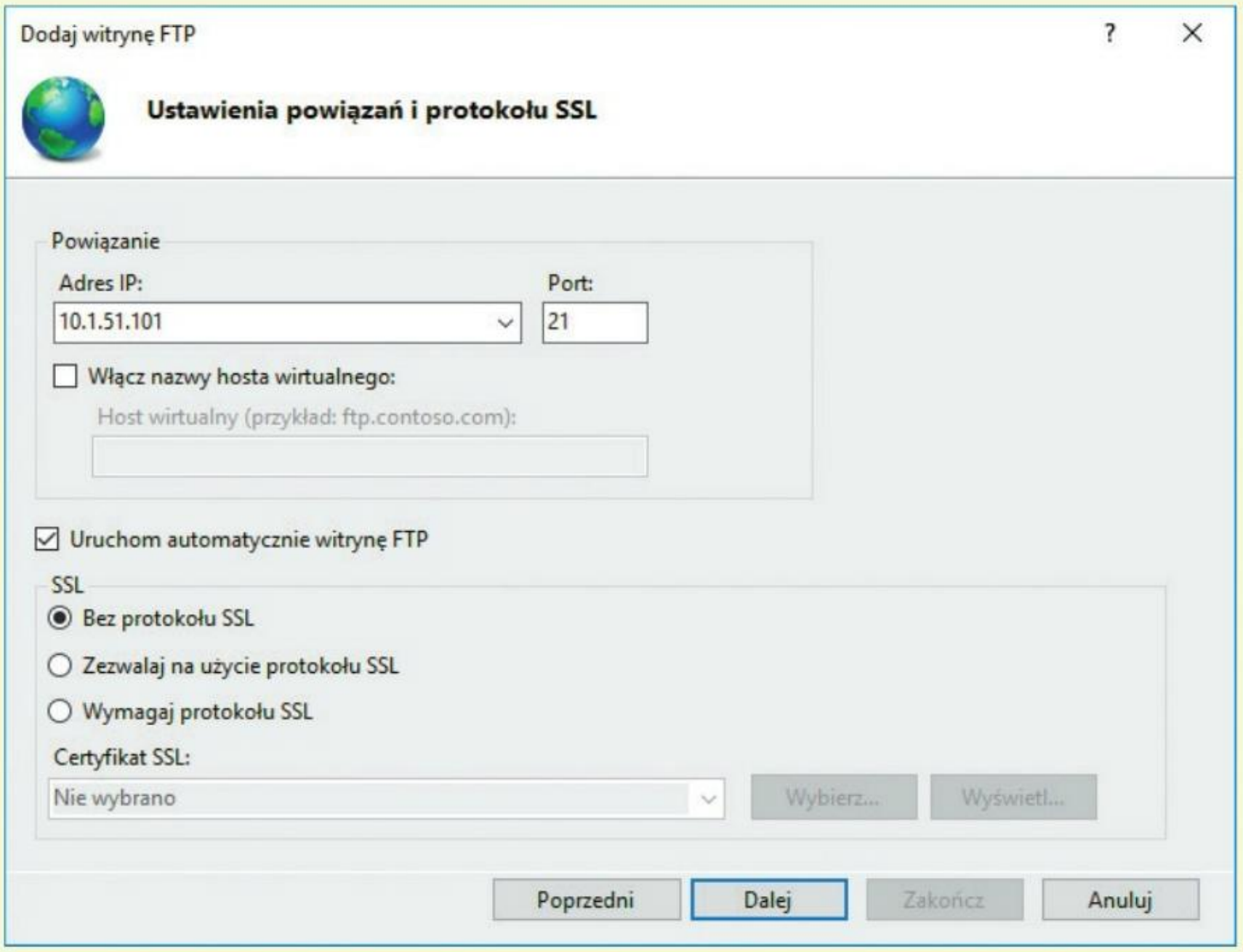
Aby utworzyć nową witrynę FTP, należy:

1. Utworzyć folder, który będzie udostępniany klientom FTP. Dla nowej witryny można utworzyć folder **`C:\inetpub\zsproot`**.
2. Kliknąć prawym przyciskiem myszy gałąź **`Witryny`**, a następnie wybrać z menu kontekstowego opcję **`Dodaj witrynę FTP`**.
3. Wprowadzić nazwę witryny w polu **`Nazwa witryny FTP`**, np. **`witryna zsp`**.
4. Wprowadzić ścieżkę do folderu domowego FTP, np. **`C:\inetpub\zsproot`** (rys. 33.3). Kliknąć przycisk **`Dalej`**.

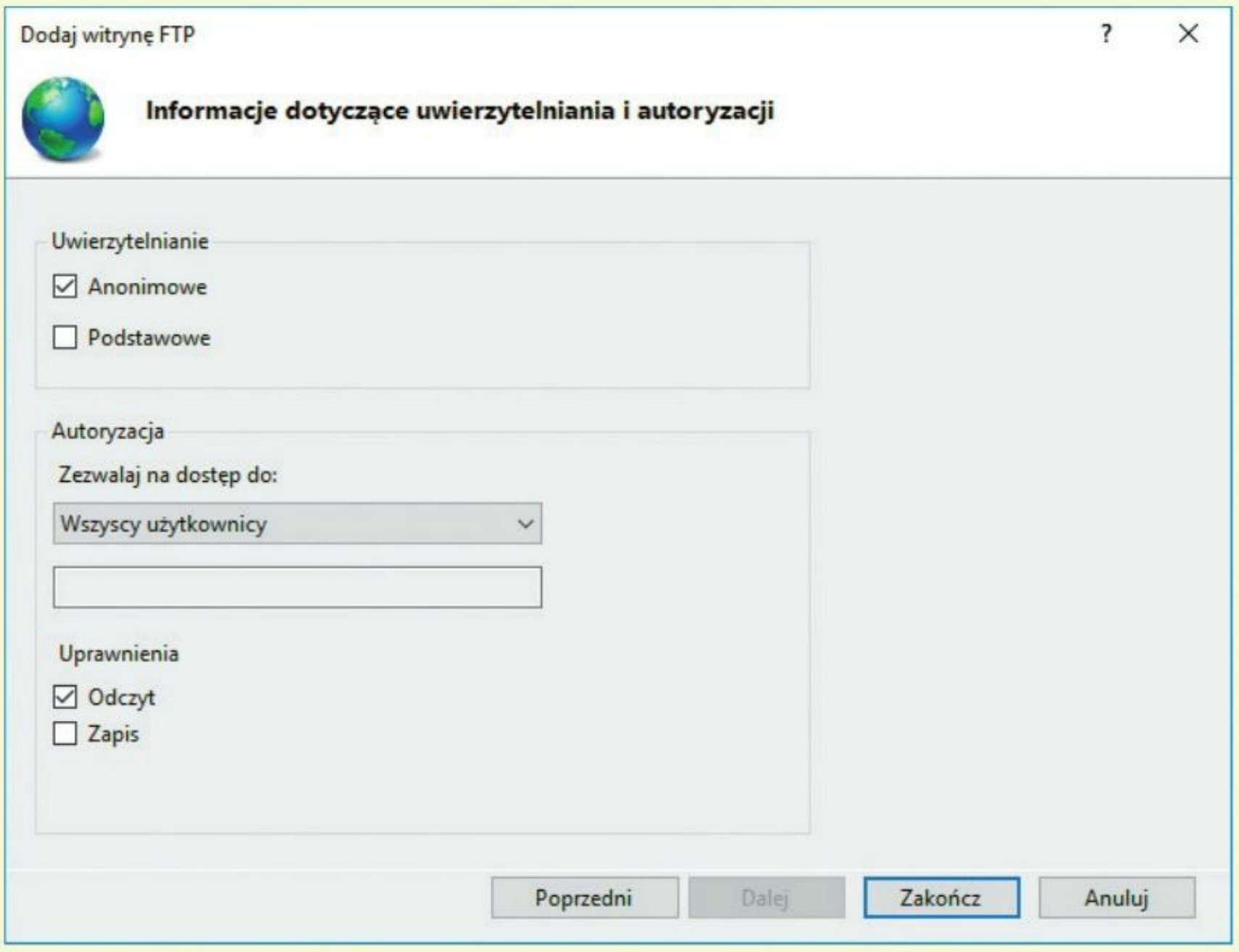


Rys. 33.3. **Okno informacji o witrynie**

5. Wybrać adres IP z listy lub/i zmienić numer portu, na którym witryna ma być dostępna. Zaznaczyć opcję **`Uruchom automatycznie witrynę FTP`**. Jeżeli witryna nie wymaga szyfrowania przesyłanych danych, zaznaczyć opcję **`Bez protokołu SSL`** (rys. 33.4). Kliknąć przycisk **`Dalej`**.
6. Wprowadzić informacje dotyczące uwierzytelniania i autoryzacji, np. uwierzytelnianie anonimowe, zezwolić na dostęp wszystkim użytkownikom tylko do odczytu (rys. 33.5). Kliknąć przycisk **`Zakończ`**.



Rys. 33.4. **Okno ustawienia powiązań i protokołu SSL**



Rys. 33.5. **Okno informacji dotyczących uwierzytelniania i autoryzacji**

! UWAGA

Zapora sieciowa może blokować możliwość nawiązywania połączeń z serwerem FTP. Aby umożliwić nawiązywanie połączeń, należy wyłączyć zaporę (niebezpieczne i niezalecane) lub skonfigurować reguły zezwalające na komunikację na port 20 i 21 i zezwolić aplikacji **`svchost.exe`** (Proces hosta dla usług systemu Windows) na dostęp.

Konfiguracja zapory składa się z następujących kroków:

1. Uruchomić **`Panel sterowania/System i zabezpieczenia/Zapora systemu Windows`**.
2. W gałęzi **`Ustawienia zaawansowane`** wybrać opcję **`Reguły przychodzące`**.
3. Kliknąć polecenie **`Nowa reguła`**.
4. W kreatorze nowej reguły ustawić regułę dla portów 20 i 21 protokołu TCP.
5. Wybrać zezwalanie na połączenie.
6. Zastosować regułę dla profili domenowego, prywatnego i publicznego.
7. Wprowadzić nazwę, np. przepuszczanie FTP i opis reguły.

Zezwolenie na komunikację aplikacji składa się z następujących kroków:

1. Uruchomić **`Panel sterowania/System i zabezpieczenia/Zapora systemu Windows`**.
2. W gałęzi **`Zezwalaj aplikacji lub funkcji na dostęp przez zaporę systemu Windows`** kliknąć przycisk **`Zezwalaj na dostęp innej aplikacji`**, a następnie przycisk **`Przeglądaj`**.
3. W oknie wyszukiwania wpisać **`svchost`** i wskazać aplikację **`svchost.exe`**. Kliknąć przycisk **`Otwórz`**, a następnie **`OK`**.
4. Zezwolić (zaznaczyć odpowiednie opcje) aplikacji **`Proces hosta dla usług systemu Windows`** na dostęp w profilach domenowym, prywatnym i publicznym. Kliknąć przycisk **`OK`**.

Po zakończeniu działania kreatora można sprawdzić i ewentualnie zmodyfikować konfigurację witryny w oknie właściwości witryny. W oknie właściwości witryny znajdują się zakładki, za pomocą których można skonfigurować m.in. następujące elementy:

- **Izolowanie użytkowników** – dzięki tej funkcji każdy logujący się do FTP, mający konto w systemie, będzie automatycznie przekierowany do własnego folderu i nie będzie mógł wyjść powyżej niego.
- **Komunikaty** – pozwala zdefiniować komunikaty wyświetlane w czasie pracy serwera:
  - **Transparent** – komunikat wyświetlany przed zalogowaniem się do systemu;
  - **Zapraszamy** – komunikat wyświetlany po zalogowaniu;
  - **Zakończ** – komunikat wyświetlany po wylogowaniu.

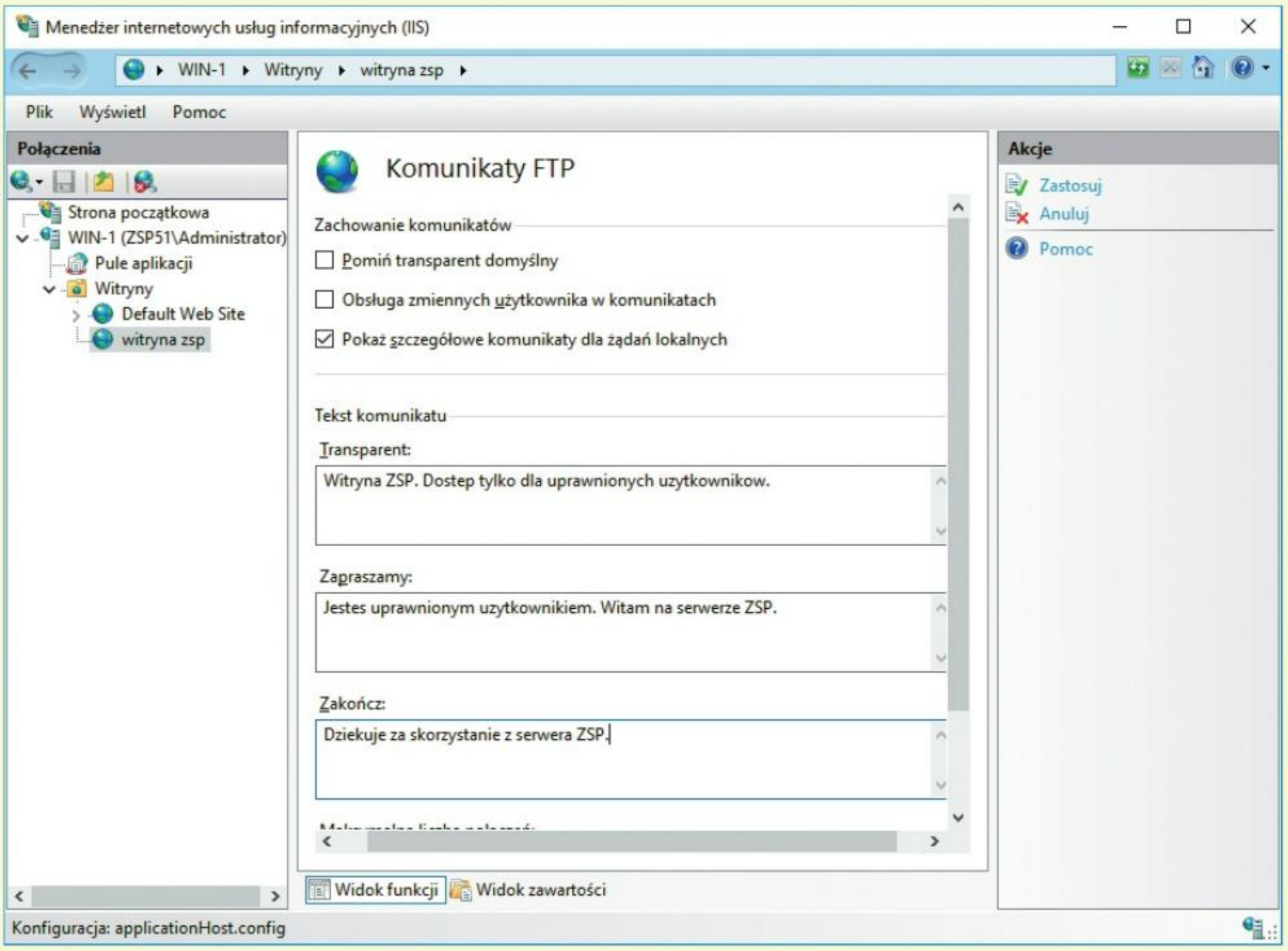
PRZYKŁAD 33.2

Konfigurowanie komunikatów wyświetlanych w czasie pracy serwera

Aby skonfigurować komunikaty wyświetlane w czasie pracy serwera, należy:

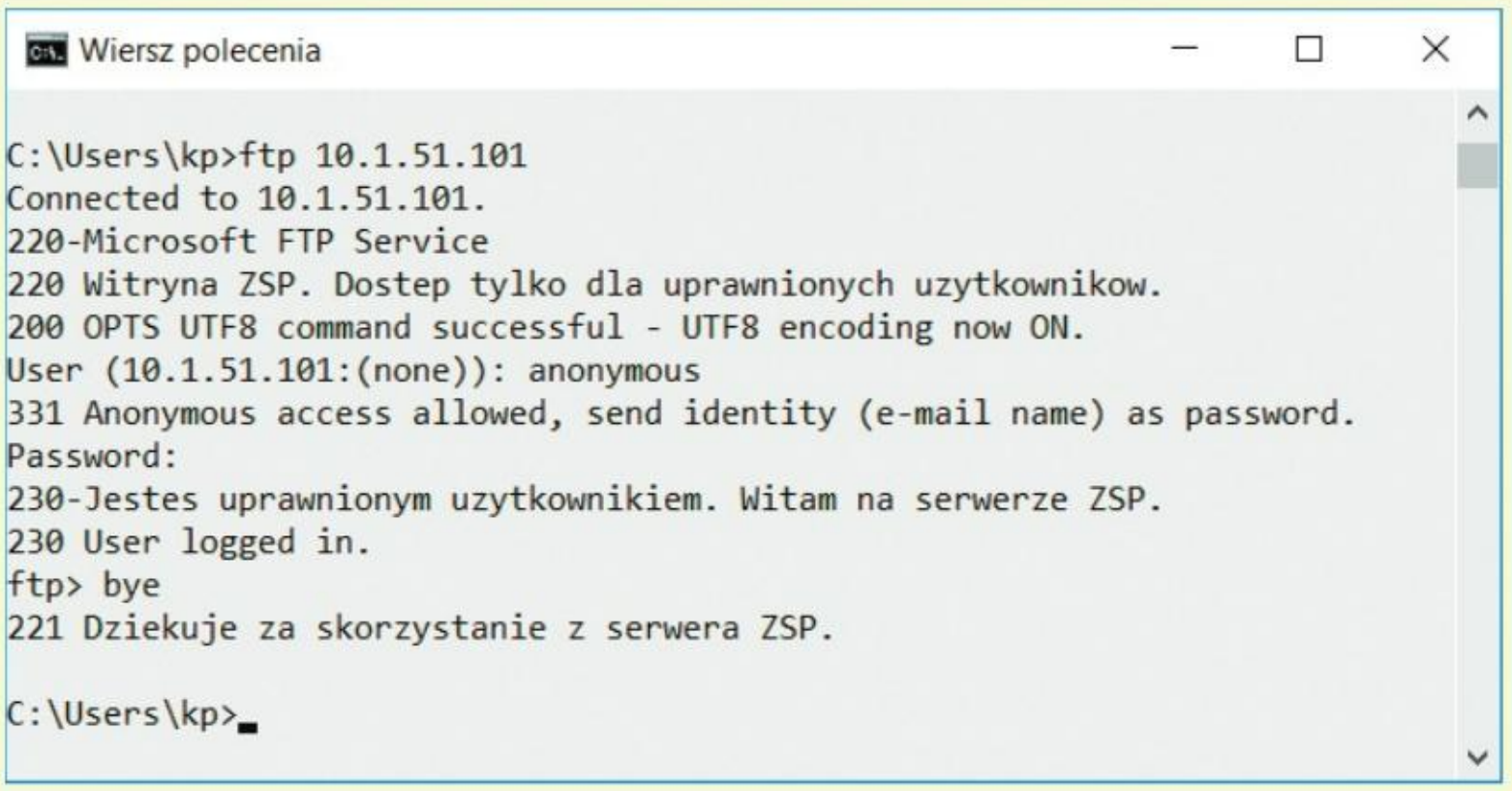
1. Kliknąć na ikonę witryny i w prawym panelu wybrać **`Komunikaty FTP`**.
2. W sekcji **`Tekst komunikatu`** wprowadzić treść komunikatów, np. jak na rys. 33.6:
   - Transparent – „Witryna ZSP. Dostęp tylko dla uprawnionych użytkowników”;
   - Powitanie – „Jesteś uprawnionym użytkownikiem. Witam na serwerze ZSP”;
   - Zakończenie – „Dziękuję za skorzystanie z serwera ZSP”.

3. Kliknąć odnośnik **`Zastosuj`**.



Rys. 33.6. **Wprowadzanie komunikatów wyświetlanych w czasie pracy serwera**

4. Przetestować działanie serwera.



Rys. 33.7. **Przebieg sesji FTP z wyświetlonymi komunikatami**

Przebieg sesji FTP z wyświetlonymi komunikatami przedstawiono na rys. 33.7

33.2. Konfigurowanie serwera WWW

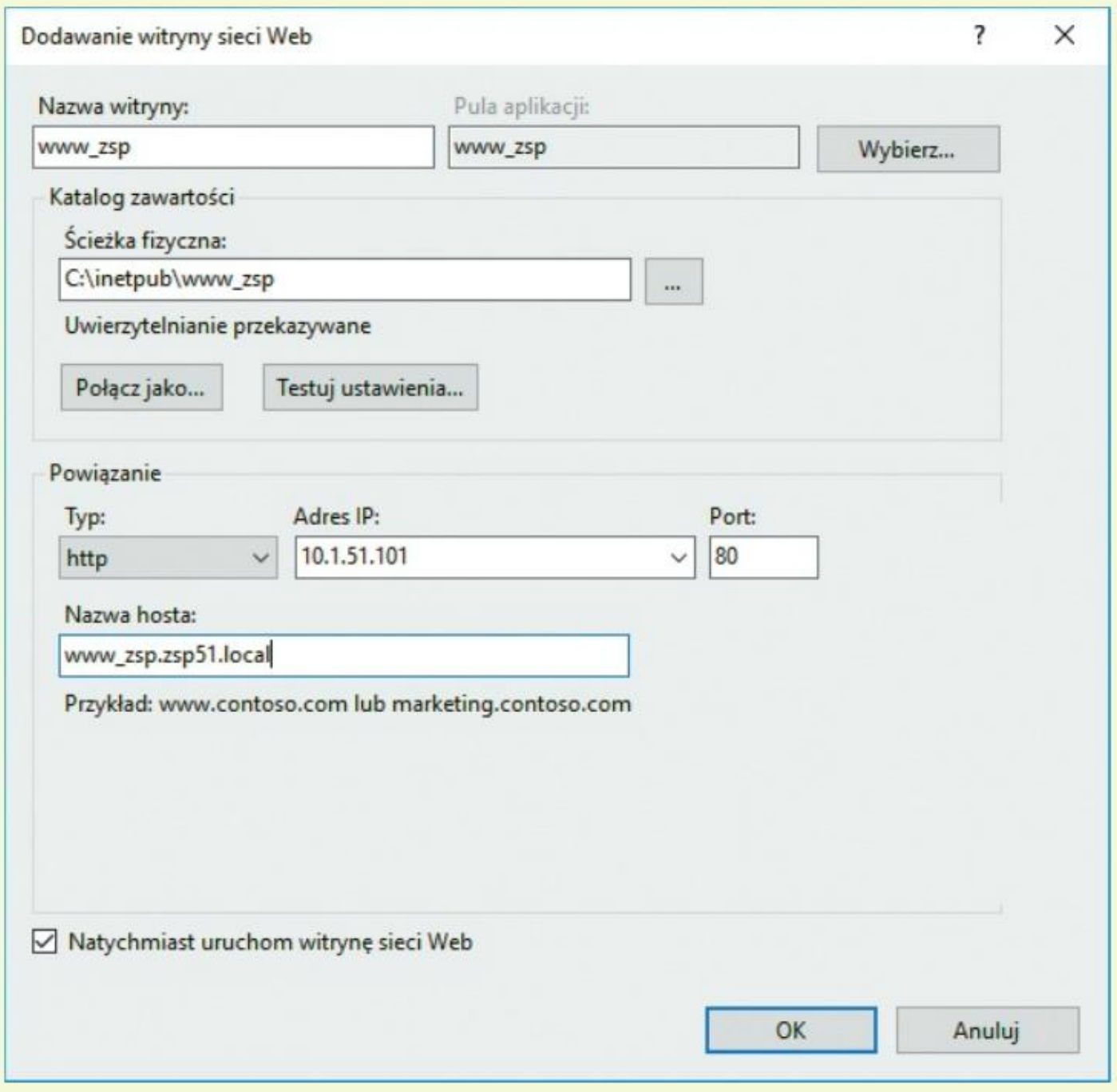
W gałęzi **Witryny** aplikacji **Menedżer internetowych usług informacyjnych (IIS)** standardowo jest skonfigurowana **Domyślna witryna sieci Web** (ang. *Default Web Site*). Na podstawie tej witryny można dokonać analizy konfiguracji i zmian mających na celu dostosowanie jej działania do potrzeb użytkownika. Można również utworzyć nową witrynę.

PRZYKŁAD 33.3

Tworzenie nowej witryny WWW

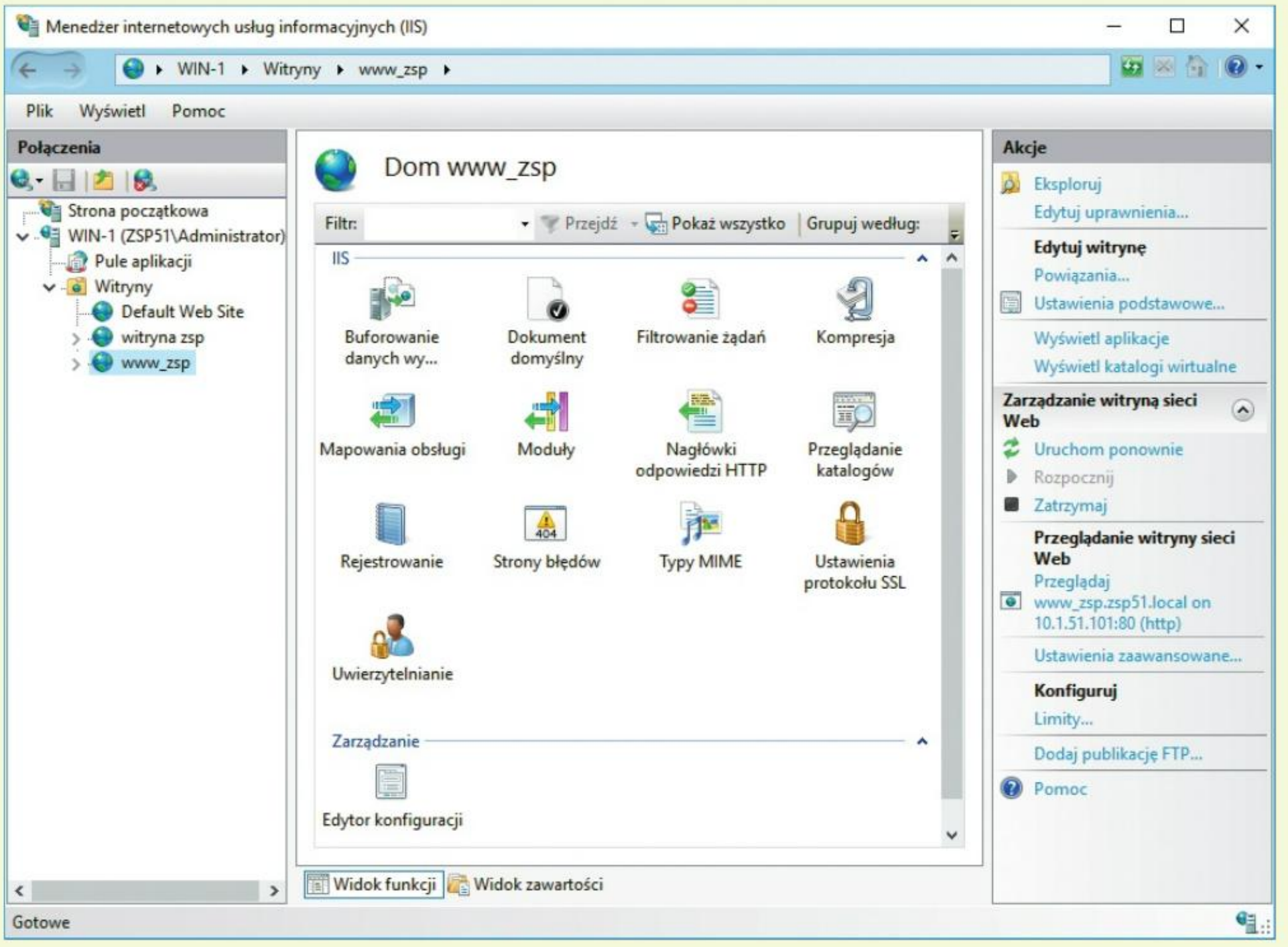
Aby utworzyć nową witrynę sieci Web, należy:

1. Utworzyć folder, w którym będą udostępniane pliki. Domyślna witryna sieci Web używa folderu **C:\Inetpub\wwwroot**, dla nowej witryny można utworzyć folder, np. **C:\Inetpub\www_zsp**.
2. Kliknąć prawym przyciskiem myszy gałąź **Witryny**, a następnie wybrać z menu kontekstowego **Dodaj witrynę sieci Web**.
3. W oknie **Dodawanie witryny sieci Web** wprowadzić nazwę witryny, np. **www_zsp**. W pole Ścieżka fizyczna wprowadzić ścieżkę do folderu zawierającego pliki witryny sieci Web, np. **C:\Inetpub\www_zsp**. Wybrać adres IP z listy lub/i zmienić numer portu, na którym witryna ma być dostępna. Wybranie opcji **Wszystkie nieprzypisane** spowoduje, że serwer będzie odpowiadał na zapytania ze wszystkich interfejsów sieciowych. W polu **Nazwa hosta** wpisać adres witryny. Adres musi być wpisany dokładnie tak, jak został zapisany w pliku **hosts** lub w danych serwera DNS. Na rys. 33.8 przedstawiono okno tworzenia nowej witryny internetowej.



Rys. 33.8. **Okno tworzenia nowej witryny internetowej**

Po zakończeniu działania kreatora możemy sprawdzić i ewentualnie zmodyfikować konfigurację witryny w oknie właściwości witryny (rys. 33.9).



Rys. 33.9. **Okno właściwości witryny**

W oknie **`Właściwości witryny`** znajduje się wiele ikon, za pomocą których można skonfigurować ustawienia witryny, np. **`Dokument domyślny`** – określa listę plików, które będą przeszukiwane w wypadku, gdy adres URL będzie się kończył na nazwie folderu. W internecie przyjęto, że przeglądanie stron rozpoczyna się od pliku **`index.html`**. Jeżeli takiego pliku nie ma na liście, należy go dopisać i najlepiej przenieść do góry (pliki są poszukiwane w kolejności jak na liście).

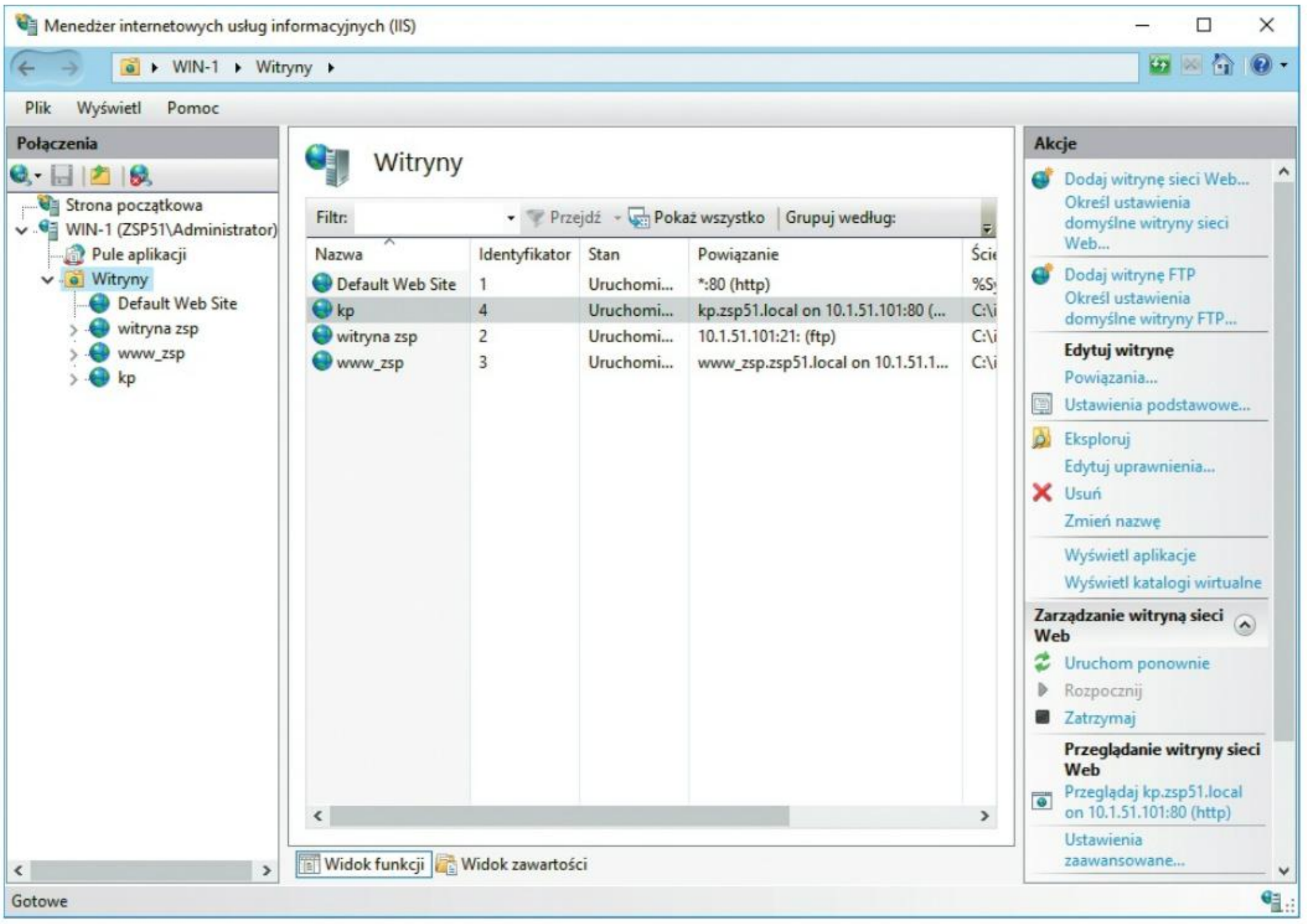
Serwer internetowych usług informacyjnych (IIS) pozwala skonfigurować komputer do udostępniania wielu różnych i odseparowanych od siebie witryn sieci WWW. Każda z nich jest udostępniana przez inny wirtualny serwer i może mieć inną zawartość oraz uprawnienia użytkowników. Wirtualne serwery mogą być rozróżniane za pomocą:

- **adresu IP**, który jest przypisany witrynie sieci WWW;
- **numeru portu TCP**, który jest przypisany witrynie sieci WWW;
- **nazwy hosta**, która jest przypisana witrynie sieci WWW.

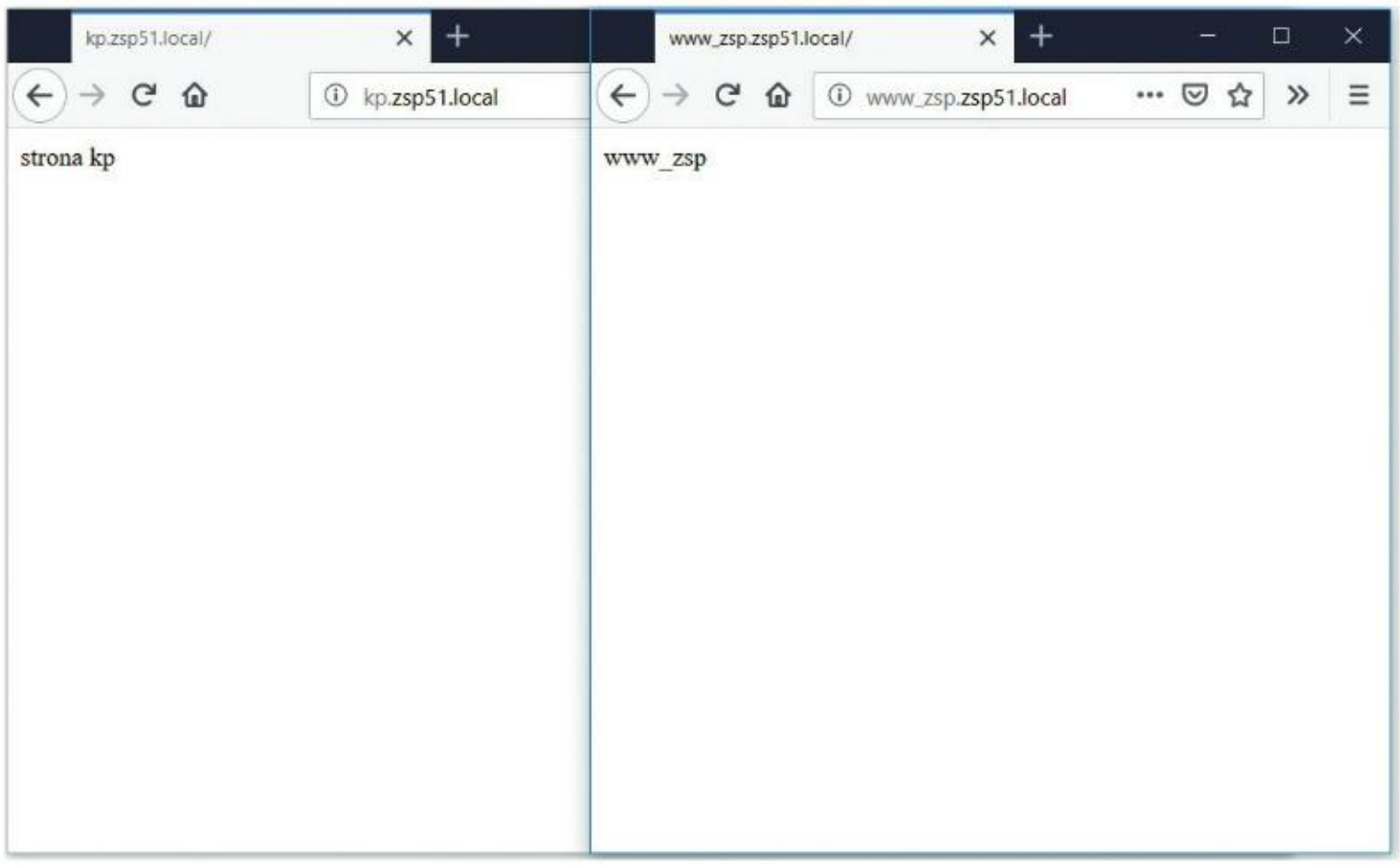
Oznacza to, że na serwerze IIS może być wiele witryn sieci WWW działających na tym samym adresie IP i używających tego samego portu domyślnego (80), jeśli każdemu serwerowi wirtualnemu zostanie przypisana unikatowa nazwa hosta. Nazwa hosta jest pobierana z okna adresu przeglądarki (np. www.onet.pl). Musi istnieć w sieci mechanizm odwzorowania nazw hostów na adresy IP. Nazwy muszą być rozróżniane przez system DNS. Wpisany w przeglądarkę adres

strony, np. **www_zsp.zsp51.local**, powinien zostać skojarzony z odpowiednim adresem IP serwera. W razie braku dostępu do serwera DNS należy zmodyfikować pliki **hosts** w każdym komputerze w sieci, korzystającym z wirtualnych serwerów.

Na rys. 33.10 przedstawiono konfigurację dwóch serwerów wirtualnych: **kp.zsp51.local** i **www_zsp.zsp51.local**. Odpowiednie nazwy zostały dopisane do systemu DNS. Wynik testowania działania wirtualnych serwerów przedstawiono na rys. 33.11.



Rys. 33.10. Konfiguracja wirtualnych serwerów WWW



Rys. 33.11. Testowanie wirtualnych serwerów WWW

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Utwórz nową witrynę FTP. Zaplanuj treść komunikatów wyświetlanych przez serwer przed logowaniem i po nim. Zmodyfikuj konfigurację tak, aby serwer wyświetlał komunikaty. Przetestuj działanie witryny.
2. Uruchom witrynę tak, aby serwer oczekiwał na połączenia na niestandardowym porcie wskazanym przez nauczyciela. Przetestuj działanie witryny.
3. W systemie Windows Server zainstaluj wszystkie wymagane sterowniki. Wykonaj konfigurację kart grafiki i sieciowej. Sprawdź dzienniki zdarzeń powstałe podczas instalacji.
4. Utwórz konta domenowe pięciu koleżankom / kolegom i grupę *znajomi*. Przypisz koleżanki / kolegów do grupy *znajomi*. Ogranicz czas logowania na konta tylko do okresu, w którym odbywają się zajęcia w szkole.
5. Utwórz katalog dostępny dla wszystkich koleżanek / kolegów. Nadaj odpowiednie uprawnienia.
6. Zainstaluj drukarkę i udostępnij ją w sieci.
7. Zmień konfigurację serwera tak, aby domyślnie była wczytywana strona o nazwie **`strona.html`**. Zmień kolejność nazw tak, aby **`strona.html`** była wczytywana pierwsza.
8. Skonfiguruj wirtualne serwery WWW dla każdej z klas technikum informatycznego w twojej szkole. Umieść przykładowe strony i przetestuj działanie serwerów.
9. Uruchom serwer WWW tak, aby oczekiwał na połączenia na porcie **`2080`**. Przetestuj działanie witryny.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wymień zalety i wady architektury *peer-to-peer* i klient–serwer.
2. Jaka jest różnica między minimalnymi i zalecanymi wymaganiami systemu operacyjnego?
3. Jaka jest rola pamięci wirtualnej?
4. Jakie systemy i mechanizmy zwiększające bezpieczeństwo są stosowane w serwerach, a jakie w stacjach roboczych?

34 Konfigurowanie usługi RRAS

ZAGADNIENIA

Funkcje usługi RRAS **Konfigurowanie usług RRAS** **Korzystanie z usług RRAS** **Cel korzystania z usługi zdalnego dostępu** **Funkcje Wirtualnych Sieci Prywatnych** **Sposób nadawania uprawnień do logowania się za pomocą VPN** **Zainstalowanie i skonfigurowanie usługi dostępu zdalnego** **Skonfigurowanie połączenia sieciowego klienta VPN** **Konfigurowanie roli routingu między sieciami lokalnymi w Windows Server 2016** **Testowanie routingu między sieciami lokalnymi w Windows Server 2016**

Routing i dostęp zdalny RRAS (ang. *Remote and Routing Access*) to usługa, która obsługuje routing sieciowy protokołów IPv4 i IPv6 oraz łączność użytkowników zdalnych za pomocą wirtualnej sieci prywatnej (VPN) typu *site-to-site* lub połączeń telefonicznych. Funkcja **dostępu zdalnego** zapewnia usługi sieci VPN, dzięki czemu użytkownicy mogą uzyskać bezpieczny dostęp do sieci firmowych przez internet tak, jakby byli bezpośrednio połączeni. Usługa RRAS może również odgrywać rolę **programowego routera**. Z usług routingu mogą korzystać organizacje w sieciach lokalnych LAN, sieci rozległych WAN i przez internet za pomocą bezpiecznych połączeń wirtualnej sieci prywatnej VPN. Usługa Routing i dostęp zdalny udostępnia również usługi translacji adresów sieciowych NAT.

PRZYKŁAD 34.1

Instalowanie roli RRAS

Instalacje roli RRAS można przeprowadzić za pomocą kreatora uruchamianego w oknie **`Menedżera serwera`**. Aby zainstalować usługę, należy:

1. Zainstalować w systemie dwie karty sieciowe. Jedna z kart umożliwi dostęp do internetu, druga – komunikację z urządzeniami w sieci lokalnej.
2. W oknie **`Menedżer serwera`** kliknąć odnośnik **`Dodaj role i funkcje`**, wskazać opcję **`Instalacja oparta na rolach lub oparta na funkcjach`** oraz serwer do zainstalowania usługi. Kliknąć przycisk **`Dalej`**.
3. Zaznaczyć usługę **`Dostęp zdalny`** (ang. *Remote Access*). Kliknąć przycisk **`Dalej`**.
4. Zatwierdzić wybór funkcji. Kliknąć przycisk **`Dalej`**.
5. Po zapoznaniu się z informacjami o usłudze RRAS kliknąć przycisk **`Dalej`**.
6. Zaznaczyć role **`DirectAccess i VPN (RAS)`** oraz **`Routing`**. Dodać funkcje niezbędne do działania usług. Kliknąć przycisk **`Dalej`**.
7. Kliknąć przycisk **`Zainstaluj`**, a po zakończeniu działania kreatora kliknąć przycisk **`Zamknij`**.
8. Po zainstalowaniu usługi dostępu zdalnego należy ją skonfigurować i uruchomić.

34.1. Sieci wirtualne VPN – narzędzia dostępu zdalnego do serwera

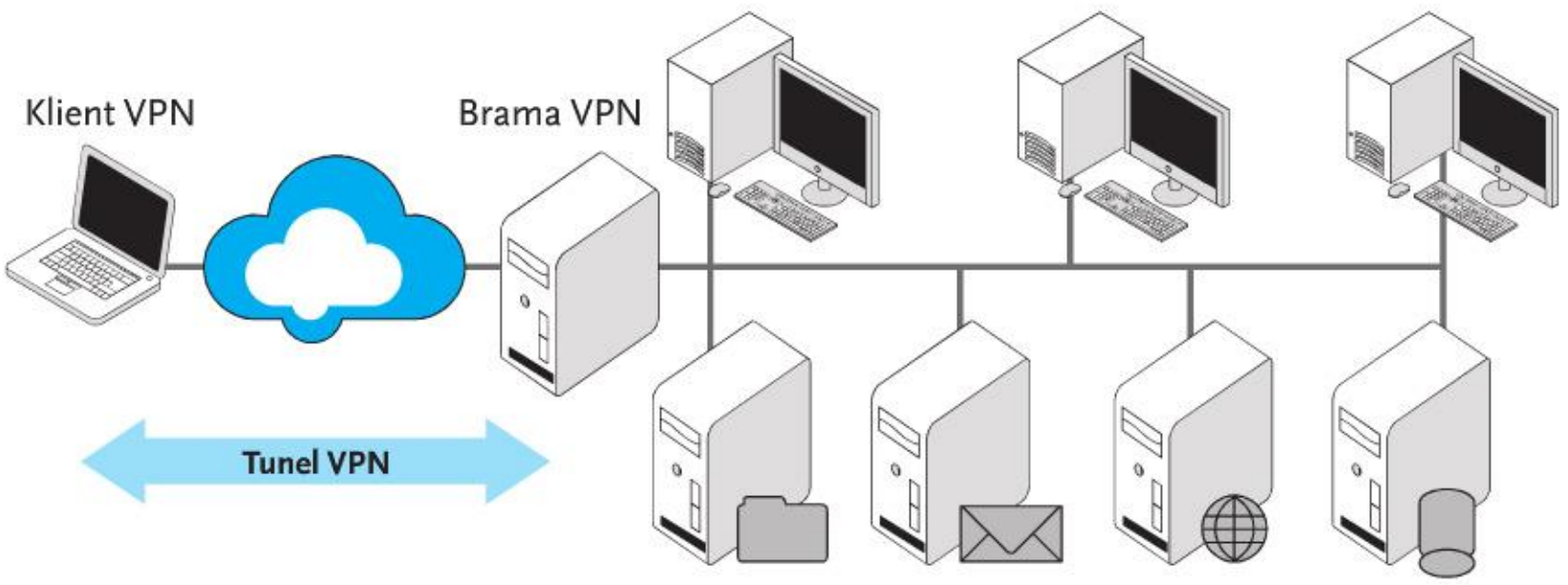
Dostęp zdalny jest usługą umożliwiającą użytkownikom znajdującym się poza siecią uzyskanie dostępu do zasobów zlokalizowanych w sieci. Jednym ze sposobów uzyskania zdalnego dostępu do zasobów znajdujących się w sieci lokalnej było skorzystanie z linii telefonicznej. Połączenia telefoniczne odbywały się za pomocą modemów przez normalne linie telefoniczne i miały maksymalną prędkość 56 kb/s. Ze względu na niskie prędkości i wysokie koszty te rozwiązania nie są już powszechnie stosowane. Obecnie zdalny dostęp do zasobów sieci może być realizowany za pomocą **Wirtualnych Sieci Prywatnych – VPN** (ang. *Virtual Private Network*).

Wirtualna sieć prywatna pozwala w bezpieczny sposób łączyć sieci i komputery z wykorzystaniem niezaufanego i niebezpiecznego medium, jakim jest np. internet. Transmisja między poszczególnymi sieciami i komputerami odbywa się przez szyfrowane i zabezpieczone **wirtualne tunele**. Tunel, przez który płynie ruch, jest ustanawiany między urządzeniami końcowymi tak, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Stacje końcowe mogą korzystać z VPN, jak gdyby istniało między nimi łącze fizyczne. Dane przesyłane w sieci VPN są obudowywane w specjalnym nagłówku, w którym jest określone ich miejsce docelowe. Określenie „wirtualna" oznacza, że ta sieć istnieje jedynie jako struktura logiczna działająca w ramach sieci publicznej, np. internetu. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.

Windows Server 2016 obsługuje trzy rodzaje połączeń VPN:

- **PPTP** (ang. *Point-to-Point Tunneling Protocol*) – najprostsza metoda, według której można ustanowić połączenie VPN, ale również najmniej bezpieczna (uwierzytelnienie użytkowników następuje przez niezabezpieczone połączenie, a szyfrowanie połączenia rozpoczyna się dopiero po wymianie uwierzytelnień);
- **L2TP/IPSec** (ang. *Layer Two Tunneling Protocol/Internet Protocol Security*) – wspólnie opracowany przez Microsoft i Cisco. W L2TP/IPSec zabezpieczona sesja jest ustanawiana, zanim zostaną przesłane uwierzytelnienia. IPSec zapewnia wzajemne sprawdzanie autentyczności komputerów i urządzeń, integralności danych, poufność i niezaprzeczalność;
- **SSTP** (ang. *Secure Socket Tunneling Protocol*) – korzysta z zaszyfrowanych połączeń http do ustanowienia połączenia VPN do bramki VPN. W SSTP uwierzytelnienia użytkownika nie są wysyłane do czasu, aż bezpieczny tunel SSL zostanie ustanowiony przy bramce VPN. SSTP nie ma problemów z zaporami sieciowymi i urządzeniami NAT.

Komputer z zainstalowanym Windows Server i skonfigurowaną usługą dostępu zdalnego może pełnić funkcję bramy, za pomocą której zdalni użytkownicy uzyskają dostęp do zasobów sieci lokalnej. Schemat konfiguracji sieci przedstawiono na rys. 34.1.



Rys. 34.1. Schemat wirtualnej sieci prywatnej

Serwer odgrywający rolę bramy VPN musi być wyposażony w dwie karty sieciowe (jedna dla sieci lokalnej, a druga do uzyskania połączenia z internetem). Użytkownicy sieci VPN są uwierzytelniani w usłudze Active Directory, co oznacza, że muszą mieć konta domenowe z uprawnieniami do logowania się przez VPN.

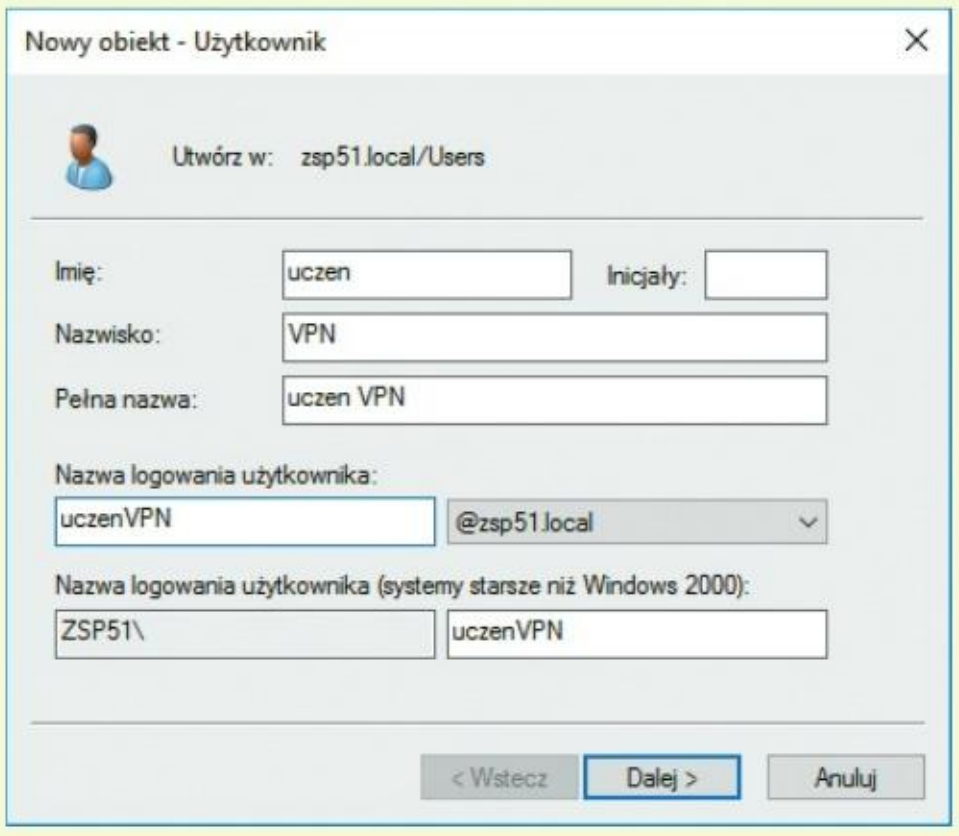
PRZYKŁAD 34.2

Tworzenie konta użytkownika do logowania się za pomocą VPN

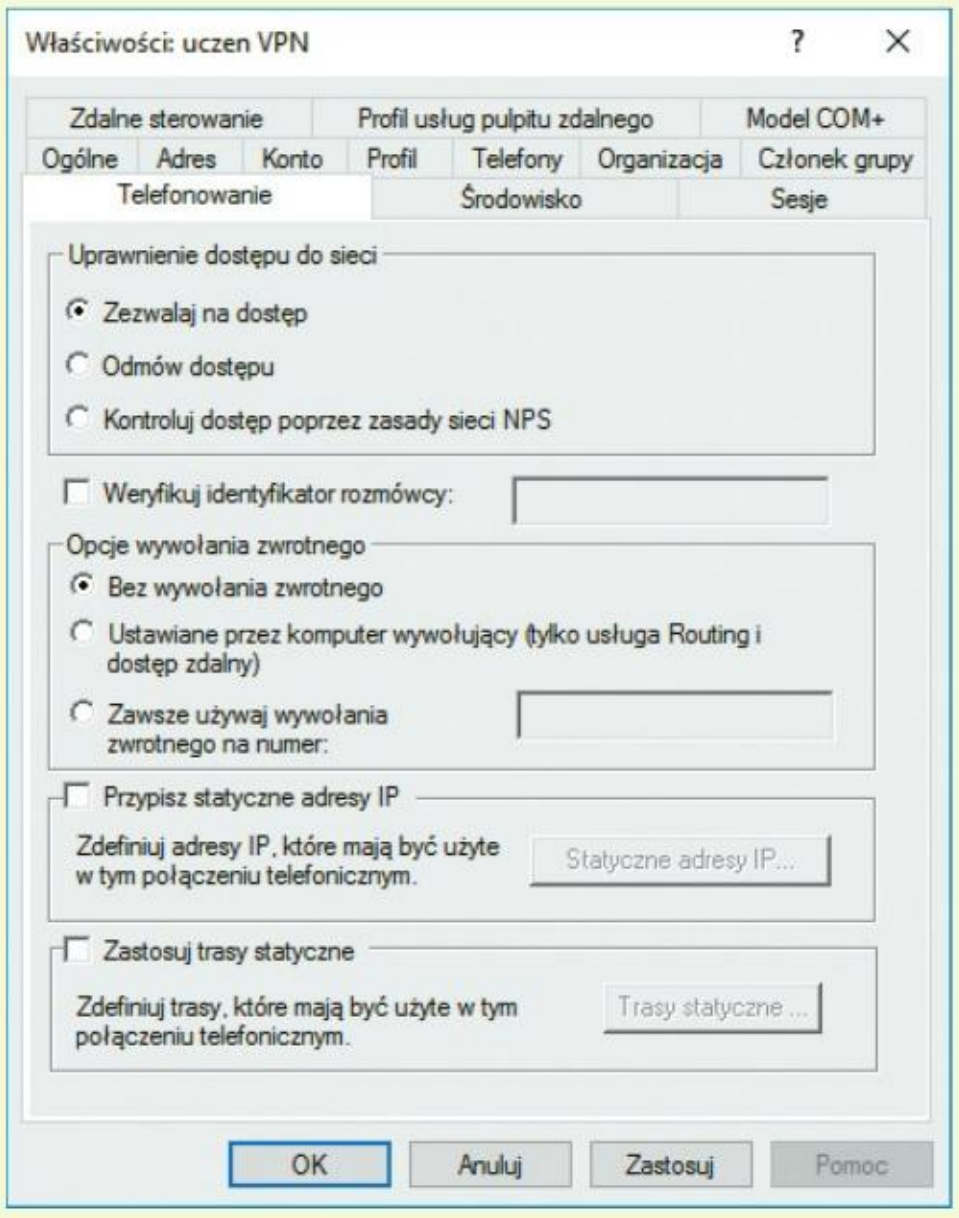
Aby użytkownik mógł połączyć się z siecią VPN, musi mieć konto domenowe z uprawnieniami do logowania się przez VPN.

Aby utworzyć konto i nadać odpowiednie uprawnienia, należy:

1. Zalogować się na serwer na konto z uprawnieniami do administrowania użytkownikami.
2. Utworzyć konto użytkownika, np. *uczenVPN* (rys. 34.2).
3. Kliknąć prawym przyciskiem myszy konto użytkownika i z menu kontekstowego wybrać **`Właściwości`**. W zakładce **`Telefonowanie`** zaznaczyć opcję **`Zezwalaj na dostęp`** (rys. 34.3).



Rys. 34.2. **Tworzenie użytkownika**



Rys. 34.3. **Nadawanie użytkownikowi uprawnienia do logowania przez VPN**

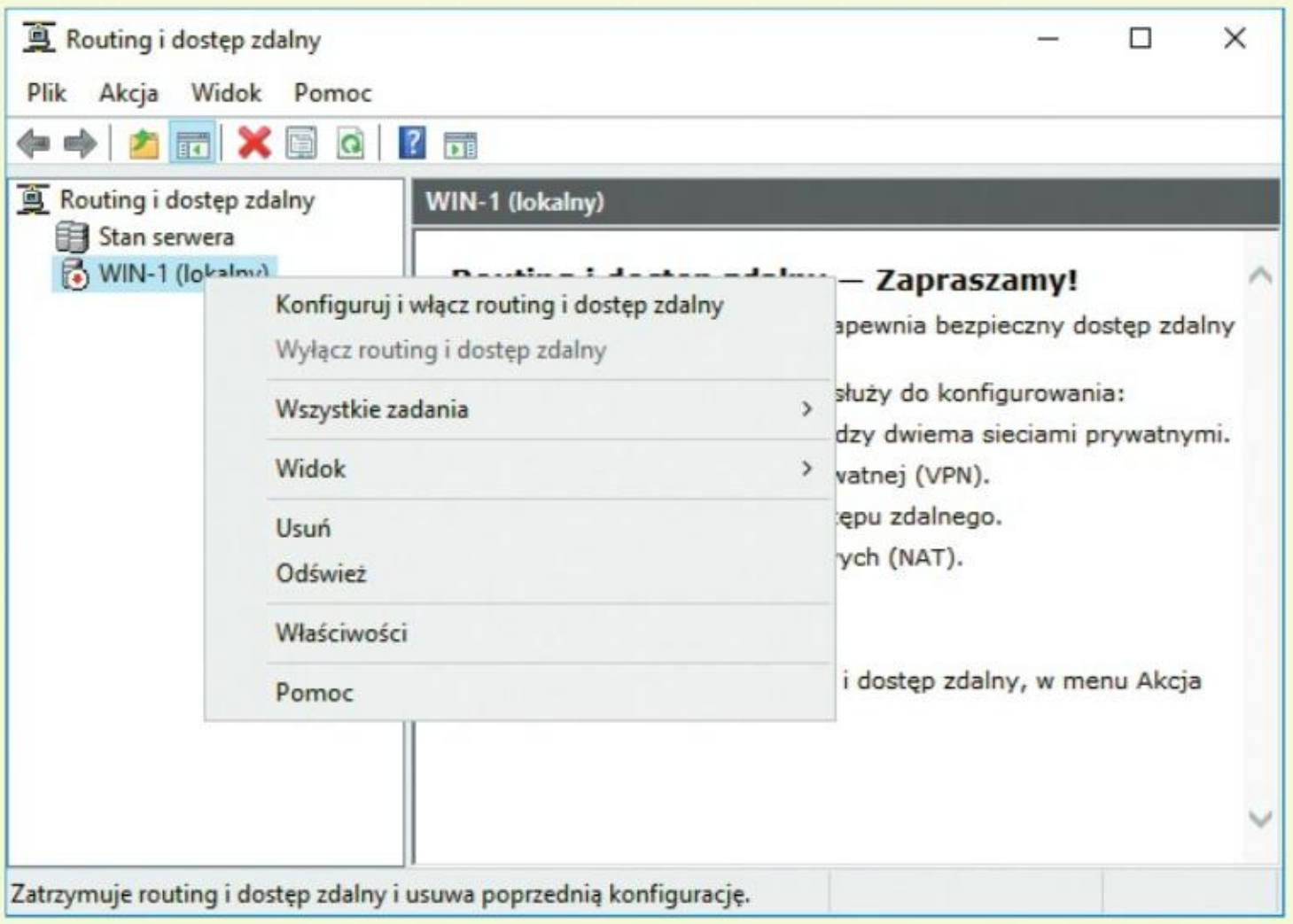
PRZYKŁAD 34.3

Konfigurowanie usługi dostępu zdalnego

Do konfigurowania dostępu zdalnego służy kreator, uruchamiany w oknie **`Menedżera serwera`**. Aby skonfigurować usługę dostępu zdalnego do pracy jako brama VPN, należy:

1. W oknie **`Menedżera serwera`** uruchomić konsolę **`Routing i dostęp zdalny`** (kliknąć **`Narzędzia/Routing i dostęp zdalny`**).

2. Kliknąć prawym przyciskiem myszy nazwę serwera i z menu kontekstowego wybrać **`Konfiguruj i włącz routing i dostęp zdalny`** (rys. 34.4).

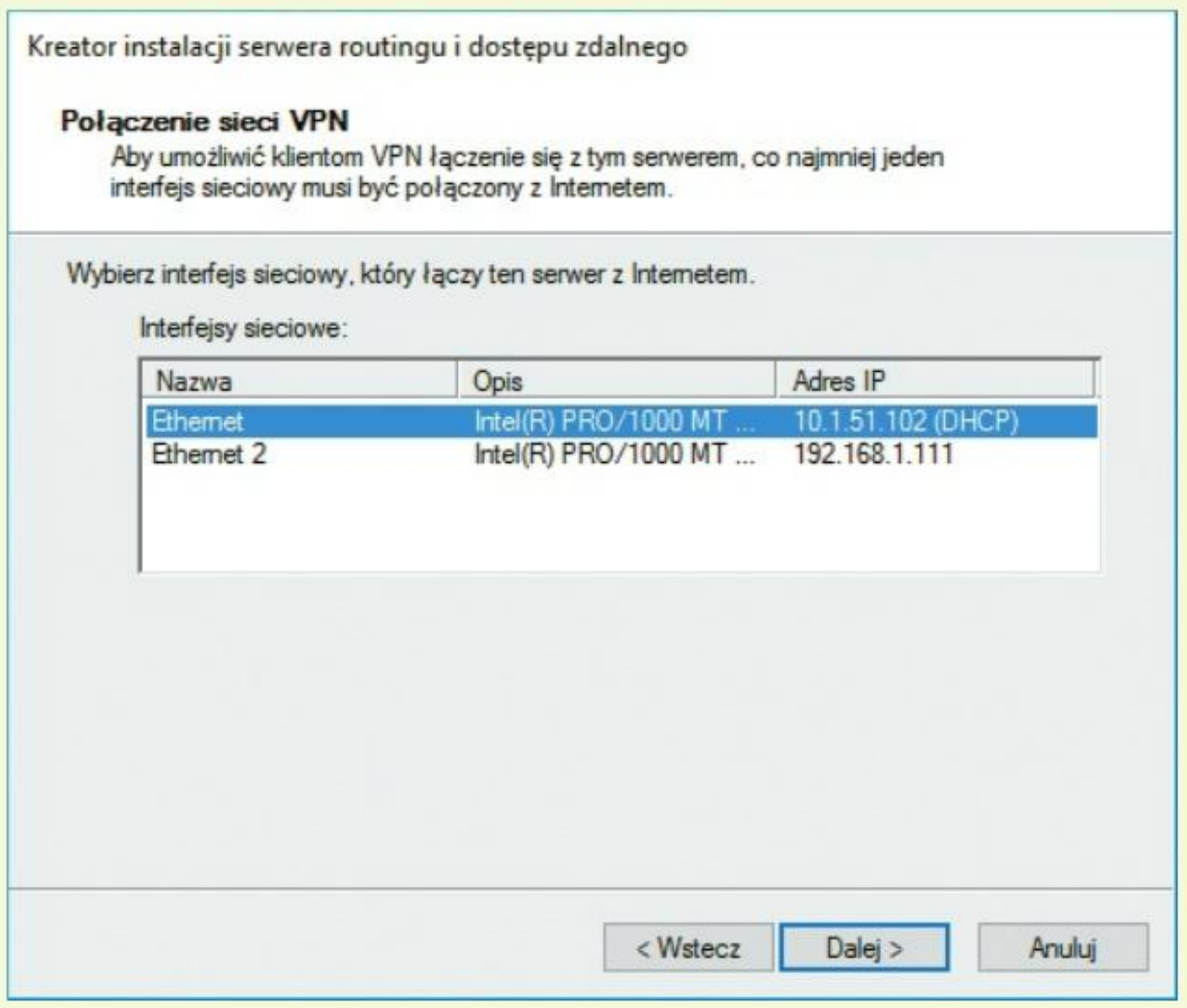


Rys. 34.4. **Uruchamianie kreatora konfiguracji dostępu zdalnego**

3. Zapoznać się z informacją w oknie powitalnym i kliknąć przycisk **`Dalej`**.

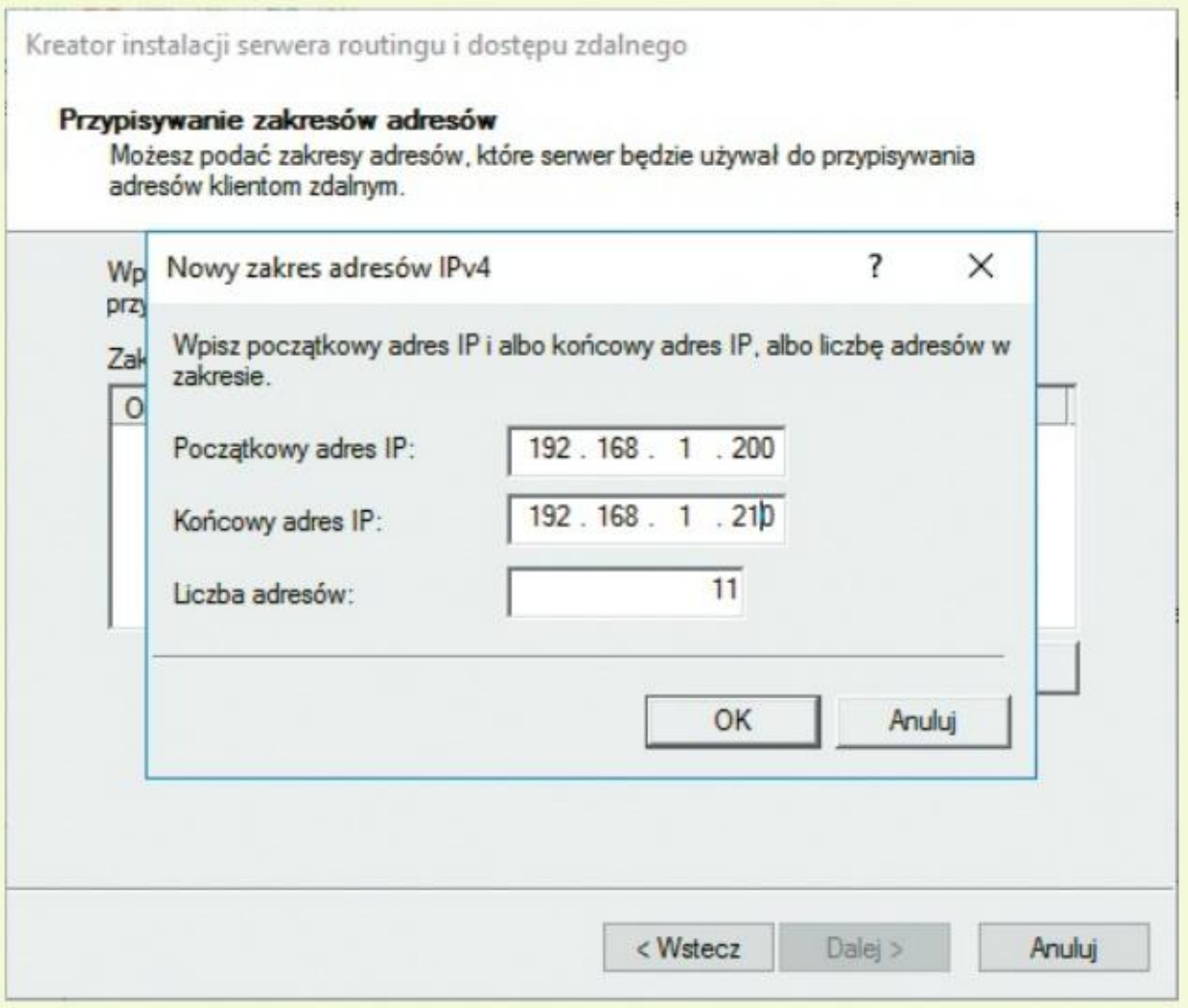
4. W oknie **`Konfiguracja`** wybrać typ usługi, np. **`Dostęp zdalny`** – jeżeli serwer ma pełnić tylko funkcję bramy VPN, lub **`Dostęp prywatnej sieci wirtualnej i translator adresów`** – jeżeli dodatkowo klienci z sieci lokalnej będą mogli łączyć się z internetem. Kliknąć przycisk **`Dalej`**.

5. W oknie **`Połączenie sieci VPN`** wskazać interfejs, którym serwer jest połączony z internetem (rys. 34.5). Kliknąć przycisk **`Dalej`**.



Rys. 34.5. **Wybór interfejsu, którym serwer jest połączony z internetem**

6. W oknie **Przypisywanie adresów IP** można zaznaczyć opcję Z **określonego zakresu adresów**, a następnie w oknie **Przypisywanie zakresów adresów** wprowadzić zakres adresów, które będą przydzielane klientom w sposób dynamiczny (rys. 34.6). Zaznaczenie opcji **Automatycznie** umożliwia przydzielanie adresów przez serwer DHCP – jeżeli istnieje i ma odpowiednio skonfigurowany zakres. Kliknąć przycisk **Dalej**.



Rys. 34.6. **Definiowanie puli adresów przydzielanych klientom VPN**

7. W dużych sieciach do uwierzytelniania może być wykorzystywany serwer **RADIUS**. W małych sieciach wystarczy uwierzytelnianie lokalne – w oknie **Zarządzanie wieloma serwerami dostępu zdalnego** trzeba wybrać opcję **Nie, użyję usługi routingu i dostępu zdalnego do uwierzytelniania żądań połączeń**. Kliknąć przycisk **Dalej**.
8. W oknie **Podsumowanie** zweryfikować wybór opcji i kliknąć przycisk **Zakończ**.
9. Po zakończeniu pracy kreatora kliknąć przycisk **Zamknij**.

Ostatnim elementem konfiguracji dostępu zdalnego jest konfigurowanie nowego połączenia sieciowego w komputerze, który będzie pełnił funkcję klienta sieci VPN. W następnym przykładzie zostanie skonfigurowane połączenie z komputera z systemem Windows 10, ale możliwe jest korzystanie z dowolnego systemu operacyjnego.

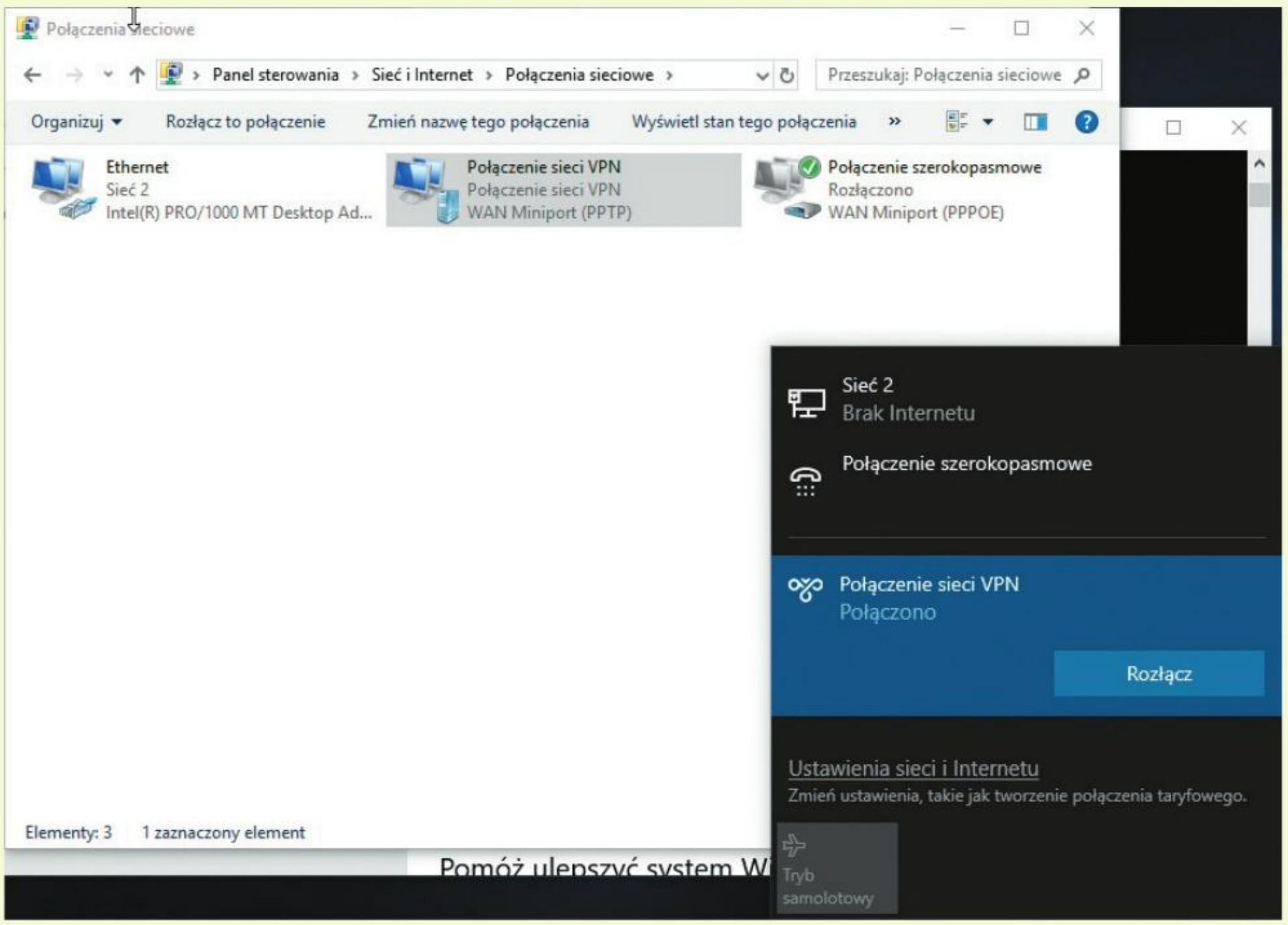
PRZYKŁAD 34.4

Konfigurowanie połączenia sieciowego klienta VPN

Aby skonfigurować nowe połączenie sieciowe klienta, należy:

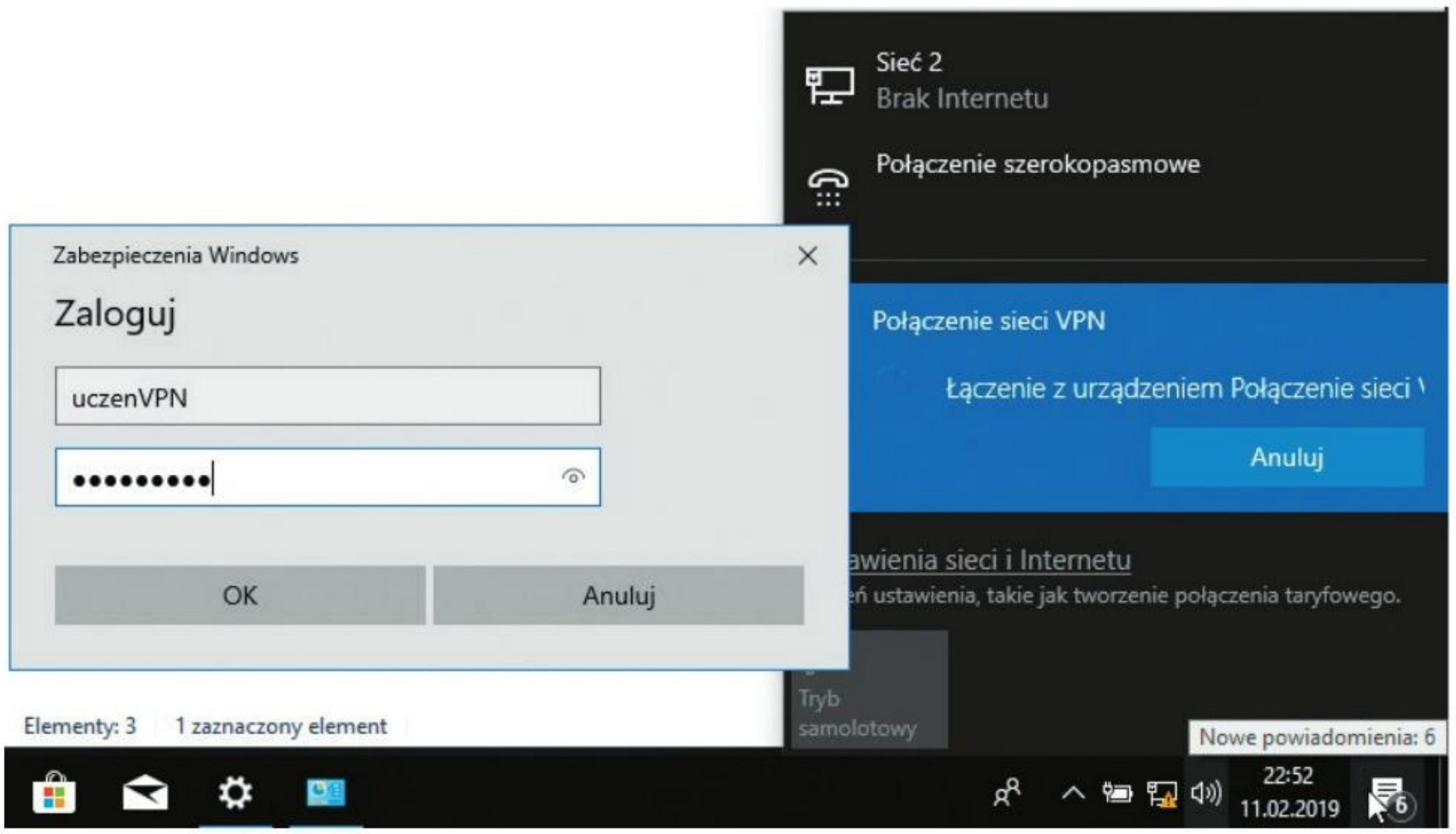
1. Zalogować się na konto z uprawnieniami administratora.
2. Sprawdzić, czy klient może komunikować się z serwerem (polecenie **ping**).
3. Otworzyć aplikację **Centrum sieci i udostępniania** – wybrać **Start/Panel sterowania/Sieć i Internet/Centrum sieci i udostępniania**.

4. Wybrać odnośnik **Skonfiguruj nowe połączenie lub nową sieć**.
5. W oknie **Wybierz opcję połączenia** wskazać **Połącz z miejscem pracy**. Kliknąć przycisk **Dalej**.
6. W oknie **Jak chcesz się łączyć** wybrać opcję **Użyj mojego połączenia internetowego (VPN)**. Kliknąć przycisk **Dalej**.
7. Wybrać opcję **Konfiguruj połączenie sieciowe**, a następnie **Połączenie szerokopasmowe (PPPoE)**.
8. Wpisać nazwę i hasło użytkownika mającego uprawnienia do logowania się do sieci VPN. Kliknąć przycisk **Połącz**.
9. Jeżeli połączenie nie powiedzie się, należy wybrać opcję **Mimo to skonfiguruj połączenie**.
10. Wpisać adres internetowy lub IP serwera pełniącego funkcję bramy VPN i nazwę połączenia. Kliknąć przycisk **Utwórz**.
11. Sprawdzić, czy w oknie połączeń sieciowych pojawiło się nowe połączenie sieci VPN (rys. 34.7).



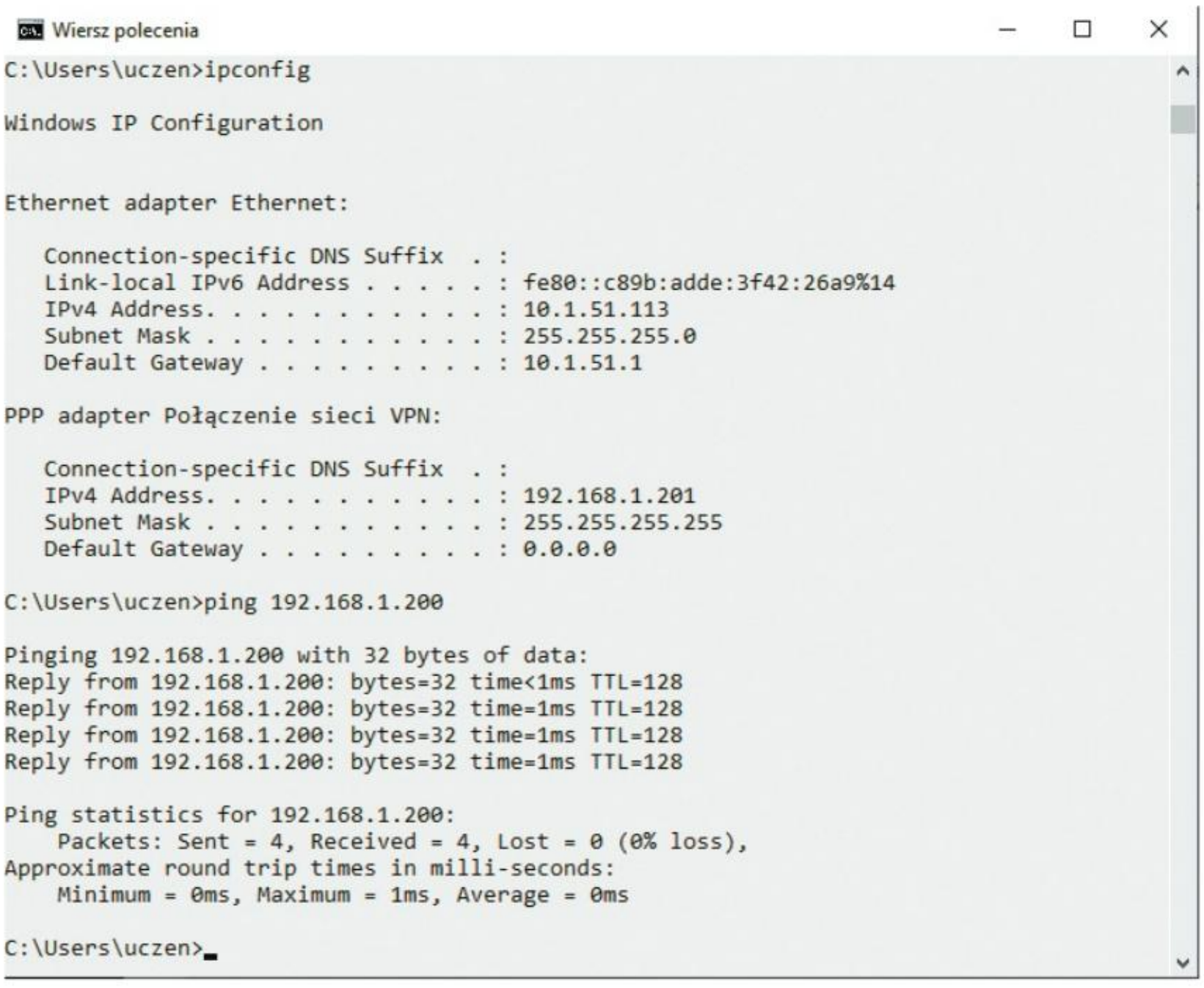
Rys. 34.7. **Nowe połączenie VPN**

Połączenie VPN zostaje włączone po konfiguracji. Jeżeli nie jest potrzebne, można je wyłączyć – kliknąć prawym przyciskiem myszy i z menu kontekstowego wybrać **Rozłącz**. Aby ponownie nawiązać połączenie VPN, należy kliknąć prawym przyciskiem myszy połączenie i z menu kontekstowego wybrać **Połącz**. W oknie łączenia z siecią VPN trzeba wprowadzić nazwę użytkownika i hasło (rys. 34.8), a następnie kliknąć przycisk **Połącz**.



Rys. 34.8. Nawiązywanie połączenia VPN

Po nawiązaniu połączenia można przetestować jego działanie. Na rys. 34.9 przedstawiono konfigurację połączeń sieciowych w komputerze z systemem Windows 10. W komputerze zostały skonfigurowane karta sieciowa z adresem **`10.1.51.113`** i połączenie VPN z przydzielonym dynamicznie adresem **`192.168.1.201`**. Polecenie **`ping`** pozwala na sprawdzenie możliwości komunikacji z siecią VPN.

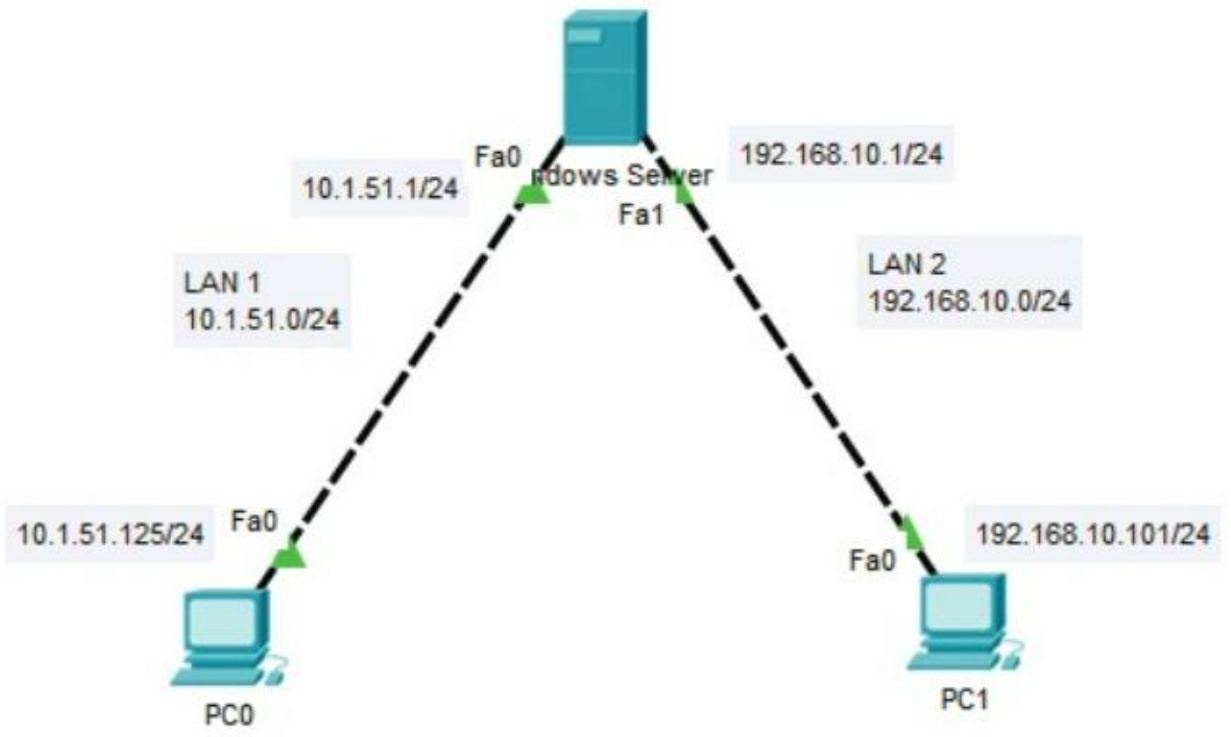


Rys. 34.9. Testowanie połączenia VPN

34.2. Konfigurowanie routingu między sieciami lokalnymi w Windows 2016

W tematach dotyczących konfigurowania routerów zostało omówione, jak konfigurować routery i protokoły routingu, korzystając z routerów sprzętowych. W małych sieciach lokalnych stosuje się również routery programowe, np. oparte na Windows Server. Możliwości konfiguracji routingu w Windows Server są mniejsze niż w przypadku dedykowanych urządzeń. W małych sieciach takie rozwiązanie może być jednak wystarczające i jednocześnie tańsze.

Najprostsza sieć, w której można zaimplementować rolę routingu, jest złożona z serwera (pełniącego fukcję routera) i dwóch sieci lokalnych. Schemat takiej sieci pokazano na rys. 34.10. W sieci LAN 1 hostom przypisano adresy z sieci 10.1.51.0/24, a hostom w sieci LAN 2 – adresy z sieci 192.168.10.0/24. Routing powinien zapewnić możliwość komunikacji między hostami w sieciach LAN 1 i LAN 2.



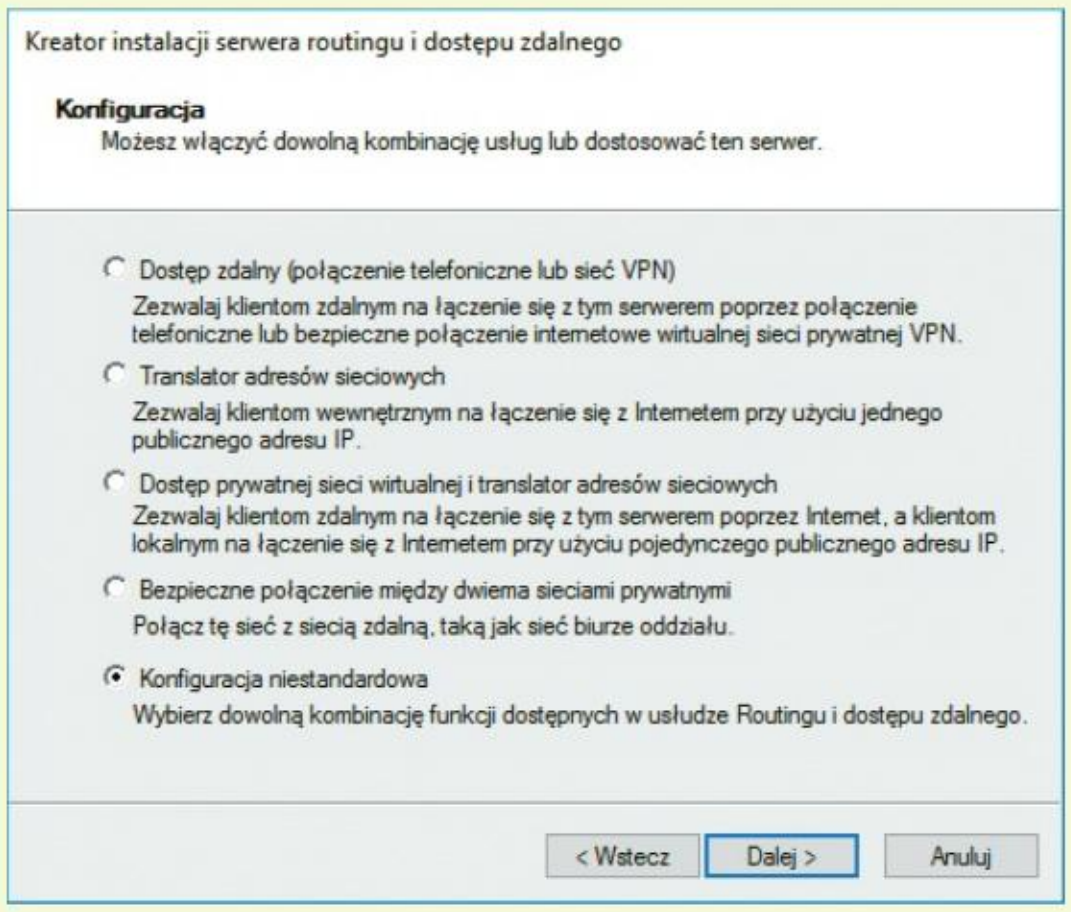
Rys. 34.10. Schemat sieci do testowania konfiguracji routingu

PRZYKŁAD 34.5

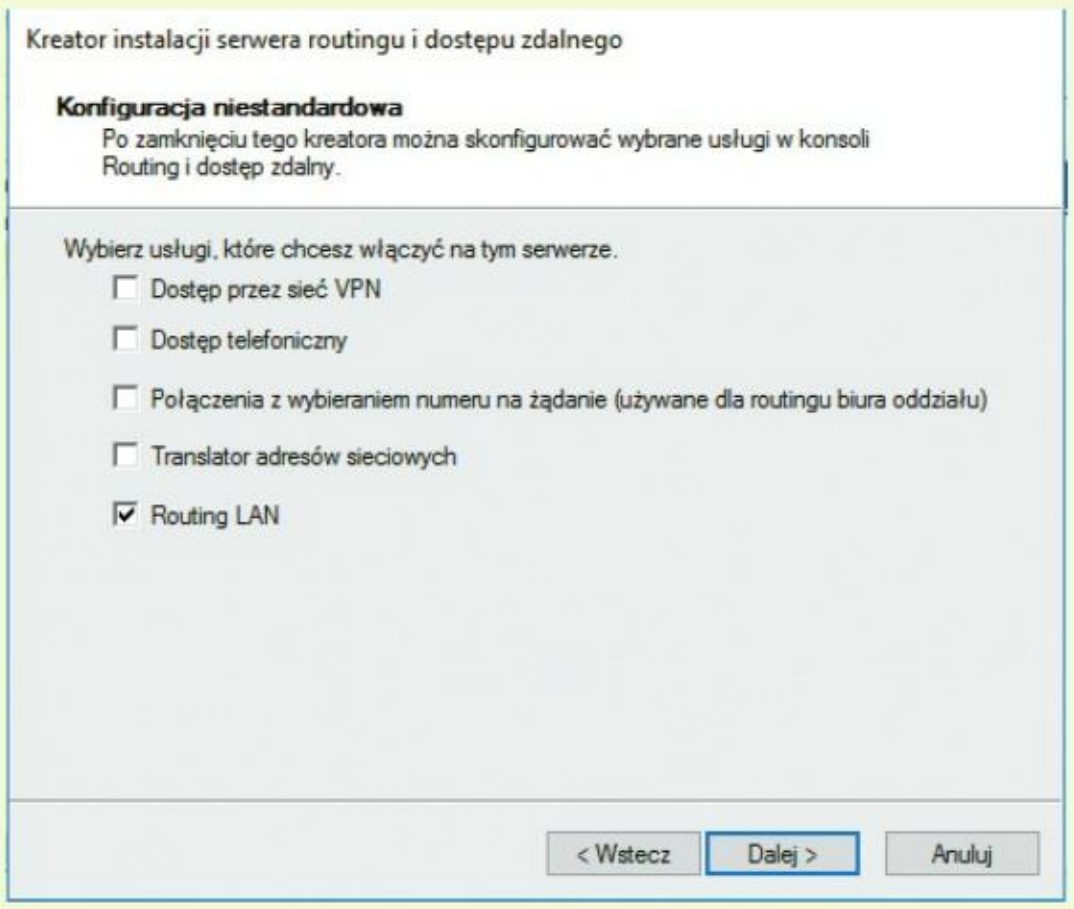
Konfigurowanie roli routingu między sieciami LAN w systemie Windows Server 2016

Aby skonfigurować rolę routingu między sieciami LAN, należy:

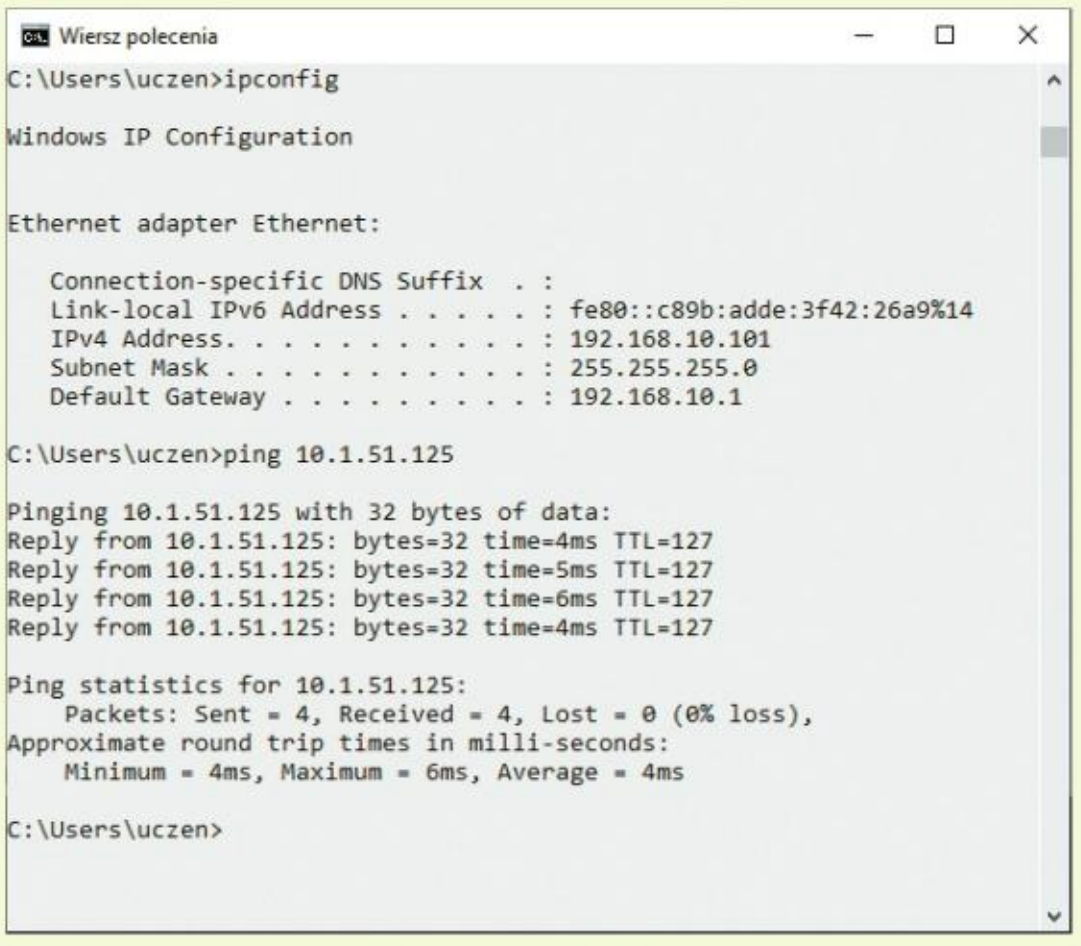
1. Połączyć urządzenia zgodnie z rys. 34.10 i skonfigurować adresy IP poszczególnych urządzeń.
2. Zainstalować w serwerze rolę RRAS i funkcję routingu (zob. przykład 34.1).
3. W oknie **Menedżer serwera** wybrać z menu polecenie **Narzędzia/Routing i dostęp zdalny**.
4. Uruchomić kreatora konfiguracji – w lewym panelu kliknąć prawym przyciskiem myszy ikonę serwera i z menu wybrać polecenie **Konfiguruj i włącz routing i dostęp zdalny**.
5. Po zapoznaniu się z informacjami kreatora kliknąć przycisk **Dalej**.
6. Wybrać konfigurację niestandardową (rys. 34.11). Kliknąć przycisk **Dalej**.
7. Wybrać konfigurację **Routing LAN** (rys. 34.12). Kliknąć przycisk **Dalej**.
8. Po weryfikacji ustawień kreatora kliknąć przycisk **Zakończ**, a następnie **Uruchom usługę**.
9. Przetestować możliwość komunikacji między stacjami roboczymi w sieciach LAN 1 i LAN 2. Na rys. 34.13 przedstawiono wynik działania polecenia **ping**, uruchomionego na komputerze w sieci LAN 2, testującego komunikację ze stacją w sieci LAN 1.



Rys. 34.11. Wybór typu konfiguracji



Rys. 34.12. Wybór konfiguracji Routing LAN



Rys. 34.13. Testowanie komunikacji między sieciami LAN 1 i LAN 2

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj serwer jako bramę sieci VPN. Nawiąż połączenie w serwerem skonfigurowanym przez koleżankę / kolegę. Przetestuj możliwość komunikacji.
2. Sieci VPN używają szyfrowania i jednokierunkowych funkcji haszujących.
   - Wyjaśnij, na czym polega szyfrowanie.
   - Wyjaśnij, co to są jednokierunkowe funkcje haszujące i gdzie są one używane.
   - Podaj przykładowe nazwy metod szyfrowania.
   - Podaj nazwy jednokierunkowych funkcji haszujących.
3. Utwórz sieć lokalną złożoną z co najmniej dwóch komputerów (mogą być maszyny wirtualne). Skonfiguruj serwer z Windows 2016 tak, aby mógł odgrywać rolę routera przekazującego pakiety między siecią szkolną a utworzoną siecią lokalną.
4. Skonfiguruj funkcję dostępu zdalnego przez sieć VPN do swojego komputera z Windows 2016. Nawiąż połączenie VPN z komputerem koleżanki / kolegi. Sprawdź, czy koleżanki / koledzy mogą nawiązywać połączenie z twoim komputerem.

SPRAWDŹ SWOJĄ WIEDZĘ

1. W jakich innych dziedzinach informatyki używa się pojęcia „wirtualny”? Co ono oznacza?
2. Jakie są zalety i wady stosowania sieci VPN?

35 Zarządzanie serwerem za pomocą pulpitu zdalnego

ZAGADNIENIA

- **Funkcja usługi pulpitu zdalnego**
- **Uruchomienie usługi pulpitu zdalnego**
- **Nawiązanie połączenia za pomocą pulpitu zdalnego**

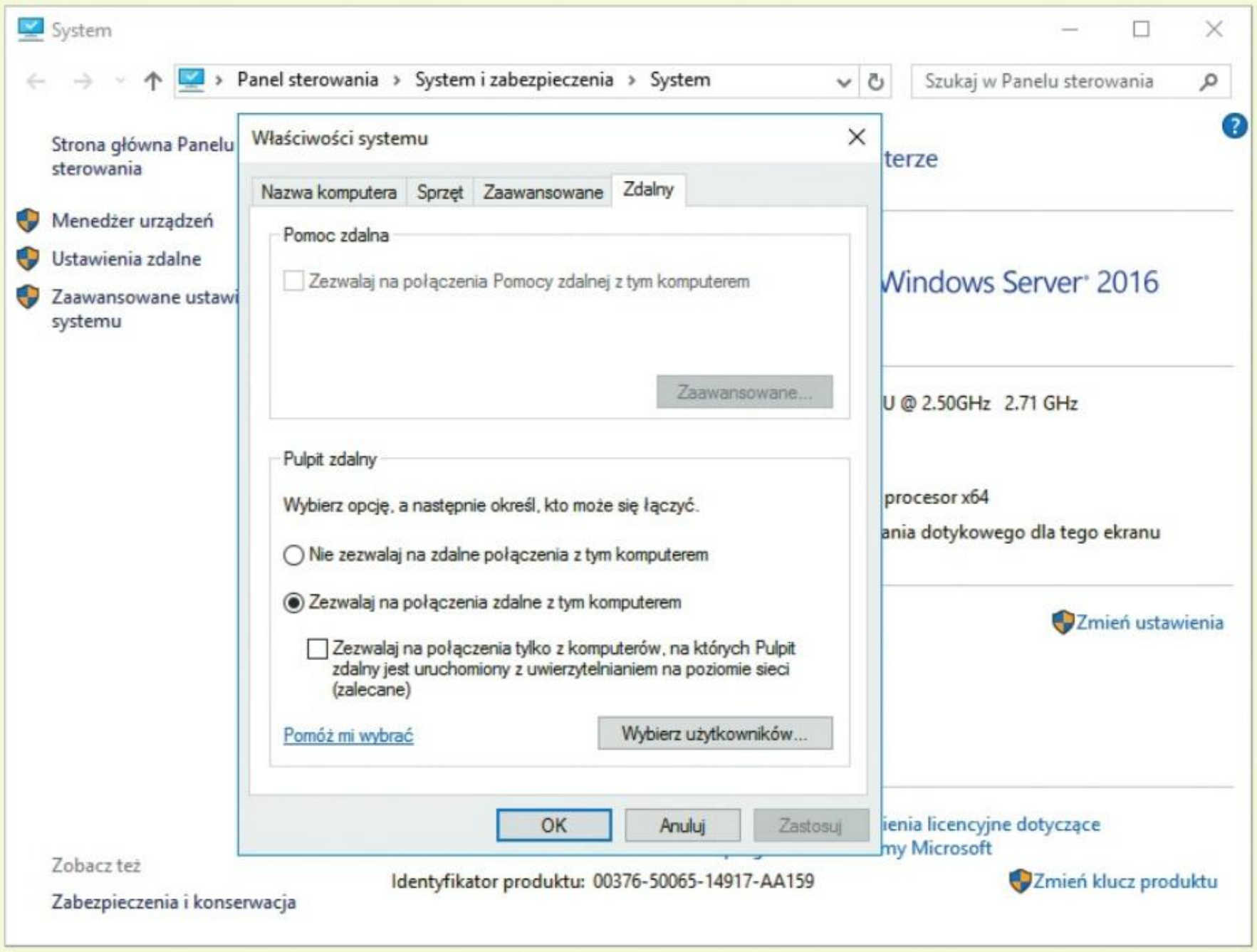
Do połączenia z serwerem i zdalnego zarządzania można wykorzystać usługę **pulpitu zdalnego**. Usługa korzysta z protokołu **RDP** (ang. *Remote Desktop Protocol*), który pozwala na komunikację z usługą terminalu graficznego w Windows. Dzięki pulpitowi zdalnemu można zalogować się i w środowisku graficznym wykonywać zadania na odległym komputerze. Wspomniana usługa jest standardowo zainstalowana w systemie Windows Server, ale nie jest aktywna. Aby z niej korzystać, należy ją aktywować i przydzielić użytkownikom odpowiednie uprawnienia.

PRZYKŁAD 35.1

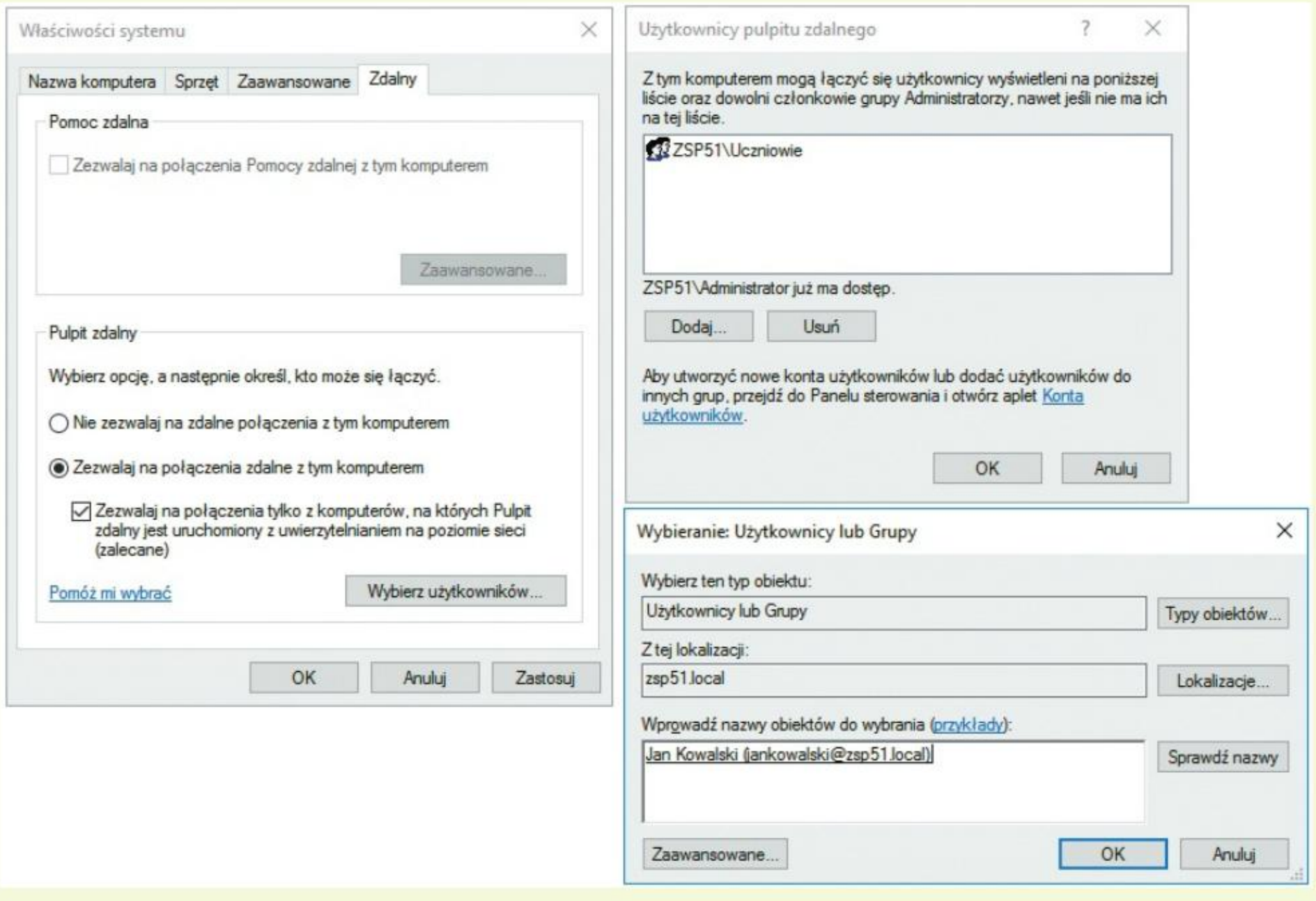
Uruchomienie usługi pulpitu zdalnego

Aby aktywować usługę pulpitu zdalnego, należy:

1. Zalogować się na konto użytkownika z uprawnieniami administratora.
2. Uruchomić aplikację wyświetlającą informacje o komputerze **`Start/Panel sterowania/System i zabezpieczenia/System`**. Kliknąć odnośnik **`Zmień ustawienia`** i wybrać zakładkę **`Zdalny`** (rys. 35.1).
3. W oknie **`Właściwości systemu`** w zakładce **`Zdalny`** zaznaczyć opcję **`Zezwalaj na połączenia zdalne z tym komputerem`**. Opcja **`Zezwalaj na połączenia tylko z komputerów, na których Pulpit zdalny jest uruchomiony z uwierzytelnianiem na poziomie sieci`** nie powinna być zaznaczona. Mechanizm pulpitu zdalnego może stanowić zagrożenie dla systemu, a więc zostać wyświetlony komunikat o włączeniu wyjątku w zaporze sieciowej serwera.
4. Kliknąć przycisk **`Wybierz użytkowników`** i dodać do listy tych użytkowników, którzy mogą mieć uprawnienia do korzystania ze zdalnego pulpitu (rys. 35.2). W tym ćwiczeniu użytkownicy *uczen1*, *uczen2* i *uczen3* uzyskają prawo korzystania z pulpitu jako członkowie grupy *uczniowie*. Ponadto to prawo otrzyma również użytkownik *jankowalski*. Kliknąć przycisk **`OK`**, aby zakończyć dodawanie użytkowników do listy.
5. Kliknąć przycisk **`OK`**, aby zakończyć konfigurację usługi.



Rys. 35.1. **Otwieranie okna właściwości systemu**



Rys. 35.2. **Tworzenie listy użytkowników uprawnionych do korzystania z pulpitu zdalnego**

Użytkownik, który będzie logował się do systemu za pomocą pulpitu zdalnego, musi mieć uprawnienia wystarczające do zalogowania się na komputerze (np. należeć do grupy *Administratorzy*) i korzystania z usługi pulpitu zdalnego (np. być członkiem grupy *Użytkownicy pulpitu zdalnego*).

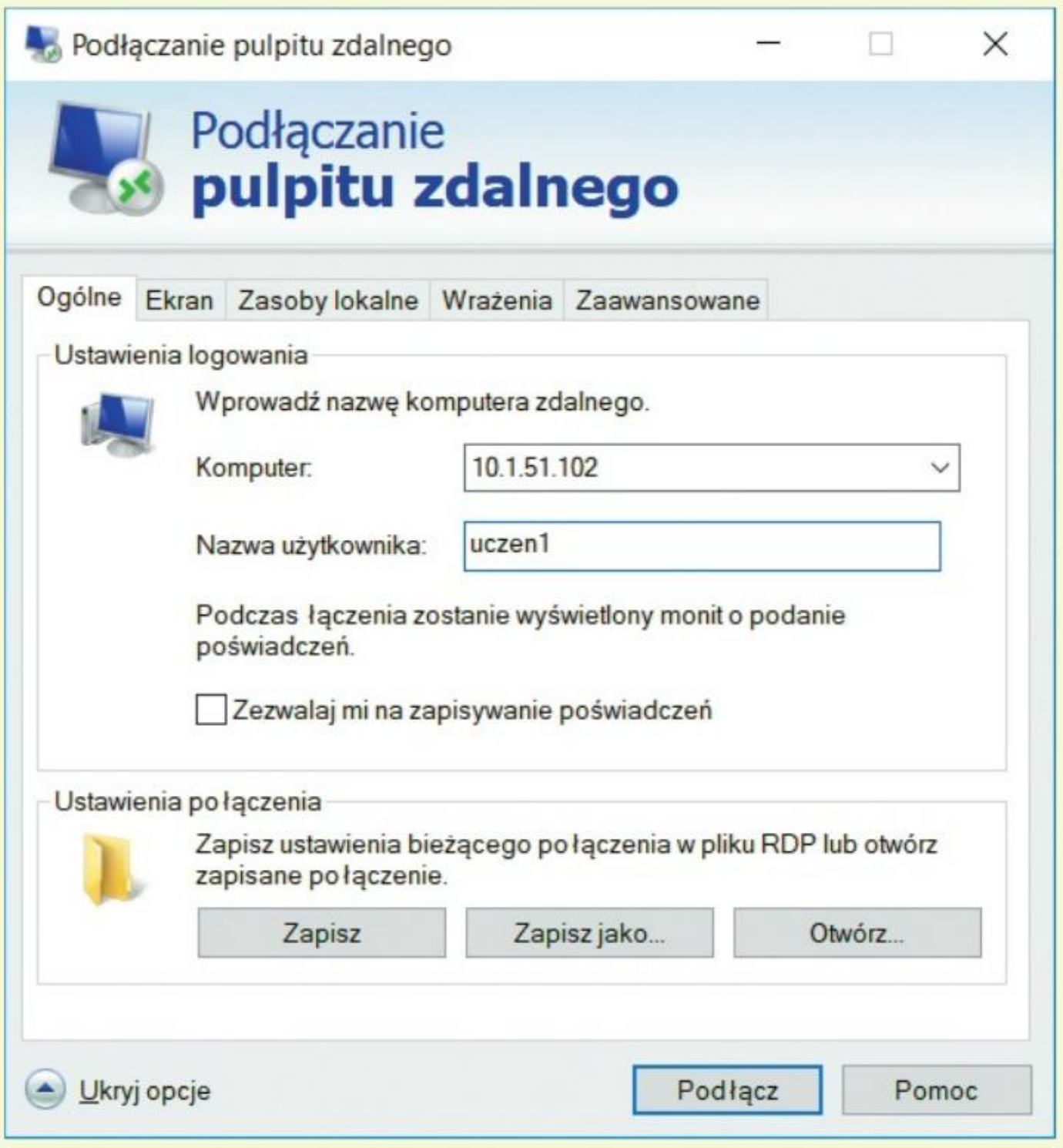
PRZYKŁAD 35.2

Nawiązywanie połączenia za pomocą pulpitu zdalnego

Z komputerem z zainstalowanym Windows Server można nawiązywać połączenia za pomocą pulpitu zdalnego, korzystając z różnych wersji systemu Windows.

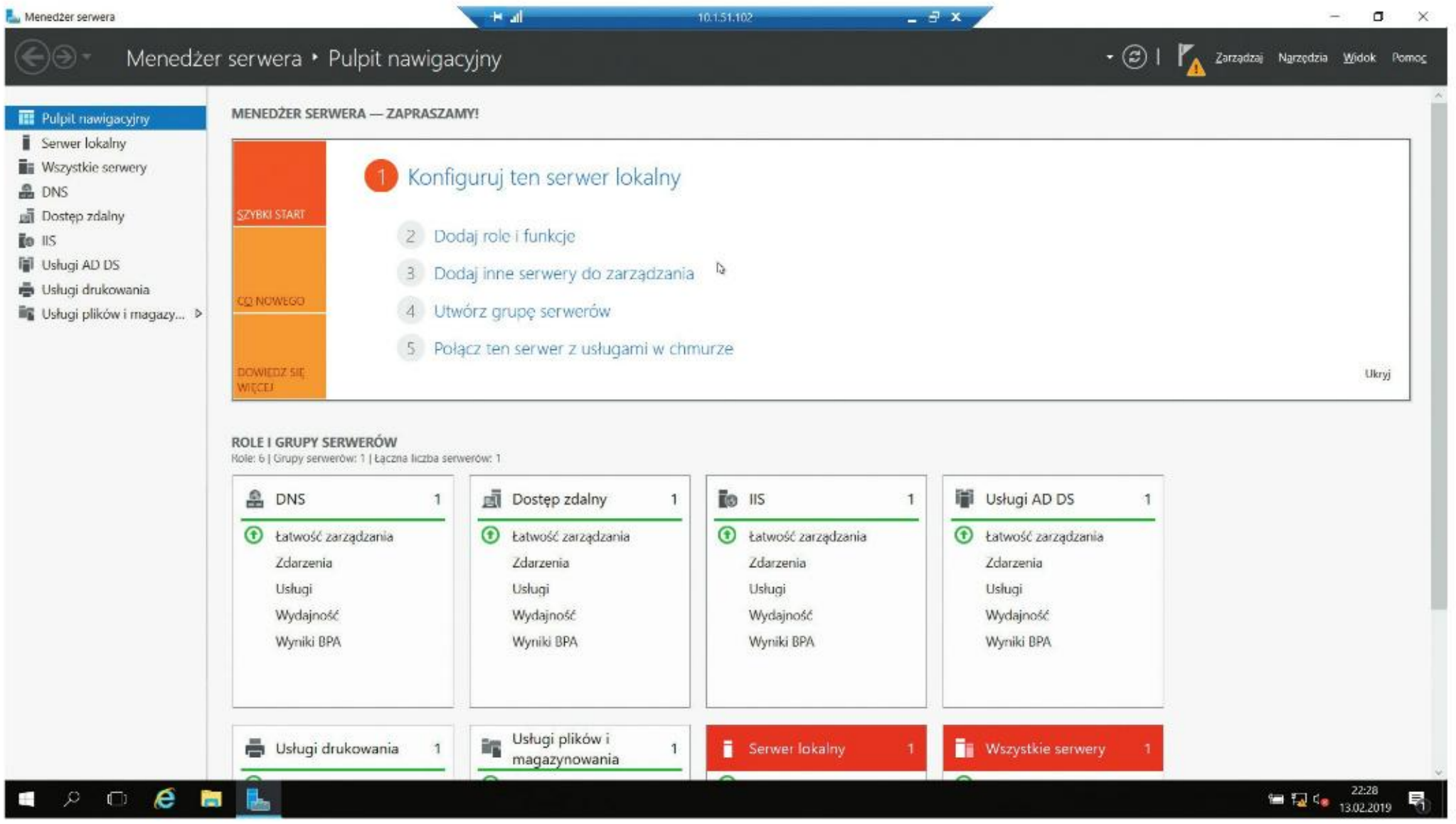
Aby nawiązać połączenia za pomocą Windows 10, należy:

1. Zalogować się do systemu.
2. Uruchomić aplikację **`Podłączanie pulpitu zdalnego`** – polecenie **`Start/Podłączanie pulpitu zdalnego`**.
3. W oknie **`Podłączanie pulpitu zdalnego`** w zakładce **`Ogólne`** w pole **`Komputer`** wprowadzić nazwę lub adres IP komputera udostępniającego pulpit, a w pole **`Nazwa użytkownika`** – nazwę konta użytkownika z odpowiednimi uprawnieniami, np. *uczen1* (rys. 35.3).
4. Kliknąć przycisk **`Podłącz`**.



Rys. 35.3. **Podłączanie pulpitu zdalnego**

Przykład połączenia realizowanego za pomocą pulpitu zdalnego przedstawiono na rys. 35.4.



Rys. 35.4. **Połączenie z pulpitem zdalnym**

Po nawiązaniu połączenia z pulpitem zdalnym można wykonywać operacje na zdalnym komputerze, tak samo jak na komputerze lokalnym.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

Za pomocą pulpitu zdalnego połącz się z komputerem koleżanki / kolegi. Zdalnie wykonaj następujące działania:

1. Sprawdź adres IP komputera.
2. Utwórz konto użytkownika z własnym imieniem.
3. Uruchom notatnik i napisz tekst „Ala ma kota”.
4. Przetestuj możliwość połączenia z bramą i twoim lokalnym komputerem (polecenie **`ping`**).

SPRAWDŹ SWOJĄ WIEDZĘ

1. W jakim celu korzysta się z usługi pulpitu zdalnego?
2. Jakie inne usługi sieciowe umożliwiają zdalne wykonywanie poleceń?

36 Usługi terminalowe

ZAGADNIENIA

Działanie usług terminalowych **Konfigurowanie usług terminalowych** **Korzystanie z usług terminalowych**

Usługi terminalowe (ang. *Remote Desktop Services*) to system umożliwiający komunikację między klientami i serwerem oraz uruchamianie z dowolnego komputera aplikacji i zarządzanie serwerem. Terminal serwera jest uruchomiony w komputerze zdalnym, natomiast wszystkie operacje są wykonywane z wykorzystaniem zasobów serwera, np. procesora i pamięci. Przez sieć są przesyłane tylko informacje o działaniach użytkownika, np. przemieszczaniu kursora myszy, znakach wprowadzanych za pomocą klawiatury i obrazy generowane przez serwer. Dzięki temu ilość informacji przesyłanych przez sieć jest niewielka i do pracy nie jest wymagana duża przepustowość sieci.

Usługi terminalowe umożliwiają korzystanie z lokalnych dysków, urządzeń dźwiękowych, drukarki, portów itp. Dzięki zastosowaniu centralnego serwera aplikacji użytkownicy mogą korzystać z prostych i tanich terminali, co pozwala obniżyć koszty wdrożenia systemu. Aplikacje udostępnione na serwerze działają z punktu widzenia użytkownika tak, jak zainstalowane lokalnie. Wszystkie zadania związane z instalacją aplikacji są wykonywane tylko na serwerze.

Usługi terminalowe mogą działać w dwóch różnych trybach:

- **tryb pulpitu zdalnego** – może być wykorzystany przez administratora do zdalnego zarządzania serwerem. Liczba jednocześnie korzystających użytkowników zdalnych jest ograniczona do dwóch (trzecim może być administrator korzystający z konsoli lokalnej). Nie są wymagane dodatkowe licencje;
- **tryb serwera terminali** – umożliwia korzystanie każdemu uprawnionemu użytkownikowi, ale wymaga zakupienia dodatkowej **licencji CAL** (ang. *Client Access Licence*) dla każdego połączenia. Aby zarządzać licencjami CAL, jest potrzebny dodatkowy **serwer licencji** (ang. *Terminal Services Licence Server*).

Usługi terminalowe mogą być wdrożone na dwa sposoby:

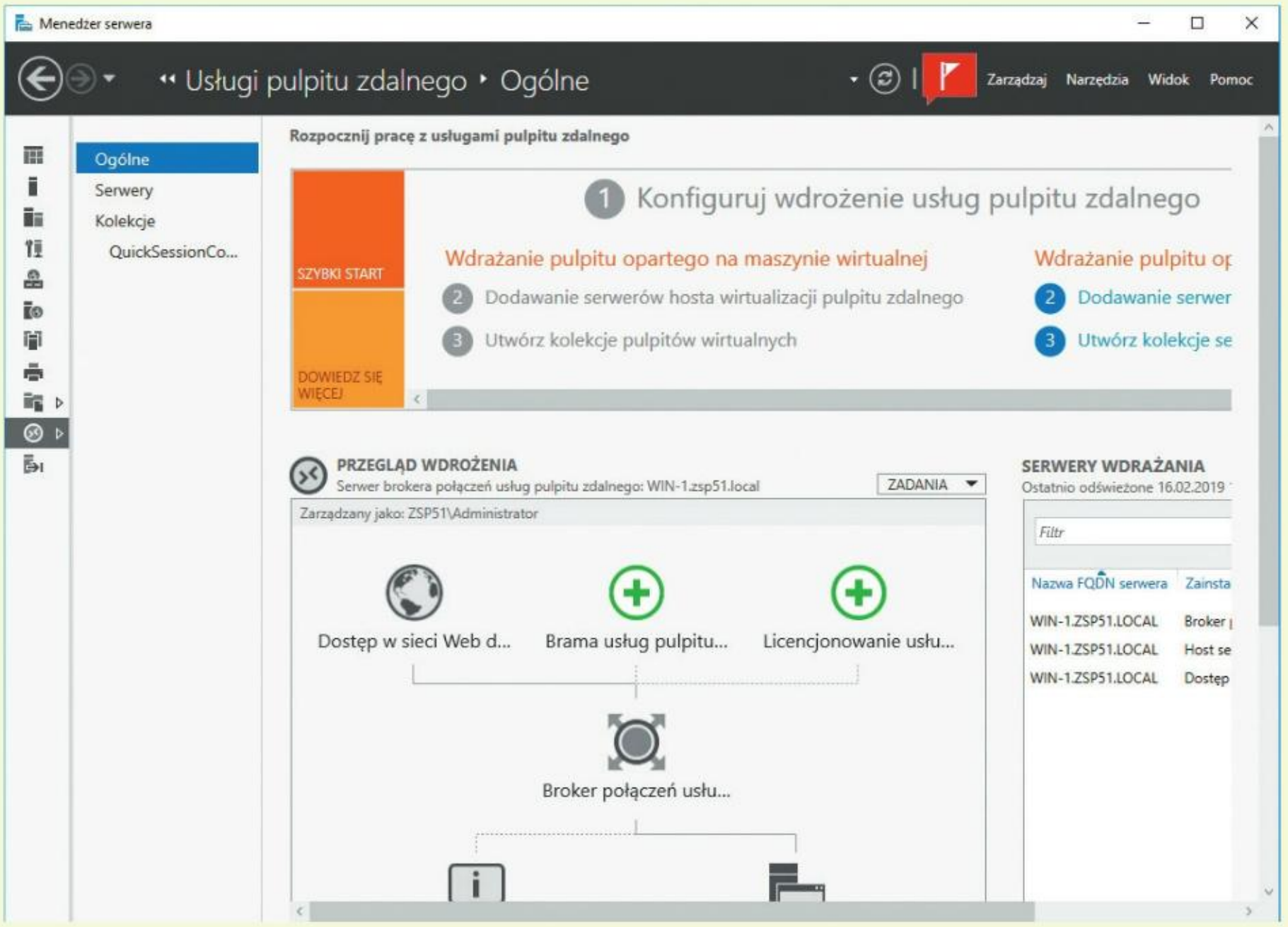
- **wdrożenie oparte na maszynach wirtualnych** (ang. *Virtual machine-based desktop deployment*), które pozwala użytkownikom na łączenie się z przygotowanymi wcześniej maszynami wirtualnymi i korzystanie z zainstalowanych na nich aplikacji;
- **wdrożenie oparte na sesjach** (ang. *Session-based desktop deployment*), które pozwala użytkownikom na łączenie się z kolekcjami sesji, zawierającymi opublikowane aplikacje i pulpity.

PRZYKŁAD 36.1

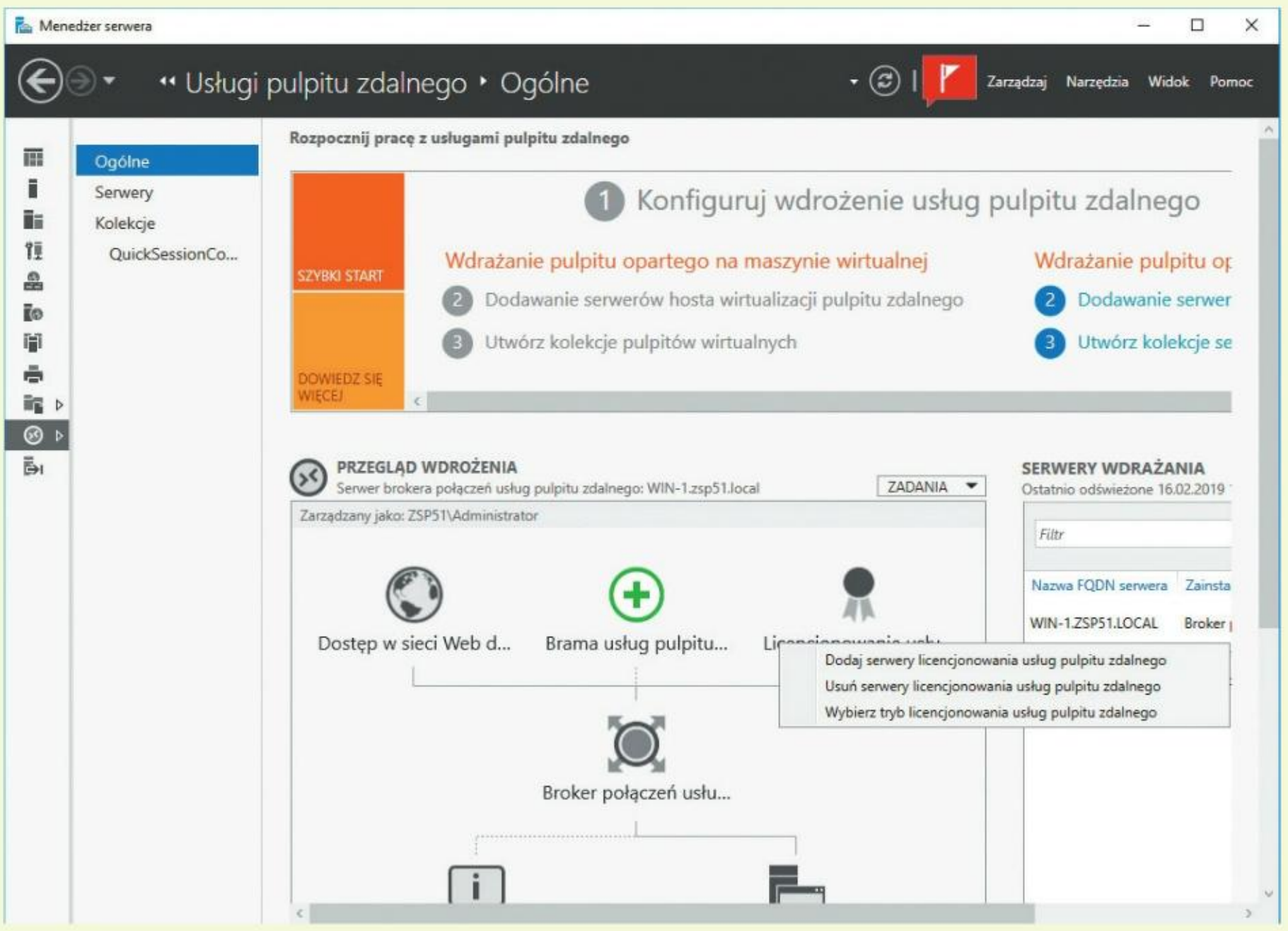
Instalowanie usług terminalowych na serwerze

Instalacje usług terminalowych można wykonać w oknie **Menedżer serwera** przez kreatora. Aby uruchomić kreatora i przeprowadzić procedurę instalacji, należy:

1. W oknie **Menedżer serwera** kliknąć odnośnik **Dodaj role i funkcje**, wskazać opcję **Instalacja usług pulpitu zdalnego** (ang. *Remote Desktop Services installation*). Kliknąć przycisk **Dalej**.
2. Wybrać typ wdrożenia, np. **Szybki start** (ang. *quick start*). Wybranie tej opcji spowoduje zainstalowanie na jednym serwerze wszystkich usług związanych z rolą serwera terminalowego. Zostaną zainstalowane następujące role:
   - **RDS Connection Broker** – usługa wspierająca korzystanie z farm serwerów terminalowych, pozwalających na równoważenie obciążenia (ang. *load-balancing*) serwerów RDS, wchodzących w skład danych farm.
     Usługa umożliwia m.in.:
     – równomierne rozłożenie obciążenia sesjami między serwery pulpitu zdalnego należące do danej farmy;
     – nawiązywanie ponownego połączenia z istniejącymi sesjami w farmie serwerów usług pulpitu zdalnego; funkcja zapobiega rozpoczęciu nowej sesji, na nowym serwerze przez użytkownika, który jest zalogowany na jednym z serwerów RDS w farmie, ale w danej chwili jest od niego odłączony;
     – zapewnia użytkownikom dostęp do pulpitów wirtualnych lub programów typu RemoteApp, hostowanych na określonych serwerach;
   - **RD Web Access** – usługa umożliwiająca dostęp do programów typu RemoteApp lub pulpitów zdalnych za pośrednictwem przeglądarki internetowej.
   - **RD Session Host** – usługa odpowiadająca za hostowanie na danym serwerze sesji pulpitu zdalnego lub programów typu RemoteApp.
3. Kliknąć przycisk **Dalej**.
4. Wybrać wdrożenie oparte na sesjach. Kliknąć przycisk **Dalej**.
5. Wybrać serwer, na którym będą instalowane usługi. Kliknąć przycisk **Dalej**.
6. Zaznaczyć opcje **Automatycznie uruchom ponownie serwer docelowy, jeżeli będzie to potrzebne** (ang. *Restart the destination server automatically if required*). Kliknąć przycisk **Wdróż**.
7. Po zakończeniu procesu instalacji, kliknąć przycisk **Zamknij**.
   Po skonfigurowaniu roli serwera terminalowego – domyślnie – dostęp do serwera mają wszyscy członkowie domeny. W oknie **Menedżer serwera** można sprawdzić stan usługi lub nią zarządzać. W tym celu trzeba kliknąć odnośnik do usługi w lewym panelu (rys. 36.1).
8. Skonfigurować serwer licencji. Kliknąć odnośnik **Licencjonowanie usług pulpitu zdalnego** (ang. *RD Licensing*).
9. Zaznaczyć serwer. Kliknąć przycisk **Dalej**, a następnie **Dodaj**. Po zakończeniu procesu instalacji kliknąć przycisk **Zamknij**.
10. Kliknąć prawym przyciskiem myszy odnośnik **Licencjonowanie usług pulpitu zdalnego** i z menu kontekstowego wybrać opcję **Wybierz tryb licencjonowania usług pulpitu zdalnego** (rys. 36.2).

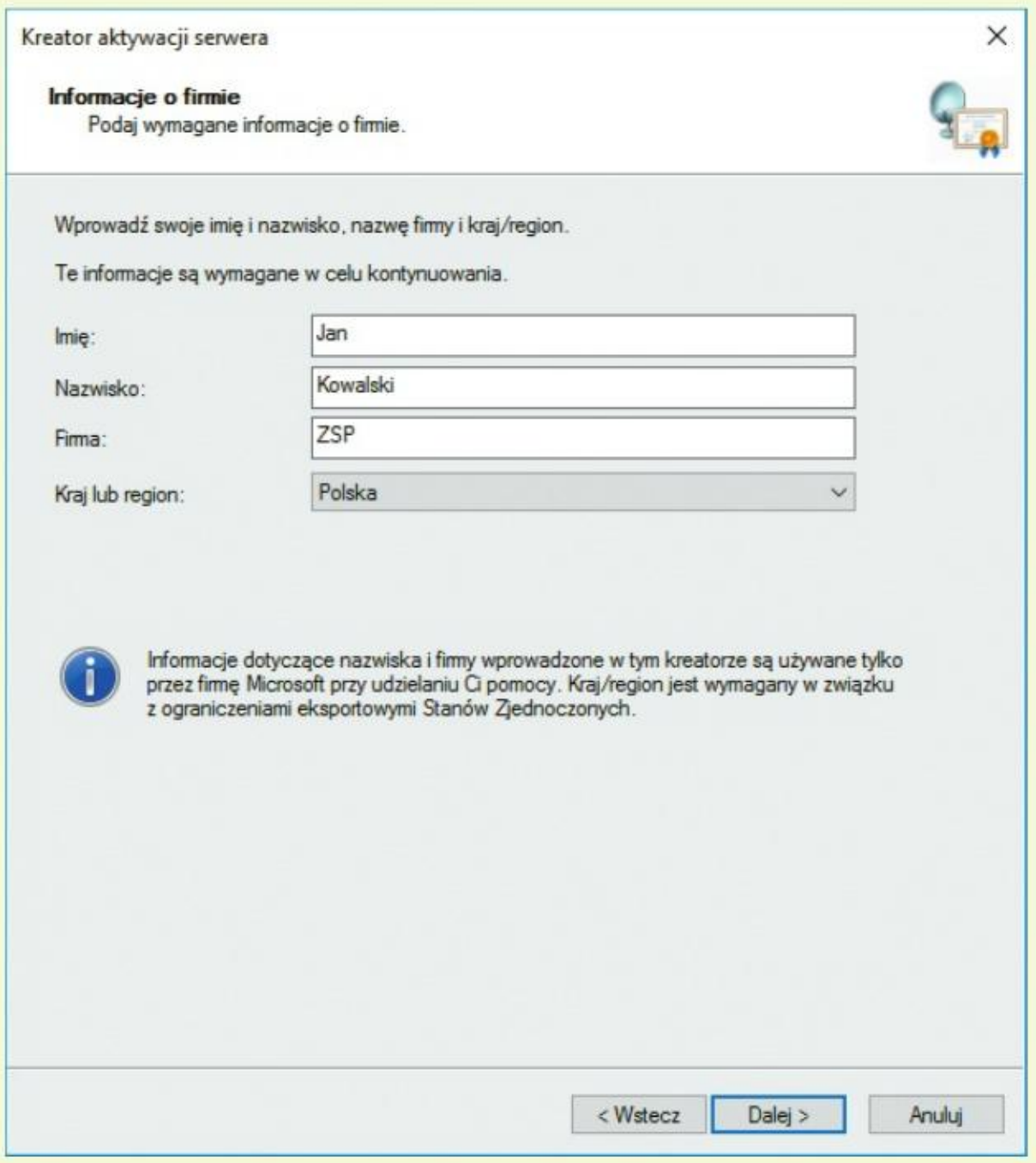


Rys. 36.1. **Zarządzanie usługami serwera terminali**



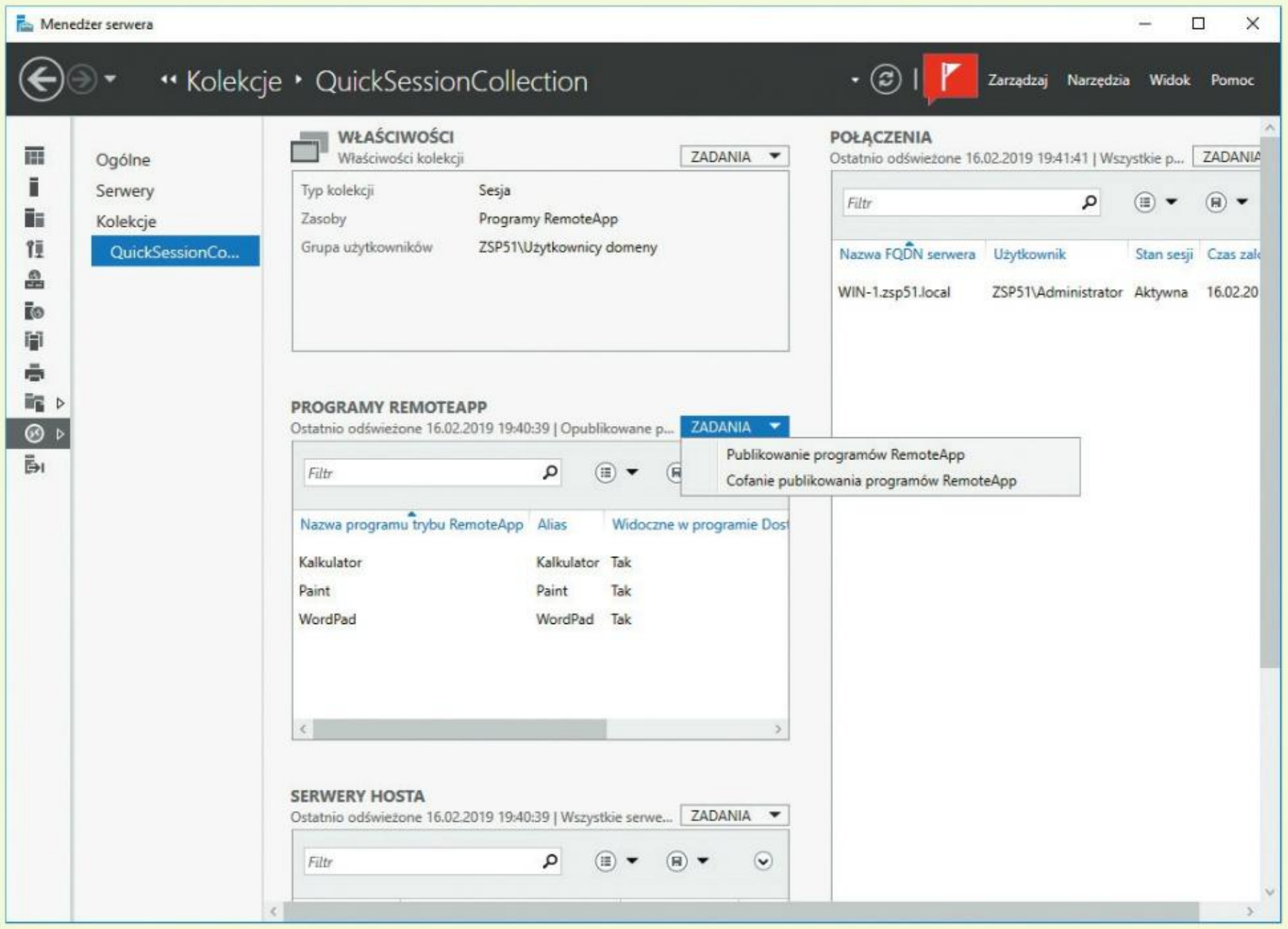
Rys. 36.2. **Wybór trybu licencjonowania usług pulpitu zdalnego**

11. Wybrać tryb licencjonowania **Na użytkownika** (ang. *Per User*). Kliknąć przycisk **OK**.
12. Z menu wybrać polecenie **Narzędzia/Remote Desktop Services/Menedżer licencjonowania usług pulpitu zdalnego**.
13. Kliknąć prawym przyciskiem myszy nazwę serwera i z menu kontekstowego wybrać polecenie **Uaktywnij serwer**. Zostanie uruchomiony **Kreator aktywacji serwera**.
14. W oknie **Metoda połączenia** wybrać opcję **Połączenie automatyczne (zalecane)**. Kliknąć przycisk **Dalej**.
15. Wprowadzić informacje o użytkowniku i organizacji (rys. 36.3). Kliknąć przycisk **Dalej**.

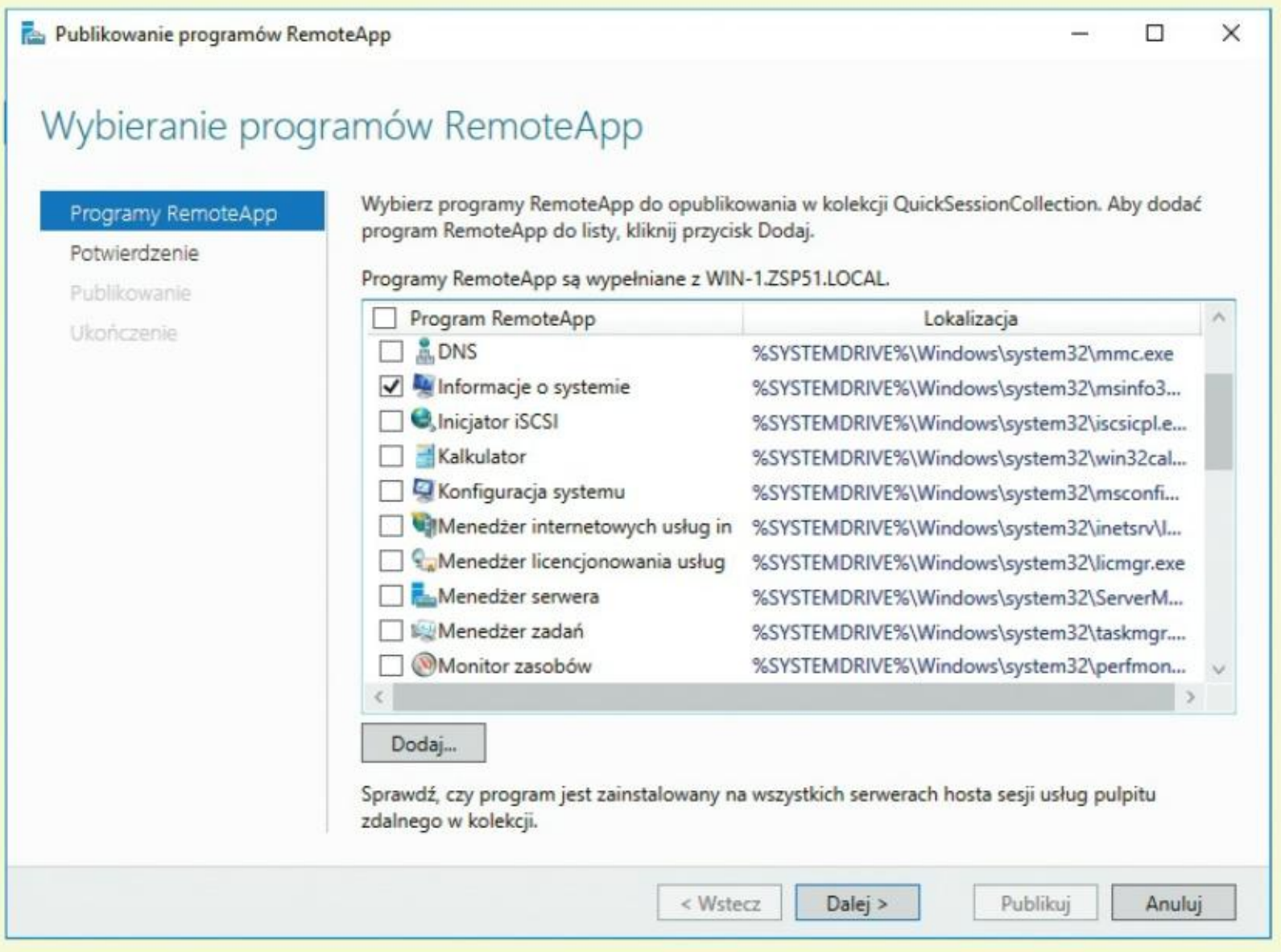


Rys. 36.3. **Informacje o użytkowniku i organizacji**

16. Wprowadzić opcjonalne informacje o firmie. Kliknąć przycisk **Dalej**.
17. Zaznaczyć opcję **Uruchom teraz Kreatora instalacji licencji** (ang. *Start Install Licenses Wizard now*). Kliknąć przycisk **Dalej**. Jeżeli licencje nie zostaną dodane, to standardowo z usługi może korzystać dwóch użytkowników.
18. Zapoznać się z informacjami o kreatorze instalacji licencji. Kliknąć przycisk **Dalej**.
19. Wybrać program licencjonowania, np. **Pakiet licencji**. Kliknąć przycisk **Dalej**.
20. Wprowadzić kod licencji. Kliknąć przycisk **Dalej**.
21. Po aktywacji można dodawać udostępniane aplikacje. W lewym panelu okna **Menedżer serwera** wybrać **QuickSessionCollection** (rys. 36.4).
22. W sekcji **Programy REMOTEAPPS** kliknąć przycisk **Zadania/Publikowanie programów RemoteApp**.
23. Wskazać programy do opublikowania, np. **Informacje o systemie** (rys. 36.5). Kliknąć przycisk **Dalej**, a następnie **Publikuj** i **Zamknij**.



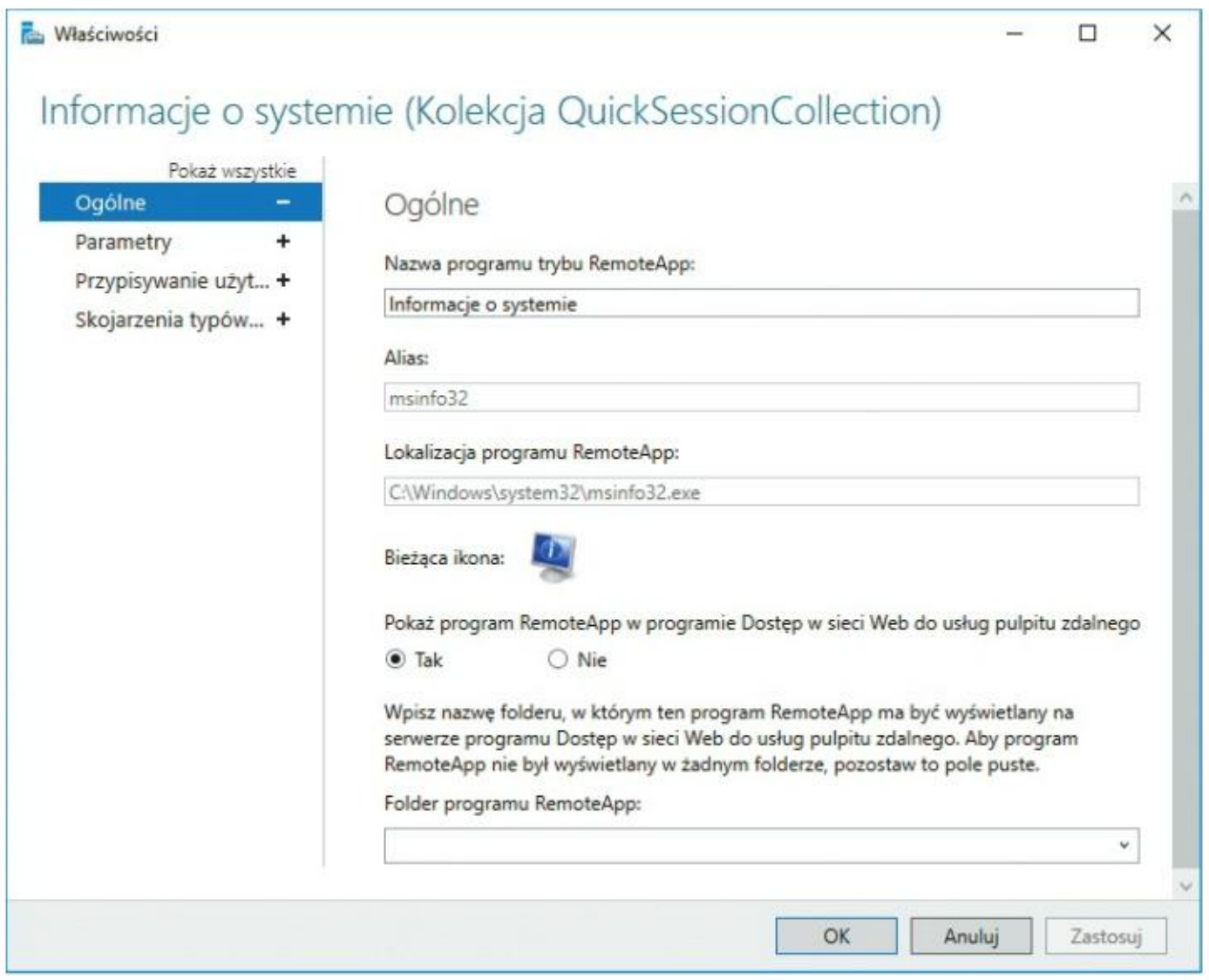
Rys. 36.4. **Okno `QuickSessionCollection`**



Rys. 36.5. **Wybór programów do opublikowania**

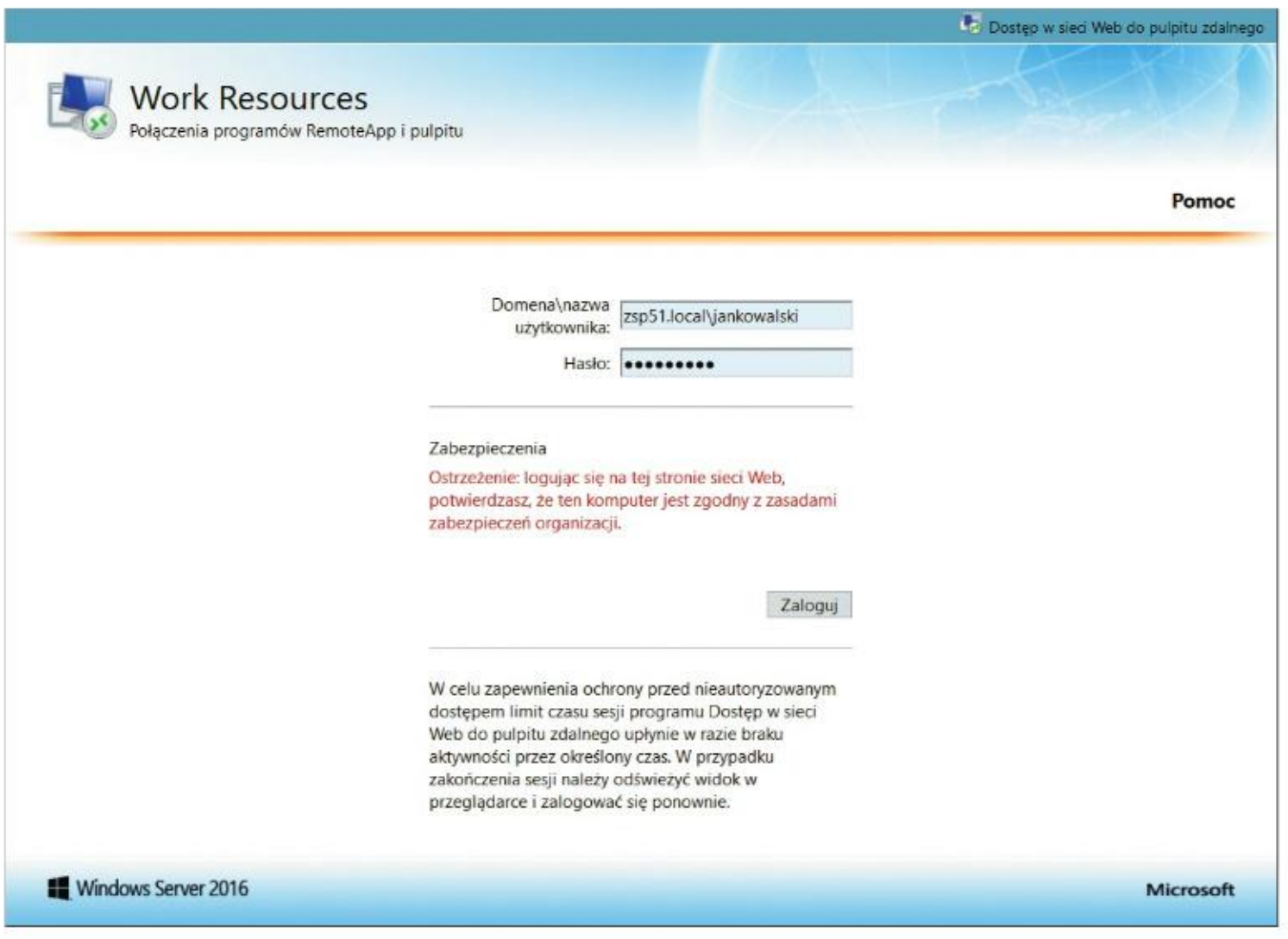
24. Sprawdzić, czy opublikowany program pojawił się na liście.

Dla każdej opublikowanej aplikacji można modyfikować ustawienia. W tym celu należy kliknąć prawym przyciskiem myszy nazwę opublikowanej aplikacji i z menu kontekstowego wybrać **`Edytuj właściwości`** (rys. 36.6).



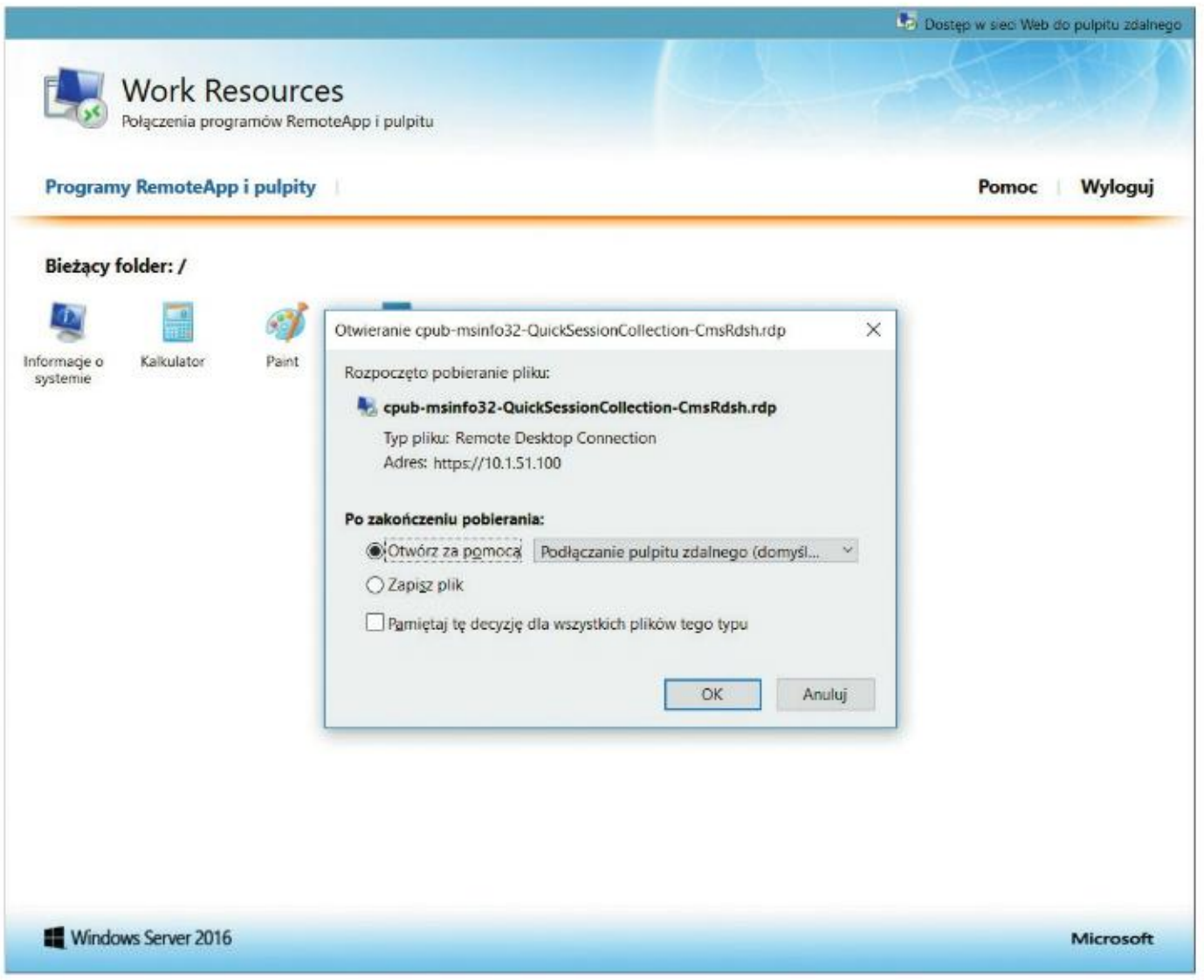
Rys. 36.6. Właściwości opublikowanej aplikacji

Aby uruchomić opublikowaną aplikację, należy uruchomić na komputerze klienckim przeglądarkę internetową i wpisać adres: **`https://adres_serwera/RDWeb`**, np. **`10.1.51.100\RDWeb`**, i zalogować się, korzystając z konta domenowego, np. **`zsp51.local\jankowalski`** (rys. 36.7).



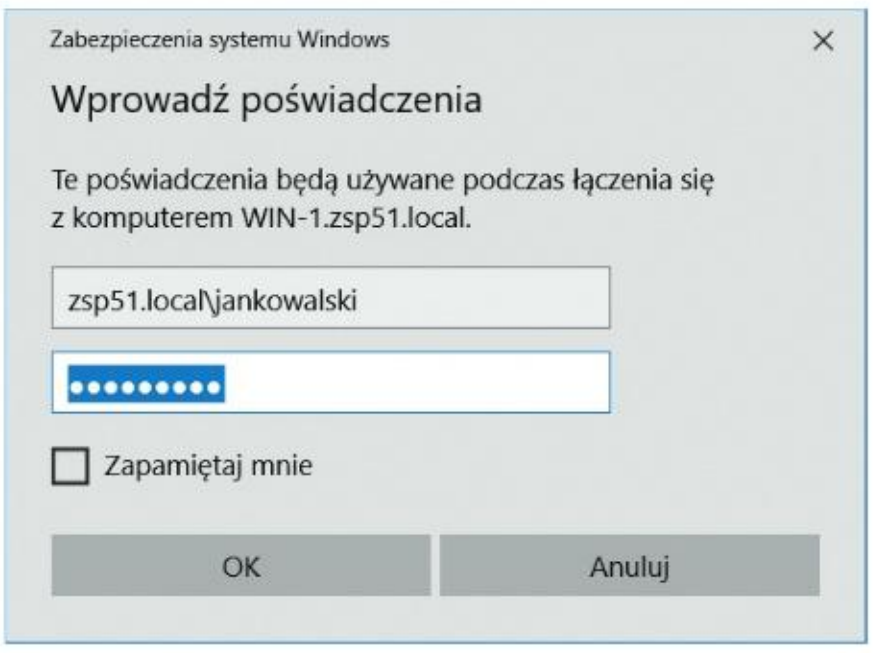
Rys. 36.7. Okno logowania do serwera terminali

Wybrać aplikację z listy dostępnych i po pobraniu uruchomić lub zapisać na dysku (rys. 36.8).



Rys. 36.8. Otwieranie aplikacji terminalowej

Podczas uruchamiania aplikacji należy wprowadzić poświadczenia tożsamości (rys. 36.9). Po ich zweryfikowaniu można rozpocząć pracę z aplikacją.



Rys. 36.9. Wprowadzanie poświadczenia tożsamości

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj serwer terminali.
2. Opublikuj w serwerze terminali wybraną aplikację.
3. Uruchom aplikację opublikowaną przez koleżankę / kolegę.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wymień zalety korzystania z usług terminalowych.
2. Sporządź listę aplikacji, które twoim zdaniem powinny być udostępniane w twojej szkole jako usługi terminalowe.

37 Konfigurowanie usługi WDS

ZAGADNIENIA

- **Instalowanie usługi WDS**
- **Przygotowanie obrazu systemu operacyjnego**
- **Instalowanie systemu przez usługę WDS**

Windows w wersji Server zawiera wiele usług, które mogą być wykorzystywane do zarządzania stacjami roboczymi i użytkownikami w sieci komputerowej organizacji. Jedną z często wykonywanych i wymagających dużo czasu operacji jest instalowanie systemu operacyjnego stacji roboczej. **Usługi wdrażania systemu Windows – WDS** (ang. *Windows Deployment System*) są prostym i bezpiecznym rozwiązaniem do automatycznego instalowania systemów z rodziny Microsoft Windows. Systemy mogą być instalowane przez sieć komputerową LAN bez udziału człowieka. Obrazy systemów powinny być przygotowane w formacie **Windows Imaging Format** (**WIM**).

Usługi WDS wymagają, aby stacje robocze były wyposażone w karty sieciowe zgodne ze **standardem PXE** (ang. *Preboot Execution Environment*). Ten standard umożliwia uruchomienie na komputerze systemu operacyjnego, nawet wtedy, gdy nie jest on na nim zainstalowany. Komputer nie musi mieć dysku twardego ani innych urządzeń, takich jak napędy CD/DVD czy dyski USB. Łączy się z serwerem obsługującym protokoły DHCP i TFTP i z niego pobiera dane konfiguracyjne i system operacyjny.

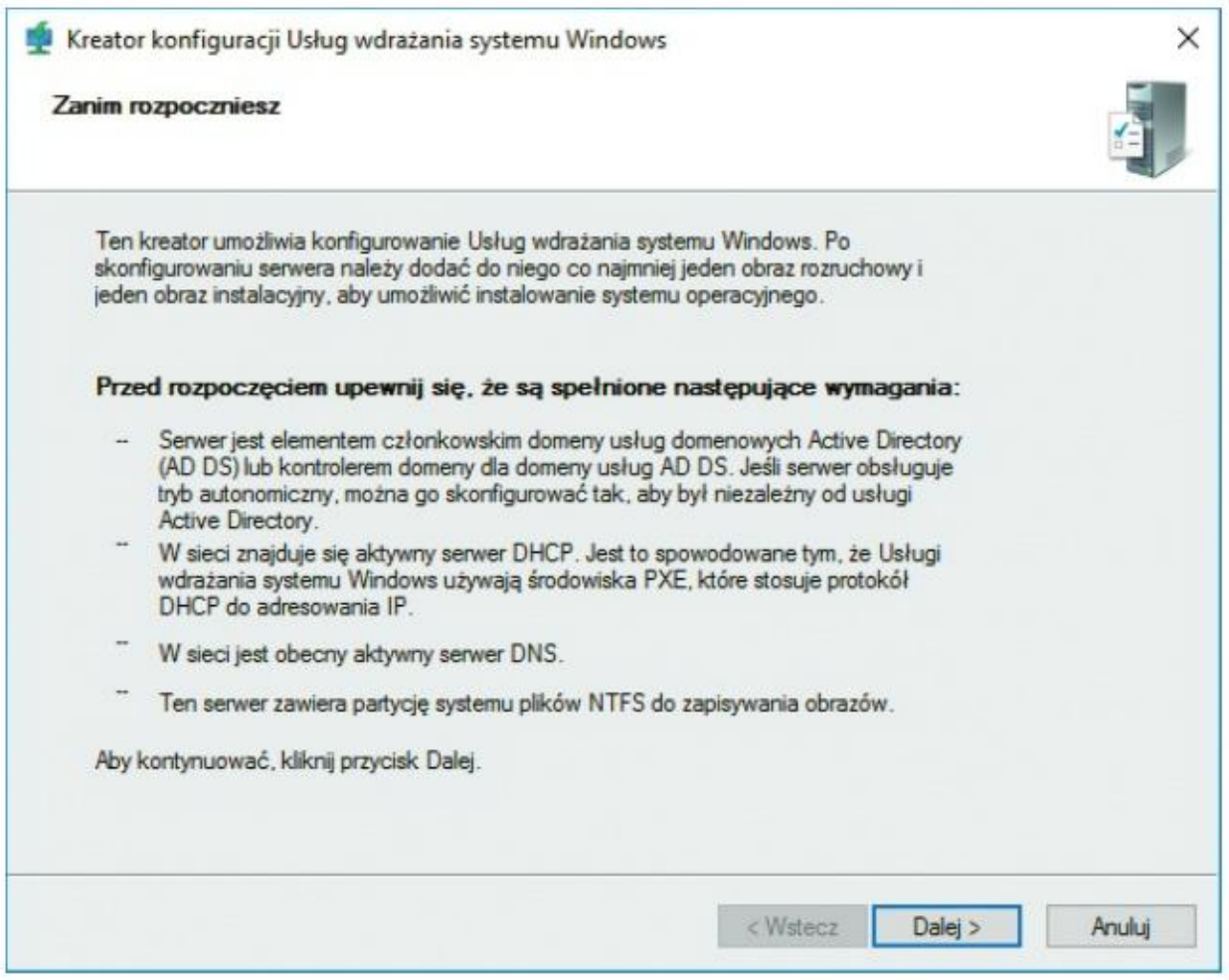
Uruchomienie komputera przebiega według następującego schematu:

- po włączeniu komputera uruchamia się procedura BIOS z pamięci karty sieciowej. Program znajduje w lokalnej sieci serwer DHCP;
- od serwera DHCP otrzymuje adres IP i inne dane potrzebne do konfiguracji oraz nazwę pliku z **programem rozruchowym** (ang. *bootloader*), przechowywanego na serwerze;
- za pomocą protokołu TFTP pobiera z serwera plik z programem rozruchowym;
- program rozruchowy pobiera z serwera TFTP pliki z systemem operacyjnym, instaluje je w pamięci RAM komputera i przeprowadza właściwy start systemu operacyjnego.

Przygotowanie środowiska do instalowania systemów na stacjach roboczych za pomocą WDS obejmuje następujące działania:

- instalacja usługi na serwerze;
- konfiguracja usługi na serwerze;
- przygotowanie obrazu sytemu i umieszczenie go na serwerze;
- przygotowanie stacji roboczej i instalacja systemu operacyjnego.

Korzystanie z usługi i jej poprawna konfiguracja wymagają, aby zostały spełnione wymagania wstępne, przedstawione na rys. 37.1.



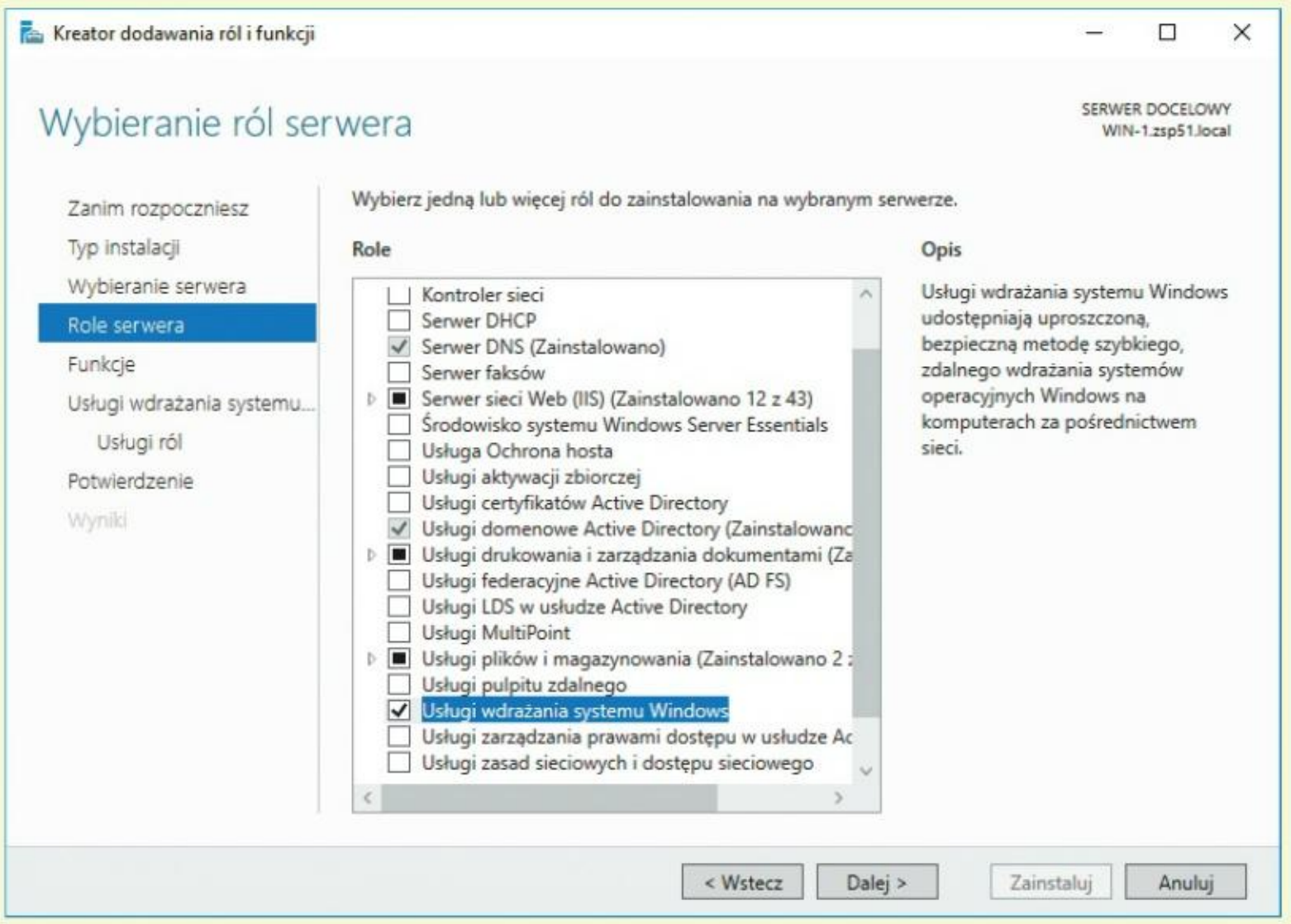
Rys. 37.1. **Wymagania wstępne konfiguracji usługi WDS**

PRZYKŁAD 37.1

Instalowanie usługi WDS na serwerze

Instalację usługi można wykonać w oknie **Menedżer serwera** przez kreatora. Aby uruchomić kreatora i przeprowadzić procedurę instalacji, należy:

1. W oknie **Menedżer serwera** kliknąć odnośnik **Dodaj role i funkcje**, wskazać opcję **Instalacja oparta na rolach lub oparta na funkcjach** i serwer do zainstalowania usługi. Kliknąć przycisk **Dalej**.
2. Zaznaczyć usługę **Usługi wdrażania systemu Windows** (ang. *Windows Deployment Services*). Kliknąć przycisk **Dalej** (rys. 37.2).



Rys. 37.2. **Wybór usług wdrażania systemu Windows do instalacji**

3. Dodać funkcje niezbędne do działania usługi.
4. Zatwierdzić wybór funkcji. Kliknąć przycisk **Dalej**.
5. Po zapoznaniu się z informacjami o usłudze kliknąć przycisk **Dalej**.
6. W oknie **Wybieranie usług ról** zaznaczyć usługi **Serwer transportu** i **Serwer wdrażania**. Kliknąć przycisk **Dalej**.
7. Zapoznać się z informacjami w oknie **Potwierdzenie opcji instalacji**. Kliknąć przycisk **Zainstaluj**, a po zakończeniu działania kreatora kliknąć przycisk **Zamknij**.

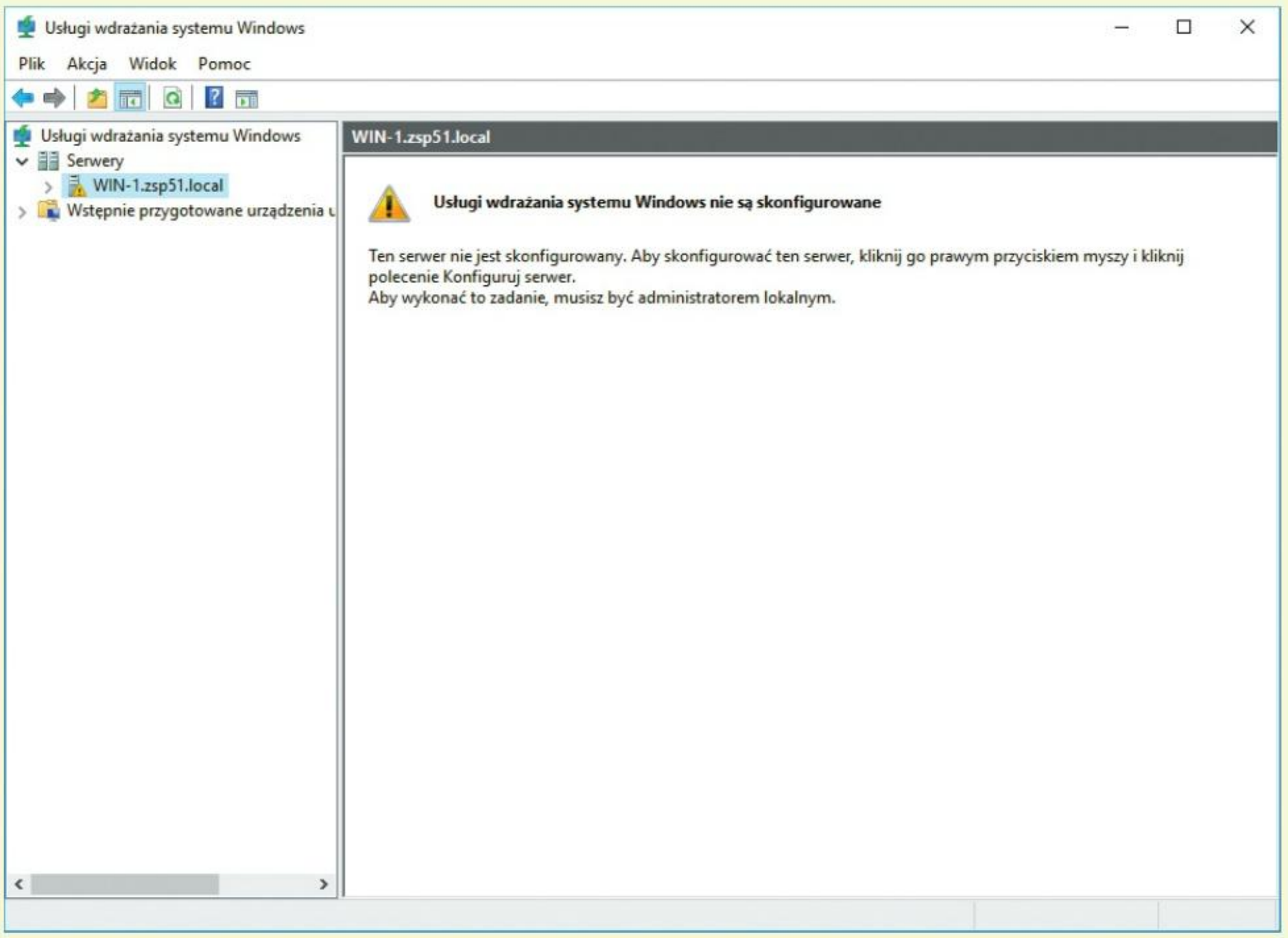
Po zainstalowaniu usługi wdrażania systemu Windows należy ją skonfigurować i uruchomić.

PRZYKŁAD 37.2

Konfigurowanie i uruchomienie usługi WDS na serwerze

Po poprawnym zainstalowaniu usługi WDS należy ją skonfigurować. W tym celu trzeba:

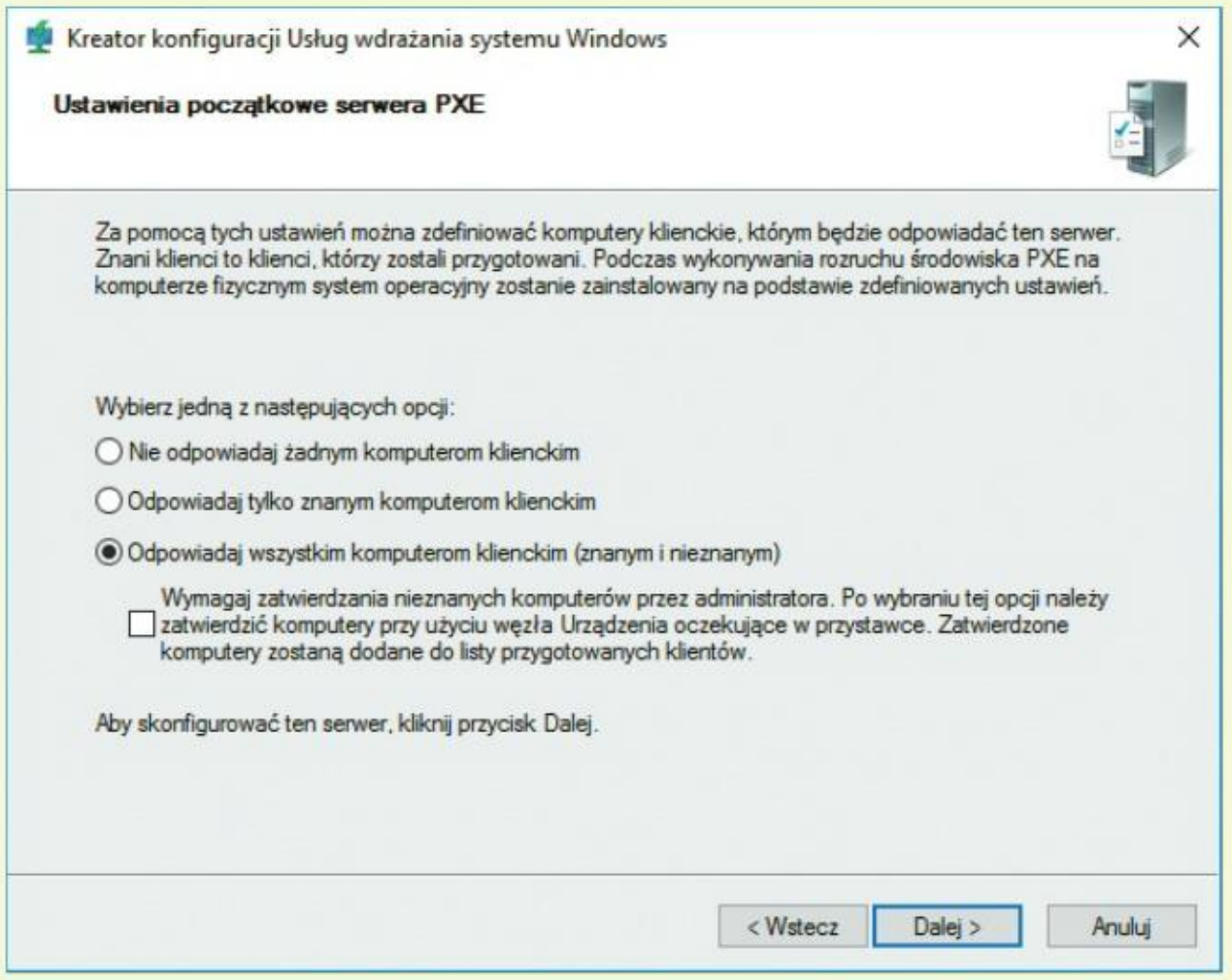
1. W oknie **Menedżer serwera** wybrać z menu **Narzędzia/Usługi wdrażania systemu Windows**. W lewym panelu rozwinąć gałąź **Serwery** i wskazać nazwę serwera (rys. 37.3).



Rys. 37.3. **Okno aplikacji usługi wdrażania systemu Windows**

2. Kliknąć prawym przyciskiem myszy ikonę serwera i z menu podręcznego wybrać polecenie **Skonfiguruj serwer** (ang. *Configure Server*). Po zapoznaniu się z informacjami o kreatorze kliknąć przycisk **Dalej**.

3. Wybrać typ serwera, np. **Serwer zintegrowany z usługą Active Directory** (ang. *Integrated with Active Directory*). Kliknąć przycisk **Dalej**.
4. Wybrać lokalizację folderu, w którym będą umieszczane obrazy i inne pliki, np. **C:\RemoteInstall**. Kliknąć przycisk **Dalej**.
5. Zatwierdzić opcje konfiguracji serwera DHCP. Kliknąć przycisk **Dalej**.
6. Wybrać komputery klienckie, którym będzie odpowiadał serwer (rys. 37.4), np. zaznaczyć opcję **Odpowiadaj wszystkim komputerom klienckim** (ang. *Respond to all client computers*). Wybranie opcji **Odpowiadaj tylko znanym komputerom klienckim** (ang. *Respond only to known client computers*) będzie wymagało, aby administrator każdorazowo akceptował komputery klienckie. Kliknąć przycisk **Dalej**. Jeżeli zostanie zaznaczona opcja **Dodaj teraz obrazy do serwera** (ang. *Add images to the server now*), to po zakończeniu kreatora automatycznie zostanie uruchomiony kreator dodawania obrazów. Jeżeli obrazy będą dodawane później, to można usunąć zaznaczenie opcji i kliknąć przycisk **Zakończ**.



Rys. 37.4. Okno wyboru komputerów klienckich, którym będzie odpowiadał serwer

Obraz bootowania umożliwia uruchamianie systemu z sieci. Taki plik znajduje się na każdym pliku ISO zawierającym wersję instalacyjną Windows. Plik **boot.wim** jest zlokalizowany w folderze **Sources** i powinien być dodany do folderu **Obrazy rozruchowe** (ang. *Boot Images*). Obraz instalacyjny (plik **install.wim**) powinien być dodany do grupy obrazów w folderze **Obrazy instalacyjne** (ang. *Install Images*).

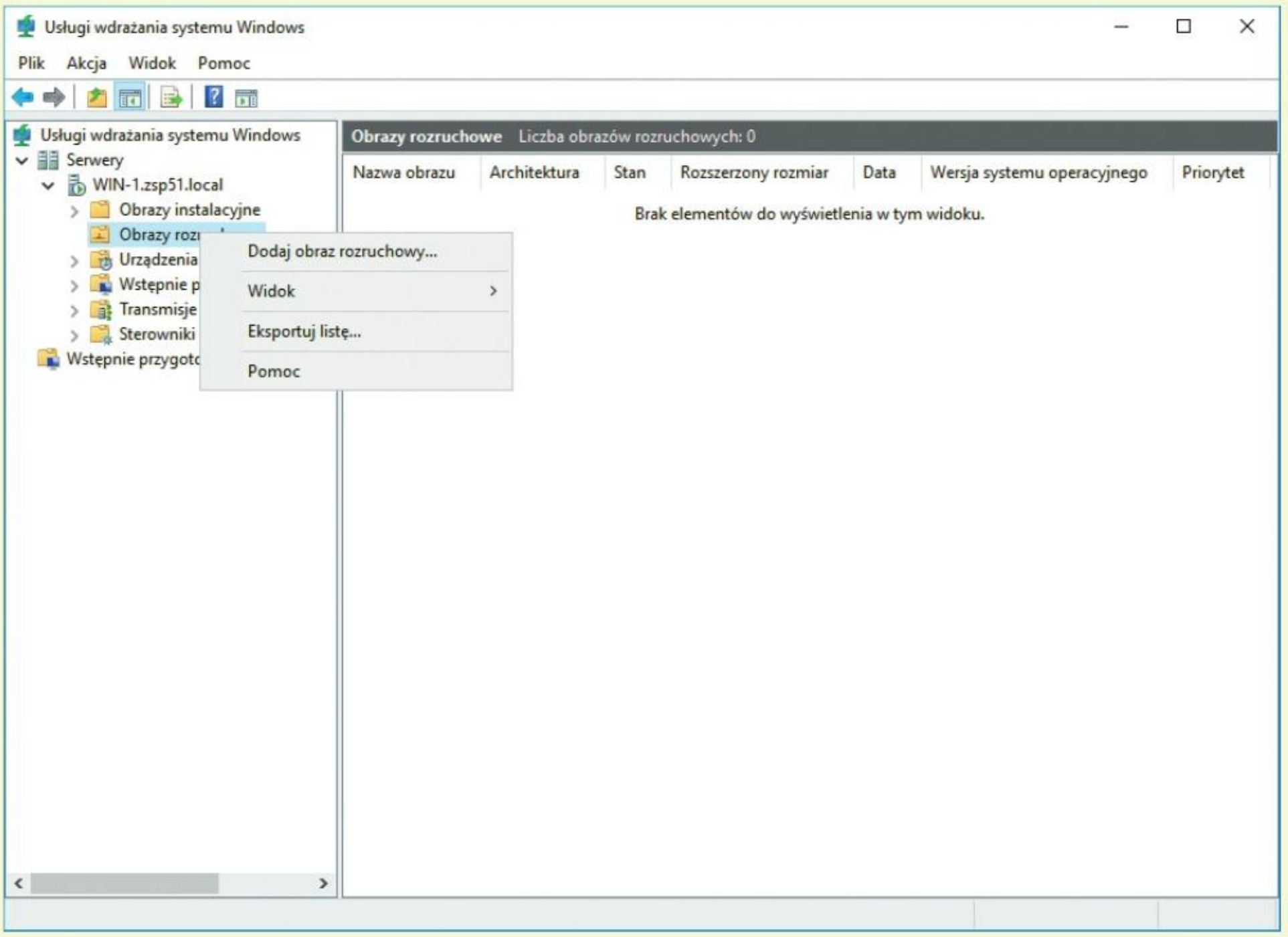
PRZYKŁAD 37.3

Przygotowanie obrazu sytemu i umieszczenie go na serwerze

Aby przygotować i dodać obraz systemu, należy:

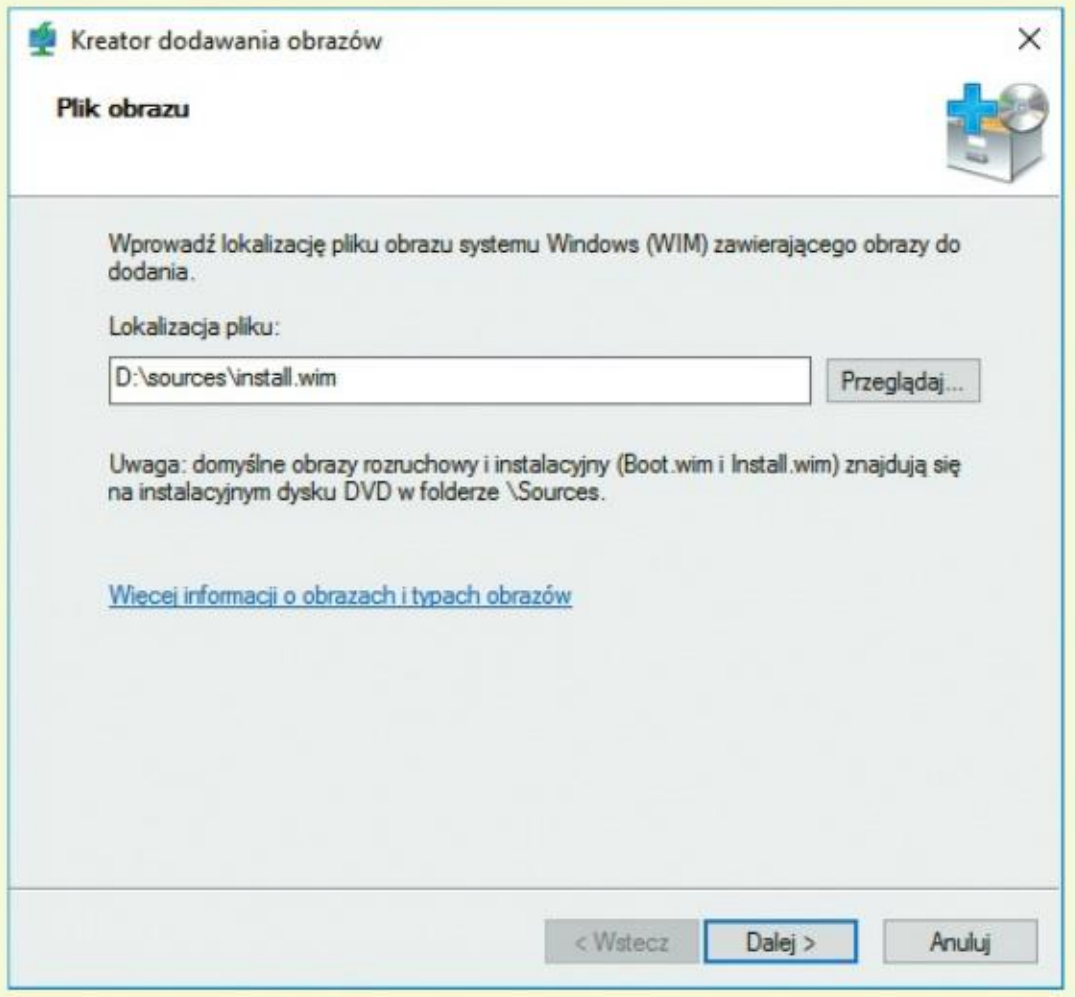
1. Uruchomić kreatora dodawania nowego obrazu. W lewym panelu okna **Usługi wdrażania systemu Windows** rozwinąć gałąź z nazwą serwera, kliknąć prawym przyciskiem myszy **Obrazy rozruchowe** i z menu podręcznego (rys. 37.5) wybrać **Dodaj obraz rozruchowy** (ang. *Add Boot Image*).

2. Wskazać położenie pliku rozruchowego **`boot.wim`**, np. **`d:\sources\boot.wim`**. Kliknąć przycisk **`Dalej`**.
3. Wprowadzić nazwę i opis obrazu, np. **`Microsoft Windows Setup (x64)`**. Kliknąć przycisk **`Dalej`**.
4. Zapoznać się z podsumowaniem. Kliknąć przycisk **`Dalej`**.
5. Po zakończeniu zadania dodawania obrazu kliknąć przycisk **`Zakończ`**. Sprawdzić, czy nowo dodany obraz pojawił się na liście dostępnych obrazów.



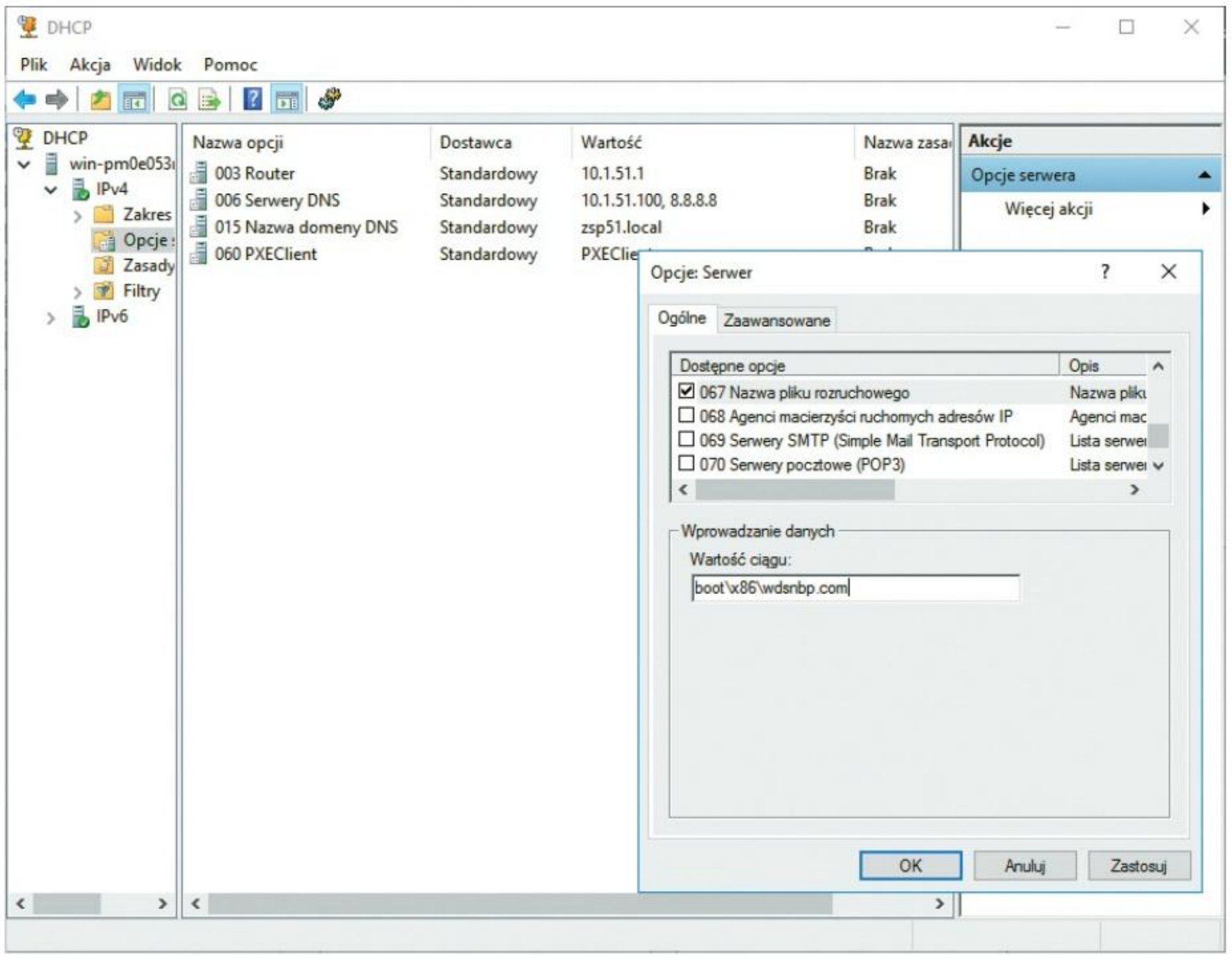
Rys. 37.5. **Uruchamianie kreatora dodawania obrazu rozruchowego**

6. Kliknąć prawym przyciskiem myszy **`Obrazy instalacyjne`** i z menu podręcznego wybrać **`Dodaj grupę obrazów`** (ang. *Add Image Group*). Wprowadzić nazwę grupy, np. **`Windows 10`**. Kliknąć przycisk **`OK`**.
7. Kliknąć prawym przyciskiem myszy nazwę grupy i z menu podręcznego wybrać **`Dodaj obraz instalacyjny`** (ang. *Add Install Image*). Wprowadzić lokalizację pliku, np. **`d:\sources\install.wim`** (rys. 37.6). Kliknąć przycisk **`Dalej`**.
8. W pliku instalacyjnym może znajdować się wiele obrazów. Zaznaczyć te, które mają być wykorzystywane, np. **`Windows 10 Pro`**, lub pozostawić zaznaczone wszystkie. Kliknąć przycisk **`Dalej`**.
9. W podsumowaniu sprawdzić, czy zostały wybrane wszystkie potrzebne obrazy. Kliknąć przycisk **`Dalej`**, a po zakończeniu dodawania obrazów kliknąć przycisk **`Zakończ`**.
10. Sprawdzić, czy nowo dodane obrazy pojawiły się na liście dostępnych obrazów.



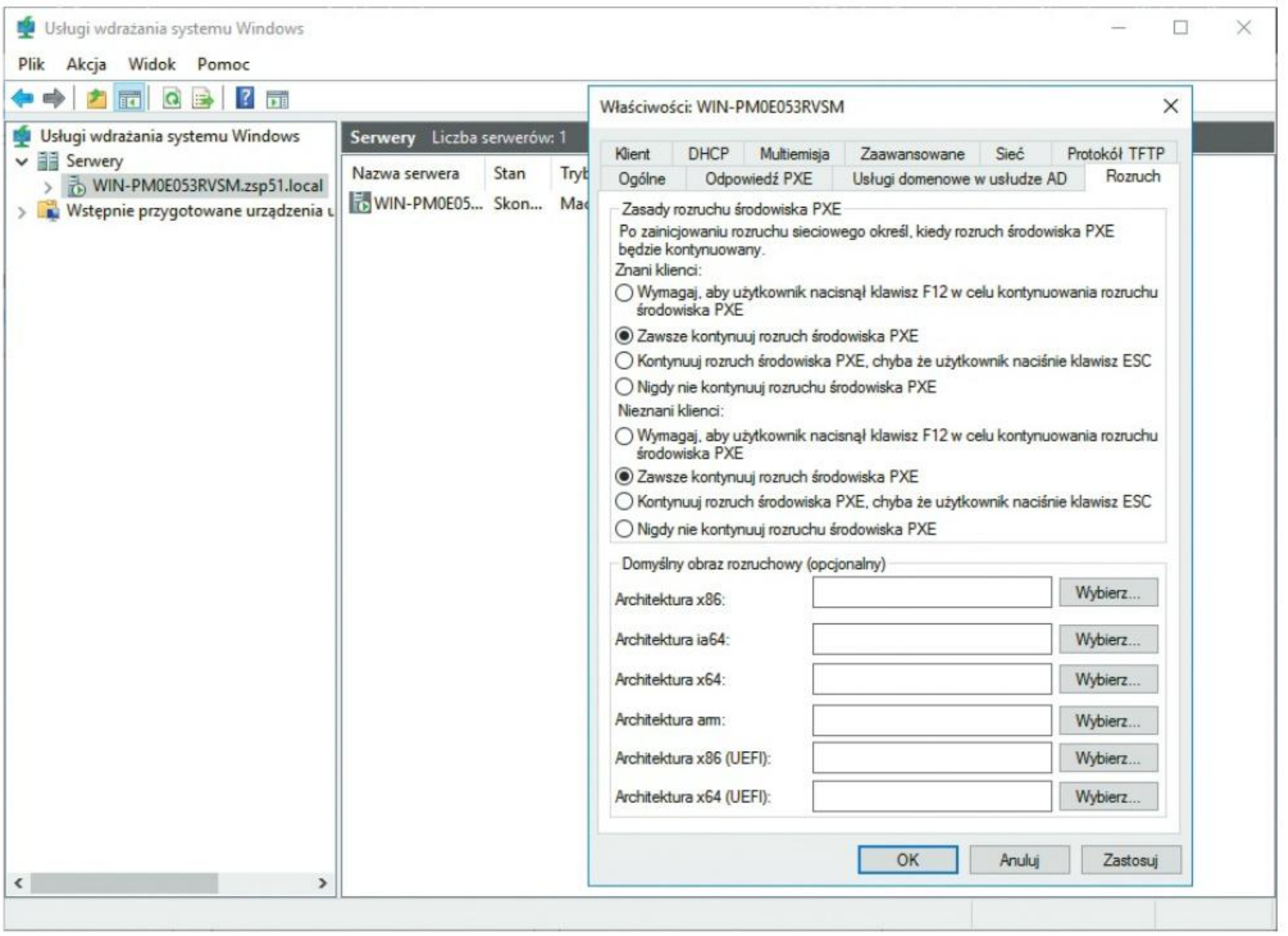
Rys. 37.6. **Dodawanie obrazów instalacyjnych**

Przed rozpoczęciem instalacji systemu na stacji roboczej należy zweryfikować lub zmodyfikować ustawienia serwera DHCP. Opcja 67 serwera DHCP powinna wskazywać nazwę pliku rozruchowego, pobieranego z serwera i uruchamianego za pośrednictwem sieci. W opcjach konfiguracyjnych serwera trzeba dodać odpowiedni wpis, np. **`boot\x86\wdsnbp.com`** (rys. 37.7).



Rys. 37.7. **Dodawanie opcji konfiguracyjnych serwera DHCP**

Standardowo uruchomienie instalacji systemu na stacji roboczej następuje po naciśnięciu klawisza [F12] w momencie rozruchu środowiska PXE. Jeżeli użytkownik nie skorzysta z klawisza w odpowiednim momencie, nastąpi próba uruchomienia systemu z dysku twardego lub innego nośnika, a w przypadku, gdy są niedostępne, jest wyświetlany komunikat błędu. Ustawienie można zmienić w konfiguracji ustawień WDS serwera. Opcja **`Zawsze kontynuuj rozruch środowiska PXE`** (rys. 37.8) spowoduje, że będzie ono uruchamiane niezależnie od wciśnięcia klawisza [F12]. Po zakończeniu instalacji należy przywrócić wcześniejsze ustawienia lub zmienić kolejność bootowania urządzeń.



Rys. 37.8. Konfigurowanie opcji rozruchu środowiska PXE

PRZYKŁAD 37.4

Przygotowanie stacji roboczej i instalacja systemu operacyjnego

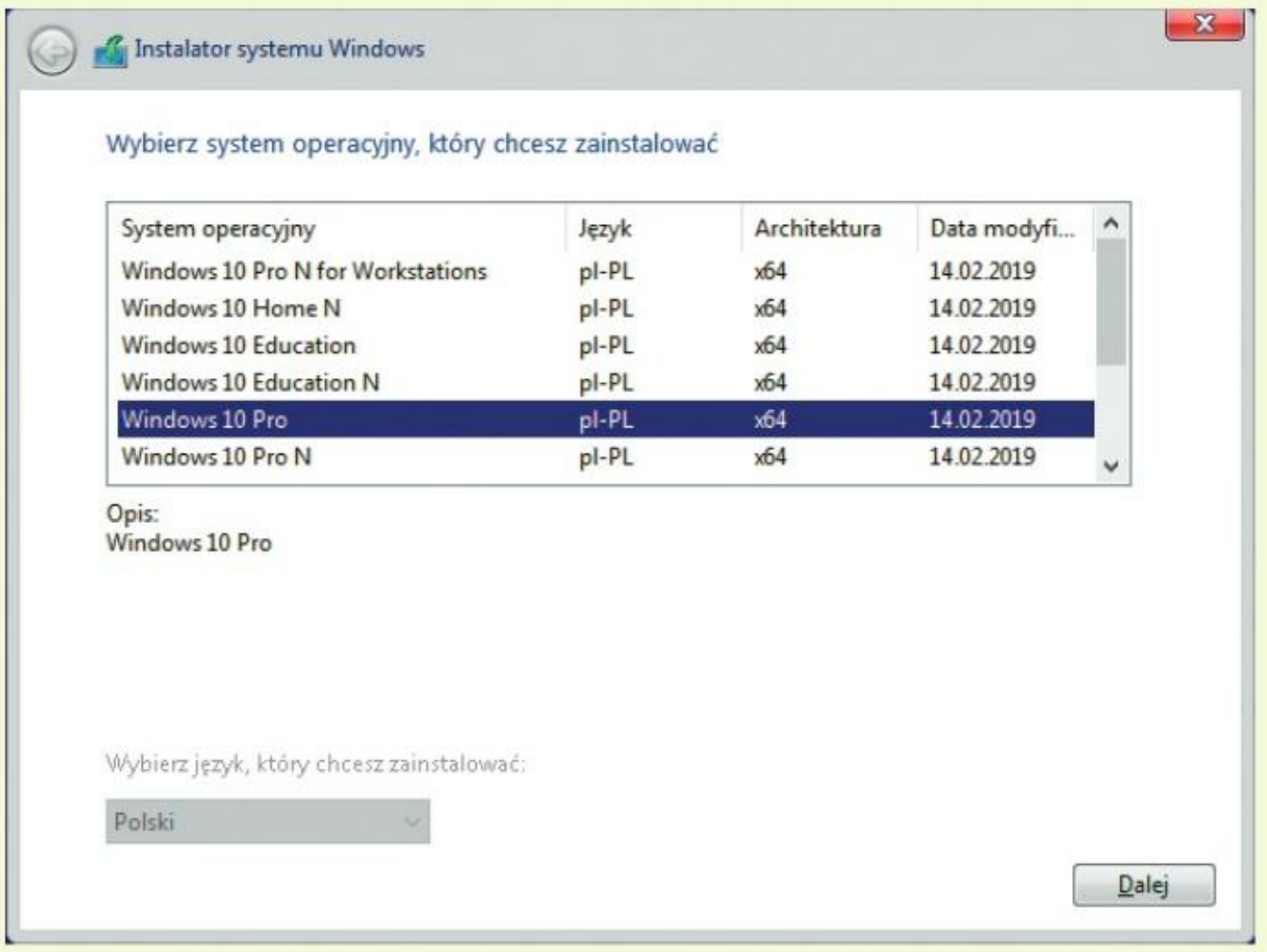
Aby przygotować stację roboczą do instalacji i przeprowadzić proces instalacji systemu, należy:

1. Podłączyć stację roboczą i serwer z uruchomionymi usługami AD, DNS, DHCP i WDS do tej samej sieci.
2. Skonfigurować kolejność uruchamiania systemu z nośników tak, aby karta sieciowa znajdowała się w kolejce wcześniej niż dysk twardy lub inne urządzenia, z których mógłby być uruchomiony system.
3. Włączyć lub ponownie uruchomić stację roboczą.
4. Po uruchomieniu okna **`Instalator systemu Windows`** wybrać ustawienia regionalne i klawiatury. Kliknąć przycisk **`Dalej`**.

5. Wprowadzić nazwę konta i hasło użytkownika domeny mającego uprawnienia do instalowania systemów za pomocą WDS (rys. 37.9).

Rys. 37.9. **Poświadczanie tożsamości użytkownika domeny**

6. Wybrać obraz systemu, który ma być zainstalowany (rys. 37.10). Kliknąć przycisk **`Dalej`**.

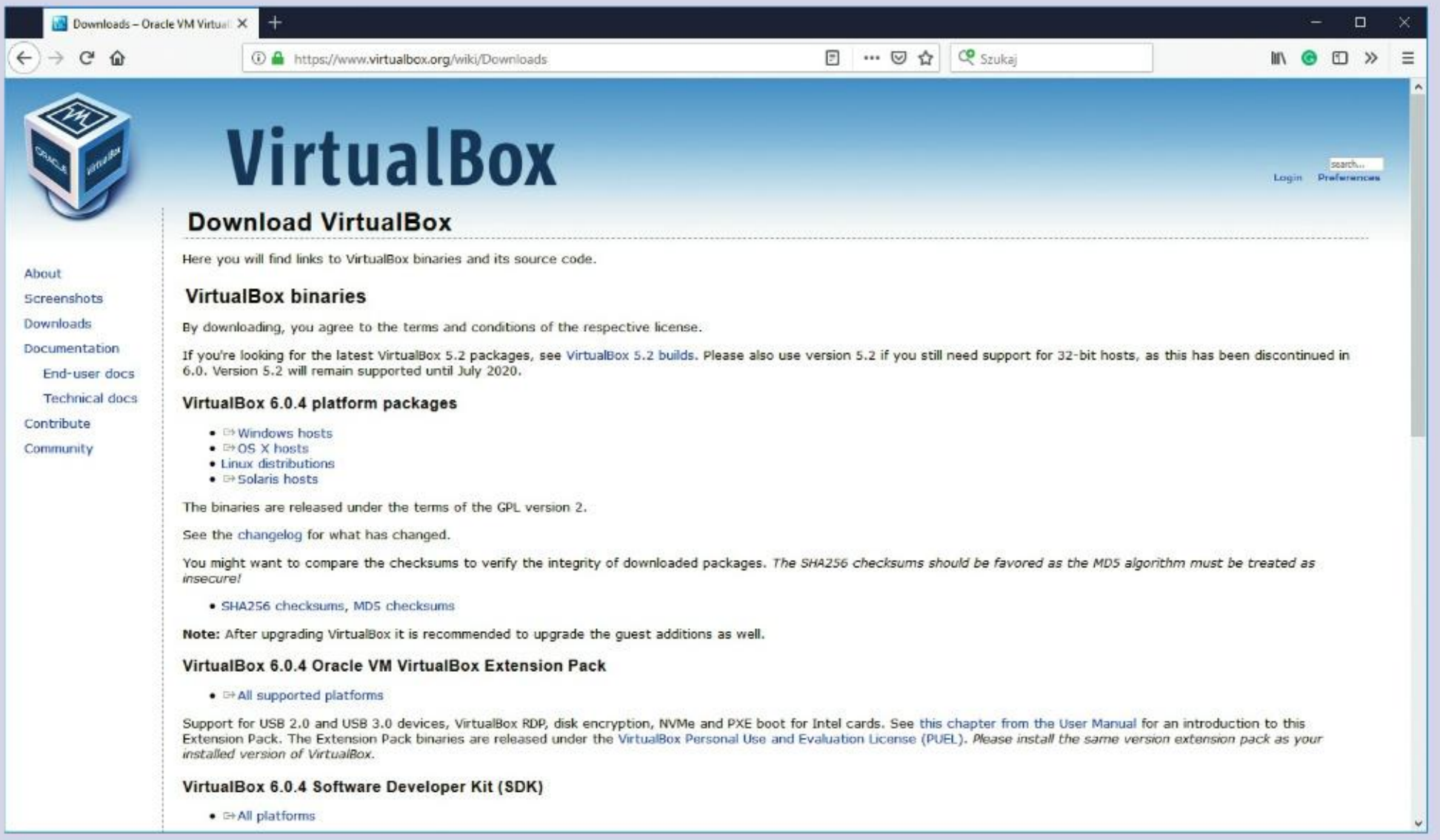


Rys. 37.10. **Wybór obrazu systemu, który ma być zainstalowany**

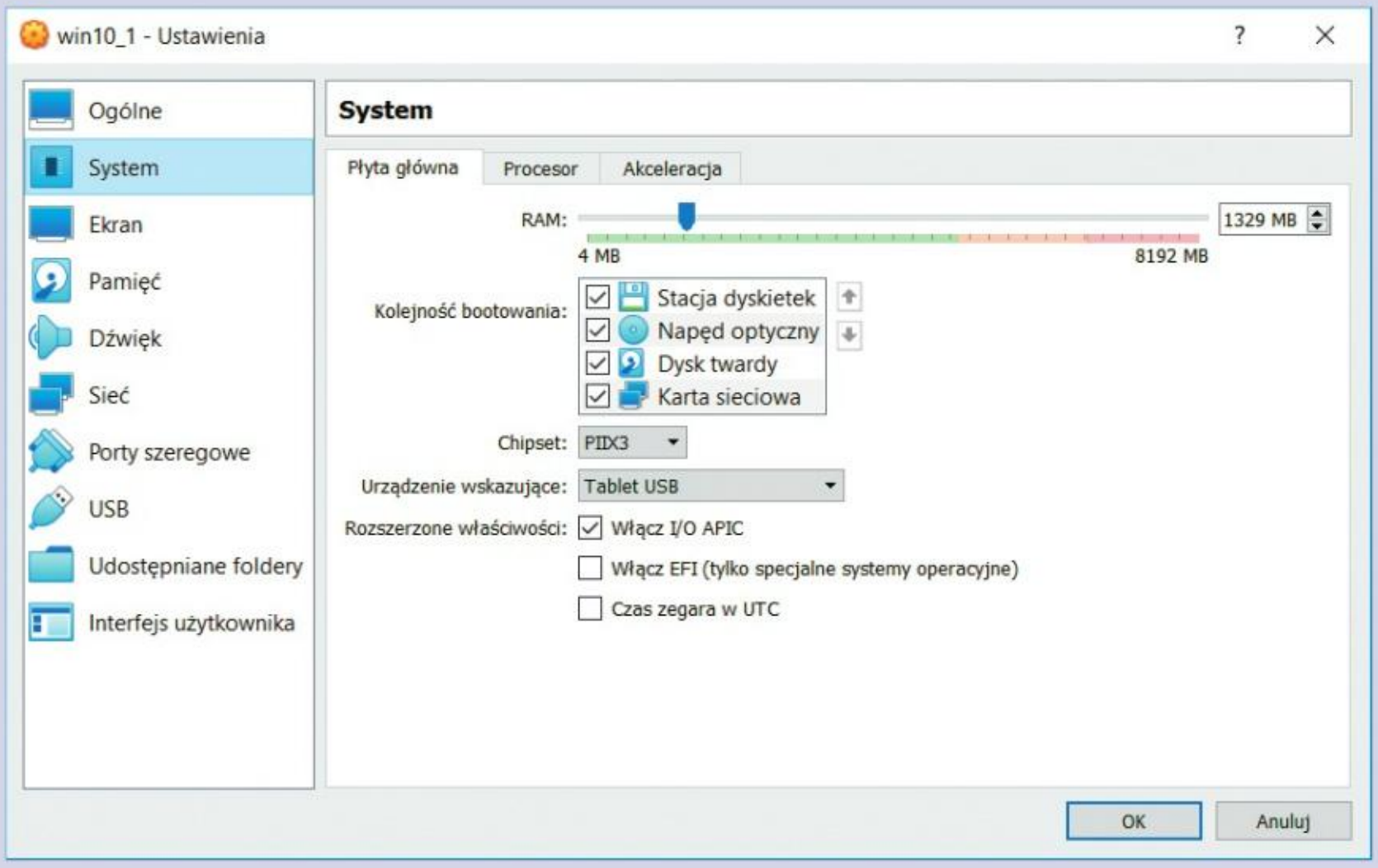
7. Postępować zgodnie z procedurą instalacji wskazywaną przez kreatora instalacji.
8. Po zakończeniu instalacji sprawdzić jej poprawność i wykonać wstępną konfigurację systemu, zgodnie z oczekiwaniami użytkownika.

! UWAGA

Jeżeli konfiguracja jest wykonywana z wykorzystaniem maszyn wirtualnych VirtualBox, to należy pobrać i zainstalować dodatek Oracle VM VirtualBox Extension Pack (rys. 37.11) i włączyć uruchamianie systemu za pośrednictwem karty sieciowej w ustawieniach stacji klienckiej (rys. 37.12).



Rys. 37.11. Strona pobierania dodatku Oracle VM VirtualBox



Rys. 37.12. Ustawianie kolejności bootowania w VirtualBox

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj usługę WDS na serwerze w szkole.
2. Przygotuj obrazy instalacyjne dla różnych wersji systemu Windows, np. XP, Vista, 7, 10, i umieść je na serwerze.
3. Przetestuj możliwość instalacji systemów przez WDS.

38 Usługi serwera aktualizacji Windows

ZAGADNIENIA

- **Zasada działania usługi aktualizacji**
- **Konfigurowanie usługi aktualizacji**
- **Zarządzanie usługami aktualizacji**
- **Korzystanie z usług aktualizacji**

Wraz ze wzrostem liczby stacji roboczych w dużych firmach rośnie liczba zadań dla administratorów, np. instalowanie aktualizacji systemu operacyjnego Windows, programu antywirusowego, pakietu biurowego i innych aplikacji. Narzędziem ułatwiającym wykonywanie aktualizacji są **Usługi serwera aktualizacji Windows WSUS** (ang. *Windows Software Update Services*).

Usługi WSUS umożliwiają:

- zmniejszenie obciążenia łącza internetowego przez jednokrotne pobranie aktualizacji z serwerów Microsoft, przechowywanie ich lokalnie i dystrybucję w obrębie lokalnej sieci;
- kontrolę administratora nad tym, które aktualizacje będą instalowane;
- określenie, które komputery mają instalować aktualizację;
- monitorowanie postępów aktualizacji i generowanie raportów o stanie aktualizacji danego komputera.

Usługi WSUS wymagają zainstalowania następujących ról:

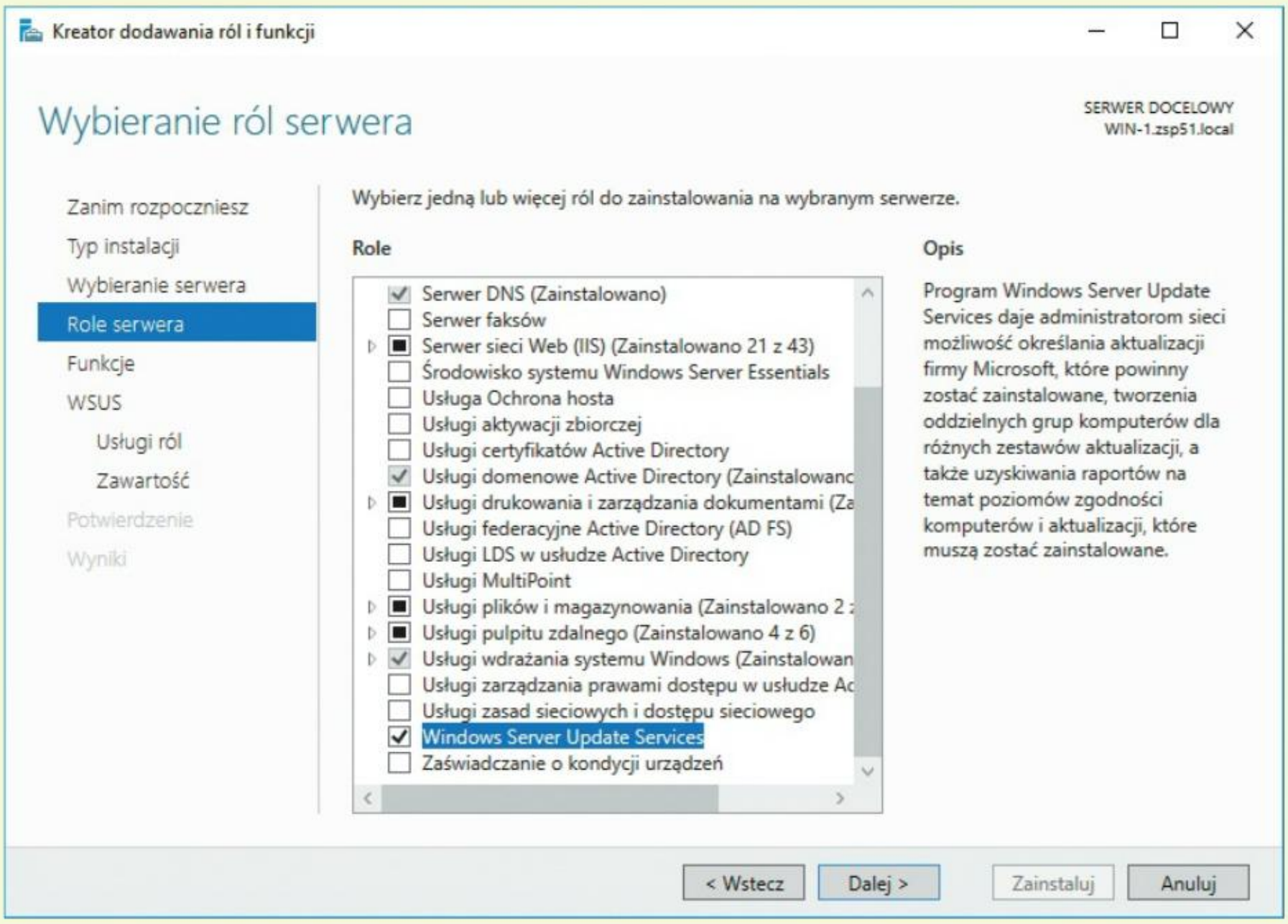
- internetowe usługi informacyjne IIS – niezbędne do łączności z komputerami klienckimi;
- Windows Internal Database – niezbędne do przechowywania konfiguracji, statusów i raportów usług WSUS; można ją zastąpić zewnętrzną bazą MSSQL.

PRZYKŁAD 38.1

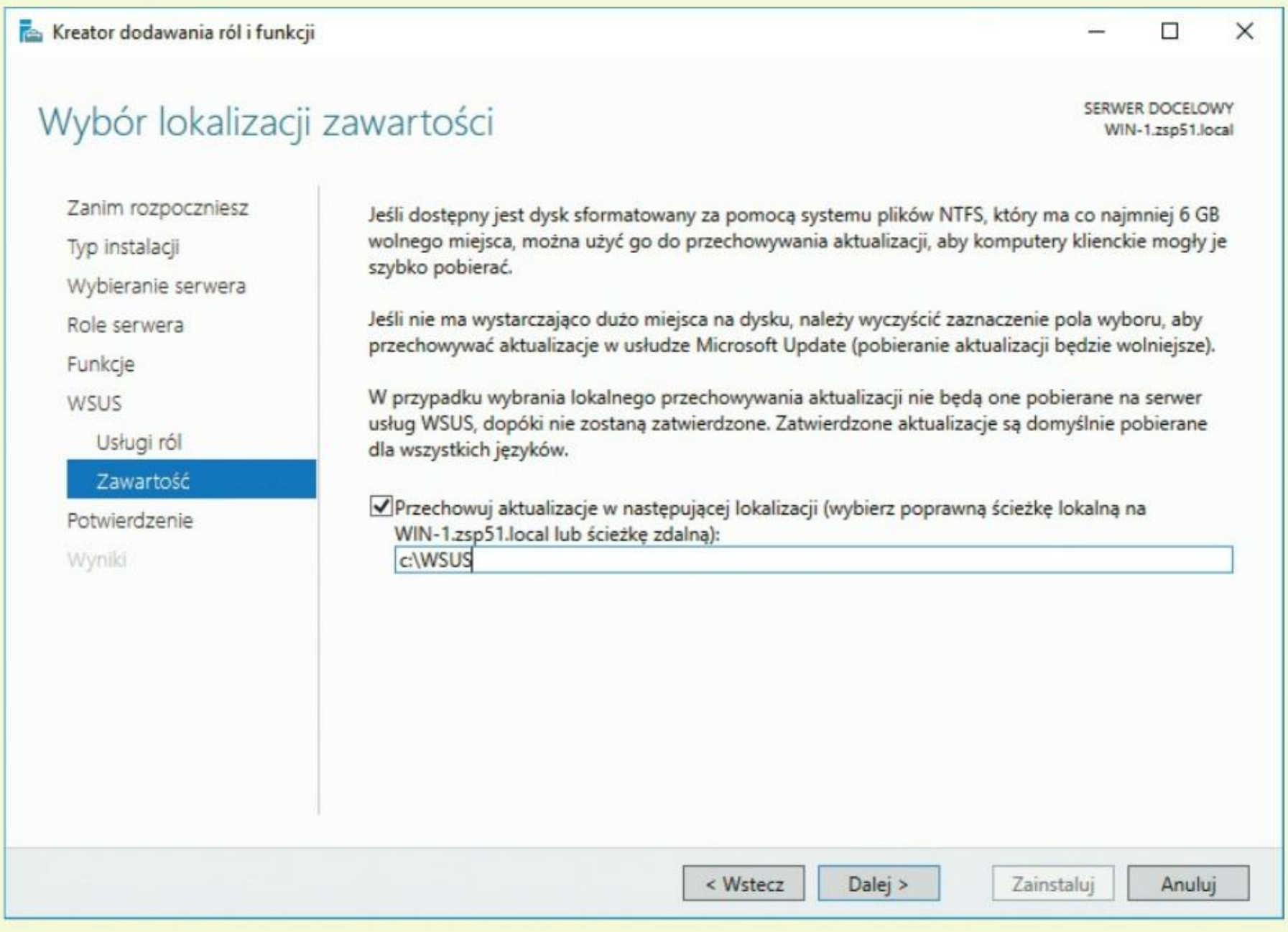
Instalacja usługi serwera aktualizacji Windows WSUS

Aby zainstalować usługi serwera aktualizacji Windows, należy:

1. Zainstalować rolę **`Windows Server Update Service`**. W oknie **`Menedżer serwera`** wybrać opcję **`Dodaj role i funkcje`**. Po zapoznaniu się z ekranem powitalnym kreatora wybrać opcję **`Instalacja oparta na rolach lub oparta na funkcjach`**. Kliknąć przycisk **`Dalej`**.
2. Wybrać serwer, który będzie odgrywać rolę serwera WSUS. Kliknąć przycisk **`Dalej`**.
3. Z listy ról wybrać **`Windows Server Update Services`** (rys. 38.1). Kliknąć przycisk **`Dalej`**. Potwierdzić zainstalowanie dodatkowych ról niezbędnych do prawidłowego działania usług, np. serwer IIS. Kliknąć przycisk **`Dodaj funkcje`**.
4. Zaakceptować bez zmian listę instalowanych funkcji. Kliknąć przycisk **`Dalej`**.
5. Wybrać usługi ról, np. **`Usługi WSUS i Łączność z bazą WID`**. Kliknąć przycisk **`Dalej`**.
6. Określić lokalizację, w której mają być przechowywane aktualizacje, np. **`C:\WSUS`** (rys. 38.2). Kliknąć przycisk **`Dalej`**.



Rys. 38.1. **Wybór roli `Windows Server Update Services`**



Rys. 38.2. **Określanie lokalizacji, w której mają być przechowywane aktualizacje**

7. Na ekranie podsumowania zweryfikować wybrane role i ustawienia. Kliknąć przycisk **Zainstaluj**, a po zakończeniu instalacji kliknąć przycisk **Zamknij**.
8. Uruchomić zadania poinstalacyjne. W lewym panelu okna **Menedżer serwera** wybrać rolę WSUS, kliknąć przycisk **Więcej**, a następnie kliknąć odnośnik **Uruchom zadania poinstalacyjne**.

Po zakończeniu procesu poinstalacyjnego można przejść do konfiguracji usług.

PRZYKŁAD 38.2

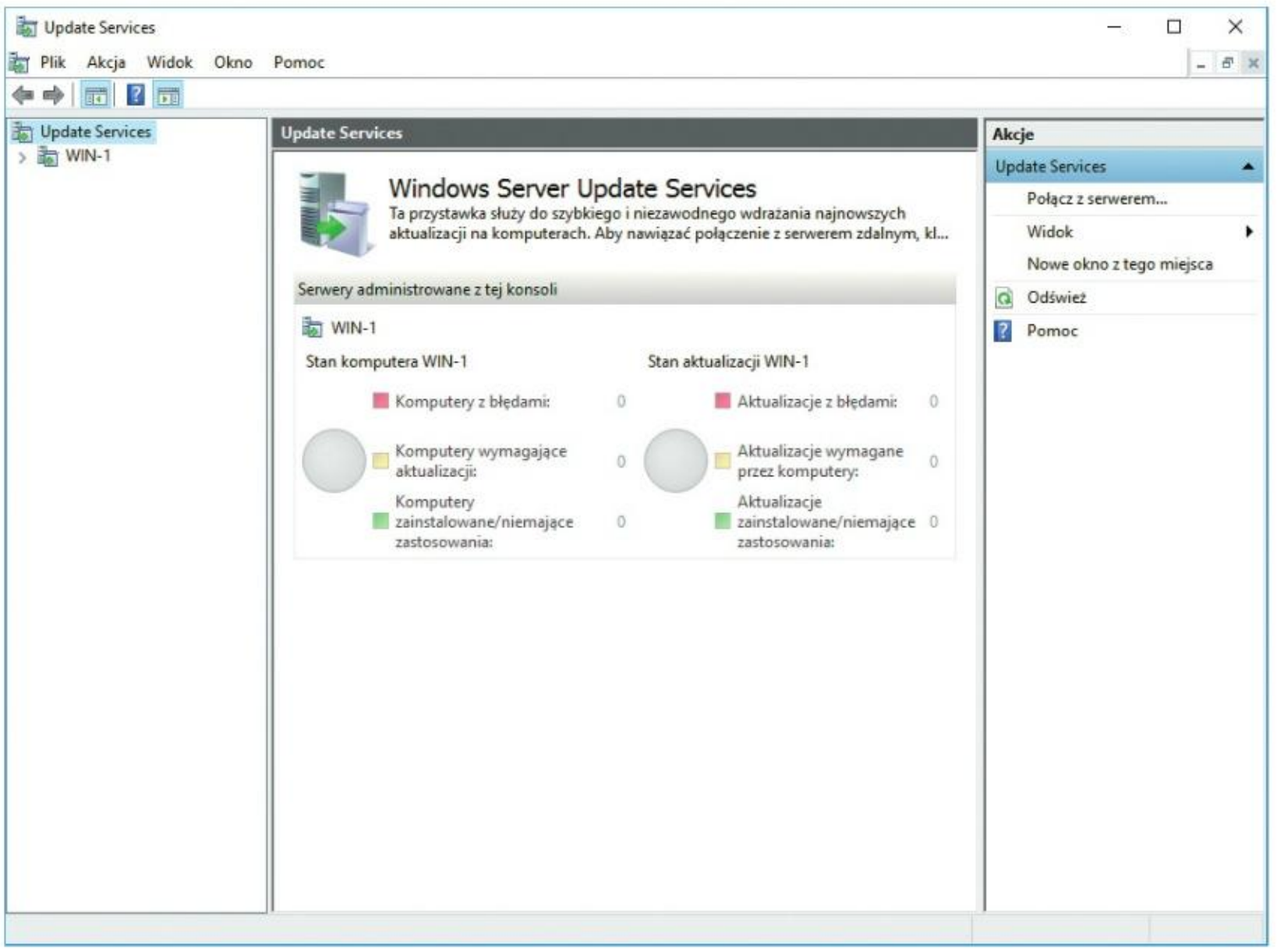
Konfiguracja usługi serwera aktualizacji Windows WSUS

Aby skonfigurować usługi serwera aktualizacji Windows do pracy, należy:

1. W oknie **Menedżer serwera** z menu wybrać polecenie **Narzędzia/Windows Software Update Services**.
2. W oknie **Kreator konfiguracji** zapoznać się z informacjami o procesie konfiguracji. Kliknąć przycisk **Dalej**.
3. Określić, czy użytkownik chce przystąpić do **Programu poprawy jakości rozszerzenia Microsoft Update**. Z tej opcji można zrezygnować, ponieważ serwer jest konfigurowany w celach edukacyjnych.
4. Wybrać serwer nadrzędny. Jeżeli jest konfigurowany serwer podstawowy w organizacji, to należy wskazać, że serwerem nadrzędnym będą Serwery Windows Update. Jeżeli jest konfigurowany serwer podrzędny w organizacji, to trzeba zaznaczyć opcję **Synchronizowany z innym serwerem Windows Server Update Services** i wskazać nazwę serwera nadrzędnego. Wybrać opcję **Synchronizuj z witryną Microsoft Update**. Kliknąć przycisk **Dalej**.
5. Określić, czy w organizacji jest używany serwer proxy do połączenia z serwerem Windows Update. Jeśli tak, to trzeba podać dane niezbędne do połączenia. Pozostawić opcję niezaznaczoną. Kliknąć przycisk **Dalej**.
6. Pobrać ustawienia z serwera nadrzędnego. Kliknąć przycisk **Rozpocznij połączenie**. Po zakończeniu pobierania kliknąć przycisk **Dalej**.
7. Po pobraniu ustawień wskazać języki aktualizacji, np. wybrać tylko języki polski i angielski. Kliknąć przycisk **Dalej**.
8. Wybrać produkty, do których mają być instalowane aktualizacje, np. tylko Windows 10. Kliknąć przycisk **Dalej**.
9. Klasyfikacje aktualizacji do pobrania – pozostawić te opcje bez zmian. Kliknąć przycisk **Dalej**.
10. Skonfigurować harmonogram synchronizacji, np. raz dziennie, i określić, kiedy ma być wykonana pierwsza synchronizacja, np. po zakończeniu kreatora. Kliknąć przycisk **Dalej**.
11. Zaznaczyć opcję **Rozpocznij wstępną synchronizację**. Kliknąć przycisk **Dalej**, a następnie **Zakończ**.

Po zakończeniu tej procedury serwer WSUS jest wstępnie przygotowany do pracy (rys. 38.3).

Serwer należy opublikować w organizacji i zatwierdzić aktualizacje po zsynchronizowaniu z serwerem nadrzędnym.



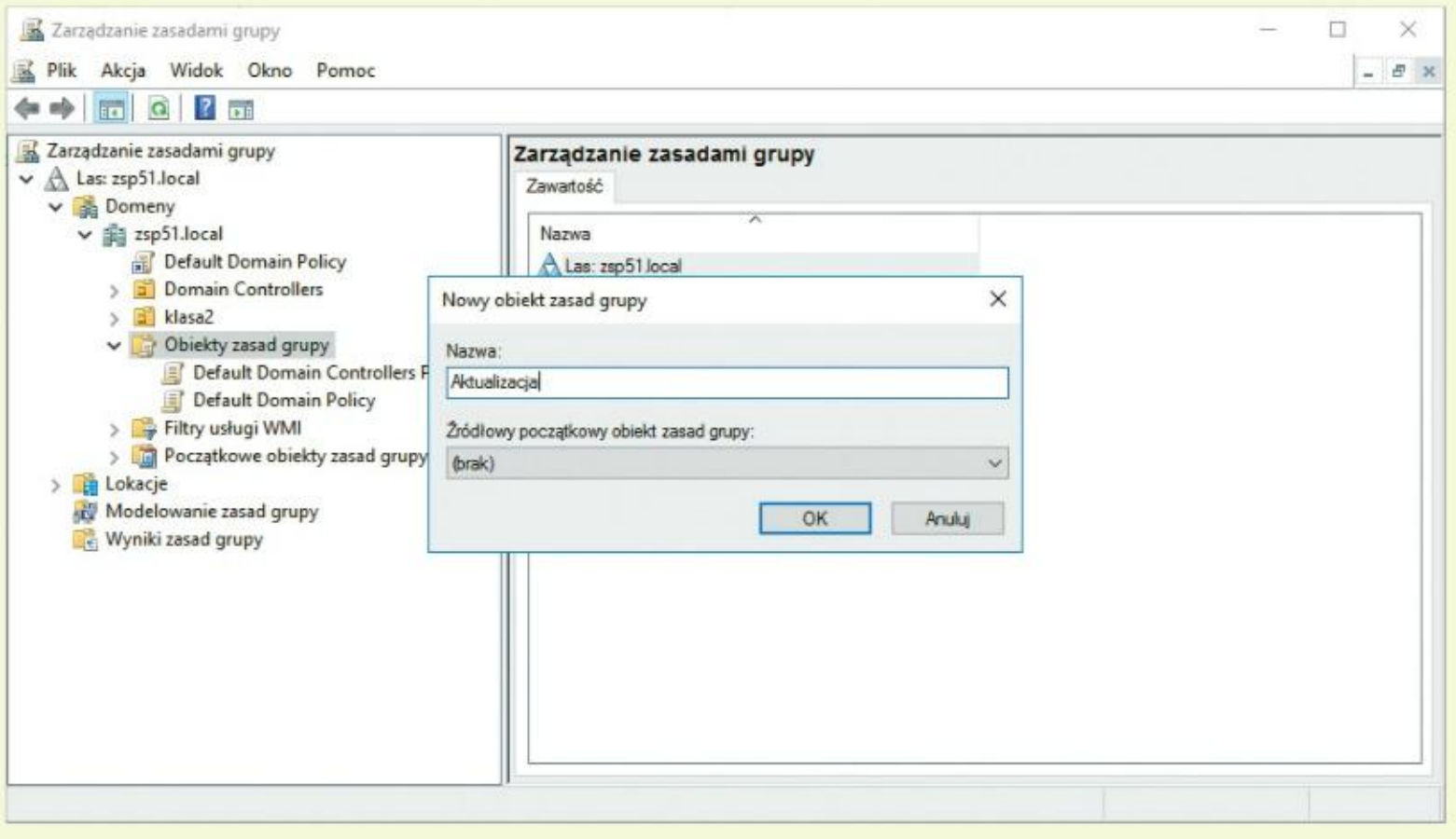
Rys. 38.3. Konsola zarządzania usługą `Update Services`

PRZYKŁAD 38.3

Udostępnienie usługi serwera aktualizacji Windows WSUS

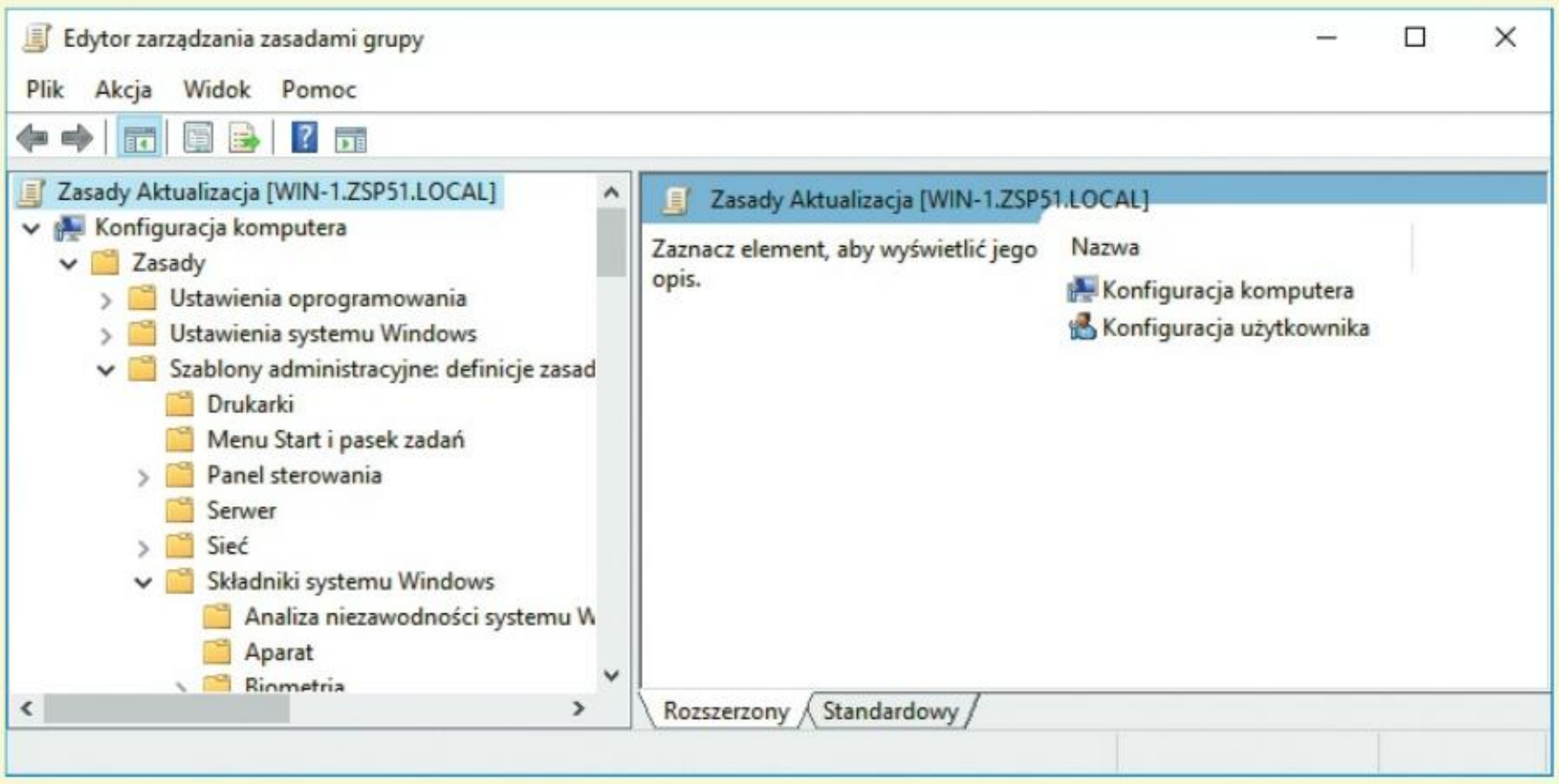
Aby udostępnić usługi serwera aktualizacji Windows dla użytkowników, należy:

1. Utworzyć i skonfigurować **`obiekt zasad grupy GPO`** (ang. *Group Policy Object*) w domenie Active Directory. Uruchomić edytor zasad grupy **`Start/Narzędzia administracyjne/Zarządzanie zasadami grupy`**.
2. W lewym panelu rozwinąć gałąź **`Las/Domeny/Nazwa domeny`**. Kliknąć prawym klawiszem myszy **`Obiekty zasad grupy`** i z menu kontekstowego wybrać **`Nowe`**. Wprowadzić nazwę obiektu, np. **`Aktualizacja`** (rys. 38.4), i kliknąć przycisk **`OK`**.

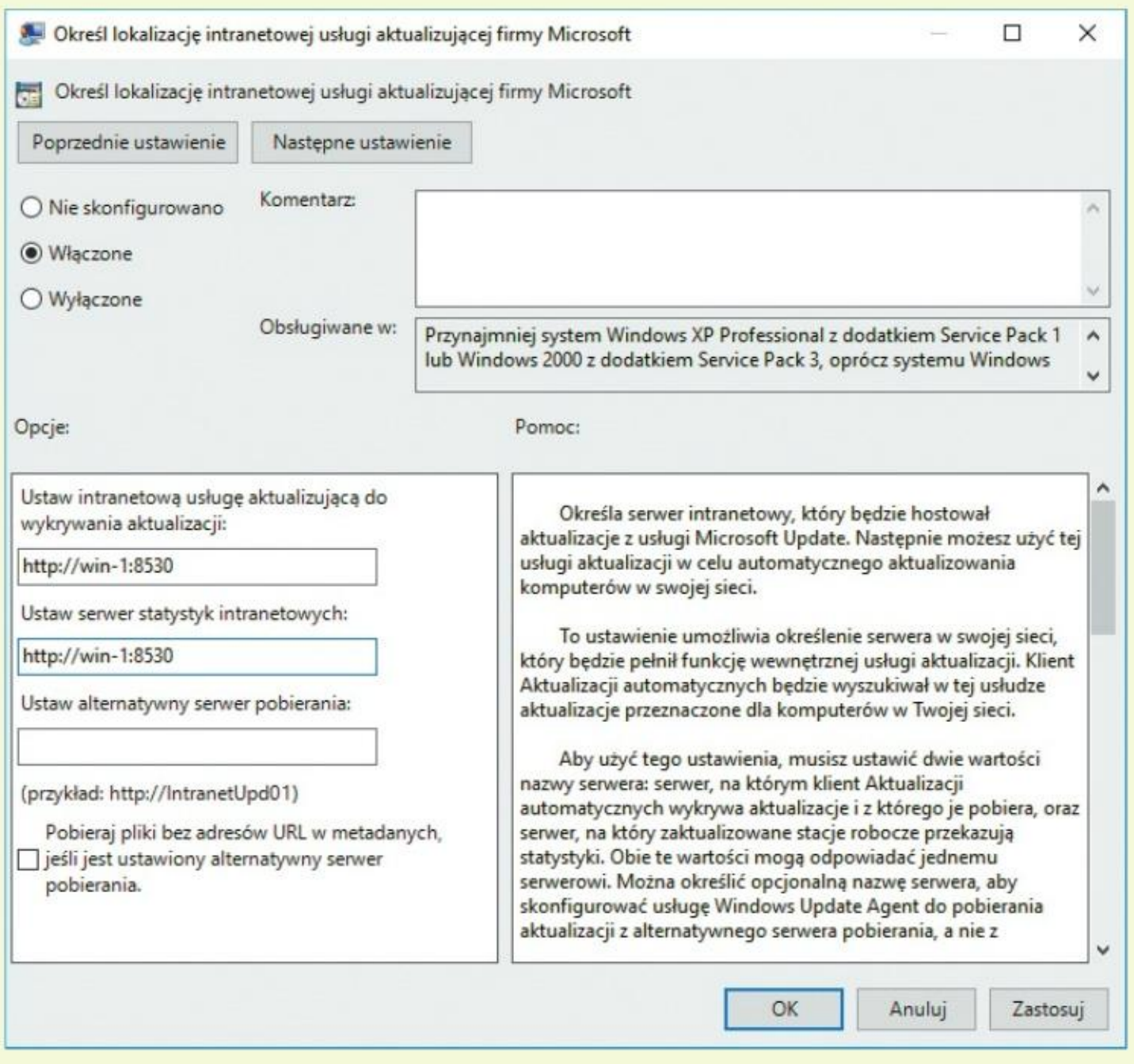


Rys. 38.4. Tworzenie obiektu zasad grupy

3. Kliknąć prawym klawiszem myszy obiekt i z menu kontekstowego wybrać **Edytuj**. W gałęzi **Konfiguracja komputera/Zasady/Szablony Administracyjne/Składniki systemu Windows** (rys. 38.5) kliknąć klucz **Usługa Windows Update**. Odszukać i dwukrotnie kliknąć ustawienie **Określ lokalizację internetową usługi aktualizującej firmy Microsoft** (rys. 38.6). Zaznaczyć opcję **Włączone**. W sekcji **Opcje** wprowadzić adres IP lub nazwę wdrażanego serwera i numer portu, na którym nasłuchuje, np. **http://win-1:8530**. Kliknąć przycisk **OK**.

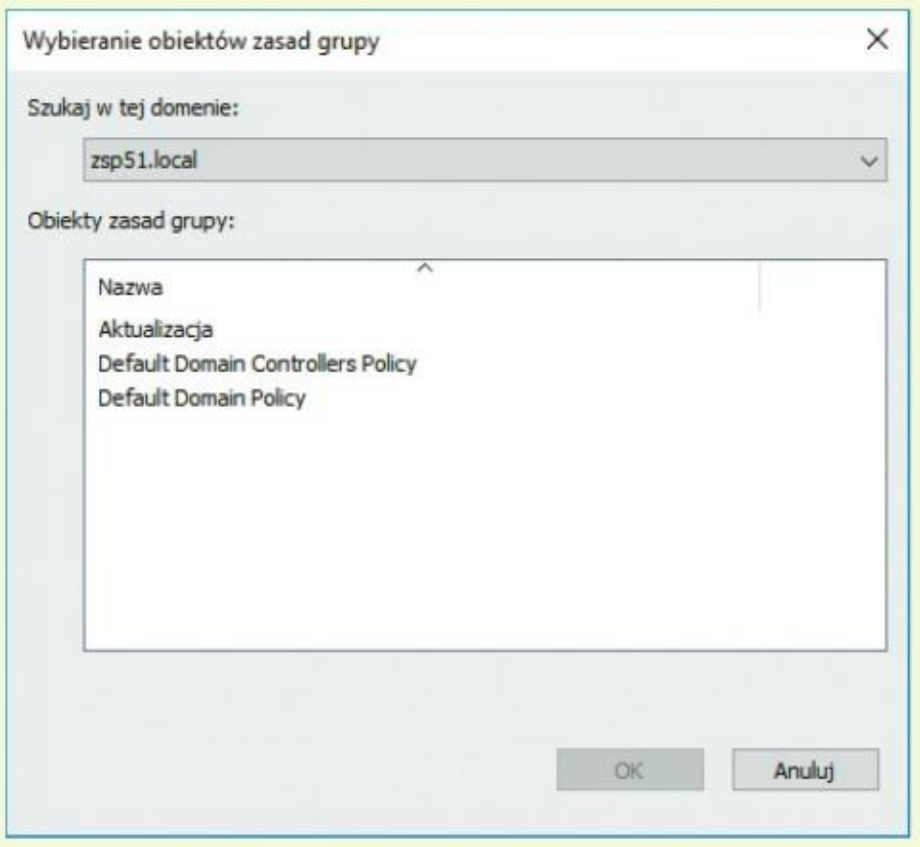


Rys. 38.5. **Lokalizowanie szablonu administracyjnego do konfiguracji usługi `Windows Update`**



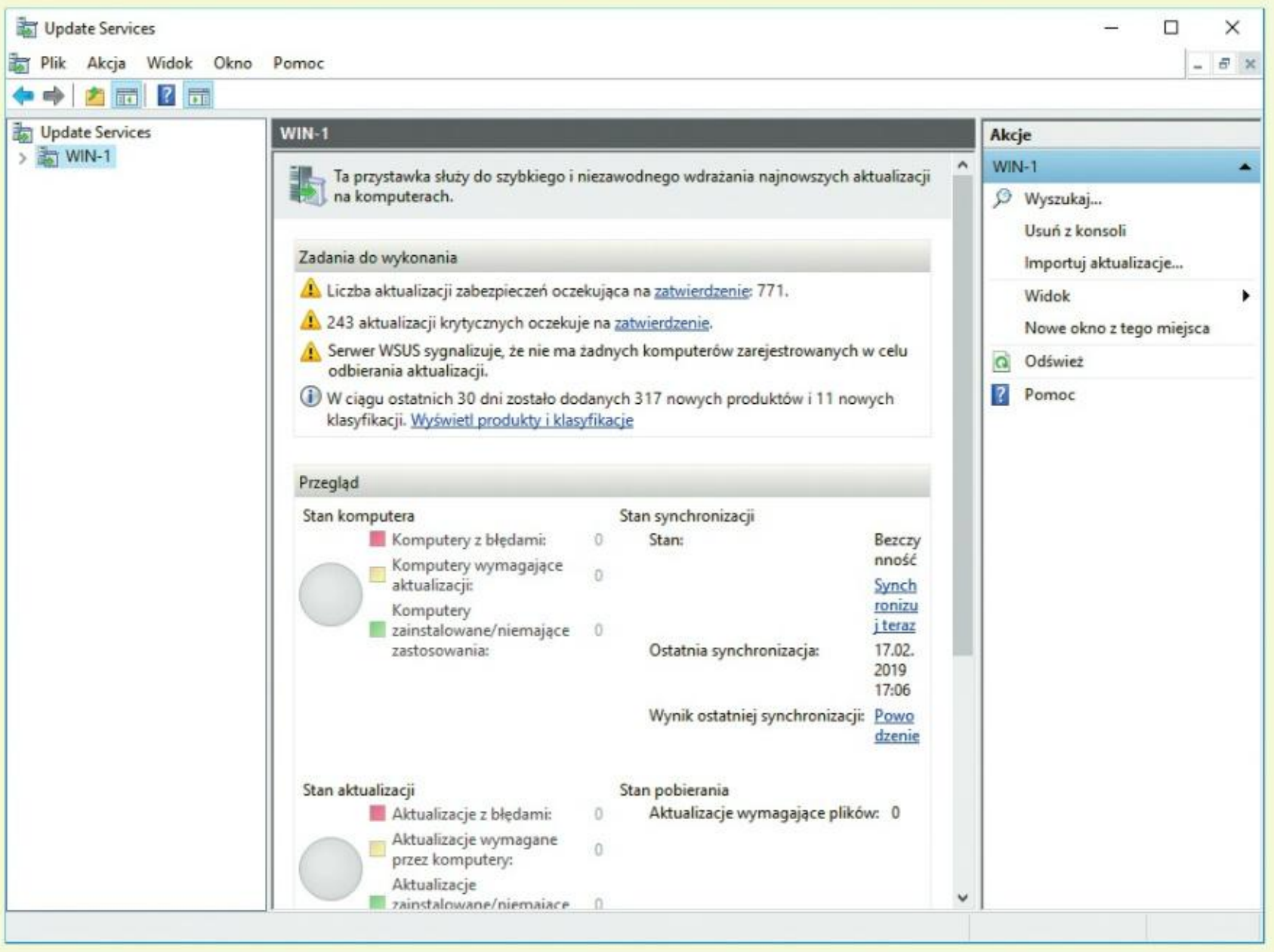
Rys. 38.6. **Określanie lokalizacji internetowej usługi aktualizującej firmy Microsoft**

4. W konsoli **Zarządzanie Zasadami Grupy** przypisać zasadę do jednostki organizacyjnej lub domeny w Active Directory. Kliknąć prawym klawiszem myszy nazwę domeny lub jednostki organizacyjnej, np. **zsp51.local**, i z menu kontekstowego wybrać polecenie **Połącz z istniejącym obiektem zasad grupy** (rys. 38.7). Wskazać nazwę obiektu, np. **Aktualizacja**. Kliknąć przycisk **OK**.



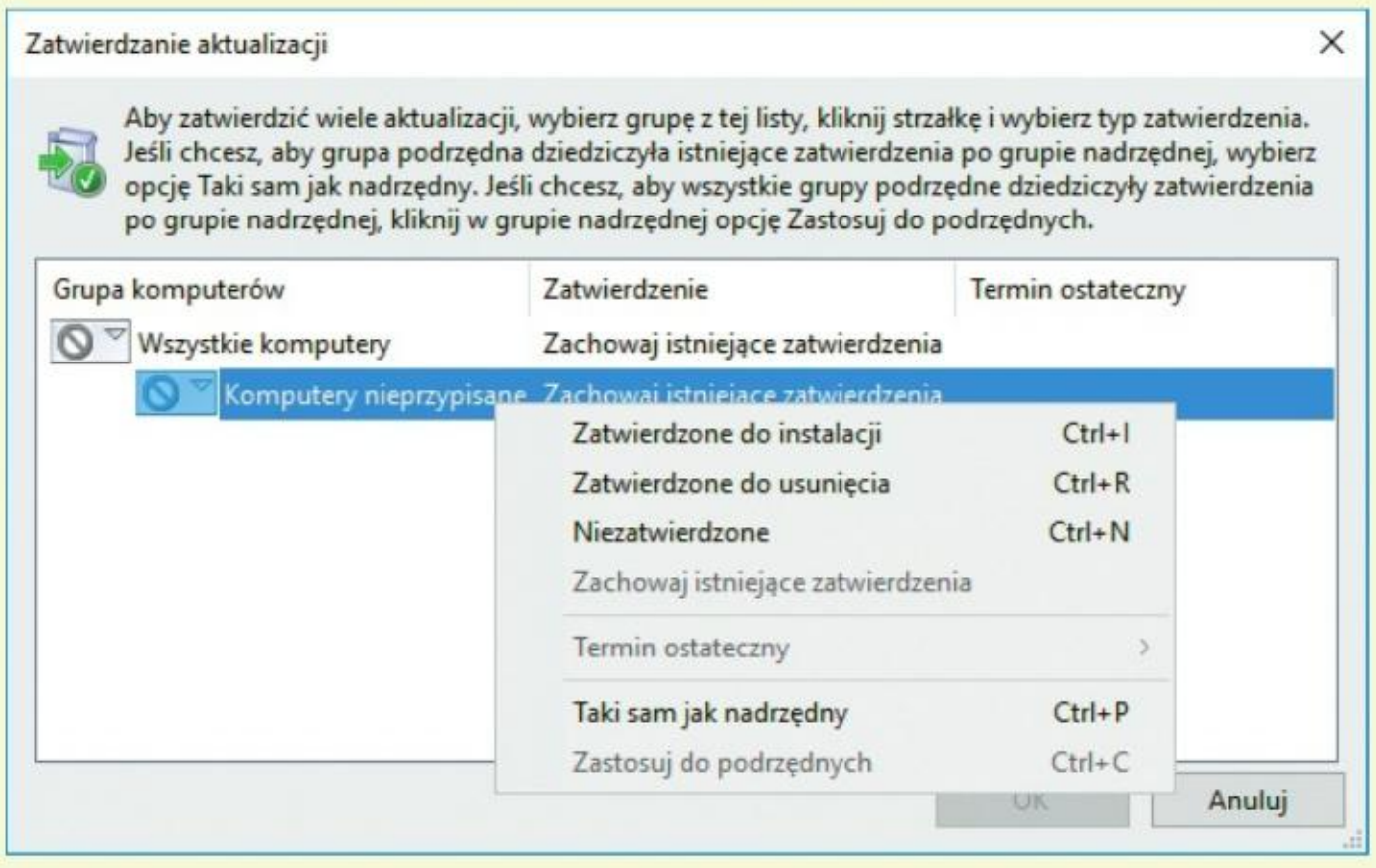
Rys. 38.7. **Łączenie obiektu GPO z domeną**

5. Zatwierdzić aktualizację do instalacji. Na serwerze WSUS uruchomić konsolę zarządzania **Windows Server Update Services** i po wybraniu nazwy serwera w drzewie konsoli sprawdzić status synchronizacji z serwerami **Windows Update** (rys. 38.8).



Rys. 38.8. **Sprawdzanie statusu synchronizacji z serwerami Windows Update**

6. W lewym panelu rozwinąć gałąź **Update Services/Nazwa serwera/Aktualizacje**. Zaznaczyć aplikacje do zatwierdzenia i z menu kontekstowego wybrać polecenie **Zatwierdź**.
7. Kliknąć prawym klawiszem myszy **Wszystkie komputery** i wybrać z menu polecenie **Zatwierdzone do instalacji** (rys. 38.9). Kliknąć przycisk **OK**.



Rys. 38.9. **Zatwierdzanie aktualizacji**

Jeśli synchronizacja zakończy się powodzeniem, to usługa jest gotowa do pracy. Postępy instalacji aktualizacji na stacjach roboczych można obserwować po wybraniu opcji **Wszystkie komputery** w drzewie konsoli.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Skonfiguruj usługę serwera aktualizacji na serwerze w szkole.
2. Sporządź listę aktualizacji, która powinna być dostępna na serwerze w szkole.

39 Usługi zasad sieciowych i dostępu sieciowego

ZAGADNIENIA

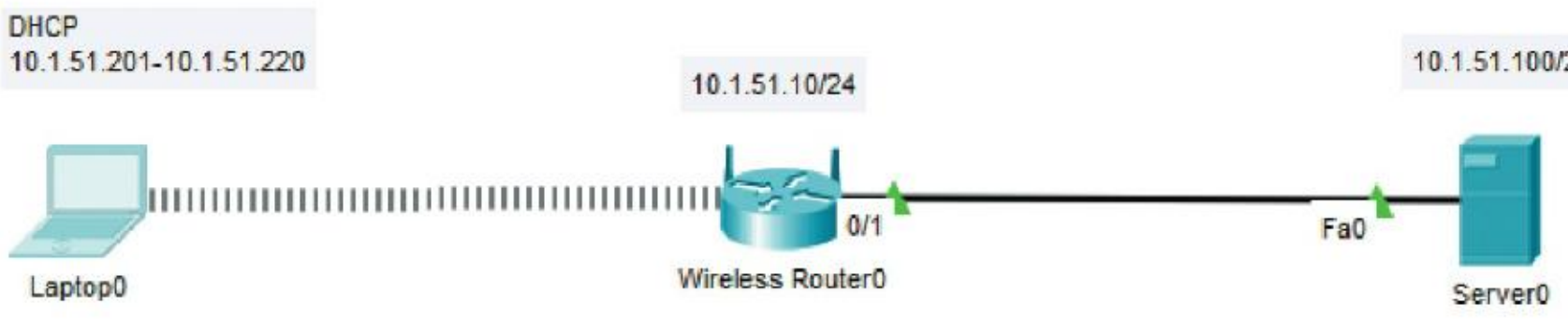
Zadania serwera zasad sieciowych i dostępu sieciowego **Konfigurowanie serwera zasad sieciowych i dostępu sieciowego** **Korzystanie z serwera zasad sieciowych i dostępu sieciowego**

Serwer zasad sieciowych – NPS (ang. *Network Policy Server*) umożliwia tworzenie i wymuszanie zasad dostępu do sieci, aby uwierzytelnić i autoryzować użytkowników. Serwer zasad sieciowych może przeprowadzać scentralizowane uwierzytelnianie, autoryzację i ewidencjonowanie aktywności dla połączeń bezprzewodowych Wi-Fi, przełączników mających funkcje uwierzytelniania, zdalnego dostępu telefonicznego i połączeń sieci VPN. Serwer NPS jest używany jako **serwer RADIUS**, natomiast urządzenia sieciowe, takie jak bezprzewodowe punkty dostępowe lub przełączniki, odgrywają rolę **klientów RADIUS**.

Proces konfiguracji usługi obejmuje:

- konfigurację punktu dostępowego do obsługi uwierzytelniania RADIUS;
- utworzenie konta użytkownika uprawnionego do logowania i przypisanie go do grupy;
- instalowanie i konfigurowanie Usługi certyfikatów Active Directory;
- generowanie i instalowanie certyfikatów kontrolera domeny;
- instalowanie i konfigurowanie serwera zasad sieciowych i serwera DHCP;
- konfigurowanie serwera zasad sieciowych i roli serwera dostępu;
- konfigurowanie połączenia sieci bezprzewodowej w komputerze użytkownika.

Poszczególne elementy procesu konfiguracji zostaną opisane w kolejnych przykładach.



Rys. 39.1. **Schemat sieci do implementacji usługi zasad sieciowych i dostępu sieciowego**

PRZYKŁAD 39.1

Konfigurowanie punktu dostępowego do obsługi uwierzytelniania RADIUS

Aby zainstalować i skonfigurować punkt dostępowy do obsługi uwierzytelniania RADIUS, należy:

1. Połączyć urządzenia według schematu z rys. 39.1. Skonfigurować adresy IP urządzeń: serwer – `10.1.51.100`, punkt dostępowy – `10.1.51.11`. Ustawić maskę sieciową `255.255.255.0` i domyślną bramę `10.1.51.1`.

2. Za pomocą przeglądarki internetowej połączyć się z punktem dostępowym.
3. Skonfigurować identyfikator SSID, np. **`zsp51`**, i ustawienia bezpieczeństwa sieci bezprzewodowej (jak na rys. 39.2).

Rys. 39.2. **Ustawienia bezpieczeństwa sieci bezprzewodowej**

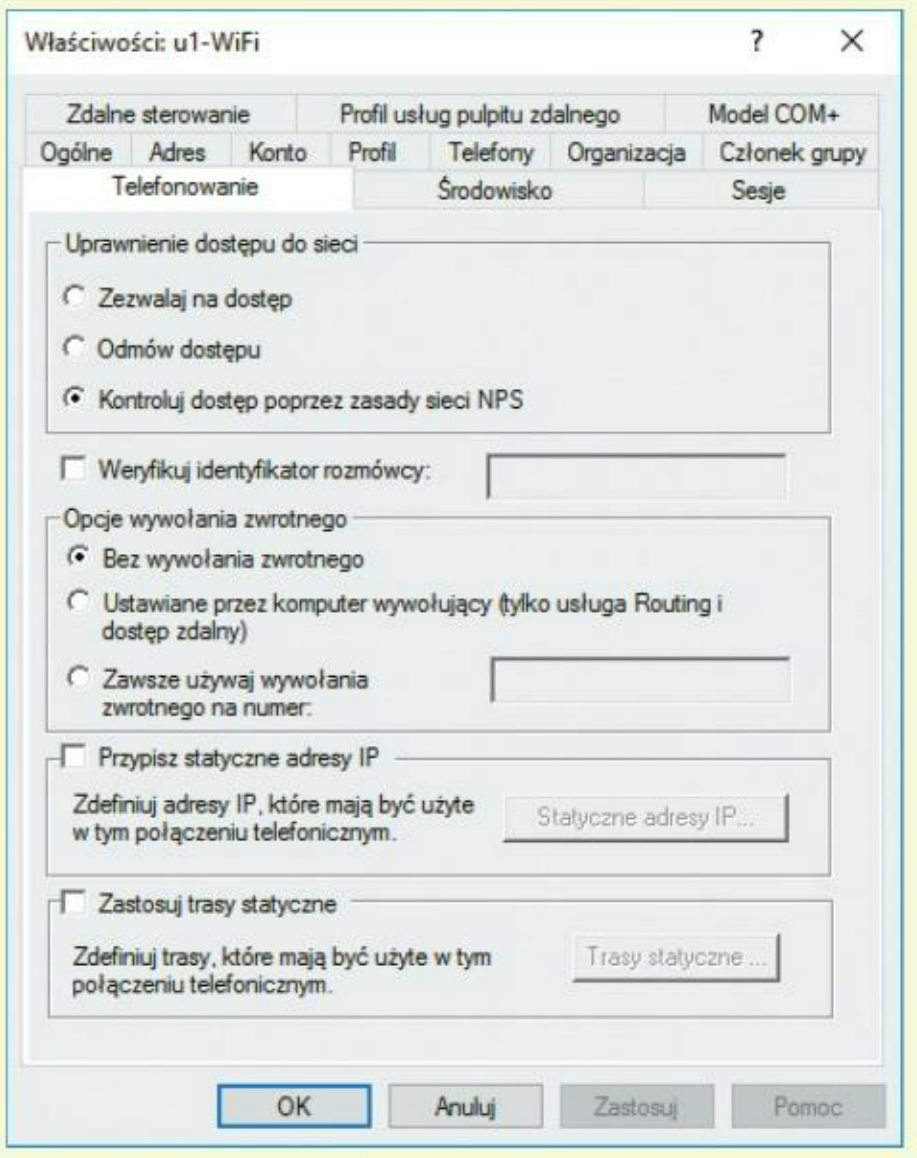
4. Zapisać konfigurację.

PRZYKŁAD 39.2

Utworzenie konta użytkownika uprawnionego do logowania i przypisanie go do grupy

Aby utworzyć konto użytkownika uprawnionego do logowania i przypisać go do grupy, należy:

1. Uruchomić przystawkę **`Użytkownicy i komputery usługi Active Directory`** w konsoli mmc.
2. Utworzyć jednostkę organizacyjną, np. **`ou-WiFi`**.
3. Utworzyć w jednostce organizacyjnej **`ou-WiFi`** globalną grupę użytkowników, np. **`gr-WiFi`**.
4. Utworzyć w jednostce organizacyjnej **`ou-WiFi`** trzech użytkowników, np. *u1-WiFi*, *u2-WiFi*, *u3-WiFi*, ustawić hasło, np. *Qwerty123*, i atrybut **`Hasło nigdy nie wygasa`**.
5. We właściwościach kont użytkowników w zakładce **`Telefonowanie`** ustawić opcję **`Kontroluj dostęp poprzez zasady sieci NPS`** (rys. 39.3).
6. Przypisać użytkowników *u1-WiFi*, *u2-WiFi*, *u3-WiFi* do grupy *gr-WiFi*.



Rys. 39.3. **Ustawienia zakładki `Telefonowanie`**

PRZYKŁAD 39.3

Instalowanie i konfigurowanie Usługi certyfikatów Active Directory

Aby zainstalować Usługi certyfikatów Active Directory, należy:

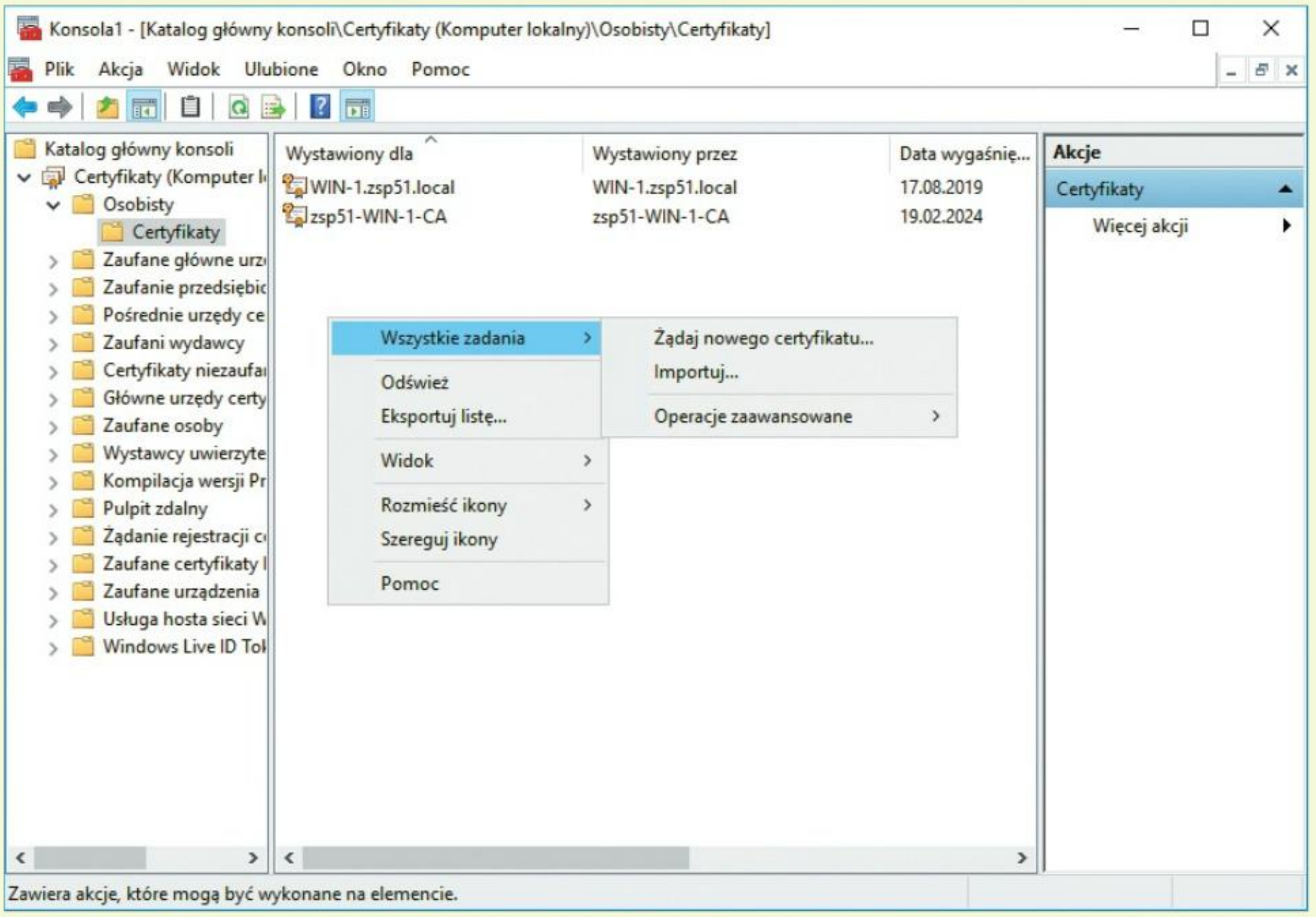
1. W oknie **Menedżer serwera** wybrać **Dodaj role i funkcje**. Po zapoznaniu się z ekranem powitalnym kreatora wybrać opcję **Instalacja oparta na rolach lub oparta na funkcjach**. Kliknąć przycisk **Dalej**.
2. Wybrać serwer, na którym będą instalowane usługi. Kliknąć przycisk **Dalej**.
3. Z listy ról wybrać **Usługi certyfikatów Active Directory**. Kliknąć przycisk **Dalej**. Potwierdzić zainstalowanie dodatkowych ról, niezbędnych do prawidłowego działania usług. Kliknąć przycisk **Dalej**.
4. Zapoznać się z informacjami w oknie **Usługi certyfikatów Active Directory**. Kliknąć przycisk **Dalej**.
5. Wybrać rolę **Urząd certyfikacji**. Kliknąć przycisk **Dalej**.
6. Zapoznać się z informacjami w oknie **Potwierdzenie opcji instalacji**. Kliknąć przycisk **Zainstaluj**.
7. Po zakończeniu instalacji kliknąć przycisk **Zamknij**.
8. W oknie **Menedżer serwera** kliknąć ikonę **Powiadomienia** i z menu wybrać opcję **Konfiguruj usługi certyfikatów Active Directory na serwerze docelowym**.
9. W oknie poświadczenia wskazać konto z uprawnieniami wystarczającymi do dokończenia instalacji, np. konto *Administrator*. Kliknąć przycisk **Dalej**.
10. Wybrać rolę **Urząd certyfikacji** do skonfigurowania. Kliknąć przycisk **Dalej**.
11. Wybrać opcję **Urząd certyfikacji przedsiębiorstwa**. Kliknąć przycisk **Dalej**.
12. Wybrać opcję **Główny urząd certyfikacji**. Kliknąć przycisk **Dalej**.
13. Wybrać opcję **Utwórz nowy klucz prywatny**. Kliknąć przycisk **Dalej**.
14. Wybrać algorytm **SHA1**. Kliknąć przycisk **Dalej**.
15. Zaakceptować nazwę urzędu certyfikacji. Kliknąć przycisk **Dalej**.
16. Podać okres ważności certyfikatu, np. pięć lat. Kliknąć przycisk **Dalej**.
17. Zaakceptować lokalizację baz danych urzędów certyfikacji. Kliknąć przycisk **Dalej**.
18. Zapoznać się z informacjami w oknie **Potwierdzenie**. Kliknąć przycisk **Konfiguruj**.
19. Po zakończeniu konfiguracji kliknąć przycisk **Zamknij**.

PRZYKŁAD 39.4

Generowanie i instalowanie certyfikatów kontrolera domeny

Aby wygenerować i zainstalować certyfikat kontrolera domeny, należy:

1. Uruchomić konsolę mmc i dodać przystawkę **Certyfikaty**. W menu konsoli wybrać **Plik/Dodaj/Usuń przystawkę.../Certyfikaty**. Kliknąć przycisk **Dodaj**. W oknie **Przystawka certyfikatów** wskazać **Konto komputera** i kliknąć **Dalej**. Wskazać **komputer lokalny** i kliknąć **Zakończ**, a następnie **OK**.
2. W lewym panelu rozwinąć gałąź **Certyfikaty/Osobisty/Certyfikaty**. W prawym panelu kliknąć prawym przyciskiem myszy i z menu kontekstowego wybrać **Wszystkie zadania/Żądaj nowego certyfikatu** (rys. 39.4).



Rys. 39.4. **Żądanie nowego certyfikatu**

3. Zapoznać się z informacjami w oknie **`Rejestracja certyfikatów`**. Kliknąć przycisk **`Dalej`**.
4. Wybrać zasady rejestracji usługi Active Directory. Kliknąć przycisk **`Dalej`**.
5. Zażądać certyfikatów dla **`kontrolera domeny`**. Kliknąć przycisk **`Zarejestruj`**.
6. Po zarejestrowaniu i zainstalowaniu certyfikatu na komputerze kliknąć przycisk **`Zakończ`**.

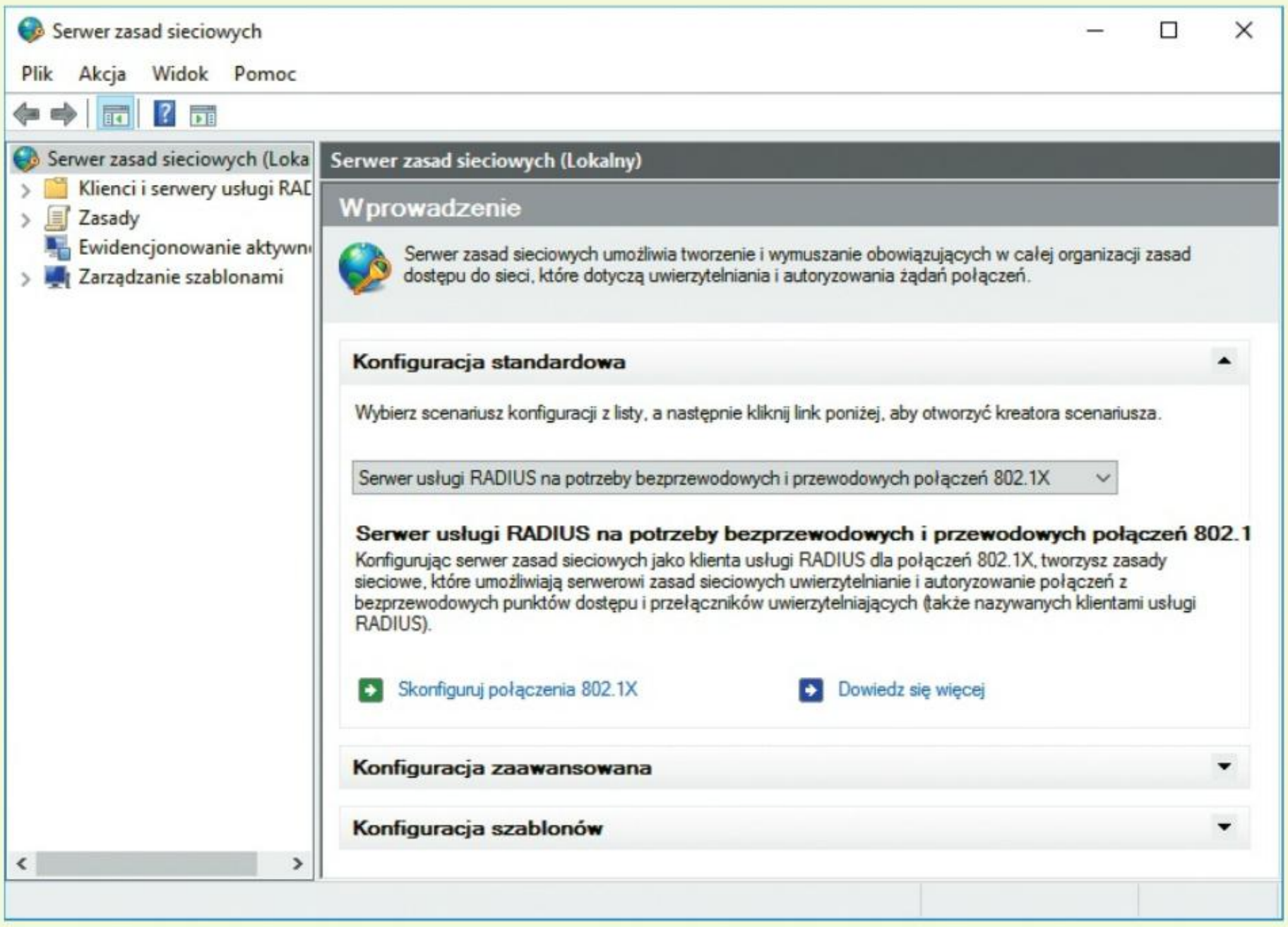
PRZYKŁAD 39.5

Instalowanie i konfigurowanie serwera zasad sieciowych i serwera DHCP

Aby zainstalować i skonfigurować serwer zasad sieciowych i serwer DHCP, należy:

1. W oknie **`Menedżer serwera`** wybrać **`Dodaj role i funkcje`**. Po zapoznaniu się z ekranem powitalnym kreatora wybrać opcję **`Instalacja oparta na rolach lub oparta na funkcjach`**. Kliknąć przycisk **`Dalej`**.
2. Wybrać serwer, na którym będą instalowane usługi. Kliknąć przycisk **`Dalej`**.
3. Z listy ról wybrać **`Usługi zasad sieciowych i dostępu sieciowego`**. Kliknąć przycisk **`Dalej`**. Potwierdzić zainstalowanie dodatkowych funkcji niezbędnych do prawidłowego działania usług. Dodać funkcję serwera DHCP. Kliknąć przycisk **`Dalej`**.
4. Zapoznać się z informacjami w oknie **`Usługi zasad sieciowych i dostępu sieciowego`**. Kliknąć przycisk **`Dalej`**.
5. Zapoznać się z informacjami w oknie **`Potwierdzenie opcji instalacji`**. Kliknąć przycisk **`Zainstaluj`**.

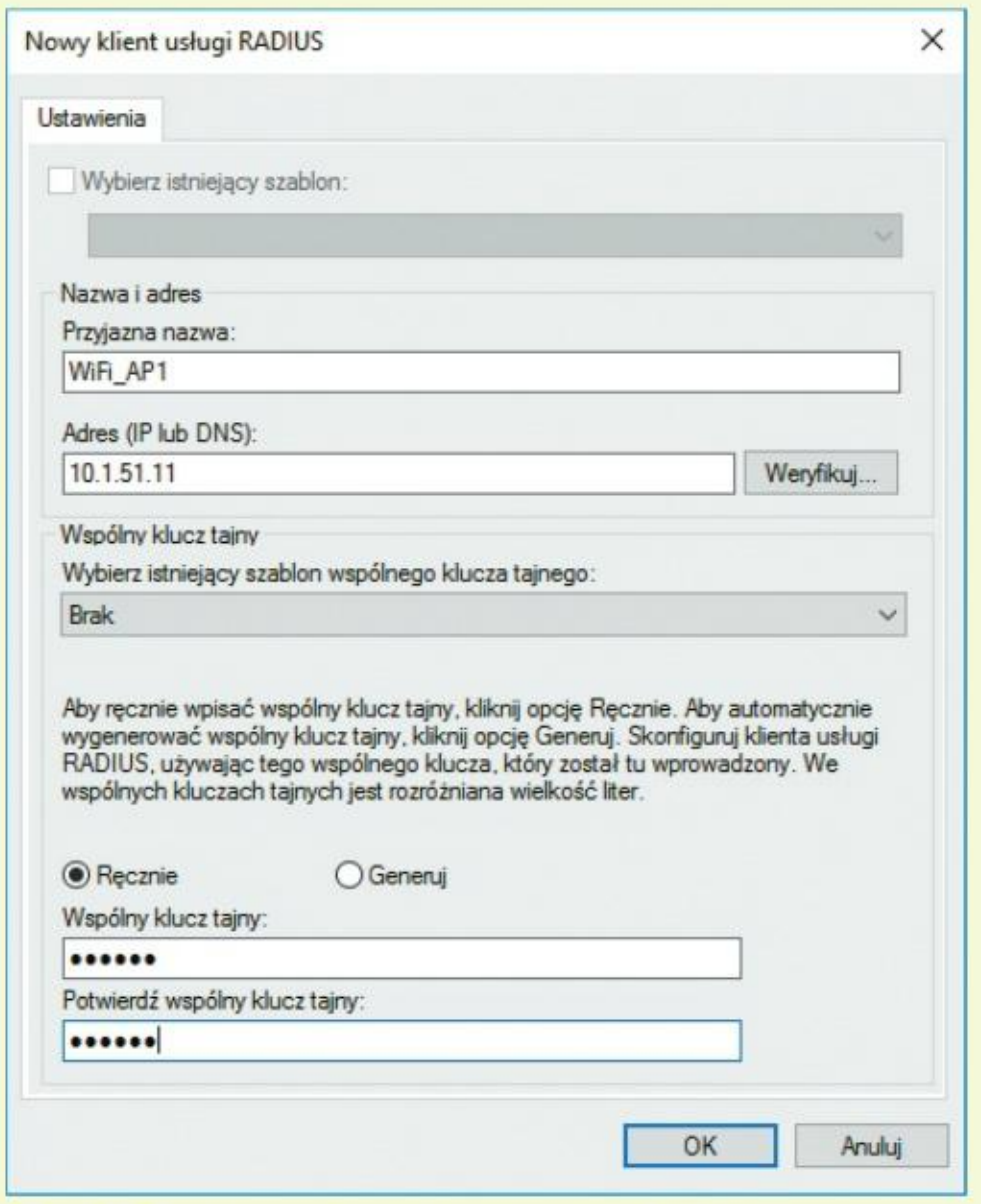
6. Po zakończeniu instalacji kliknąć przycisk **Zamknij**.
7. W oknie **Menedżer serwera** kliknąć ikonę **Powiadomienia** i z menu wybrać opcję **Dokończ konfigurację funkcji DHCP**. Autoryzować serwer DHCP w domenie.
8. Skonfigurować pulę adresów IP przydzielanych przez serwer DHCP dla klientów sieci Wi-Fi. W **Menedżerze serwera** wybrać z menu **Narzędzia/DHCP**. W lewym panelu wybrać nazwę serwera oraz protokół IPv4 i utworzyć nowy zakres, np. nazwa: **WiFi zakres**, początkowy adres: **10.1.51.201**, końcowy adres: **10.1.51.220**, długość maski: **24**. Kliknąć przycisk **Dalej**.
9. Skonfigurować opcje zakresu DHCP, np. brama **10.1.51.1**, w pozostałych opcjach pozostawić wartości domyślne. Aktywować zakres.
10. Wykonać restart serwera DHCP. W oknie DHCP kliknąć prawym przyciskiem myszy **nazwę serwera/Wszystkie zadania/Uruchom ponownie**.
11. Uruchomić konsolę zarządzania serwerem zasad sieciowych. W oknie **Menedżer serwera** z menu wybrać opcję **Narzędzia/Serwer zasad sieciowych**.
12. Wybrać scenariusz **Serwer usługi RADIUS na potrzeby bezprzewodowych i przewodowych połączeń 802.1X**. Kliknąć odnośnik **Skonfiguruj połączenia 802.1X** (rys. 39.5).



Rys. 39.5. **Wybór scenariusza tworzenia zasad dostępu**

13. Wybrać typ połączenia: **Bezpieczne połączenie bezprzewodowe**. Kliknąć przycisk **Dalej**.
14. Wprowadzić informacje o kliencie (klientem jest punkt dostępowy), np. nazwę *WiFi_AP1*, adres IP **10.1.51.11** i hasło *Qwerty* (rys. 39.6). Kliknąć przycisk **OK**. Kliknąć przycisk **Dalej**.

15. Wybrać typ protokołu EAP, np. **Microsoft Chroniony protokół EAP (PEAP)**. Kliknąć przycisk **Dalej**.
16. Określić grupę użytkowników, np. *gr-WiFi*. Kliknąć przycisk **Dalej**.
17. Zatwierdzić dane w oknie **Konfigurowanie elementów kontroli ruchu w sieci**. Kliknąć przycisk **Dalej**.
18. Zakończyć działanie kreatora. Kliknąć przycisk **Zakończ**.
19. Zarejestrować serwer w usłudze Active Directory. W oknie **Serwer zasad sieciowych** kliknąć prawym przyciskiem myszy nazwę serwera i z menu kontekstowego wybrać polecenie **Zarejestruj serwer w usłudze Active Directory**.



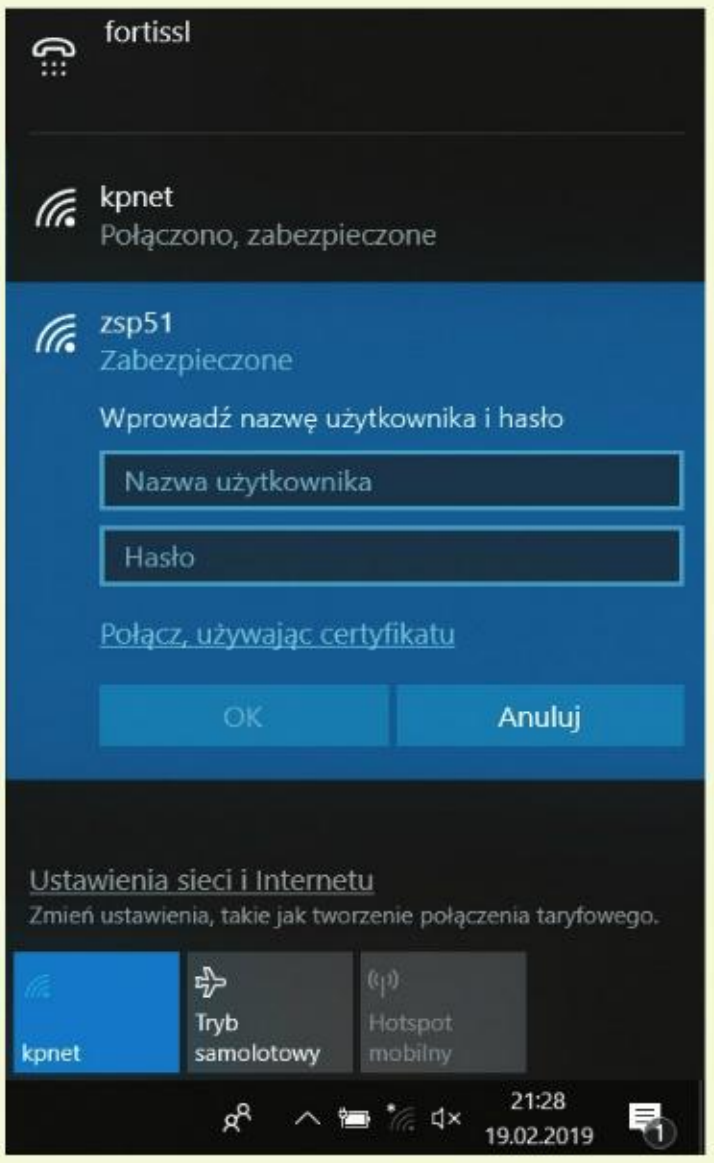
Rys. 39.6. **Informacje o kliencie usługi RADIUS**

PRZYKŁAD 39.6

Konfigurowanie serwera zasad sieciowych i roli serwera dostępu

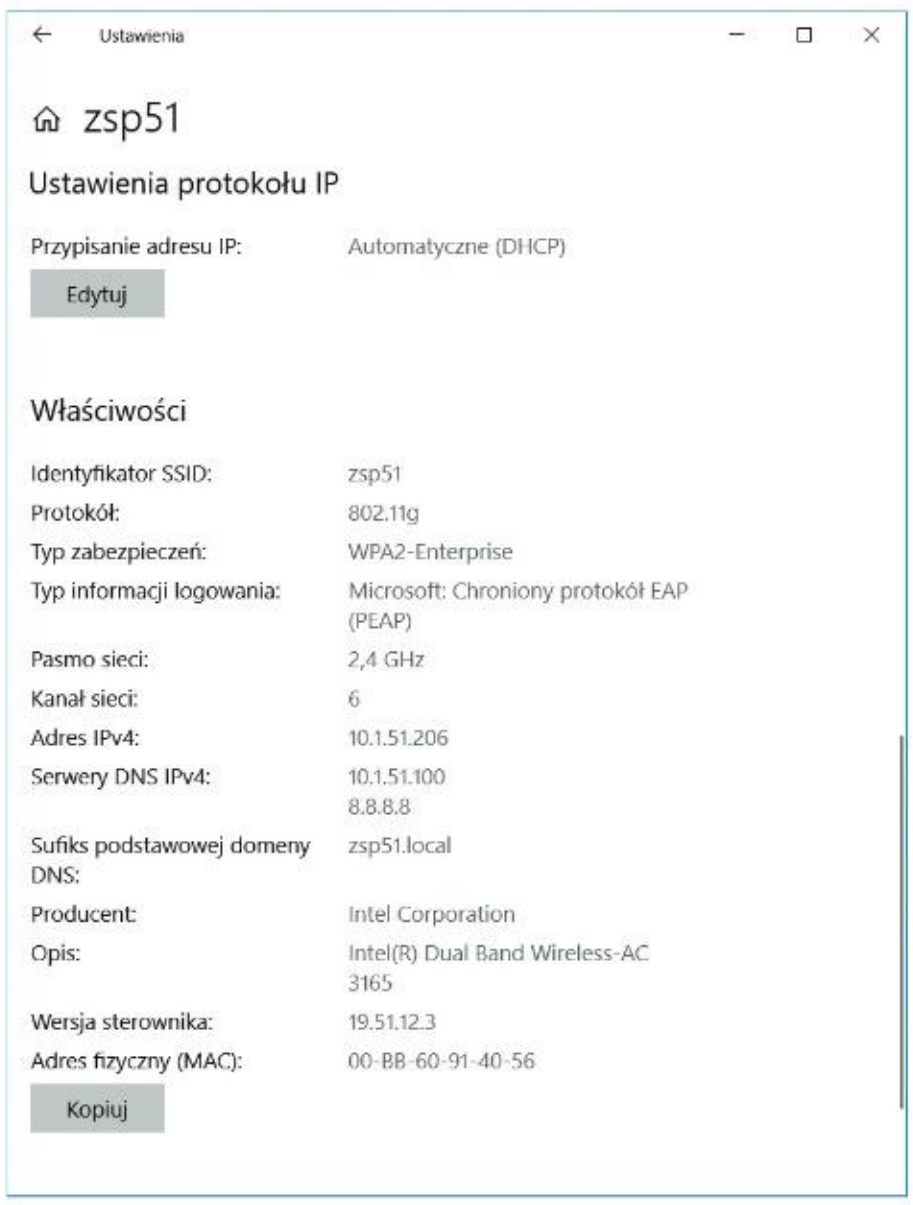
Aby skonfigurować serwer zasad sieciowych i rolę serwera dostępu, należy:

1. Wyeksportować certyfikat serwera. Uruchomić konsolę mmc i dodać przystawkę **Certyfikaty**. W menu konsoli wybrać **Plik/Dodaj/Usuń przystawkę.../Certyfikaty**. Kliknąć przycisk **Dodaj**. W oknie **Przystawka certyfikatów** wskazać **Konto komputera** i kliknąć **Dalej**. Wskazać **komputer lokalny** i kliknąć **Zakończ**, a następnie **OK**.
2. W lewym panelu rozwinąć gałąź **Certyfikaty/Osobisty/Certyfikaty**. W prawym panelu kliknąć prawym przyciskiem myszy certyfikat i z menu kontekstowego wybrać **Wszystkie zadania/Eksportuj**.
3. Zapoznać się z informacjami w oknie **Kreator eksportu certyfikatów**. Kliknąć przycisk **Dalej**.
4. Wybrać opcję **Nie eksportuj klucza prywatnego**. Kliknąć przycisk **Dalej**.
5. Wybrać format certyfikatu: **Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER)**. Kliknąć przycisk **Dalej**.
6. Wprowadzić nazwę pliku, do którego zostanie wyeksportowany certyfikat, np. **wifi_cert.cer**. Kliknąć przycisk **Dalej**, a następnie **Zakończ**.
7. Skopiować certyfikat do komputera przyłączanego do sieci Wi-Fi.
8. W komputerze przyłączanym do sieci uruchomić konsolę mmc i dodać przystawkę **Certyfikaty**. W menu konsoli wybrać **Plik/Dodaj/Usuń przystawkę.../Certyfikaty**. Kliknąć przycisk **Dodaj**. W oknie **Przystawka certyfikatów** wskazać **Konto komputera** i kliknąć **Dalej**. Wskazać **komputer lokalny** i kliknąć **Zakończ**, a następnie **OK**.



Rys. 39.7. Nawiązywanie połączenia z zabezpieczoną siecią Wi-Fi

9. W lewym panelu rozwinąć gałąź **Certyfikaty/Zaufane główne urzędy certyfikacji**. Kliknąć prawym przyciskiem myszy **Certyfikaty** i z menu kontekstowego wybrać **Wszystkie zadania/Importuj**.
10. Zapoznać się z informacjami w oknie **Kreator importu certyfikatów**. Kliknąć przycisk **Dalej**.
11. Wprowadzić nazwę pliku, z którego jest importowany certyfikat, np. **wifi_cert.cer**. Kliknąć przycisk **Dalej**.
12. Zatwierdzić magazyn certyfikatów. Kliknąć przycisk **Dalej**, a następnie **Zakończ**.
13. Kliknąć ikonę połączeń sieciowych w prawym dolnym rogu ekranu (rys. 39.7). Wybrać sieć Wi-Fi i kliknąć przycisk **Połącz**. Wprowadzić poświadczenia użytkownika, np. konto *u1-WiFi* i hasło *Qwerty123*.
14. Sprawdzić możliwość komunikacji.



W ustawieniach połączenia Wi-Fi (rys. 39.8) można odczytać informacje o konfiguracji połączenia.

Rys. 39.8. Informacje o ustawieniach połączenia z siecią Wi-Fi

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wymień i scharakteryzuj inne metody zwiększające bezpieczeństwo sieci bezprzewodowych.
2. Wyjaśnij, do czego służy i jak działa algorytm **AES**. Jakie znasz inne algorytmy tego typu?

40 Zabezpieczenie kontrolera domeny przed atakami

ZAGADNIENIA

- **Przyczyny stosowania zabezpieczenia**
- **Zasady zabezpieczenia kontrolera domeny**
- **Rodzaje zabezpieczeń kontrolera domeny**

Kontroler domeny może świadczyć usługi dla użytkowników sieci lokalnej, a w wielu przypadkach również dla użytkowników internetu. Jest przez to szczególnie narażony na ataki użytkowników, zarówno z sieci lokalnej, jak i z internetu. Zapewnienie bezpieczeństwa dla kontrolera to trudne zadanie wymagające podejmowania działań na różnych poziomach, ale niezbędne do jego prawidłowego funkcjonowania. Administrator powinien zapewnić z jednej strony możliwość komunikowania się z serwerem legalnym użytkownikom, a z drugiej ograniczyć możliwość kontaktu z osobami nieuprawnionymi.

Zabezpieczenia najlepiej funkcjonują w strukturze warstwowej. W takim wypadku, nawet jeżeli atakujący przełamie jedną warstwę zabezpieczeń, pozostałe warstwy mogą działać skutecznie. Zabezpieczenia mogą obejmować różne aspekty bezpieczeństwa, np.:

- zabezpieczenie fizyczne;
- ograniczenia logowania;
- ograniczanie dostępu do plików i folderów;
- stosowanie szyfrowania plików i folderów;
- stosowanie zapór sieciowych;
- ochrona przed wirusami i innymi typami szkodliwego oprogramowania;
- stosowanie aktualizacji systemu;
- tworzenie kopii zapasowych.

Zabezpieczenie fizyczne dla kontrolerów domeny jest niezbędnym elementem systemu bezpieczeństwa. Jeżeli agresor będzie miał fizyczny dostęp do serwera, może go wyłączyć, zniszczyć, ukraść np. dyski lub inne nośniki pamięci. Może uruchomić serwer, korzystając z bootowalnych dysków lub pamięci, i w ten sposób ominąć zabezpieczenia. Dostęp fizyczny do kontrolera (jak również innych urządzeń sieciowych) powinien być ograniczony tylko do uprawnionych osób.

Najczęściej serwer umieszcza się w specjalnym pomieszczeniu – **serwerowni** z ograniczonym dostępem i dodatkowymi systemami bezpieczeństwa, np. przeciwpożarowym, klimatyzacją, systemami podtrzymania napięcia. Kolejną warstwą zabezpieczeń mogą być mechanizmy zamykania obudów serwerów, stosowane przez niektórych producentów. Jeżeli kontrolery domeny nie mogą być przechowywane w zamykanych pomieszczeniach w lokacjach, należy wdrożyć je jako kontrolery tylko do odczytu RODC. Jeżeli kontrolery domeny są instalowane jako maszyny wirtualne, to każdy z nich powinien być uruchomiony na oddzielnym hoście.

Ograniczenia logowania w domyślnej konfiguracji pozwalają na logowanie do kontrolera domeny tylko administratorowi. Pozostali użytkownicy muszą uzyskać stosowne uprawnienia od administratora. Powinna obowiązywać **zasada minimalnych uprawnień** – użytkownik ma wówczas tylko uprawnienia niezbędne do wykonywania powierzonych mu zadań. Przyznanie

nadmiarowych uprawnień jest błędem. Ograniczenia logowania można wprowadzić przez przypisanie użytkowników do grup, zasady grup i konfigurację kont, np. ograniczenie czasu logowania, lub komputera wykorzystywanego do logowania. Do uwierzytelniania użytkownika najczęściej są wykorzystywane konto i hasło. Należy zadbać o bezpieczeństwo haseł i rozważyć wprowadzenie dodatkowych form zabezpieczeń, np. logowanie za pomocą kart inteligentnych lub metod biometrycznych.

Podstawową metodą **ograniczania dostępu do plików i folderów** jest system kont i uprawnień NTFS. Należy przeanalizować posiadane przez użytkowników uprawnienia w celu wykrycia potencjalnych zagrożeń. Szczególną uwagę warto zwrócić na dziedziczenie uprawnień i blokowanie dziedziczenia. Innym mechanizmem jest stosowanie inspekcji dostępu do plików, dzięki czemu administrator może być informowany o próbach dostępu do ważnych folderów i plików.

Woluminy dysków kontrolerów domeny mogą być chronione za pomocą **szyfrowania dysków i folderów**, np. funkcją **BitLocker**. BitLocker jest wbudowana w systemach operacyjnych. Szyfruje ona za pomocą algorytmu AES (128 bitów lub 256 bitów) każdy sektor partycji. Szyfrowanie i odszyfrowanie odbywają się niezauważalnie dla systemu i użytkownika.

Stosowanie **zapór sieciowych** jest niezbędne w każdej sieci połączonej z internetem. Windows Server dysponuje domyślnie włączoną zaporą sieciową, która może być zintegrowana z usługą Active Directory i innymi usługami świadczonymi przez serwer. Zapewnia ona kontrolę danych przepływających przez serwer, co znacznie podnosi poziom bezpieczeństwa.

Na serwerze są przechowywane ważne zbiory systemowe i zbiory poszczególnych użytkowników. Ochronę przed wirusami i innymi typami szkodliwego oprogramowania powinno zapewnić na bieżąco aktualizowane **oprogramowanie antywirusowe**. Serwerowe wersje oprogramowania często mają możliwość skanowania i usuwania wirusów nie tylko z serwera, lecz również ze stacji roboczych, przyłączonych do domeny.

Zaleca się, aby systemy operacyjne serwerów i stacji roboczych były **regularnie aktualizowane**. Pozwoli to na utrzymywanie systemów w dobrej kondycji oraz uniknięcie luk i błędów wykrywanych w systemach operacyjnych. Jeżeli w sieci działa wiele serwerów, zaleca się aktualizowanie systemów operacyjnych do najnowszych wersji obsługiwanej w danej organizacji, np. Windows Server 2016. Dzięki temu będą dostępne nowe funkcje i zabezpieczenia niedostępne we wcześniejszych wersjach systemów.

Kopie zapasowe pozwalają zabezpieczyć pliki, np. dokumenty, zdjęcia, pliki wideo przed przypadkową utratą. Kopie zapasowe powinny być przechowywane w bezpiecznym miejscu, poza pomieszczeniem, w którym znajdują się dane oryginalne. Kopie zapasowe należy wykonywać regularnie, zgodnie z przyjętym schematem tworzenia kopii, i regularnie przeprowadzać próby odtworzenia danych z kopii. Kopie powinny być zabezpieczone (z zachowaniem takiego samego poziomu bezpieczeństwa) jak dane oryginalne.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Sporządź listę czynności, które należy wykonać, aby zabezpieczyć swój serwer.
2. Wyszukaj w internecie oprogramowanie, które pozwoli zwiększyć poziom bezpieczeństwa twojego serwera. Sporządź listę tego oprogramowania i kosztorys jego zakupu.

- Cyberbezpieczeństwo
- Kopie bezpieczeństwa
- Zasady grup
- Monitorowanie pracy serwera
- Monitorowanie wydajności serwera
- Narzędzia do diagnostyki serwera
- Metody ataków sieciowych
- Metody zabezpieczania zasobów sieciowych
- Rodzaje i dobór UPS
- Archiwizacja zasobów sieciowych
- Konfiguracja firewalla w Windows Server

Bezpieczeństwo danych

V

41 Cyberbezpieczeństwo

ZAGADNIENIA

Poprawianie poziomu bezpieczeństwa przez użytkownika sieci i organizację
Konsekwencje naruszenia bezpieczeństwa **Podmioty odpowiedzialne w Polsce za cyberbezpieczeństwo**

We współczesnym świecie sieć informacyjna stała się integralną częścią naszego codziennego życia. Wszystkie instytucje publiczne, np. edukacyjne, medyczne, rządowe i komercyjne, wykorzystują sieci informacyjne do efektywnego działania. Gromadzą i przetwarzają duże ilości informacji dotyczących wszystkich aspektów naszego życia. Ochrona tych informacji jest bardzo ważna zarówno dla naszego bezpieczeństwa, jak i bezpieczeństwa instytucji i organizacji oraz zapewnienia stabilności gospodarczej i politycznej. **Bezpieczeństwo cybernetyczne** można rozumieć jako ochronę systemów informatycznych i przetwarzanych w nich danych przed nieuprawnionym użyciem, uszkodzeniem lub zniszczeniem.

Bezpieczeństwo danych powinno być zapewnione na wszystkich możliwych poziomach:

- na poziomie osobistym należy chronić swoją tożsamość, dane i urządzenia komputerowe;
- obowiązkiem każdej instytucji i organizacji jest ochrona gromadzonych i przetwarzanych danych oraz infrastruktury wykorzystywanej do ich przetwarzania;
- na szczeblu państwowym celem jest zapewnienie bezpieczeństwa narodowego oraz bezpieczeństwa instytucji i obywateli.

O bezpieczeństwo tożsamości i danych prywatnych musimy zadbać samodzielnie. **Tożsamość** w sieci jest wykorzystywana do komunikowania się z użytkownikiem. Określa sposób, w jaki osoba prezentuje się innym. Powinna ujawniać tylko ograniczoną ilość informacji, którą można udostępnić innym. Utrata tożsamości, np. przejęcie konta w portalu społecznościowym, może sprawić, że ktoś będzie komunikował się lub wykonywał inne działania w imieniu osoby niekoniecznie zgodnie z jej oczekiwaniami. Kradzież tożsamości umożliwia złodziejowi dostęp do kontaktów użytkownika, np. można uzyskać adresy e-mail lub numery telefonów znajomych, wykorzystać reputację użytkownika zdobytą w portalach społecznościowych bądź uzyskać dostęp do danych firmowych lub rządowych.

Dane osobowe mogą jednoznacznie identyfikować osobę fizyczną. Obejmują wszystkie informacje, takie jak imię i nazwisko, data i miejsce urodzenia, adres zamieszkania, dane biometryczne, które mogą być wykorzystane do identyfikacji użytkownika. Udostępnianie danych osobowych należy ograniczyć do przypadków niezbędnych i rozważyć, czy mają one być udostępniane publicznie. Szczególną uwagę trzeba zwrócić na tzw. **dane wrażliwe**, takie jak pochodzenie rasowe lub etniczne, dotyczące poglądów politycznych, przekonań religijnych i światopoglądowych, przynależności do związków zawodowych, danych genetycznych, danych biometrycznych, zdrowia, seksualności lub orientacji seksualnej. Przetwarzanie tego typu danych jest z zasady zabronione i dopuszczalne tylko przez uprawnione do tego instytucje w określonych warunkach i z zachowaniem szczególnych środków ostrożności.

Przed udostępnieniem jakichkolwiek danych osobowych należy rozważyć celowość takiego działania, aby w przyszłości nie narażać się na przykre konsekwencje niekontrolowanego upublicznienia danych. Dane osobowe mogą być wykorzystane do uzyskiwania dostępu do usług lub zaciągania zobowiązań, np. finansowych, w imieniu użytkownika. Zasady przetwarzania danych osobowych objęto **rozporządzeniem o ochronie danych osobowych** – **RODO** (ang. *General Data Protection Regulation*, GDPR).

Urządzenia komputerowe są wykorzystywane do gromadzenia i przetwarzania danych. Stanowią cenny zasób nie tylko z powodu ceny, jaką należy za nie zapłacić. Niejednokrotnie ważniejsza jest możliwość komunikacji i dostępu do danych. Brak możliwości dostępu do usług i portali społecznościowych przez wiele osób jest odbierany jako dyskomfort. Przejęcie kontroli nad urządzeniami komputerowymi pozwala hakerom uzyskać dostęp do zgromadzonych w nich danych, wykorzystywać ich moc obliczeniową do wykonywania obliczeń (np. łamania haseł), uzyskiwania dostępu do zasobów (np. wykonywanie ataków z wykorzystaniem urządzeń innych użytkowników) lub przeprowadzania ataków na innych użytkowników.

Organizacje publiczne i komercyjne gromadzą i przetwarzają różnego typu dane, np. dokumentację pracowników i klientów (historię pracy, płacy, kontakty itp.), własności intelektualne (patenty, znaki towarowe, utwory), dane finansowe (faktury VAT, bilanse, plany finansowe, wyciągi z kont bankowych itp.). Przetwarzając dane, powinny one zapewnić:

- **poufność** – zapewnia, że dostęp do danych będą miały tylko osoby upoważnione. Poufność zapewnia się przez szyfrowanie danych, system kont i haseł użytkowników, system podwójnej autoryzacji i minimalizację ekspozycji poufnych informacji. Wszyscy pracownicy powinni zostać przeszkoleni w zakresie ochrony poufnych informacji i polityki bezpieczeństwa w organizacji;
- **integralność danych** – zapewnia, że informacje są dokładne, spójne i wiarygodne. Integralność danych podczas przesyłania w sieci zapewnia się przez sumy kontrolne, np. funkcje **MD5** lub **SHA-1**. Uprawnienia do plików i folderów oraz kontrola dostępu użytkowników zapobiegają nieuprawnionemu dostępowi. Modyfikacje danych mogą wykonywać tylko uprawnione osoby z zachowaniem prawa rozliczalności (za zachowaniem historii i informacji, kto dokonał zmiany). Dane powinny być chronione przed uszkodzeniem lub utratą dzięki regularnemu tworzeniu kopii zapasowych;
- **dostępność** – oznacza, że uprawnieni użytkownicy mogą korzystać z danych. Wpływ na dostępność danych mają konserwacje i naprawy sprzętu, aktualizacje systemów operacyjnych i oprogramowania oraz procesy tworzenia i odtwarzania kopii zapasowych. W organizacji powinny istnieć plany awaryjne zapewnienia ciągłości pracy i szybkiego przywrócenia sprawności systemów po awariach, klęskach żywiołowych lub katastrofach spowodowanych przez człowieka. Sprzęt lub oprogramowanie zabezpieczające, takie jak zapory sieciowe, chronią sieć i dane przed utratą dostępności spowodowaną atakami, np. odmowy dostępu do usługi (DoS).

Zabezpieczenie organizacji przed wszystkimi możliwymi atakami jest praktycznie niemożliwe, a na pewno bardzo kosztowne. Ponadto cały czas notuje się nowe metody ataków. Pod tym względem atakujący zawsze wyprzedzają swoje ofiary. Dla administratora ważne są ciągłe podnoszenie poziomu bezpieczeństwa systemu i bieżące śledzenie informacji o nowych zagrożeniach i metodach zapobiegania im. Administrator powinien na bieżąco aktualizować swoje wiadomości i doskonalić umiejętności ze stosowania zabezpieczeń. Konieczne jest również instalowanie aktualizacji, łat i poprawek do systemów operacyjnych i aplikacji.

Konsekwencje naruszenia bezpieczeństwa znacznie wykraczają poza straty spowodowane w sprzęcie i oprogramowaniu komputerowym. Znacznie więcej szkód może przynieść utrata zaufania klientów i użytkowników lub wizerunku, często budowanego latami, spowodowana

ujawnieniem poufnych informacji, własności intelektualnej lub brakiem możliwości świadczenia usług. Straty finansowe spowodowane naruszeniem bezpieczeństwa mogą obejmować również koszty niezbędnych inwestycji w nowe systemy zabezpieczeń, szkolenie personelu i wdrożenie odpowiednich procedur bezpieczeństwa. Organizacja może być również zmuszona do poinformowania wszystkich osób, których dotyczy naruszenie, i wypłatę odszkodowań.

Pomimo wysokich kosztów stosowania różnego typu zabezpieczeń ich koszt na ogół jest niższy niż straty spowodowane brakiem lub niedostatecznym poziomem zabezpieczeń albo nieprzestrzeganiem procedur bezpieczeństwa. Duży wpływ na wysokość strat mają szybkość i sposób reakcji na atak oraz szybkość i skuteczność procedur przywracania funkcjonalności w organizacji.

Zagrożenia dla bezpieczeństwa systemów można podzielić na:

- **wewnętrzne** – powodują je pracownicy lub partnerzy mający legalny dostęp do systemu informacyjnego. Mogą powodować zagrożenia umyślne i nieumyślne: kasowanie plików i folderów, wprowadzanie nieprawidłowych danych, zagrożenie dla pracy wewnętrznych serwerów lub urządzeń infrastruktury sieciowej, ułatwienia ataków z zewnątrz (np. po podłączeniu zainfekowanych nośników USB do systemu komputerowego), uruchamianie złośliwego oprogramowania z wiadomości e-mail lub strony internetowej. Użytkownicy wewnętrzni mają dostęp do systemu i jego urządzeń oraz dysponują wiedzą na temat sieci, jej zasobów i zabezpieczeń, co zwiększa ryzyko ataku;
- **zewnętrzne** – powodują je użytkownicy spoza organizacji. Mogą oni dysponować dużą wiedzą na temat systemów informacyjnych i luk w systemach zabezpieczeń oraz stosować wyrafinowane techniki, np. z dziedziny inżynierii społecznej.

Napastników można podzielić na grupy o różnym stopniu zaawansowania:

- **amatorzy** (ang. *Script Kiddies*) – zazwyczaj z małymi umiejętnościami, często wykorzystujący istniejące narzędzia lub instrukcje znalezione w internecie do przeprowadzania ataków. Mogą testować lub demonstrować swoje (i administratorów) umiejętności, używając podstawowych narzędzi. Jeżeli system nie jest odpowiednio zabezpieczony, są w stanie wyrządzić duże szkody;
- **hakerzy** – włamują się do komputerów lub sieci. „Białe kapelusze" włamują się do sieci lub systemów komputerowych, aby odkryć luki w zabezpieczeniach i poprawić bezpieczeństwo. Wyniki włamań są zgłaszane właścicielowi. „Czarne kapelusze" wykonują ataki, aby osiągnąć korzyści, np. osobiste lub finansowe. „Szare kapelusze", jeżeli leży to w ich interesie, to mogą zgłaszać podatność systemu właścicielowi lub wykorzystać ją we własnym celu;
- **hakerzy zorganizowani** – zorganizowane grupy przestępców internetowych, stosujących zaawansowane techniki w celu osiągnięcia korzyści finansowych, politycznych lub innych.

Bezpieczeństwo cybernetyczne jest przedmiotem troski każdego państwa. Nie jest tajemnicą, że każda armia ma jednostki wyspecjalizowane w prowadzeniu wojny elektronicznej. Wykorzystuje się w niej wszelkie środki umożliwiające ataki na systemy przeciwnika (nie tylko ściśle militarne, lecz także infrastrukturę, np. systemy łączności, komunikacji lub energetyczne), zdobywanie informacji i zapewniające bezpieczeństwo własnych systemów. Bardzo ważnymi elementami są również działania informacyjne i kształtowanie opinii publicznej, np. za pomocą mediów społecznościowych.

Podstawowym dokumentem opisującym problemy cyberbezpieczeństwa w Polsce jest *Doktryna cyberbezpieczeństwa RP* opracowana przez Biuro Bezpieczeństwa Narodowego. Dokument jest dostępny pod adresem **`https://www.bbn.gov.pl/pl/wydarzenia/6336,Doktryna-cyberbezpieczenstwa-RP.html`**.

Przykładami instytucji zajmujących się problemami cyberbezpieczeństwa w Polsce są Ministerstwo Cyfryzacji (**`https://www.gov.pl/web/cyfryzacja/departament-cyberbezpieczenstwa`**) i NASK – Naukowa i Akademicka Sieć Komputerowa (**`https://www.nask.pl/pl/dzialalnosc/cyberbezpieczenstwo/3284,Cyberbezpieczenstwo.html`**).

SPRAWDŹ SWOJĄ WIEDZĘ

1. Odszukaj w internecie dokument *Doktryna cyberbezpieczeństwa RP*. Jak w tym dokumencie zdefiniowano pojęcie „cyberbezpieczeństwo RP”?
2. Skorzystaj z dokumentu *Doktryna cyberbezpieczeństwa RP* i wymień zagrożenia w wymiarach wewnętrznym i zewnętrznym.

42 Kopie bezpieczeństwa

ZAGADNIENIA

Cel tworzenia kopii bezpieczeństwa **Zainstalowanie narzędzi do tworzenia kopii zapasowych** **Tworzenie i odzyskiwanie danych z jednorazowej kopii zapasowej**

Jednym z obowiązków administratora sieci jest zapewnienie bezpieczeństwa danych. Za bezpieczeństwo danych odpowiadają mechanizmy:

- zabezpieczenia danych przed niepowołanym dostępem (np. system kont);
- zabezpieczenia danych przed nieumyślnym usunięciem (np. system uprawnień, kopie zapasowe);
- zabezpieczenia danych przed awarią sprzętu (np. systemy UPS, pamięci redundantne).

Kopia zapasowa (ang. *backup copy*) to kopia danych, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia. Niektóre edytory i inne programy wykonują taką kopię automatycznie w określonych odstępach, aby umożliwić odtworzenie zawartości pliku w razie awarii komputera lub samego programu. Większość programów takich kopii jednak nie robi. Jednym z najważniejszych zadań administratora jest tworzenie kopii zapasowych. Administrator musi opracować plan tworzenia kopii zapasowych i ewentualnego przywracania danych uwzględniającego:

- rodzaj danych przeznaczonych do archiwizacji;
- częstotliwość wykonywania kopii;
- szybkość ewentualnego odtwarzania danych (zależy od rodzaju nośnika i rodzaju kopii);
- rodzaj nośnika przeznaczonego do przechowywania kopii;
- harmonogram wykonywania kopii zapasowych;
- miejsce przechowywania kopii.

W Windows Server 2016 można tworzyć następujące typy kopii zapasowych:

- **normalna kopia zapasowa** – wykonywana dla wszystkich zaznaczonych plików. Po wykonaniu kopii atrybut **`Archive`** jest czyszczony. Jest czasochłonna podczas tworzenia;
- **przyrostowa kopia zapasowa** – zawiera tylko te pliki, które były modyfikowane lub utworzone od momentu ostatniej kopii normalnej lub przyrostowej. Po wykonaniu kopii atrybut **`Archive`** jest czyszczony. To najszybszy i zajmujący najmniej miejsca rodzaj kopii. Przywracanie danych zaczyna się od normalnej kopii zapasowej, a następnie w kolejności tworzenia przywraca się każdą kolejną kopię przyrostową;
- **różnicowa kopia zapasowa** – zawiera tylko te pliki, które zmieniono lub utworzono od ostatniej normalnej kopii zapasowej. Po wykonaniu kopii atrybut **`Archive`** nie jest czyszczony. To mniejsza niż normalna kopia zapasowa, a większa niż przyrostowa. Do odtworzenia danych są potrzebne normalna kopia zapasowa i ostatnia kopia różnicowa;
- **codzienna kopia zapasowa** – kopia wszystkich danych zmienionych w określonym dniu. Lista plików umieszczonych w kopii powstaje na podstawie daty modyfikacji. Atrybut **`Archive`** nie jest używany ani zerowany.

W systemie Windows Server 2016 do tworzenia kopii można wykorzystać narzędzie **Kopia zapasowa systemu Windows Server**. Nie jest ono instalowane standardowo; można je zainstalować, gdy będzie potrzebne.

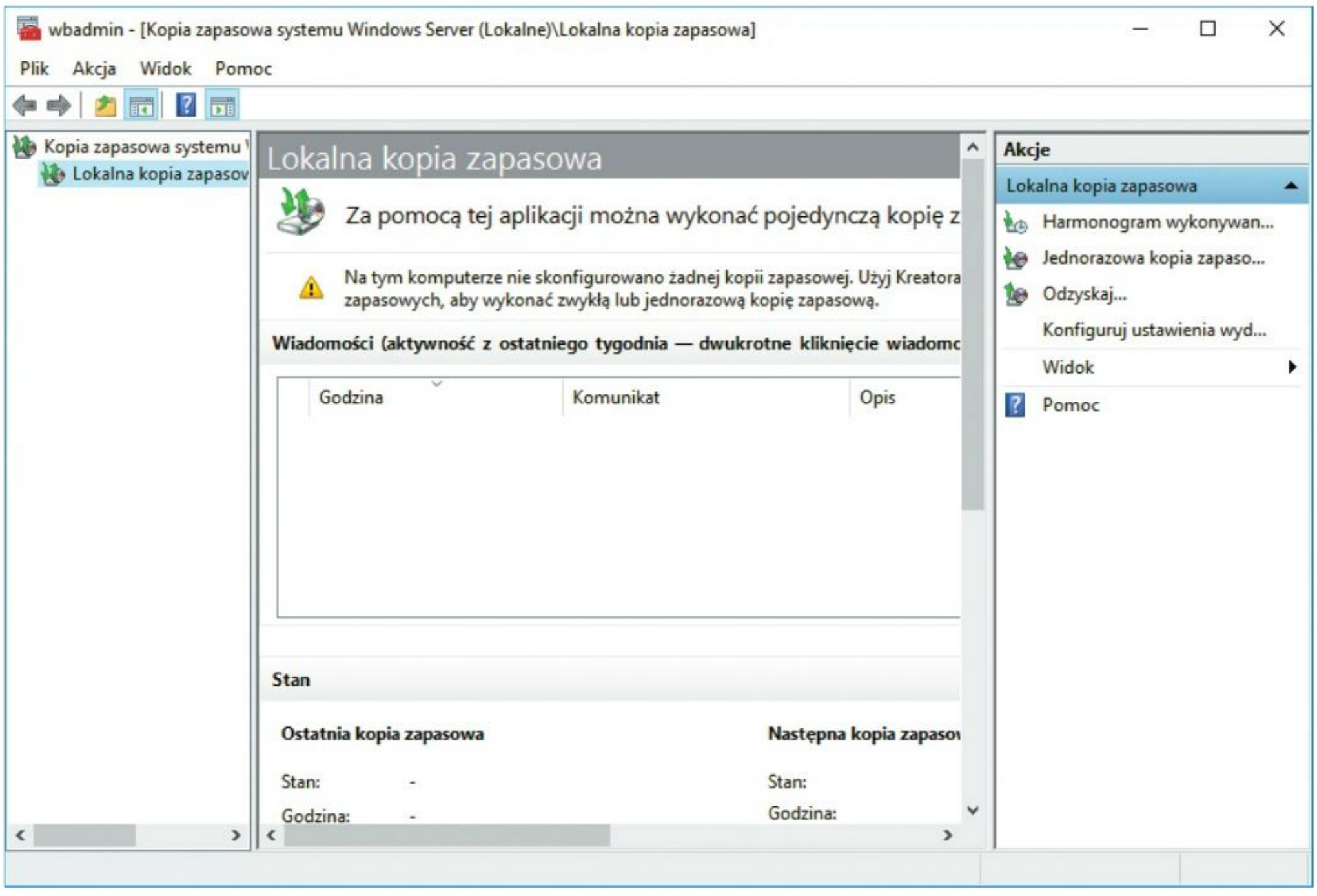
PRZYKŁAD 42.1

Instalowanie narzędzia do tworzenia kopii zapasowych

Aby zainstalować funkcję **Kopia zapasowa systemu Windows Server**, należy:

1. Uruchomić **Menedżer serwera**.
2. W oknie **Menedżer serwera** kliknąć odnośnik **Dodaj role i funkcje**, wskazać opcję **Instalacja oparta na rolach lub oparta na funkcjach** i serwer do zainstalowania usługi. Kliknąć przycisk **Dalej**.
3. W oknie **Wybieranie ról serwera** nie wprowadzać zmian. Kliknąć przycisk **Dalej**.
4. W oknie **Wybieranie funkcji** zaznaczyć opcje **Kopia zapasowa systemu Windows Server** i **Narzędzia wiersza polecenia**. Kliknąć przycisk **Dalej**.
5. W oknie **Potwierdzanie opcji** instalacji zweryfikować wybór opcji i kliknąć przycisk **Zainstaluj**.
6. Po zakończeniu pracy kreatora kliknąć przycisk **Zamknij**.

Narzędzie do tworzenia kopii zapasowych uruchamia się za pomocą aplikacji **Menedżer serwera**, po wybraniu z menu polecenia **Narzędzia/Kopia zapasowa systemu Windows Server** (rys. 42.1).



Rys. 42.1. Okno główne narzędzia Kopia zapasowa systemu Windows Server

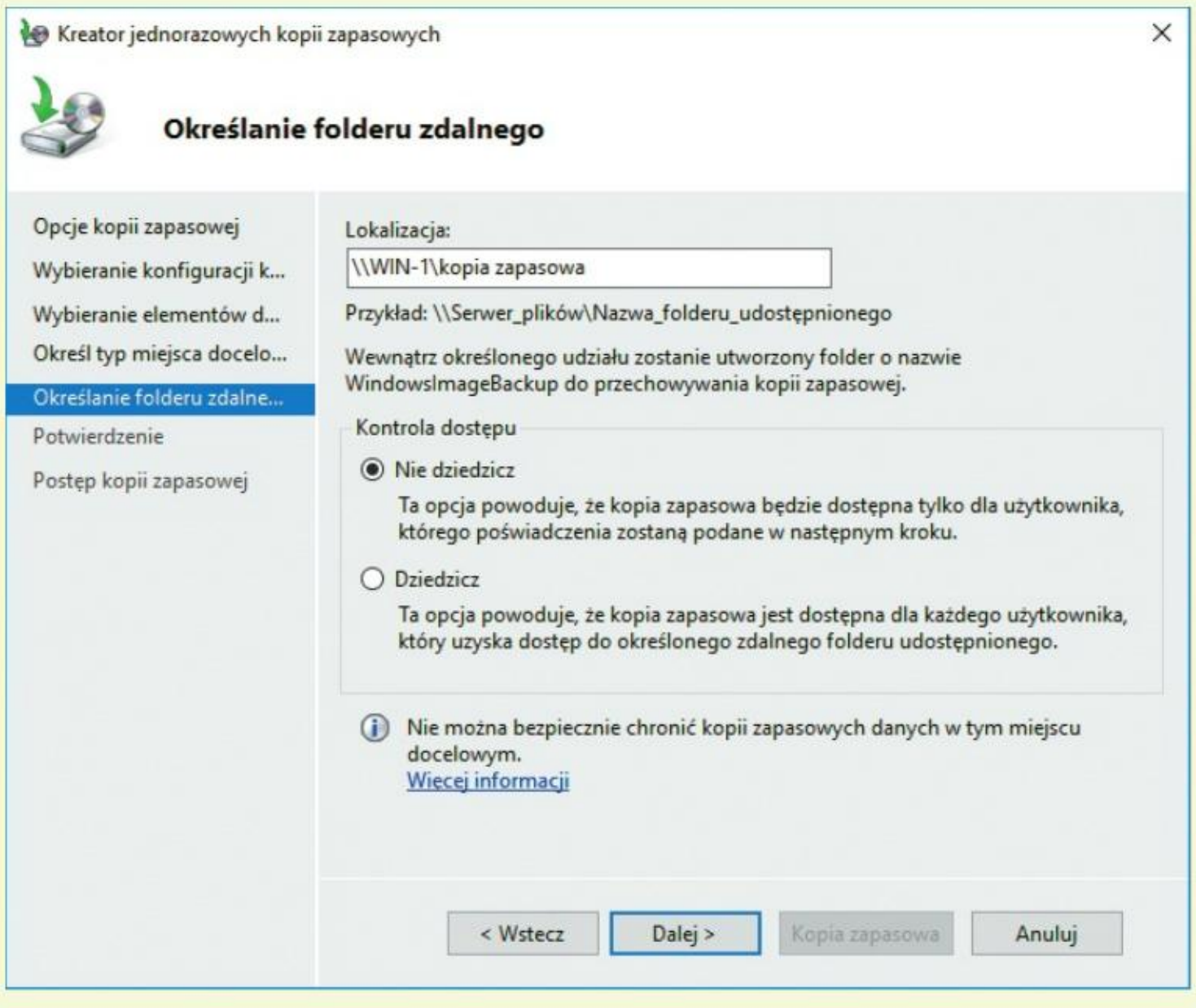
Za jego pomocą można tworzyć kopie zapasowe i odtwarzać dane z przygotowanych wcześniej kopii. We wszystkich tych czynnościach pomaga kreator, który podpowiada kolejne czynności. Do dyspozycji jest również narzędzie do planowania zadań, dzięki któremu można zlecić systemowi automatyczne wykonywanie kopii zapasowych chronionych zbiorów w określonym czasie. W dowolnym momencie można wykonać jednorazową kopię systemu.

PRZYKŁAD 42.2

Tworzenie jednorazowej kopii zapasowej

Aby wykonać jednorazową kopię systemu, należy:

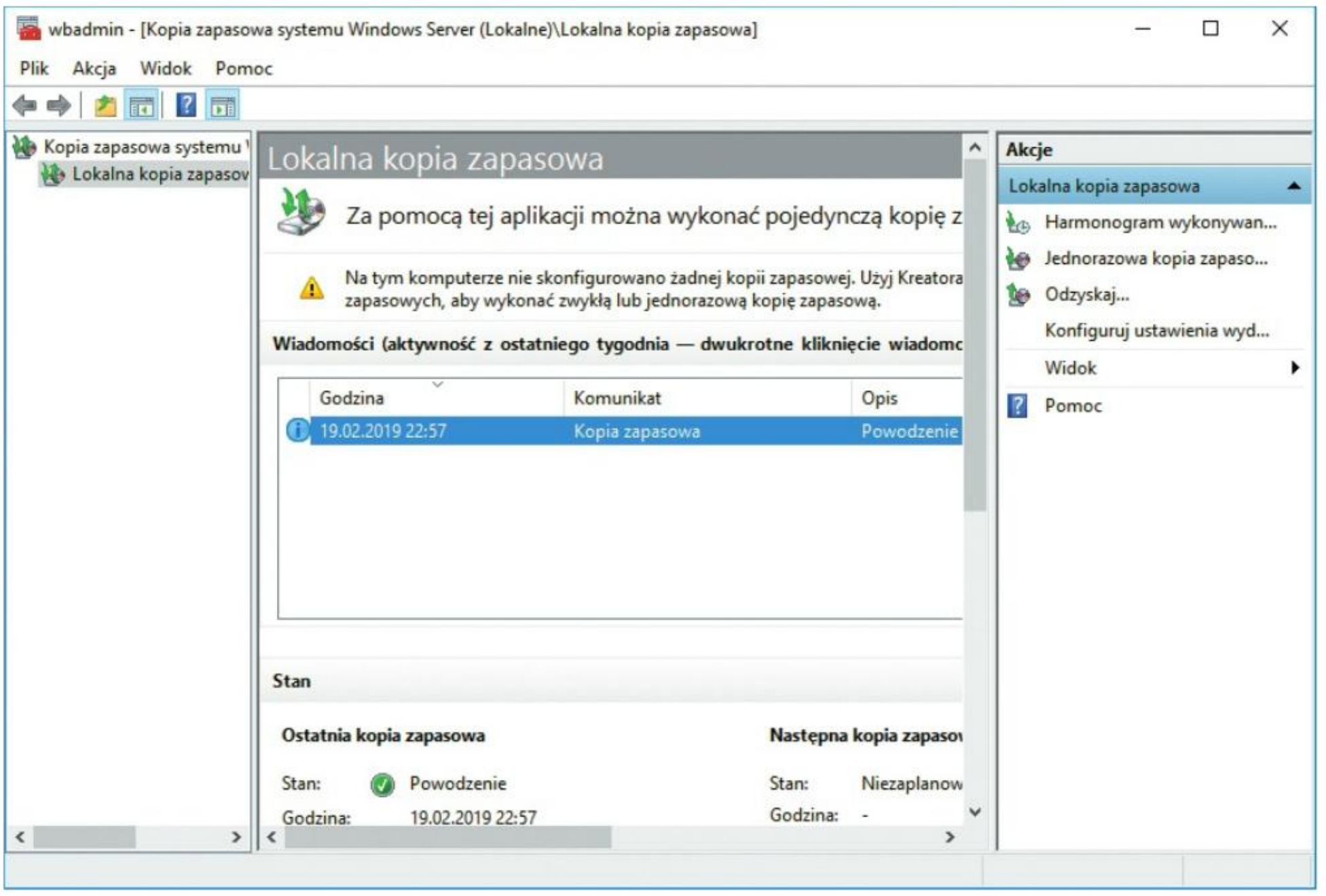
1. Uruchomić **Menedżer serwera**.
2. Wybrać z menu polecenie **Narzędzia/Kopia zapasowa systemu Windows Server**. Rozwinąć gałąź **Magazyn/Kopia zapasowa systemu Windows Server** i kliknąć odnośnik **Jednorazowa kopia zapasowa**.
3. W oknie **Opcje kopii zapasowej** zaznaczyć **Inne opcje**. Kliknąć przycisk **Dalej**.
4. W oknie **Wybieranie konfiguracji kopii zapasowej** zaznaczyć opcję **Niestandardowa**. Pozwoli to na wybranie woluminów lub plików, których kopia ma być wykonana. Można zaznaczyć **Cały serwer**, jeżeli ma być wykonana kopia wszystkich danych z serwera. Kliknąć przycisk **Dalej**.
5. W oknie **Wybieranie elementów do wykonania kopii zapasowej** wskazać zbiory, których kopia ma być utworzona. Kliknąć przycisk **Dodaj elementy**, wskazać elementy i zatwierdzić klawiszem **OK**. Kliknąć przycisk **Dalej**.
6. Kliknąć przycisk **Ustawienia zaawansowane**. W zakładce **Ustawienia usługi VSS** zaznaczyć opcję **Pełna kopia zapasowa VSS**. Kliknąć przycisk **OK**, a następnie **Dalej**.



Rys. 42.2. Okno określania folderu zdalnego

7. Określić miejsce docelowe, w którym będzie tworzona kopia, np. **Zdalny folder udostępniony**. Taki folder musi istnieć i mieć prawo do zapisu. Kliknąć przycisk **Dalej**.
8. Wprowadzić ścieżkę do udostępnionego folderu, w którym ma być tworzona kopia, np. **\\win-1\kopia zapasowa** (rys. 42.2). Zaznaczyć opcję **Nie dziedzicz**. Kliknąć przycisk **Dalej**.
9. Wprowadzić poświadczenia użytkownika uprawnionego do wykonania kopii zapasowej.
10. W oknie **Potwierdzenie** zweryfikować wybór opcji i kliknąć przycisk **Kopia zapasowa**.
11. Po zakończeniu pracy kreatora kliknąć przycisk **Zamknij**.

Jeżeli proces przebiegnie poprawnie, na liście kopii zapasowych pojawi się nowa pozycja opisana za pomocą znacznika czasu powstania kopii (rys. 42.3).



Rys. 42.3. **Lista lokalnych kopii zapasowych**

W razie utraty lub uszkodzenia danych kopia zapasowa może być wykorzystana do odtworzenia oryginalnych danych.

PRZYKŁAD 42.3

Odzyskiwanie danych z jednorazowej kopii zapasowej

Aby odtworzyć dane z jednorazowej kopii systemu, należy:

1. Uruchomić **Menedżer serwera**.

2. Wybrać z menu polecenie **Narzędzia/Kopia zapasowa systemu Windows Server**. Rozwinąć gałąź **Magazyn/Kopia zapasowa systemu Windows Server** i kliknąć odnośnik **Odzyskaj**.
3. W oknie **Wprowadzenie** zaznaczyć **Ten serwer**. Kliknąć przycisk **Dalej**.
4. W oknie **Wybieranie daty kopii zapasowej** wprowadzić datę i godzinę utworzenia kopii zapasowej. **Kliknąć** przycisk **Dalej**.
5. W oknie **Wybieranie typu odzyskiwania** zaznaczyć opcję **Pliki i foldery**. Zaznaczenie opcji **Woluminy** pozwala na odtworzenie zawartości całego woluminu. Kliknąć przycisk **Dalej**.
6. W oknie **Wybieranie elementów do odzyskania** zaznaczyć foldery, których zawartość ma zostać odtworzona. Kliknąć przycisk **Dalej**.
7. W oknie **Określanie opcji odzyskiwania** zaznaczyć opcje **Lokalizacja oryginalna** i **Zastąp istniejące pliki odzyskanymi plikami**. Opcja **Inna lokalizacja** pozwala na utworzenie struktury danych w innym miejscu i ewentualne ręczne przekopiowanie wybranych plików. Kliknąć przycisk **Dalej**.
8. W oknie **Potwierdzenie** zweryfikować wybór opcji i kliknąć przycisk **Odzyskaj**.
9. Po zakończeniu pracy kreatora kliknąć przycisk **Zamknij**.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Za pomocą narzędzia **Kopia zapasowa systemu Windows Server** wykonaj kopię zapasową wybranych folderów, a następnie odzyskaj dane z kopii do innej lokalizacji.
2. Sporządź listę folderów z twojego komputera, które powinny być zabezpieczone przez tworzenie kopii zapasowych.

43 Zasady grup

ZAGADNIENIA

Funkcje polis bezpieczeństwa **Rodzaje polis bezpieczeństwa** **Modyfikowanie zasad grup dotyczących np. polityki haseł** **Zainstalowanie za pomocą GPO programów na stacjach roboczych**

W Windows Server administrator określa zestaw uprawnień obowiązujących w danej sieci za pomocą tzw. **polis bezpieczeństwa**. Polisy, dzięki mechanizmowi dystrybucji, mogą być dystrybuowane na każdy z komputerów w sieci. Polisa jest **zbiorem zasad** określających ogólne uprawnienia komputera lub użytkownika. Polisy mogą obowiązywać na lokalnym komputerze, w lokacji, w domenie lub w jednostce organizacyjnej, a sposób konfiguracji i zakres elementów są bardzo podobne. Wszystkie ustawienia są przechowywane w **obiektach zasad grupy** – **GPO** (ang. *Group Policy Objects*). Każdy komputer z systemem Windows przechowuje jeden **lokalny GPO**. Jeśli komputer należy do środowiska Active Directory, to ustawienia zawarte w lokalnym GPO mogą zostać zastąpione przez **nielokalne obiekty zasad grupy**.

Administrator może opracowywać nowe polisy lub modyfikować istniejące, a następnie rozpowszechnić je w sieci, tak aby obowiązywała w niej wspólna polityka bezpieczeństwa. Zależnie od zakresu stosowania rozróżnia się polisy bezpieczeństwa:

- **zasady lokalne** – określają ustawienia związane z bezpieczeństwem na lokalnym komputerze (mogą być stosowane, gdy komputer nie jest przyłączony do sieci);
- **zasady kontrolera domeny** – określają ustawienia związane z bezpieczeństwem dla kontrolera domeny (obowiązują tylko na kontrolerze domeny);
- **zasady domenowe** – określają ustawienia związane z bezpieczeństwem dla całej domeny (obowiązują na wszystkich komputerach w sieci, z wyjątkiem kontrolera domeny).

Wraz z instalacją Windows Server są instalowane standardowe polisy, które określają zabezpieczenia zależnie od tego, jaką funkcję ma pełnić dany komputer. Domyślnie w momencie instalacji Active Directory są tworzone dwa nielokalne obiekty zasad grupy:

- **domyślne zasady domeny** (ang. *Default Domain Policy*) – GPO połączony z domeną, mający zastosowanie do wszystkich użytkowników i komputerów w domenie (na zasadzie dziedziczenia);
- **domyślne zasady kontrolerów domen** (ang. *Default Domain Controllers Policy*) – GPO połączony z jednostką organizacyjną *domain controllers* (kontrolery domen), który zazwyczaj ma zastosowanie tylko do kontrolerów domen.

Do zarządzania obiektami GPO służy **konsola zarządzania zasadami grupy** (ang. *Group Policy Management Console*).

W obiektach GPO ustawienia podzielono na dwa typy:

- **ustawienia komputera** (ang. *computer configuration*) – ustawienia są stosowane dla komputerów niezależnie od zalogowanego użytkownika;

- **ustawienia użytkownika** (ang. *user configuration*) – ustawienia wprowadzane podczas logowania użytkownika, niezależnie od komputera, na którym jest przeprowadzane logowanie.

Ustawienia zasad są stosowane w następującej kolejności:

- lokalny GPO;
- GPO lokacji – stosowane synchronicznie, w kolejności określonej przez administratora;
- GPO domeny – stosowane synchronicznie, w kolejności określonej przez administratora;
- GPO jednostek organizacyjnych – w pierwszej kolejności są stosowane GPO powiązane z jednostką organizacyjną usytuowaną najwyżej w hierarchii Active Directory, a następnie GPO powiązane z jej podrzędną jednostką organizacyjną itd.

Na każdym poziomie może być używany jeden GPO, kilka GPO lub żaden GPO. Jeśli dana jednostka organizacyjna jest powiązana z kilkoma GPO, to są one stosowane synchronicznie, w kolejności określonej przez administratora. W wypadku konfliktu między ustawieniami konfiguracji komputera a ustawieniami konfiguracji użytkownika pierwszeństwo mają ustawienia konfiguracji użytkownika. Jeżeli konflikt nie występuje, to obowiązują zarówno ustawienia użytkownika, jak i komputera.

Zasady są przetwarzane w trakcie pewnych zdarzeń:

- zasady zawarte w **konfiguracji komputera** są stosowane w trakcie uruchamiania komputera oraz jego wyłączania, a także cyklicznie w czasie pracy (domyślnie co 90 minut na serwerach członkowskich oraz stacjach roboczych, co 5 minut na kontrolerach domeny);
- zasady zawarte w **konfiguracji użytkownika** są przetwarzane podczas logowania danego użytkownika, wylogowania oraz cyklicznie w czasie pracy (domyślnie co 90 minut). Można również wymusić odświeżenie zasad.

Zasady grupy mogą być **dziedziczone** z kontenerów nadrzędnych do kontenerów podrzędnych w obrębie domeny, ale zasady powiązane z domeną nie są dziedziczone przez jej domeny podrzędne.

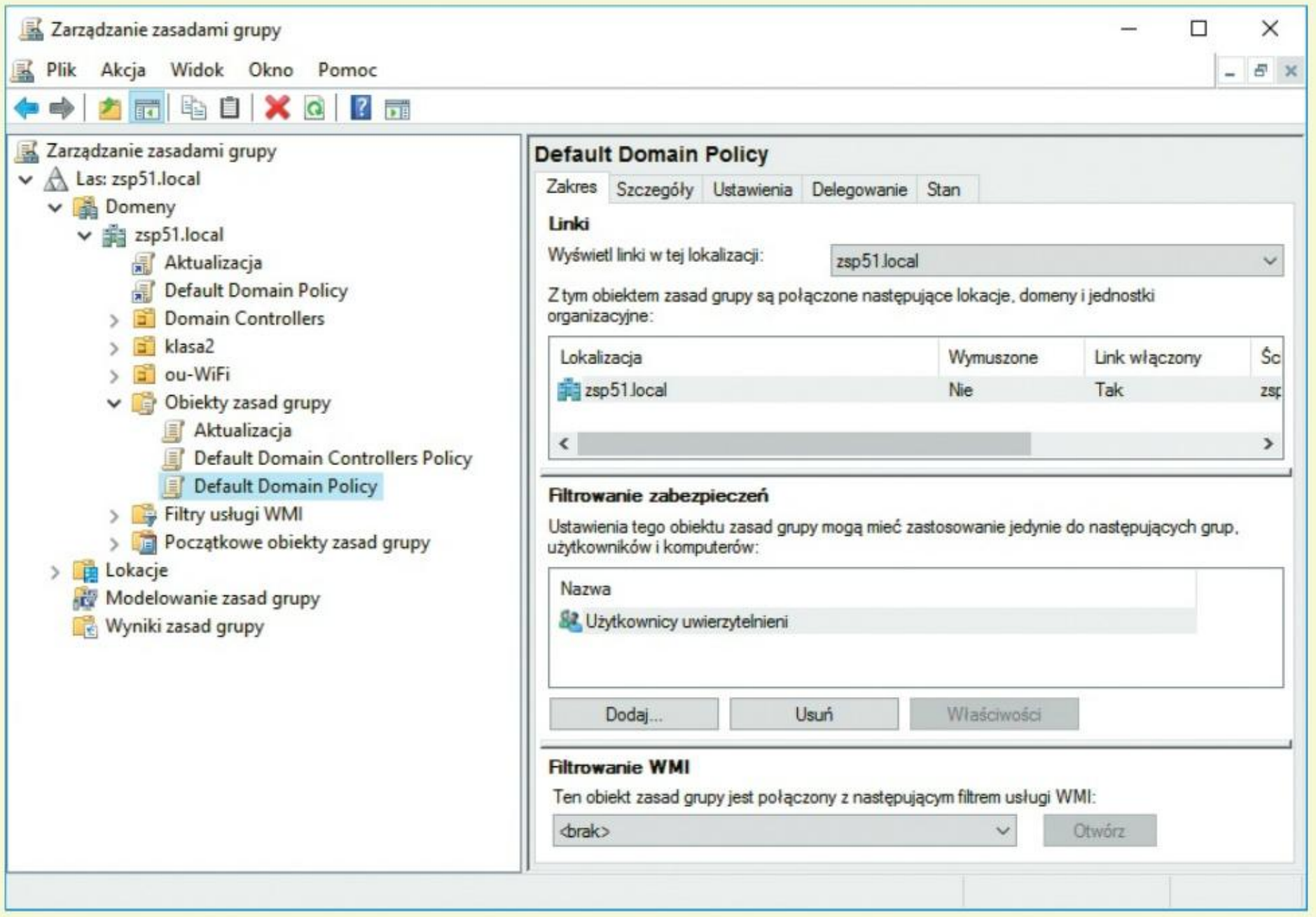
PRZYKŁAD 43.1

Modyfikowanie zasad grupy dotyczących polityki haseł

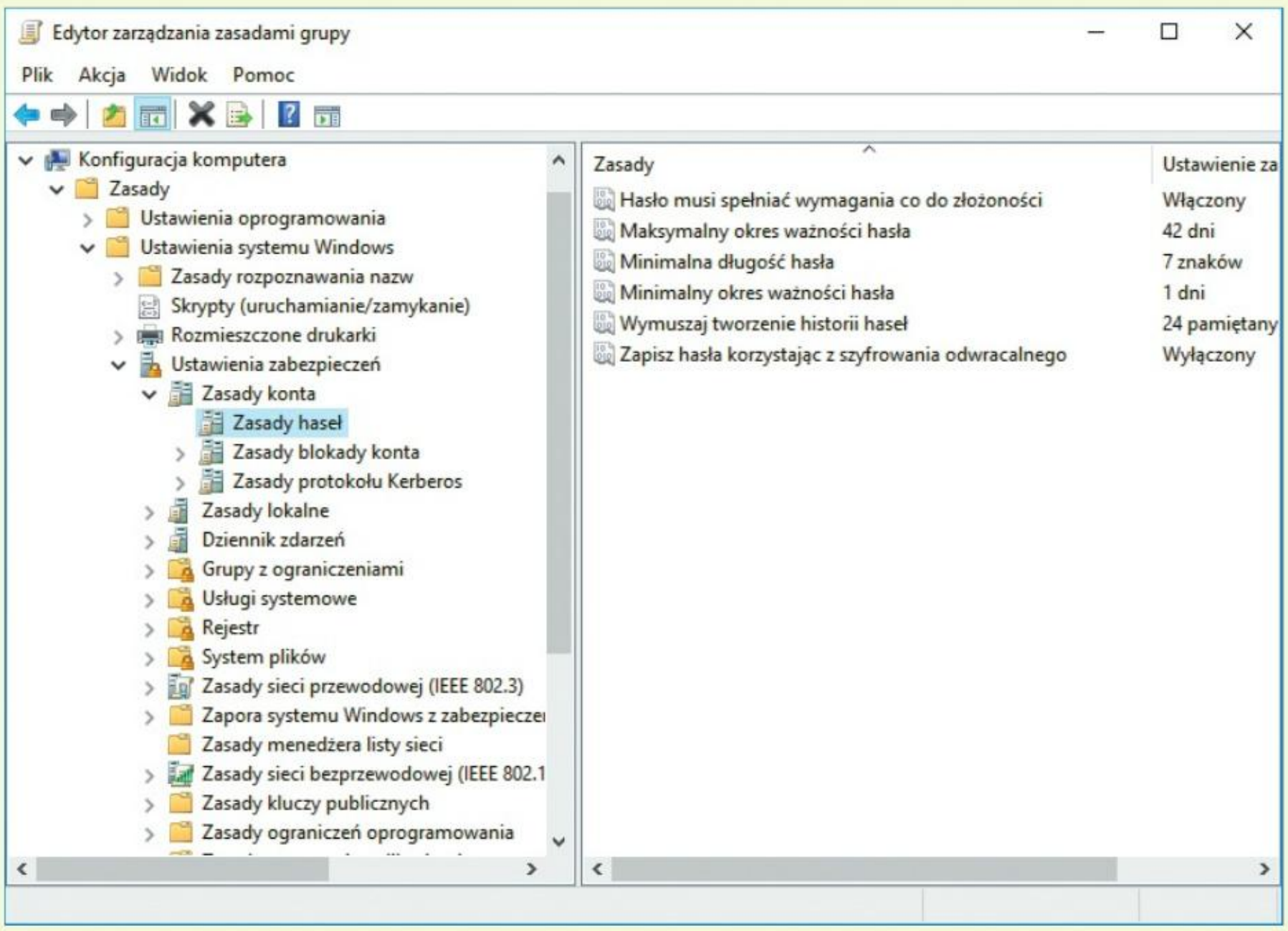
Jedną z przykładowych możliwości wykorzystania polisy bezpieczeństwa jest stworzenie polityki haseł w domenie. Do zdefiniowania polityki haseł zostanie wykorzystany **`Edytor zarządzania zasadami grupy`**.

Aby zmodyfikować politykę haseł obowiązującą w domenie, należy:

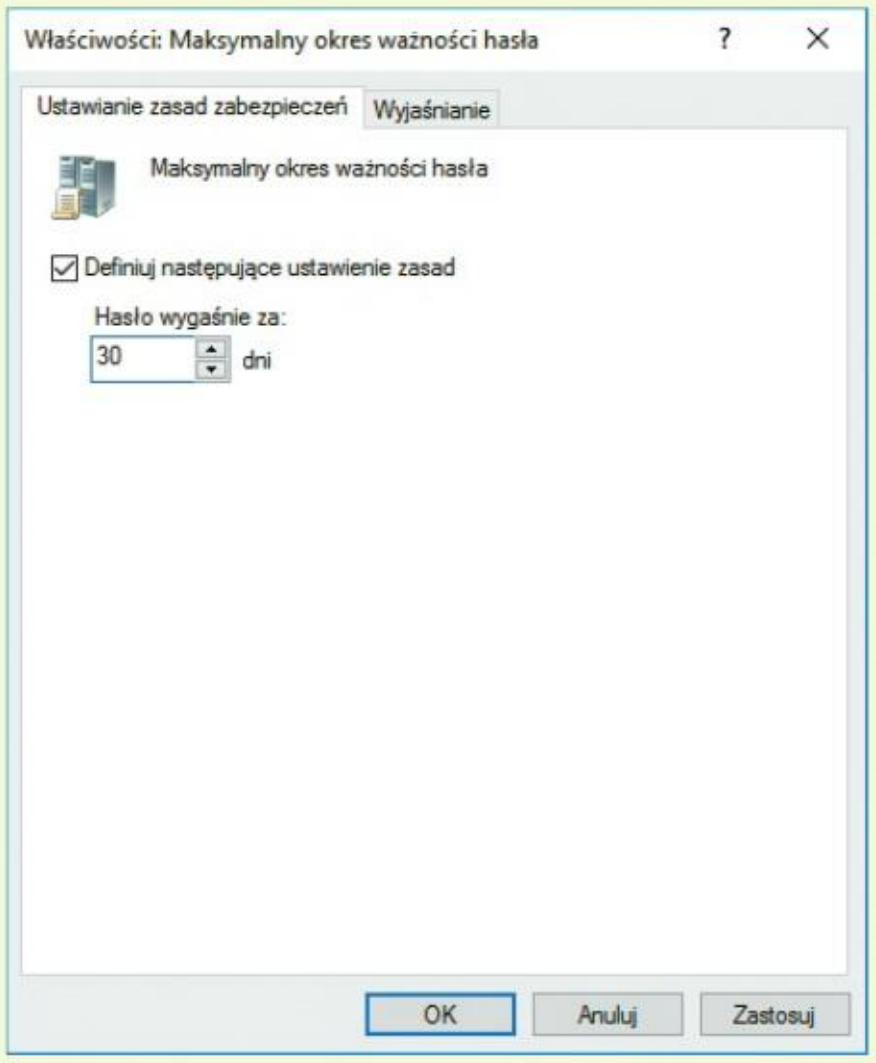
1. Uruchomić aplikację **`Zarządzanie zasadami grupy`** – w oknie **`Menedżer serwera`** z menu wybrać polecenia **`Narzędzia/Zarządzanie zasadami grupy`**.
2. Odszukać w strukturze domyślną polisę zasad domeny – w lewym panelu rozwinąć gałęzie **`Las/Domeny/Nazwa domeny/Obiekty zasad grupy/Default Domain Policy`** (rys. 43.1).
3. Kliknąć prawym przyciskiem myszy **`Default Domain Policy`** i z menu kontekstowego wybrać **`Edytuj`**.
4. Rozwinąć gałąź **`Konfiguracja komputera/Zasady/Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zasady konta/Zasady haseł`** (rys. 43.2).
5. Kliknąć prawym przyciskiem myszy wybrane ustawienie i z menu kontekstowego wybrać **`Właściwości`**. W oknie **`Właściwości`** wprowadzić wartość i kliknąć przycisk **`Zastosuj`** (rys. 43.3).



Rys. 43.1. **Okno zasad domyślnej polisy w domenie**



Rys. 43.2. **Okno zasad haseł**



Rys. 43.3. **Ustawienie wartości zasad haseł**

Aby zasady obowiązywały, trzeba włączyć opcję **`Hasło musi spełniać wymagania co do złożoności`**. Pozostałe opcje oznaczają odpowiednio:

- **Maksymalny okres ważności hasła** – liczbę dni, po której użytkownik musi zmienić hasło;
- **Minimalna długość hasła** – minimalną liczbę znaków w haśle;
- **Minimalny okres ważności hasła** – okres, jaki musi upłynąć, aby użytkownik mógł ponownie zmienić hasło. Musi upłynąć określony czas, aby użytkownik mógł ponownie zmienić hasło;
- **Wymuszaj tworzenie historii haseł** – liczbę haseł, które system będzie pamiętał i nie pozwalał na ponowne wprowadzenie hasła wcześniej używanego;
- **Zapisz hasła, korzystając z szyfrowania odwracalnego** – to, że niektóre aplikacje wymagają włączenia szyfrowania haseł, ale w większości przypadków powinno być ono wyłączone.

PRZYKŁAD 43.2

Ograniczanie dostępu użytkowników do panelu sterowania za pomocą zasad grupy

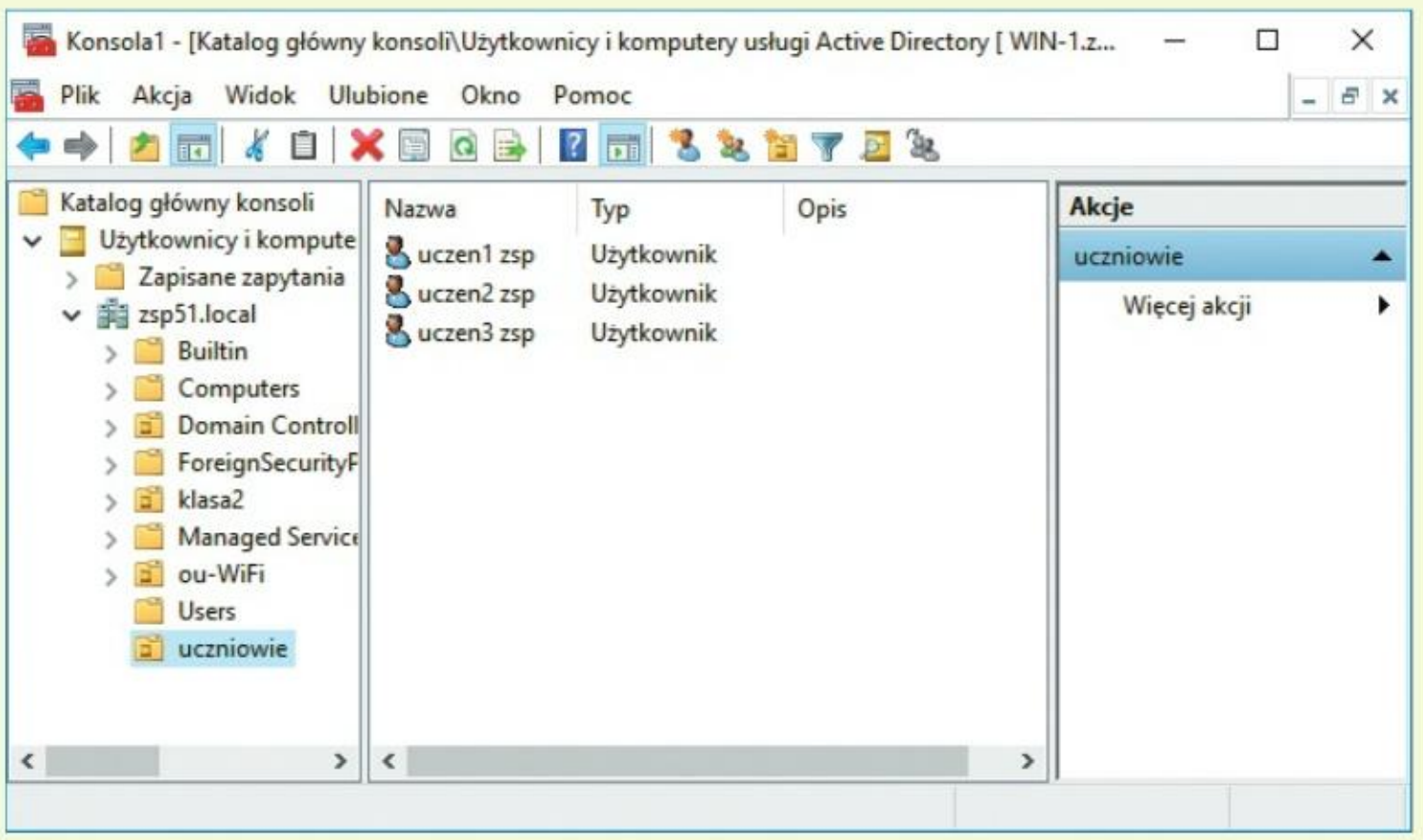
Za pomocą polis bezpieczeństwa można ograniczyć dostęp użytkowników do wybranych funkcji systemu, np. panelu sterowania, ustawień pulpitu, dysków przenośnych. Administrator lub inna uprawniona osoba ma **prawo tworzenia nowych obiektów zasad grup (GPO)**. Zarządzanie zasadami grupy składa się z dwóch etapów: **utworzenia obiektu zasad** i **połączenia obiektu GPO z kontenerem**, np. domeną, lokacją lub jednostką organizacyjną.

W tym przykładzie zostanie utworzona jednostka organizacyjna *uczniowie*, a w niej trzy konta użytkowników: *uczen1*, *uczen2* i *uczen3*. Obiekt GPO zablokuje dostęp do panelu sterowania dla kont *uczen1* i *uczen2* w jednostce organizacyjnej *uczniowie* (*uczen3* będzie miał prawo dostępu do panelu, co pozwoli na weryfikację polityki).

Aby utworzyć nowy obiekt GPO i połączyć go z jednostką, należy:

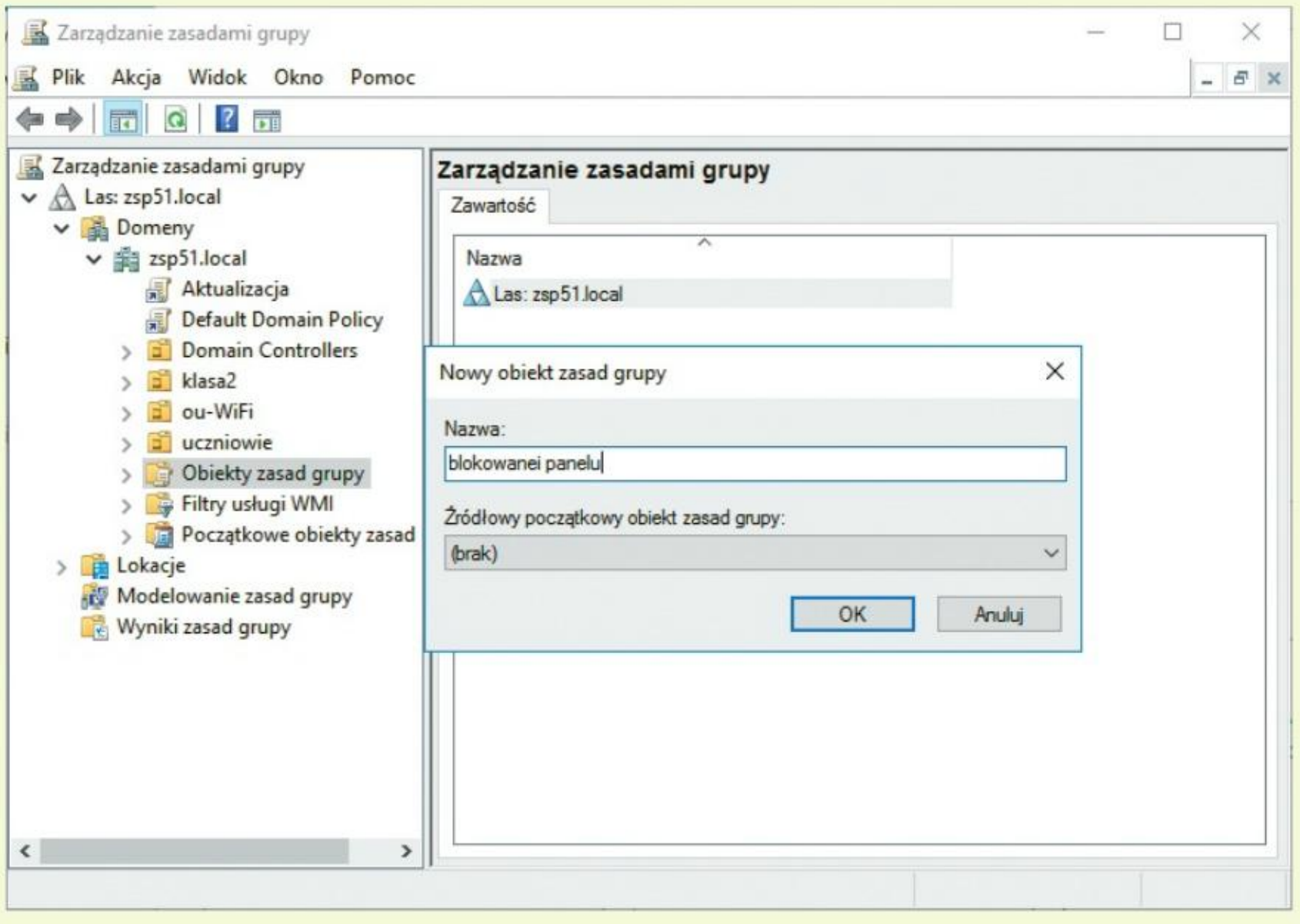
1. Utworzyć jednostkę organizacyjną *uczniowie* i w niej trzy konta: *uczen1*, *uczen2* i *uczen3*. W tym celu można wykorzystać przystawkę **`Użytkownicy i komputery usługi Active Directory`** w konsoli mmc. Okno konsoli z utworzoną w domenie

zsp51.local jednostką organizacyjną i kontami użytkowników przedstawiono na rys. 43.4.



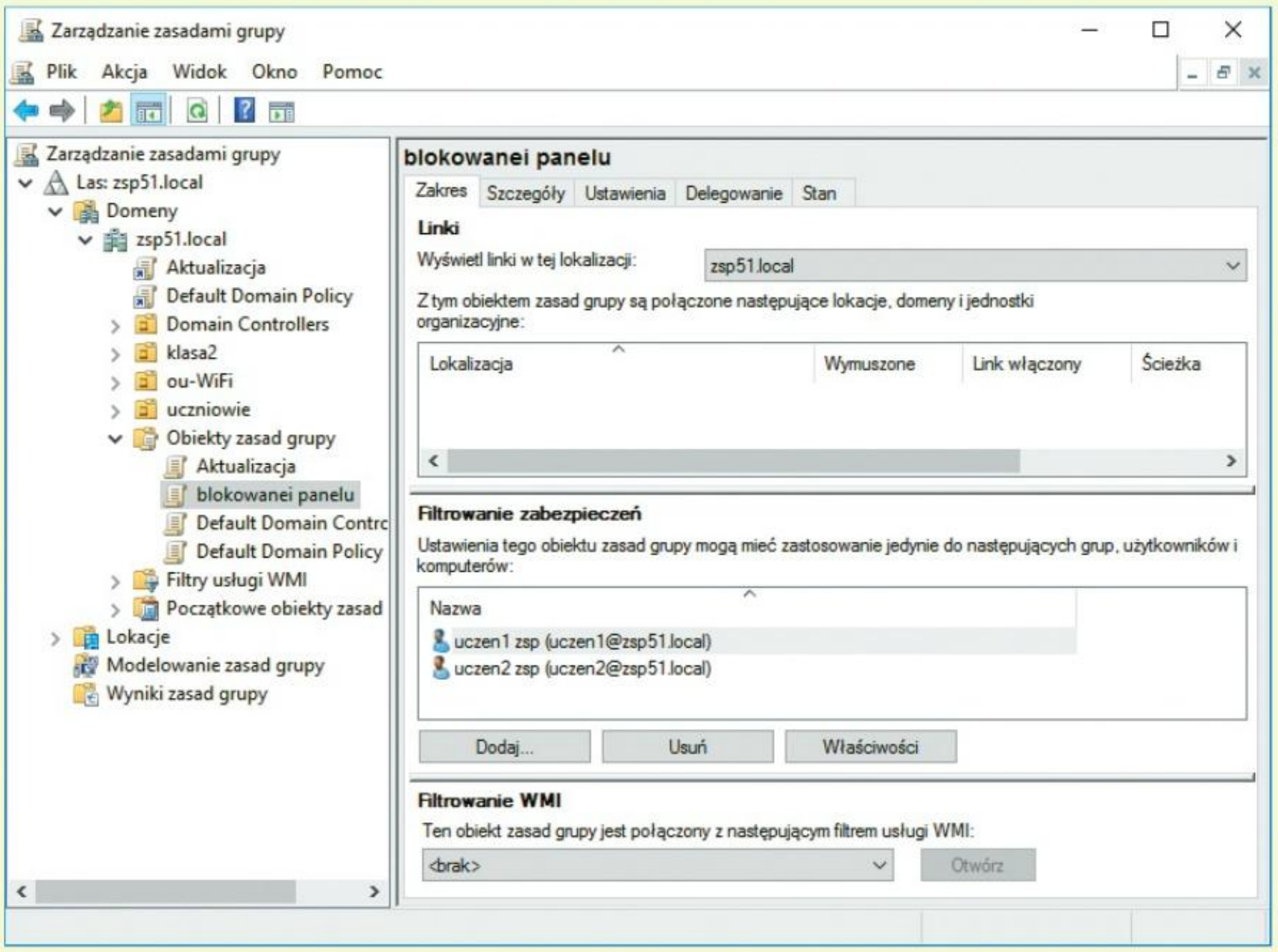
Rys. 43.4. **Okno konsoli z utworzoną w domenie zsp51.local jednostką organizacyjną i kontami użytkowników**

2. Utworzyć obiekt GPO o nazwie **blokowanie panelu**. Uruchomić aplikację **Zarządzanie zasadami grupy** – polecenie **Narzędzia/Zarządzanie zasadami grupy** w oknie **Menedżer serwera**. W lewym panelu odszukać domenę **zsp51.local**, kliknąć prawym klawiszem myszy gałąź **Obiekty zasad grupy** i z menu kontekstowego wybrać **Nowe**. Wpisać nazwę tworzonego obiektu, np. **blokowanie panelu** (rys. 43.5), i kliknąć **OK**.



Rys. 43.5. **Tworzenie nowego obiektu zasad grupy**

Edycję nowo utworzonego obiektu rozpoczynamy od dwukrotnego kliknięcia jego nazwy. W zakładce **Zakres** w sekcji **Filtrowanie zabezpieczeń** można określić, których użytkowników będzie dotyczyć wprowadzana polityka. Domyślnie są to *Użytkownicy uwierzytelnieni*. Polityka powinna obowiązywać tylko użytkowników *uczen1* i *uczen2* (do sprawdzenia skuteczności polityka nie będzie dotyczyła użytkownika *uczen3*), dlatego w jednostce *uczniowie* należy do listy dodać (przycisk **Dodaj**) konta użytkowników *uczen1* i *uczen2* oraz usunąć grupę *Użytkownicy uwierzytelnieni* (rys. 43.6).

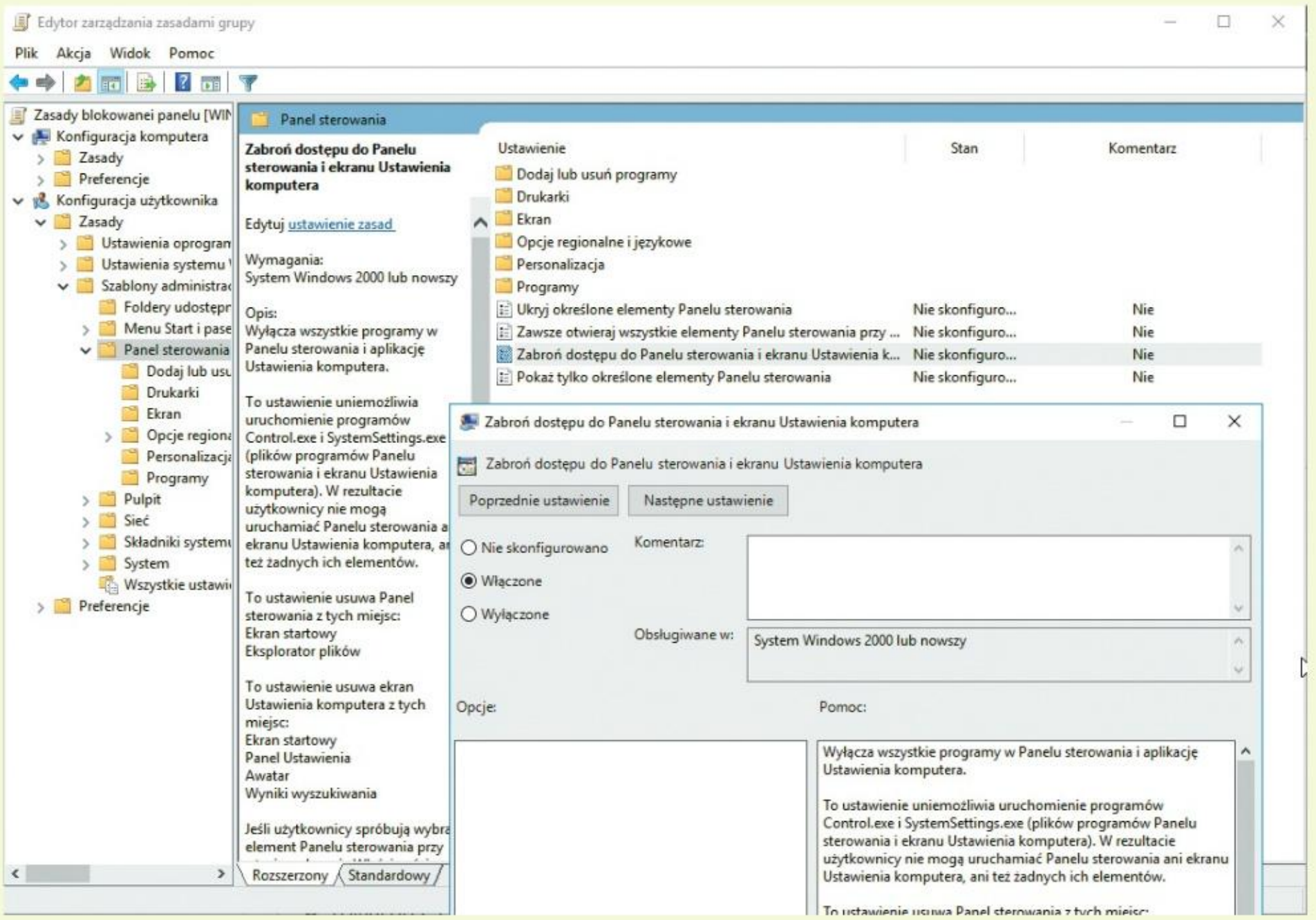


Rys. 43.6. **Tworzenie listy użytkowników, których będzie dotyczyć polityka**

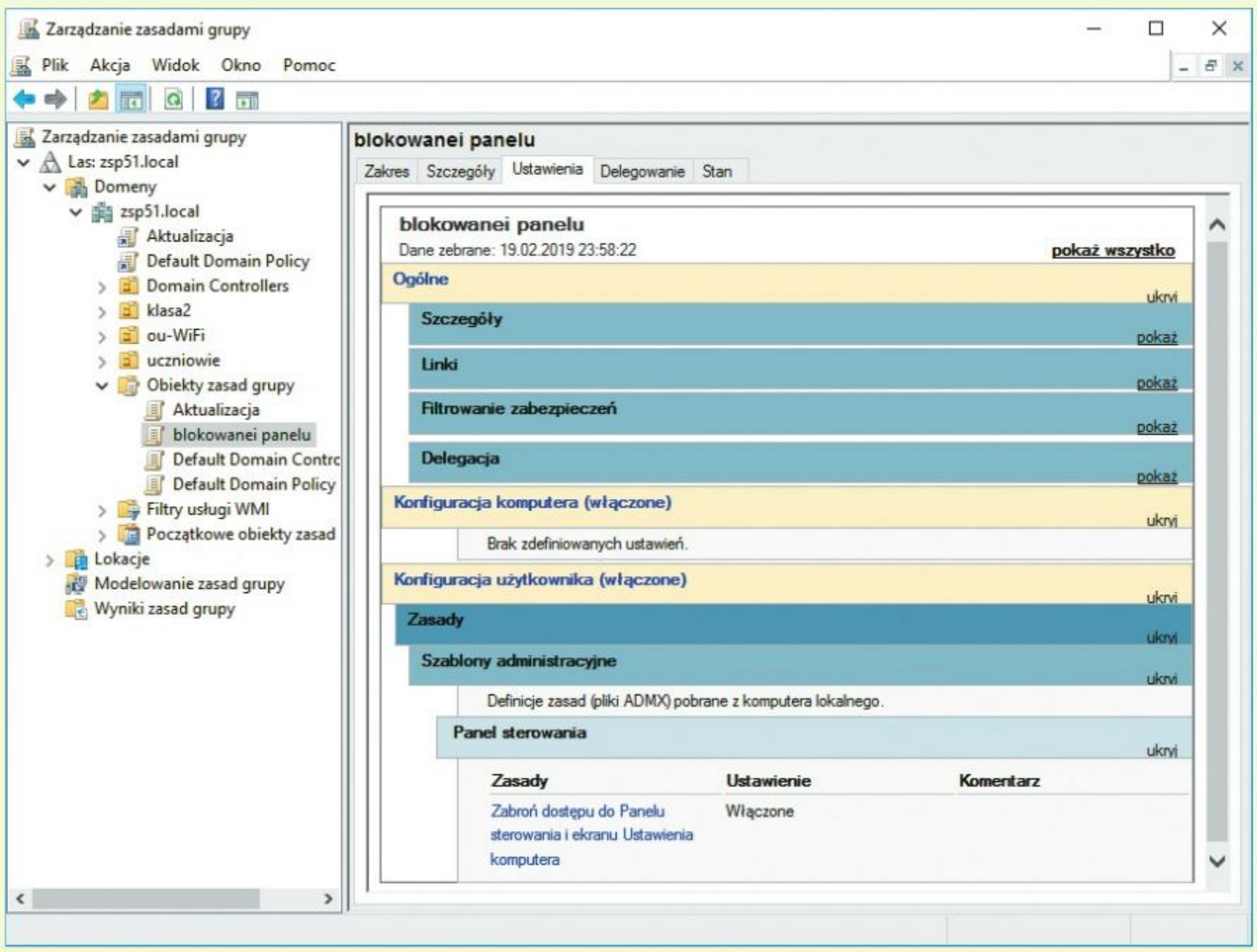
W zakładce **Ustawienia** należy kliknąć prawym przyciskiem myszy białe pole i z menu kontekstowego wybrać **Edytuj**. W lewym panelu rozwinąć gałąź **Konfiguracja użytkownika/Zasady/Szablony administracyjne/Panel sterowania**. Kliknąć ustawienie **Zabroń dostępu do Panelu sterowania** i ustawić wartość na **Włączone** (rys. 43.7).

Po odświeżeniu okna można sprawdzić poprawność zasady (rys. 43.8).

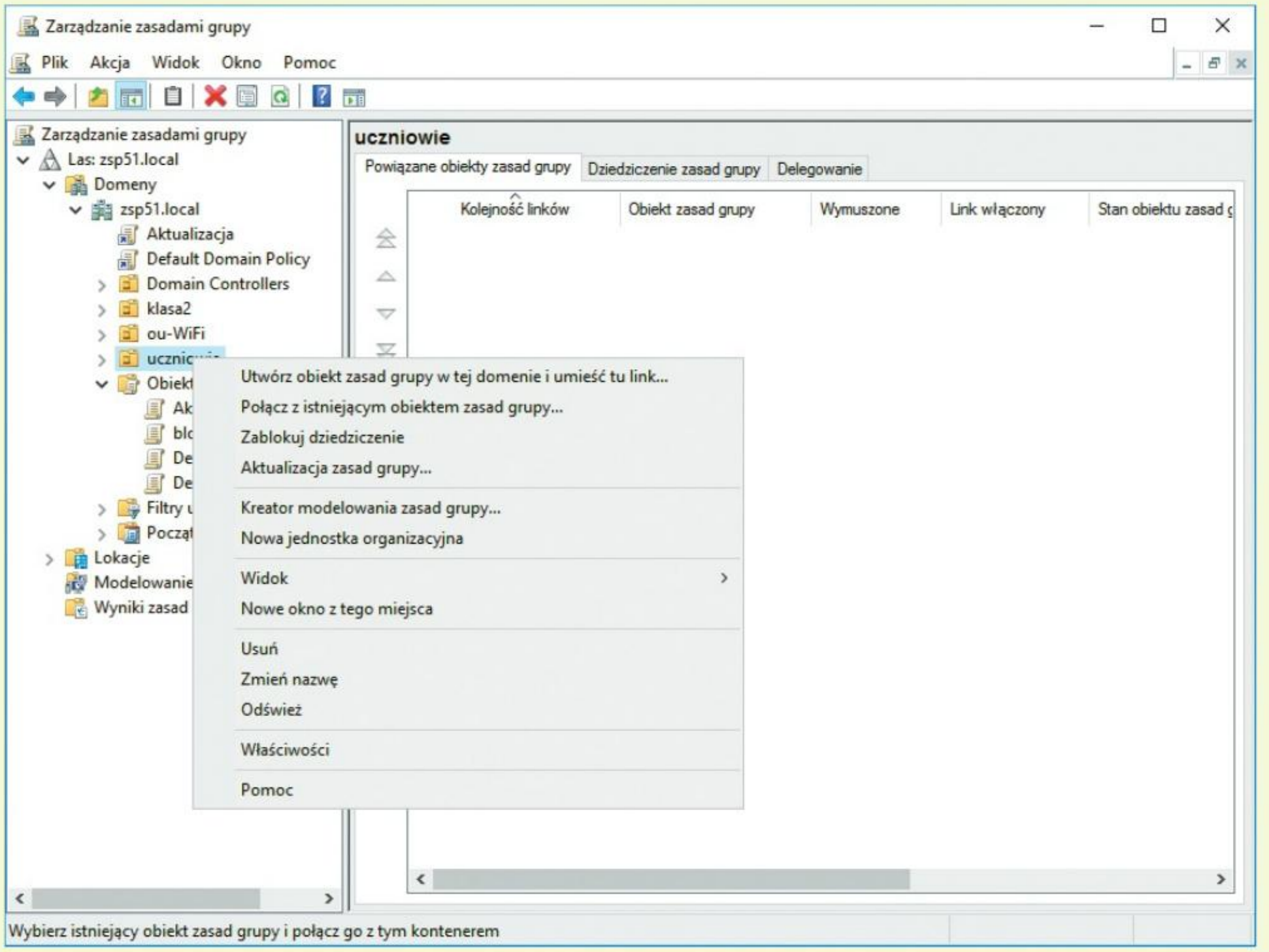
3. Połączyć obiekt GPO **blokowanie panelu** z jednostką organizacyjną *uczniowie*. W lewym panelu odszukać kontener jednostki organizacyjnej *uczniowie*, kliknąć go prawym klawiszem myszy i z menu kontekstowego wybrać **Połącz z istniejącym obiektem zasad grupy** (rys. 43.9). W oknie **Wybieranie obiektu zasad grupy** wskazać obiekt **blokowanie panelu** i kliknąć **OK**.



Rys. 43.7. **Włączenie blokowania Panelu sterowania**

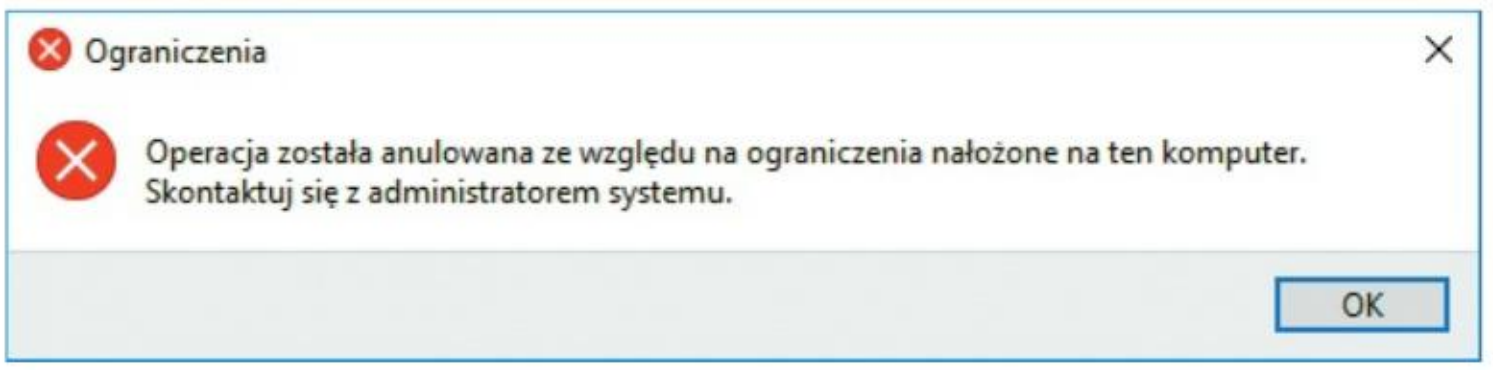


Rys. 43.8. **Weryfikacja zasady blokowania panelu sterowania**



Rys. 43.9. **Łączenie kontenera jednostki organizacyjnej z obiektem zasad grupy**

Zasada zacznie obowiązywać po odświeżeniu polityki, np. po określonym czasie lub w trakcie następnego zalogowania użytkownika. Na rys. 43.10 przedstawiono, że panel sterowania został zablokowany dla użytkowników *uczen1* i *uczen2*. Użytkownik *uczen3* może w dalszym ciągu korzystać z panelu, ponieważ nie został dodany do listy w sekcji **`Filtrowanie zabezpieczeń`** okna **`Zakres`**.



Rys. 43.10. **Próba uruchomienia Panelu sterowania przez użytkownika uczen1**

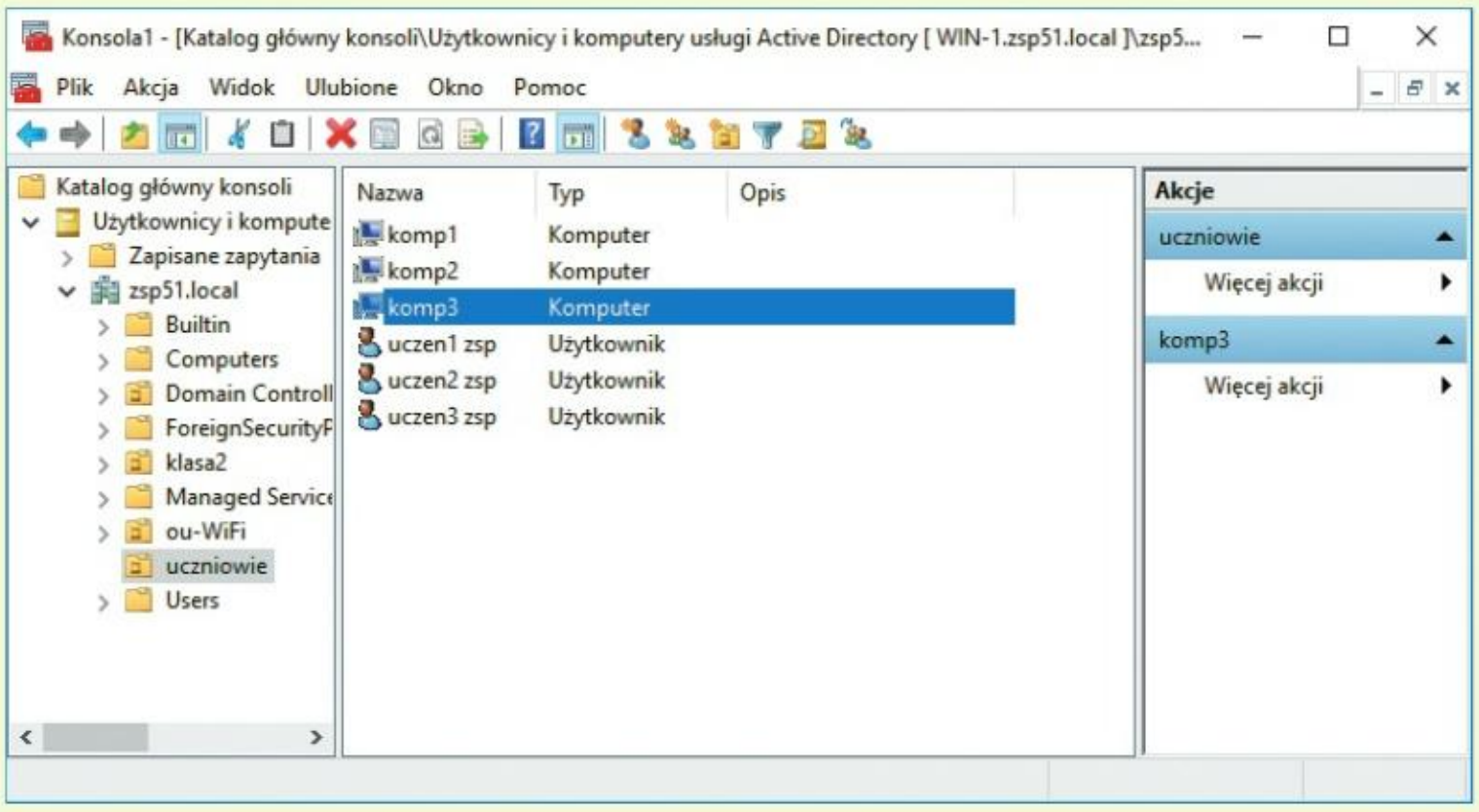
Obiekty zasad grupy można wykorzystać również do instalacji i aktualizacji oprogramowania stacji roboczych, przyłączonych do domeny. Konta komputerów, na których należy automatycznie instalować oprogramowanie, trzeba umieścić w jednostce organizacyjnej. Następnie utworzyć obiekt zasad grupy, którego zadaniem jest instalacja oprogramowania, i powiązać ten obiekt z jednostką organizacyjną. Instalacja oprogramowania będzie przeprowadzana podczas uruchomienia komputera, bez konieczności podejmowania jakichkolwiek działań przez użytkownika.

PRZYKŁAD 43.3

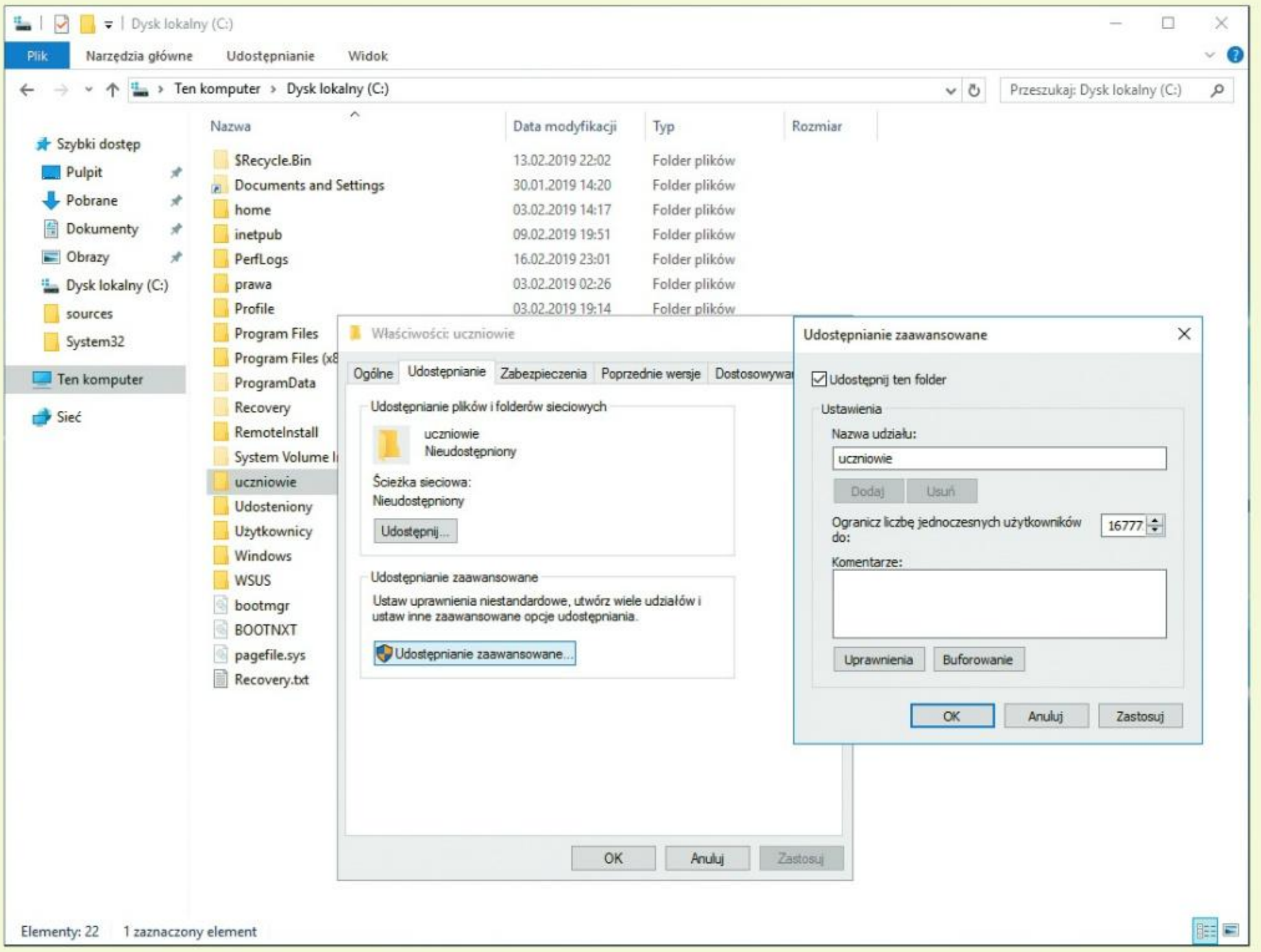
Konfigurowanie systemu dystrybucji oprogramowania stacji roboczych

W tym przykładzie zostanie pokazana metoda dystrybucji oprogramowania do stacji roboczych pracujących w domenie. Aby skonfigurować ten system, należy:

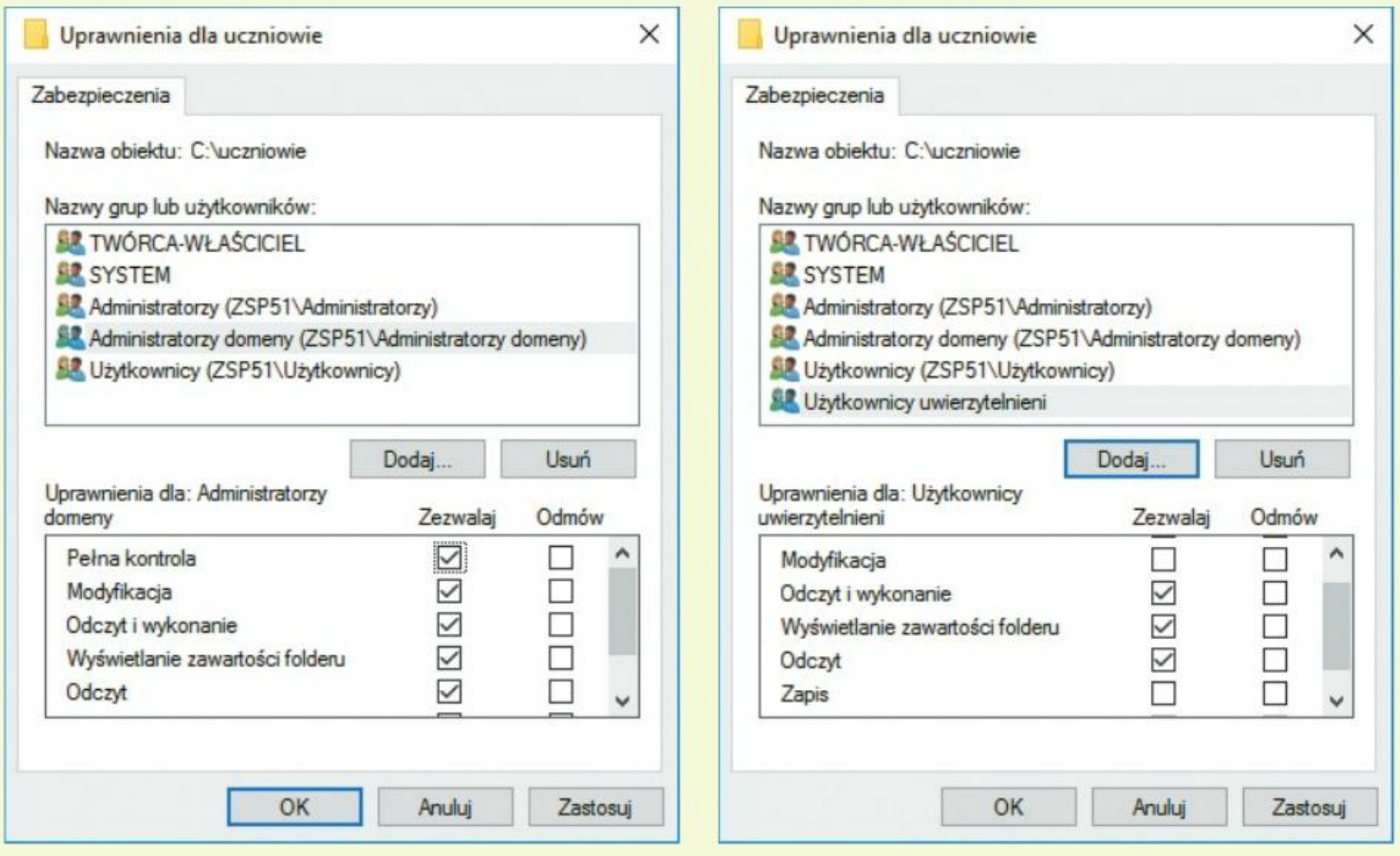
1. Utworzyć jednostkę organizacyjną, np. *uczniowie* (można skorzystać z jednostki utworzonej w poprzednim przykładzie) i w niej konta komputerów, np. *komp1*, *komp2*, *komp3*. W tym celu można wykorzystać przystawkę **Użytkownicy i komputery usługi Active Directory** w konsoli mmc. Okno konsoli z utworzoną w domenie **zsp51.local** jednostką organizacyjną i kontami komputerów przedstawiono na rys. 43.11. Przyłączyć komputery do domeny.
2. Utworzyć na dysku serwera folder zawierający programy przeznaczone do dystrybucji, np. folder **C:\uczniowie**. Skopiować do folderu pakiety instalacyjne instalowanych programów (pliki ***.msi**).
3. Udostępnić folder **uczniowie** (rys. 43.12). Dla wszystkich użytkowników nadać uprawnienia **Pełna kontrola**.
4. Nadać uprawnienia w systemie NTFS do folderu **uczniowie**. Grupa *Administratorzy domeny* powinna mieć prawa pełnej kontroli, natomiast grupa *Użytkownicy uwierzytelnieni* prawa odczytu (rys. 43.13).
5. Umieścić w folderze **uczniowie** pakiety instalacyjne programów (pliki **.msi**), które mają być automatycznie instalowane.
6. Wybrać w oknie **Menedżer serwera** polecenie **Narzędzia/Zarządzanie zasadami grupy**. Odszukać jednostkę organizacyjną *uczniowie*, kliknąć prawym przyciskiem myszy i z menu kontekstowego wybrać opcję **Utwórz obiekt zasad grup w tej domenie i umieść tu link**. W oknie **Nowy obiekt zasad grupy** wprowadzić nazwę, np. **instalowanie oprogramowania** (rys. 43.14).
7. Kliknąć prawym przyciskiem myszy utworzony obiekt i z menu kontekstowego wybrać opcję **Edytuj**.
8. Rozwinąć gałąź **Konfiguracja komputera/Zasady/Ustawienia oprogramowania/Instalacja oprogramowania**. Kliknąć prawym przyciskiem myszy białe pole prawego panelu i z menu kontekstowego wybrać opcję **Nowy/Pakiet** (rys. 43.15).



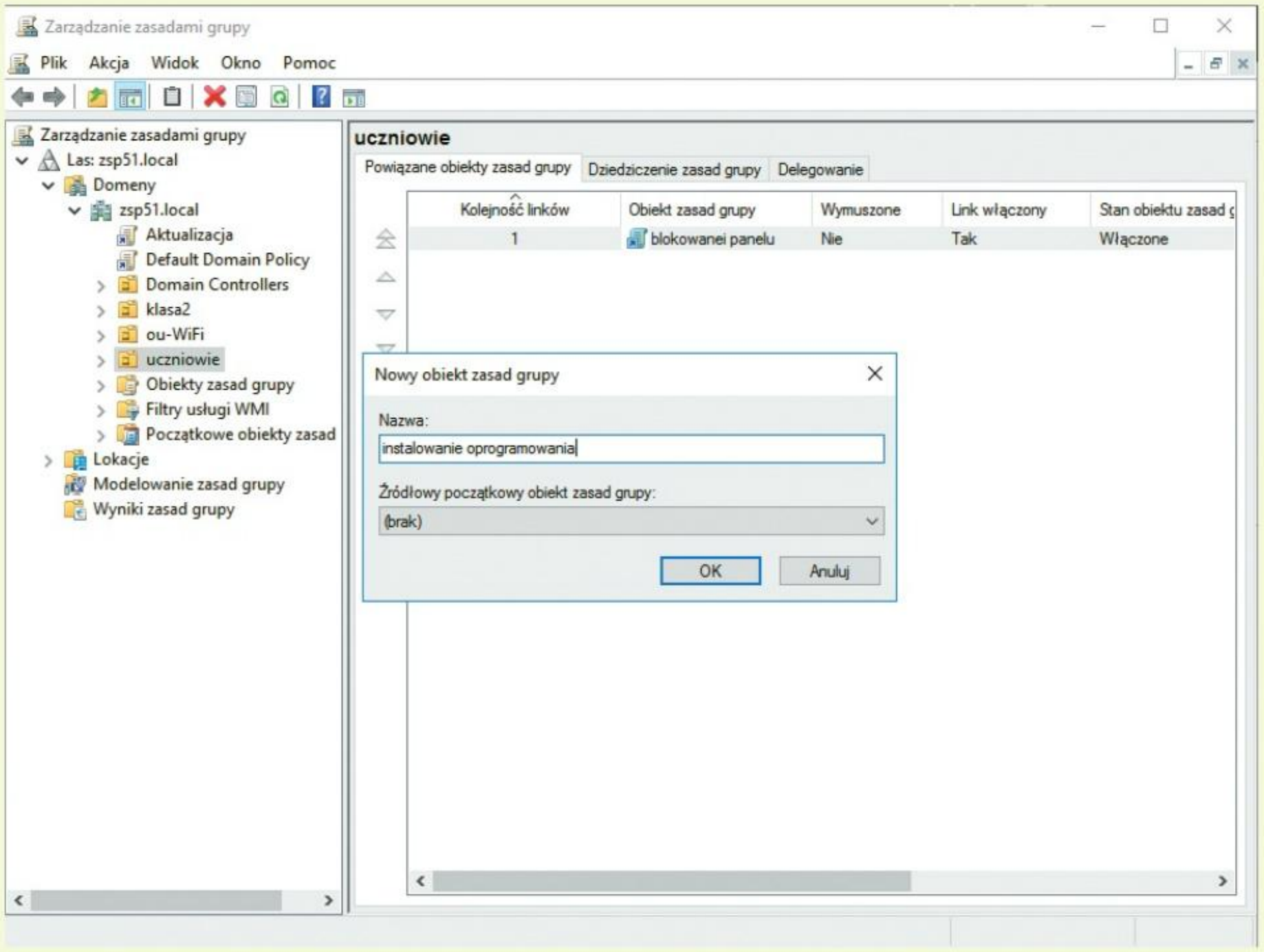
Rys. 43.11. **Jednostka organizacyjna z kontami komputerów**



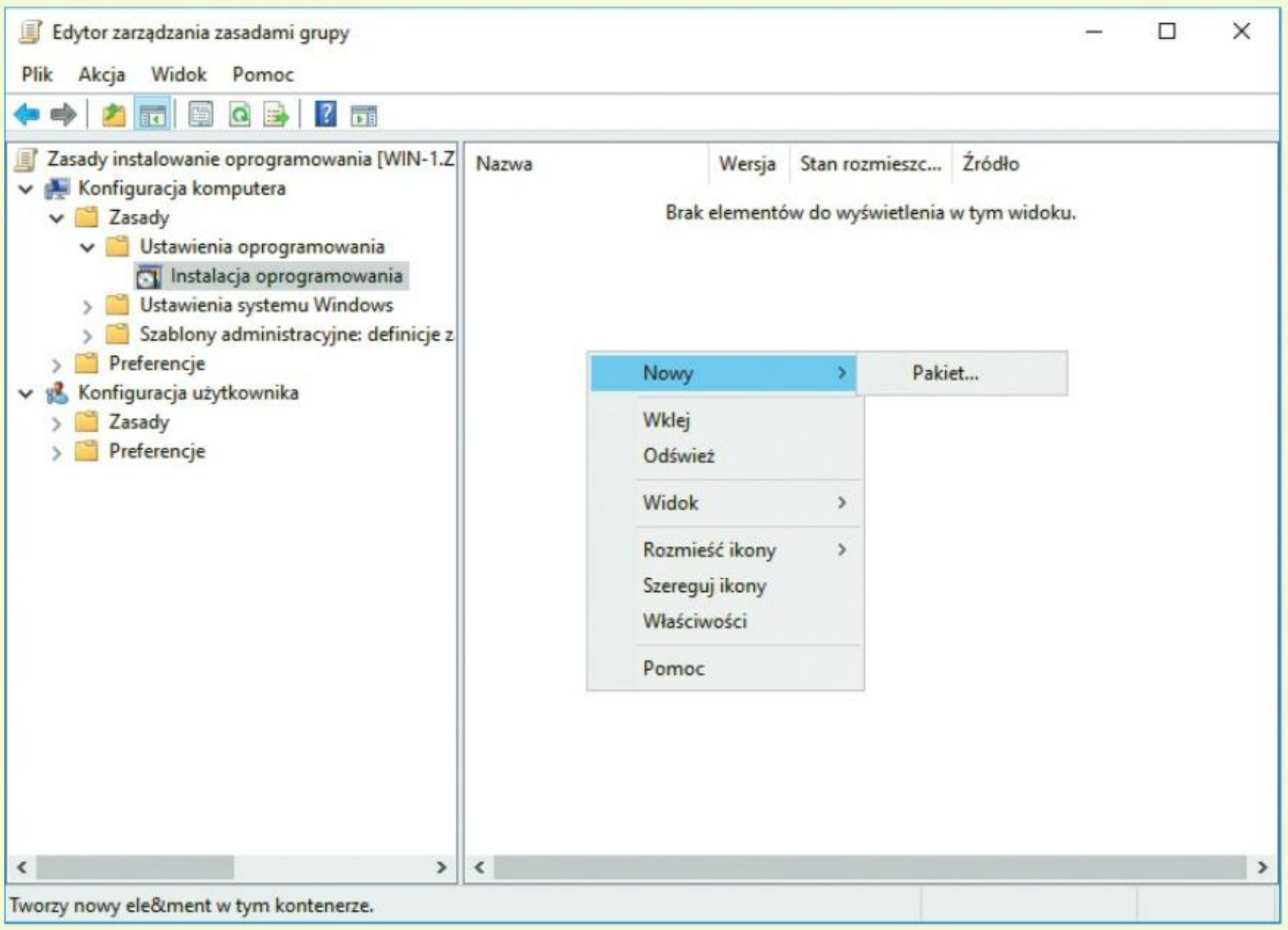
Rys. 43.12. **Udostępnianie folderu `uczniowie`**



Rys. 43.13. **Uprawnienia folderu `uczniowie`**

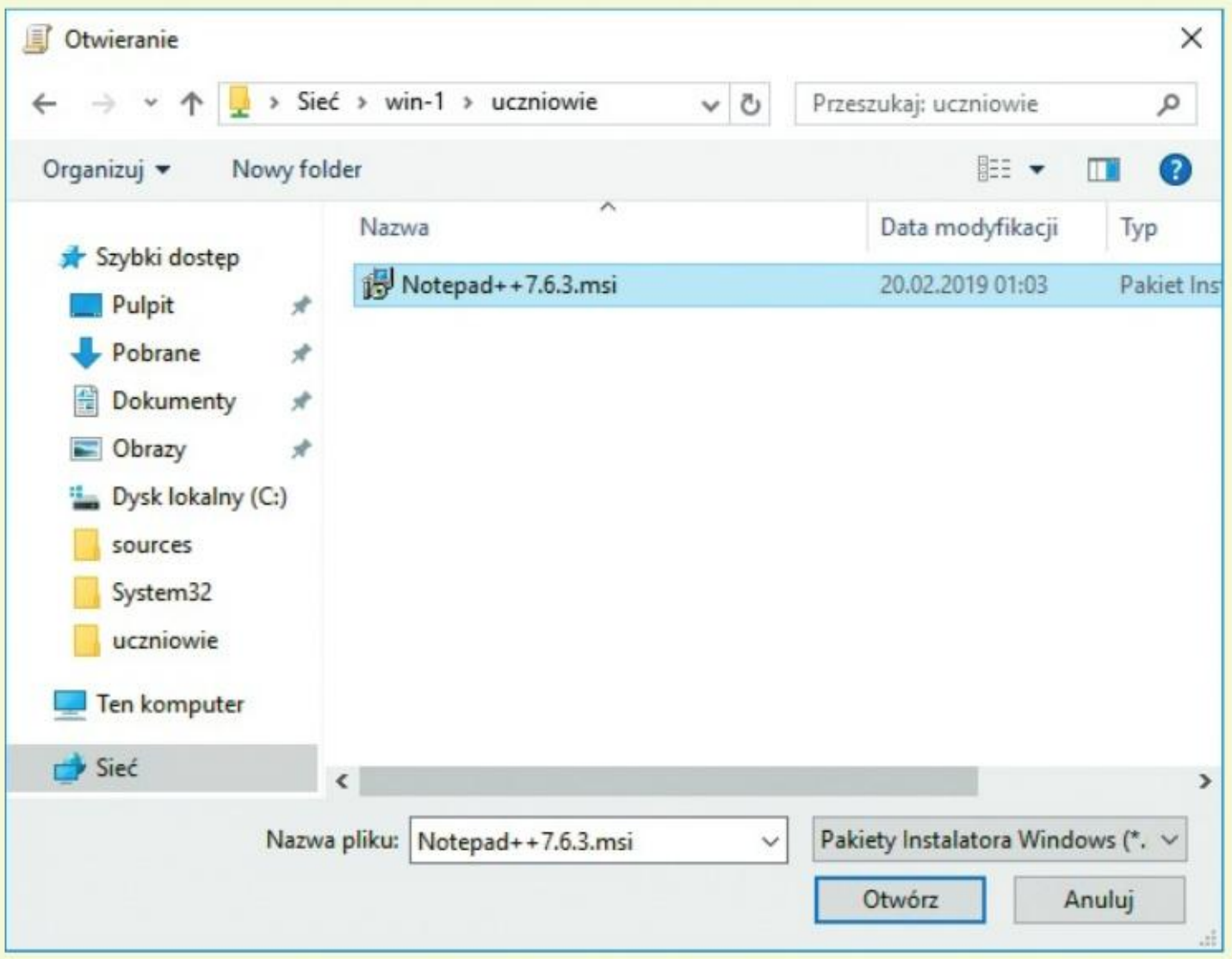


Rys. 43.14. **Tworzenie nowego obiektu zasad grupy**



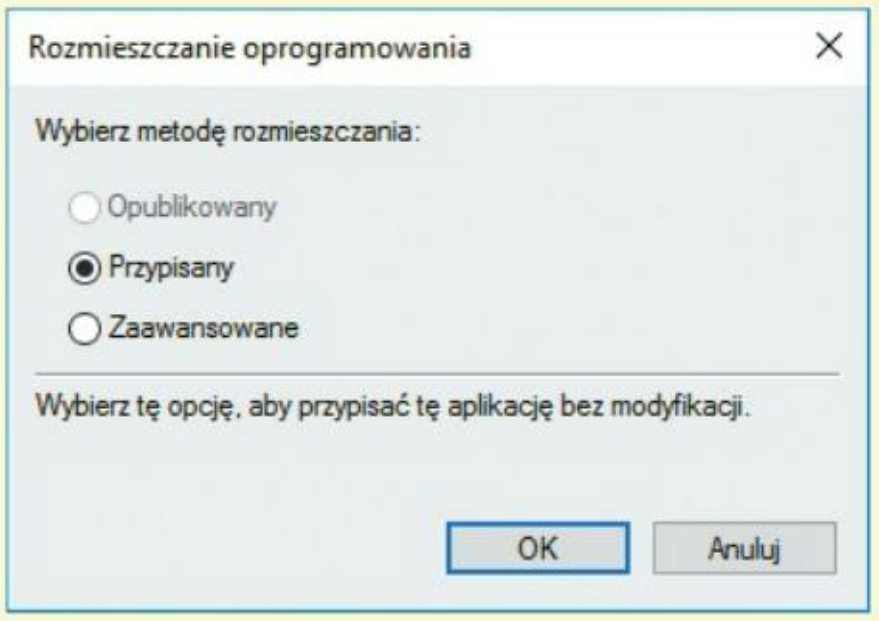
Rys. 43.15. **Edytowanie nowego obiektu zasad grupy**

9. Wskazać ścieżkę do pliku zawierającego pakiet instalacyjny oprogramowania na serwerze, np. **`\\win-1\uczniowie\Notepad++7.6.3.msi`**, i kliknąć przycisk **`Otwórz`** (rys. 43.16).



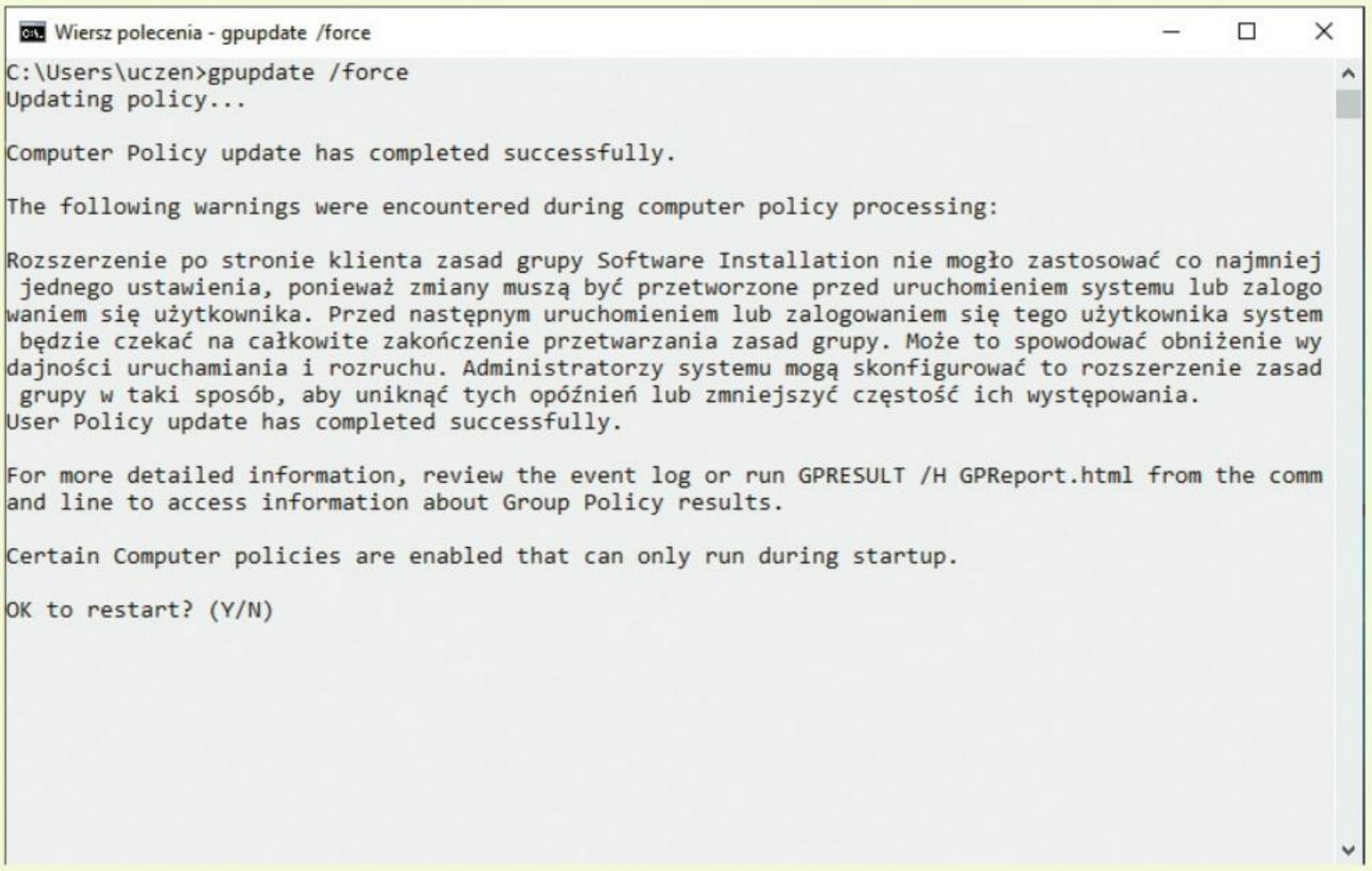
Rys. 43.16. **Wybór pakietu instalacyjnego**

10. W oknie **`Rozmieszczenie oprogramowania`** jako metodę rozmieszczenia wybrać opcję **`przypisany`** i kliknąć **`OK`** (rys. 43.17).
11. Powtórzyć operacje z punktów od 8. do 10. dla każdego programu, który ma być instalowany automatycznie.



Rys. 43.17. **Wybór metody**

12. Na stacji roboczej odświeżyć ustawienia obiektów zasad grupy poleceniem **`gpupdate /force`** i ponownie uruchomić komputer (rys. 43.18).
13. Podczas ponownego uruchamiania stacji roboczej oprogramowanie zostanie automatycznie zainstalowane na wszystkich komputerach, których konta zostały umieszczone w jednostce organizacyjnej *uczniowie*.
14. Sprawdzić poprawność instalacji programu.



Rys. 43.18. **Odświeżanie ustawień obiektów zasad grupy**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

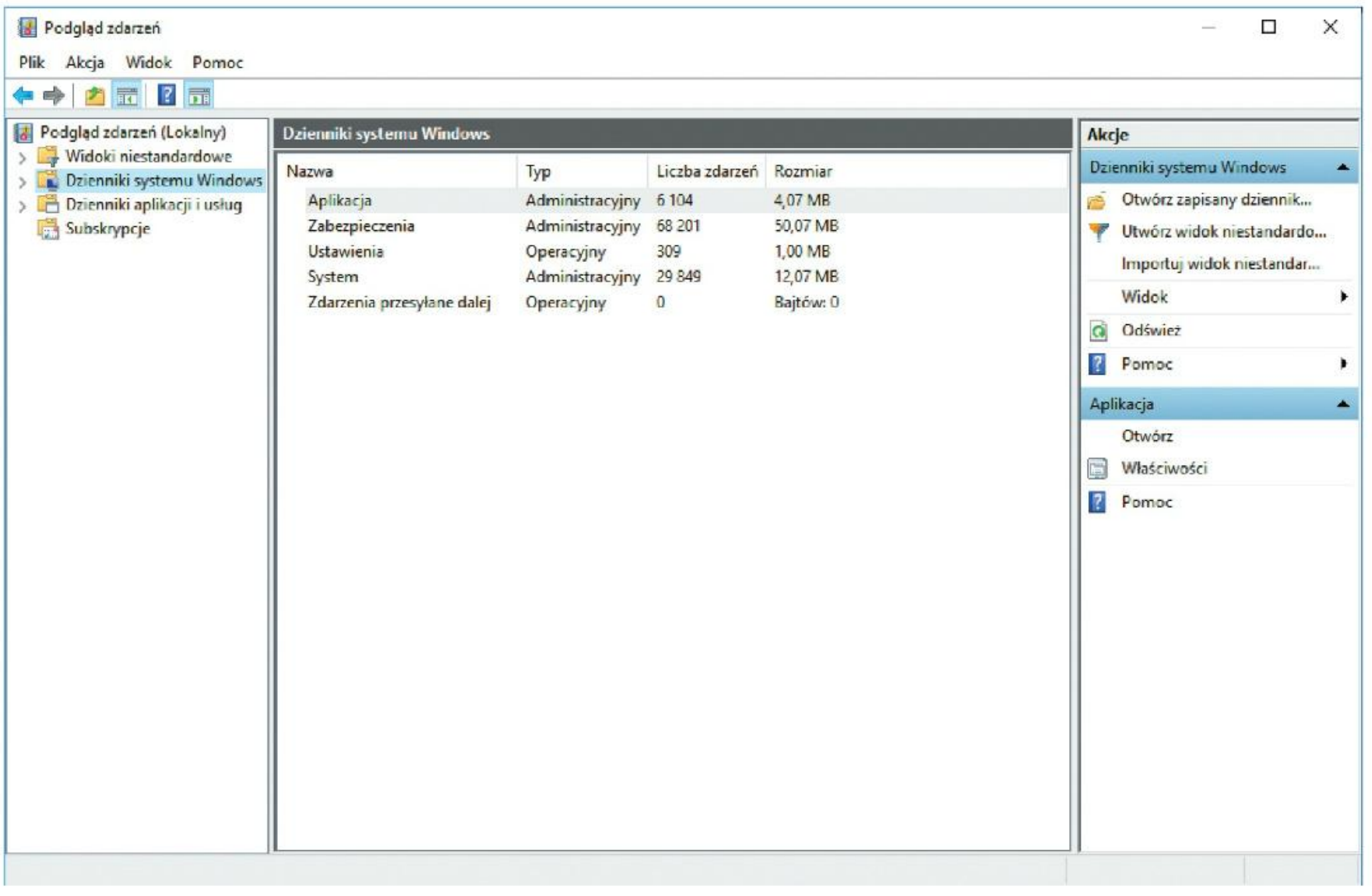
1. Wymuś w domenie używanie haseł o długości co najmniej pięciu znaków i ich zmianę co 30 dni.
2. Sporządź listę programów, które twoim zdaniem powinny być instalowane na stacjach roboczych za pomocą GPO.

44 Monitorowanie pracy serwera

ZAGADNIENIA

- **Funkcje dzienników zdarzeń**
- **Dane zapisane w poszczególnych dziennikach**
- **Przeglądanie dzienników zdarzeń**

Podczas eksploatacji system zapisuje informacje o zdarzeniach w **dziennikach zdarzeń**. Zawartość tych dzienników można odczytać za pomocą aplikacji **Podgląd zdarzeń**. W oknie aplikacji **Menedżer serwera** należy wybrać z menu polecenia **Narzędzia/Podgląd zdarzeń** i wykorzystać odpowiedni dziennik. W dziennikach są gromadzone zdarzenia krytyczne, komunikaty o błędach, ostrzeżenia, informacje oraz sukcesy i niepowodzenia inspekcji. W widoku okna (rys. 44.1) pokazano liczbę zarejestrowanych zdarzeń i rozmiar, jaki zajmują na dysku. Informacje można sortować i filtrować, np. ze względu na czas wystąpienia lub rodzaj informacji. W lewym panelu okna aplikacji można zauważyć dwie gałęzie: **Dzienniki systemu Windows** i **Dzienniki aplikacji i usług**.



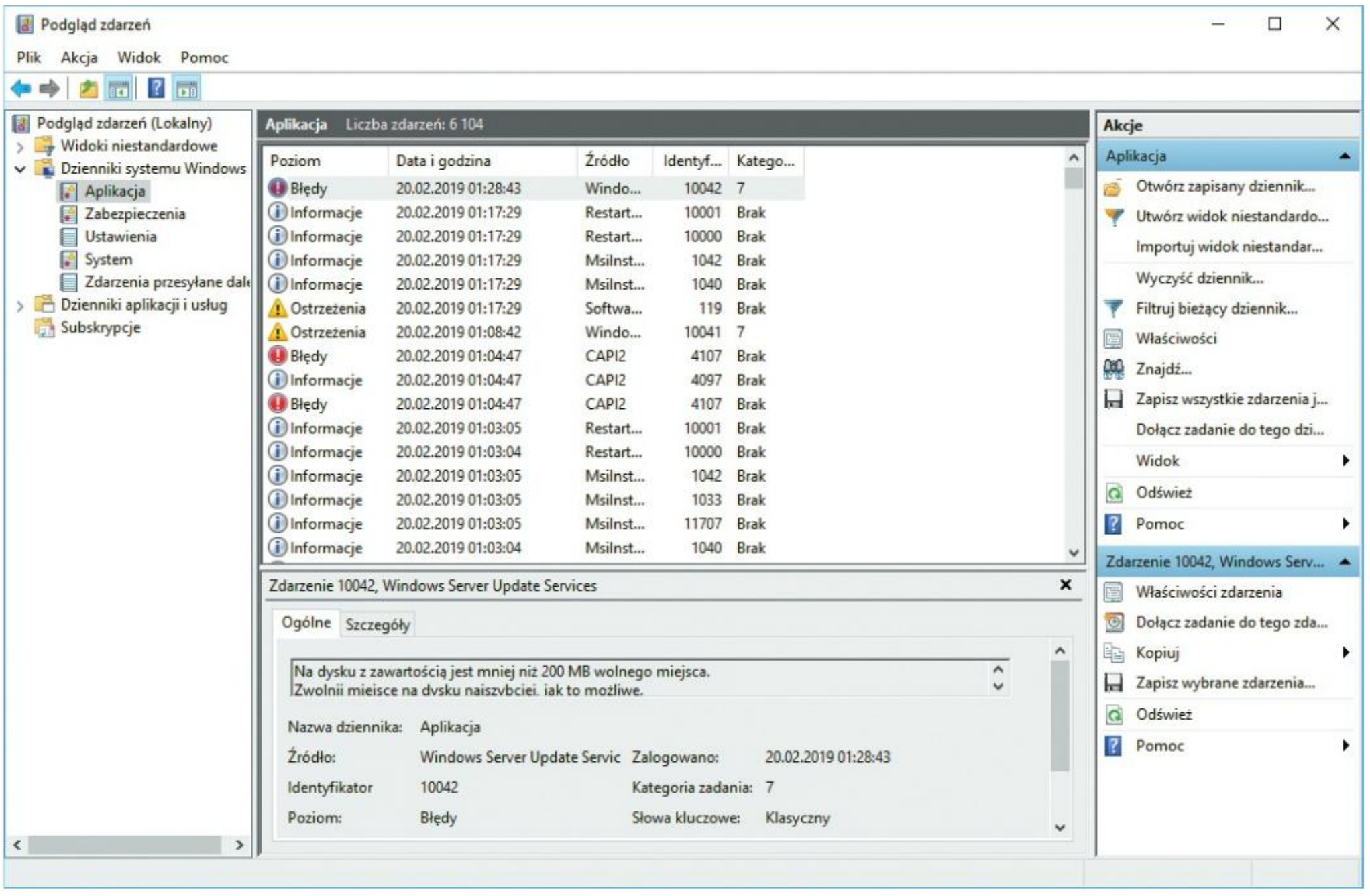
Rys. 44.1. Widok okna podglądu zdarzeń aplikacji `Dzienniki systemu Windows`

Informacje zebrane przez system w aplikacji **Dzienniki systemu Windows** są podzielone na następujące części:

- **Aplikacja** – zawiera zdarzenia zarejestrowane przez aplikacje lub programy;
- **Zabezpieczenia** – zawiera zdarzenia dotyczące zabezpieczeń, takie jak poprawne i niepoprawne próby logowania, i zdarzenia związane z użyciem zasobów, np. tworzenie, otwieranie lub usuwanie plików albo innych obiektów;
- **Ustawienia** – zawiera zdarzenia związane z instalacją aplikacji;
- **System** – zawiera zdarzenia zarejestrowane przez składniki systemu, np. niepowodzenia ładowania sterownika lub innego składnika systemu, i zdarzenia generowane przez usługi;
- **Zdarzenia przesyłane dalej** – rejestruje zdarzenia zebrane z komputerów zdalnych, jeżeli ta funkcja jest dostępna.

Administrator musi tworzyć i przeglądać logi systemowe (rys. 44.2), a ponadto ograniczyć do nich dostęp zwykłym użytkownikom. Zdarzenia należą do jednego z następujących typów:

- **Informacja** (ang. *information*) – to najczęściej komunikat o pomyślnie zakończonej operacji;
- **Ostrzeżenia** (ang. *warning*) – informuje o możliwych błędach lub niewłaściwej konfiguracji;
- **Błąd** (ang. *error*) – informacje o błędach, m.in. o nieuruchomieniu usługi;
- **Inspekcja sukcesów** (ang. *succes audit*) – zdarzenie zakończone sukcesem, np. logowanie;
- **Inspekcja niepowodzeń** (ang. *failure audit*) – zdarzenie zakończone niepowodzeniem.

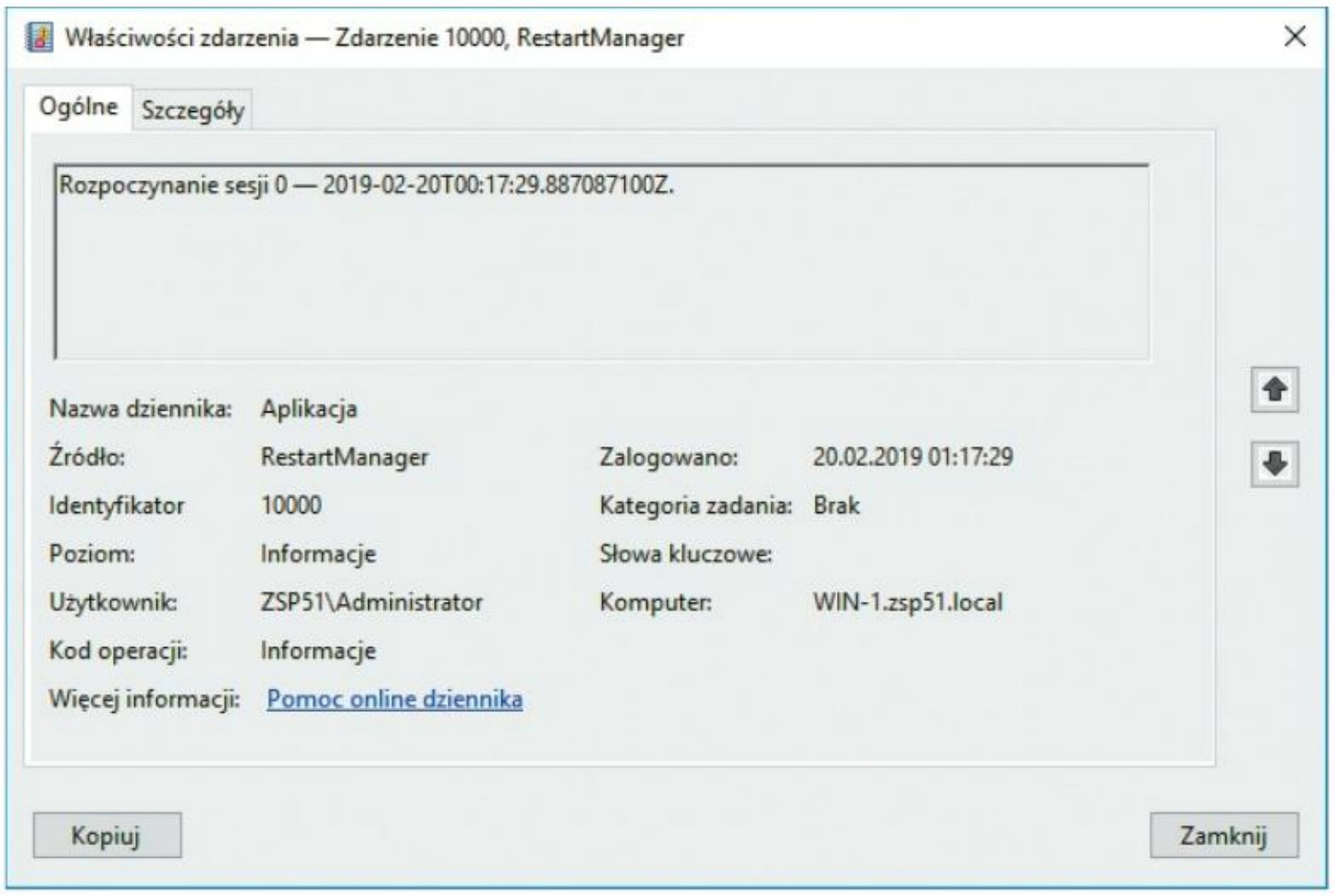


Rys. 44.2. Podgląd zdarzeń dziennika `Aplikacja`

W celu uzyskania informacji dotyczących zdarzenia należy dwukrotnie kliknąć zdarzenie. Pojawi się nowe okno **`Zdarzenie`** (rys. 44.3) przedstawiające szczegółowe informacje dotyczące wybranego zdarzenia.

W oknie znajduje się wiele informacji, m.in.:

- kiedy zaistniało zdarzenie;
- kto wywołał zdarzenie;
- typ zdarzenia;
- opis zdarzenia.



Rys. 44.3. Szczegóły dotyczące zdarzenia

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Uruchom narzędzie **`Podgląd zdarzeń`** na swoim komputerze. Wyszukaj w logach wszystkie typy zdarzeń: błąd, ostrzeżenie, informację. Zapoznaj się ze szczegółami wybranych zdarzeń.
2. Wyszukaj w dzienniku informacje o czasie ostatniego logowania do twojego komputera.
3. Wyszukaj w dzienniku informacje o czasie ostatniej instalacji programu.

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wyjaśnij różnicę między ostrzeżeniem a błędem.
2. Wymień typy dzienników w systemie Windows Server. Scharakteryzuj zawartość dwóch wybranych przez ciebie dzienników.

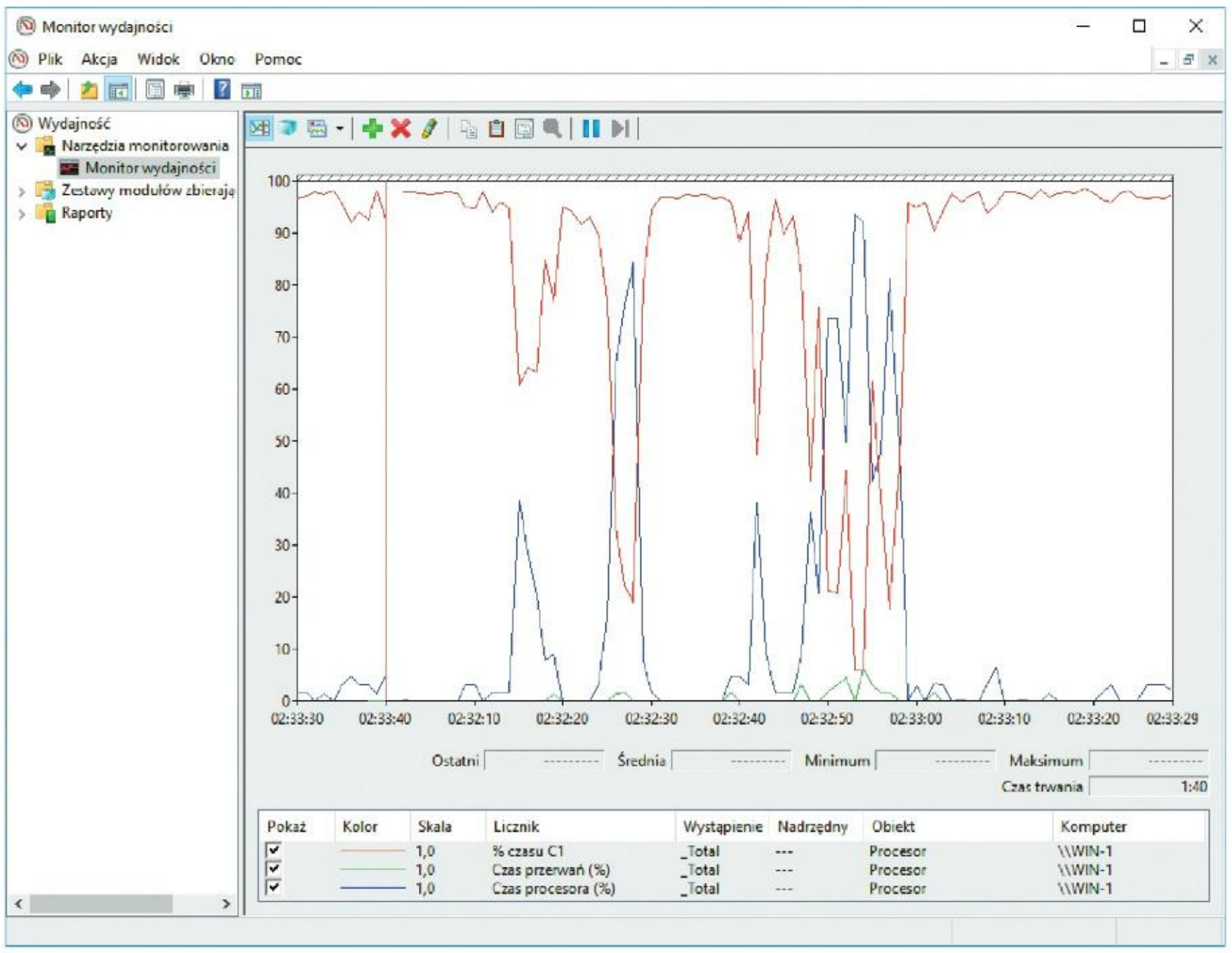
45 Monitorowanie wydajności serwera

ZAGADNIENIA

- **Funkcje monitora wydajności**
- **Zadania spełniane przez monitor niezawodności**
- **Przeglądanie i analizowanie raportów wydajności systemu**

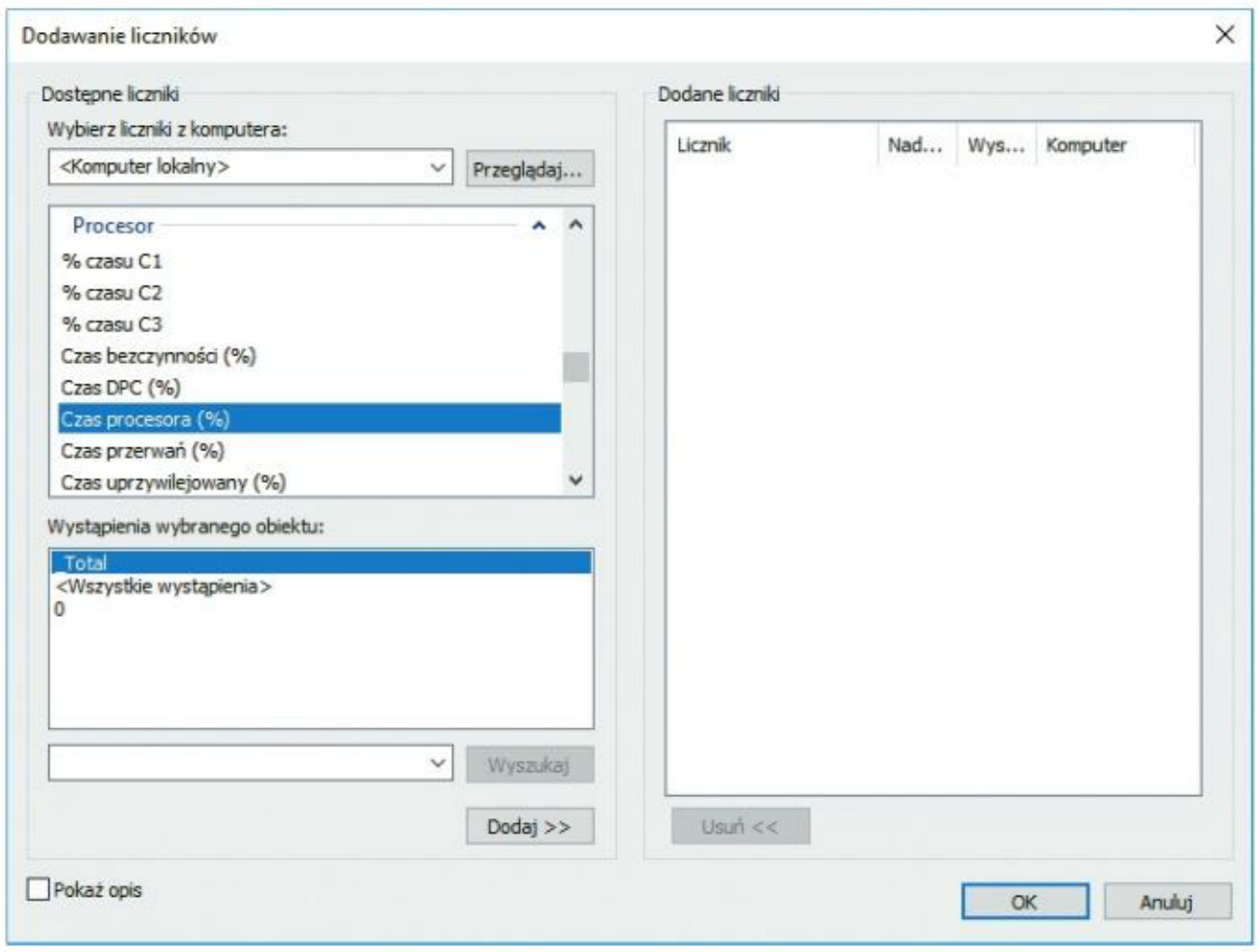
Narzędziem umożliwiającym ciągłe monitorowanie różnych parametrów pracy serwera jest aplikacja **`Monitor wydajności`** – dostępna w **`Menedżerze serwera`** w menu **`Narzędzia/Monitor wydajności`**.

Monitor wydajności jest narzędziem umożliwiającym monitorowanie na bieżąco parametrów pracy lokalnego lub zdalnego serwera. Dane w aplikacji mogą być przedstawiane w postaci wykresu (rys. 45.1).



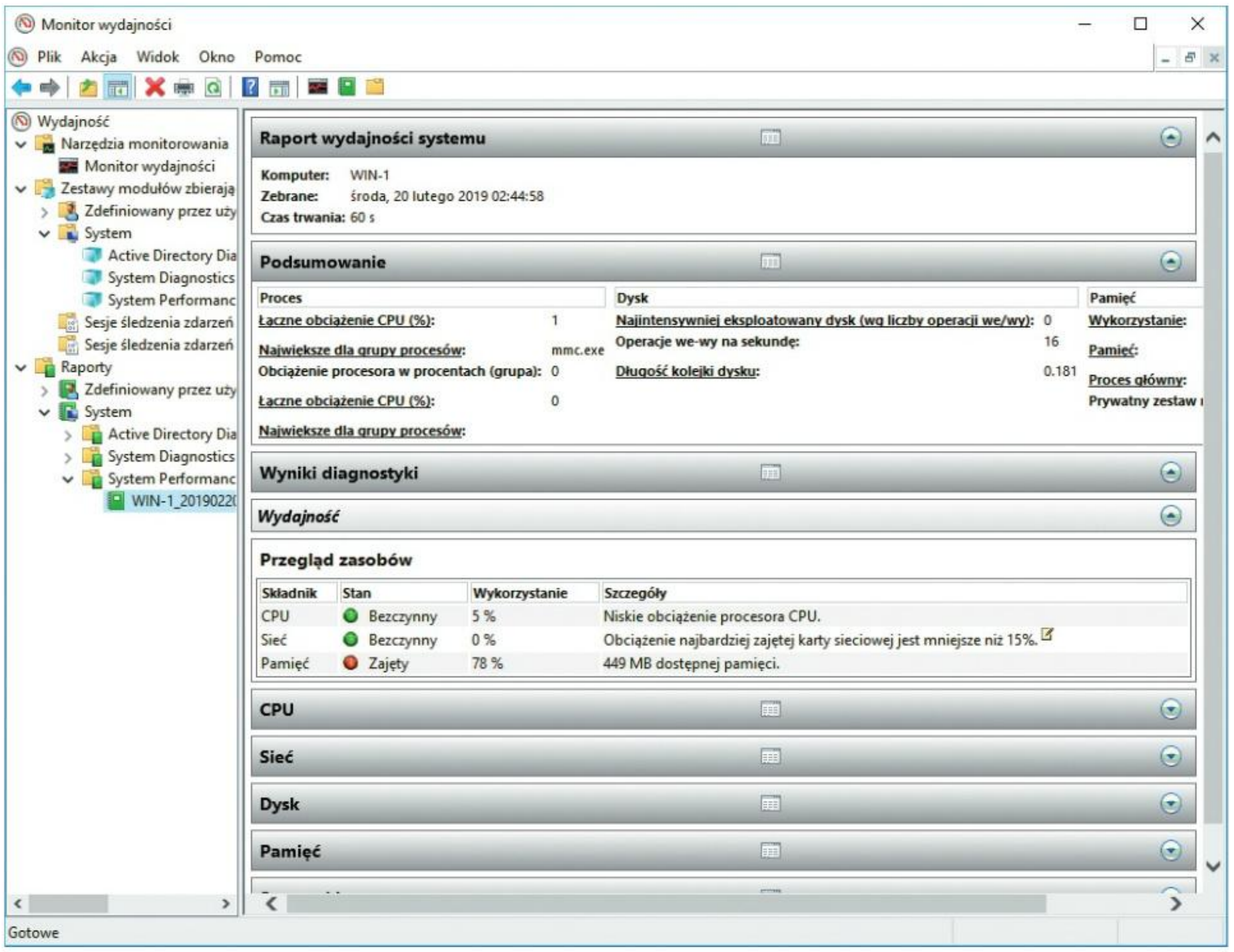
Rys. 45.1. Wykres wydajności systemu

Administrator ma możliwość definiowania liczników wykorzystywanych do monitorowania różnych funkcji systemu (rys. 45.2). Aby dodać nowy licznik, należy kliknąć ikonę dodawania (**+**) i wybrać licznik z dostępnej listy.



Rys. 45.2. Dodawanie licznika wydajności

W węźle **`Zestawy modułów zbierających dane`** są zdefiniowane gotowe zestawy liczników umożliwiających sporządzenie raportu wydajności serwera lub jego systemów. Użytkownik może zdefiniować również własne zestawy. Po uruchomieniu testu przez 60 sekund są gromadzone dane, a następnie jest generowany raport. Raporty mogą być przeglądane i analizowane w gałęzi **`Raporty`** (rys. 45.3).



Rys. 45.3. Przykładowy raport wydajności systemu

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

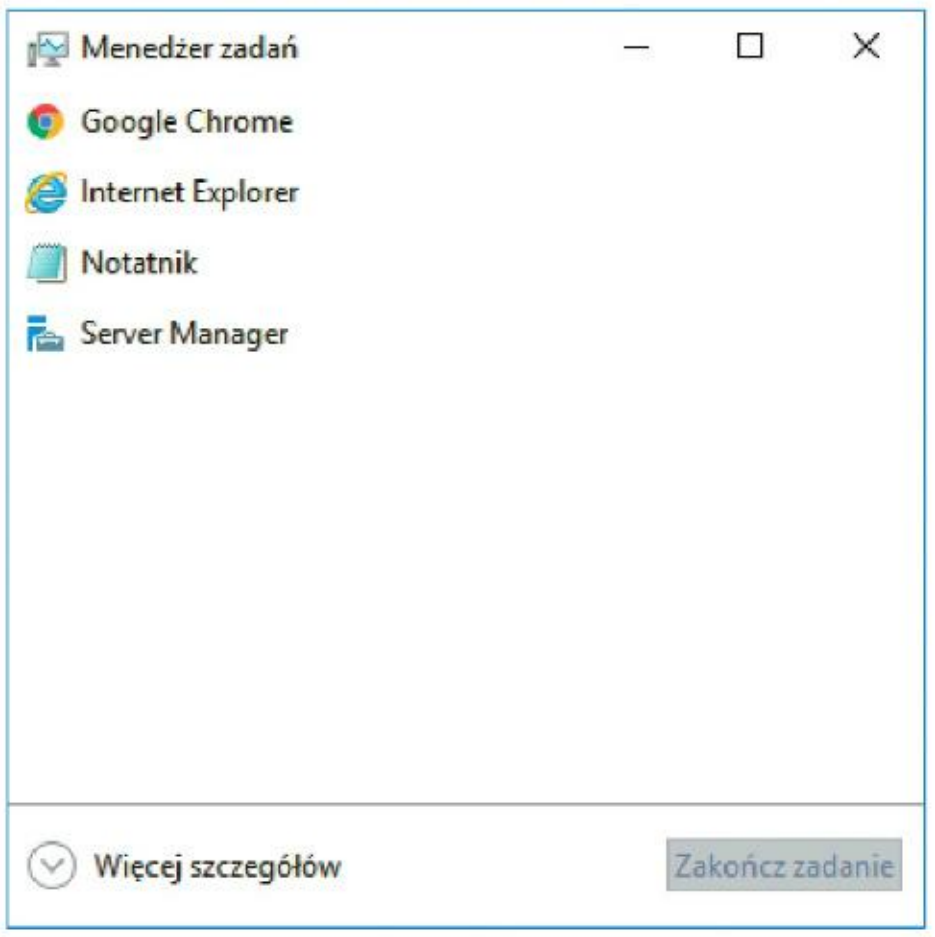
1. Sporządź dwa raporty wydajności serwera: jeden w czasie, gdy nie wykonuje on żadnych dodatkowych zadań, i drugi w czasie pracy z obciążeniem. Porównaj uzyskane wyniki.
2. W oknie aplikacji **`Monitor wydajności`** odczytaj ilość wykorzystywanej pamięci fizycznej. Uruchom kilka aplikacji i ponownie dokonaj odczytu. Porównaj uzyskane wyniki.
3. W oknie monitora wydajności dodaj licznik czasu pracy dysku fizycznego.
4. Sporządź listę parametrów serwera, które twoim zdaniem powinny być monitorowane.

46 Narzędzia do diagnostyki serwera

ZAGADNIENIA

- **Narzędzia służące do diagnostyki serwera i sposób ich uruchomienia**

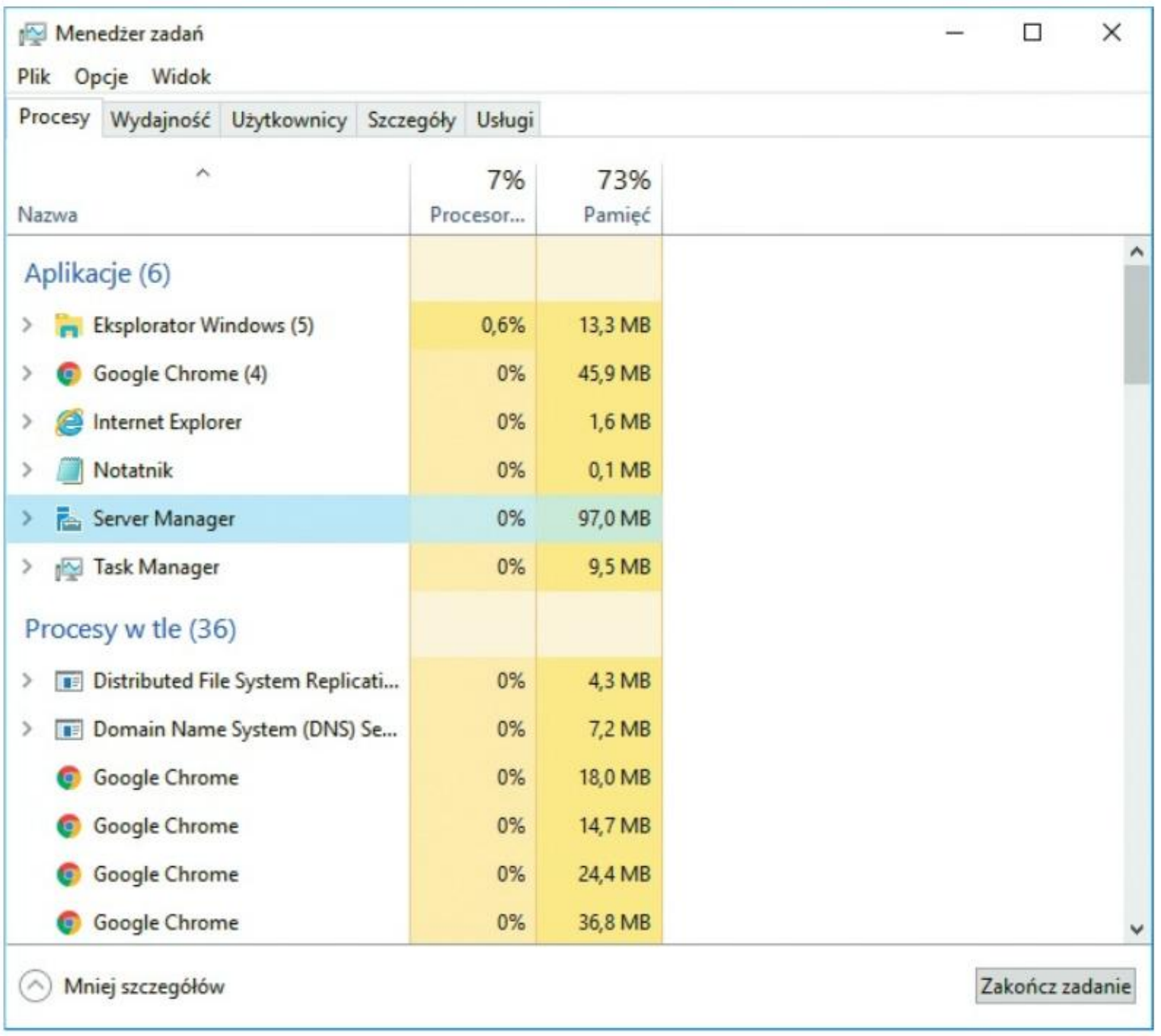
Procesy w systemie operacyjnym są uruchamiane przez sam system operacyjny i jego usługi, a także przez aplikacje uruchamiane przez użytkowników. Każdy proces wykorzystuje pewne **zasoby komputera**, np. pamięć i czas procesora. Podstawowym narzędziem do zarządzania procesami i aplikacjami jest **Menedżer zadań**. Aby otworzyć okno **Menedżera zadań**, należy wcisnąć klawisze [Ctrl] + [Alt] + [Del] i wybrać polecenie **Menedżer zadań**. Domyślnie jest wyświetlane okno **Aplikacje** (ang. *Applications*) zawierające tylko podstawowe informacje o uruchomionych aplikacjach (rys. 46.1). W oknie znajduje się lista uruchomionych aplikacji. Aplikację można zakończyć przez jej zaznaczenie i następnie wybranie przycisku **Zakończ zadanie** (rys. 46.1).



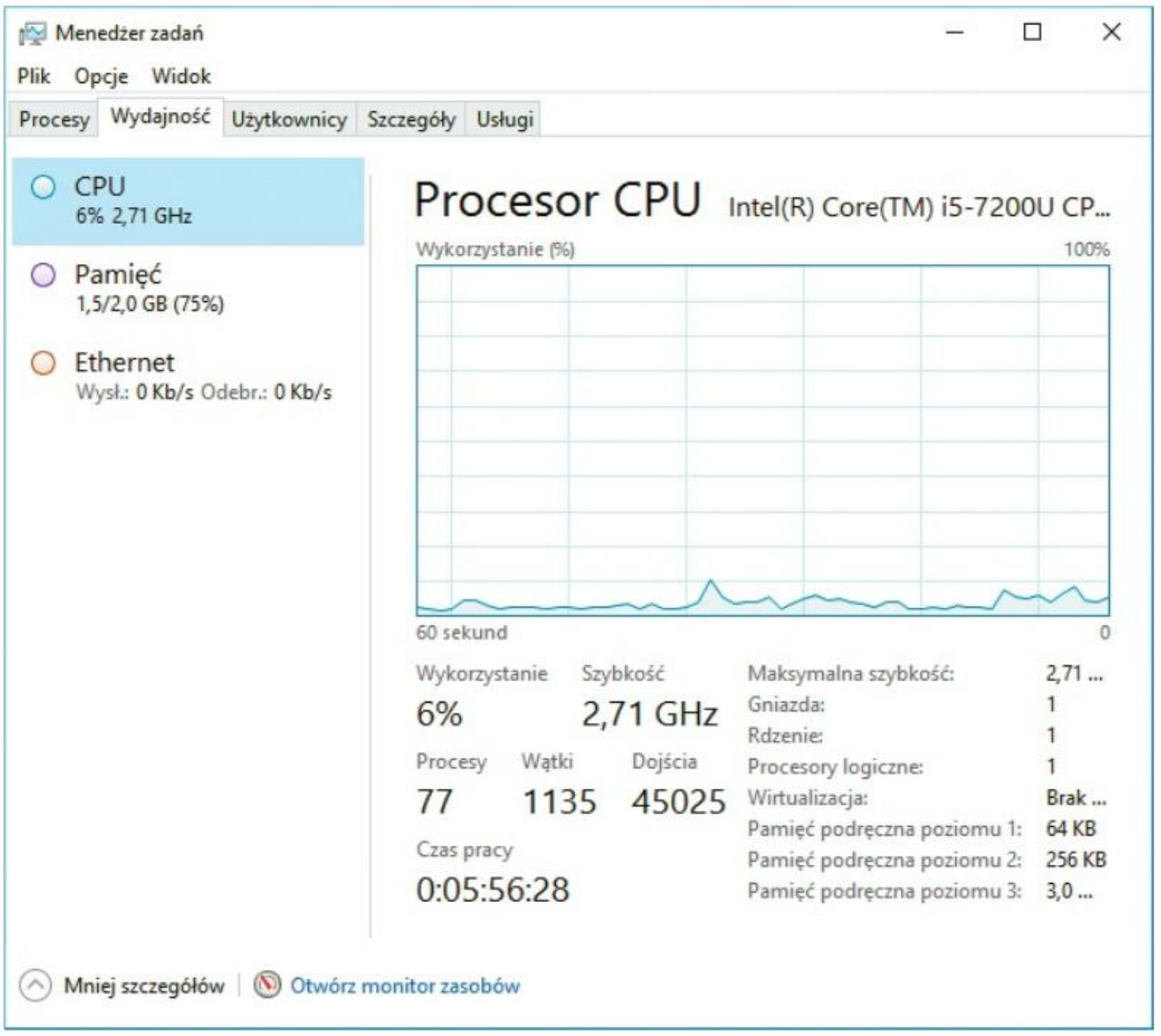
Rys. 46.1. **Wykaz aplikacji**

Po kliknięciu odnośnika **Więcej szczegółów** jest wyświetlane okno zawierające zakładki:

- **Procesy** (ang. *processes*) – pokazuje uruchomione procesy i (zależnie od wybranych kolumn) umożliwia przeglądanie procesów i analizę ich różnych parametrów. Domyślnie są wyświetlane (rys. 46.2):
  - nazwa obrazu (pliku);
  - procentowe wykorzystanie procesora (CPU);
  - użycie pamięci;
- **Wydajność** (ang. *performance*) – przedstawione wykresy mogą pokazywać procentowe wykorzystanie procesora, pamięci lub sieci (rys. 46.3);

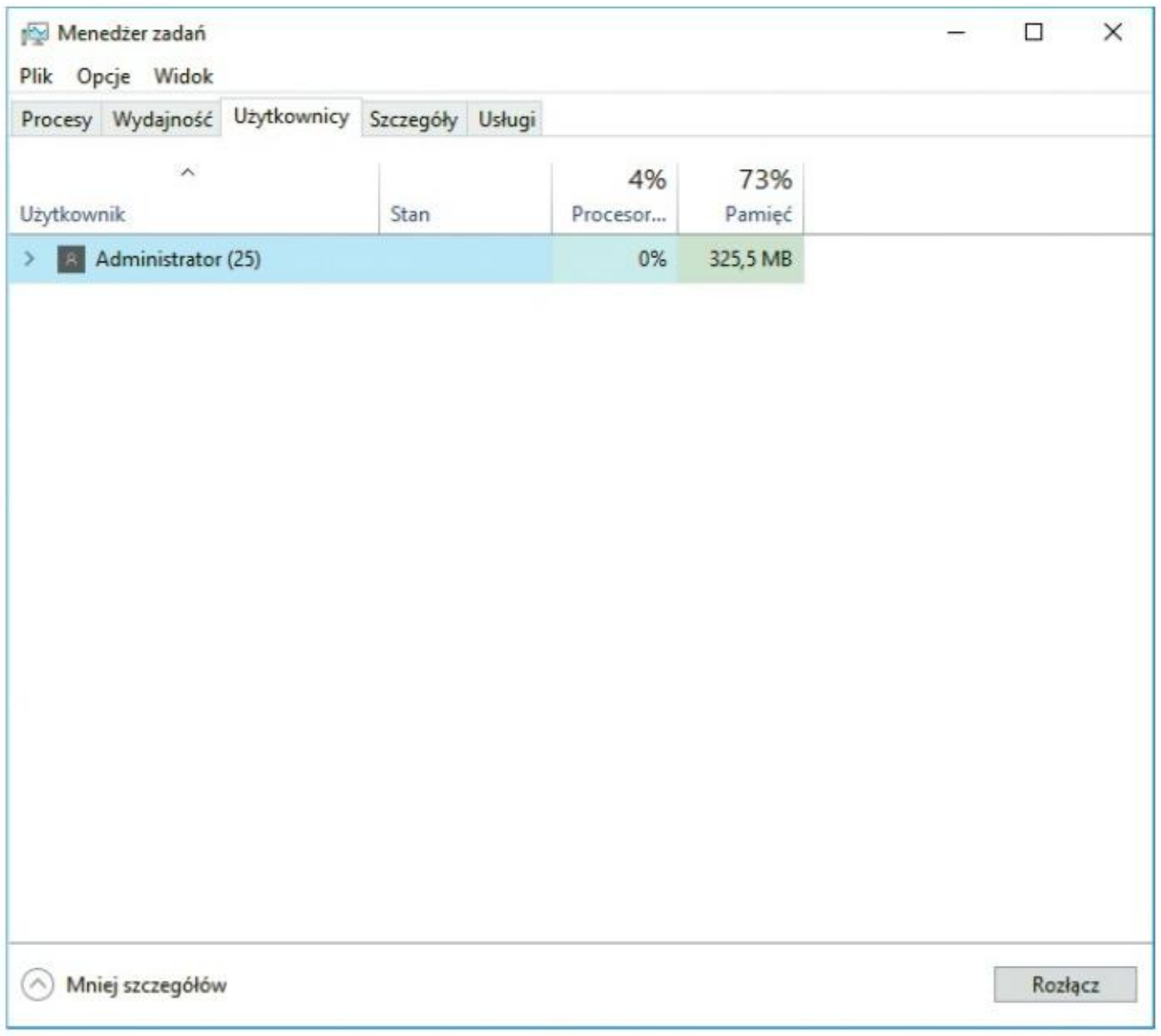


Rys. 46.2. Wykaz procesów uruchomionych w systemie



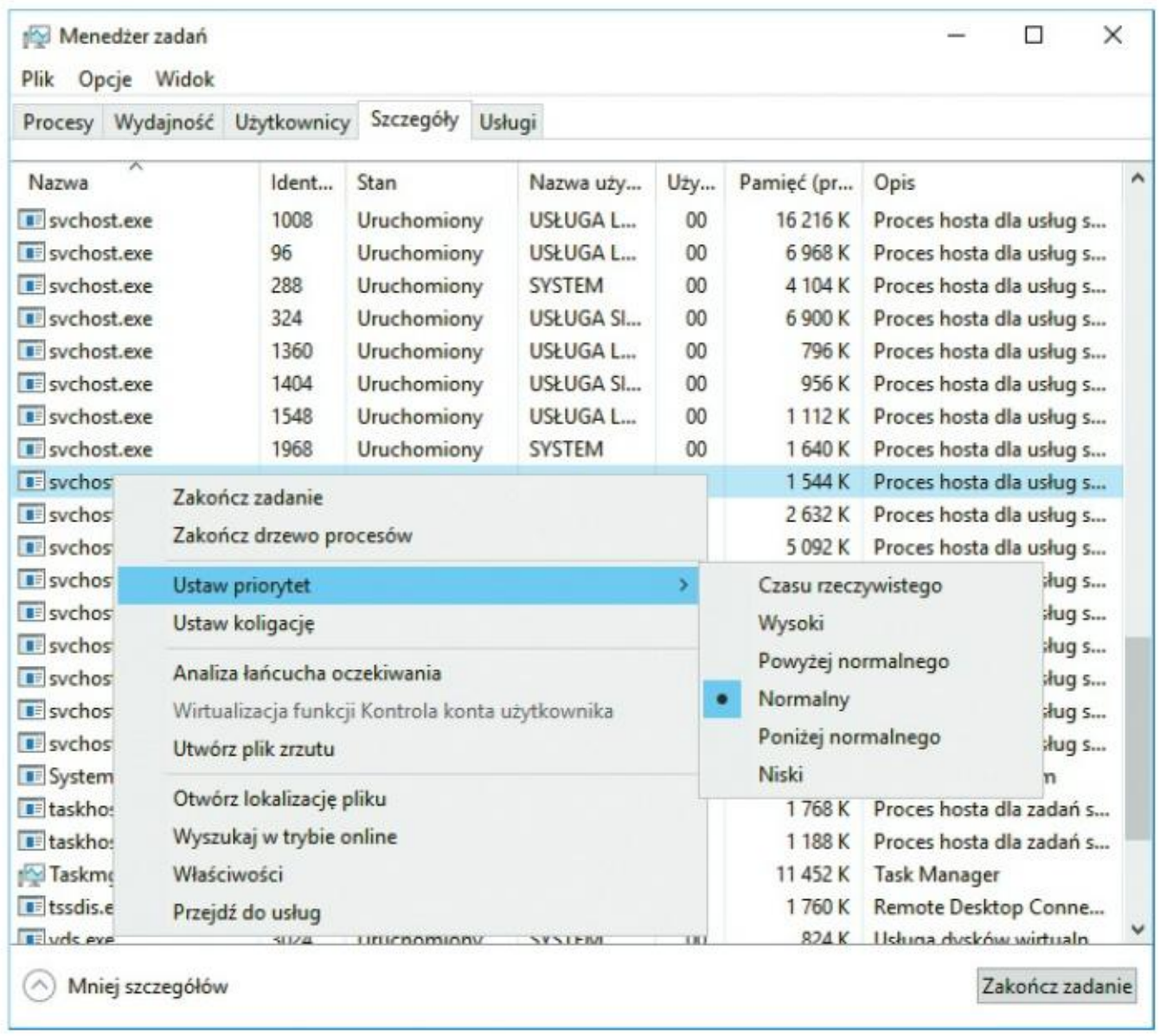
Rys. 46.3. Zakładka `Wydajność` menedżera zadań

- **Użytkownicy** (ang. *users*) – przedstawia użytkowników zalogowanych w systemie. Umożliwia zerwanie połączenia z użytkownikiem (rys. 46.4);



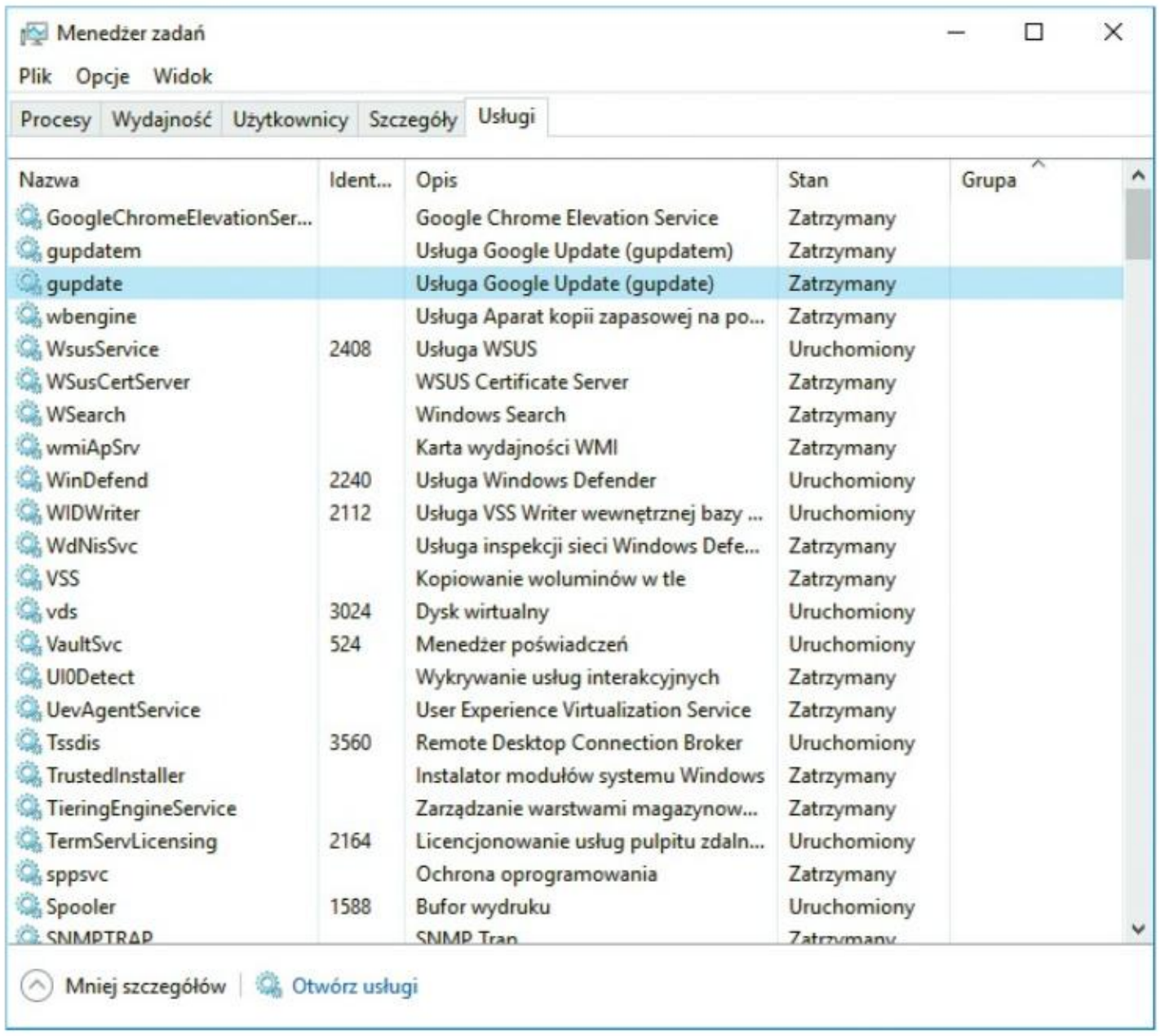
Rys. 46.4. Zakładka `Użytkownicy` menedżera zadań

- **Szczegóły** (ang. *details*) – wyświetla szczegóły dotyczące uruchomionych procesów i usług oraz ich identyfikatory (PID), opis i stan (rys. 46.5). Można zmieniać priorytety poszczególnych procesów przez kliknięcie prawym przyciskiem myszy danego procesu i wybranie menu **`Ustaw priorytet`**.



Rys. 46.5. Szczegółowe informacje o procesach i usługach uruchomionych w systemie

- **Usługi** (ang. *services*) – wyświetla listę udostępnianych na serwerze usług oraz identyfikatory (PID), opis i stan (rys. 46.6).



Rys. 46.6. Wykaz usług uruchomionych w systemie

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wyświetl listę użytkowników zalogowanych do twojego komputera. Skorzystaj z narzędzia **`Menedżer zadań`** i odłącz wybranego użytkownika od serwera.
2. W oknie programu **`Menedżer zadań`** oblicz liczbę usług w stanie uruchomienia. Wybierz jedną z usług i wyszukaj w internecie informacje na temat roli, jaką odgrywa.

47 Metody ataków sieciowych

ZAGADNIENIA

Rodzaje ataków na sieć komputerową **Fazy ataku na sieć** **Wybrane ataki pasywne i aktywne** **Zapobieganie atakom sieciowym**

W sieciach komputerowych są przesyłane niekiedy dane o bardzo dużej wartości dla użytkowników i przedsiębiorstw. Bardzo duże znaczenie ma odpowiednie zabezpieczenie danych i urządzeń przed dostępem osób nieupoważnionych. Techniki włamań do sieci są zróżnicowane: od bardzo prostych do niezwykle wyrafinowanych. Można je ogólnie podzielić na dwie kategorie: ataki **pasywne** i ataki **aktywne**.

Ataki pasywne (ang. *passive attacks*) polegają na śledzeniu i podsłuchiwaniu w celu pozyskania informacji lub analizy ruchu sieciowego. Z reguły ataki pasywne są pierwszym krokiem do przeprowadzenia ataku aktywnego i mają za zadanie zebranie jak najwięcej informacji o celu ataku. Ponieważ ataki pasywne nie dokonują zmian danych, są właściwie nie do wykrycia. W postępowaniu z nimi należy raczej skupić się na zapobieganiu, a nie wykrywaniu.

Ataki aktywne (ang. *active attacks*) polegają na modyfikacji strumienia danych lub tworzeniu danych o zmienionej strukturze. Istnieje wiele typów ataków aktywnych.

Przyjmuje się, że atak składa się z takich faz, jak: **przygotowanie ataku**, **przeprowadzenie ataku**, **zacieranie śladów** i/lub **pozostawienie otwartej drogi do ponownego włamania**. Przeprowadzenie ataku na sieć jest na ogół poprzedzone zbadaniem środowiska obranego celu. Najczęściej powodzenie ataku jest uwarunkowane poziomem przygotowania napastnika i ilością zgromadzonych przez niego informacji. Przygotowanie do włamania rozpoczyna się zdobyciem niezbędnych informacji, kończy natomiast na uzyskaniu potrzebnych programów do przeprowadzenia ataku. Nie wszystkie ataki są związane z wykorzystaniem sprzętu komputerowego, w niektórych przypadkach łatwiejszym celem są użytkownicy sieci.

47.1. Przykłady ataków pasywnych

Social engineering to sposób na pozyskanie informacji istotnych z punktu widzenia bezpieczeństwa, takich jak: hasła, loginy, procedury bezpieczeństwa. *Social engineering* polega na manipulowaniu ludzką lekkomyślnością w celu osiągnięcia korzyści. Wiele osób nie przywiązuje wagi do zagadnień bezpieczeństwa, przez co narażają siebie i swoich pracodawców na poważne niebezpieczeństwo. Przykładami metod pozyskiwania danych są:

- fałszywe e-maile, w których pod pretekstem awarii systemu i powstałych w ten sposób błędów nadawca prosi o ponowne podanie loginu i hasła;
- podglądanie wpisywanych z klawiatury loginów i haseł;
- telefony od osób, które pod pretekstem awarii proszą o wpisanie kilku poleceń w konsoli tekstowej;
- przeglądanie wyrzuconej dokumentacji, z której można pozyskać prywatne informacje.

Najlepszą metodą obrony jest szkolenie personelu pod kątem stosowania procedur bezpieczeństwa.

Każdy użytkownik sieci komputerowej ma swoje konto i hasło, które umożliwia identyfikowanie i przydzielanie uprawnień do zasobów, dlatego jest narażony na **ataki na hasła**. Założenie konta wiąże się z przypisaniem hasła początkowego, wygenerowanego automatycznie lub przez administratora. Użytkownik powinien je niezwłocznie zmienić po pierwszym zalogowaniu. Systemy mają zazwyczaj domyślnie ustawiony poziom złożoności hasła, które użytkownik powinien wprowadzić. W bezpiecznych hasłach musi wystąpić kombinacja cyfr, liter małych i dużych oraz znaków specjalnych o odpowiedniej długości. Atak na hasło może być przeprowadzony metodą **siłową** lub **słownikową**. W **metodzie siłowej** (ang. *brute force*) są sprawdzane wszystkie możliwe kombinacje znaków. Daje ona pewność znalezienia hasła, ale problemem jest długi czas (zwłaszcza w przypadku bezpiecznych haseł) potrzebny do złamania hasła. W **metodzie słownikowej** (ang. *dictionary attack*) wykorzystuje się zbiór potencjalnych haseł, które są sprawdzane po kolei. Programy do łamania haseł mogą w ciągu sekundy testować po kilkaset tysięcy haseł. Jedną z metod zwiększenia odporności systemu na ataki siłowe i słownikowe jest blokowanie na określony czas możliwości wprowadzenia kolejnego hasła. Przykładowo, jeżeli użytkownik wprowadzi trzykrotnie nieprawidłowe hasło, to system zostanie zablokowany na 15 min. Jest to rozwiązanie mało uciążliwe dla człowieka, ale może skutecznie zabezpieczyć system przed programem przeprowadzającym atak.

Skanowanie sieci jest czynnością wykonaną przez włamywacza przed dokonaniem właściwego ataku. Jego celem jest zebranie jak największej ilości informacji na temat usług działających w sieci, wersji systemu operacyjnego i struktury sieci. Skanowanie może dotyczyć również pojedynczego komputera lub serwera, aby uzyskać informacje na temat otwartych portów, wersji oprogramowania itp.

Istnieje wiele metod skanowania. Niektóre z nich to:

- **TCP connect scanning** – polega na nawiązywaniu połączenia z wybranymi portami – jeżeli połączenie zostanie nawiązane, oznacza to, że port jest otwarty. Wadą metody jest łatwy sposób jej wykrycia, ponieważ pozostawia ślady w logach na serwerze docelowym;
- **TCP SYN scanning** – w tej metodzie nawiązywanie połączenia jest przerywane przed jego zakończeniem; nie dochodzi do pełnego połączenia, brak wpisów w logach serwera i trudniej wykryć próbę skanowania;
- **ICMP echo** – pozwala ustalić za pomocą polecenia **`ping`** adresy IP, pod którymi pracują hosty.

Nasłuchiwanie (ang. *sniffing*) polega na przechwytywaniu pakietów przesyłanych w sieci. W sieci lokalnej każda maszyna ma swój unikatowy adres MAC i odbiera tylko ramki kierowane na ten adres i adres rozgłoszeniowy. Ustawienie karty sieciowej w specjalnym **trybie diagnostycznym** (ang. *promiscuous mode*) pozwala odbierać wszystkie ramki przesyłane w danym segmencie sieci. Aplikacje wykorzystywane do tego typu zadań są nazywane **snifferami**. Zabezpieczeniem sieci jest **szyfrowanie danych** – nawet jeżeli dane zostaną przechwycone, to ich odczytanie bez klucza będzie niemożliwe.

47.2. Przykłady ataków aktywnych

Spoofing polega na podszywaniu się pod inne komputery upoważnione do nawiązywania połączeń. Istnieje wiele metod podszywania się, z których najpopularniejsze to DNS-spoofing i IP-spoofing. **DNS-spoofing** polega na ataku na serwer DNS, w którym znajduje się baza danych na temat adresów IP dla poszczególnych hostów. Modyfikacja wpisów w systemie DNS może spowodować, że klient zamiast do hosta docelowego będzie przekierowany do innego komputera. **IP-spoofing** opiera się na fałszowaniu źródłowego adresu IP w wysyłanym przez komputer

pakiecie sieciowym. Dzięki temu napastnik może podszyć się pod legalnego użytkownika sieci i wykorzystać uprawnienia posiadane przez atakowany adres.

Przechwycenie sesji (ang. *hijacking*) polega na przechwyceniu sesji w protokole TCP. Atakujący zrywa połączenie między serwerem i klientem, aby jako autoryzowany użytkownik mógł kontynuować komunikację (bez konieczności logowania).

Koń trojański (ang. *trojan horse*) to program, który podszywa się pod aplikacje użytkownika i dodatkowo implementuje niepożądane, ukryte przed użytkownikiem funkcje, np. wysyłanie do serwera napastnika informacji o kontach i hasłach, umożliwienie zalogowania się na komputerze z prawami administratora lub uruchomienie innych programów.

Ataki typu DOS (ang. *Denial of Service*) mają na celu uniemożliwienie legalnym użytkownikom dostępu do wybranych lub wszystkich usług. Mogą być wykonywane zarówno zdalnie, jak i lokalnie. Ataki typu DOS najczęściej są wykorzystywane w celu:

- rewanżu na użytkownikach sytemu lub administratorach;
- uzyskania korzyści finansowych przez nieuczciwych konkurentów;
- nieuzasadnionej, złośliwej rozrywki.

Przykładami ataków typu DOS są:

- **ataki typu SYN Flood** – polegają na nawiązywaniu dużej liczby połączeń TCP z komputerem, tak aby wyczerpać jego zasoby. Atakowany komputer po wyczerpaniu zasobów nie może już przyjmować nowych połączeń, spowalnia pracę lub może się zawiesić;
- **atak Ping of Death** – polega na wysłaniu bardzo dużej liczby pakietów testowych za pomocą polecenia **ping** z ustawionym rozmiarem pakietu testowego przekraczającego dopuszczalny zakres. Atakowany komputer musi odpowiadać na żądania programu **`ping`**, co może spowolnić jego działanie lub zupełnie je uniemożliwić;
- **atak smerfów** (ang. *smurf attack*) – jego działanie opiera się na generowaniu dużej liczby poleceń **ping**, kierowanych na adresy rozgłoszeniowe z adresami źródłowymi zamienionymi na adres ofiary. W efekcie tego ataku wszystkie komputery, które odbiorą żądanie, wysyłają odpowiedzi na **ping** pod adres ofiary, której komputer może ulec przeciążeniu;
- **e-mail bombing** – polega na wysłaniu dużej liczby wiadomości z nieistotnymi treściami, adresowanych do skrzynki osoby poszkodowanej. Użytkownik jest zmuszony ponieść dodatkowe koszty połączenia i poświęcić czas, aby pozbyć się niechcianych listów. Niekiedy dochodzi do blokowania skrzynki w wyniku jej przepełnienia;
- **e-mail spamming** – polega na wysyłaniu listów do wszystkich osób korzystających z określonego serwera. Metoda z reguły jest wykorzystywana do rozsyłania reklam, nie zaś do czynienia szkody;
- **disable accounts** – systemy blokują funkcjonowanie konta po określonej liczbie niewłaściwych logowań bądź narzucają przerwy między kolejnymi próbami. Wykonanie kilku nieudanych prób logowania na konto ofiary powoduje tymczasowe zablokowanie korzystania z serwera;
- **ataki przepełnienia bufora** (ang. *buffer overflow*) – wykorzystują błąd programistyczny polegający na zapisaniu do wyznaczonego obszaru pamięci (bufora) większej ilości danych, niż zarezerwował na ten cel programista. Powoduje to nadpisanie danych znajdujących się w pamięci bezpośrednio za buforem, a w rezultacie błędne działanie programu. W szczególnym przypadku może dojść do nadpisania struktur kontrolnych programu w taki sposób, by zaczął on wykonywać operacje określone przez atakującego;
- **metoda tylnych drzwi** (ang. *backdoor*) – polega na uzyskaniu dostępu do systemu operacyjnego bez procedury autoryzacji. Z tego ataku można skorzystać w momencie, kiedy wcześniej zainstalujemy odpowiedni program, taki jak koń trojański. Napastnik, który ma uprawnienia administratora, instaluje odpowiednie oprogramowanie umożliwiające mu ponowny dostęp

do systemu. Jedną z najprostszych metod jest stworzenie nowego użytkownika i nadanie mu prawa administratora lub wykorzystanie istniejącego użytkownika, nadanie mu praw administratora i uzyskiwanie dostępu przez jego konto.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wybierz hasło dla swojego konta w sieci szkolnej spełniające wymagania bezpieczeństwa.
2. Opracuj listę zaleceń, np. dla koleżanek / kolegów z klasy o profilu nieinformatycznym, dotyczących zasad bezpiecznego posługiwania się siecią komputerową.
3. Wyszukaj w internecie informacje na temat ataków na hasła metodą *brute force* i słownikową oraz różnicy między nimi.
4. Uczniowie technikum informatycznego powinni mieć świadomość zagrożeń wynikających ze stosowania „słabych" haseł. Zaplanuj zasady dotyczące polityki haseł w twojej szkole.
5. Przygotuj dla uczniów instrukcję na temat tego, jak zbudować bezpieczne hasło (zgodne z przyjętą polityką).

48 Metody zabezpieczania zasobów sieciowych

ZAGADNIENIA

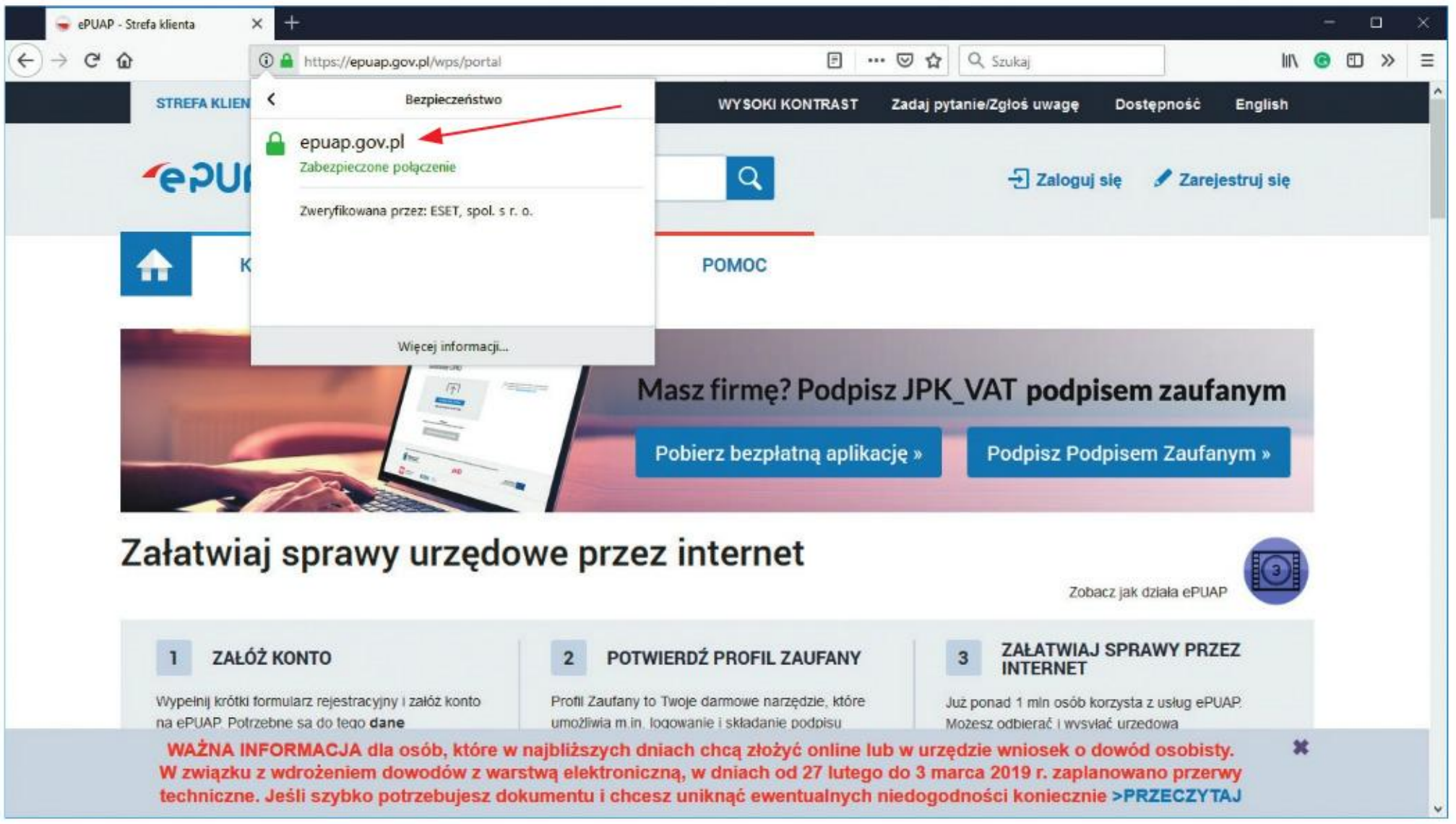
Zagrożenia podczas pracy w sieci **Netykieta dla użytkownika sieci** **Zweryfikowanie prawdziwości strony internetowej** **Włączanie firewalla na routerze** **Korzystanie z list kontroli dostępu ACL na routerze** **Funkcja polityki bezpieczeństwa** **Programy i urządzenia pomagające administratorowi zabezpieczyć sieć przed zagrożeniami** **Działanie systemów IDS/IPS** **Działanie wirtualnej sieci prywatnej VPN** **Skonfigurowanie sieci VPN na urządzeniu sprzętowym** **Zarządzanie zasobami serwera plików**

Korzystanie z internetu dla wielu ludzi stało się codzienną czynnością. Czasami powoduje to narażanie się na niekorzystne czynniki. Głównym z nich jest uzależnienie się od internetu. Wielu ludzi, zwłaszcza młodych, przestaje dostrzegać różnicę między światem realnym a wirtualnym. Zdarza się, że internauta ma problemy z bezpośrednimi kontaktami z ludźmi. Młodzi ludzie często poświęcają cały swój czas na surfowanie po sieci, gry online lub pogawędki, co wiąże się z zaniedbywaniem obowiązków i innych form życia społecznego. W sieci wolność słowa jest nieograniczona, co jest niewątpliwie wielką pokusą, ale często bywa ona złudna.

Wprawdzie istnieje **netykieta**, czyli zbiór zasad zachowania w sieci, ale wielu ludzi jej nie przestrzega. Ludzie czują się w internecie anonimowi (choć w rzeczywistości tacy nie są), w związku z tym nie zawsze zachowują się tak jak w środowisku realnym, w którym podlegają kontroli otoczenia. Internet stanowi również doskonały środek do propagowania treści niezgodnych z ogólnie przyjętymi normami. Na treści faszystowskie, pornografię, sceny przemocy itp. są narażone zwłaszcza dzieci.

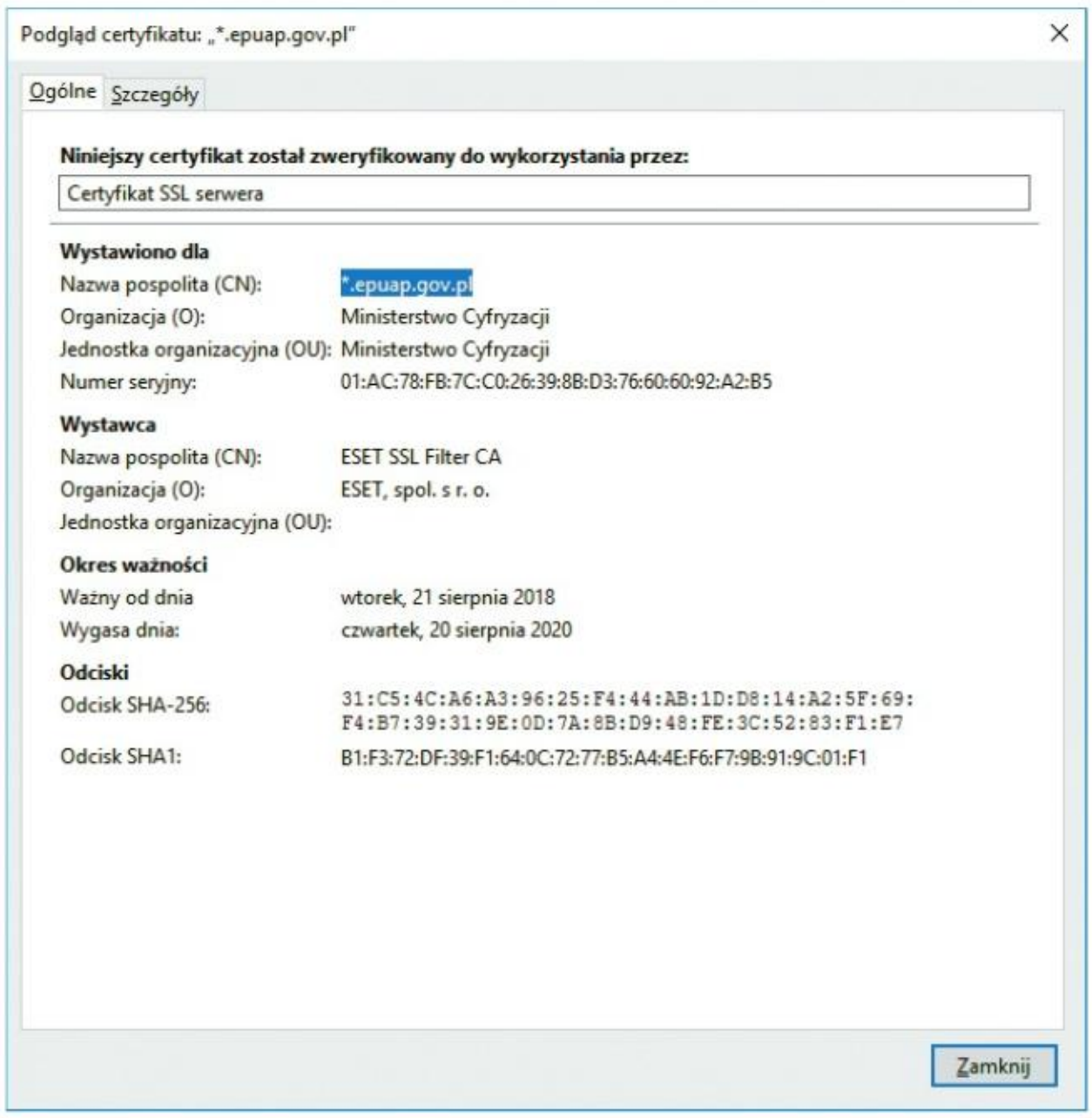
Inną kategorią zagrożeń jest **zagrożenie prywatności**. Wielu użytkowników sieci udostępnia swoje dane personalne, adresy, numery telefonów, a w przypadku transakcji finansowych – również numery kont i kart kredytowych. Informacje tego typu mogą być wykorzystane przez innych użytkowników sieci, nie zawsze zgodnie z prawem i przez to narażają internautę na nieprzyjemności i straty finansowe. Szczególną rozwagą należy kierować się podczas korzystania z usług wymagających podania hasła lub numeru karty kredytowej. W czasie korzystania z tego typu usług trzeba bezwzględnie używać „bezpiecznych protokołów", które stosują szyfrowanie informacji przesyłanych przez sieć. Aby odczytać ich treść, konieczna jest znajomość klucza kryptograficznego. Przed dokonaniem transakcji internetowej należy upewnić się, że korzysta się z bezpiecznego protokołu. W przypadku przeglądarki internetowej, zamiast domyślnego protokołu HTTP, będzie używany szyfrowany protokół HTTPS, a dodatkowo pojawi się symbol kłódki, oznaczający szyfrowanie treści przesyłanych danych. Na rys. 48.1 zaznaczono miejsca, na które powinniśmy zwrócić uwagę.

W razie wątpliwości dotyczących autentyczności strony można dodatkowo zweryfikować certyfikat serwera. Każda instytucja dokonująca transakcji finansowych powinna mieć aktualny



Rys. 48.1. Bezpieczny protokół przeglądania stron

certyfikat potwierdzający autentyczność swojej strony internetowej. Przedstawiony na rys. 48.2 certyfikat można sprawdzić po kliknięciu ikony kłódki, najechaniu kursorem na połączenie i kliknięciu **Wyświetl informacje o połączeniu**. W oknie bezpieczeństwo trzeba kliknąć przycisk **Więcej informacji**, wybrać zakładkę **Bezpieczeństwo** i kliknąć przycisk **Wyświetl certyfikat**.



Rys. 48.2. Certyfikat potwierdzający autentyczność strony

Sieci komputerowe i dane przesyłane za ich pomocą są narażone na różnego rodzaju zagrożenia. Aby im przeciwdziałać i zapewnić bezpieczeństwo, administrator sieci i wszyscy użytkownicy powinni przestrzegać zasad określonych w polityce bezpieczeństwa firmy. **Polityka bezpieczeństwa** to dokument obejmujący wiele aspektów działania sieci i uwzględniający m.in. poniższe zagadnienia.

1. Fizyczny nadzór związany z bezpieczeństwem:
   - Czy spodziewamy się podłączenia intruza do sieci w celu podsłuchania przysłanych danych?
   - Czy intruz ma możliwość uzyskania fizycznego dostępu do infrastruktury?
   - Jakie są rodzaj nośnika i topologia sieci?
   - Jakie są fizyczne zabezpieczenia urządzeń i ich lokalizacja?
   - Jak wygląda fizyczny dostęp do urządzeń (kto, kiedy)?
   - Jak wyglądają zabezpieczenia środowiskowe (temperatura, wilgotność, pole elektromagnetyczne itp.)?
2. Logiczny nadzór związany z bezpieczeństwem:
   - granice podsieci (adresacja, routing itp.);
   - kontrola logicznego dostępu do sieci;
   - zapewnienie uwierzytelniania użytkowników;
   - zagrożenia spowodowane czynnikiem ludzkim.
3. Zapewnienie integralności systemu i danych:
   - ściany ogniowe i kontrola ruchu w sieci;
   - dostępne usługi sieciowe;
   - zabezpieczenia przed atakami (wyeksponowane usługi, wewnętrzne komputery klienckie itp.).
4. Zapewnienie poufności danych:
   - szyfrowanie danych i ustalenie, które dane szyfrować, a które przesyłać otwartym tekstem;
   - zasady i procedury dla personelu, który będzie odpowiedzialny za sieć firmową:
     - polityka tworzenia kopii bezpieczeństwa;
     - zasady korzystania z komputerów przenośnych;
     - zasady zarządzania kontami użytkowników;
     - procedury obsługi incydentów;
   - organizacja szkoleń mających na celu podniesienie świadomości użytkowników sieci.

Polityka musi być na bieżąco aktualizowana, tak aby zapewnić ciągłe podnoszenie poziomu bezpieczeństwa. Administrator sieci jest zobowiązany dysponować narzędziami ułatwiającymi zapewnienie bezpieczeństwa sieci. Niezbędnym składnikiem oprogramowania każdego komputera w sieci jest program antywirusowy. **Program antywirusowy** (ang. *antivirus*) to program komputerowy, którego celem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych i innych rodzajów niechcianego oprogramowania. Najczęściej jest to pakiet programów chroniących komputer przed różnego typu zagrożeniami.

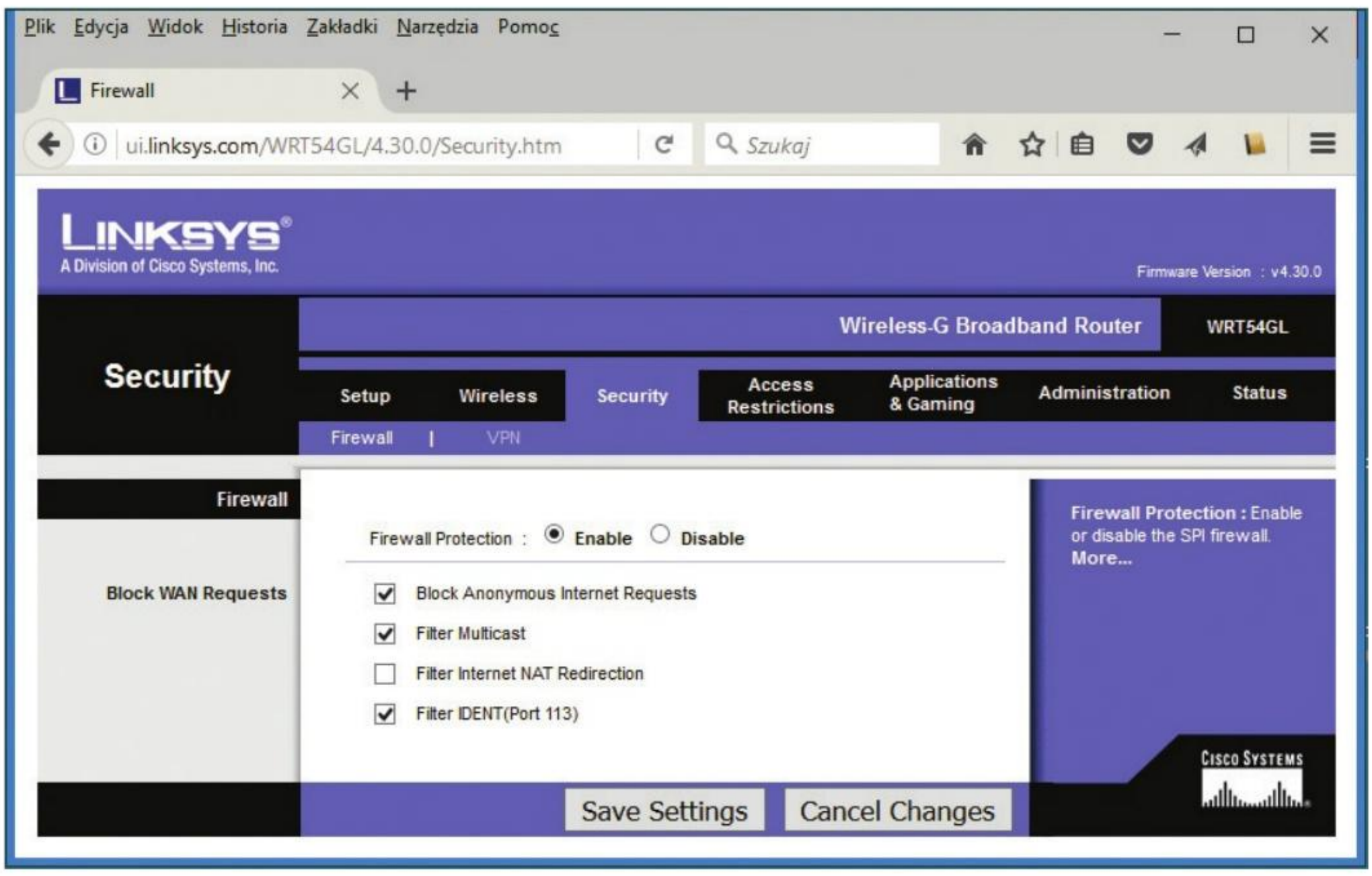
Programy antywirusowe mogą być również instalowane na urządzeniach sieciowych i w takim przypadku chronią całą sieć. Przykładowo, zainstalowanie antywirusa na bramie sieciowej powoduje, że cały ruch odbywający się przez tę bramę będzie analizowany pod kątem wystąpienia wirusów, natomiast skanowanie wszystkich wiadomości poczty elektronicznej może zapewnić program antywirusowy zainstalowany na serwerze pocztowym. Istnieją również sieciowe wersje programów antywirusowych – taki program zainstalowany na serwerze jest w stanie skanować wszystkie stacje robocze w sieci i w razie konieczności usuwać z nich wirusy.

Ochronę sieci przed dostępem nieuprawnionych użytkowników może zapewnić system **zapór sieciowych** (ang. *firewall*). Funkcję zapory sieciowej może pełnić komputer z zainstalowanym

oprogramowaniem lub urządzenie sieciowe specjalnie do tego przeznaczone. Takie urządzenie może chronić całą sieć lub tylko jej fragment przed nieuprawnionym dostępem z zewnątrz, np. z internetu, albo wypływem danych z sieci lokalnej na zewnątrz. Firewall, na podstawie zdefiniowanych reguł, filtruje połączenia wchodzące i wychodzące oraz blokuje żądania dostępu uznane za niebezpieczne. Reguły pozwalają na filtrowanie ruchu na różnych poziomach na podstawie informacji w nagłówkach:

- warstwy dostępu do sieci (źródłowe i docelowe adresy MAC);
- warstwy sieciowej (adresy IP nadawcy i odbiorcy, rodzaj przenoszonego protokołu);
- warstwy transportowej (porty źródłowe i docelowe);
- warstwy aplikacji (protokoły, takie jak FTP, HTTP, telnet).

Najbardziej zaawansowane rozwiązania pozwalają również na kontrolowanie zawartości pakietów w poszukiwaniu np. słów uznawanych za niebezpieczne. Firewall może zapisywać w logach informacje o naruszeniach reguł, co stanowi źródło informacji dla administratora i umożliwia mu podjęcie działań w celu poprawy zabezpieczeń lub analizy metod i skutków włamań do systemu. Wiele urządzeń sieciowych, takich jak routery, ma wbudowane funkcje firewalla; należy je tylko skonfigurować dla konkretnej sieci i włączyć. Przykład panelu konfiguracyjnego firewalla w routerze WRT54GL przedstawiono na rys. 48.3.



Rys. 48.3. **Konfigurowanie zapory w routerze sprzętowym**

48.1. Korzystanie z list kontroli dostępu na routerze

Na routerze Cisco można skonfigurować prostą zaporę sieciową, która za pomocą list ACL będzie wykonywała proste filtrowanie ruchu. **Listy kontroli dostępu** (ang. *Access Control List*, ACL) to sekwencyjne listy instrukcji **zezwalających** (ang. *permit*) albo **odmownych** (ang. *deny*), odnoszących się do adresów lub protokołów warstwy wyższej. Pozwalają na kontrolowanie ruchu

wchodzącego i wychodzącego z sieci. Można je skonfigurować dla wszystkich routowanych protokołów sieciowych. Składają się z **warunków** używanych do sprawdzania ruchu w sieci, który jest kierowany przez interfejs routera, i informują router, które rodzaje pakietów zaakceptować, a które odrzucić.

Router sprawdza każdy pakiet i albo go przekaże, albo odrzuci, zależnie od warunków określonych na liście ACL. Jeśli na routerze nie skonfigurowano list ACL, wszystkie pakiety przechodzące przez router będą przepuszczane. Do podejmowania decyzji o przekazaniu lub zablokowaniu pakietu mogą być wykorzystywane adres źródłowy IP, adres docelowy IP, protokół i numery portów wyższych warstw.

Listy ACL mogą zostać utworzone osobno dla każdego protokołu, kierunku i interfejsu (rys. 48.4). Jeśli router ma dwa interfejsy skonfigurowane dla protokołów IP i IPX, można utworzyć maksymalnie osiem oddzielnych list ACL (dwa protokoły, dwa interfejsy i dwa kierunki), ale nie wszystkie muszą być tworzone i wykorzystywane.

Rys. 48.4. **Listy ACL**

Kolejność instrukcji na liście ACL jest istotna. Kiedy system sprawdza pakiet, porównuje go z każdą z instrukcji warunkowych w kolejności od początku do końca listy. Po znalezieniu na liście pasującej pozycji zostaje przeprowadzona czynność akceptacji lub odrzucenia i nie są wykonywane żadne inne instrukcje z listy ACL, np. jeśli na początku listy znajduje się instrukcja dopuszczająca cały ruch, żadna z instrukcji znajdujących się niżej nie będzie nigdy sprawdzana, a cały ruch zostanie przepuszczony. Jeśli nie udało się dopasować żadnej instrukcji ACL, domyślnie, na końcu listy, jest umieszczana **niejawna instrukcja blokująca cały ruch** (ang. *deny any*).

Nowe instrukcje są dodawane na końcu listy. Jeśli niezbędne jest dodanie nowych instrukcji warunkowych w środku listy kontroli dostępu, należy usunąć całą listę i utworzyć ją na nowo, razem z nową instrukcją warunku.

Listy ACL można podzielić na:

- **standardowe** – sprawdzają tylko adres źródłowy routowanych pakietów IP;
- **rozszerzone** – sprawdzają źródłowy i docelowy adres IP, numery portów źródłowych i docelowych oraz inne informacje.

Router rozróżnia listy na podstawie ich numeru. Standardowa lista ACL może mieć numer z przedziału od 1 do 99 lub – w nowszych systemach również – od 1300 do 1999. Lista rozszerzona może mieć numer z zakresu od 100 do 199, a w nowszych systemach również od 2000 do 2699.

W listach ACL do określenia zakresu adresów są wykorzystywane **maski wieloznaczne** (ang. *wildcard mask*). W tych maskach bit 0 oznacza konieczność dopasowania do wartości odpowiadającego bitu w adresie, natomiast bit 1 – możliwość zignorowania wartości odpowiadającego bitu w adresie. Dodatkowo zdefiniowano dwa specjalne słowa kluczowe: **any** – zastępuje 255.255.255.255 dla maski wieloznacznej – pasuje do dowolnego adresu, z którym jest porównywana, i **host** – zastępuje 0.0.0.0 dla maski wieloznacznej – wymaga, aby wszystkie bity w adresie ACL i adresie pakietu pasowały do siebie. Ta opcja wymusza dopasowanie do jednego konkretnego adresu. Przykładowo, maska podsieci 255.255.255.0 odpowiada masce wieloznacznej 0.0.0.255.

Procedura tworzenia standardowej listy ACL przebiega w następujący sposób:

1. **Utworzenie listy**

   Pełna składnia polecenia standardowej listy ACL:

   ```
   Router(config)#access-list numer-listy-dostępu {deny | permit |
   remark} źródło [wieloznaczna maska-źródła ] [log]
   ```

   Przykładowo w poleceniu:

   ```
   R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
   ```

   zostanie dodany warunek do listy numer 1, zezwalający (ang. *permit*) na przesyłanie pakietów z sieci **192.168.1.0** z maską wieloznaczną **0.0.0.255**. Aby usunąć listę ACL, należy wydać polecenie:

   ```
   Router(config)#no access-list numer-listy-dostępu
   ```

2. **Wybór interfejsu**

   Lista ACL może być zastosowana na interfejsie fizycznym, np. **fastEthernet 0/0**, lub wirtualnym, np. **vty 0 4**. Standardowe listy ACL umieszcza się jak najbliżej miejsca przeznaczenia pakietu. Rozszerzone listy ACL umieszcza się jak najbliżej źródła pakietu.

3. **Zastosowanie listy na interfejsie fizycznym lub wirtualnym**

   Polecenie **ip access-group** wydane w trybie konfiguracji wybranego interfejsu łączy istniejącą listę ACL z interfejsem fizycznym, np. **fastEthernet 0/0** na kierunku wychodzącym, np.:

   ```
   R1(config-if)#ip access-group 1 out
   ```

   Polecenie **ip access-class** wydane w trybie konfiguracji wybranego interfejsu łączy istniejącą listę ACL z interfejsem wirtualnym, np. **vty 0 4** na kierunku wchodzącym, np.:

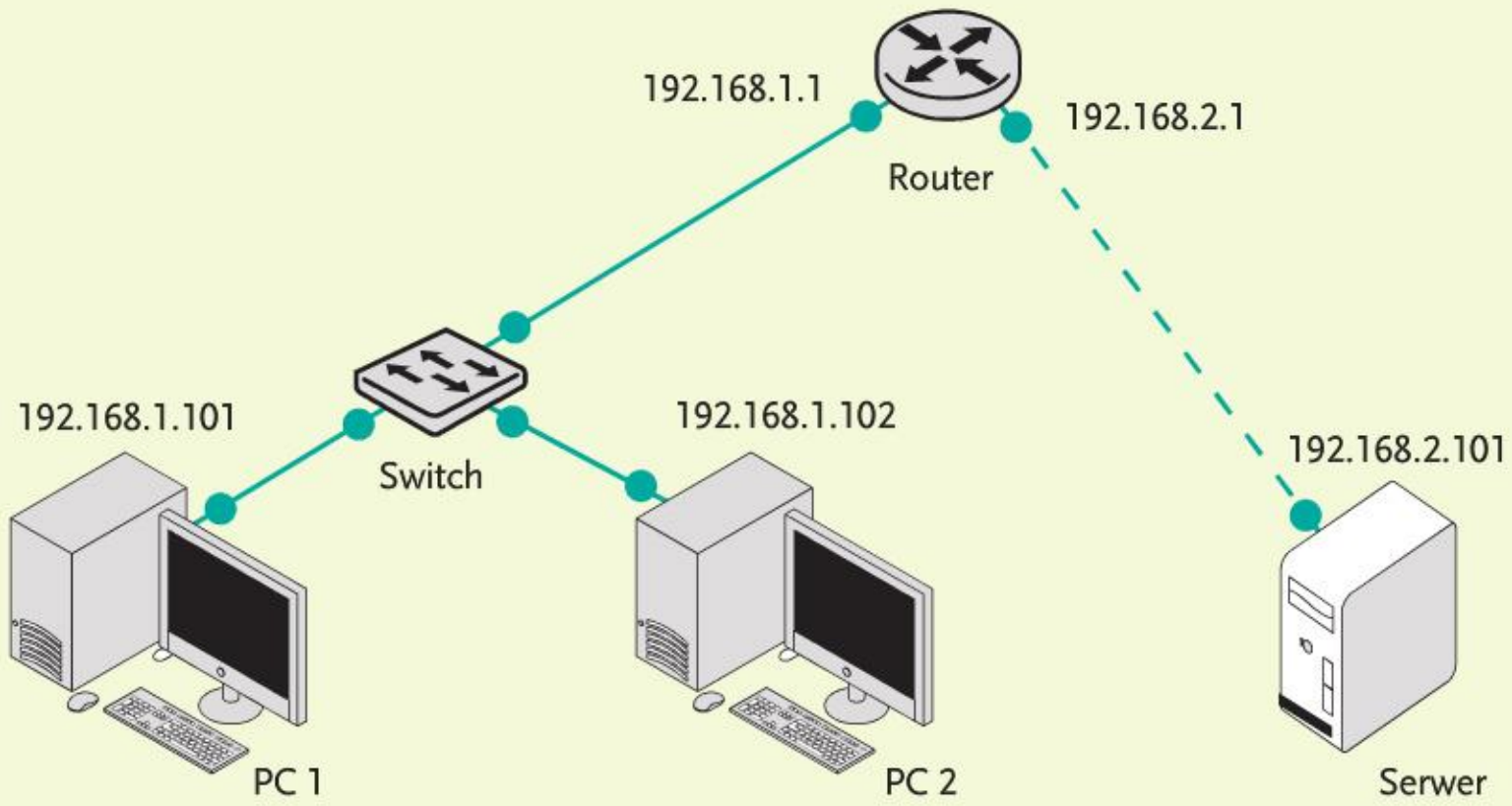
   ```
   R1(config-if)#ip access-class 1 in
   ```

PRZYKŁAD 48.1

Tworzenie standardowej listy ACL

Aby utworzyć standardową listę ACL zezwalającą na przesyłanie pakietów tylko z adresu **192.168.1.101**, należy:

1. Uruchomić Cisco Packet Tracer i skonfigurować sieć jak na rys. 48.5.



Rys. 48.5. **Schemat sieci do testowania list ACL**

2. Skonfigurować adresy IP komputerów i serwera zgodnie z opisem na rysunku.
3. Nawiązać połączenie z routerem i skonfigurować jego interfejsy zgodnie z opisem na rysunku.
4. W trybie konfiguracji globalnej utworzyć standardową listę ACL za pomocą poleceń:

```
Router(config)#no access-list 1
Router(config)#access-list 1 permit 192.168.1.101 0.0.0.0
Router(config)#access-list 1 deny any
```

5. Wybrać interfejs, do którego jest przyłączony komputer:

```
Router(config)#interface fastEthernet 0/0
```

6. Połączyć listę ACL z interfejsem:

```
Router(config)#ip access-group 1 in
```

7. Przetestować możliwość komunikacji między komputerami i serwerem.

PRZYKŁAD 48.2

Stosowanie standardowej listy ACL na interfejsie wirtualnym

W tym przykładzie za pomocą standardowej listy ACL zostanie ograniczony dostęp do routera za pomocą telnetu. W takim przypadku listę ACL należy połączyć z interfejsem wirtualnym **`vty 0 4`**. Aby utworzyć standardową listę ACL zezwalającą na dostęp do routera za pomocą telnetu tylko z adresu **`192.168.1.101`**, należy:

1. Uruchomić Cisco Packet Tracer i skonfigurować sieć jak na rys. 48.5.
2. Skonfigurować adresy IP komputerów i serwera zgodnie z opisem na rysunku.
3. Nawiązać połączenie z routerem i skonfigurować jego interfejsy zgodnie z opisem na rysunku.
4. W trybie konfiguracji globalnej zabezpieczyć router hasłem:

```
Router(config)#enable secret cisco
```

5. W trybie konfiguracji globalnej utworzyć standardową listę ACL za pomocą poleceń:

```
Router(config)#no access-list 1
Router(config)#access-list 1 permit 192.168.1.101 0.0.0.0
Router(config)#access-list 1 deny any
```

6. Wybrać interfejsy wirtualne, wykorzystywane przez usługę telnet:

```
Router(config)#line vty 0 4
```

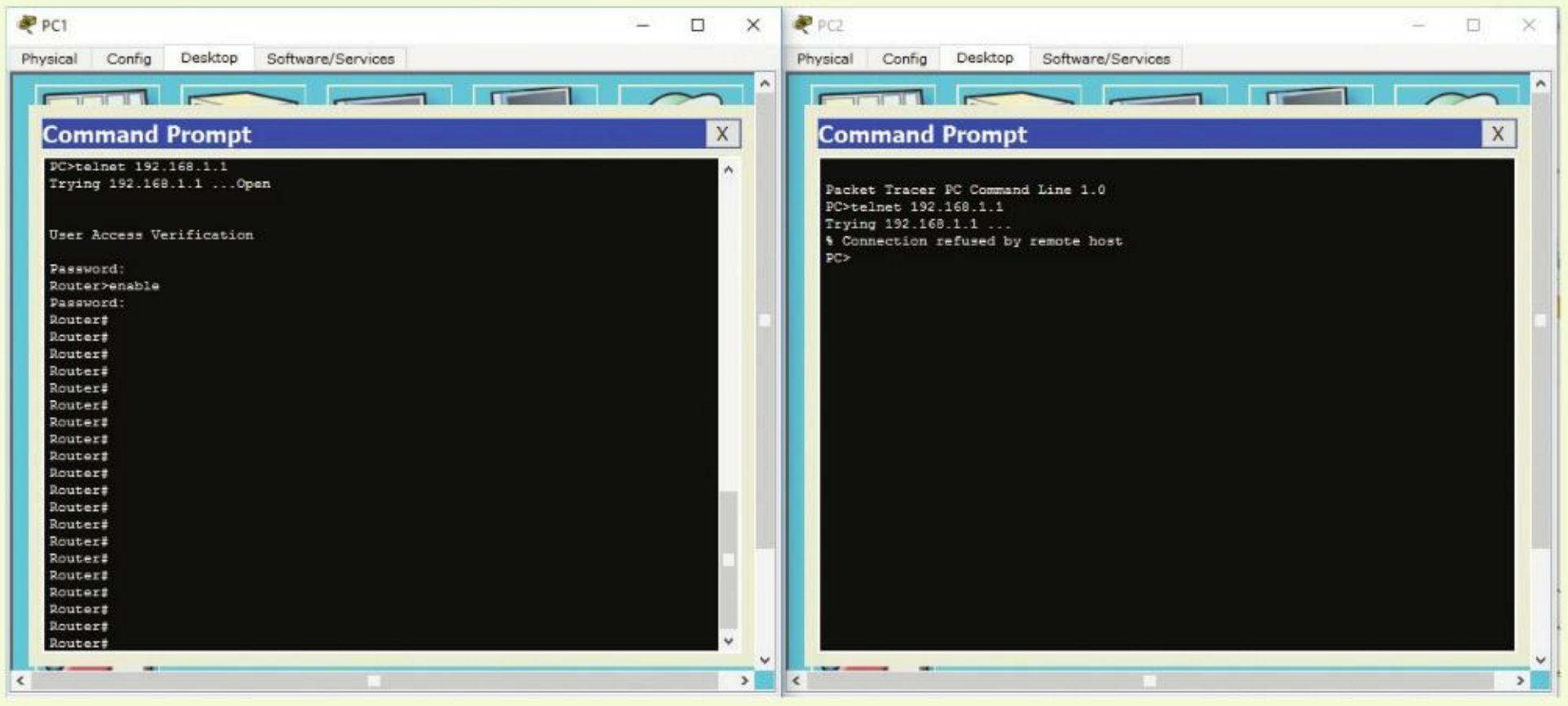
7. Umożliwić nawiązywanie połączenia z routerem za pomocą poleceń:

```
password cisco
login
```

8. Połączyć listę ACL z interfejsem:

```
Router(config)#ip access-class 1 in
```

9. Przetestować możliwość nawiązania połączenia przez telnet z komputerów do routera (rys. 48.6).



Rys. 48.6. **Testowanie list ACL za pomocą usługi telnet**

Rozszerzone listy ACL służą do sprawdzania źródłowych i docelowych adresów pakietów oraz mogą sprawdzać protokoły i numery portów. Dostępem można sterować na podstawie: adresów IP nadawcy i odbiorcy pakietu, typu protokołu, portu lub usługi. Proces tworzenia rozszerzonej listy kontroli dostępu jest taki sam, jak w przypadku standardowej listy kontroli dostępu.

Przykładowe polecenie do tworzenia rozszerzonej listy ACL jest następujące:

```
R1(config)#access-list 101 permit tcp 192.168.1.101 0.0.0.0 host
192.168.2.101 eq 23
```

W tym poleceniu:

- **101** – numer listy ACL;
- **permit** – pozwolenie na przekazanie pakietu;
- **tcp** – protokół; inne przykładowe możliwości to: **ip**, **udp**, **icmp**;
- **192.168.1.101 0.0.0.0** – adres IP i maska wieloznaczna źródła – wskazuje na pojedynczy adres;
- **host 192.168.2.101** – adres IP i maska wieloznaczna miejsca docelowego – wskazuje na pojedynczy adres (słowo **host** odpowiada masce wieloznacznej **0.0.0.0**);
- **eq 23** – numer portu docelowego (**eq** oznacza równe, **neq** – różne, **lt** – mniej niż, **gt** – więcej niż). Zamiast numeru portu można podać nazwę usługi, np. **telnet**, **ftp**, **ftp-data**.

PRZYKŁAD 48.3

Stosowanie rozszerzonej listy ACL na interfejsie

W tym przykładzie za pomocą rozszerzonej listy ACL zostanie ograniczony dostęp do serwera z komputera o adresie **192.168.1.101**. Ograniczenie nie będzie dotyczyło pozostałych komputerów z sieci **192.168.1.0/24**. Aby utworzyć rozszerzoną listę ACL realizującą powyższą politykę, należy:

1. Uruchomić Cisco Packet Tracer i skonfigurować sieć jak na rys. 48.5.
2. Skonfigurować adresy IP komputerów i serwera zgodnie z opisem na rysunku.
3. Nawiązać połączenie z routerem i skonfigurować jego interfejsy zgodnie z opisem na rysunku.

4. W trybie konfiguracji globalnej utworzyć rozszerzoną listę ACL za pomocą poleceń:

```
Router(config)#no access-list 101
Router(config)#access-list 101 deny tcp host 192.168.1.101 host
192.168.2.101 eq 80
Router(config)#access-list 101 deny tcp host 192.168.1.101 host
192.168.2.101 eq 20
Router(config)#access-list 101 deny tcp host 192.168.1.101 host
192.168.2.101 eq 21
Router(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.255
host 192.168.2.101
Router(config)#access-list 101 deny ip any any
```

   W pierwszym poleceniu jest usuwana lista ACL o numerze **101** (jeśli istniała). Kolejne polecenia oznaczają:
   - blokowanie komunikacji komputera o adresie **192.168.1.101** z serwerem na porcie **80** (WWW);
   - blokowanie komunikacji komputera o adresie **192.168.1.101** z serwerem na porcie **20** (ftp-data);
   - blokowanie komunikacji komputera o adresie **192.168.1.101** z serwerem na porcie **21** (ftp);
   - zezwolenie na komunikację komputerów z sieci **192.168.1.0/24** z serwerem;
   - blokowanie pozostałego ruchu.
5. Wybrać interfejs, do którego jest przyłączony komputer:

```
Router(config)# interface fastEthernet 0/0
```

6. Połączyć listę ACL z interfejsem:

```
Router(config)#ip access-group 101 in
```

7. Przetestować możliwość nawiązania komunikacji komputerów z routerem.

Polecenie **show access-lists** służy do wyświetlania zawartości wszystkich list ACL na routerze (aby wyświetlić konkretną listę, jako opcję tego polecenia należy podać numer listy ACL). Polecenie **show running-config** również wyświetla listy kontroli dostępu na routerze i informacje o ich przypisaniu do interfejsów.

48.2. Systemy bezpieczeństwa IDS/IPS

Podniesienie poziomu bezpieczeństwa sieci można uzyskać przez zastosowanie systemów bezpieczeństwa IDS/IPS. **IDS** (ang. *Intrusion Detection System*) jest rozwiązaniem służącym do monitorowania zagrożeń oraz incydentów naruszenia bezpieczeństwa i powiadamiania o ich wystąpieniu. **IPS** (ang. *Intrusion Prevention System*) podejmuje dodatkowo działania mające na celu powstrzymanie ataku, minimalizację jego skutków lub aktywną odpowiedź na naruszenie bezpieczeństwa. Systemy IDS/IPS działają przez analizę ruchu sieciowego za pomocą dwóch metod:

- **analizy heurystycznej** – polega na łączeniu pakietów w strumienie danych, analizie nagłówków pakietów i analizie protokołów aplikacyjnych. Pozwala wytypować pakiety mogące zakłócić działanie docelowej aplikacji;
- **analizy sygnaturowej** – polega na wyszukiwaniu w pakietach ciągów danych charakterystycznych dla znanych ataków sieciowych. System korzysta z bazy sygnatur, podobnej do bazy wirusów z programów antywirusowych. Baza sygnatur jest również aktualizowana przez internet.

Głównym składnikiem systemów IDS/IPS jest **sonda** (ang. *sensor*) lub wiele sond zbierających przepływające dane oraz analizujących ruch sieciowy i wykrywających ataki. Sondy wykorzystują do identyfikacji ataku bazę danych zawierającą informacje o znanych atakach. Analizator logów umożliwia ich analizę i przedstawienie w formie wykresów. Zależnie od zakresu analizowanych zdarzeń systemy IDS/IPS można podzielić na:

- **hostowe** (ang. *host-based*) – zbierają i analizują dane na komputerze, który jest gospodarzem systemu, np. serwerze sieciowym;
- **sieciowe** (ang. *network-based*) – analizują ruch sieciowy we wszystkich urządzeniach w segmencie sieci, do którego są podłączone. Sieciowe systemy IPS mogą wykorzystywać **sondę pasywną** – podłączoną do portu monitorującego przełącznika, która analizuje wszystkie pakiety w danym segmencie sieci. **Sonda inline** jest umieszczona między dwoma segmentami sieci, analizuje wszystkie pakiety w sieci i bezpośrednio uczestniczy w ich przekazywaniu. W tym trybie sonda ma możliwość blokowania pakietów rozpoznanych jako niebezpieczne.

Oprócz wymienionych systemów, w warunkach szkolnych musi funkcjonować program odpowiedzialny za ochronę uczniów przed niebezpiecznymi treściami. Programy tego typu filtrują ruch sieciowy pod kątem niedozwolonych treści, takich jak przemoc, pornografia, narkotyki. Najczęściej korzystają z bazy adresów URL i słów kluczowych.

48.3. Zarządzanie zasobami serwera plików

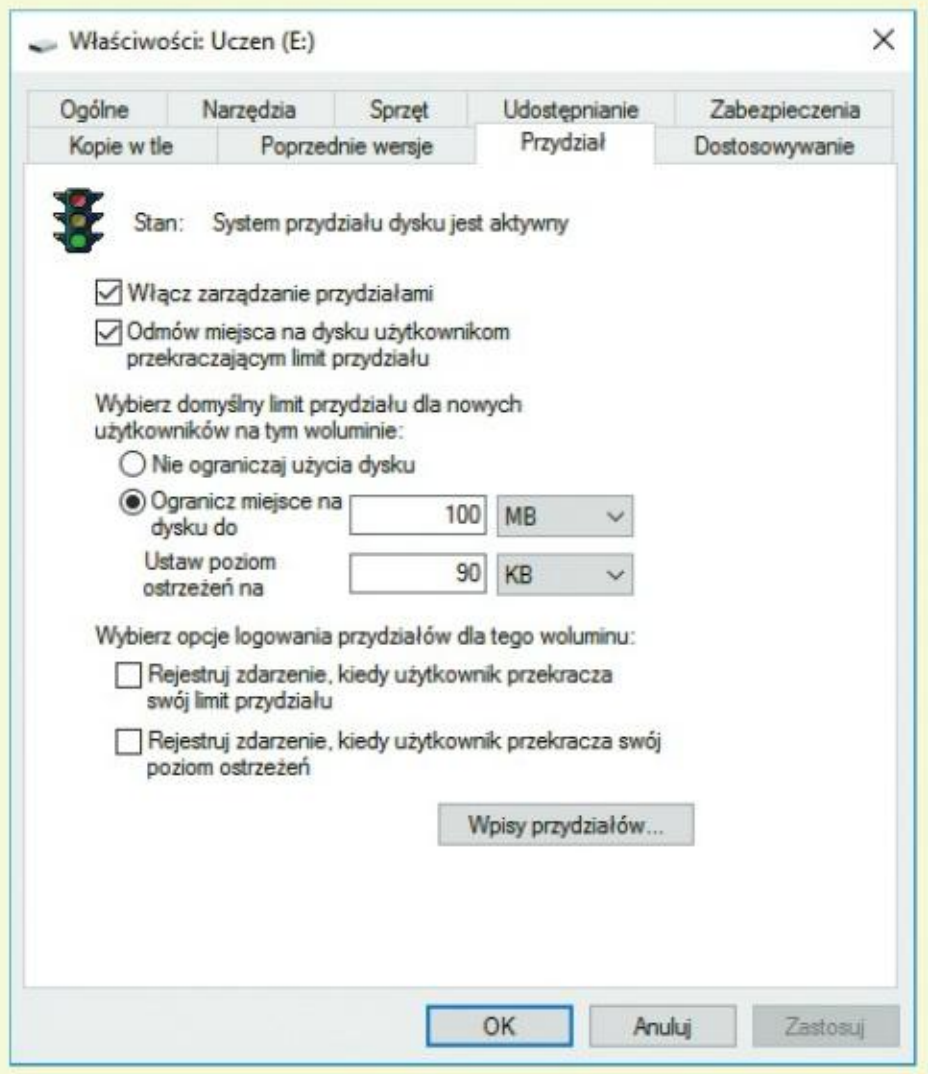
Quota jest funkcją systemów plików umożliwiającą limitowanie miejsca dyskowego, z którego użytkownik może korzystać. Jest to szczególnie ważne na serwerach z wieloma użytkownikami. Pozwala zabezpieczyć partycje dyskowe przed zapełnieniem i w konsekwencji zablokowaniem możliwości tworzenia i zapisywania zbiorów.

PRZYKŁAD 48.4

Konfigurowanie i korzystanie z Quoty w systemie Windows Server

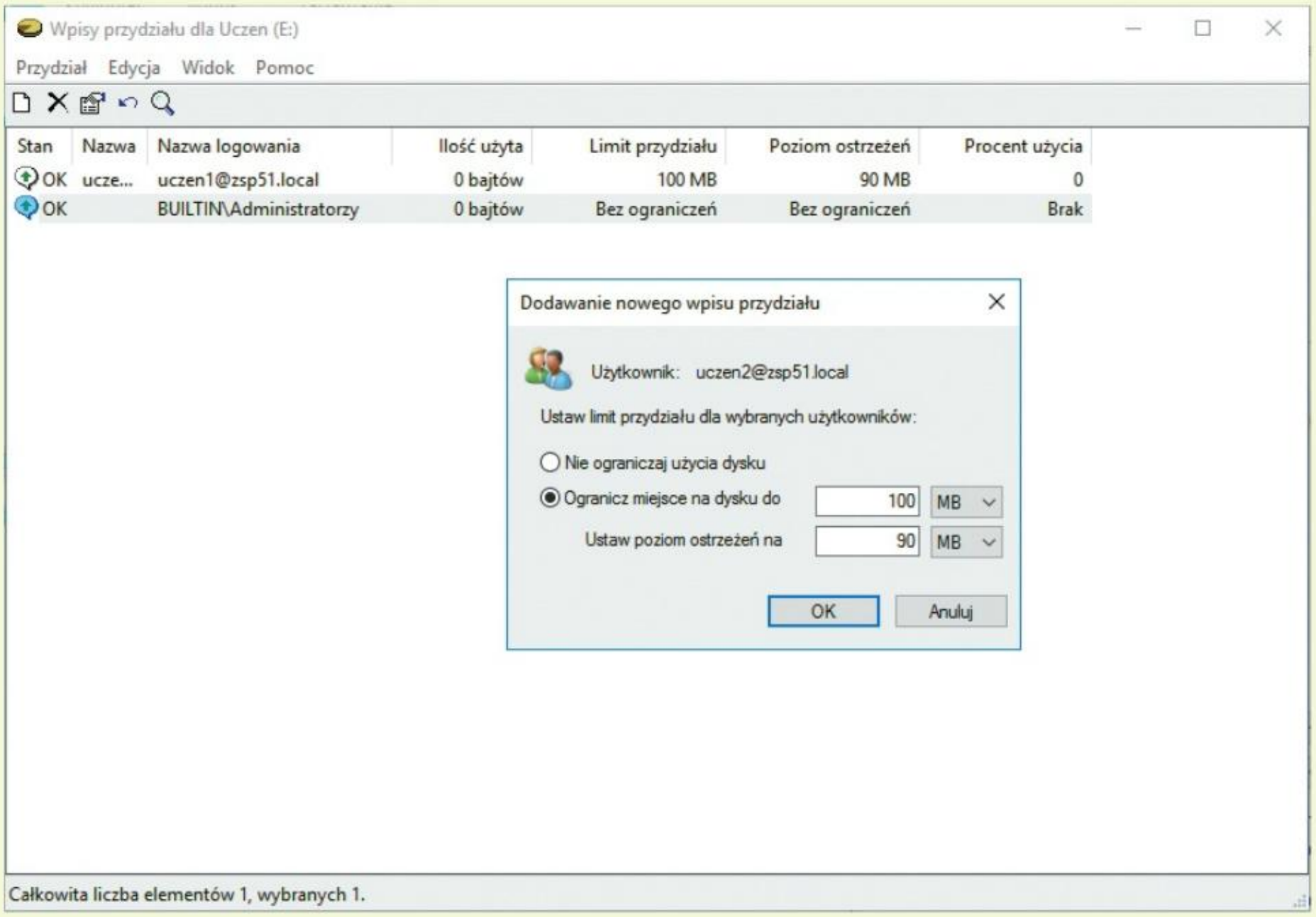
W tym przykładzie za pomocą Quoty zostanie ograniczona ilość przestrzeni dyskowej na partycji dostępnej dla użytkownika. Przykładowo, użytkownicy *uczen1* i *uczen2* uzyskają prawo do 100 MB przestrzeni dyskowej. Po przekroczeniu 90 MB zostanie wygenerowane ostrzeżenie. Aby skonfigurować mechanizm Quoty, należy:

1. Uruchomić **`Eksplorator plików`** i kliknąć prawym przyciskiem myszy ikonę dysku, na którym jest wprowadzany mechanizm Quota. Z menu podręcznego wybrać polecenie **`Właściwości`**.
2. W zakładce **`Przydział`** (rys. 48.7) zaznaczyć opcje **`Włącz zarządzanie przydziałami`** i **`Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału`**.

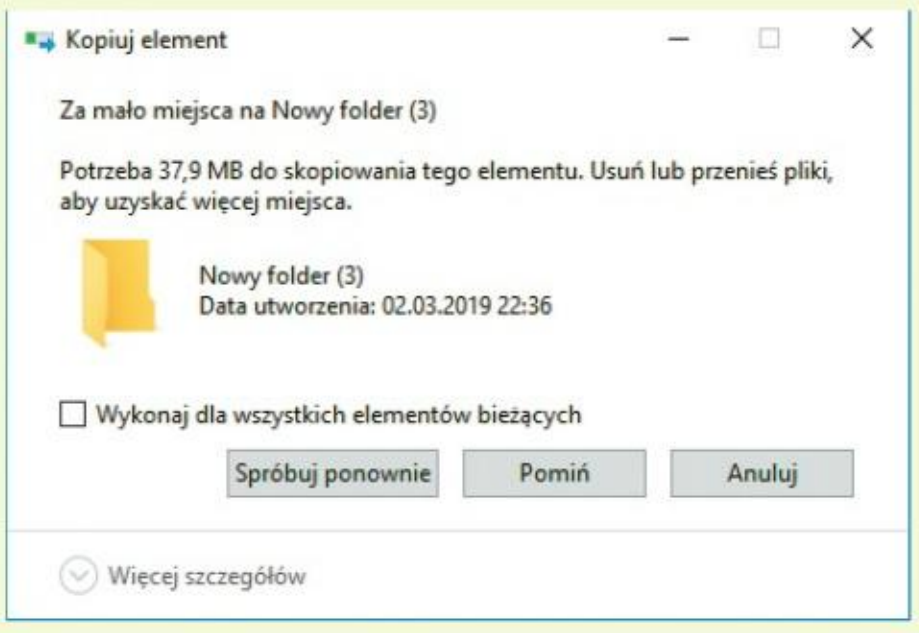


Rys. 48.7. Zakładka **`Przydział`**

3. Ustawić wartość domyślnego limitu dla nowych użytkowników na woluminie. Zaznaczyć opcję **Ogranicz miejsce na dysku do** i wskazać wartości limitu, np. 100 MB (tzw. limit twardy, którego przekroczenie nie jest możliwe), oraz poziom ostrzeżeń, np. 90 MB (tzw. limit miękki, który można przekroczyć, ale spowoduje to wygenerowanie ostrzeżenia).
4. Ustawić wartości przydziałów użytkowników. Kliknąć przycisk **Wpisy przydziałów**. W oknie **Wpisy przydziałów** (rys. 48.8) wprowadzić wpisy limitu twardego i miękkiego dla użytkowników. Kliknąć przycisk **OK** i zamknąć okno edycji przydziałów.



Rys. 48.8. **Edycja przydziałów dyskowych użytkowników**



Rys. 48.9. **Komunikat o przekroczeniu limitu**

5. Kliknąć przycisk **Zastosuj**, a następnie **OK**.
6. Przetestować system przydziałów. Jako użytkownik *uczen1* kopiować pliki aż do wyczerpania dostępnej przestrzeni dyskowej i wygenerowania komunikatu o przekroczeniu limitu (rys. 48.9).

Bardziej zaawansowanym narzędziem umożliwiającym zarządzanie zasobami plikowymi serwera jest **Menedżer zasobów serwera plików FSRM** (ang. *File Server Resource Manager*). Jest to usługa, która umożliwia klasyfikację i zarządzanie danymi przechowywanymi na serwerach plików. **Menedżer zasobów serwera plików** realizuje następujące funkcje:

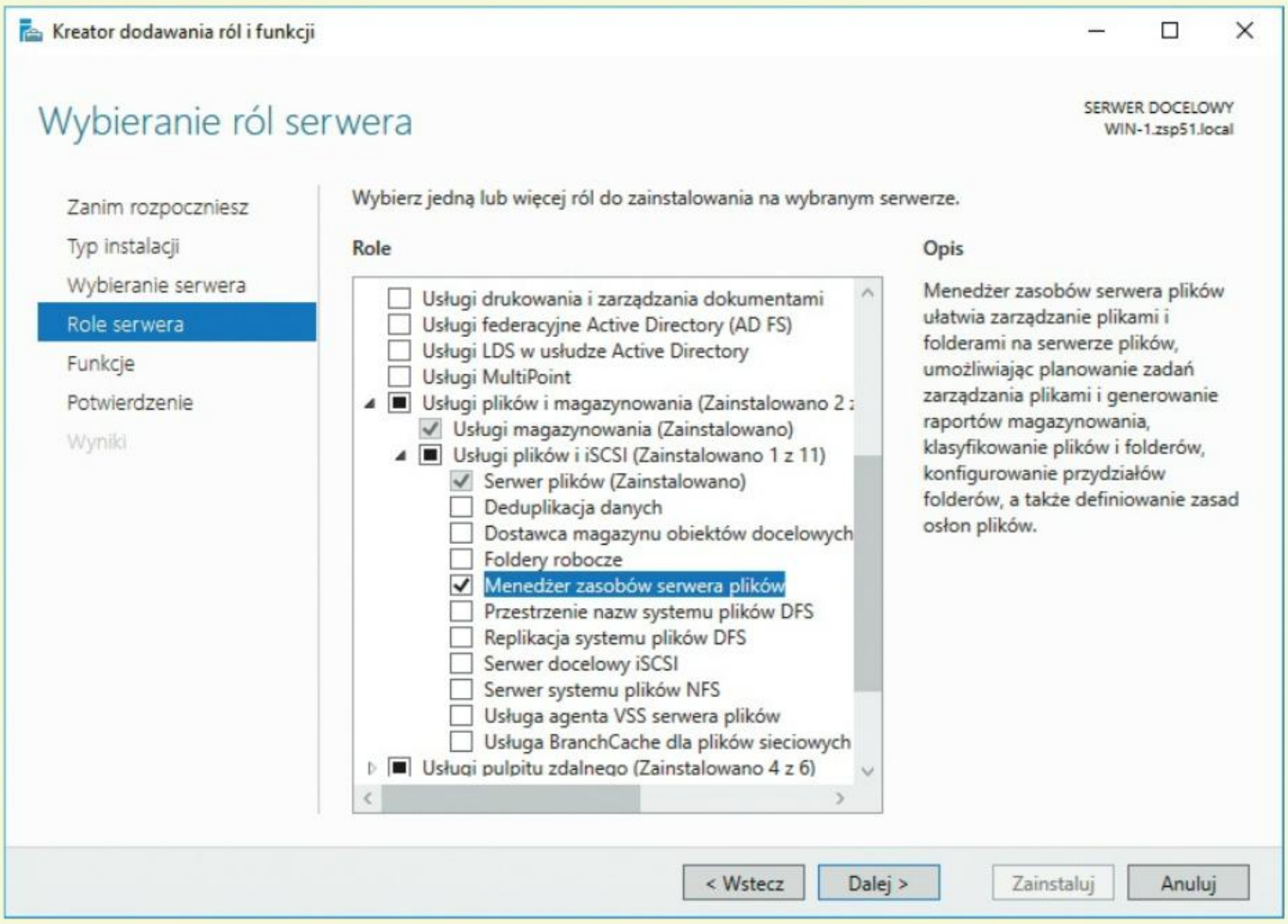
- **infrastruktura klasyfikacji plików** – umożliwia klasyfikację plików i stosowanie zasad, np. dynamiczną kontrolę dostępu w celu ograniczania dostępu do plików, szyfrowanie plików i wygaśnięcie pliku;
- **zadania zarządzania plikami** – umożliwiają stosowanie zasad warunkowych do plików lub wykonywanie na nich czynności na podstawie klasyfikacji. Przykładowymi warunkami mogą być: lokalizacja pliku, właściwości klasyfikacji, data utworzenia pliku, data jego ostatniej modyfikacji lub czas ostatniego dostępu do niego. Warunki decydują o czynnościach zarządzania plikami, umożliwiają wygasanie plików, szyfrowanie plików lub uruchamianie poleceń niestandardowych;
- **zarządzanie przydziałami** – umożliwia ograniczenie ilości miejsca dostępnego dla woluminu lub folderu; mogą być automatycznie stosowane do nowych folderów tworzonych na woluminie. Istnieje również możliwość definiowania szablonów przydziałów, które można stosować do nowych woluminów lub folderów.
- **zarządzanie osłonami plików** – umożliwia kontrolę typów plików, które użytkownik może przechowywać na serwerze plików. Można ograniczyć rozszerzenia plików, które mogą być przechowywane, np. utworzyć osłonę plików, która nie zezwala na przechowywanie plików z rozszerzeniem mp3 w folderach udostępnionych na serwerze plików.
- **raporty magazynowania** – umożliwia planowanie raportów czynności związanych z magazynowaniem, wykonywanych okresowo, za pomocą których np. będzie generowana lista plików najczęściej używanych w ciągu ostatnich dni lub będą monitorowane próby zapisywania nieautoryzowanych plików.

PRZYKŁAD 48.5

Instalacja usługi Menedżer zasobów serwera plików

Aby zainstalować usługi **Menedżer zasobów serwera plików**, należy:

1. W oknie aplikacji **Menedżer serwera** wybrać **Dodaj role i funkcje**. Po zapoznaniu się z ekranem powitalnym kreatora wybrać opcję **Instalacja oparta na rolach lub oparta na funkcjach**. Kliknąć przycisk **Dalej**.
2. Wybrać serwer, na którym będzie instalowana usługa. Kliknąć przycisk **Dalej**.
3. Z listy ról wybrać **Usługi plików i magazynowania/Usługi plików i iSCSI/Menedżer zasobów serwera plików** (rys. 48.10). Kliknąć przycisk **Dalej**. Potwierdzić zainstalowanie dodatkowych ról, niezbędnych do prawidłowego działania usługi. Kliknąć przycisk **Dodaj funkcje**. Kliknąć przycisk **Dalej**.
4. Zapoznać się z informacjami w oknie **Wybieranie funkcji**. Kliknąć przycisk **Dalej**.
5. Zapoznać się z informacjami w oknie **Potwierdzenie opcji instalacji**. Kliknąć przycisk **Zainstaluj**.
6. Po zakończeniu instalacji kliknąć przycisk **Zamknij**.



Rys. 48.10. **Wybieranie usługi `Menedżer zasobów serwera plików`**

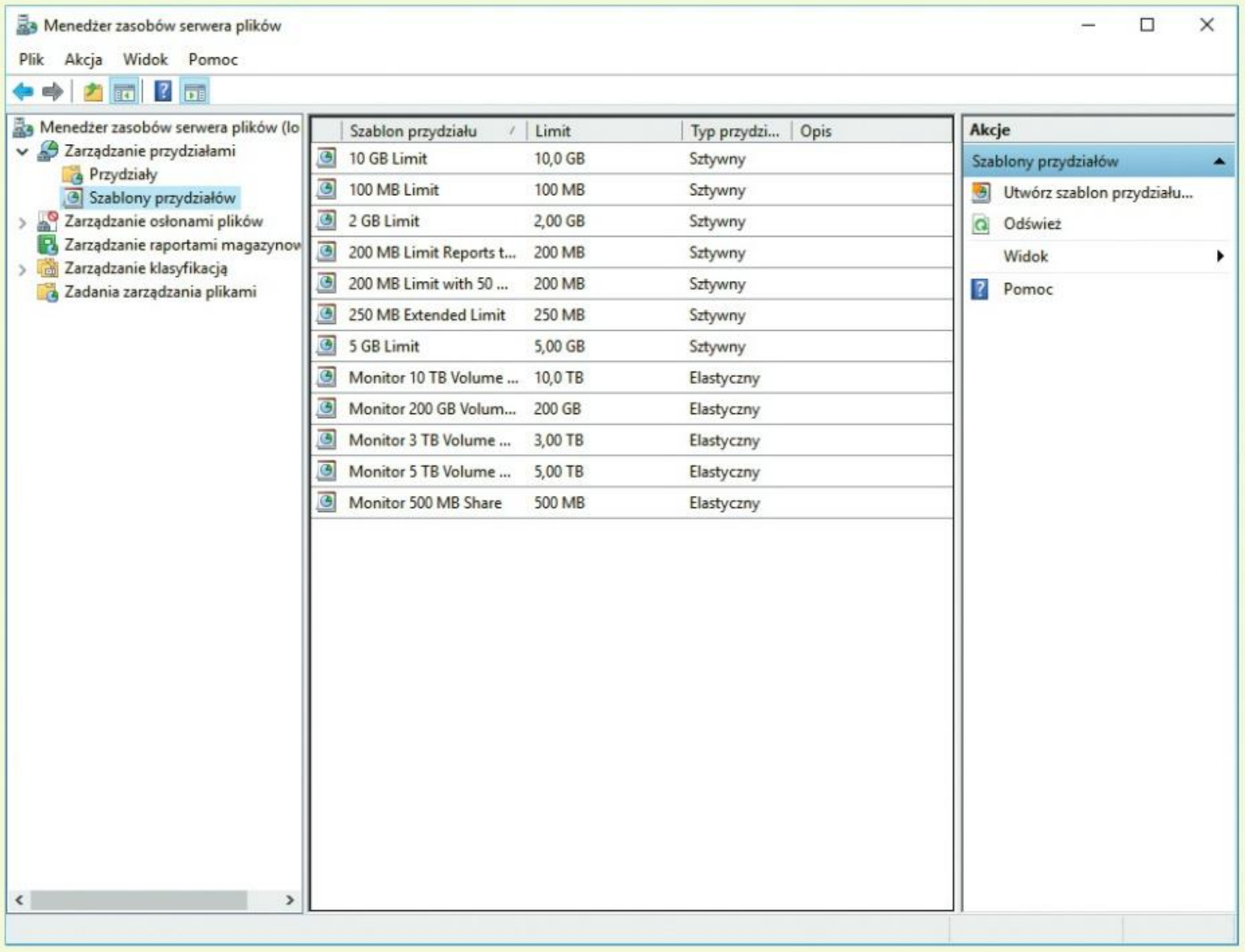
We wcześniejszym przykładzie został skonfigurowany mechanizm Quota na poziomie partycji dyskowej. Limit dotyczył przestrzeni dyskowej zajmowanej przez pliki użytkownika we wszystkich folderach na danej partycji. Za pomocą usługi **`Menedżer zasobów serwera plików`** można limitować przestrzeń dyskową w poszczególnych folderach.

PRZYKŁAD 48.6

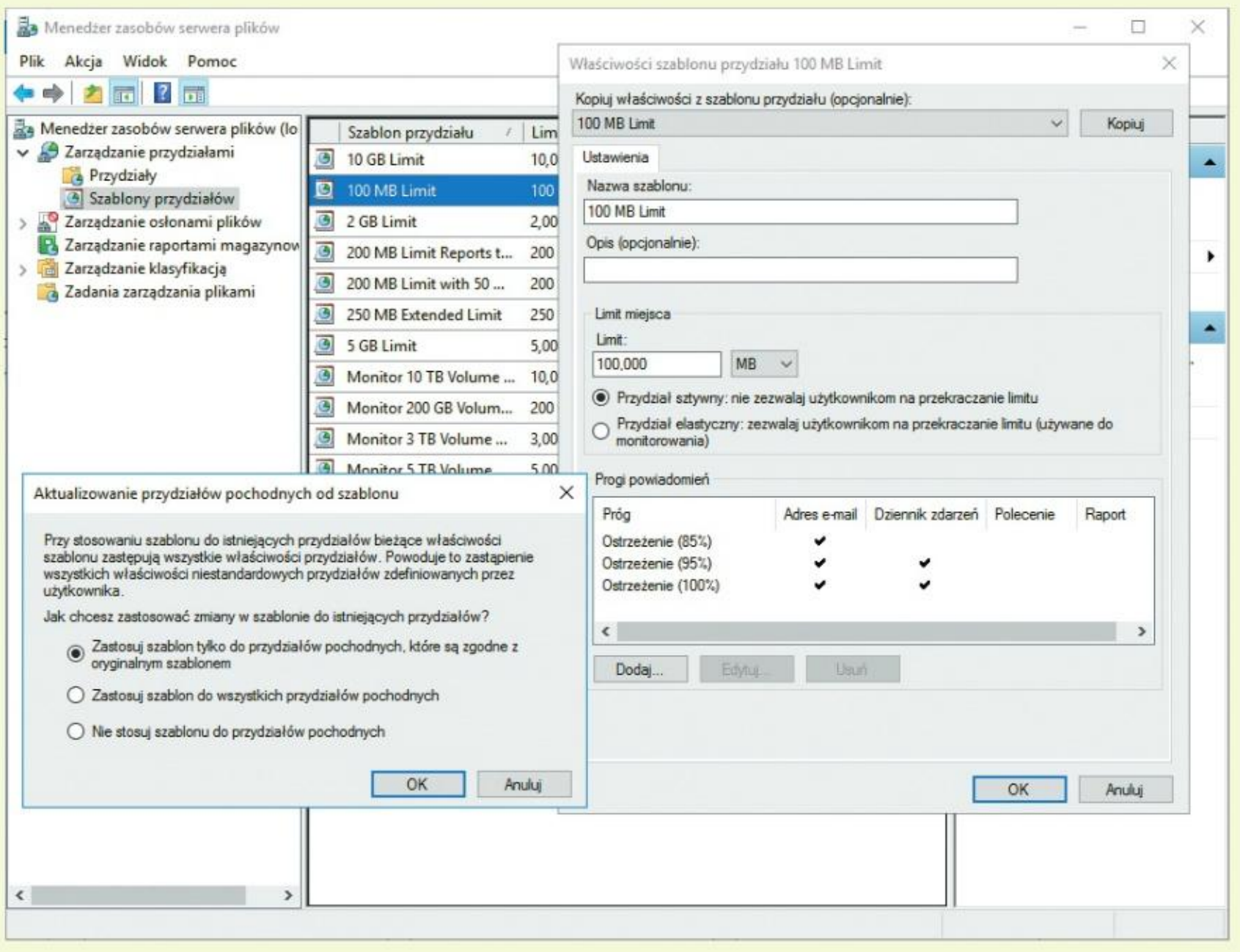
Konfigurowanie Quoty za pomocą usługi Menedżer zasobów serwera plików

W tym przykładzie za pomocą Quoty zostanie ograniczona ilość przestrzeni dyskowej dostępnej dla użytkownika w wybranym folderze. Przykładowo, użytkownik *uczen2* uzyska prawo do 100 MB przestrzeni dyskowej w wybranym folderze, np. **`C:\Udostępniony`**. Po przekroczeniu 85 MB zostanie wygenerowane ostrzeżenie wysłane za pomocą adresu e-mail, a po przekroczeniu 95 MB informacja zostanie również umieszczona w dzienniku zdarzeń. Aby skonfigurować mechanizm Quoty, należy:

1. Uruchomić **`Menedżer zasobów serwera plików`**. W oknie **`Menedżer serwera`** wybrać z menu polecenia **`Narzędzia/File Server Resource Manager`**.
2. Rozwinąć gałąź **`Zarządzanie przydziałami/Szablony przydziałów`** (rys. 48.11).
3. Wybrać (przez dwukrotne kliknięcie) lub utworzyć nowy szablon przydziałów. Parametry w szablonie, np. limit lub progi ostrzeżeń, można zmodyfikować według potrzeb (rys. 48.12). Kliknąć przycisk **`OK`**.

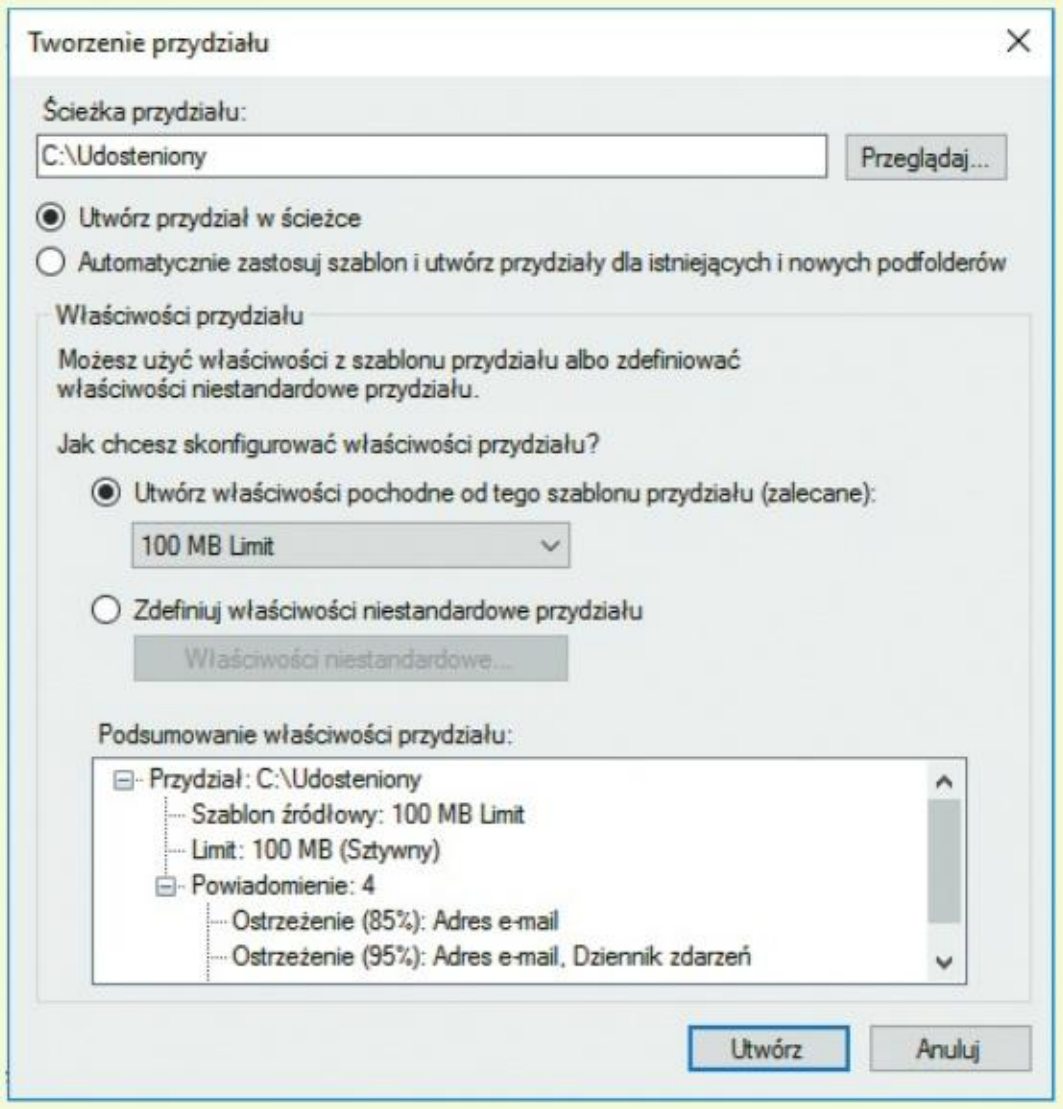


Rys. 48.11. **Wybieranie szablonu przydziałów**



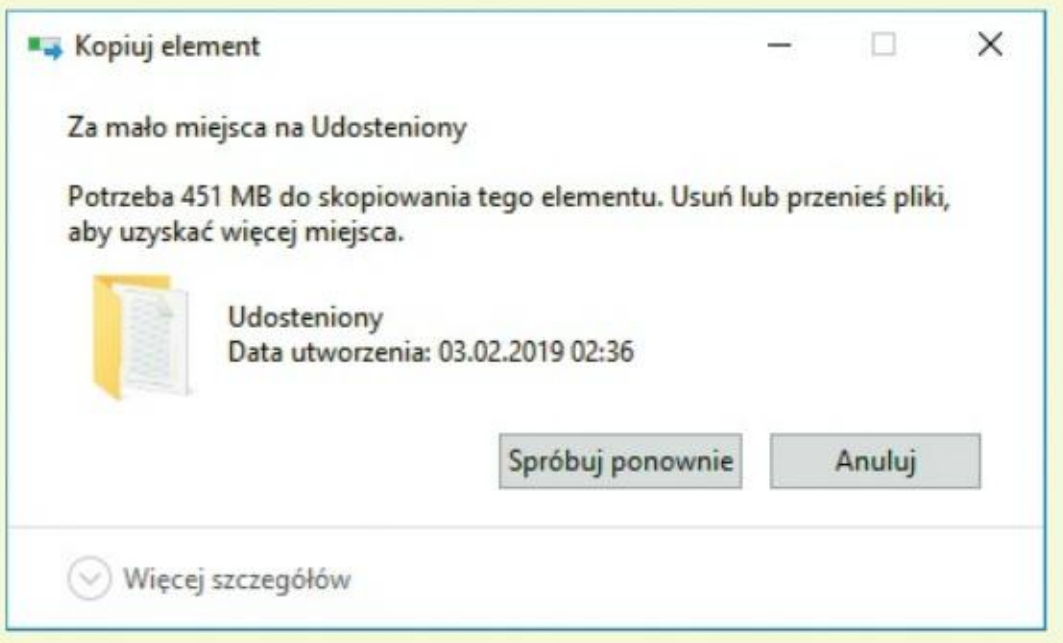
Rys. 48.12. **Modyfikowanie szablonu przydziałów**

4. W oknie **Aktualizowanie przydziałów pochodnych od szablonu** pozostawić wartość domyślną **Zastosuj szablon tylko do przydziałów pochodnych**, które są zgodne z oryginalnym szablonem. Kliknąć przycisk **OK**.
5. Zdefiniować nowy przydział. Kliknąć prawym przyciskiem myszy **Przydziały** i z menu podręcznego wybrać **Utwórz przydział**.
6. W oknie **Tworzenie przydziału** wskazać ścieżkę do folderu, np. **C:\Udostępniony**, i wybrać limit z szablonu, np. **100 MB Limit** (rys. 48.13). Kliknąć przycisk **Utwórz**.



Rys. 48.13. **Tworzenie przydziału**

7. Sprawdzić na liście, czy przydział został utworzony poprawnie.
8. Przetestować działanie usługi. Podczas próby skopiowania danych, których rozmiar przekracza limit, jest generowany komunikat o błędzie (rys. 48.14).



Rys. 48.14. **Komunikat o błędzie przekroczenia limitu przydziału**

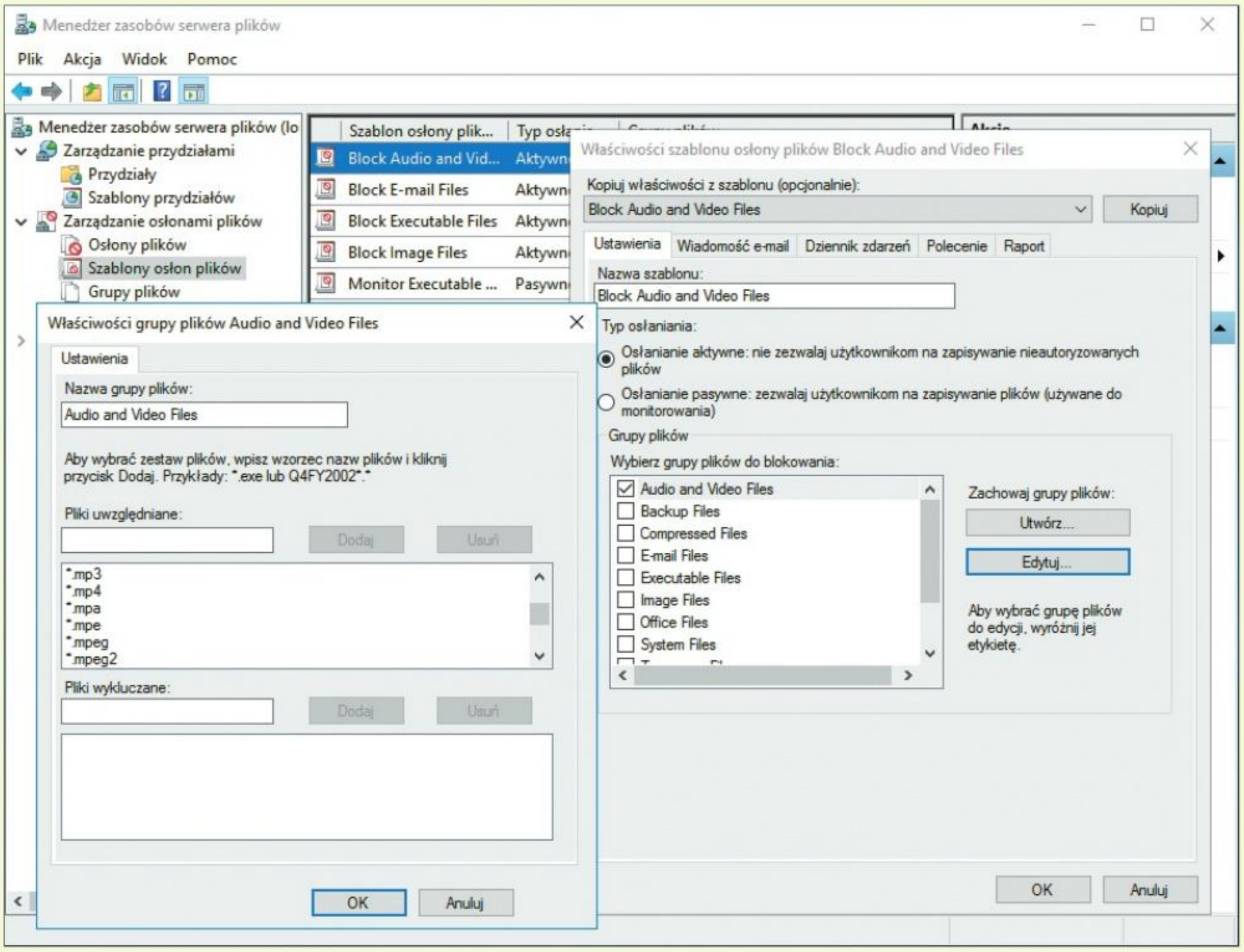
Osłona plików umożliwia kontrolę typów plików, które użytkownik może przechowywać na serwerze plików.

PRZYKŁAD 48.7

Konfigurowanie osłony plików za pomocą usługi Menedżer zasobów serwera plików

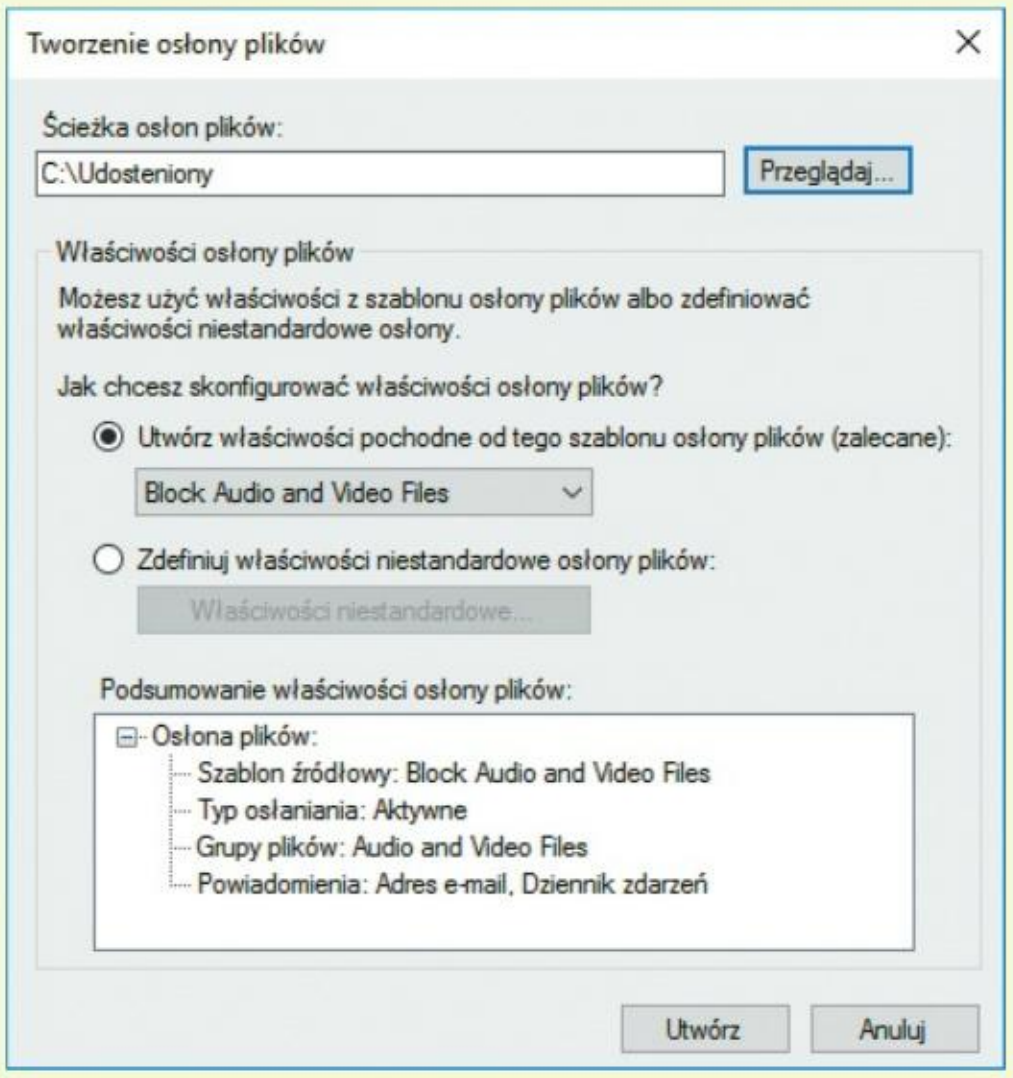
W tym przykładzie za pomocą osłony plików zostanie ograniczona możliwość przechowywania plików określonego typu, np. zawierających utwory audio i video. Aby skonfigurować osłony plików, należy:

1. Uruchomić **Menedżer zasobów serwera plików**. W oknie **Menedżer serwera** wybrać z menu polecenia **Narzędzia/File Server Resource Manager**.
2. Rozwinąć gałąź **Zarządzanie osłonami/Szablony osłon plików** (rys. 48.15).



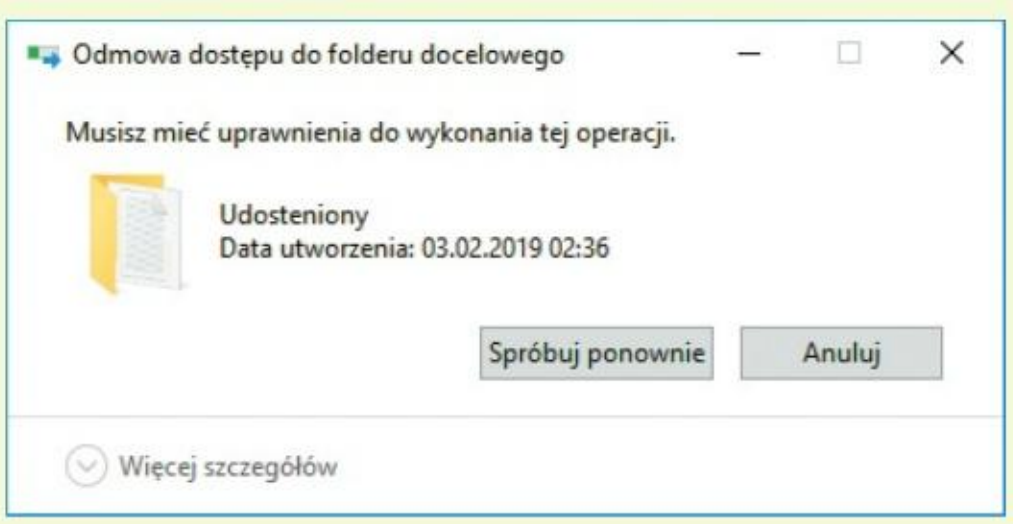
Rys. 48.15. **Modyfikowanie szablonu przydziałów**

3. Wybrać (przez dwukrotne kliknięcie) lub utworzyć nowy szablon osłon plików. W szablonie można wybrać typy plików, np. **Audio and Video Files**, i wskazać rozszerzenia nazw plików związane z danym typem. Kliknąć przycisk **OK**.
4. W oknie **Aktualizowanie przydziałów pochodnych od szablonu** pozostawić wartość domyślną **Zastosuj szablon tylko do przydziałów pochodnych**, które są zgodne z oryginalnym szablonem. Kliknąć przycisk **OK**.
5. Zdefiniować nową osłonę plików. Kliknąć prawym przyciskiem myszy **Osłony plików** i z menu podręcznego wybrać **Utwórz osłonę plików**.
6. W oknie **Tworzenie osłony plików** wskazać ścieżkę do folderu, np. **C:\Udostępniony**, i wybrać sposób działania osłony plików, np. **Block Audio and Video Files** (rys. 48.16). Kliknąć przycisk **Utwórz**.



Rys. 48.16. **Tworzenie osłony plików**

7. Sprawdzić na liście, czy przydział został utworzony poprawnie.
8. Przetestować działanie usługi. Podczas próby skopiowania danych, np. plików z rozszerzeniem mp3, jest generowany komunikat o błędzie (rys. 48.17).



Rys. 48.17. **Komunikat o błędzie naruszenia osłony plików**

48.4. Zapewnienie integralności danych

Dane, np. przesyłane przez sieć komputerową lub zapisane na dysku, mogą być zmienione, zarówno przez przypadkowy błąd podczas transmisji, jak i w wyniku celowych działań związanych z atakiem. **Integralność danych** to właściwość, która gwarantuje, że dane nie zostaną zmodyfikowane w sposób inny niż przez celowe działanie uprawnionej osoby. Narzędziem pozwalającym zapewnić integralność danych są **funkcje skrótu** (ang. *hash function*), zwane także funkcjami haszującymi.

Funkcja skrótu to algorytm przetwarzający wiadomości dowolnej długości w celu wygenerowania skrótu o stałej długości. Taki skrót powinien mieć następujące właściwości:

- odwrócenie skrótu nie jest w praktyce możliwe, tzn. na podstawie skrótu nie jest możliwe odtworzenie oryginalnej wiadomości;
- niemożliwa jest zmiana danych źródłowych bez zmiany skrótu;
- odnalezienie dwóch plików o tej samej wartości skrótu jest obliczeniowo bardzo trudne (tzw. silna bezkolizyjność);

- możliwe jest jednak istnienie dwóch takich samych skrótów odnoszących się do różnych wiadomości. Taka sytuacja jest nazywana **kolizją**. Znalezienie jakiejkolwiek wiadomości, której skrót byłby tożsamy ze skrótem innej wiadomości (tzw. bezkolizyjność słaba), jest również obliczeniowo bardzo trudne.

> **! UWAGA**
>
> Zadanie obliczeniowo bardzo trudne oznacza, że próba przeprowadzenia ataku typu *brute force* (o bardzo dużej liczbie możliwych kombinacji), przy obecnym poziomie technologicznym i w rozsądnym czasie, ma w praktyce prawdopodobieństwo sukcesu bliskie zeru.

Istnieje wiele funkcji skrótu, ale najpopularniejsze korzystają z dwóch typów algorytmów: MD (ang. *Message Digest*) i SHA (ang. *Secure Hash Algorithm*). **MD5** powstał w 1991 r. i obecnie nie jest uważany za bezpieczny. Zamiast niego zaleca się używanie funkcji skrótów z rodziny SHA. **SHA** jest zestawem algorytmów zaprojektowanych przez NSA (ang. *National Security Agency*). Algorytmy SHA-0 i SHA-1 obecnie również nie są uważane za bezpieczne. SHA-2 występuje w kilku wersjach bitowych: 256, 384 i 512 (ta wersja jest obecnie standardem powszechnie używanym w internecie).

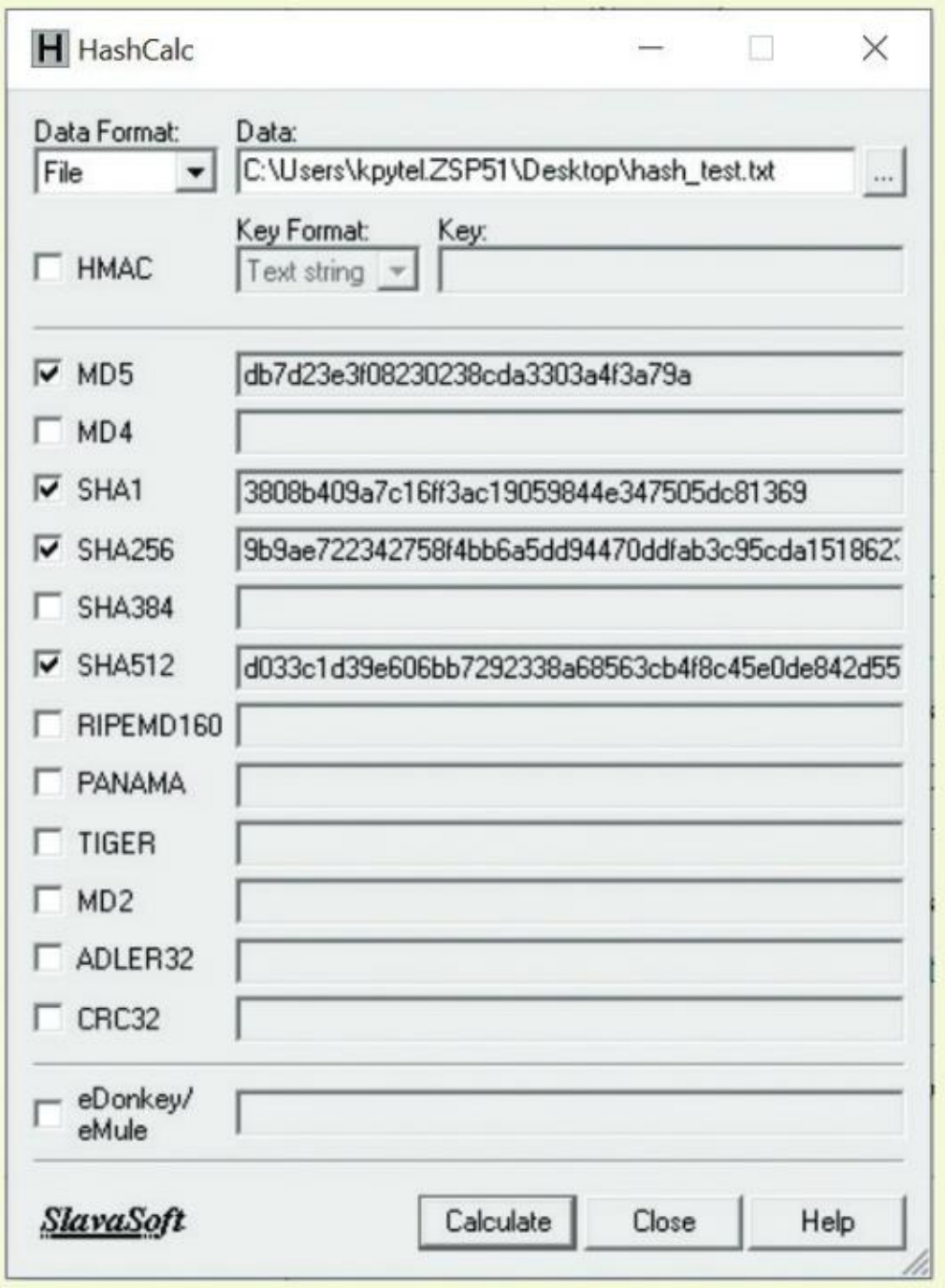
Do obliczenia funkcji skrótu można wykorzystać moduły wbudowane w wiele aplikacji typu **`Menedżer plików`** lub wyspecjalizowane aplikacje, np. **HashCalc**, dostępny na stronie https://www.slavasoft.com/download.htm.

PRZYKŁAD 48.8

Obliczanie wartości funkcji skrótu

W tym przykładzie zostanie zainstalowany program HashCalc do obliczania wartości funkcji skrótu. Program będzie wykorzystany do wykrycia modyfikacji w pliku użytkownika. Aby wykonać zadanie, należy:

1. Pobrać ze strony https://www.slavasoft.com/download.htm plik instalacyjny programu i zapisać na dysku. Wypakować plik z archiwum.
2. Uruchomić plik **`setup.exe`** i przeprowadzić instalację programu.
3. Utworzyć plik tekstowy, np. **`hashtest.txt`** zawierający tekst „Ala ma kota".



Rys. 48.18. **Obliczanie funkcji skrótu dla pliku `hashtest.txt`**

4. Uruchomić program HashCalc. W oknie **`Data Format:`** ustawić **`File`**, a w pole **`Data:`** wprowadzić ścieżkę do pliku **`hashtest.txt`**. Wybrać funkcje, np. MD5, **`SHA-1`**, **`SHA-256`**, **`SHA-512`** (rys. 48.18). Kliknąć przycisk **`Calculate`**. Zanotować wartości obliczonych funkcji.
5. Zmodyfikować plik **`hashtest.txt`**. Zamienić tekst na „Ala ma psa".
6. Ponownie obliczyć wartości funkcji skrótu. Porównać wyniki przed modyfikacją pliku i po niej.

Niektóre strony w internecie, np. oferujące pliki do instalacji systemów operacyjnych lub programów, oprócz plików zawierają również wartości funkcji skrótu dla plików. Użytkownik po pobraniu pliku może samodzielnie obliczyć wartość funkcji skrótu i porównać je z wartością na stronie. Jeżeli wartości są identyczne, to oznacza, że plik nie uległ modyfikacji podczas przesyłania.

! UWAGA

Należy pobierać pliki tylko z zaufanych stron. Kontrola integralności nie przyniesie korzyści w przypadku, gdy plik był już wcześniej zmodyfikowany przed opublikowaniem na stronie internetowej. Wartość funkcji skrótu może w takim wypadku wskazywać np. na plik z wirusem lub innym niechcianym oprogramowaniem.

PRZYKŁAD 48.9

Wykorzystanie funkcji skrótu do sprawdzenia poprawności pobierania pliku z internetu

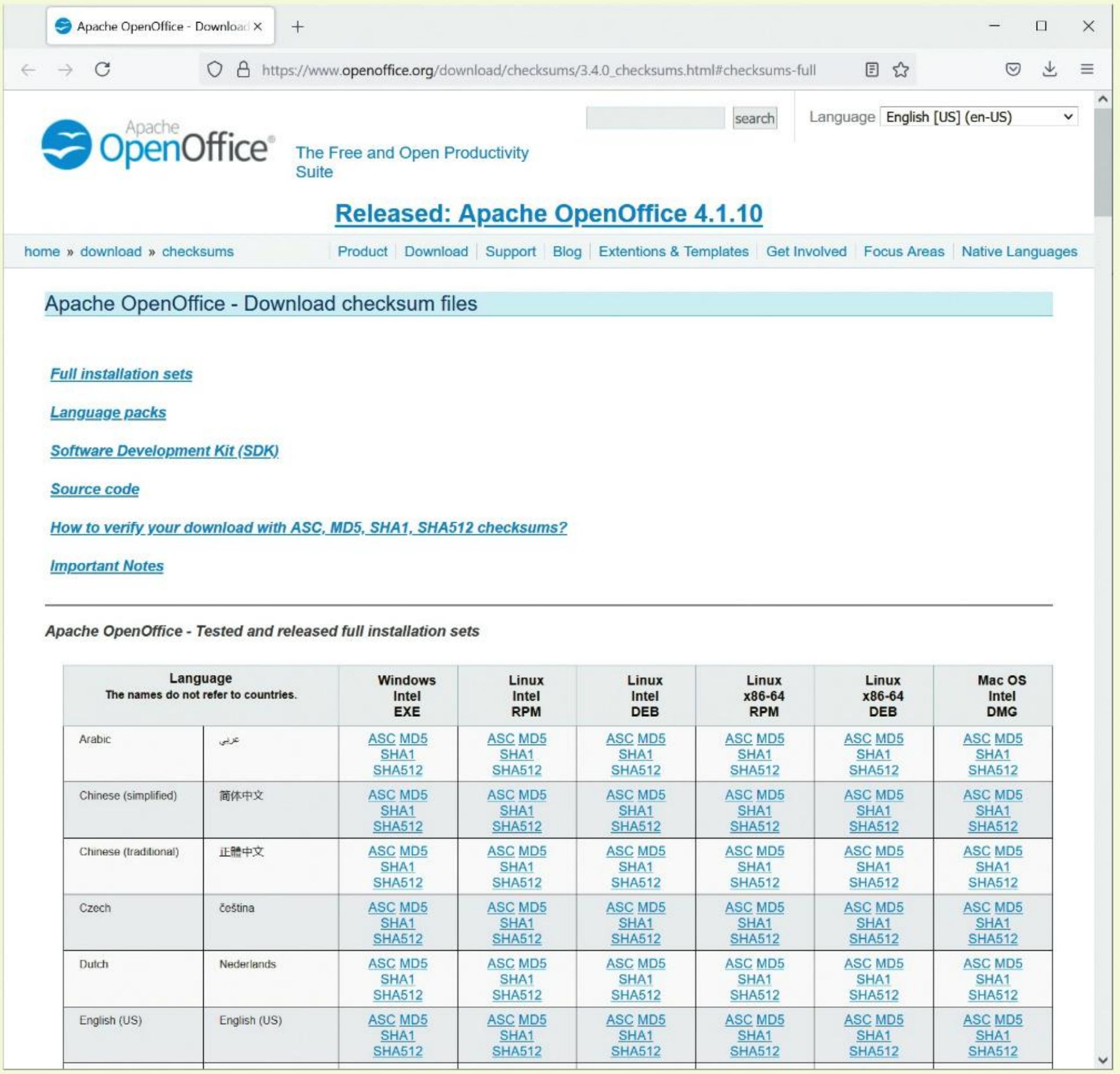
W tym przykładzie zostanie przeprowadzona weryfikacja, czy plik pobrano poprawnie z zachowaniem zasad integralności. Aby wykonać zadanie, należy:

1. Odszukać w internecie stronę z wersjami instalacyjnymi wybranego oprogramowania, np. OpenOffice (rys. 48.19) na stronie https://www.openoffice.org/download/checksums/3.4.0_checksums.html#checksums-full.
2. Pobrać plik instalacyjny wybranej wersji oprogramowania, np. **`Windows Intel EXE`**.
3. Otworzyć odnośnik do wybranej funkcji skrótu, np. **`SHA1`**. Zapisać w notatniku wartość skrótu.
4. Obliczyć wartość skrótu dla pobranego pliku. Porównać z wartością pobraną ze strony.
5. Jeżeli wartości są identyczne, to oznacza spełnienie warunku integralności pobieranego pliku.

! UWAGA

Funkcje skrótu są również wykorzystywane do kontroli integralności danych przesyłanych w sieciach, np. sieciach VPN. W takim wypadku strumień danych jest dzielony na fragmenty o stałej długości, a następnie dla każdego fragmentu jest obliczana wartość funkcji skrótu.

Kolejnym obszarem, w którym są wykorzystywane funkcje skrótu, jest podpis cyfrowy dokumentów elektronicznych. Taki podpis gwarantuje zarówno integralność dokumentu, jak i uwierzytelnienie tożsamości osoby podpisującej (do uwierzytelniania wykorzystuje się inny mechanizm).



Rys. 48.19. **Strona pobierania programu OpenOffice**

48.5. Szyfrowanie danych

Dane przesyłane w sieci mogą zostać przechwycone przez nieuprawnionych użytkowników. **Szyfrowanie danych** zapewnia, że bez znajomości klucza kryptograficznego odczytanie zaszyfrowanych danych będzie niemożliwe. Szyfrowanie polega na przekształceniu wiadomości (nazywanej **tekstem jawnym**) w inną postać (nazywaną **tekstem tajnym**) za pomocą **algorytmu szyfrującego**. Za bezpieczeństwo procesu odpowiada **klucz szyfrowania**.

> **! UWAGA**
>
> Zauważ, że algorytm szyfrowania jest znany (szczegółowe opisy i gotowe implementacje są dostępne w internecie). Tekst jawny i tajny jest znany – każdy może utworzyć dowolny tekst i przy pomocy dostępnego algorytmu szyfrowania wygenerować tekst tajny.

Wyróżnia się algorytmy szyfrowania z kluczem symetrycznym lub kluczem asymetrycznym. W szyfrowaniu z **kluczem symetrycznym** klucz szyfrujący może być wyznaczony z klucza deszyfrującego, a klucz deszyfrujący wyznaczony z klucza szyfrującego. W najprostszym przypadku używa się tego samego klucza do szyfrowania i deszyfrowania, np. algorytmy **DES**, **3DES**, **AES**. Szyfrowanie symetryczne nie pozwala na jednoznaczne ustalenie, która ze stron jest autorem wiadomości – obie strony znają ten sam klucz, który może być wykorzystany do szyfrowania.

W szyfrowaniu z **kluczem asymetrycznym** istnieje para wzajemnie powiązanych kluczy. Klucz szyfrujący (**klucz publiczny**) jest inny niż klucz deszyfrujący (**klucz prywatny**), a ponadto nie można wyznaczyć klucza deszyfrującego z klucza szyfrującego i na odwrót. Przykładem takiego algorytmu jest **RSA**. Do szyfrowania wiadomości używa się klucza publicznego odbiorcy – tylko odbiorca wiadomości mający odpowiedni klucz prywatny będzie mógł taką wiadomość odczytać. W takim przypadku możliwe jest zapewnienie **poufności** wiadomości. Jeżeli do zaszyfrowania wiadomości zostanie wykorzystany klucz prywatny, to do jej odczytania należy wykorzystać klucz publiczny tego użytkownika – ten jest powszechnie znany, więc każdy może taką wiadomość odczytać. W tym przypadku nie może być mowy o poufności wiadomości, ale skoro do szyfrowania użyto klucza prywatnego, to autorem wiadomości może być tylko właściciel tego klucza. Uzyskuje się w ten sposób **niezaprzeczalność** autorstwa wiadomości. Obie metody mogą być łączone, np. wykonując podwójne szyfrowanie, szyfrowanie kluczem prywatnym zapewnia niezaprzeczalność autorstwa, a szyfrowanie kluczem publicznym odbiorcy – poufność wiadomości.

Poczta elektroniczna pozwala na dołączenie do korespondencji plików w postaci załączników. Aby zachować bezpieczeństwo danych, należy zaszyfrować załączniki, aby uniemożliwić ich odczytanie nieupoważnionym użytkownikom. Do szyfrowania poczty można wykorzystać program **Gpg4win**, dostępny na stronie https://www.gpg4win.org/.

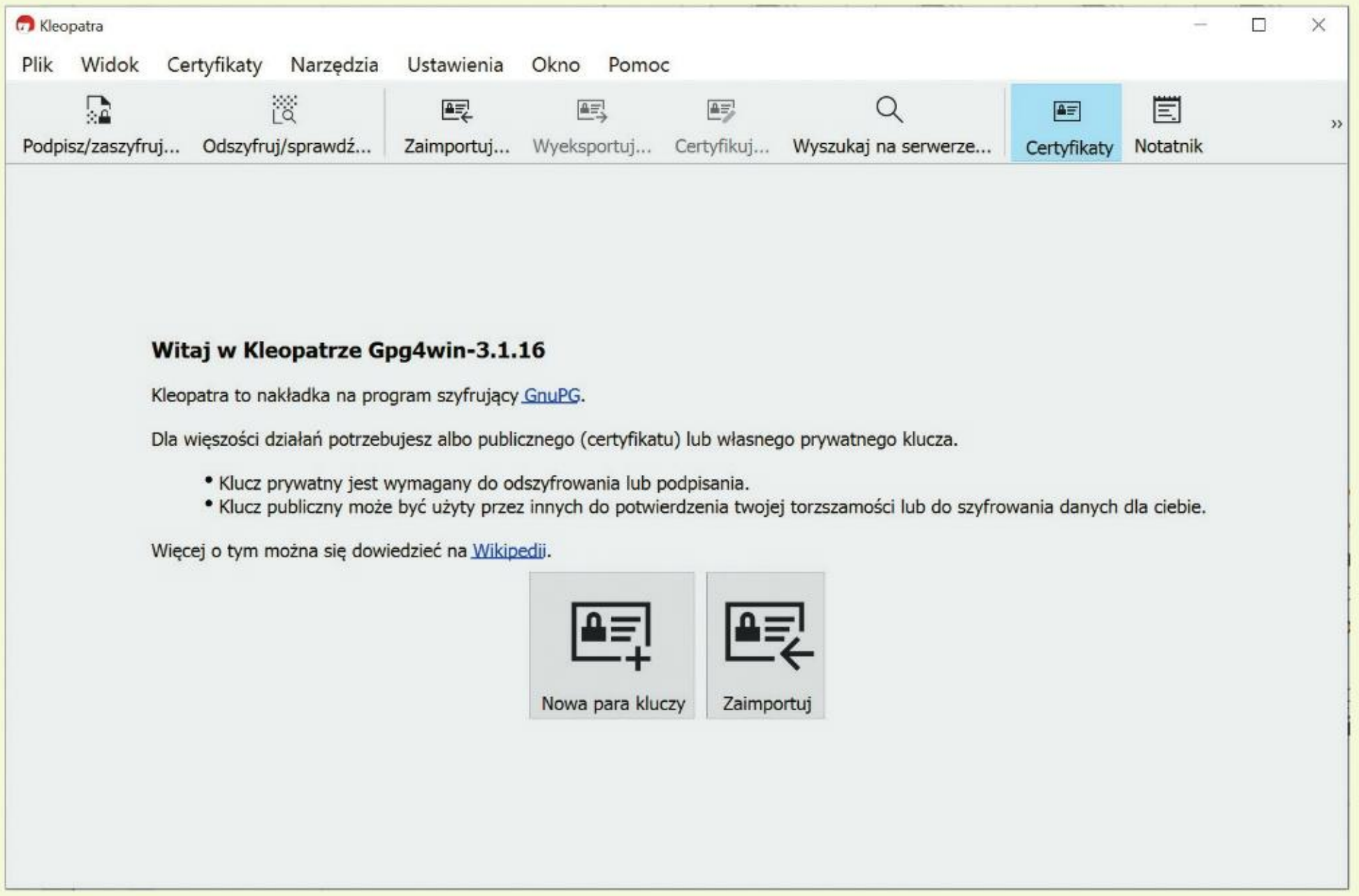
PRZYKŁAD 48.10

Instalowanie programu Gpg4win wraz z nakładką Kleopatra

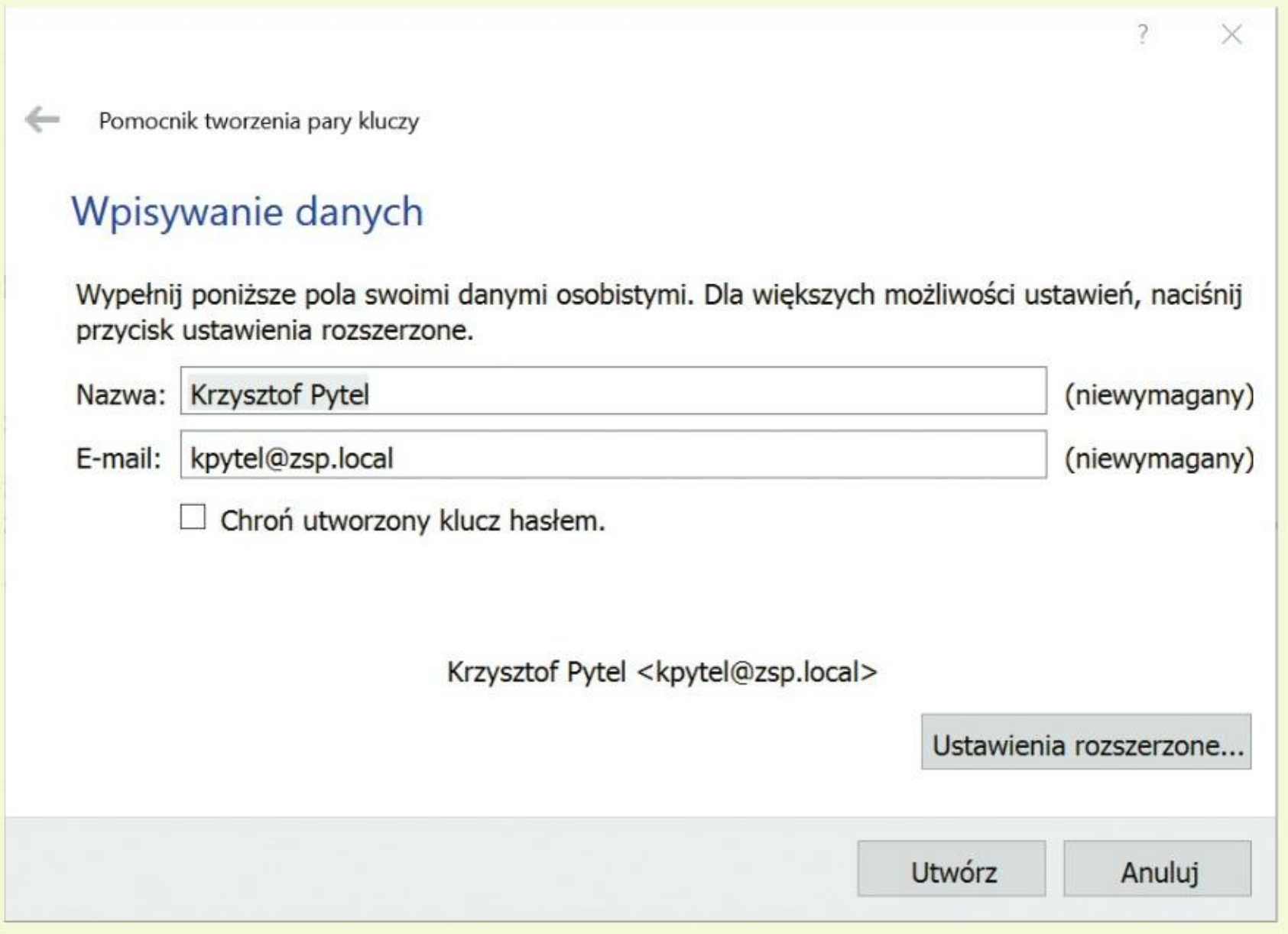
W tym przykładzie zostanie zainstalowany i skonfigurowany program Gpg4win.

Aby wykonać zadanie, należy:

1. Pobrać program, np. ze strony https://www.gpg4win.org/, i wykonać procedurę instalacji. Podczas instalacji zainstalować również nakładkę **`Kleopatra`**.
   Po zakończeniu instalacji uruchomić **`Kleopatrę`** (rys. 48.20).
2. Wygenerować klucz prywatny i publiczny. Kliknąć przycisk **`Nowa para kluczy`**.
3. Wprowadzić dane osobiste użytkownika (rys. 48.21). Kliknąć przycisk **`Utwórz`**, a następnie **`Zakończ`**.
4. Wyeksportować klucz publiczny. Wskazać użytkownika i kliknąć przycisk **`Wyeksportuj`**. Wskazać nazwę i lokalizację pliku z kluczem. Kliknąć przycisk **`Zapisz`**. Przykładowy plik z kluczem przedstawiono na rys. 48.22.
5. Plik z kluczem publicznym można opublikować na stronie internetowej, umieścić na specjalnym serwerze z kluczami lub inną metodą przekazać wszystkim zainteresowanym.
6. Zaimportować klucz publiczny innego użytkownika. Kliknąć przycisk **`Zaimportuj`** i wskazać plik z kluczem. Oznaczyć certyfikat jako ważny – kliknąć przycisk **`Tak`**, a następnie **`Certyfikuj`**.
7. Sprawdzić, czy klucz publiczny został dodany (rys. 48.23).



Rys. 48.20. **Okno startowe nakładki `Kleopatra`**



Rys. 48.21. **Wprowadzanie danych osobistych użytkownika**

Krzysztof Pytel_public.asc — Notatnik

Plik Edycja Format Widok Pomoc

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGDlsH8BDADSP4N4PdTOgSOqpFlvK6KGhFFbrAcVdKXNAHvF/rczBK/S6Yj9
On+EbfEMey7ejP2UcfQECiM/3xOxvGBpPOFb2Yx5VvxF4iW3e1NLerV2h2t4LSwq
vvLleN9aNq9iA3qqzW0wOZ0cS4GfYI3lrgkdySKjoJ/AQ9CZq7q88+tkBuY8xsgd
+LnYQUvK0kE8odjxUqhQqDt9A+dZLhsTF4w4TO68VNGzCqfZ0liQkIb3+0HDSA9e
kjf2+Bj6d8HFY+US4P3wH+TQWQxIcHE3dIYKHzwYi+Q8xuaMzsjZvwNDqmpjz/ti
qeebGV4GtPUDYiEp6tXJGSAjewj2MhpfMqzeL1mSjxDaiQvOlIair/zFq7r/D1JQ
myVGsl39yVI3GqDmBXAyrAj3LUuzRO6cIVnG05YnLya9K5Z6wQks/LxMCDK5M7Aa
BCQq/arlmFgZISnP0f6Gi96il8T7D6F97g3srqfxYXGqeUgawtsaBLzs4oQ5Vr1I
QKPg0l4wJZ7Jz9kAEQEAAbQiS3J6eXN6dG9mIFB5dGVsIDxrcHl0ZWxAenNwLmxv
Y2FsPokB1AQTAQgAPhYhBIgI70goR/pB7yM7sUd+05Giq+zZBQJg5bB/AhsDBQkD
wjGhBQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEEd+05Giq+zZS6EL/2QhcooC
cCM1fUv10fn46EflSmn5Desi1JztZkocrBzeXGZAOF9t+t5ZLJ5rf9aUiMKmwTvd
I4l99SBpmioCGJ3BammzuyTd1sTd4WglCqfx1VH/19neLi7mFYfPlKmK2dvMJhfq
ibQmYG7vX7r/K7Dr5HpaLL5i/1KisBBLjjhxUNxKgm+f49oD89qiKz+7yGKVCBuL
YxS/MLCzc32rG8UBEw7vDi6XxDPu+BRXAwU3oxauGwLq5szbomi56gkOE1M22SVV
TNTnDLtbYkVskCyMZk4xT+MyvP5FF8FooTBG+1Kpr4xCBH2OG05OxPT6yNLbjrRa
WVpelarveMy7ITjyUV1msfMxjz7dTiyKegNrN4d7N4dt9zK555cD1w00Rm76071I
0+Fmqga8uI6+e2LxX5pHf7BBFRwd7Hfl4qGq7bT6pDPnngXQmu0gtr6DSedXSzXB
bzawfituAd86gvlQUT9hqW1PAZ0S5rsBEe4/ROpdOAGzlY5/9P69+KdsFLkBjQRg
5bB/AQwA4y3tQHtPgiXUo5ZUEuxlNxsBrjTWahm/TCwsJ2s5j15t3VgR0SgWnxeq
KPEowAytJes97/iQYaTNOJf2ofR8PsTa0dwSU6yjL76cCX2+bFGBjfkC3nCYZsa3
9nTcE0gQoPL8SgAqIZjiTMvIIP2T3iV3Zk34jI9J1N/1zB4XE8Ms0Ib1OH+r6dss
4GSIDbrMYfg2Chuu2aSq1tg6NBfgc53eieLRbrTrpLWp2acLiFkqC2JklVMuBb5C
zF911gotWb/C315figOFmJHaCp7KUiUiTG2UryE0at5hK5RQd/byZHx+7ePilWZn
S4YvKO37QghrA0EgJTTW3ok6UO+vxxcHpxKCNeEVUrwtBCdY8HBdbjF6C1M7nHq3
JoaGm920ZgqqtCzlahZIi9i1sfdeVCgftqR/Z8nOX3A29jDE6kAdHGvN0BHmGRgh
VTpXtvN5NXarKI4iCg6gZAyGDIv7JYfSdVF8EjPUXYejcid2CMFD1ygWiqOL/k87
vAVlHgaBABEBAAGJAbwEGAEIACYWIQSICO9IKEf6Qe8jO7FHftORoqvs2QUCYOWw
fwIbDAUJA8IxoQAKCRBHftORoqvs2ajoC/4wEHGmsY8RLoQCkfr50LGOoVRyoh3Z
wnA+PVl+yj2dlHD4LkTobRMJjaCy7Vn1pnS+yFBzHdrdBx6duBpeiQHk+G09q/IJ
UbhZ4UkYNUuci1i1J9x12RrXy312miXSvzmsA2/QTrYzI+7mrpzszNM++JDWw25f
l50Z+hfcF1OvzYTZbRKrw+ditJOPHTTI/9+KzhKz+Wq0pEVZls/0WUxSq9LGC+7f
5RylNFfHTOm1jn/UqRJvYGujFGmVsss2+OkL1EkPIfSFbKJvRDh88dnmfukoQB8m
t7MuXEted2X+/SOG8f9oyuaX4L+z7aEqmmczd1d+qMPnOW8n80SjMQuBw42Vs4aF
AjsP77wT0/9cNkel0K6IazfFvufvnNdF4b/Imi52e+vaUwfqWUjc48QRPwoEZQ46
pmdp2FjtsaQoySJzfH5H5KWGqkB1LnBAh0R6rIL2ZERMyGroK1z+t8b1aaNaG09r
xYw8bzUIX73sF1pT6QvySqErEZyKG3HUaAY=
=VlZh
-----END PGP PUBLIC KEY BLOCK-----
```

Lin 1, kol 1 | 100% | Windows (CRLF) | UTF-8

Rys. 48.22. **Przykładowy plik z kluczem publicznym**

Kleopatra

Plik Widok Certyfikaty Narzędzia Ustawienia Okno Pomoc

Podpisz/zaszyfruj... | Odszyfruj/sprawdź... | Zaimportuj... | Wyeksportuj... | Certyfikuj... | Wyszukaj na serwerze... | Certyfikaty | Notatnik | Karta inteligentna

Szukaj...<Alt+Q> | Wszystkie certyfikaty

Nazwa	E-mail	Identyfikatory użytkownika	Ważny od	Ważny do
Krzysztof Pytel	**kpytel@zsp.local**	**certyfikowane**	**07.07.2...**	**07.07.2...**
Sylwia Osetek	sosetek@zsp.local	certyfikowane	07.07.2021	07.07.2023

Rys. 48.23. **Lista kluczy w programie Kleopatra**

PRZYKŁAD 48.11

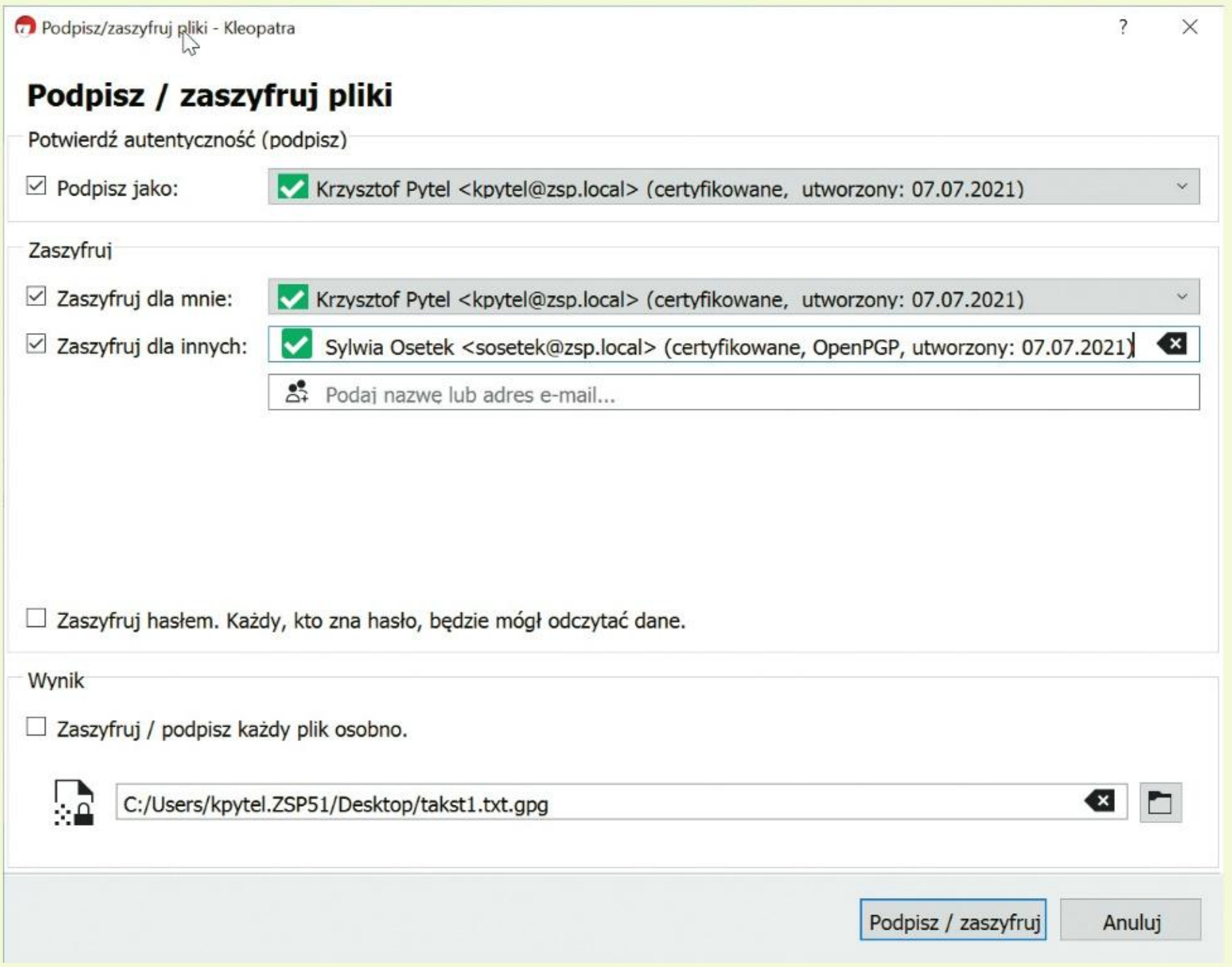
Szyfrowanie i deszyfrowanie wiadomości w programie Kleopatra

Aby zaszyfrować wiadomość za pomocą klucza publicznego użytkownika, należy:

1. Utworzyć plik, np. **`tekst1.txt`**, z wiadomością „Ala ma kota”.
2. Uruchomić program **`Kleopatra`**. Kliknąć przycisk **`Podpisz/zaszyfruj`** i wskazać plik do szyfrowania.
3. W oknie **`Podpisz/zaszyfruj plik`** wskazać odbiorcę wiadomości w polu **`Zaszyfruj dla innych`**. Kliknąć przycisk **`Podpisz/zaszyfruj`** (rys. 48.24). Po zakończeniu szyfrowania kliknąć przycisk **`Zakończ`**.

UWAGA

W polu **`Zaszyfruj dla innych`** można dodać tylko użytkowników, których klucz publiczny został wcześniej dodany. Pozostawienie opcji **`Podpisz jako`** spowoduje zaszyfrowanie pliku również kluczem prywatnym autora (niezaprzeczalność, zapewnienie autentyczności autora). Pozostawienie opcji **`Zaszyfruj dla mnie`** spowoduje zaszyfrowanie pliku również kluczem publicznym autora.

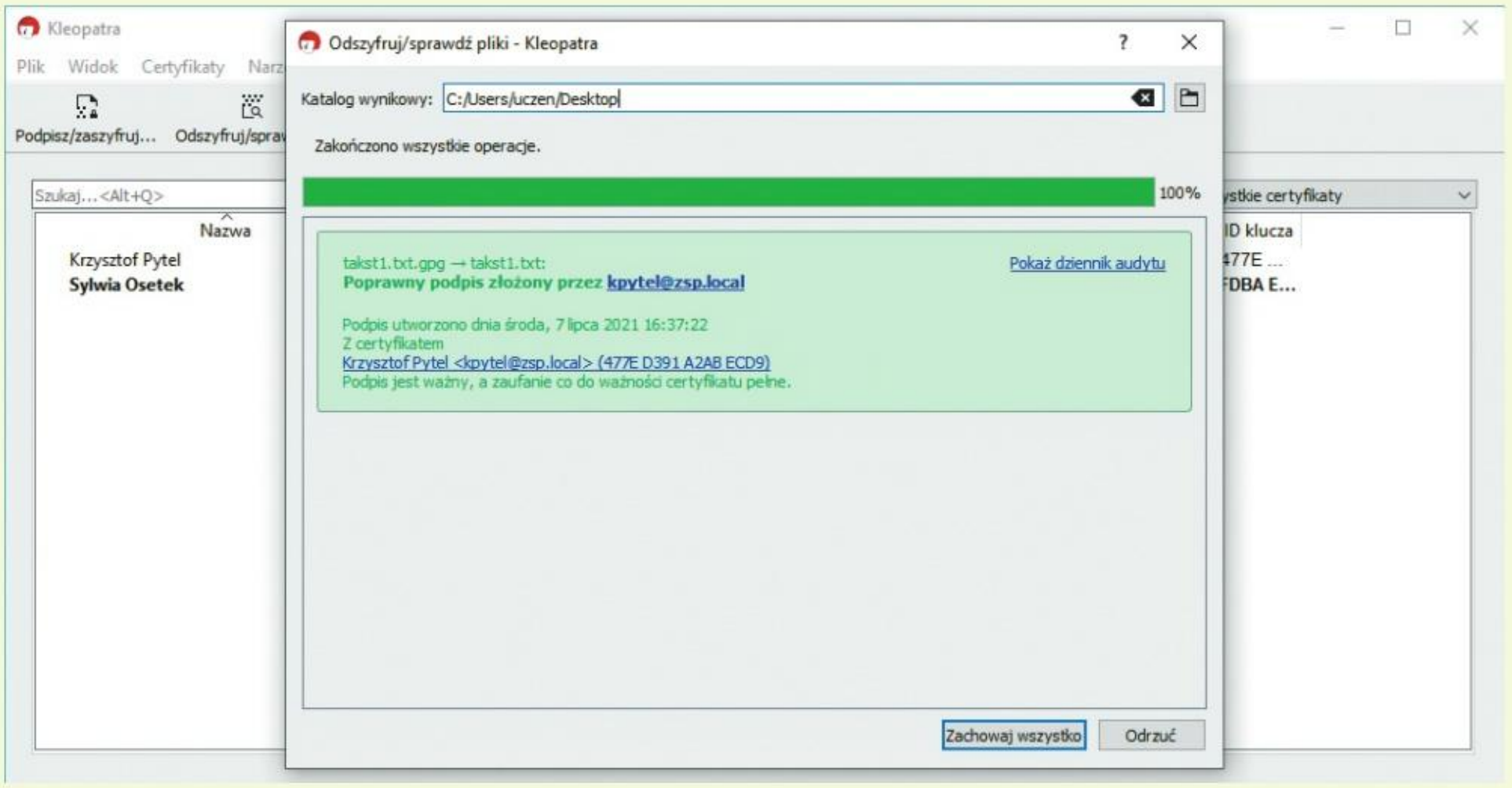


Rys. 48.24. **Szyfrowanie wiadomości**

4. Przesłać wiadomość do odbiorcy, np. przez e-mail.
5. Odszyfrować wiadomość na komputerze odbiorcy. Uruchomić program **Kleopatra**, kliknąć przycisk **Odszyfruj/sprawdź pliki** i wskazać zaszyfrowany plik (rys. 48.25). Kliknąć **Zachowaj wszystko**.

! UWAGA

Wiadomość można odszyfrować tylko na komputerze, na którym jest klucz prywatny odbiorcy. Weryfikacja autentyczności podpisu wymaga wcześniejszego zaimportowania klucza publicznego autora.



Rys. 48.25. **Odszyfrowanie wiadomości i weryfikacja podpisu autora**

6. Sprawdzić, czy we wskazanym folderze docelowym pojawił się odszyfrowany plik i czy jest możliwe odczytanie jego zawartości.

Szyfrowane mogą być również całe dyski. W systemie Windows do tego celu służy funkcja **BitLocker**. Pozwala ona na szyfrowanie dysków twardych i przenośnych, np. pendrive'a. Możliwość szyfrowania dysków przenośnych jest ważna w przypadku zapisywania na nich np. danych osobowych. Wiele firm wymaga, aby wszystkie nośniki mobilne, które opuszczają obszar przetwarzania danych w firmie, były zaszyfrowane.

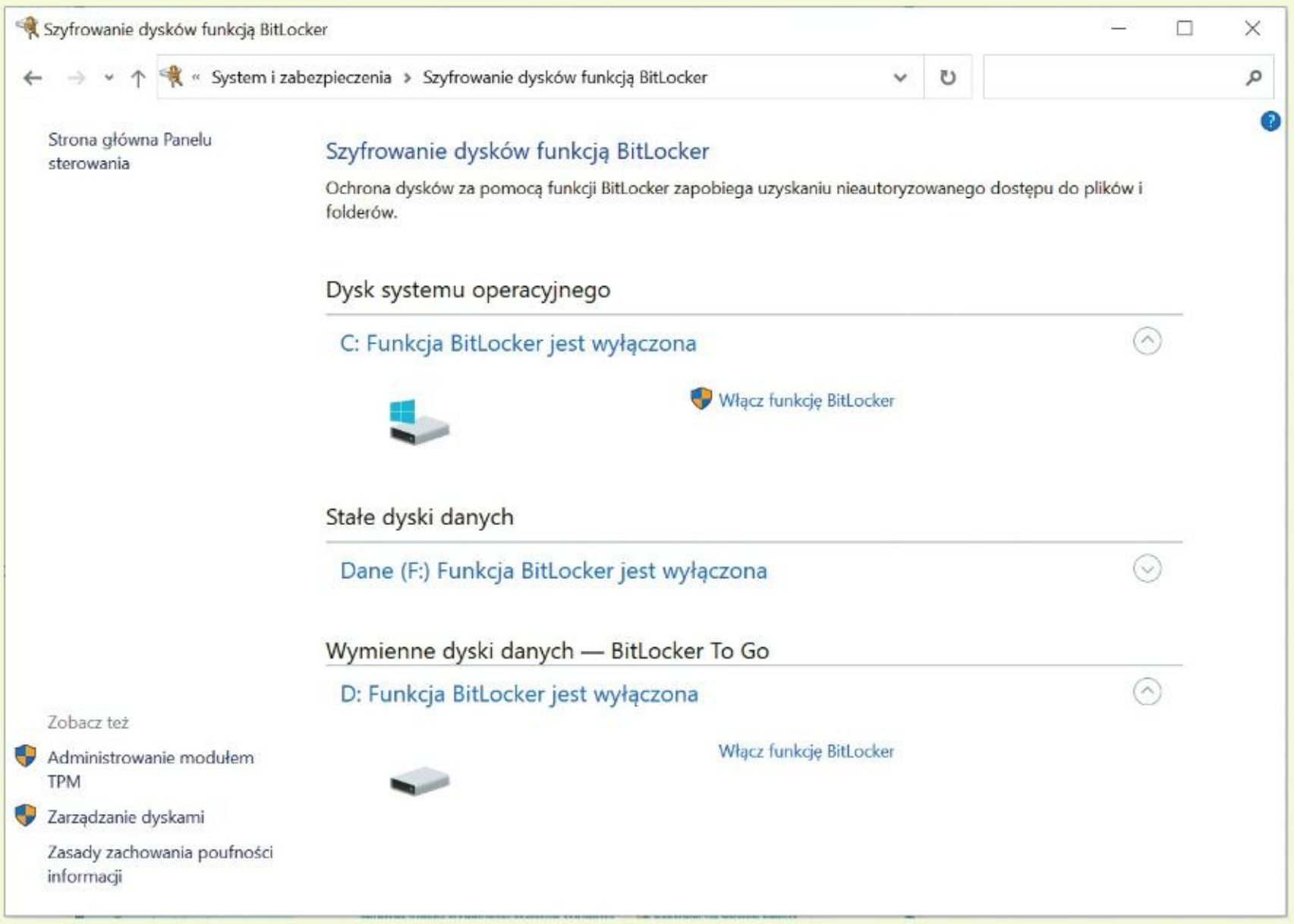
PRZYKŁAD 48.12

Szyfrowanie i deszyfrowanie dysku USB za pomocą BitLocker

Aby zaszyfrować dysk USB za pomocą funkcji BitLocker, należy:

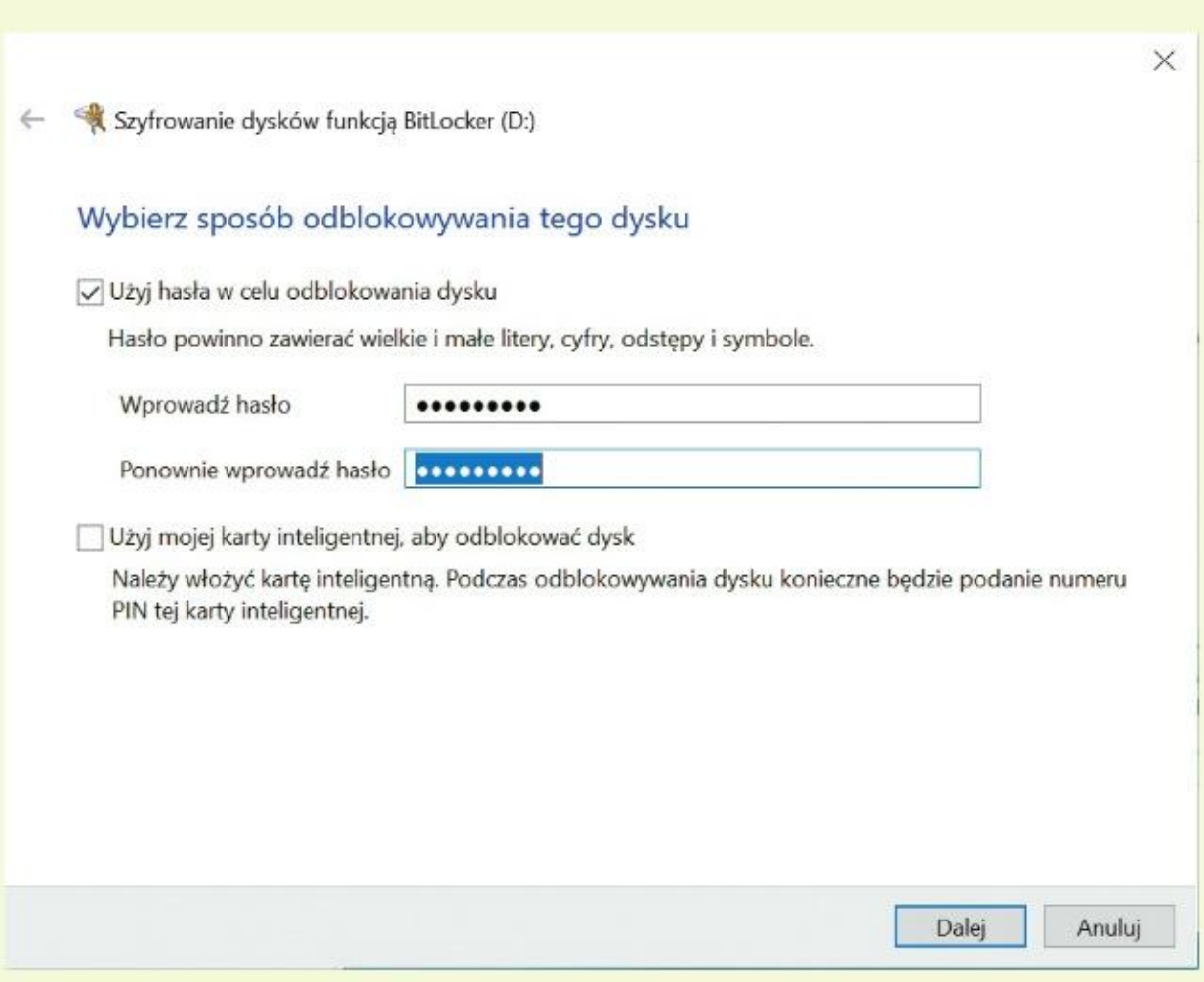
1. Podłączyć dysk USB do komputera i sprawdzić, czy zawiera zawartość do szyfrowania.

2. Uruchomić **Panel sterowania** (**Start/Panel sterowania**). W sekcji **System i zabezpieczenia** wybrać **Szyfrowanie dysków funkcją BitLocker** (rys. 48.26).



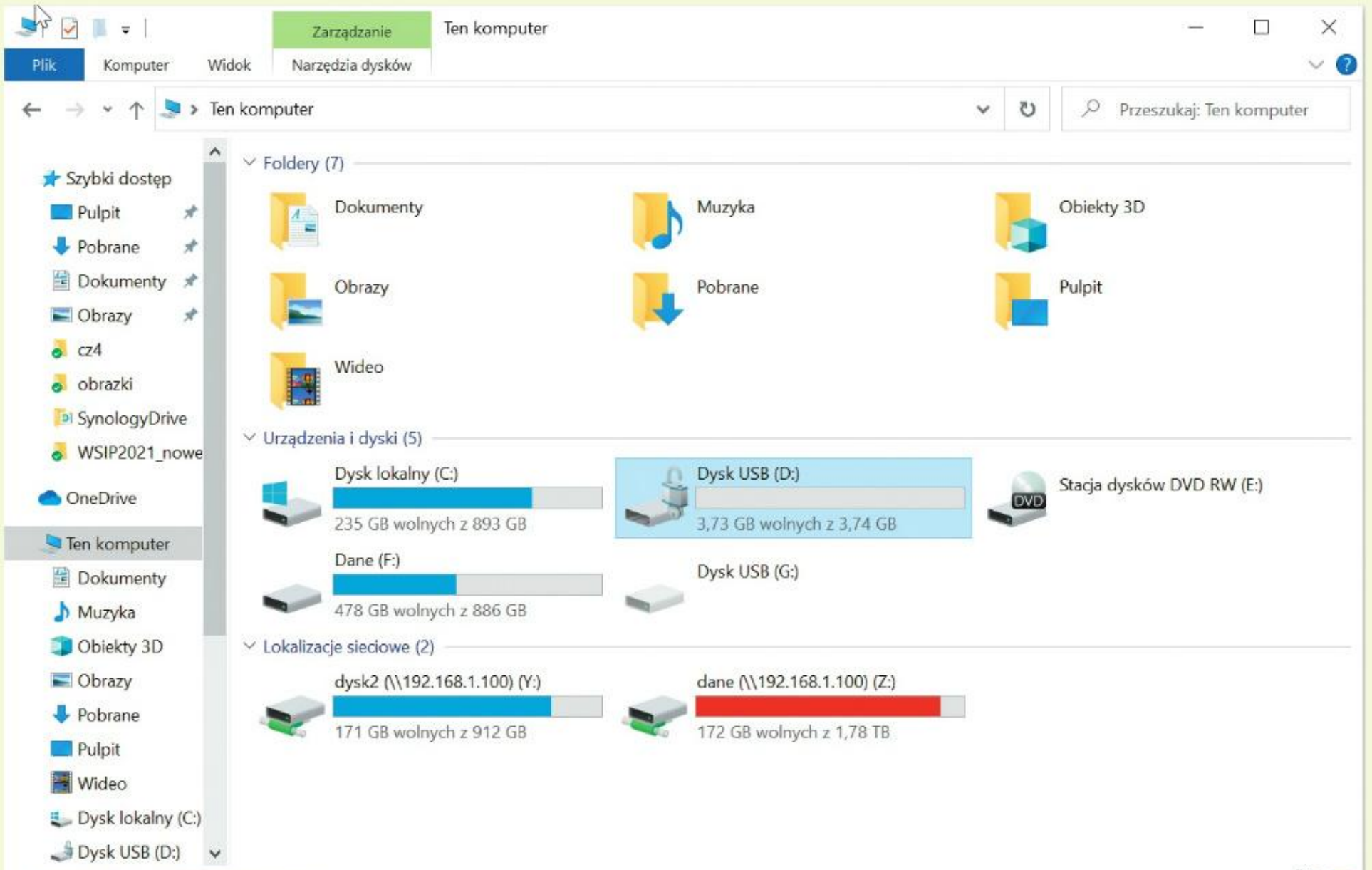
Rys. 48.26. **Okno Szyfrowanie dysków funkcją BitLocker**

3. Aktywować funkcję BitLocker dla dysku USB. Kliknąć odnośnik **Włącz funkcję BitLocker** w sekcji **Wymienne dyski danych – BitLocker To Go**.
4. Wybrać opcję **Użyj hasła w celu odblokowania dysku** i dwukrotnie wprowadzić hasło, np. *Qwerty123* (rys. 48.27). Kliknąć przycisk **Dalej**.



Rys. 48.27. **Wprowadzanie hasła funkcji BitLocker**

5. Wybrać sposób przechowywania kopii klucza odzyskiwania. Klucz pozwoli na odzyskanie danych z dysku w przypadku, gdy użytkownik zapomni hasła. Wybrać opcję **Zapisz w pliku**, wskazać lokalizację dla pliku i kliknąć przycisk **Zapisz**. Sprawdzić w lokalizacji, czy plik powstał.
6. Wybrać opcję **Zaszyfruj tylko zajęte miejsce na dysku**... Kliknąć przycisk **Dalej**.
7. Wybrać szyfrowanie w **Tryb zgodności**. Kliknąć przycisk **Dalej**. Kliknąć przycisk **Rozpocznij szyfrowanie**.
8. Po zakończeniu szyfrowania kliknąć przycisk **Zamknij**.
9. Sprawdzić możliwość uzyskania dostępu do dysku w oknie **Ten komputer** (rys. 48.28).

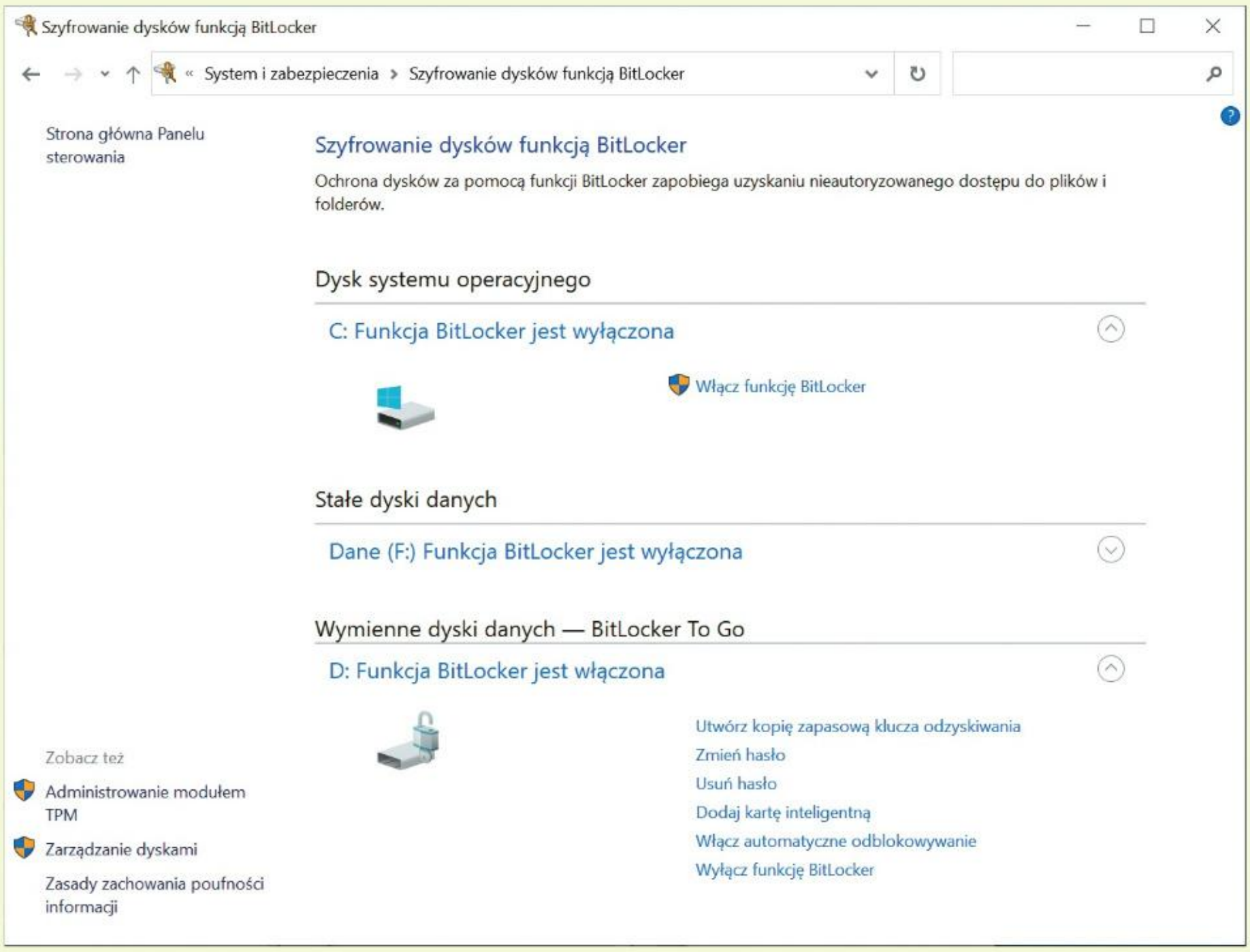


Rys. 48.28. **Zaszyfrowany dysk USB w oknie Ten komputer**

10. Kliknąć ikonę dysku i w oknie wprowadzić hasło (rys. 48.29).

Rys. 48.29. **Odblokowanie dostępu do dysku zaszyfrowanego funkcją BitLocker**

Do zarządzania zaszyfrowanym dyskiem można wykorzystać okno **Szyfrowanie dysków funkcją BitLocker** (rys. 48.30), uruchamianą przez **Start/Panel sterowania/System i zabezpieczenia/Szyfrowanie dysków funkcją BitLocker**.



Rys. 48.30. **Zarządzanie dyskiem zaszyfrowanym funkcją BitLocker**

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Sprawdź wersję programu antywirusowego w twoim komputerze.
2. Zaplanuj politykę bezpieczeństwa w twojej szkole:
   - politykę haseł;
   - zasady korzystania z urządzeń przenośnych.
3. Sporządź listę limitów przydziałów dyskowych dla użytkowników do poszczególnych partycji i folderów. Zaimplementuj system Quota wdrażający te zasady.
4. Sporządź listę plików, których nie wolno przechowywać na serwerze w katalogach udostępnianych. Zaimplementuj system osłon plików wdrażających te zasady.
5. Wyszukaj w internecie trzy przykładowe portale zawierające pliki instalacyjne wraz z wartościami funkcji skrótu.
6. Wyślij do koleżanki / kolegi e-mail z zaszyfrowanym plikiem. Odbierz i odczytaj plik wysłany przez koleżankę / kolegę.
7. Przygotuj pendrive do zapisywania poufnych danych. Pendrive powinien być szyfrowany funkcją BitLocker.
8. Wyszukaj w internecie procedurę uzyskiwania dostępu do zaszyfrowanego dysku za pomocą klucza odzyskiwania (w przypadku, gdy użytkownik zapomni hasła).

49 Rodzaje i dobór UPS

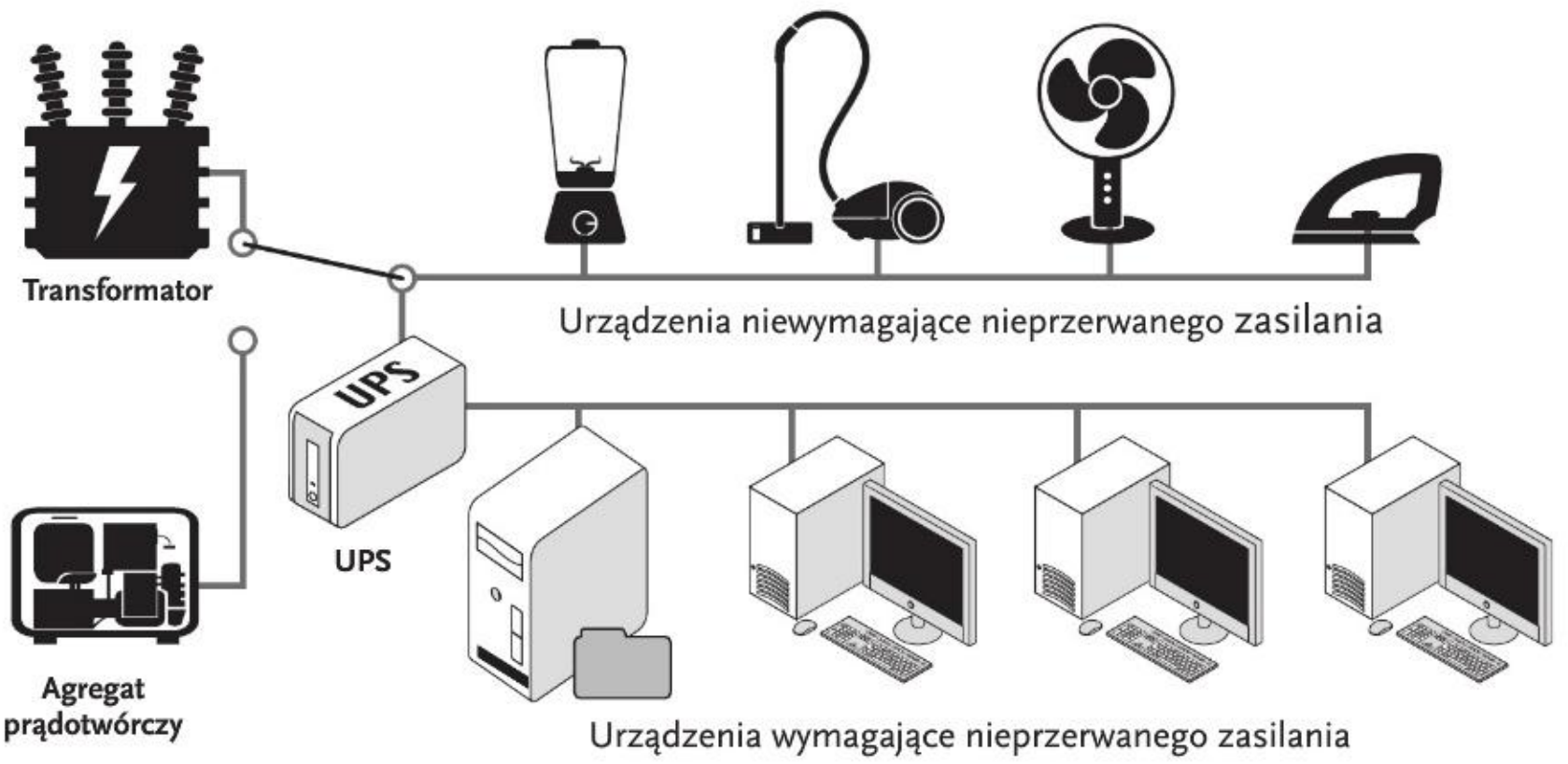
ZAGADNIENIA

- **Funkcje systemów UPS**
- **Rodzaje systemów UPS**
- **Dobór systemu UPS**

Jednym z elementów zapewnienia ciągłości i niezawodności pracy urządzeń komputerowych jest system awaryjnego zasilania energią elektryczną. To zadanie można rozwiązać różnymi sposobami, np. przez zasilacze awaryjne, agregaty prądotwórcze lub alternatywne zasilanie z kilku źródeł prądu.

Zasilacz UPS (zasilacz awaryjny) jest wtórnym źródłem energii elektrycznej, które prąd pobiera z wcześniej naładowanych akumulatorów. Czas podtrzymywania napięcia zależy od pojemności akumulatorów i obciążenia. Zasilacz awaryjny jest umieszczany między siecią energetyczną a chronionymi odbiornikami. Gdy zanika lub spada napięcie w instalacji elektrycznej, UPS natychmiast dostarcza napięcie, tak że komputer może pracować bez przerwy.

Agregat prądotwórczy to urządzenie elektroenergetyczne stanowiące samodzielne źródło prądu. Agregat składa się z silnika spalinowego i prądnicy oraz urządzeń kontrolno-pomiarowych umieszczonych na wspólnej konstrukcji. Agregat prądotwórczy charakteryzuje się dłuższym czasem włączania niż UPS, ale jego czas pracy nie jest uzależniony od pojemności akumulatorów. Agregat prądotwórczy może być zainstalowany przed zasilaczem UPS jako alternatywne źródło zasilania, na które jest przełączana instalacja zasilająca po awarii głównego źródła (rys. 49.1).



Rys. 49.1. Schemat instalacji zasilania awaryjnego

Aby zwiększyć niezawodność systemów zasilania, stosuje się **systemy zasilania z redundancją**. W najprostszym przypadku używa się dwóch agregatów prądotwórczych. W razie awarii jednego z nich drugi może kontynuować pracę. W centrach przetwarzania danych stosuje się podwójne układy dystrybucji prądu, w których energia jest dostarczana przez dwóch różnych dostawców energii lub z dwóch różnych źródeł jednego dostawcy, np. z różnych transformatorów.

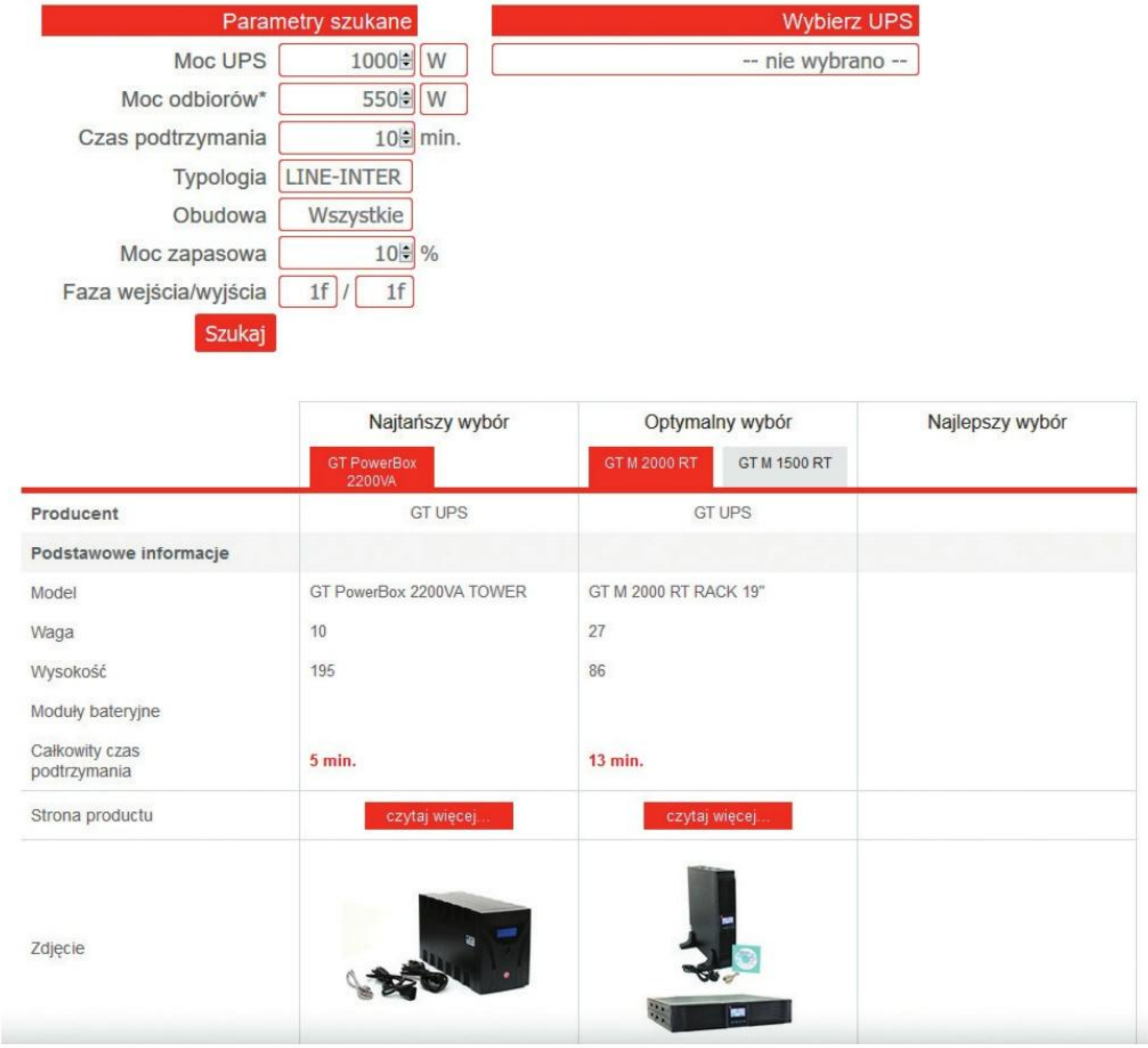
Moc zasilacza awaryjnego podaje się jako moc pozorną mierzoną w VA. Do zabezpieczenia stacji roboczych wystarcza moc 300–500 VA, natomiast do zasilania serwerów potrzeba mocy od 500 VA do kilkudziesięciu kVA. W instalacjach zasilania awaryjnego stosuje się różne typy zasilaczy UPS:

- **zasilacze online** – całkowicie odseparowują układ podłączony na wyjściu od napięcia wejściowego. Działają na zasadzie podwójnego przetwarzania napięcia – napięcie zmienne sieciowe jest przetwarzane na napięcie stałe w układzie prostownikowym, a następnie z tego stałego napięcia w układzie falownikowym jest wytwarzane napięcie przemienne. W razie zaniku napięcia sieciowego falownik jest nadal zasilany z akumulatora, z którym został połączony na stałe. Taki układ zapewnia natychmiastowe działanie, stabilne napięcie na wyjściu i jest niemal całkowicie odporny na zakłócenia i zaniki napięcia wejściowego;
- **zasilacze offline** – urządzenie chronione jest zasilane bezpośrednio z sieci. W czasie normalnej pracy jest zasilany jedynie układ sterowania, a w razie potrzeby akumulatory są doładowywane automatycznie. Napięcie zasilania jest cały czas monitorowane i w razie jego zaniku, zbyt dużego wzrostu lub spadku układ sterowania odłącza zasilanie sieciowe i UPS przechodzi w stan pracy akumulatorowej. Z opóźnieniem kilku milisekund pracę rozpoczyna falownik, który przekształca napięcie stałe z akumulatora w napięcie przemienne, podawane na wyjście. Układ sterowania zapewnia synchronizację fazową falownika z siecią zasilającą;
- **zasilacze line-interactive AVR** – to ulepszony typ offline. Zasilacz po stronie sieci zasilającej wyposażono w autotransformator, co umożliwia automatyczną regulację napięcia.

Instalacja zasilania awaryjnego może wykorzystywać duże centralne zasilacze awaryjne zabezpieczające zasilanie całego obiektu czy wydzielonego lokalu lub małe zasilacze UPS zabezpieczające pojedyncze urządzenia. Zasilacze pracujące w centralnym systemie zasilania awaryjnego są wykonywane w technologii online. Centralne zasilacze awaryjne produkuje się w zakresie mocy od kilku do kilkuset kVA. Zasilacze dużych mocy wymagają wydzielonych, klimatyzowanych pomieszczeń i wykonania instalacji elektrycznej przeznaczonej tylko dla urządzeń wymagających nieprzerwanego zasilania. Gniazda zasilające w takiej instalacji powinny być zabezpieczone tak, aby uniemożliwić podłączenie do nich innych urządzeń niewymagających zabezpieczenia, takich jak odkurzacze, czajniki elektryczne. Do zasilania pojedynczych urządzeń stosuje się zasilacze małej mocy. Zasilacze małej mocy są z reguły wykonywane w technologii line-interactive. Taki system zasilania nie wymaga inwestycji w pomieszczenia i dodatkową instalację elektryczną.

Zasilacz awaryjny dobiera się na podstawie zużycia energii chronionych urządzeń i przewidywanego czasu podtrzymania napięcia. Producenci zasilaczy na swoich stronach udostępniają kalkulatory umożliwiające dobór zasilacza zależnie od potrzeb. Na rys. 49.2 przedstawiono przykładowy kalkulator pomocny w doborze zasilacza.

BEZPIECZEŃSTWO DANYCH



Rys. 49.2. Kalkulator umożliwiający dobór zasilacza awaryjnego

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Dobierz zasilacz awaryjny dla swojego komputera.
2. Dobierz zasilacz awaryjny dla serwera w twojej szkole.
3. Dobierz zasilacz awaryjny dla systemu podtrzymania napięcia w szafie serwerowej (zasilanie awaryjne przełączników, routerów itp.).

50 Archiwizacja zasobów sieciowych

ZAGADNIENIA

Cel tworzenia kopii zapasowych **Dane włączane do kopii zapasowych** **Dobór nośnika, na którym będzie tworzona kopia zapasowa** **Programy wspierające proces tworzenia kopii zapasowych**

Obowiązkiem administratora jest zapewnienie bezpieczeństwa danych i samej sieci komputerowej, w której są one dostępne. Zdarzają się jednak sytuacje, w których następuje utrata danych. Może to być spowodowane awarią sprzętu, np. dysku twardego, lub błędem obsługi, np. przypadkowe skasowanie pliku. Administrator powinien jak najszybciej przywrócić sprawność sieci i urządzeń oraz zawartość danych. Nieocenioną pomocą w takim przypadku są **kopie zapasowe** (ang. *backup*) danych.

Dane, które powinny być chronione za pomocą kopii zapasowych, mogą znajdować się zarówno na serwerze (lub wielu serwerach), jak i na stacjach roboczych. Aby zapewnić sprawny proces tworzenia kopii zapasowych i ich odtwarzania, należy przygotować infrastrukturę sieci do wykonywania tego zadania. Proces tworzenia kopii zapasowych powinien obejmować również pliki konfiguracyjne urządzeń sieciowych, np. przełączników, routerów. W razie awarii sprzętu umożliwią one szybkie przywrócenie wcześniejszej konfiguracji urządzenia.

Kopie zapasowe mogą być tworzone na:

- nośnikach wymiennych, np. taśmach magnetycznych, CD/DVD/Blu-ray;
- dyskach twardych;
- serwerach w sieci w trybie online.

Dobór nośnika jest uzależniony od sposobu tworzenia kopii i ilości kopiowanych danych. CD/DVD/Blu-ray mogą być wykorzystywane przy niewielkiej liczbie kopiowanych danych, najczęściej tylko z lokalnego komputera lub serwera. W sieciach, w których ilość kopiowanych danych jest duża, są używane taśmy magnetyczne (coraz rzadziej) lub dyski twarde. Aby zwiększyć szybkość zapisu, dyski mogą być łączone w macierze dyskowe RAID. W sieciach tworzy się też specjalne **serwery kopii zapasowych** (ang. *backup server*), których zadaniem jest tworzenie kopii zapasowych.

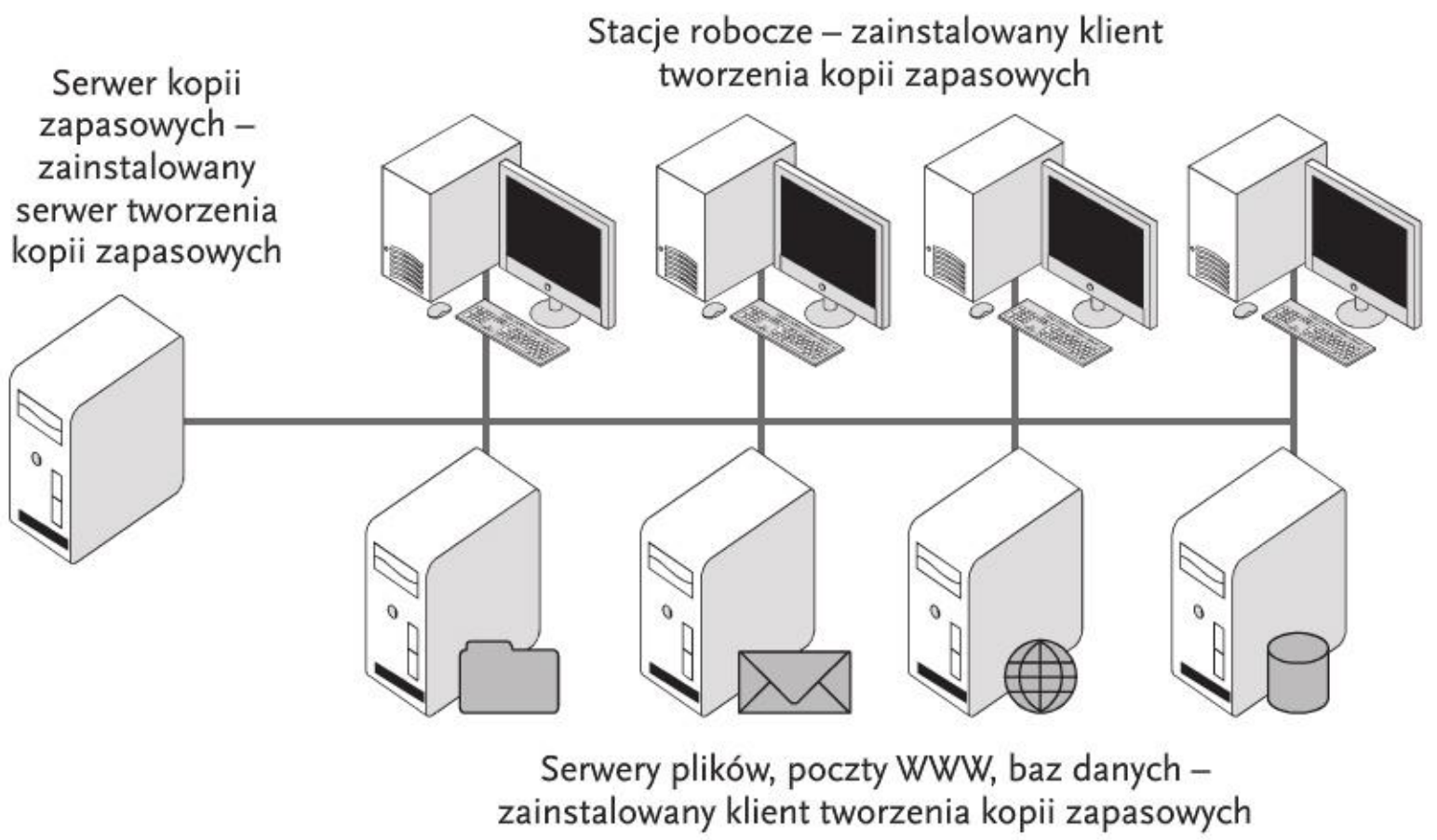
Tworzenie kopii zapasowych na serwerach „w chmurze" wymaga bardzo szybkiego połączenia z siecią lub jest wykorzystywane w przypadku, gdy serwery działają również „w chmurze". Jedną z podstawowych zasad bezpieczeństwa jest to, aby kopie zapasowe były przechowywane w innym miejscu niż kopiowane dane.

Konfiguracja serwera kopii zapasowych zależy od potrzeb i możliwości finansowych firmy. Może to być specjalnie zaprojektowany serwer, **serwer NAS** (ang. *Network Attached Storage*) lub miejsce na serwerze „w chmurze" o odpowiedniej pojemności. Przed przystąpieniem do oszacowywania wymaganej przestrzeni dyskowej należy się zastanowić, jakie dane wymagają tworzenia kopii zapasowych. Po zsumowaniu objętości danych znajdujących się na wszystkich dyskach uzyskuje się przybliżoną informację o tym, jak dużo miejsca zajmą kopie zapasowe.

Do początkowych wyliczeń trzeba dodać pewien margines błędu. Jeśli kopie przyrostowe będą wykonywane codziennie, to do rozmiaru archiwum pełnego powinno się doliczyć rozmiar dziennej kopii przyrostowej pomnożonej przez sześć.

Jeżeli serwer kopii zapasowych pracuje w sieci w standardzie FastEthernet o przepustowości 100 Mb/s, to szybkość odbioru danych będzie wynosiła maksymalnie ok. 10 MB/s. W sieci opartej na standardzie Gigabit Ethernet o przepustowości 1 Gb/s przesył danych do serwera może się odbywać z szybkością nawet do 100 MB/s. Należy zadbać o odpowiednią wydajność urządzeń magazynujących dane, tak aby zapewnić szybkie wykonanie kopii i jednocześnie odpowiedni zapas przepustowości w kanałach komunikacyjnych.

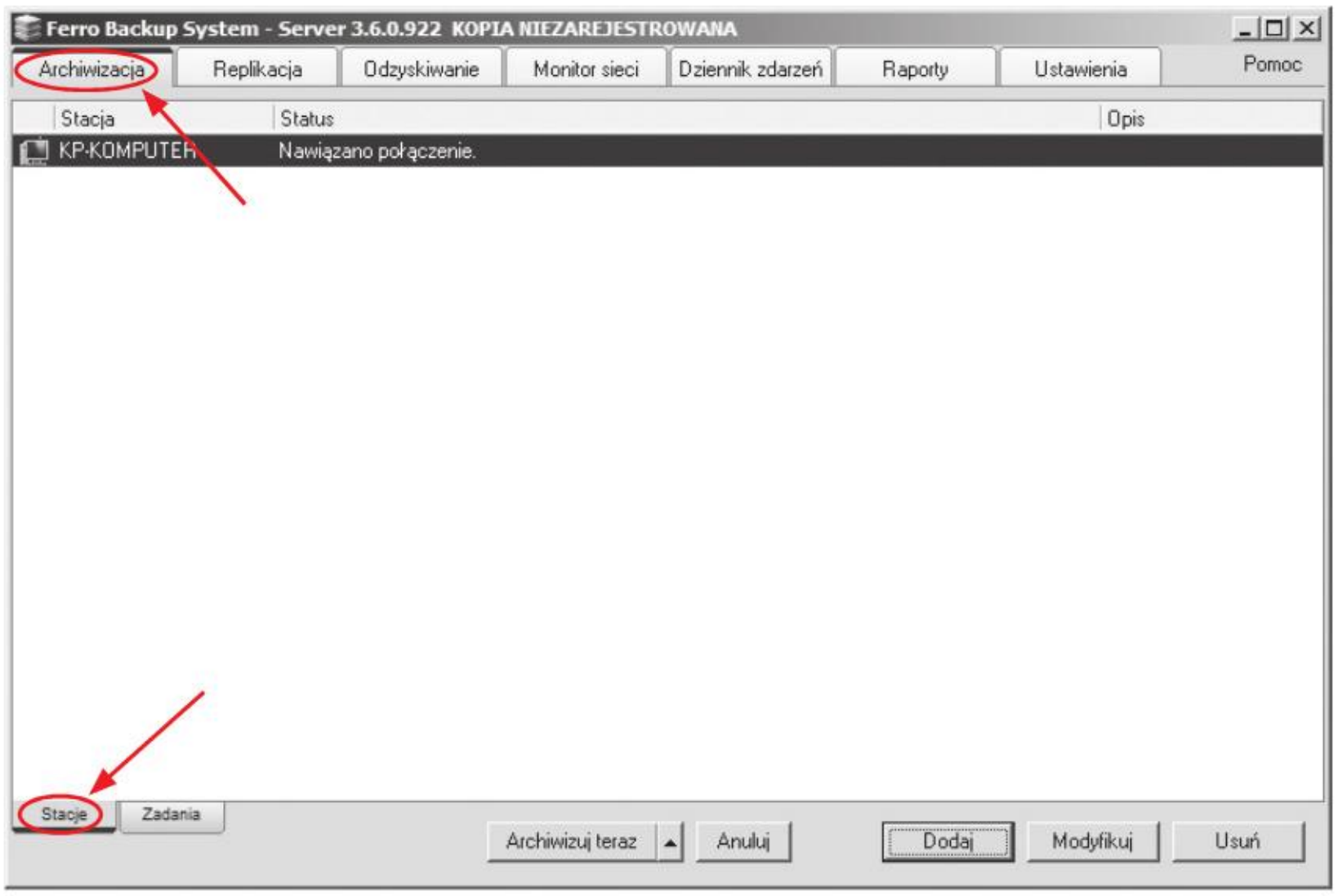
Wiele firm oferuje programy do sporządzania kopii zapasowych lub gotowe systemy obsługujące duże sieci. Systemy tego typu pracują zwykle na podstawie architektury klient–serwer. Przykładowy system składa się z dwóch programów: serwera i klienta. System został opracowany przez firmę Ferro Backup System i jest dostępny na stronie http://www.ferrobackup.com/pl/download.html. W wersji niezarejestrowanej umożliwia podłączenie maksymalnie dwóch stacji roboczych (archiwizacji dwóch komputerów), ponadto może być używany tylko w celach niezarobkowych i niekomercyjnych, np. dydaktycznych. Serwer jest uruchamiany tylko na komputerze przeznaczonym na serwer kopii, a klient – na wszystkich stacjach roboczych, z których będą pobierane dane do kopii (komputery biurowe, komputery przenośne, serwery plików, serwery bazodanowe itp.). Miejsca instalacji klienta i serwera tworzenia kopii zapasowych przedstawiono na rys. 50.1.



Rys. 50.1. Miejsca instalacji klienta i serwera tworzenia kopii zapasowych

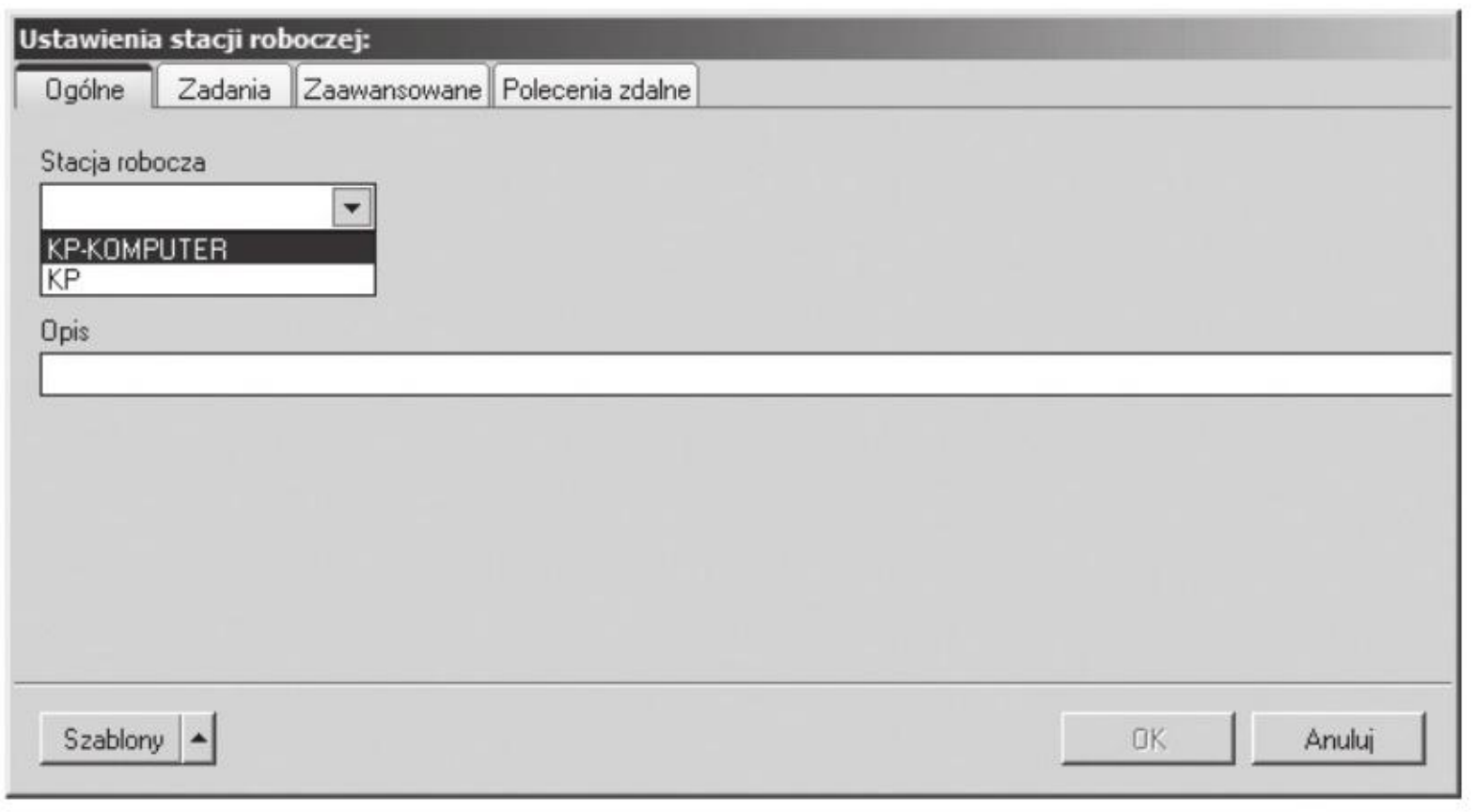
Podstawowym zadaniem serwera jest rozsyłanie w odpowiednim czasie zadań kopiowania do stacji roboczych. Takie zadanie zawiera informacje na temat tego, co ma zostać zarchiwizowane (jakie pliki, katalogi) i w jaki sposób (kopia pełna lub różnicowa). Po przyjęciu zadania stacja robocza wyszukuje pliki do kopiowania, a następnie rozpoczyna kompresję plików (generowanie archiwum ZIP). Tworzona kopia zapasowa jest na bieżąco przesyłana do serwera kopii. Serwer odbiera nadsyłaną kopię zapasową i zapisuje ją na dysku serwera. Po odebraniu ostatniej części serwer weryfikuje kopię zapasową – sprawdza sumy kontrolne skompresowanych archiwów. Planowanie zadań, czyli określenie zadań dla każdej stacji, jest wykonywane na serwerze.

Po zainstalowaniu oprogramowania na serwerze kopii zapasowych (wersja serwer oprogramowania) i stacjach roboczych (wersja klient oprogramowania) należy dodać stacje robocze do systemu. W tym celu w oknie głównym programu trzeba wybrać zakładkę **Archiwizacja** i **Stacje** (na rys. 50.2 miejsca zaznaczone strzałkami).



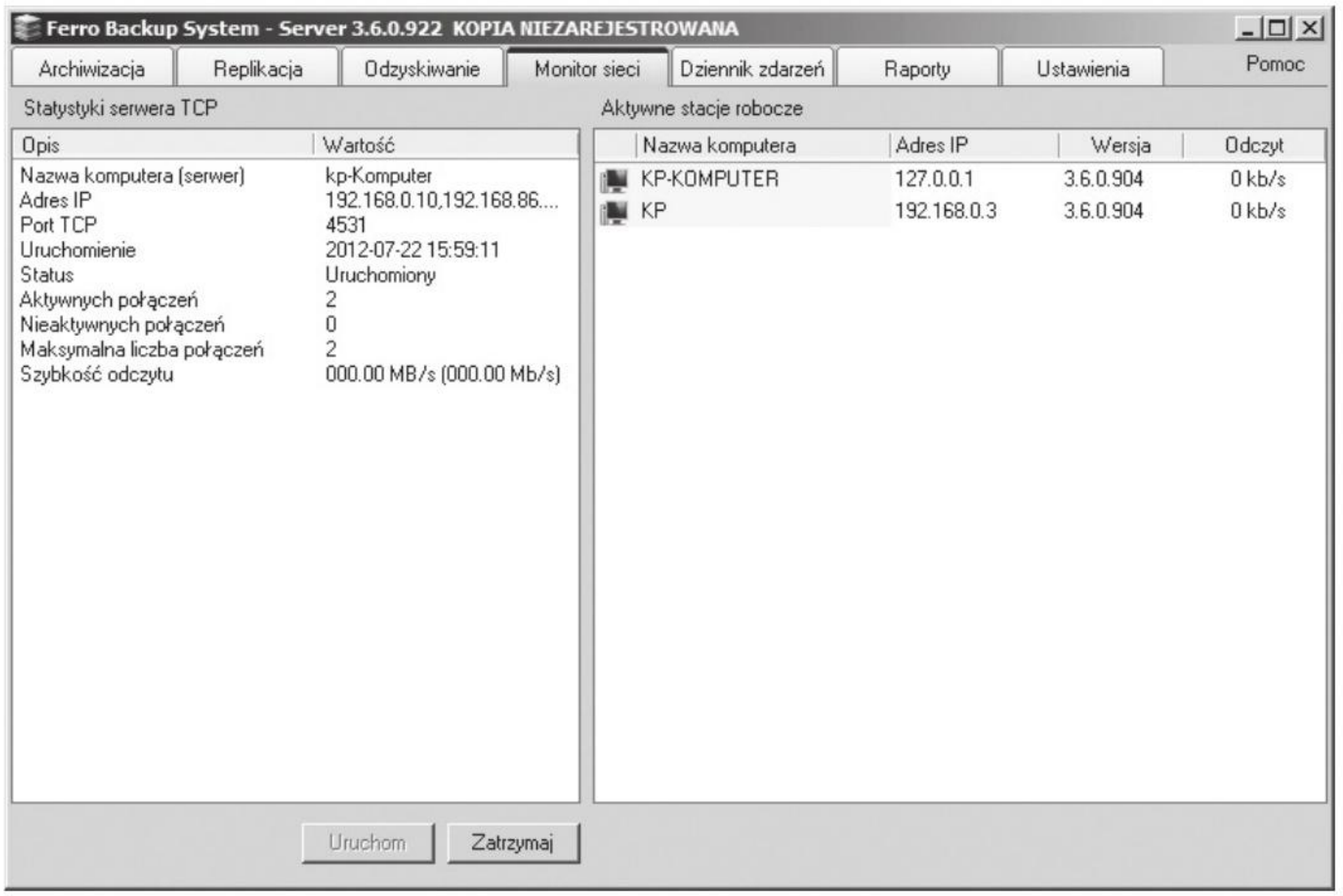
Rys. 50.2. Dodawanie nowego klienta tworzenia kopii zapasowych

Kliknąć przycisk **Dodaj** i w oknie dialogowym (rys. 50.3) wskazać stację z zainstalowanym wcześniej oprogramowaniem klienta kopii zapasowych. W polu **Opis** można umieścić krótką informację o stacji.



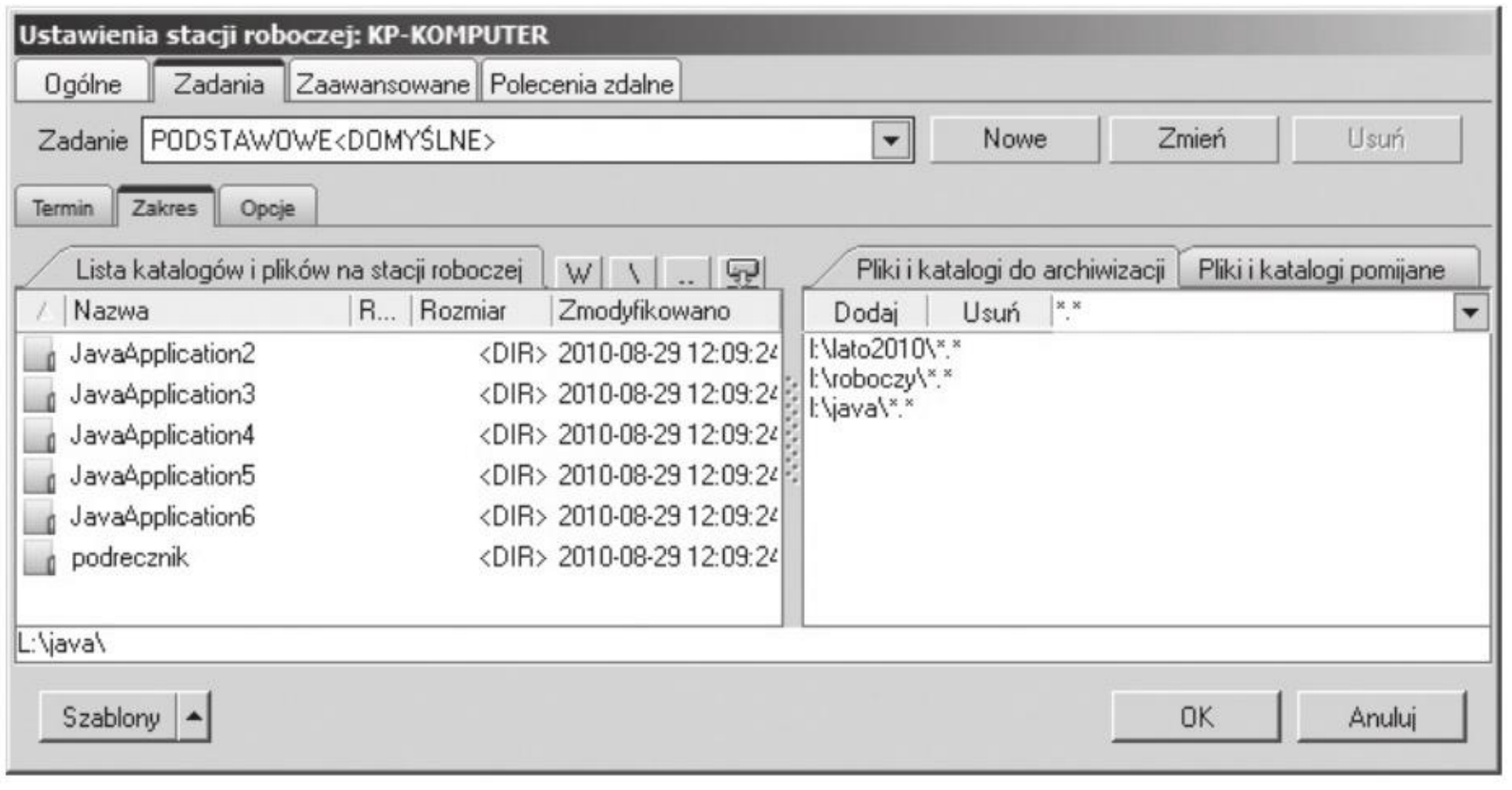
Rys. 50.3. Wskazywanie nowego klienta tworzenia kopii zapasowych

W zakładce **Monitor sieci** (rys. 50.4) można zweryfikować ustawienia sieci i poprawność konfiguracji stacji roboczych.



Rys. 50.4. **Okno monitorowania sieci**

Aby zdefiniować zadanie archiwizacji, należy wybrać zakładkę **Archiwizacja** i **Zadania**, wskazać stację roboczą i kliknąć przycisk **Dodaj**. W oknie dialogowym wpisać nazwę tworzonego zadania. W zakładce **Zadania** wybrać **Zakres** i przeciągnąć myszą do prawego panelu katalogi, które mają być zarchiwizowane (rys. 50.5). Po zakończeniu kliknąć **OK**. Nazwa utworzonego zadania powinna pojawić się w zakładce **Archiwizacja**.



Rys. 50.5. **Wybór katalogów do archiwizacji**

Aby rozpocząć proces archiwizacji, należy kliknąć przycisk **Archiwizuj teraz** lub w zakładce **Zadania/Termin** ustawić harmonogram tworzenia kopii.

Odzyskiwanie danych w przypadku kopii pełnej wymaga jedynie wypakowania wszystkich plików z wybranego archiwum (ZIP). Dla backupu różnicowego tylko pierwsze (najstarsze) archiwum zawiera wszystkie pliki określone w ustawieniach. Podczas kolejnych procesów tworzenia kopii są wykonywane kopie plików zmodyfikowanych lub utworzonych od czasu poprzedniej kopii pełnej. System przejmuje kontrolę nad przywracaniem danych, dzięki czemu użytkownik ma możliwość łatwego przywracania danych z kopii różnicowych, tak samo jak w przypadku kopii pełnych.

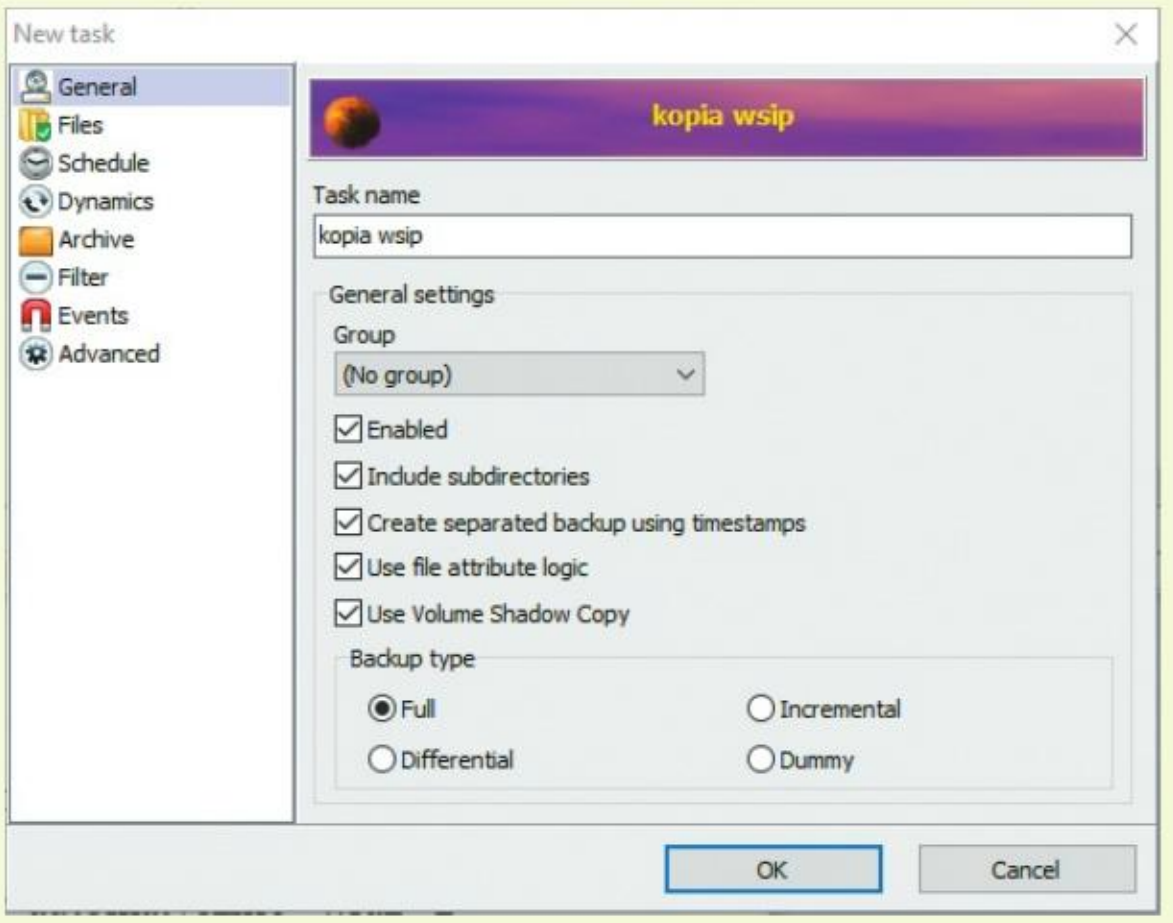
Innym programem do sporządzania kopii zapasowych jest **Cobian Backup**. Program jest dostępny bezpłatnie na stronie https://cobian-backup.en.uptodown.com/windows/download. Cobian Backup umożliwia tworzenie kopii przyrostowych i różnicowych, zapisywanych na CD, DVD, pamięci przenośnej USB lub serwerze FTP. Wspiera kompresję i szyfrowanie danych. Pozwala na skonfigurowanie harmonogramu kopii zapasowych.

PRZYKŁAD 50.1

Tworzenie kopii zapasowej przy pomocy Cobian Backup

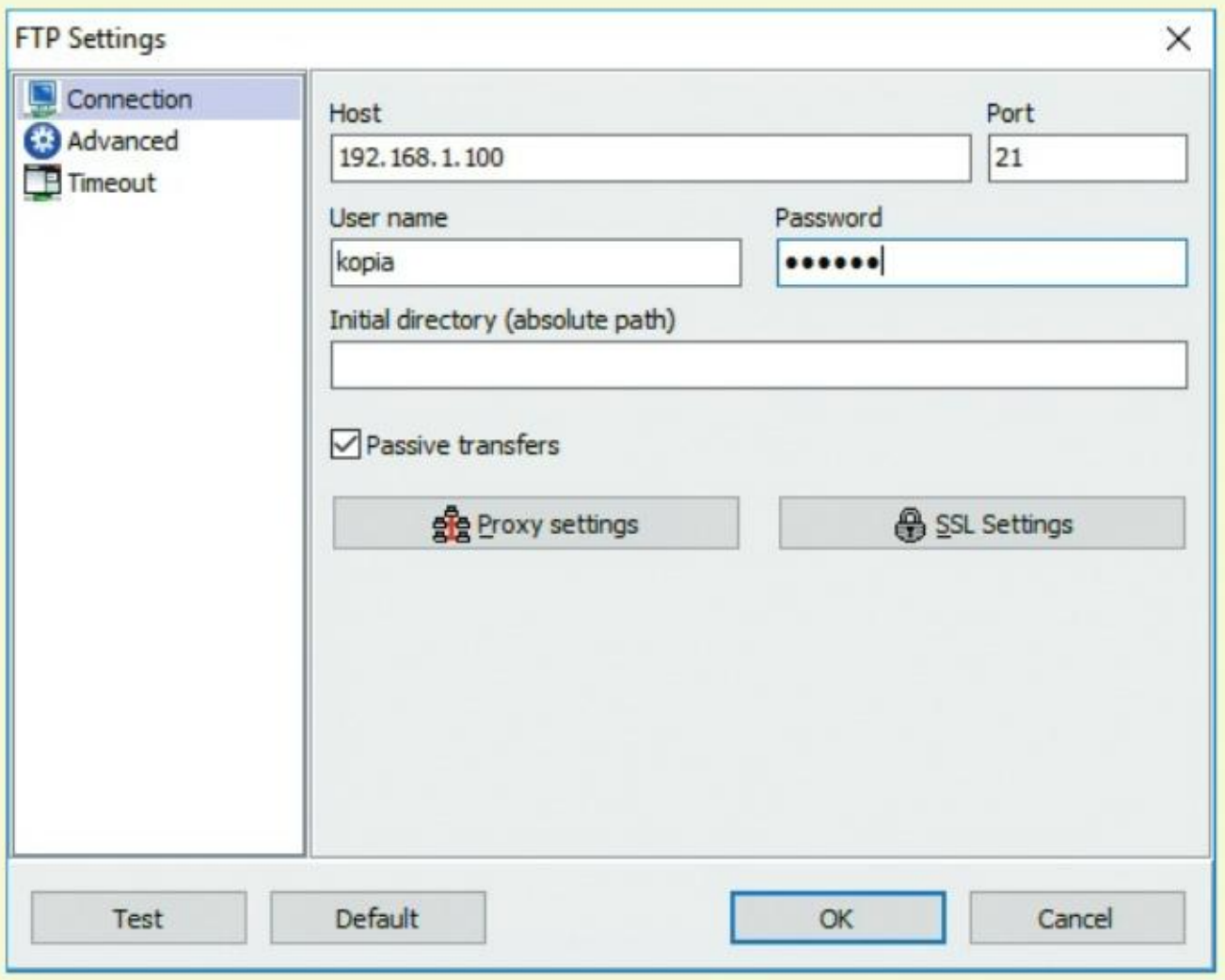
Aby utworzyć kopię zapasową za pomocą Cobian Backup, należy:

1. Uruchomić w sieci serwer FTP lub upewnić się, że serwer jest dostępny i użytkownik ma odpowiednie prawa do zapisu i odczytu danych z serwera.
2. Pobrać z sieci i zainstalować program działający jako usługa (uruchamiany automatycznie wraz z systemem).
3. Uruchomić program i dodać nowe zadanie **Task/New task** lub kliknąć przycisk ze znakiem (+) (ang. *Create a new task*).



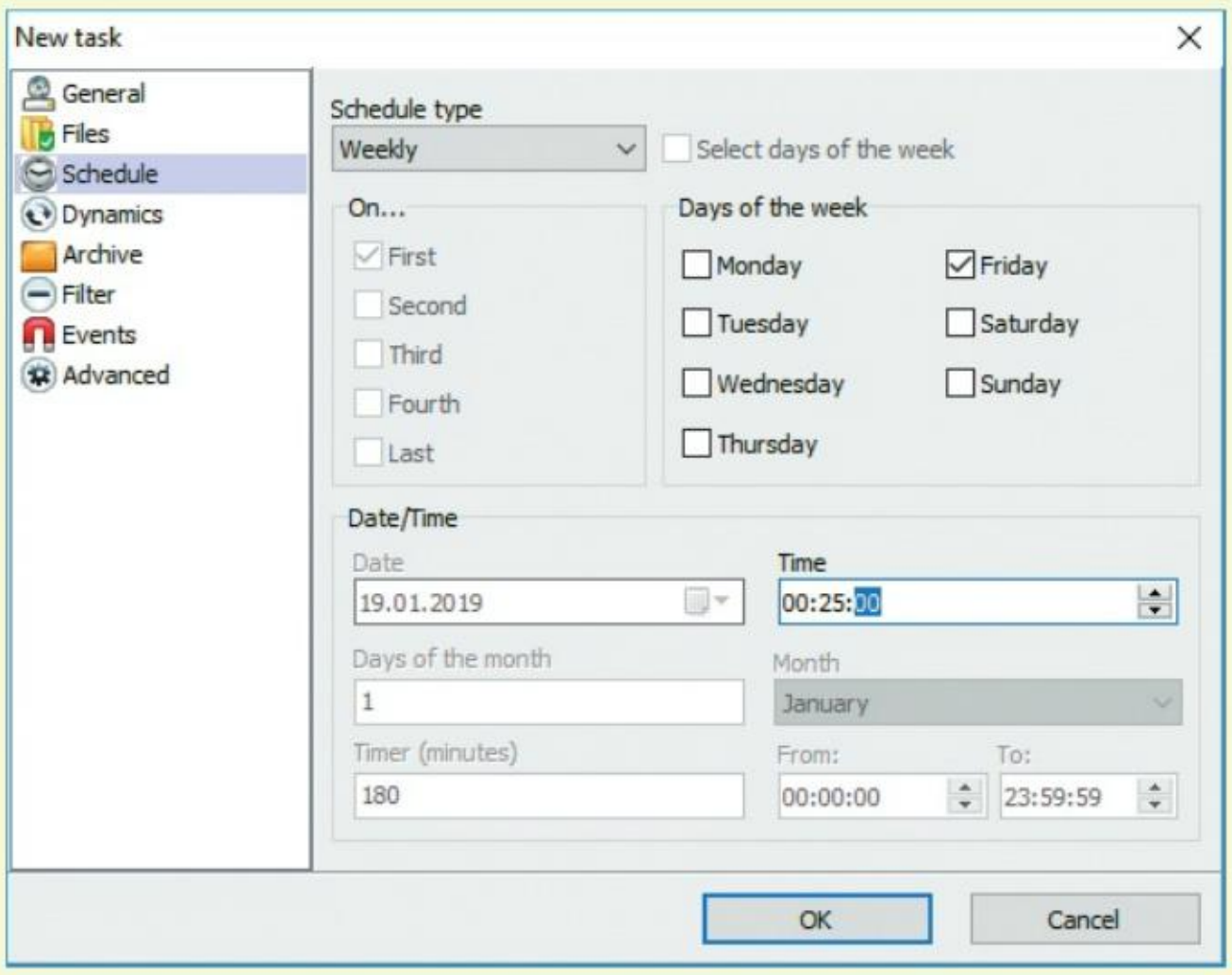
Rys. 50.6. **Tworzenie nowego zadania w Cobian Backup**

4. Wprowadzić nazwę zadania (ang. *Task name*) i typ tworzonej kopii zapasowej, np. pełna (ang. *Full*). Pozostałe opcje można pozostawić bez zmian (rys. 50.6). Kliknąć przycisk **OK**.
5. Wybrać pliki i foldery dołączone do kopii. W gałęzi **Files** w sekcji **Source** kliknąć przycisk **Add/Directory** i wskazać folder. Dodać do listy pozostałe pliki i foldery.
6. Wybrać miejsce utworzenia kopii. W gałęzi **Files** w sekcji **Destination** kliknąć przycisk **Add/FTP** i wskazać adres serwera FTP (ang. *Host*), nazwę konta (ang. *User name*) i hasło użytkownika (ang. *Password*) mającego uprawnienia do tworzenia kopii (rys. 50.7). Kliknąć przycisk **OK**.



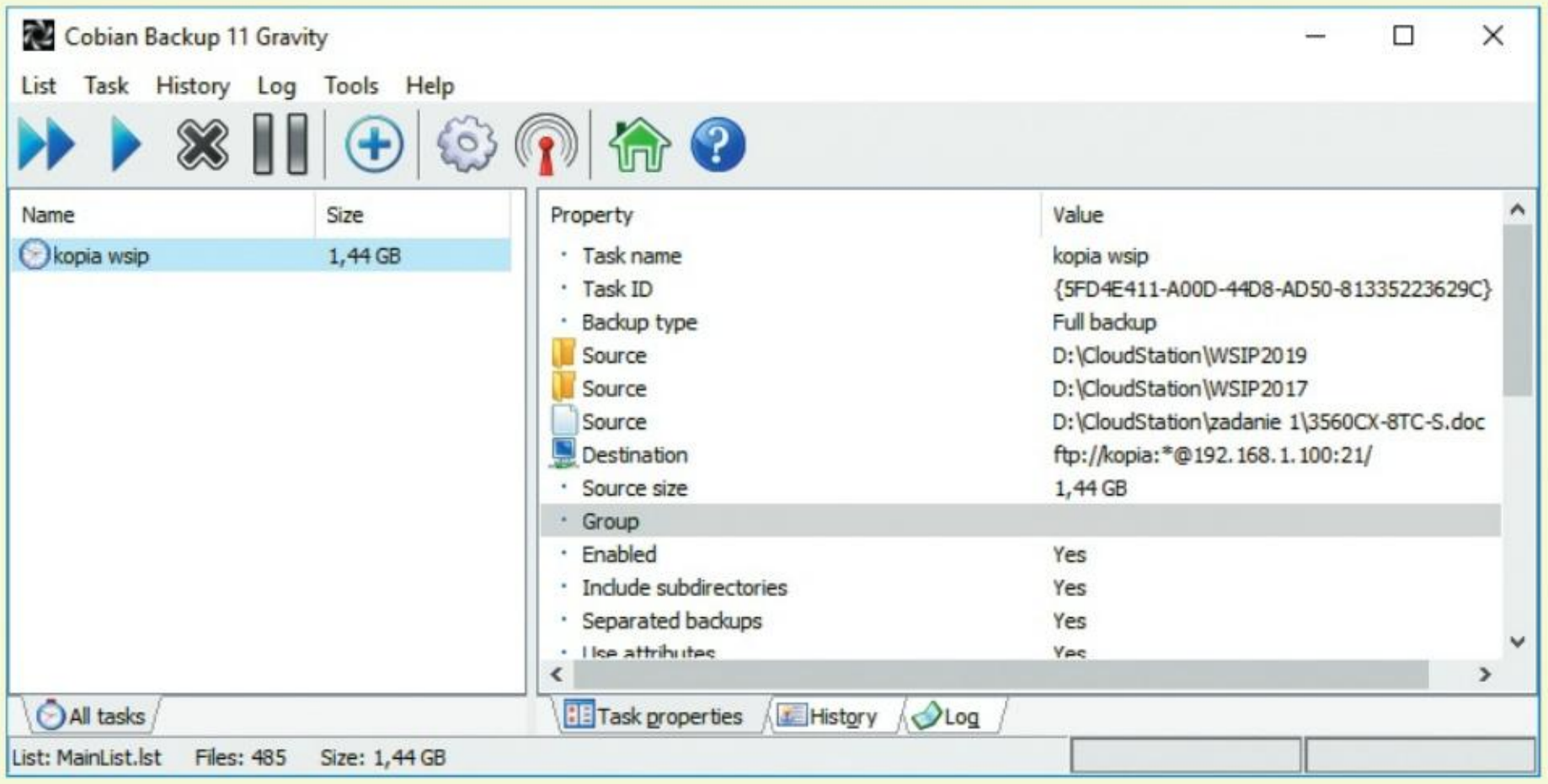
Rys. 50.7. **Określanie ścieżki docelowej dla kopii zapasowej**

7. Ustawić harmonogram tworzenia kopii. W gałęzi **`Shedule`** (rys. 50.8) ustawić uruchamianie co tydzień (ang. *Shedule type Weekly*), zaznaczyć w piątek (ang. *Friday*), rozpoczęcie o 0:25 (ang. *Time*). Kliknąć przycisk **`OK`**.
8. W gałęzi **`Archive`** można ustawić algorytmy kompresji i szyfrowania. W tym ćwiczeniu kopia zostanie wykonana bez szyfrowania i kompresji.



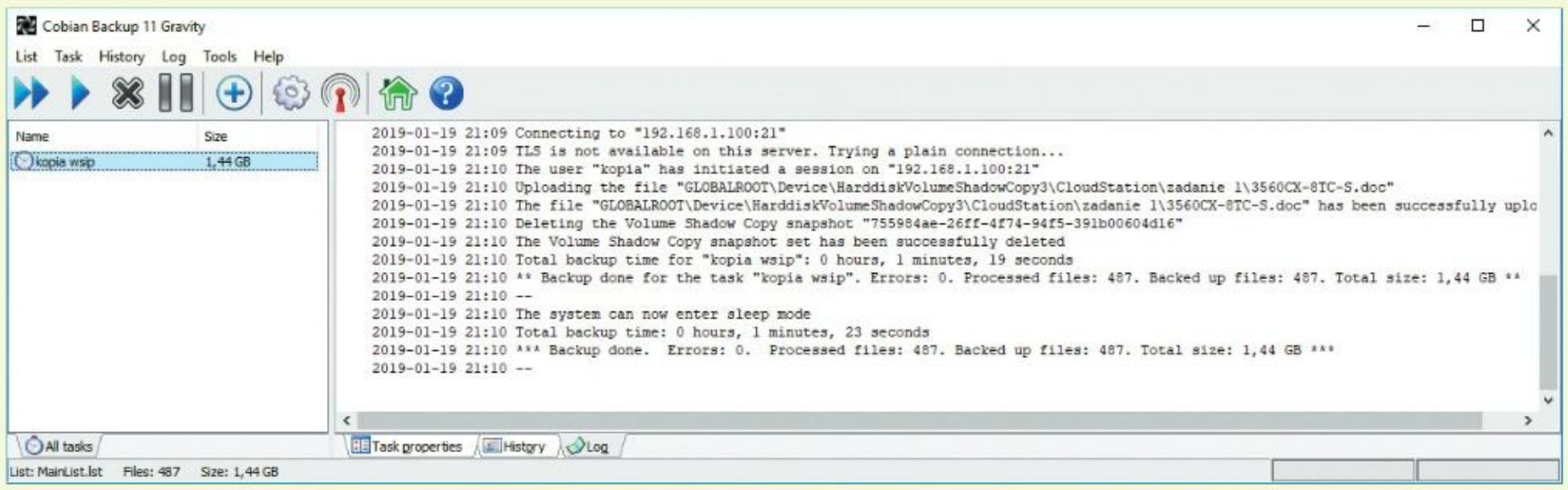
Rys. 50.8. **Określanie harmonogramu zadania**

9. W oknie głównym aplikacji (rys. 50.9) powinno pojawić się nowe zadanie. Zgodnie z ustalonym harmonogramem zostanie uruchomione w każdy piątek o 0.25. Każda kopia będzie oznaczona znacznikiem czasu. Użytkownik może uruchomić zadanie w dowolnym momencie, wybierając przycisk tworzenia kopii **`Task/Run selected task`**.



Rys. 50.9. Okno główne programu z zadaniem tworzenia kopii

10. Po zakończeniu tworzenia kopii jest wyświetlane podsumowanie wykonania zadania (rys. 50.10).



Rys. 50.10. Okno podsumowania zadania tworzenia kopii zapasowej

Cobian Backup kopiuje pliki i foldery do wybranego folderu kopii zapasowej, jako zwykłe pliki. Jeśli wybrano kompresję plików, pliki będą kompresowane za pomocą standardowych programów, np. ZIP lub 7-Zip. Aby przywrócić plik, wystarczy otworzyć folder kopii zapasowej w **`Eksploratorze Windows`**, wybrać kopię zapasową i skopiować plik z folderu.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wykonaj listę katalogów, które powinny być skopiowane z twojego komputera podczas procesu tworzenia kopii zapasowych.
2. Sporządź taką listę dla serwera szkolnego.
3. Napisz skrypt, np. w języku powłoki, który skopiuje wszystkie pliki do katalogu backup, a następnie wykonaj to samo zadanie za pomocą systemu do archiwizacji danych.

51 Konfiguracja Firewalla w Windows Server

ZAGADNIENIA

Funkcje zapory sieciowej **Rodzaje zapór sieciowych** **Skonfigurowanie zapory sieciowej**

Zapora sieciowa (ang. *firewall*) to system pozwalający zabezpieczyć komputery, serwery lub całe sieci przed nieuprawnionym przepływem danych. Pozwala określić, które urządzenia lub segmenty sieci są godne zaufania i odpowiednio filtrować dostęp do nich. Zapora sieciowa może być zlokalizowana w bramie sieciowej, na serwerze lub komputerze w sieci lokalnej. Zapory zlokalizowane w bramie sieciowej mogą być rozwiązaniami sprzętowymi, programowymi lub mieszanymi, sprzętowo-programowymi. Zwykle pełnią funkcje:

- kontroli i zarządzania ruchem w sieci – przez kontrolowanie pakietów, monitorowanie połączeń i filtrowanie danych na poziomie aplikacji;
- analizy połączeń – przez kontrolowanie komunikacji między hostami i przechowywanie zgromadzonych w ten sposób informacji w tabelach stanu;
- bramy w wirtualnej sieci prywatnej (VPN) – przez szyfrowanie, uwierzytelnianie w protokole IPsec i wykorzystanie technologii NAT (ang. *Network Address Translation*) pozwalającej na tłumaczenie adresów publicznych na adresy w sieci prywatnej.

Zapory zlokalizowane w bramie sieciowej nie są w stanie chronić zasobów sieci lokalnej przed zagrożeniami powstałymi wewnątrz sieci. Z tego względu istnieje konieczność instalowania dodatkowych zapór na komputerach i serwerach znajdujących się w sieci lokalnej, dzięki czemu będą one chronione przed nieuprawnionym dostępem i atakami z sieci lokalnej. Przykładowo, Windows Server 2016 ma udoskonaloną, w porównaniu z wcześniejszymi wersjami systemu, zaporę sieciową. Zapora jest domyślnie uaktywniana podczas każdej instalacji systemu. Do zarządzania zaporą można wykorzystać aplikację **`Menedżer serwera/Narzędzia/Zapora systemu Windows z zabezpieczeniami zaawansowanymi`** lub przystawkę w konsoli mmc o nazwie **`Zapora systemu Windows z zabezpieczeniami zaawansowanymi`**. Zapewnia ona interfejs pozwalający konfigurować zaporę sieciową Windows zarówno na lokalnych komputerach, jak i zdalnie, z wykorzystaniem narzędzi **`Group Policy`**. Ustawienia zapory są zintegrowane z protokołem **`IPsec`**, dzięki czemu może ona filtrować przepływ pakietów na podstawie wyników przeprowadzonych przez niego negocjacji.

Zapora filtruje przesyłane pakiety – wykorzystuje do tego reguły ustalone w trakcie jej konfiguracji. Zapora Windows obsługuje osobne profile komputerów przypisanych do domeny lub połączonych z prywatną albo publiczną siecią. W zaporze Windows Server 2016 zdefiniowano trzy typy lokalizacji sieciowych:

- **domeny** – Windows Server 2016 automatycznie umieszcza w tej kategorii sieci, w których można uzyskać dostęp do kontrolera domeny. Żadna inna sieć nie może zostać umieszczona w tej kategorii;

- **publiczna** – wszystkie sieci niezaklasyfikowane do kategorii domeny są wstępnie określane jako publiczne, np. sieci mające bezpośrednie połączenie z internetem lub znajdujące się w miejscach publicznych (takich jak *hot spoty* czy kawiarnie internetowe);
- **prywatna** – sieć powinna być przypisana do tej kategorii tylko wtedy, gdy jest chroniona urządzeniem z funkcją NAT, np. sieci domowe lub działające w małych firmach.

Kiedy użytkownik uzyska połączenie z siecią, która nie została zaklasyfikowana jako sieć domeny, system Windows prosi go o przypisanie jej do jednej z pozostałych dwóch kategorii. Administrator może opracować osobny profil (zawierający różne ustawienia zapory sieciowej) dla każdego typu sieci. Przykładowo, firewall może zezwalać na połączenia wykonywane przez komputer, kiedy jest połączony do sieci domeny, ale blokować te połączenia w sieciach prywatnych i publicznych.

Profil dla sieci publicznej powinien się cechować zaostrzonymi regułami w celu ochrony lokalnych zasobów przed niepowołanym dostępem. Profil dla sieci prywatnej można opracować w mniej restrykcyjny sposób, dzięki czemu będzie możliwe współdzielenie plików, zasobów i drukarek, odkrywanie urządzeń sieciowych i uzyskiwanie dostępu do urządzeń. W danej chwili może być wykorzystywany tylko jeden profil. Standardowo istnieją trzy profile zapory sieciowej:

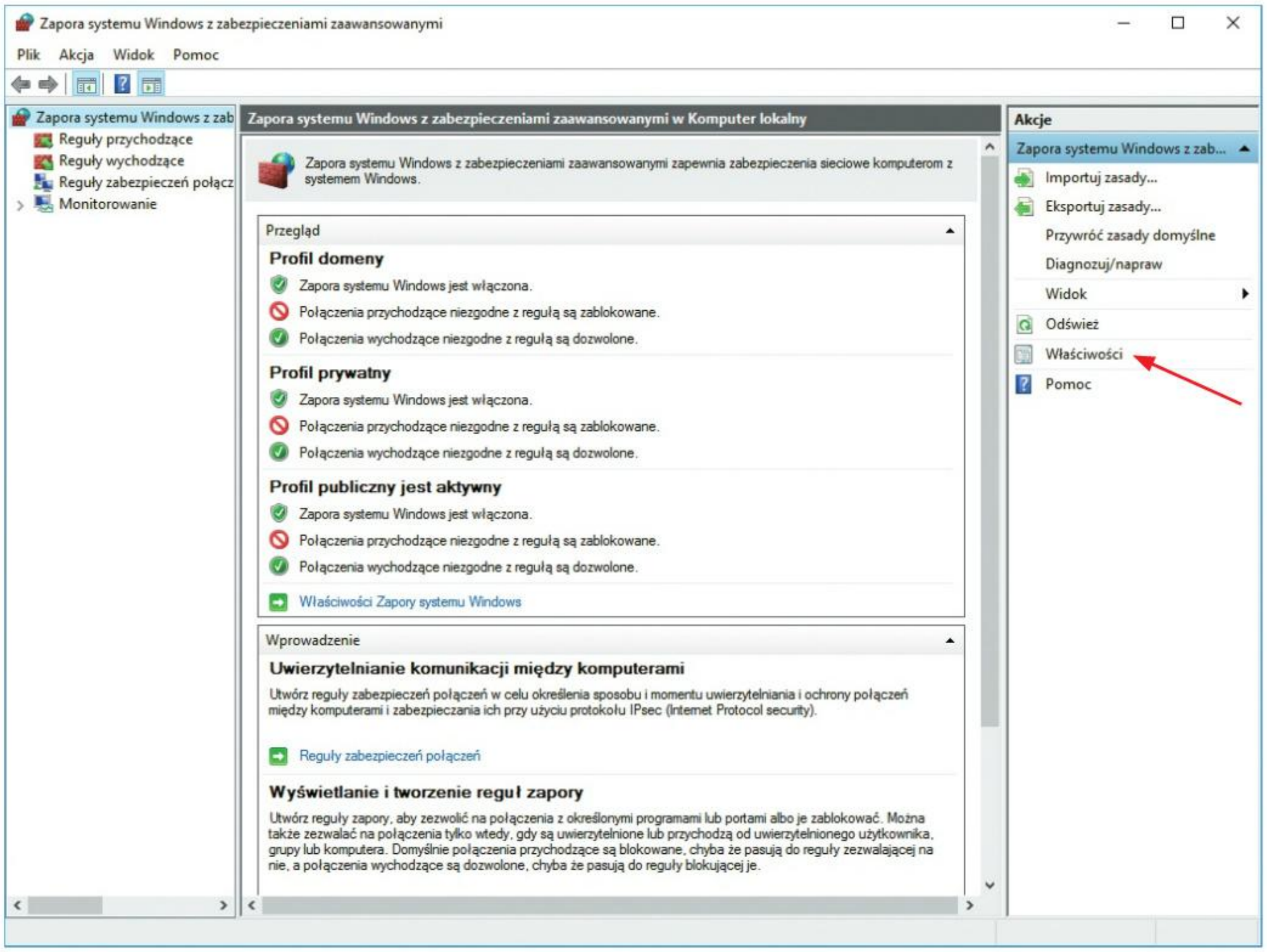
- **profil domeny** – wykorzystywany, gdy komputer jest połączony z domeną Active Directory, której jest członkiem (jest aktywny, gdy wszystkie interfejsy mogą nawiązać połączenie z kontrolerem domeny);
- **profil prywatny** – wykorzystywany, gdy komputer jest podłączony do prywatnej sieci, chronionej przez bramę lub router (sieć może być przypisana do tej kategorii wyłącznie przez użytkownika o uprawnieniach administratora);
- **profil publiczny** – stosuje się, gdy komputer jest podłączony bezpośrednio do nowej sieci w miejscu publicznym (jest stosowany, gdy komputer ma dostęp do przynajmniej jednej sieci publicznej).

Profile są przypisywane w następującej kolejności: publiczny, prywatny i domeny. Profil jest ustalany następująco:

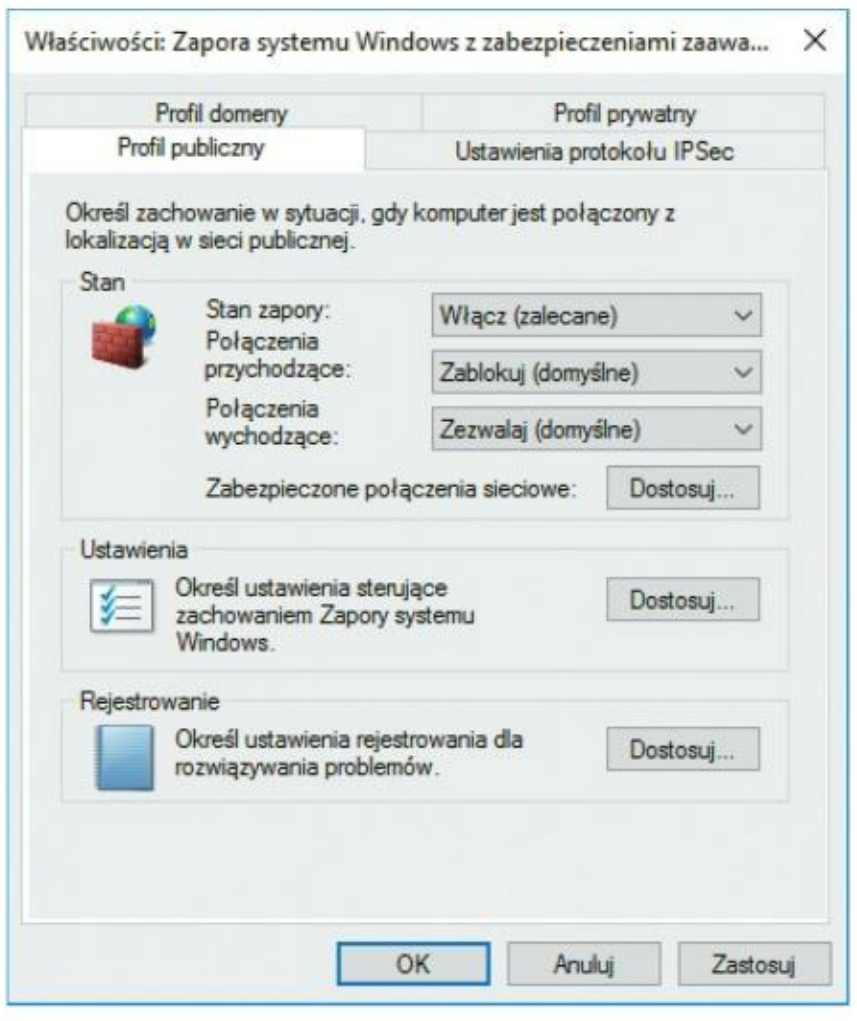
- jeśli wszystkie interfejsy zostaną przypisane do kontrolera domeny odpowiadającej danemu komputerowi, jest wybierany profil domeny;
- jeśli wszystkie interfejsy zostaną przypisane do kontrolera domeny lub są połączone z sieciami zaklasyfikowanymi jako prywatne, jest wybierany profil prywatny;
- w pozostałych przypadkach jest wybierany profil publiczny.

Większość przysyłanych pakietów jest domyślnie blokowana, tzn. są blokowane wszystkie pakiety z wyjątkiem podstawowej komunikacji w sieci. W profilu prywatnym jest dopuszczona komunikacja związana z udostępnianiem plików i drukarek, odkrywaniem urządzeń sieciowych i pomocą zdalną. Domyślne ustawienia dopuszczają połączenia wychodzące. W celu dopuszczenia innego rodzaju połączeń należy opracować specjalne reguły dla zapory sieciowej. Do skonfigurowania reguł dla połączeń wychodzących i przychodzących można wykorzystać aplikację **`Zapora systemu Windows z zabezpieczeniami zaawansowanymi`**.

Aby skonfigurować właściwości zapory sieciowej, należy kliknąć odnośnik **`Właściwości Zapory systemu Windows`** (na rys. 51.1 zaznaczony strzałką).



Rys. 51.1. Okno konfiguracji zapory systemu Windows



Rys. 51.2. Okno konfiguracji profilu zapory systemu Windows

Okno **Zapora systemu Windows z zabezpieczeniami zaawansowanymi** (rys. 51.2) zawiera jedną zakładkę dla każdego z trzech dostępnych profili (domeny, prywatnego i publicznego), a także zakładkę **Ustawienia protokołu IPSec**.

Wszystkie zakładki profili zawierają takie same opcje i kontrolują działanie aplikacji po podłączeniu komputera do danego typu sieci. Dla każdego z trzech profili można skonfigurować następujące opcje:

- **Stan zapory** – pozwala włączyć lub wyłączyć działanie zapory;
- **Połączenia przychodzące** – można ustawić:
  - zablokuj (ustawienie domyślne) – blokuje połączenia niespełniające wymogów zdefiniowanych w aktywnych regułach zapory;
  - zablokuj wszystkie połączenia – zapora ignoruje reguły i blokuje wszystkie połączenia przychodzące;
  - zezwalaj – zezwala na połączenia przychodzące, niespełniające wymogów zdefiniowanych w aktywnych regułach zapory;

- **Połączenia wychodzące** – można ustawić:
  - zezwalaj (ustawienie domyślne) – zapora zezwala na nawiązywanie połączeń niespełniających wymogów zdefiniowanych w aktywnych regułach zapory;
  - zablokuj – zapora blokuje połączenia wychodzące, które nie spełniają wymogów zdefiniowanych w aktywnych regułach zapory.

Zapora Windows pozwala na tworzenie przez administratora reguł następujących typów:

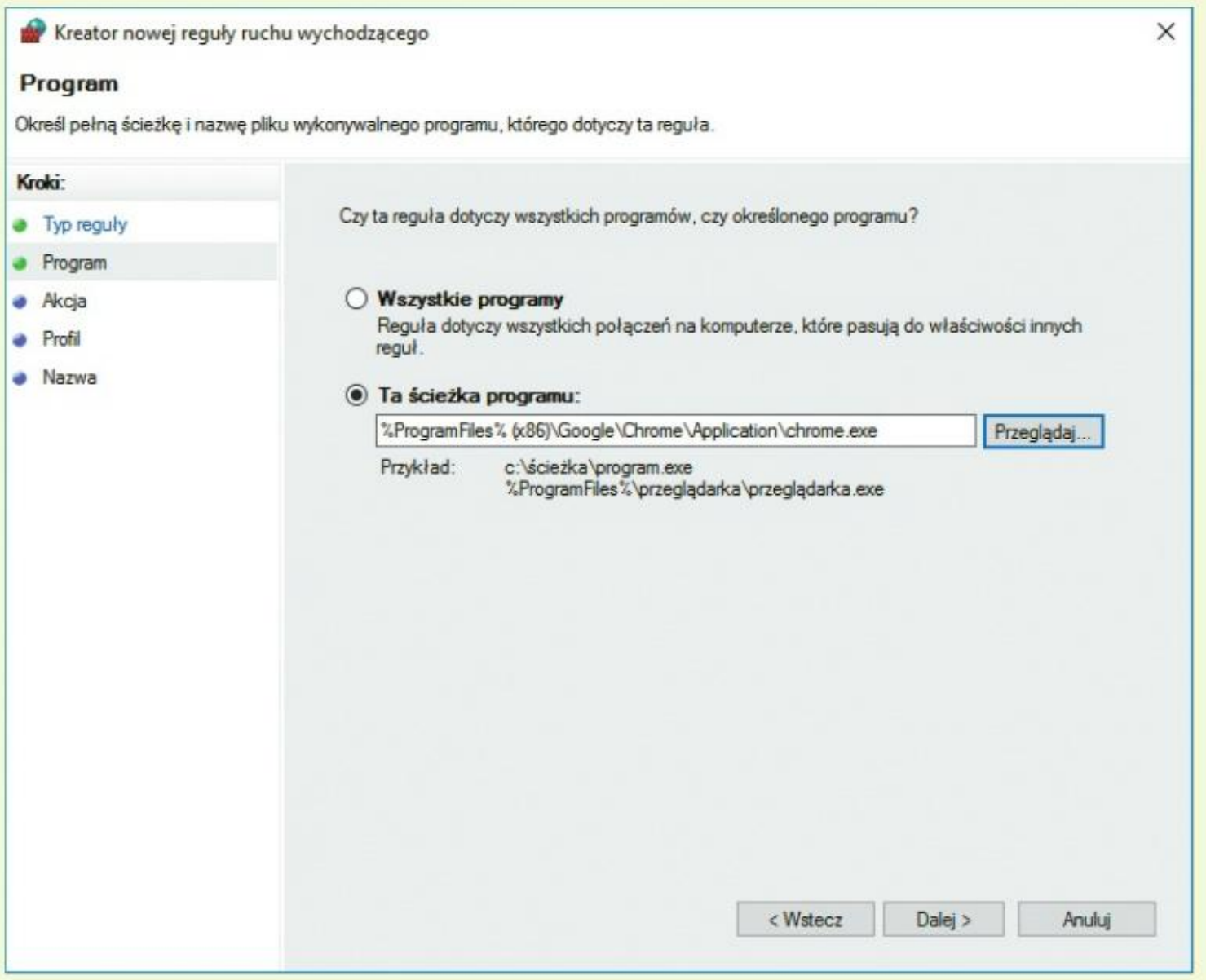
- **reguły programu** – dopuszczają przesyłanie pakietów przez wybrany program, identyfikowany przez ścieżkę dostępu i plik startowy;
- **reguły portu** – dopuszczają przesyłanie pakietów za pośrednictwem określonego numeru portu (lub ich zakresu) w protokole TCP lub UDP;
- **reguły predefiniowane** – pozwalają aktywować gotowe grupy reguł zezwalające wybranym funkcjom systemu na dostęp do sieci, np. narzędzia udostępniania plików i drukarek;
- **własne reguły** – reguły, których nie można utworzyć z użyciem reguł innych typów.

PRZYKŁAD 51.1

Tworzenie nowej reguły programu blokującej połączenia wychodzące

Aby utworzyć nową regułę, np. blokującą działanie aplikacji **`Chrome`**, podczas gdy połączenie realizowane przez inną przeglądarkę będzie możliwe, należy:

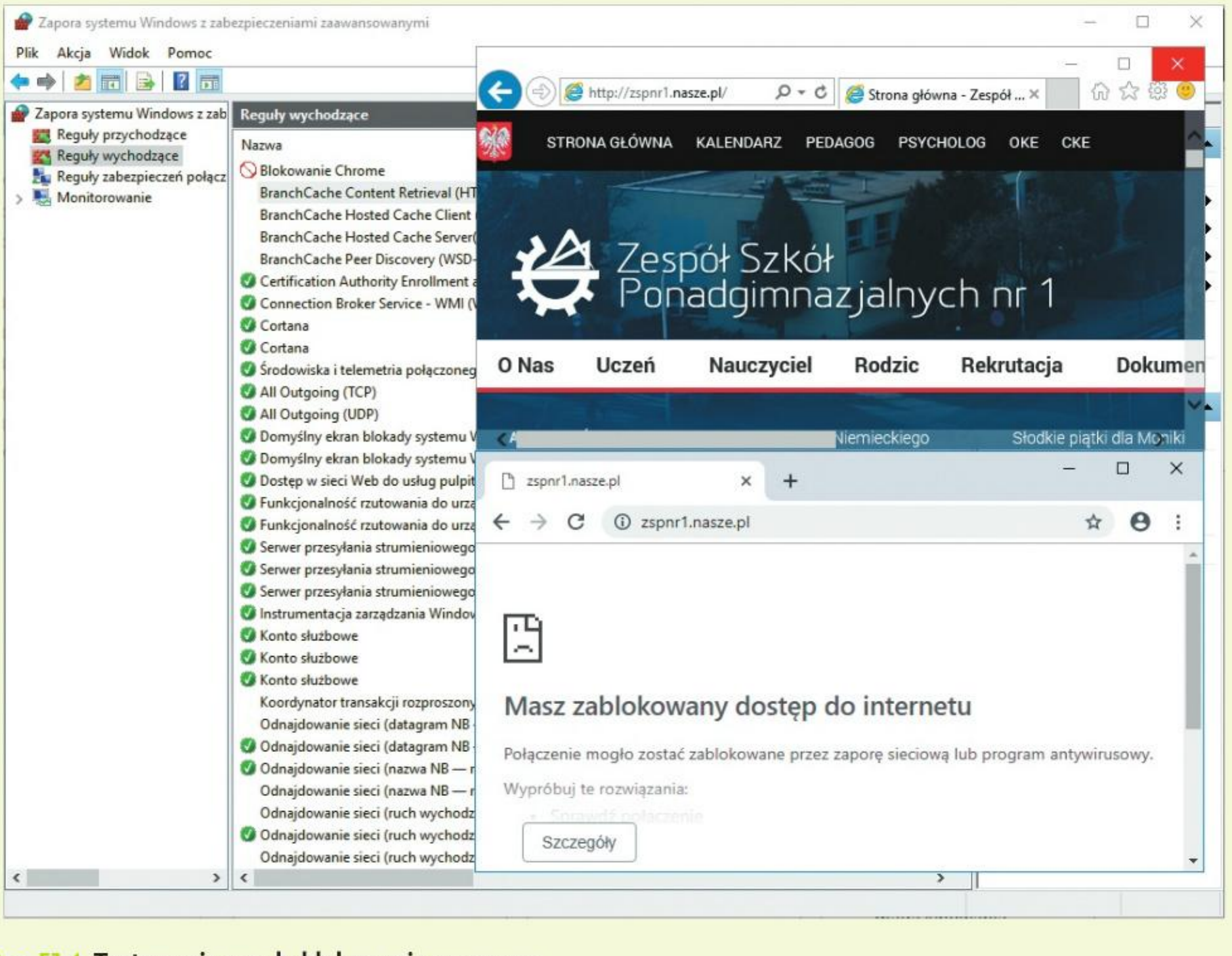
1. Zalogować się do systemu na konto z uprawnieniami administratora.
2. Uruchomić aplikację **`Zapora systemu Windows z zabezpieczeniami zaawansowanymi`**.
3. Rozwinąć gałąź **`Reguły wychodzące`** i kliknąć odnośnik **`Nowa reguła`**.
4. W oknie **`Kreator nowej reguły wychodzącej`** wybrać typ reguły **`Program`**. Kliknąć przycisk **`Dalej`**.
5. W pole **`Ta ścieżka programu`** wpisać (lub kliknąć przycisk **`Przeglądaj`**) i wskazać ścieżkę do programu, który ma być blokowany (rys. 51.3). Kliknąć przycisk **`Dalej`**.



Rys. 51.3. Ścieżka do blokowanego programu

6. Wybrać typ akcji – **Zablokuj połączenie**. Kliknąć przycisk **Dalej**.
7. Zaznaczyć profil, dla którego reguła będzie stosowana (można wybrać wszystkie profile). Kliknąć przycisk **Dalej**.
8. Wprowadzić nazwę reguły i jej opis. Kliknąć przycisk **Zakończ**.
9. Przetestować działanie reguły.

Na rys. 51.4 przedstawiono utworzoną regułę blokującą połączenia wychodzące i dwie aplikacje – **Chrome**, który został zablokowany, i aktywne połączenie realizowane przez **Internet Explorer**.



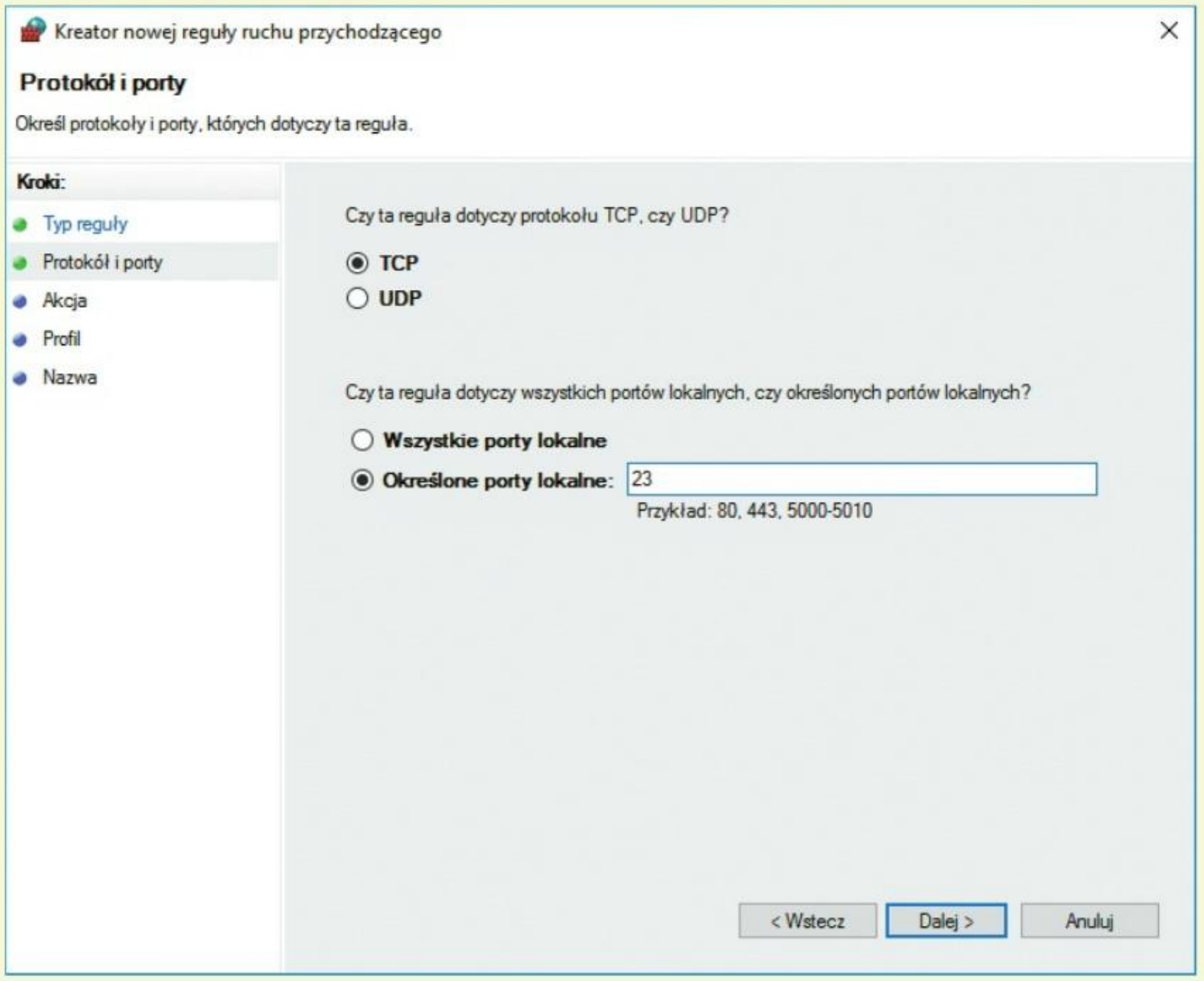
Rys. 51.4. **Testowanie reguły blokowania programu**

PRZYKŁAD 51.2

Tworzenie nowej reguły programu blokującej połączenia przychodzące na port

Aby utworzyć nową regułę, np. blokującą połączenia przychodzące na port, należy:

1. Zalogować się do systemu na konto z uprawnieniami administratora.
2. Uruchomić aplikację **Zapora systemu Windows z zabezpieczeniami zaawansowanymi**.
3. Rozwinąć gałąź **Reguły przychodzące** i kliknąć odnośnik **Nowa reguła**.
4. W oknie **Kreator nowej reguły przychodzącej** wybrać typ reguły **Port**. Kliknąć przycisk **Dalej**.
5. Zaznaczyć protokół i wprowadzić numer lub numery portów, dla którego / których reguła ma obowiązywać (rys. 51.5). Kliknąć przycisk **Dalej**.



Rys. 51.5. **Określanie portu, dla którego obowiązuje reguła**

6. Wybrać typ akcji – **`Zablokuj połączenie`**. Kliknąć przycisk **`Dalej`**.
7. Zaznaczyć profil, dla którego reguła będzie stosowana (można wybrać wszystkie profile). Kliknąć przycisk **`Dalej`**.
8. Wprowadzić nazwę reguły i jej opis. Kliknąć przycisk **`Zakończ`**.
9. Przetestować działanie reguły.

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Wprowadź reguły zapory:
   - Blokowanie połączeń wychodzących aplikacji Opera, podczas gdy Internet Explorer może realizować połączenia.
   - Blokowanie portu, na którym działa SSH (połączenie przychodzące).
   - Włączenie wcześniej zdefiniowanej reguły dla serwera FTP.

WYKAZ POJĘĆ

Active Directory, AD – usługa katalogowa dla systemów Windows.

Adres fizyczny MAC (ang. *Media Access Control*) – adres nadawany przez producenta każdej karcie sieciowej NIC (ang. *Network Interface Card*) podczas jej wytwarzania.

Adres logiczny – adres nadawany przez administratora sieci. Wskazuje punkt przyłączenia do sieci, który jest nazywany interfejsem.

Adres prywatny – adres przeznaczony do stosowania w sieciach lokalnych. Nie jest widoczny w internecie.

Adres rozgłoszeniowy (ang. *broadcast address*) – adres, dzięki któremu komputer może wysłać wiadomość do wszystkich urządzeń w danej sieci lub podsieci (domenie rozgłoszeniowej).

Adres sieci (ang. *network address*) – adres identyfikujący całą sieć komputerową wykorzystującą protokół IP.

Agregat prądotwórczy – urządzenie elektroenergetyczne stanowiące samodzielne źródło prądu.

Architektura klient–serwer (ang. *client-server*) – organizacja sieci, w której istnieje jeden lub więcej komputerów spełniających tylko funkcję serwera.

Architektura równorzędna (ang. *peer-to-peer*) – organizacja sieci, w której każdy użytkownik może jednocześnie udostępniać zasoby swojego komputera i korzystać z zasobów innych komputerów.

Archiwizacja (ang. *backup*) – proces wykonywania kopii danych w celu zabezpieczenia ich przed utratą.

Bezprzewodowa sieć lokalna WLAN (ang. *Wireless Local Area Network*) – sieć, w której połączenia między urządzeniami sieciowymi zrealizowano bez użycia przewodów.

Bit (ang. *binary digit*) – najmniejsza jednostka danych przyjmująca dwie wartości: 0 lub 1.

Brama sieciowa (ang. *gateway*) – urządzenie, za którego pośrednictwem komputery z sieci lokalnej komunikują się z komputerami w innych sieciach.

Bramka VoIP (ang. *Voice over Internet Protocol*) – urządzenie, którego zadaniem jest umożliwienie wykonywania połączeń telefonicznych tradycyjnym aparatem telefonicznym za pośrednictwem sieci komputerowej wykorzystującej protokół IP.

Chmura obliczeniowa – model przetwarzania danych oparty na użytkowaniu usług i aplikacji dostarczonych przez usługodawcę.

Cyfrowe zarządzanie prawami DRM (ang. *Digital Rights Management*) – system zarządzania prawami do utworów oparty na mechanizmach kryptograficznych lub innych metodach ukrywania treści, mający przeciwdziałać używaniu danych w formacie elektronicznym w sposób sprzeczny z wolą ich wydawcy.

Czas procesora – określa, ile czasu procesor przeznacza na efektywne wykonanie określonego zadania.

Czytnik książek elektronicznych (ang. *ebook reader*) – urządzenie przeznaczone do czytania książek elektronicznych, wyposażone w wyświetlacz zbudowany w technologii papieru elektronicznego lub technologii LCD.

Defragmentacja – proces łączenia pofragmentowanych plików i folderów na dysku twardym komputera.

Dekapsulacja (ang. *decapsulation*) – proces łączenia jednostek danych i usuwania nagłówków realizowany podczas odbierania informacji i przesyłania danych do górnych warstw modelu OSI.

Demon – program pracujący w tle i nieprzyłączony do terminalu.

Dodatki Service Pack – zestawy poprawek, aktualizacji zabezpieczeń, aktualizacji krytycznych i innych, a także dodatkowych poprawek eliminujących problemy rozpoznane wewnętrznie od czasu wydania produktu.

Dokumentacja techniczna – zbiór informacji dotyczących urządzenia, jego instalowania i działania.

Domena – grupa komputerów połączonych w sieć, składająca się z serwera odgrywającego rolę kontrolera domeny i stacji roboczych – klientów współdzielących bazę katalogową.

Domena kolizyjna (ang. *collision domain*) – obszar sieci, w którym może dojść do kolizji danych nadawanych przez różne stacje.

Domeny najwyższego poziomu (ang. *top-level-domains*) – domeny na samym szczycie drzewa DNS obsługujące główne domeny, np.: .com, .edu, .org, oraz domeny krajowe, np.: .pl, .de.

Domena rozgłoszeniowa (ang. *broadcast domain*) – obszar sieci, w którym następuje emisja komunikatu rozgłoszeniowego wysyłanego przez jedną stację do wszystkich innych.

Dostawca usługi internetu, ISP (ang. *Internet Service Provider*) – firma oferująca usługę dostępu do internetu.

Dostęp zdalny (ang. *remote access*) – usługa umożliwiająca użytkownikom znajdującym się poza siecią uzyskanie dostępu do zasobów zlokalizowanych w sieci.

Dowiązanie (ang. *link*) – umożliwia odwoływanie się do zbioru za pomocą różnych nazw lub umieszczenie jednego zbioru w wielu miejscach w strukturze plików.

Drukarka – służy do wykonywania wydruków dokumentów tekstowych lub obrazów.

Drukarka lokalna – drukarka przyłączona bezpośrednio do komputera, z którego wykonuje się drukowanie.

Drukarka sieciowa – drukarka przeznaczona do obsługi wszystkich stacji roboczych w sieci.

Dysk sieciowy NAS (ang. *Network Attached Storage*) – technologia umożliwiająca podłączenie pamięci dyskowych bezpośrednio do sieci komputerowej.

Dysponent – obiekt, który został umieszczony na liście ACL danego folderu lub pliku.

Ethernet, Fast Ethernet, Gigabit Ethernet – technologie używane w sieciach lokalnych.

Enkapsulacja (ang. *encapsulation*) – proces podziału strumienia danych na jednostki danych i opatrywania ich nagłówkami.

Formatowanie – proces przygotowania partycji do zapisu danych.

Fragmentacja danych – naturalny proces, w wyniku którego pliki znajdujące się na dysku twardym są zapisane na klastrach niesąsiadujących ze sobą.

FTP – protokół służący do transmisji plików w sieci.

Główny punkt dystrybucyjny, MDF (ang. *Main Distribution Facility*) – centrum okablowania w topologii gwiazdy.

Główne serwery nazw (ang. *root level servers*) – serwery podłączone do szybkich sieci szkieletowych internetu; przechowują adresy serwerów nazw dla domen najwyższego poziomu, np.: .com, .edu, .org, i domen krajowych, np.: .pl, .de, .uk.

Gniazda abonenckie – punkty przyłączenia użytkownika do sieci.

Grupa robocza – grupa komputerów, które pracują w sieci niezapewniającej centralnej administracji zasobami.

Grupy dyskusyjne – usługa umożliwiająca przesyłanie poczty do grupy użytkowników zainteresowanych danym zagadnieniem, co może prowadzić do otwartej dyskusji na dany temat.

Host – stacja w sieci.

Internet – ogólnoświatowa sieć komputerowa logicznie połączona w jednorodną sieć adresową opartą na protokole IP (ang. *Internet Protocol*).

Jednostka alokacji – najmniejsza ilość miejsca na dysku, która może być przeznaczona do przechowywania pliku.

Jednostkowy nakład rzeczowy – wielkość danego nakładu przypadająca na wybraną jednostkę obmiarową danego rodzaju robót. Służy do szacowania kosztów.

Kabel koncentryczny (ang. *coaxial cable*) – kabel zbudowany z miedzianego rdzenia umieszczonego w osi kabla otoczonego izolatorem i ekranem.

Kabel prosty (ang. *straight-through*) – wtyki na obu końcach są wykonane według jednego standardu.

Kabel skrosowany (ang. *crossover*) – wtyk na jednym końcu jest wykonany według standardu 568A, a na drugim według standardu 568B.

Kamień milowy – warunek określający zakończenie etapu realizacji projektu.

Kamera internetowa – umożliwia nagranie filmu lub prowadzenie wideokonferencji.

Klawiatura – podstawowe urządzenie peryferyjne wejścia służące do wprowadzania danych.

Karta sieciowa (ang. *Network Interface Card*, NIC) – urządzenie łączące komputer z lokalną siecią komputerową.

Katalog nakładów rzeczowych – zbiór jednostkowych nakładów rzeczowych, będący podstawą szacowania kosztów.

Klient – dowolny komputer lub program nawiązujący połączenie z usługami lub żądający usług od innego komputera lub programu.

Klucz rejestru (ang. *registry key*) – obiekt-kontener przechowujący podklucze i wartości rejestru.

Kolejka drukowania (ang. *print queue*) – podfolder, w którym są magazynowane zadania drukowania (ang. *print job*).

Kompresja danych (ang. *data compression*) – zmiana sposobu zapisu informacji w taki sposób, aby zmniejszyć objętość zbioru.

Komputerowy system sieciowy – system złożony z serwerów, stacji roboczych, urządzeń sieciowych i okablowania wraz z oprogramowaniem sieciowym i użytkowym.

Koncentrator (ang. *hub*) – urządzenie sieciowe wyposażone w wiele portów służących do przyłączania stacji roboczych lub innych urządzeń.

Konie trojańskie – szkodliwe oprogramowanie, które umożliwia m.in. kontrolowanie komputera przez sieć komputerową.

Konto użytkownika – zbiór zasobów i uprawnień do systemu przypisanych konkretnemu użytkownikowi. Proces autoryzacji w systemie (logowania) wymaga zwykle podania nazwy konta (login) i hasła.

Kontroler domeny – komputer, na którym uruchomiono usługę Active Directory zarządzającą dostępem użytkowników do sieci i jej zasobów.

Kopia zapasowa (ang. *backup copy*) – kopia danych, które mogą służyć do odtworzenia danych oryginalnych w razie ich utraty lub uszkodzenia.

Kopia pełna (ang. *full copy*) – polega na skopiowaniu wszystkich plików i oznaczeniu każdego z nich jako zarchiwizowanego (usunięcie atrybutu archiwizacji).

Kopia przyrostowa (ang. *incremental copy*) – polega na kopiowaniu jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii przyrostowej lub pełnej, i na oznaczeniu ich jako zarchiwizowanych.

Kopia różnicowa (ang. *differential copy*) – polega na kopiowaniu jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii pełnej.

Licencja oprogramowania – umowa na korzystanie np. z utworu, jakim jest aplikacja komputerowa, zawierana między podmiotem, któremu przysługują prawa autorskie do utworu, a osobą, która zamierza z danej aplikacji korzystać.

Lista kontroli dostępu, ACL (ang. *Access Control List*) – określa, jakie prawa do zasobu mają poszczególni użytkownicy.

Lista zgodności sprzętu, HCL (ang. *Hardware Compatibility List*) – określa urządzenia, które pomyślnie przeszły testy zgodności sprzętowej.

Logowanie – proces autoryzacji w systemie wymagający zwykle podania nazwy konta i hasła.

Lokacja – grupa komputerów i kontrolerów domen połączona szybką siecią.

Łącze komunikacyjne – zespół środków technicznych służących do przesyłania sygnałów między oddalonymi stacjami sieci teleinformatycznej.

Łączność bezprzewodowa – rodzaj łączności, która do transmisji danych wykorzystuje fale elektromagnetyczne.

Magazyn danych konfiguracji rozruchu, BCD (ang. *Boot Configuration Data*) – magazyn, w którym systemy Windows przechowują pliki i ustawienia aplikacji dotyczące rozruchu.

Mapowanie dysków – mechanizm tworzenia w systemie Windows nowego dysku sieciowego i przypisania mu zasobu sieciowego serwera, np. folderu. W takim przypadku odwołanie do zasobu sieciowego odbywa się przez wskazanie odpowiedniego dysku oznaczonego literą, tak jak dyski lokalne.

Maska podsieci (ang. *subnetwork mask*) – określa, ile bitów w adresie jest przeznaczonych do identyfikacji sieci i podsieci, a ile do identyfikacji hosta.

Mechanizm PnP (ang. *Plug&Play*) – zestaw specyfikacji, które pozwalają komputerowi automatycznie wykrywać i konfigurować urządzenia oraz instalować odpowiednie sterowniki urządzeń.

Medium transmisyjne – medium, przez które są przesyłane dane.

Mikrofon – umożliwia wprowadzanie dźwięku w postaci cyfrowej.

Model hierarchiczny sieci – trójwarstwowy model wykorzystywany do projektowania sieci przełączanych.

Modem (ang. *Modulator/Demodulator*) – urządzenie, które zamienia cyfrowe dane generowane przez komputer na sygnały analogowe i wysyła je za pomocą sieci.

Most (ang. *bridge*) – urządzenie sieciowe wyposażone w dwa porty służące do łączenia segmentów sieci.

Mysz – urządzenie ułatwiające pracę na komputerze, umożliwia wybieranie i aktywowanie opcji dostępnych w wykorzystywanych programach komputerowych.

Nadmiarowość – metoda zwiększenia niezawodności sieci.

Nagłówek IP – część pakietu IP zawierająca informacje niezbędne do przesyłania i kontroli pakietu (m.in. adresy IP nadawcy i odbiorcy oraz pole TTL).

Netykieta – zbiór zasad zachowania w sieci.

Obiekt – wyróżniony, nazwany zbiór atrybutów reprezentujący np. użytkownika, drukarkę lub komputer.

Oczyszczanie dysku – usuwanie plików tymczasowych, opróżnianie kosza i usuwanie różnego typu plików systemowych i innych elementów, które nie są już potrzebne.

Odtwarzacz mp3 – urządzenie służące do odsłuchiwania plików dźwiękowych.

Okablowanie pionowe (wewnątrz budynku) – kable miedziane lub/i światłowodowe ułożone zazwyczaj w głównych pionach telekomunikacyjnych budynków, realizujące połączenia między punktami rozdzielczymi systemu.

Okablowanie poziome – część okablowania między punktem rozdzielczym a gniazdem użytkownika.

Okablowanie strukturalne – system modularny, pozwalający na realizację połączeń systemu teleinformatycznego, z możliwością zmian konfiguracji i rozbudowy z użyciem takich samych elementów.

Oprogramowanie diagnostyczne – zbiór specjalistycznych programów (lub czasem jeden program) pozwalających na diagnostykę systemu komputerowego i komponentów sprzętowych.

Oprogramowanie komunikacyjne (ang. *communication software*) – oprogramowanie, które korzysta z protokołów i sterowników do wymiany danych.

Oprogramowanie monitorujące – aplikacje umożliwiające przeglądanie czynności wykonywanych przez użytkownika na danym komputerze.

Oprogramowanie OCR (ang. *Optical Character Recognition*) – oprogramowanie do optycznego rozpoznawania pisma.

Opóźnienie urządzenia sieciowego – czas poświęcony przez urządzenie na przetwarzanie pakietu lub ramki.

Pakiet – podstawowa jednostka informacji w warstwie sieciowej modelu OSI. Składa się z nagłówka sieci i obszaru danych.

Pakiet – archiwum zawierające pliki programu i dodatkowe informacje o pakiecie oraz wymaganiach i sposobie jego instalacji. Pakiety przygotowuje się w taki sposób, aby ułatwić użytkownikowi wykonanie procesu instalacji oprogramowania, a w razie potrzeby usunięcia z systemu zbędnych programów lub też ich weryfikacji i naprawy.

Pamięć RAM (ang. *Random Access Memory*) – pamięć o dostępie swobodnym.

Pamięć ROM (ang. *Read-Only Memory*) – pamięć tylko do odczytu.

Papier elektroniczny (ang. *e-paper*) – rodzaj wyświetlacza stosowany w czytnikach książek elektronicznych, który imituje papier.

Partycja – obszar na dysku twardym, który może być formatowany w systemie plików i identyfikowany za pomocą litery alfabetu.

Partycja podstawowa – część dysku fizycznego, która działa, jakby była fizycznie oddzielnym dyskiem.

Partycja rozszerzona – rodzaj partycji, która może być tworzona tylko na dyskach podstawowych.

Partycja systemowa – partycja, na której zainstalowano system operacyjny.

Ploter – wyspecjalizowane urządzenie podobne do drukarki, przeznaczone do rysowania wykresów, map, schematów, rysunków technicznych itp.

Piractwo komputerowe – łamanie praw autorskich, nielegalne posługiwanie się programem komputerowym bez zgody autora lub producenta oraz bez uiszczenia odpowiedniej opłaty.

Planista – program, który realizuje algorytm szeregowania zadań w kolejce do przyznania czasu procesora.

Plik stronicowania – ukryty plik na dysku twardym używany przez system Windows do przechowywania części plików i danych zbyt dużych i niemieszczących się w pamięci.

Plik wsadowy – program komputerowy, który jest wykonywany w trybie wsadowym bez ingerencji użytkownika.

Poczta elektroniczna (ang. *e-mail*) – usługa polegająca na przesyłaniu informacji tekstowych lub HTML w postaci elektronicznej między użytkownikami sieci. Do informacji mogą być dołączone inne pliki (załączniki).

Posłaniec – usługa używana do wysyłania krótkich wiadomości po sieci. Mogą ją wykorzystywać niektóre aplikacje do rozsyłania SPAMU.

Połączenia systemowe – połączenia między serwerami a szkieletem sieci.

Połączenia telekomunikacyjne budynków (okablowanie międzybudynkowe lub kampusowe) – okablowanie pionowe łączące różne budynki.

Port protokołu – liczba identyfikująca proces działający na odległym komputerze.

Pośredni punkt dystrybucyjny, IDF (ang. *Intermediate Distribution Facility*) – lokalny punkt rozdzielczy obsługujący najczęściej dany obszar roboczy lub piętro.

Prawo autorskie – zespół norm i aktów prawnych, mających na celu zabezpieczenie wytworów ludzkiej działalności przed nielegalnym rozpowszechnianiem, kopiowaniem bądź czerpaniem korzyści majątkowych.

Priorytet procesu – parametr pozwalający na określenie poziomu wykorzystania czasu procesora przez dany proces.

Proces – egzemplarz wykonywanego programu wyposażony we własną przestrzeń adresową.

Profil użytkownika – zbiór ustawień, które dostosowują wygląd ekranu i pracę komputera do osobistych preferencji.

Program antywirusowy – program komputerowy, którego celem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych.

Programy szpiegujące (ang. *spyware*) – programy komputerowe, których celem jest szpiegowanie działań użytkownika.

Projekt – działania, w których celem jest opracowanie czegoś nowego, wymagające nierutynowego podejścia.

Protokoły (ang. *protocols*) – określają sposoby komunikowania się urządzeń, np. protokół IP.

Protokoły bezpołączeniowe – protokoły komunikacyjne, w których komunikaty są przekazywane niezależnie.

Protokoły internetowe – podzbiór protokołów komunikacyjnych stosowanych w internecie.

Protokoły komunikacyjne – zbiór reguł postępowania automatycznie wykonywanych przez urządzenia komunikacyjne w celu nawiązania łączności i wymiany danych.

Protokoły połączeniowe – protokoły komunikacyjne, w których ustanawia się logiczne połączenie między dwoma komunikującymi się ze sobą urządzeniami.

Protokoły routingu – protokoły wykorzystywane przez routery do wymiany między sobą informacji o trasach lub topologii sieci.

Protokół IP (ang. *Internet Protocol*) – protokół warstwy sieciowej odpowiedzialny za przesyłanie pakietów między użytkownikami sieci.

Protokół SNMP (ang. *Simple Network Management Protocol*) – protokół warstwy aplikacji, który został opracowany w celu ułatwienia wymiany informacji związanych z zarządzaniem między urządzeniami sieci.

Protokół STP (ang. *Spanning-Tree Protocol*) – protokół używany w sieciach przełączanych w celu utworzenia topologii logicznej bez pętli, na podstawie topologii fizycznej z pętlami.

Protokół TCP (ang. *Transmission Control Protocol*) – protokół warstwy transportowej działający w trybie połączeniowym.

Protokół UDP (ang. *User Datagram Protocol*) – protokół warstwy transportowej działający w trybie bezpołączeniowym.

Przekazywanie żetonu (ang. *token-passing*) – metoda dostępu do nośnika, w której w pierścieniu krąży specjalna ramka (token).

Przełącznik (ang. *switch*) – wieloportowe urządzenie sieciowe, które oferuje te same funkcje co koncentrator, a dodatkowo pozwala, podobnie jak most, podzielić sieć na segmenty.

Pulpit (ang. *desktop*) – podstawowy obszar roboczy w systemach operacyjnych z graficznym interfejsem użytkownika (GUI).

Punkt demarkacyjny – punkt, który oddziela sieć lokalną od sieci globalnej (internetu).

Punkt dostępowy (ang. *access point*) – urządzenie sieciowe zapewniające stacjom bezprzewodowym dostęp do zasobów sieci za pomocą bezprzewodowego medium transmisyjnego.

Punkt montowania – katalog uważany przez system za miejsce, od którego zaczyna się partycja. Wszystkie dane zapisane na partycji będą traktowane tak, jakby znajdowały się w katalogu stanowiącym punkt montowania.

Punkty rozdzielcze – węzły sieci w topologii gwiazdy, w których zbiegają się okablowanie poziome i okablowanie pionowe.

Ramka – jednostka danych w warstwie łącza danych.

Rejestr – hierarchiczna baza danych przechowująca informacje dotyczące konfiguracji systemu, zainstalowanych aplikacji i sprzętu znajdujących się w komputerze użytkownika.

Ripowanie – tworzenie plików, np. mp3, z plików CD audio.

Rozdzielczość – ustawienie określające mierzoną w pikselach liczbę informacji wyświetlanych na ekranie.

Router – urządzenie sieciowe łączące sieci, wyposażone w co najmniej dwa interfejsy sieciowe. Jeden z nich może być wykorzystywany do przyłączenia sieci do internetu (interfejs zewnętrzny WAN), drugi umożliwia przyłączenie sieci lokalnej (interfejs wewnętrzny LAN).

Rysunek techniczny – typ dokumentacji rysunkowej pozwalający na wierne odzwierciedlenie zarówno ogólnego kształtu produktu, jak i jego szczegółów technicznych.

ScanDisk – program narzędziowy dostępny w systemach MS-DOS i Windows, umożliwiający sprawdzanie dysku twardego w poszukiwaniu błędów.

Segment – jednostka danych w warstwie transportowej modelu OSI.

Sektor – najmniejsza fizyczna jednostka zapisu danych na dyskach twardych.

Serwer – komputer udostępniający zasoby innym komputerom w sieci.

Serwer pośredniczący (ang. *proxy server*) – specjalny serwer, którego zadaniem jest buforowanie na dysku lokalnym odwiedzonych wcześniej stron WWW.

Sieciowy system operacyjny – system operacyjny instalowany na serwerze.

Sieć komputerowa (ang. *Computer network*) – grupa komputerów lub innych urządzeń połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów.

Sieci osobiste, PAN (ang. *Personal Area Network*) – sieci o zasięgu kilku metrów wykorzystywane np. do bezprzewodowego połączenia telefonu komórkowego ze słuchawką.

Sieci lokalne, LAN (ang. *Local Area Network*) – sieci łączące użytkowników na niewielkim obszarze (pomieszczenie, budynek).

Sieci miejskie, MAN (ang. *Metropolitan Area Network*) – sieci o zasięgu miasta, najczęściej szybkie.

Sieci rozległe, WAN (ang. *Wide Area Network*) – sieci, których zasięg przekracza granice miast, państw i kontynentów, np. internet.

Skalowalność – podatność sieci na rozbudowę.

Skaner – urządzenie wczytujące do komputera różnego rodzaju dokumenty lub zdjęcia, tworzące w ten sposób plik z elektronicznym obrazem zeskanowanego dokumentu.

Skrętka (ang. *twisted pair*) – najpopularniejsze medium transmisyjne używane obecnie do budowy sieci lokalnych.

Skrót – obiekt, który może wskazywać na plik, folder, aplikację lub miejsce sieciowe, np. w sieci lokalnej lub internecie.

Smartfon – rozbudowany telefon komórkowy, wyposażony w wiele funkcji.

Sniffer – program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i analizowanie danych przepływających w sieci.

Standard DLNA (ang. *Digital Living Network Alliance*) – standard, za pomocą którego można odtwarzać filmy albo muzykę bezpośrednio na nowoczesnym telewizorze lub innym odtwarzaczu.

Sterownik – oprogramowanie umożliwiające komputerowi komunikację ze sprzętem lub urządzeniami.

Strategie kopii zapasowych – określają kolejność używania nośników, np. taśm, potrzebnych do sporządzania kopii.

Strategia Dziadek–Ojciec–Syn (ang. *Grandfather/Father/Son*, GFS) – zapewnia możliwość odtworzenia danych z dowolnego dnia z pięciu ostatnich dni, dowolnego tygodnia z czterech ostatnich tygodni i dowolnego miesiąca (ograniczeniem jest wielkość archiwum organizacji).

Strategia Wieże Hanoi – pozwala w bezpieczny sposób odtwarzać dane starsze w jednym cyklu taśm.

Superdemon – narzędzie kontrolujące wybrane porty i uruchamiające usługi tylko w razie potrzeby.

Szum – niepożądany sygnał pochodzący ze źródeł naturalnych lub sztucznych.

System komputerowy – układ dwóch składowych współdziałających ze sobą: sprzętu komputerowego i oprogramowania.

System operacyjny (ang. *operating system*) – oprogramowanie zarządzające sprzętem komputerowym, tworzące środowisko do uruchamiania i kontroli zadań użytkownika.

System plików – podstawowa struktura używana przez komputer do organizowania danych na dysku twardym.

Ścieżka dostępu – ciąg znaków określający położenie dowolnego obiektu w strukturze plików.

Ścieżka krytyczna – nieprzerwany ciąg zadań o najdłuższym czasie realizacji.

Średnica sieci komputerowej – liczba urządzeń, przez które dane muszą przejść, zanim dotrą do swojego miejsca docelowego.

Światłowód (ang. *fiber optic cable*) – nośnik transmisji przewodowej, wykonany ze szkła kwarcowego lub specjalnego tworzywa sztucznego, przystosowany do przesyłania wiązki światła.

Tablet – urządzenie mające postać tabliczki z rysikiem, umożliwiające przenoszenie odręcznych rysunków i pisma bezpośrednio do komputera.

TELNET – protokół umożliwiający wykonywanie operacji na odległym komputerze.

TFTP (ang. *Trivial File Transfer Protocol*) – prosty protokół wykorzystywany do przesyłania plików.

Token Ring – technologia sieciowa, w której stosuje się metodę dostępu do nośnika nazywaną przekazywaniem żetonu (ang. *token-passing*).

Topologia fizyczna sieci – określa geometryczną organizację sieci lokalnej, graficznie przedstawiając jej kształt i strukturę.

Topologia logiczna sieci – opisuje reguły komunikacji, z których korzystają urządzenia komunikujące się w sieci.

Topologia sieci – określa sposób jej wykonania, czyli połączenia urządzeń komputerowych za pomocą medium transmisyjnego.

Transmisja dupleks (ang. *full-duplex*) – transmisja jednoczesna i dwukierunkowa.

Transmisja grupowa (ang. *multicast*) – transmisja, w której dane są przeznaczone tylko do wybranej grupy urządzeń.

Transmisja jednokierunkowa (ang. *simplex*) – transmisja, w której jedno z urządzeń tylko wysyła dane (nadajnik), a drugie urządzenie tylko odbiera dane (odbiornik).

Transmisja jednostkowa (ang. *unicast*) – w komunikacji biorą udział dwa urządzenia, jedno urządzenie wysyła dane do dokładnie jednego urządzenia.

Transmisja półdupleks (ang. *half-duplex*) – transmisja dwukierunkowa, naprzemienna.

Transmisja rozgłoszeniowa (ang. *broadcast*) – transmisja, w której dane są przeznaczone do wszystkich urządzeń w sieci.

Transmisja szerokopasmowa (ang. *broadband*) – polega na podziale pojedynczego łącza na wiele kanałów.

Transmisja w paśmie podstawowym (ang. *baseband*) – polega na utworzeniu w łączu tylko jednego kanału transmisyjnego, za pomocą którego jest przesyłany tylko jeden ciąg sygnałów.

Trasowanie, routing – proces wyznaczania trasy do miejsca przeznaczenia pakietów.

Tryb zgodności – specjalny tryb pracy systemu, w którym stara się on emulować środowisko starszego systemu operacyjnego,

dzięki czemu można korzystać ze starszych programów, napisanych dla innych systemów z rodziny Windows.

TWAIN – standard komunikacji między skanerami, aparatami cyfrowymi a programami graficznymi.

Urządzenia dostępu – urządzenia odpowiedzialne za formatowanie danych w taki sposób, aby nadawały się one do przesyłania w sieci, a także za umieszczanie danych w sieci i ich odbieranie.

Urządzenia peryferyjne – urządzenia umożliwiające komunikację użytkownika z systemem komputerowym.

Urządzenia transmisji – nośniki używane do transportu sygnałów biegnących przez sieć do miejsc docelowych.

Urządzenia wzmacniania przesłanych sygnałów – urządzenia, które odbierają przesyłane sygnały, wzmacniają je i wysyłają z powrotem do sieci.

USB (ang. *Universal Serial Bus*) – złącze uniwersalnej magistrali szeregowej.

Usługa APIPA (ang. *Automatic Private IP Addressing*) – usługa odpowiedzialna za automatyczne przydzielanie adresu IP komputerowi w przypadku, gdy karta sieciowa komputera jest skonfigurowana do żądania przyznania adresu IP z serwera DHCP, a serwer DHCP w danym momencie jest nieosiągalny.

Usługa DEP (ang. *Data Execution Prevention*) – ochrona przed przepełnieniami buforów; jest mechanizmem zabezpieczeń zintegrowanym w systemach z rodziny Windows. Umożliwia ochronę środowiska pracy przed działaniem wirusów i innego szkodliwego oprogramowania – monitoruje obszary pamięci i zapobiega aktywności złośliwego kodu na komputerze. Usługa działa na poziomie programowym i sprzętowym.

Usługa NAT (ang. *Network Address Translation*) – tłumaczenie adresów prywatnych na publiczne realizowane w bramie lub routerze.

Usługa SSH (ang. *Secure Shell*) – następca protokołu telnet, służy do terminalowego łączenia się ze zdalnymi komputerami. W odróżnieniu od telnetu transfer danych jest szyfrowany.

Usługi katalogowe – wyspecjalizowane bazy danych przeznaczone przede wszystkim do szybkiego czytania, przeglądania i przeszukiwania.

Wątek (ang. *thread*) – część programu wykonywana współbieżnie w obrębie jednego procesu.

Węzeł sieci – urządzenie sieciowe, w którym zbiega się wiele łączy komunikacyjnych.

Wielodostępność – oznacza, że wielu użytkowników może jednocześnie korzystać z systemu. Każdy użytkownik ma przydzielone zasoby, np. pamięć, czas procesora, miejsce na dysku, do których nikt oprócz niego nie ma dostępu, chyba że sam je udostępni.

Wielozadaniowość – cecha systemu operacyjnego umożliwiająca mu równoczesne wykonywanie więcej niż jednego procesu.

Wi-Fi – zestaw standardów stworzonych do budowy bezprzewodowych sieci komputerowych.

Wirtualna sieć lokalna, VLAN (ang. *Virtual Local Area Network*) – sieć komputerowa wydzielona logicznie w ramach innej większej sieci fizycznej.

Wirusy komputerowe – programy tworzone specjalnie do zakłócania pracy komputera, rejestrowania, uszkadzania lub usuwania danych albo rozprzestrzeniania się do innych komputerów za pomocą internetu, często w celu spowolnienia pracy systemu.

Współczynnik kompresji – miara stosunku rozmiaru pliku pierwotnego do jego rozmiaru po kompresji.

Wtyczki (ang. *plugins*) – zewnętrzne biblioteki lub programy, które umożliwiają przeglądarce obsługę innych dokumentów niż standardowe pliki HTML.

Wykres Gantta – typ wykresu ilustrującego terminarz działań.

Wyświetlacz LCD (ang. *Liquid Crystal Display*) – wyświetlacz korzystający z technologii wyświetlania obrazu polegającej na zmianie polaryzacji światła na skutek zmian orientacji cząsteczek ciekłego kryształu pod wpływem przyłożonego pola elektrycznego.

Wywłaszczanie – polega na przerwaniu wykonywania procesu, odebraniu mu czasu przydzielonego do wykonania zadania przez procesor i przekazaniu sterowania do planisty.

Wzmacniak, regenerator – urządzenie sieciowe wykorzystywane w miejscach, w których jest wymagane wzmocnienie lub regeneracja sygnału niezbędne do zwiększenia zasięgu sieci.

Zadanie drukowania (ang. *print job*) – powstaje w wyniku wydania polecenia drukowania przez oprogramowanie stacji roboczej.

Zapora sieciowa (ang. *firewall*) – jedna z możliwości zabezpieczania sieci i systemów komputerowych przed nieuprawnionym dostępem, np. z internetu, lub przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz.

Zasilacz UPS (zasilacz awaryjny) – wtórne źródło energii elektrycznej, które prąd pobiera z wcześniej naładowanych akumulatorów.

Zasoby projektu – środki niezbędne do zrealizowania projektu.

Znaki globalne – specjalne znaki zastępujące inne, np. * zastępuje dowolny ciąg znaków.

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH: POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
Active Directory	Active Directory	Active Directory
adres fizyczny MAC	physical address MAC – Media Access Control	Physische MAC Adresse (Media Access Control)
adres logiczny	logical address	die logische Adresse
adres prywatny	private IP address	die persönliche IP Adresse
adres rozgłoszeniowy	broadcast	die Sendeadresse
adres sieci	IP – Internet Protocol Address	IP-Adresse
agregat prądotwórczy	engine-generator	das stromerzeugende Aggregat
aktualizacja	update	die Aktualiesierung
architektura	architecture	die Architektur
architektura klient–serwer	client-server model	das Klient-Server-Modell
architektura równorzędna	peer-to-peer model	das Parallele Model
archiwizacja	data archiving	die Datenversicherung / die Archivierung
ataki aktywne	active attacks	die aktive Angriffe
ataki pasywne	passive attacks	die passive Angriffe
bezprzewodowa sieć lokalna WLAN	WLAN – Wireless Local Area Network	Wireless Local Area Network
bezprzewodowy	wireless / cordless	drahtlos / schnurlos
bit	bit	der Bit
brama sieciowa	network gateway	das Gateway
bramka VoIP	VoIP – Voice over IP gate	das Voice over IP – Tor
chłodzenie	cooling	die Kühlung
częstotliwość	frequency	die Frequenz / die Häufigkeit
czytnik książek elektronicznych	electronic book reader	Ebook-Reader
defragmentacja	defragmentation	die Defragmentierung
dekapsulacja	decapsulation	die Dekapsulation
demon	daemon	der Dämon
diagnostyka	diagnostics / diagnostic testing	die technische Überprüfung
domena	domain	das Domäne
dokumentacja	documentation	die Dokumentation

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
dokumentacja techniczna	technical documentation	die technische Dokumentation
domena kolizyjna	collision domain	die Kollisionsdomäin
domena rozgłoszeniowa	broadcast domain	die Übertragungsdomäne
domeny najwyższego poziomu	top-level domains	die Domäne oberster Stufe
dostawca usługi Internetu ISP	ISP – Internet Service Provider	der Internet-Dienstanbieter
drukarka	printer	der Drucker
drukarka lokalna	local printer	der Lokaler Drucker
drukarka sieciowa	network printer	die Netzwerkdrucker
dysponent	network administrator, trustee	der Anweisungsbefugte / der Netwerk administrator
dysk sieciowy	network drive	das Netzlaufwerk
dysk twardy	hard disk	die Festplatte
eksploatacja	operation / utilization / exploitation	der Betrieb / die Nutzung
enkapsulacja	encapsulation	die Ummantelung / die Kapselung
ergonomia	ergonomics	die Ergonomie
Ethernet / FastEthernet / Giga- bitEther-net	Ethernet / FastEthernet / Giga- bitEther-net	Ethernet / FastEthernet / GigabitEthernet
formatowanie	formatting	die Formatierung
fragmentacja	fragmentation	die Frarmentierung
głośnik	speaker	der Lautsprecher
główne serwery nazw	DNS – Domain Name System	das Domänennamesystem
główny punkt dystrybucyjny MDF	MDF – Main Distribution Facility	das Hauptabsatzkanal
gniazdo	socket	die Buchse / die Steckdose
gniazda abonenckie	socket (e.g. TV, telephone wall socket)	die Steckdose
gospodarowanie odpadami	waste management	die Abfallwirtschaft
grupa robocza	workgroup	die Arbeitsgruppe
grupy dyskusyjne	discussion group	die Diskusionsgruppe
host	host	der Host
instalacja	installation	die Installation
interfejs równoległy	parallel interface	die parallele Schnittstelle / das parallele Interface
interfejs szeregowy	serial interface	die serielle Schnittstelle / das serielle Interface
internet	Internet	das Internet
jasność	brightness	die Helligkeit
jednostka centralna	CPU – Central Processing Unit	die Zentraleinheit
jednostkowy nakład rzeczowy	unit pricing	die Einzelne Sachaufwendung
kabel koncentryczny	coaxial cable	das Koaxialkabel

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH: POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
kabel prosty	straight through / patch cable	das Patchkabel
kabel skrosowany	crossover cable	das Crossover-Kabel
kamień milowy	milestone	der Meillenstein
karta graficzna	graphics card / GFX	die Grafikkarte
karta sieciowa	network interface controller / adapter / card	die Netzkarte
karta muzyczna	sound card	die Musikkarte
karta pamięci	memory card	die Speicherkarte
karta rozszerzeń	expansion card	die Erweiterungskarte / die Stedkarte
katalog nakładów rzeczowych	unit pricing/ material outlays catalog	der Sachaufwendungskatalog
klawiatura	keyboard	die Tastatur
klient	client	der Kunde / der Benutzer
klucz rejestru	registry key	der Registrierungsschlüssel
komputerowy system sieciowy	network computer system	das Netzwerk – Computer – System
kolejka drukowania	print queue	die Druckerwarteschlange
koncentrator	hub	der Hub
kondensator	condenser	der Kondensator
konto użytkownika	user account	das Benutzerkonto
kontroler	controller	der Controller / das Stenergerät
kontroler domeny	domain controller	der Domänen-controller
kopia pełna	full copy	die volständige Sicherung
kopia przyrostowa	incremental copy	die volständige Sicherung
kopia różnicowa	differential copy	die inkrementelle Sicherung
kopia zapasowa	backup copy	die Sicherungsdatei / die Sicherheitskopie / die Datensichenng
kosztorys	estimated budget / cost estimation	die Berechnung / der Kostenvoranschlag
lista kontroli dostępu ACL	ACL – Access Control List	die ACL (Zugriffsstenerungsliste)
lista zgodności sprzętu HCL	HCL-Hardware Compatibility List	HCL-Hardware Compatibility List (die Hardware Kompatibilitätsliste)
logowanie	login	die Anmeldung
lokacja	location	der Standort / die Lokation
łącze komunikacyjne	communications link	die Kommunikationsverbindung / der Kommunikationslink
łączność bezprzewodowa	Wi-Fi	Wi-Fi (Drahtlose Übermittlung)
macierz	matrix / array	die Matrix
magistrala	Main / bus	der Bus
mapowanie dysków	disk mapping / drive mapping	die Laufwerkzuordnung
maska podsieci	subnet mask / IPv4 subnetting reference	die Subnetzmaske

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
materiał eksploatacyjny	operation material / consumable	das Betriebsmaterial
matryca	matrix	die Matrize
mechanizm PnP	Plug and Play mechanism	der PnP Mechanismus
medium transmisyjne	transmission medium	das Übertragungsmedium
mikser	mixer	der Mixer
moc	power	die Stärke
model hierarchiczny sieci	hierarchical network model	das hierarchische Netzwerkmodell
modem	modem	das Modem
modernizacja	modernization	die Modernisierung
moduł	module	das Modul
monitor	monitor / screen	der Bildschirm
montaż	assembly	die Montage
most	bridge	die Brücke / der Bus
mostek północny	northbridge	die Northbridge
mostek południowy	southbridge	die Southbridge
mysz	mouse	die Maus
nadmiarowość	redundancy	die Redundanz
nagłówek IP	IP header	IP-Überschrift
napięcie	voltage	die Spannung
napęd optyczny	optical drive	das optische Laufwerk
natężenie	intensity	die Stärke
netykieta	netiquette	die Netiquette
nośnik	medium	der Träger
obciążenie	load / encumbrance / overload	die Belastung
obiekt	object	das Objekt
obudowa	case / tower	das Gehäuse
odległość ogniskowa	focal length	die Brennweite
odtwarzacz MP3	MP3 player	MP3-Player
odzyskiwanie danych	data recovery	die Datenwiederherstellung
okablowanie pionowe (wewnątrz budynku)	vertical cabling	die Vertikale Verkabelung
okablowanie poziome	horizontal cabling	die Horizontale Verkabelung
okablowanie strukturalne	structured cabling	Struktivere / die gegliederte Verkabelun
oprogramowanie biurowe	office software	die Bürosoftware
oprogramowanie diagnostyczne	diagnostic software	die Diagnose-Software

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH: POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
oprogramowanie komunikacyjne	communications software	die Kommunikationssoftware
oprogramowanie monitorujące	monitoring software	die Überwachungssoftware
oprogramowanie narzędziowe	utility software	die Gebrauchssoftware
oprogramowanie użytkowe	application software	die Anwendungssoftware
opóźnienie urządzenia sieciowego	propagation delay	die Netzwerkgeraet-Verzögerung
pakiet	packet / suite (e.g. office suite)	das Paket
pamięć	memory	der Speicher
pamięć masowa	mass storage	der Massenspeicher
pamięć operacyjna	RAM – Random Access Memory	der Arbeitsspeicher RAM
pamięć RAM	RAM – Random Access Memory	der RAM / Direktzugriffsspeicher
pamięć ROM	ROM – Read-Only Memory	der ROM – Speicher
papier elektroniczny	electronic paper	elektronisches Papier
partycja	partition	die Partition
partycja podstawowa	primary partition	primäre Partition
partycja rozszerzona	extended partition	erweitere Partition
plik stronicowania	paging file	die Auslagerungsdatei
planista	planner	der Planer
poczta elektroniczna	e-mail	e-mail, elektronische Post
polityka bezpieczeństwa	information security policy	die Sicherheitspolitik
płyta główna	mainboard / motherboard	die Hauptplatine
pobór mocy	power consumption	die Leistungsaufnahme
pojemność	capacity	die Kapazität
połączenia systemowe	system connection	die Systemverbindung
połączenia telekomunikacyjne budynków (okablowanie międzybudynkowe lub kampusowe)	cross-building structured cabling	die Kommunikationsverbindung
port protokołu	port protocol	die Protokoll Schnittstelle
podpis cyfrowy	digital signature	digitale Signatur
pośredni punkt dystrybucyjny IDF	IDF – Intermediate Distribution Facility	der Indirekte Verteilungspunkt (IDF)
prąd elektryczny	electric current	der elektrische Strom
priorytet	priority	das Priorität
proces	process	der Prozess
procesor	processor / CPU	der Prozessor
procesor graficzny	graphics processing unit	der Grafikprozessor
profil użytkownika	user profile	das Benutzerprofil
program antywirusowy	antivirus	das Antivirenprogramm

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
program szpiegujący	spyware	die Spyware
projekt	project	das Projekt
protokoły	protocols	die Protokolle
protokoły bezpołączeniowe	connectionless protocols	die Verbindungslosen Protokolle
protokoły internetowe	Internet protocols	die Internetprotokolle
protokoły komunikacyjne	communications protocols	die Kommunikationsprotokolle
protokoły połączeniowe	connection-oriented protocols	das Connection Protokoll / das Verbindungsprotokoll
protokoły routingu	routing protocol	das Routingprotokoll
protokół IP	IP – Internet Protocol	das IP – Internet Protokoll
protokół UDP	UDP – User Datagram Protocol	das UPD – Benutzer Datagramm Protokoll
protokół SNMP	SNMP – Simple Network Management Protocol	das SNMP – Simple Network Management Protokoll
protokół STP	STP – Spanning Tree Protocol	das STP – Protokoll
protokół TCP	TCP – Transmission Control Protocol	das TCP – Transmission Control Protokoll / das Übertragungssteue rungsprotokoll
protokół TFTP	TFTP – Trivial File Transfer Protocol	das TFTP Transmission Control Protokoll
przekazywanie żetonu	token passing	die Token-Übermittlung
przełącznik	switch	der Umschalter
przewodowy	wired	Leitungs – drahtgebunden verd rahtet verkabelt
pulpit	desktop	die Arbeitsumgebung
punkt demarkacyjny	demarcation point	der Demarkationspunkt / der Grenzpunkt
punkt dostępowy	AP – Access Point	der Anschlusspunkt / die Anschlussstelle
punkt montowania	mount point	der Mount-Punkt / der Einhängepunkt
punkty rozdzielcze	distribution points	die Ausgabestellen
radiator	radiator	der Radiator / der Heizkörper
ramka	frame	der Rahmen
rejestr	registry	das Register; das Verzeichnis
rezystor	resistor	der Widerstand
router	router	der Router
rozdzielczość	resolution	die Auflösung
rysunek techniczny	technical drawing	die technische Zeichnung
segment	segment	das Segment

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH: POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
serwer	server	der Server
serwer pośredniczący	proxy server	das Segment / die Gruppe
sieciowy system operacyjny	NOS – Network Operating System	das Netzwerk-Betriebssystem
sieć komputerowa	computer network	das Computernetz
sieci osobiste PAN	PAN – Personal Area Network	das Personale Netz
sieci lokalne LAN	LAN – Local Area Network	das Lokale Netz
sieci miejskie MAN	MAN – Metropolitan Area Net- work / Municipal Area Network	das Metropolraumnetz
sieci rozległe WAN	WAN – Wide Area Network	das Weitverkehrsnetz (WAN)
skalowalność	scalability	die Skalierbarkeit
skaner	scanner	der Scanner
skrętka	twisted-pair cable	die Litze
sniffer	sniffer	der Sniffer / das Suchgerat
stanowisko pracy	workstation / workplace	der Arbeitsplatz
sterownik	driver	der Treiber
styki	points / joints	die Verbindungsstellen
superdemon	super demon	der Superdämon
synchronizacja	synchronization	die Synchronisation
system informatyczny	IT system	das IT System (das Informations-tech-nologische System)
system komputerowy	computer system	das Computersystem
system operacyjny	data bus	der Datenbus
system plików	file system	das Dateisystem
szum	noise	die Geräusche / das Gerausch
szyna danych	data bus	der Datenbus
ścieżka dostępu	path	der Pfad
ścieżka krytyczna	CPM – Critical Path Method	der kritische Pfad
średnica sieci komputerowej	network diameter	der Netzwerkdiameter
światłowód	fiber-optic cable / optical fibre	der Lichtleiter / die Lichtleitfaser
telnet	telnet	der Telnet-Dienst
toner	toner	der Toner
Token Ring	Token Ring	der Token Ring
topologia sieci	network topology	die Netzwerktopologie
topologia fizyczna sieci	physical network topology	die Physikalische Topologie des Netzwerks
topologia logiczna sieci	logical network topology	die Logische Topologie des Netzwerks
tusz	ink	die Tinte

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
transmisja	transmission / broadcasting	die Übertragung
transmisja dupleks	duplex transmission	Duplex / die doppelseitige Übertragung
transmisja grupowa	multicasting transmission	das Multicast
transmisja jednokierunkowa	simplex communication	die Simplexkommunikation
transmisja jednostkowa	unicast transmission	die Einheitliche Übermittlung / die Unit-Transmission
transmisja półdupleks	half duplex	die Halbduplex-Übertragung
transmisja rozgłoszeniowa	broadcast transmission	die Übertragung / die Sendung
transmisja szerokopasmowa	broadband transmission	die Breitband-Ubertragung
transmisja w paśmie podstawowym	baseband transmission	Übermittlung im Basisfrequenzband / die Grundfrequenzband
transformator	transformer	der Transformator
trasowanie / routing	routing	das Routing
układ sterujący	control system	das Steuerwerk; das Leitwerk
urządzenia dostępu	access device	die Zugangsgeräte
urządzenia transmisji	DCE – Data Communications Equipment	die Übertragungseinrichtung
urządzenia wzmacniania przesłanych sygnałów	signal booster device	das Signalverstärkungsgerät
urządzenie peryferyjne	peripheral (device)	das Peripheriegerät
urządzenie wielofunkcyjne	multifunction device	das Multifunktionsgerat
usługa APIPA	APIPA – Automatic Private IP Addressing	die Automatische private IP Adresseirung (APIPA)
usługa DEP	DEP – Data Execution Prevention service	DEP-Dienst (Data Execution Prevention service)
usługa NAT	NAT – Network Address Translation	die NAT-Netzwerkadresseübersetzung
usługa SSH	SSH – Secure Shell Service	SS – Dienst (Secure Shell Service)
usługi katalogowe	directory service	der Katalogdienst
usterka	malfunction	die Panne, die; Funktionsstörung
wejście	input	der Eingang
węzeł sieci	node network	der Netzknoten
wentylator	fan / ventilator	der Lüfter / der Ventilator
wielodostępność	multi-user	das Mehrbenutzersystem
wielozadaniowość	multitasking	der Multitasking
wirtualna sieć lokalna VLAN	VLAN – Virtual Local Area Network	das Virtuelle Lokalnetzwerk (VLAN)
wirus komputerowy	virus	das Computervirus
współczynnik kompresji	compression rate	der Kompressionswert
wtyczka	plugin	das Modul

WYKAZ PODSTAWOWYCH POJĘĆ W JĘZYKACH: POLSKIM, ANGIELSKIM I NIEMIECKIM

JĘZYK POLSKI	JĘZYK ANGIELSKI	JĘZYK NIEMIECKI
wyjście	output	der Ausgang
wykres Gantta	Gannt chart	das Gannt-Diagramm
wyświetlacz	display	das Display / die Anzeige
wzmacniacz	amplifier / booster	der Verstärker
wzmacniak, regenerator	repeater	der Repeater / der Verstärker
zapora sieciowa	firewall	die Firewall
zadanie drukowania	print job	der Druckerauftrag
zasilacz	feeder / power supply (unit)	das Netzteil / die Stromversorgung
zasilacz awaryjny UPS	UPS – Uninterruptible Power Supply	UPS – ungestörte / die ununterbrochene Stromversorgung
zasoby projektu	project resources	die Projekt-Ressourcen
zdalny	remote access	der Fernzugriff
złącze	joint / junction / socket	die Schnittstelle
znaki globalne	global signs	die Globalzeichen

Wydawnictwa Szkolne i Pedagogiczne oświadczają, że podjęły starania mające na celu dotarcie do właścicieli i dysponentów praw autorskich zamieszczonych utworów. Wydawnictwa Szkolne i Pedagogiczne, przytaczając w celach dydaktycznych utwory lub fragmenty, postępują zgodnie z art. 27^1 ustawy o prawie autorskim. Jednocześnie Wydawnictwa Szkolne i Pedagogiczne oświadczają, że są jedynym podmiotem właściwym do kontaktu autorów tych utworów lub innych podmiotów uprawnionych w wypadkach, w których twórcy przysługuje prawo do wynagrodzenia.