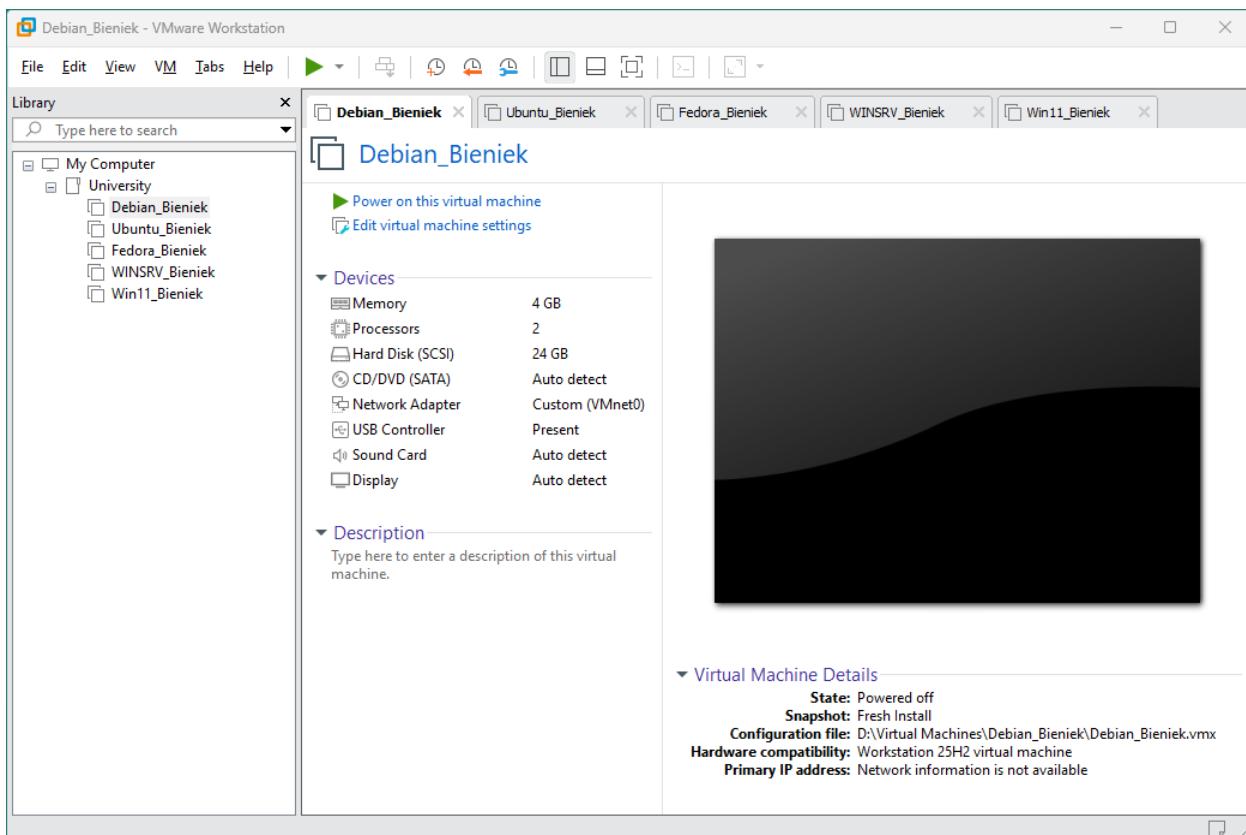


Bartosz Bieniek

gr. 7, st. 1, sem. 3, Informatyka RMS

Przygotowanie środowiska.

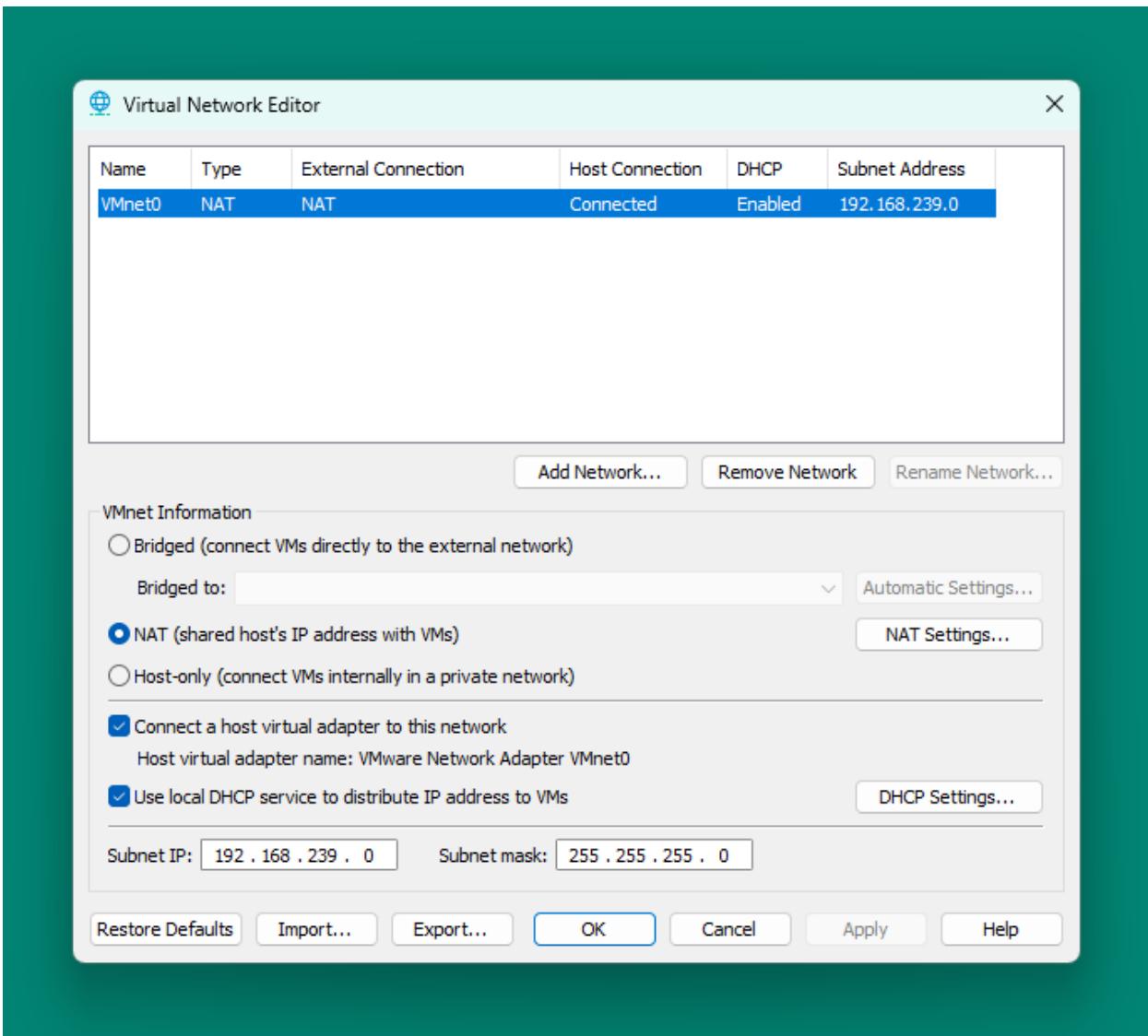
Do realizacji zadań wykorzystałem narzędzie wirtualizacyjne *VMware Workstation* pod kontrolą systemu *Windows 11 Pro*. W środowisku przygotowałem i skonfigurowałem pięć maszyn wirtualnych – trzy serwerowe dystrybucje *Linux – Debian 12 Bookworm, Ubuntu Server 24.04.3 LTS, Fedora Server 39* oraz *Windows Server 2025* i *Windows 11 Pro*. Każdej z nich przydzieliłem po 4 GB pamięci operacyjnej, dwa wątki procesora oraz 24 GB (*Linux*) lub 64 GB (*Windows*) przestrzeni dyskowej.



Zrzut ekranu 1 Podsumowanie konfiguracji maszyny wirtualnej z systemem *Debian 12 Bookworm*.

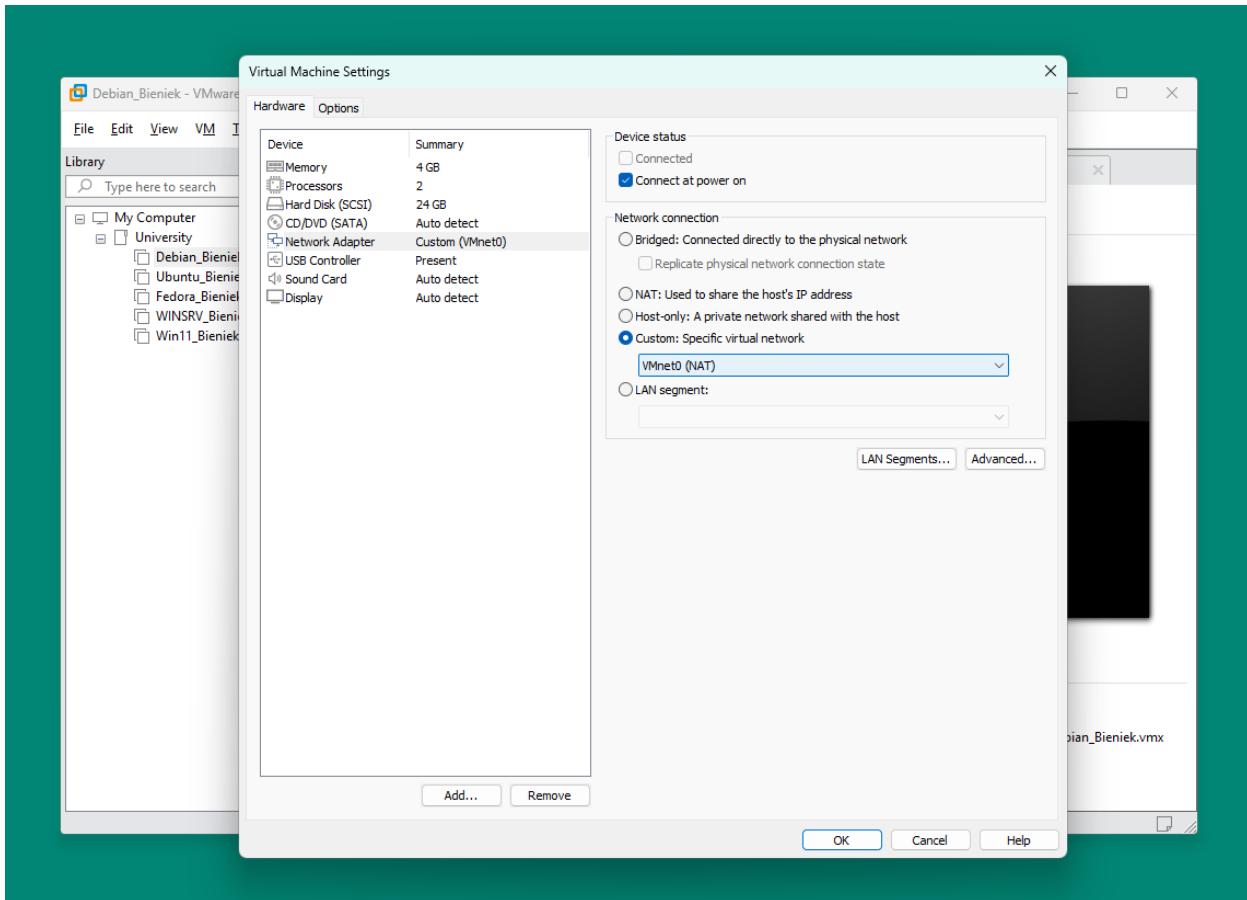
Ze względu na charakter zadania i bardzo różne poinstalacyjne konfiguracje kont w wyżej wymienionych systemach, zdecydowałem się aktywować we wszystkich systemach operacyjnych konta administracyjne (użytkownik *root* bądź *Administrator*) i usunąć wszystkich pozostałych użytkowników.

Do wykonania ćwiczenia konieczne jest także podłączenie maszyn wirtualnych do internetu i umożliwienie komunikacji między nimi oraz komputerem hosta. W tym celu utworzyłem w oprogramowaniu wirtualizacyjnym nową sieć (*Edit Virtual Network Editor...*) typu *NAT*, podłączyłem do niej wirtualną kartę sieciową komputera gospodarza i uruchomiłem usługę *DHCP*.



Zrzut ekranu 2 Konfiguracja sieci wirtualnej.

Do tak utworzonej sieci podłączyłem wszystkie maszyny wirtualne.



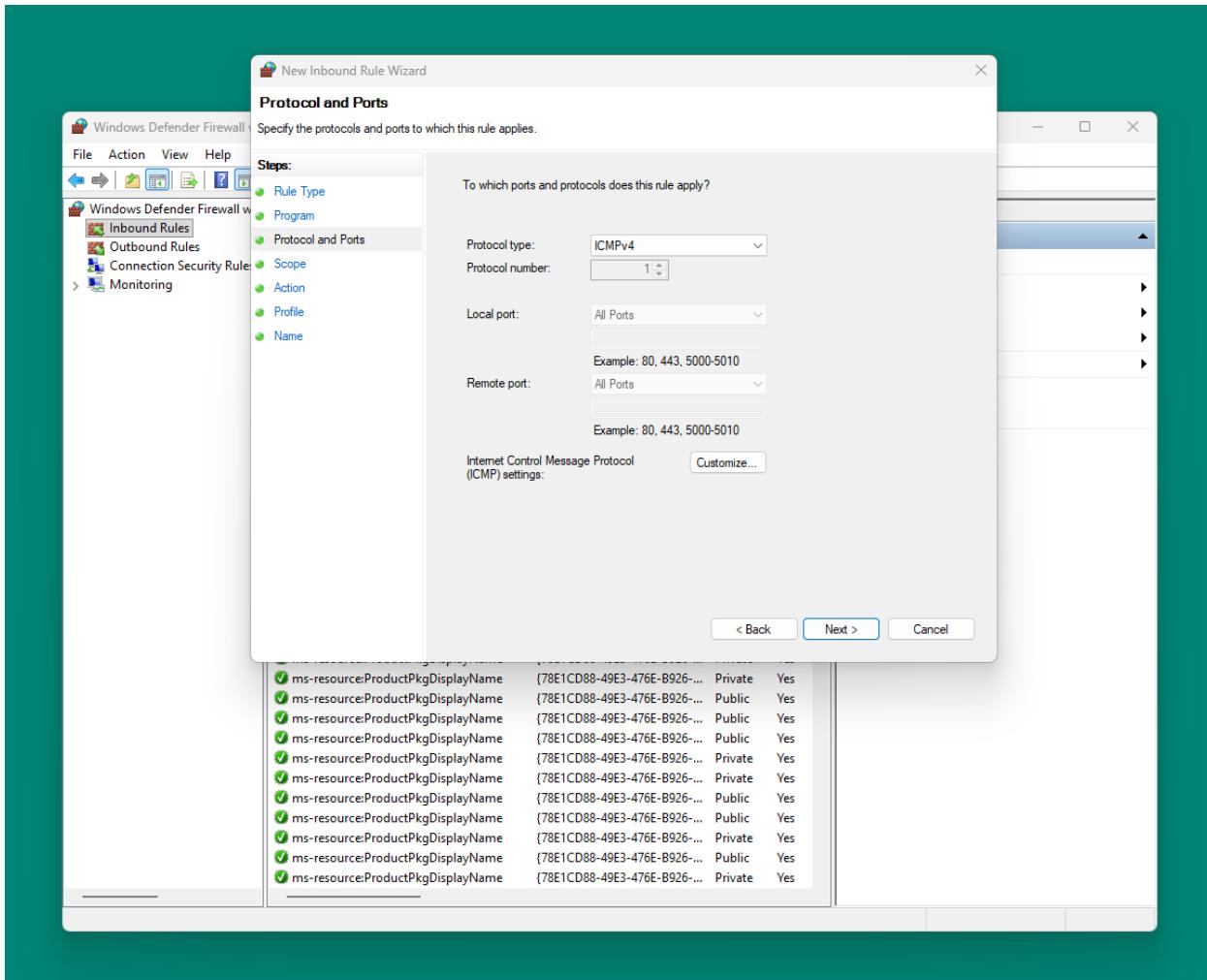
Zrzut ekranu 3 Podłączanie maszyn wirtualnych do utworzonej sieci.

Na koniec odczytałem nadane przez usługę DHCP adresy sieciowe i przetestowałem komunikację sieciową wykonując polecenie ping na dowolny serwer w internecie, komputer gospodarza oraz pozostałe wirtualne maszyny.

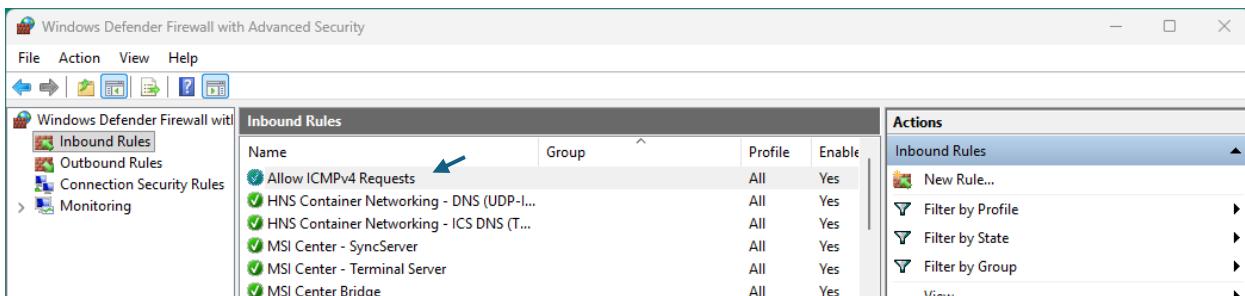
Nazwa	Adres IP
Komputer gospodarza	192.168.239.1
Debian	192.168.239.128
Ubuntu	192.168.239.129
Fedora	192.168.239.130
Windows Server	192.168.239.131
Windows 11	192.168.239.132

Tabela 1 Dane adresowe nadane przez usługę DHCP.

Należy pamiętać, iż przychodzące żądania ping są domyślnie blokowane przez zaporę systemu Windows, stąd konieczne jest dodanie odpowiedniego wyjątku na dwóch maszynach wirtualnych i komputerze hosta.



Zrzut ekranu 4 Dodanie wyjątku na żądania ICMPv4 (ping) do zapory sieciowej w systemie Windows.



Zrzut ekranu 5 Dodany w zaporze sieciowej wyjątek na żądania ping.

```

root@debian:~# ip a s
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 noprefixroute
            valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:77:37:71 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.239.128/24 brd 192.168.239.255 scope global dynamic ens3
            valid_lft 1783sec preferred_lft 1783sec
        inet6 fe80::20c:29ff:fe77:3771/64 scope link
            valid_lft forever preferred_lft forever
root@debian:~# ping google.com
PING google.com (142.251.98.139) 56(84) bytes of data.
64 bytes from nt-in-f139.ie100.net (142.251.98.139): icmp_seq=1 ttl=128 time=8.58 ms
64 bytes from nt-in-f139.ie100.net (142.251.98.139): icmp_seq=2 ttl=128 time=13.7 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 8.581/11.147/13.714/2.566 ms
root@debian:~# ping 192.168.239.1
PING 192.168.239.1 (192.168.239.1) 56(84) bytes of data.
64 bytes from 192.168.239.1: icmp_seq=1 ttl=128 time=0.692 ms
64 bytes from 192.168.239.1: icmp_seq=2 ttl=128 time=0.496 ms
^C
--- 192.168.239.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 0.496/0.594/0.692/0.098 ms
root@debian:~# ping 192.168.239.129
PING 192.168.239.129 (192.168.239.129) 56(84) bytes of data.
64 bytes from 192.168.239.129: icmp_seq=1 ttl=64 time=0.437 ms
64 bytes from 192.168.239.129: icmp_seq=2 ttl=64 time=0.419 ms
^C
--- 192.168.239.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/msdev = 0.419/0.428/0.437/0.009 ms
root@debian:~# ping 192.168.239.130
PING 192.168.239.130 (192.168.239.130) 56(84) bytes of data.
64 bytes from 192.168.239.130: icmp_seq=1 ttl=64 time=0.513 ms
64 bytes from 192.168.239.130: icmp_seq=2 ttl=64 time=0.374 ms
^C
--- 192.168.239.130 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.374/0.443/0.513/0.069 ms
root@debian:~# ping 192.168.239.131
PING 192.168.239.131 (192.168.239.131) 56(84) bytes of data.
64 bytes from 192.168.239.131: icmp_seq=1 ttl=128 time=0.463 ms
64 bytes from 192.168.239.131: icmp_seq=2 ttl=128 time=0.401 ms
^C
--- 192.168.239.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1020ms
rtt min/avg/max/mdev = 0.401/0.432/0.468/0.031 ms
root@debian:~# ping 192.168.239.132
PING 192.168.239.132 (192.168.239.132) 56(84) bytes of data.
64 bytes from 192.168.239.132: icmp_seq=1 ttl=128 time=0.495 ms
64 bytes from 192.168.239.132: icmp_seq=2 ttl=128 time=0.518 ms
^C
--- 192.168.239.132 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.495/0.506/0.518/0.011 ms
root@debian:~#

```

Zrzut ekranu 6 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Debian.

```

root@ubuntuserver:~# ip a s
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 noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:22:02:70 brd ff:ff:ff:ff:ff:ff
        altnet enp2s1
        inet 192.168.239.129/24 metric 100 brd 192.168.239.255 scope global dynamic ens33
            valid_lft 990sec preferred_lft 990sec
        inet6 fe80::20c:29ff:fe22:270/64 scope link
            valid_lft forever preferred_lft forever
root@ubuntuserver:~# ping google.com
PING google.com (142.251.98.138) 56(84) bytes of data.
64 bytes from nt-in-f138.1e100.net (142.251.98.138): icmp_seq=1 ttl=128 time=13.2 ms
64 bytes from nt-in-f138.1e100.net (142.251.98.138): icmp_seq=2 ttl=128 time=13.5 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 13.155/13.315/13.475/0.160 ms
root@ubuntuserver:~# ping 192.168.239.1
PING 192.168.239.1 (192.168.239.1) 56(84) bytes of data.
64 bytes from 192.168.239.1: icmp_seq=1 ttl=128 time=0.412 ms
64 bytes from 192.168.239.1: icmp_seq=2 ttl=128 time=0.398 ms

--- 192.168.239.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1016ms
rtt min/avg/max/mdev = 0.398/0.405/0.412/0.007 ms
root@ubuntuserver:~# ping 192.168.239.128
PING 192.168.239.128 (192.168.239.128) 56(84) bytes of data.
64 bytes from 192.168.239.128: icmp_seq=1 ttl=64 time=0.405 ms
64 bytes from 192.168.239.128: icmp_seq=2 ttl=64 time=0.467 ms
^C
--- 192.168.239.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.405/0.436/0.467/0.031 ms
root@ubuntuserver:~# ping 192.168.239.130
PING 192.168.239.130 (192.168.239.130) 56(84) bytes of data.
64 bytes from 192.168.239.130: icmp_seq=1 ttl=64 time=0.427 ms
64 bytes from 192.168.239.130: icmp_seq=2 ttl=64 time=0.435 ms
^C
--- 192.168.239.130 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1029ms
rtt min/avg/max/mdev = 0.427/0.431/0.435/0.004 ms
root@ubuntuserver:~# ping 192.168.239.131
PING 192.168.239.131 (192.168.239.131) 56(84) bytes of data.
64 bytes from 192.168.239.131: icmp_seq=1 ttl=128 time=0.441 ms
64 bytes from 192.168.239.131: icmp_seq=2 ttl=128 time=0.416 ms
^C
--- 192.168.239.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.416/0.428/0.441/0.012 ms
root@ubuntuserver:~# ping 192.168.239.132
PING 192.168.239.132 (192.168.239.132) 56(84) bytes of data.
64 bytes from 192.168.239.132: icmp_seq=1 ttl=128 time=0.563 ms
64 bytes from 192.168.239.132: icmp_seq=2 ttl=128 time=0.494 ms
^C
--- 192.168.239.132 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1040ms
rtt min/avg/max/mdev = 0.494/0.528/0.563/0.034 ms
root@ubuntuserver:~#

```

Zrzut ekranu 7 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Ubuntu.

```
[root@localhost ~]# ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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 noprefixroute
            valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:91:68:0c brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.239.130/24 brd 192.168.239.255 scope global dynamic noprefixroute ens160
        valid_lft 912sec preferred_lft 912sec
    inet6 fe80::20c:29ff:fe91:680c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@localhost ~]# ping google.com
PING google.com (142.251.98.101) 56(84) bytes of data.
64 bytes from nt-in-f101.1e100.net (142.251.98.101): icmp_seq=1 ttl=128 time=13.6 ms
64 bytes from nt-in-f101.1e100.net (142.251.98.101): icmp_seq=2 ttl=128 time=13.1 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 13.072/13.326/13.580/0.254 ms
[root@localhost ~]# ping 192.168.239.1
PING 192.168.239.1 (192.168.239.1) 56(84) bytes of data.
64 bytes from 192.168.239.1: icmp_seq=1 ttl=128 time=0.933 ms
64 bytes from 192.168.239.1: icmp_seq=2 ttl=128 time=0.305 ms
^C
--- 192.168.239.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1065ms
rtt min/avg/max/mdev = 0.305/0.619/0.933/0.314 ms
[root@localhost ~]# ping 192.168.239.128
PING 192.168.239.128 (192.168.239.128) 56(84) bytes of data.
64 bytes from 192.168.239.128: icmp_seq=1 ttl=64 time=0.396 ms
64 bytes from 192.168.239.128: icmp_seq=2 ttl=64 time=0.334 ms
^C
--- 192.168.239.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.334/0.365/0.396/0.031 ms
[root@localhost ~]# ping 192.168.239.129
PING 192.168.239.129 (192.168.239.129) 56(84) bytes of data.
64 bytes from 192.168.239.129: icmp_seq=1 ttl=64 time=0.432 ms
64 bytes from 192.168.239.129: icmp_seq=2 ttl=64 time=0.378 ms
^C
--- 192.168.239.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.378/0.405/0.432/0.027 ms
[root@localhost ~]# ping 192.168.239.131
PING 192.168.239.131 (192.168.239.131) 56(84) bytes of data.
64 bytes from 192.168.239.131: icmp_seq=1 ttl=128 time=0.392 ms
64 bytes from 192.168.239.131: icmp_seq=2 ttl=128 time=0.418 ms
^C
--- 192.168.239.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1057ms
rtt min/avg/max/mdev = 0.392/0.405/0.418/0.013 ms
[root@localhost ~]# ping 192.168.239.132
PING 192.168.239.132 (192.168.239.132) 56(84) bytes of data.
64 bytes from 192.168.239.132: icmp_seq=1 ttl=128 time=0.447 ms
64 bytes from 192.168.239.132: icmp_seq=2 ttl=128 time=0.389 ms
^C
--- 192.168.239.132 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.389/0.418/0.447/0.029 ms
[root@localhost ~]#
```

Zrzut ekranu 8 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Fedora.

```
Administrator: Windows Pow + 
PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-344LUQC1RII
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-37-B9-96
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::822e:996c:7e17:fe14%6(PREFERRED)
IPv4 Address. . . . . : 192.168.239.131(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, December 20, 2025 6:16:31 PM
Lease Expires . . . . . : Saturday, December 20, 2025 7:01:31 PM
Default Gateway . . . . . : 192.168.239.2
DHCP Server . . . . . : 192.168.239.254
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-D8-ED-D1-00-0C-29-37-B9-96
DNS Servers . . . . . : 192.168.239.2
Primary WINS Server . . . . . : 192.168.239.2
NetBIOS over Tcpip . . . . . : Enabled

PS C:\Users\Administrator> ping google.com

Pinging google.com [142.251.98.102] with 32 bytes of data:
Reply from 142.251.98.102: bytes=32 time=8ms TTL=128
Reply from 142.251.98.102: bytes=32 time=8ms TTL=128

Ping statistics for 142.251.98.102:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.1

Pinging 192.168.239.1 with 32 bytes of data:
Reply from 192.168.239.1: bytes=32 time<1ms TTL=128
Reply from 192.168.239.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.1:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.128

Pinging 192.168.239.128 with 32 bytes of data:
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.128:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.129

Pinging 192.168.239.129 with 32 bytes of data:
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.129:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.130

Pinging 192.168.239.130 with 32 bytes of data:
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.130:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
```

```
PS C:\Users\Administrator> ping 192.168.239.132
Pinging 192.168.239.132 with 32 bytes of data:
Reply from 192.168.239.132: bytes=32 time<1ms TTL=128
Reply from 192.168.239.132: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.132:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator>
```

Zrzut ekranu 9 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Windows Server.

```
Administrator: Windows Pow > + ▾
PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-T4CPOOU
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-DA-8C-5C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4b77:a9fb:e7e7:ce18%14(PREFERRED)
IPv4 Address . . . . . : 192.168.239.132(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, December 20, 2025 6:16:42 PM
Lease Expires . . . . . : Saturday, December 20, 2025 7:01:42 PM
Default Gateway . . . . . : 192.168.239.2
DHCP Server . . . . . : 192.168.239.254
DHCPv6 IAID . . . . . : 83889193
DHCPv6 Client DUID. . . . . : 00-01-00-01-30-D8-E9-B1-00-0C-29-DA-8C-5C
DNS Servers . . . . . : 192.168.239.2
Primary WINS Server . . . . . : 192.168.239.2
NetBIOS over Tcpip. . . . . : Enabled

PS C:\Users\Administrator> ping google.com

Pinging google.com [142.251.98.100] with 32 bytes of data:
Reply from 142.251.98.100: bytes=32 time=11ms TTL=128
Reply from 142.251.98.100: bytes=32 time=11ms TTL=128

Ping statistics for 142.251.98.100:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 11ms, Average = 11ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.1

Pinging 192.168.239.1 with 32 bytes of data:
Reply from 192.168.239.1: bytes=32 time<1ms TTL=128
Reply from 192.168.239.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.128

Pinging 192.168.239.128 with 32 bytes of data:
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.128:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
```

```
PS C:\Users\Administrator> ping 192.168.239.129
Pinging 192.168.239.129 with 32 bytes of data:
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.129:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.130

Pinging 192.168.239.130 with 32 bytes of data:
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.131

Pinging 192.168.239.131 with 32 bytes of data:
Reply from 192.168.239.131: bytes=32 time<1ms TTL=128
Reply from 192.168.239.131: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.131:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> |
```



Zrzut ekranu 10 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Windows 11.

Zadanie 1.1. Konfiguracja sieciowa.

Aby zapobiec nieoczekiwany zmianom konfiguracji sieciowej w trakcie wykonywania ćwiczenia, przypiszę statycznie – uzyskane wcześniej z wykorzystaniem *DHCP* – dane adresowe *IPv4*.

Do sprawdzenia aktualnej konfiguracji sieciowej wykorzystam polecenia *ip a s*, pokazujące przypisane na interfejsach adresy, *ip r*, pokazujące informacje o trasie domyślnej (bramie domyślnej) oraz wypiszę zawartość pliku */etc/resolv.conf* zawierającego definicje serwerów *DNS*.

```
root@debian:~# ip a s
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 noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:77:37:71 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
        inet 192.168.239.128/24 brd 192.168.239.255 scope global ens33
            valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:fe77:3771/64 scope link
            valid_lft forever preferred_lft forever
root@debian:~# ip r
default via 192.168.239.2 dev ens33 onlink
192.168.239.0/24 dev ens33 proto kernel scope link src 192.168.239.128
root@debian:~# cat /etc/resolv.conf
domain localdomain
search localdomain
nameserver 192.168.239.2
```

Zrzut ekranu 11 Odczytanie danych adresowych w systemie Debian.

Konfigurację sieciową w systemie *Debian* wykonuje się z poziomu pliku */etc/network/interfaces*. Po wprowadzeniu zmian konieczny jest restart usługi *networking*.

```
root@debian:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
iface ens33 inet static
    address 192.168.239.128/24
    gateway 192.168.239.2
    dns-nameservers 192.168.239.2
root@debian:~# systemctl restart networking
```

Zrzut ekranu 12 Statyczne przypisanie danych adresowych w systemie Debian.

```
root@debian:~# ip a s
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
    inetc6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:77:37:71 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.239.128/24 brd 192.168.239.255 scope global ens33
            valid_lft forever preferred_lft forever
        inetc6 fe80::20c:29ff:fe77:3771/64 scope link
            valid_lft forever preferred_lft forever
root@debian:~# ip r
default via 192.168.239.2 dev ens33 onlink
192.168.239.0/24 dev ens33 proto kernel scope link src 192.168.239.128
root@debian:~# cat /etc/resolv.conf
domain localdomain
search localdomain
nameserver 192.168.239.2
```

Zrzut ekranu 13 Odczytanie danych adresowych w systemie Debian po wprowadzeniu zmian w konfiguracji sieciowej.

Zmiany konfiguracji ustawień sieciowych w systemie Ubuntu dokonuje się z przy pomocy narzędzia *netplan*. Obecny stan usługi oraz przydzieloną adresację można sprawdzić polecienniem *netplan status*.

```
root@ubuntuserver:~# netplan status
  Online state: online
  DNS Addresses: 127.0.0.53 (stub)
                  DNS Search: localdomain

• 1: lo ethernet UNKNOWN/UP (unmanaged)
  MAC Address: 00:00:00:00:00:00
  Addresses: 127.0.0.1/8
              ::1/128

• 2: ens33 ethernet UP (networkd: ens33)
  MAC Address: 00:0c:29:22:02:70 (Intel Corporation)
  Addresses: 192.168.239.129/24 (dynamic, dhcp)
              fe80::20c:29ff:fe22:270/64 (link)
  DNS Addresses: 192.168.239.2
  DNS Search: localdomain
  Routes: default via 192.168.239.2 from 192.168.239.129 metric 100 (dhcp)
          192.168.239.0/24 from 192.168.239.129 metric 100 (link)
          192.168.239.2 from 192.168.239.129 metric 100 (dhcp, link)
          fe80::/64 metric 256
root@ubuntuserver:~# -
```

Zrzut ekranu 14 Odczytanie danych adresowych w systemie Ubuntu.

W systemie Ubuntu konfiguracji sieciowej dokonuje się z poziomu pliku(ów) YAML, znajdujących się w folderze */etc/netplan/*. Przy tworzeniu ostatecznej konfiguracji brane są pod uwagę wszystkie z nich, przy czym te występujące dalej w kolejności leksykograficznej biorą górę w przypadku konfliktu ustawień.

```
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: false
      addresses:
        - 192.168.239.129/24
      routes:
        - to: default
          via: 192.168.239.2
      nameservers:
        addresses:
          - 192.168.239.2
~
```

Zrzut ekranu 15 Konfiguracja ustawień sieciowych z wykorzystaniem *netplan* (plików YAML) w systemie Ubuntu.

Po wprowadzeniu zmian do pliku, nowe ustawienia sieciowe można przetestować przez 120 sekund poleceniem *netplan try*. Po sprawdzeniu poprawności konfiguracji, można zatwierdzić ją enterem lub wydając polecenie *netplan apply*.

```
root@ubuntuserver:~# netplan try
Do you want to keep these settings?

Press ENTER before the timeout to accept the new configuration

Changes will revert in 40 seconds
Configuration accepted.
root@ubuntuserver:~# _
```

Zrzut ekranu 16 Testowe, tymczasowe wprowadzenie konfiguracji sieciowej.

```
root@ubuntuserver:~# netplan status
  Online state: online
  DNS Addresses: 127.0.0.53 (stub)
  DNS Search: .

• 1: lo ethernet UNKNOWN/UP (unmanaged)
  MAC Address: 00:00:00:00:00:00
    Addresses: 127.0.0.1/8
                ::/128

• 2: ens33 ethernet UP (networkd: ens33)
  MAC Address: 00:0c:29:22:02:70 (Intel Corporation)
    Addresses: 192.168.239.129/24
                fe80::20c:29ff:fe22:270/64 (link)
  DNS Addresses: 192.168.239.2
    Routes: default via 192.168.239.2 (static)
              192.168.239.0/24 from 192.168.239.129 (link)
              fe80::/64 metric 256
root@ubuntuserver:~# _
```

Zrzut ekranu 17 Odczytanie danych adresowych w systemie Ubuntu po wprowadzeniu zmian w konfiguracji sieciowej.

Jak widać, ręcznie przydzielone dane adresowe są zgodne z tymi, które zostały wcześniej nadane automatycznie w ramach usługi *DHCP*. Warto zwrócić uwagę, że w wyniku działania polecenia *netplan status* nie wyświetlają się już komentarze o przydzieleniu danych przez *DHCP*.

W systemie Fedora do obsługi konfiguracji sieciowej wykorzystuje się polecenie *nmcli* (*NetworkManager CLI*).

```
[root@localhost ~]# nmcli
ens160: connected to ens160
    "VMware VMNET3"
      ethernet (vmxnet3), 00:0C:29:91:68:0C, hw, mtu 1500
      ip4 default
        inet4 192.168.239.130/24
        route4 192.168.239.0/24 metric 100
        route4 default via 192.168.239.2 metric 100
        inet6 fe80::20c:29ff:fe91:680c/64
        route6 fe80::/64 metric 1024

lo: connected (externally) to lo
    "lo"
      loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536
      inet4 127.0.0.1/8
      inet6 ::1/128

DNS configuration:
  servers: 192.168.239.2
  domains: localdomain
  interface: ens160

Use "nmcli device show" to get complete information about known devices and
"nmcli connection show" to get an overview on active connection profiles.

Consult nmcli(1) and nmcli-examples(?) manual pages for complete usage details.
[root@localhost ~]# nmcli connection show
NAME      UUID                TYPE      DEVICE
ens160   e7d3e3df-c93d-385a-ba23-696e3488fd80  ethernet  ens160
lo       0ff99b66-5dc8-4379-9e9e-ee5e6c347eab  loopback  lo
[root@localhost ~]#
```

Zrzut ekranu 18 Odczytanie danych adresowych i aktywnych połączeń w systemie Fedora.

W odróżnieniu od poprzednich dwóch systemów, modyfikacja połączenia, a więc również i statyczne przypisanie danych adresowych odbywa się z wiersza poleceń.

```
[root@localhost ~]# nmcli connection modify ens160 ipv4.method manual ipv4.addresses 192.168.239.130/24
ipv4.gateway 192.168.239.2 ipv4.dns 192.168.239.2
```

Zrzut ekranu 19 Statyczne przypisanie danych adresowych w systemie Fedora.

```
[root@localhost ~]# nmcli connection modify ens160 ipv4.method manual ipv4.addresses 192.168.239.130
[root@localhost ~]# nmcli
ens160: connected to ens160
    "VMware VMXNET3"
    ethernet (vmxnet3), 00:0C:29:91:68:0C, hw, mtu 1500
    ip4 default
    inet4 192.168.239.130/24
    route4 192.168.239.0/24 metric 100
    route4 default via 192.168.239.2 metric 100
    inet6 fe80::20c:29ff:fe91:680c/64
    route6 fe80::/64 metric 1024

lo: connected (externally) to lo
    "lo"
    loopback (unknown), 00:00:00:00:00:00, sw, mtu 65536
    inet4 127.0.0.1/8
    inet6 ::1/128

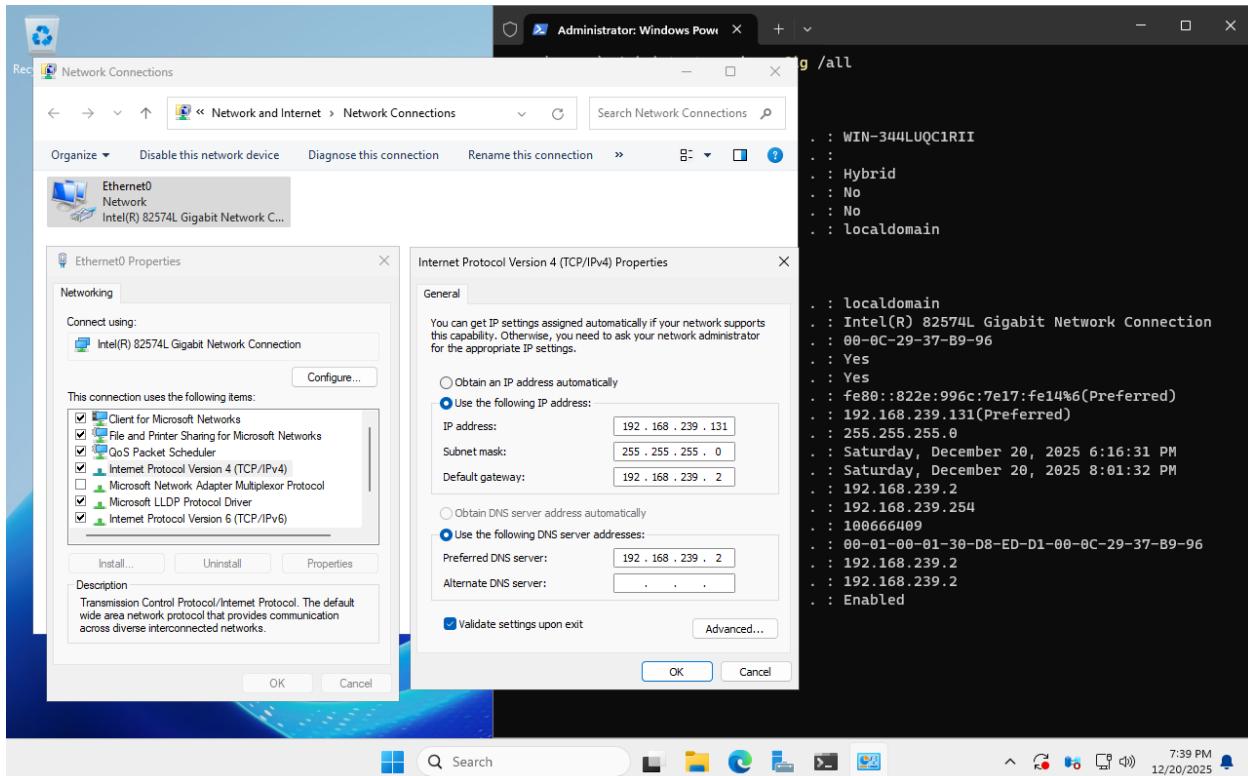
DNS configuration:
    servers: 192.168.239.2
    domains: localdomain
    interface: ens160

Use "nmcli device show" to get complete information about known devices and
"nmcli connection show" to get an overview on active connection profiles.

Consult nmcli(1) and nmcli-examples(?) manual pages for complete usage details.
[root@localhost ~]#
```

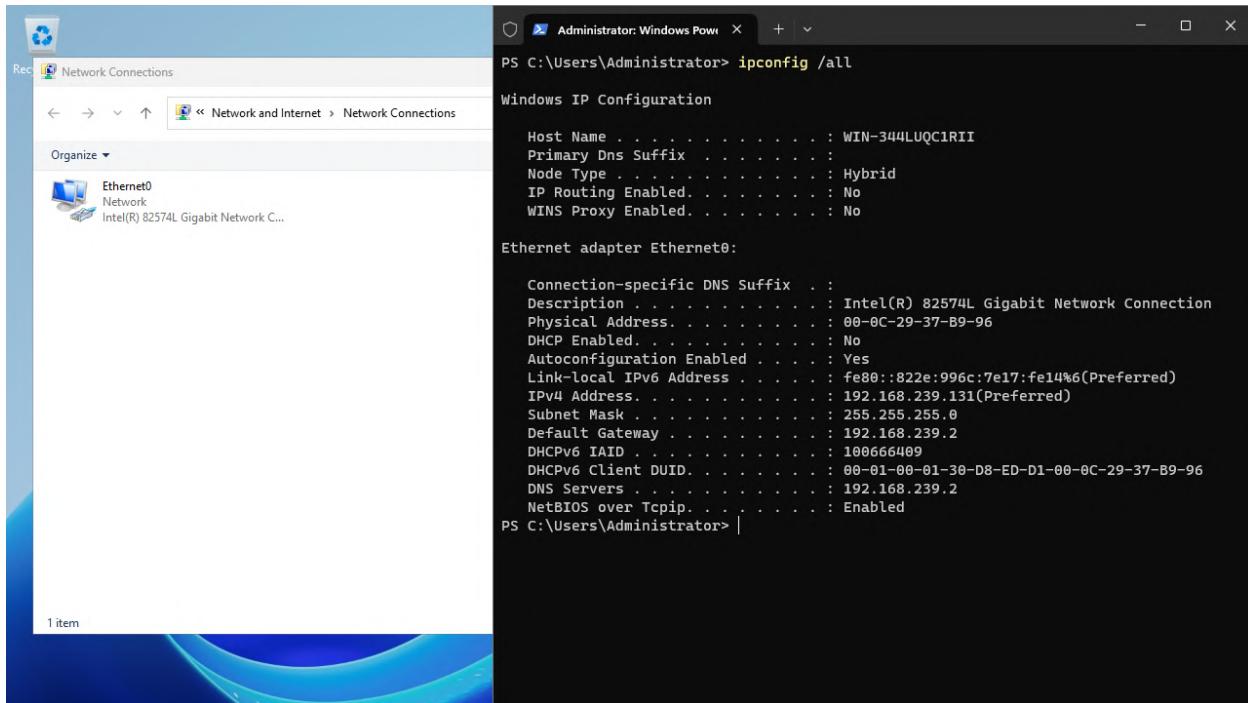
Zrzut ekranu 20 Odczytanie danych adresowych w systemie Fedora po wprowadzeniu zmian w konfiguracji sieciowej.

W systemach Windows aby sprawdzić nadane na adapterach sieciowych adresy można wykorzystać polecenie terminalowe *ipconfig /all*. Statyczny przydział danych adresowych wykonuje się natomiast z poziomu aplikacji *Network Connections*. Należy w niej wybrać właściwy adapter sieciowy, wejść w jego właściwości, właściwości elementu *Internet Protocol Version 4 (TCP/IPv4)* i ręcznie przydzielić dane.



Zrzut ekranu 21 Odczytanie i statyczne przypisanie danych adresowych w systemie Windows Server.

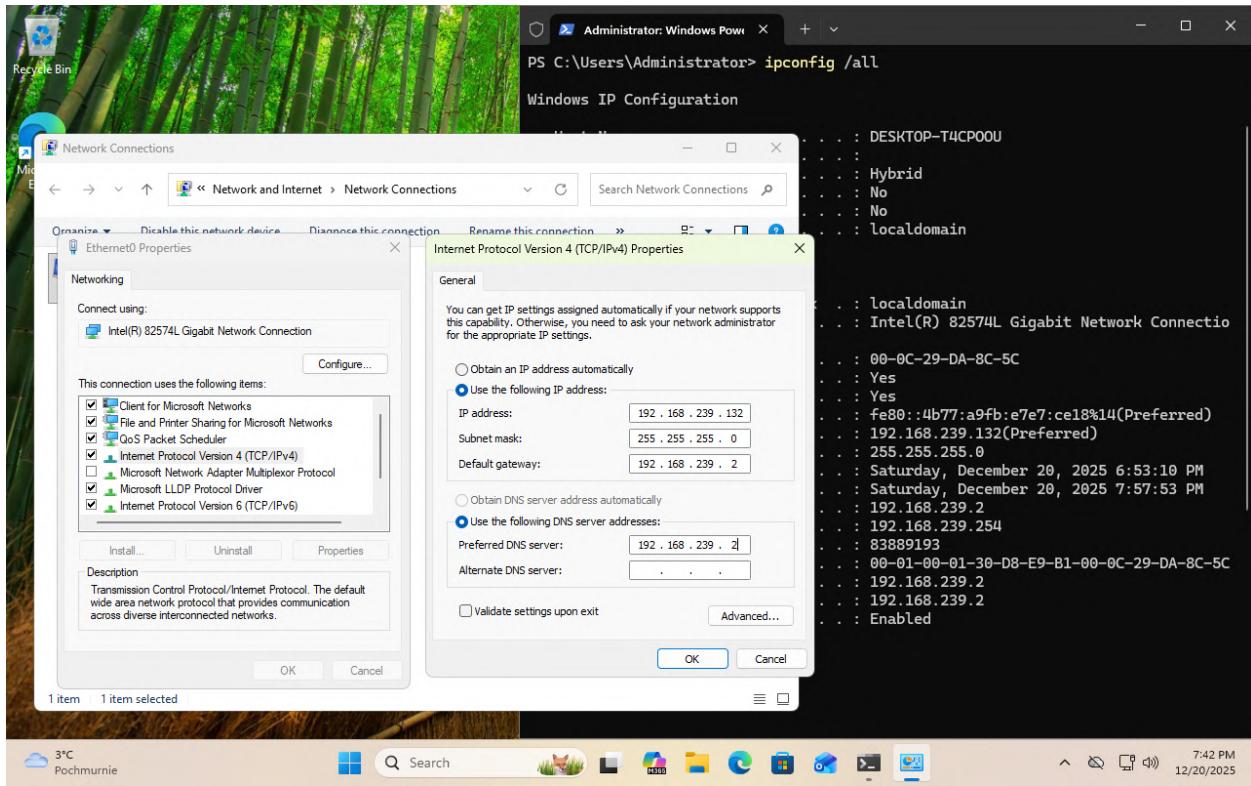
Po przepisaniu danych adresowych i zatwierdzeniu zmian możemy ponownie wykonać polecenie ipconfig /all.



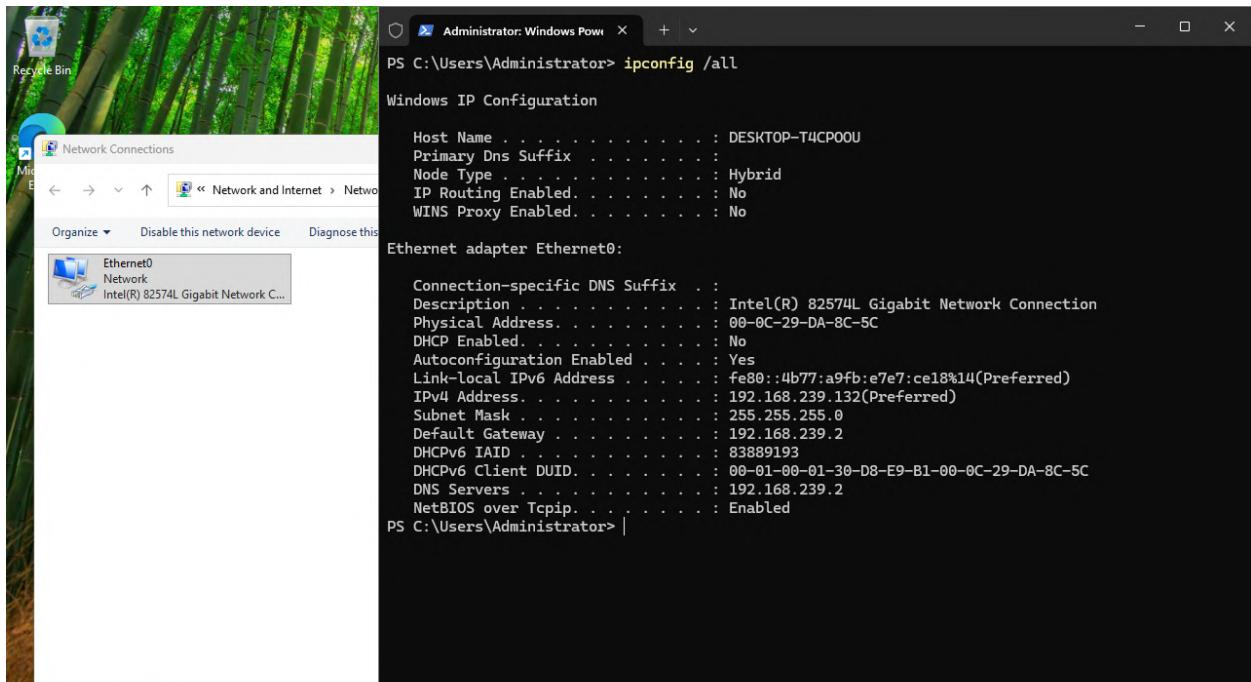
Zrzut ekranu 22 Odczytanie danych adresowych w systemie Windows Server po wprowadzeniu zmian w konfiguracji sieciowej.

Zgodnie z oczekiwaniami, dane adresowe nie zmieniły się. Dodatkowo przy wpisie „*DHCP Enabled*” pojawiło się „No”, co oznacza, że nie zostały uzyskane dynamicznie.

Proces powtarzamy analogicznie w systemie klienckim Windows 11.



Zrzut ekranu 23 Odczytanie i statyczne przypisanie danych adresowych w systemie Windows 11.



Zrzut ekranu 24 Odczytanie danych adresowych w systemie Windows 11 po wprowadzeniu zmian w konfiguracji sieciowej.

Po przypisaniu wszystkim maszynom wirtualnym *stacycznych adresów IP* możemy ponownie sprawdzić, czy możliwa jest między nimi komunikacja.

```
root@debian:~# ping google.com
PING google.com (142.251.98.102) 56(84) bytes of data.
64 bytes from nt-in-f102.ie100.net (142.251.98.102): icmp_seq=1 ttl=128 time=8.76 ms
64 bytes from nt-in-f102.ie100.net (142.251.98.102): icmp_seq=2 ttl=128 time=13.2 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 8.764/11.002/13.241/2.238 ms
root@debian:~# ping 192.168.239.1
PING 192.168.239.1 (192.168.239.1) 56(84) bytes of data.
64 bytes from 192.168.239.1: icmp_seq=1 ttl=128 time=0.325 ms
64 bytes from 192.168.239.1: icmp_seq=2 ttl=128 time=0.311 ms
^C
--- 192.168.239.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1017ms
rtt min/avg/max/mdev = 0.311/0.318/0.325/0.007 ms
root@debian:~# ping 192.168.239.129
PING 192.168.239.129 (192.168.239.129) 56(84) bytes of data.
64 bytes from 192.168.239.129: icmp_seq=1 ttl=64 time=0.862 ms
64 bytes from 192.168.239.129: icmp_seq=2 ttl=64 time=0.456 ms
^C
--- 192.168.239.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1013ms
rtt min/avg/max/mdev = 0.456/0.659/0.862/0.203 ms
root@debian:~# ping 192.168.239.130
PING 192.168.239.130 (192.168.239.130) 56(84) bytes of data.
64 bytes from 192.168.239.130: icmp_seq=1 ttl=64 time=0.464 ms
64 bytes from 192.168.239.130: icmp_seq=2 ttl=64 time=0.387 ms
^C
--- 192.168.239.130 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.387/0.425/0.464/0.038 ms
root@debian:~# ping 192.168.239.131
PING 192.168.239.131 (192.168.239.131) 56(84) bytes of data.
64 bytes from 192.168.239.131: icmp_seq=1 ttl=128 time=0.512 ms
64 bytes from 192.168.239.131: icmp_seq=2 ttl=128 time=0.473 ms
^C
--- 192.168.239.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.473/0.492/0.512/0.019 ms
root@debian:~# ping 192.168.239.132
PING 192.168.239.132 (192.168.239.132) 56(84) bytes of data.
64 bytes from 192.168.239.132: icmp_seq=1 ttl=128 time=0.917 ms
64 bytes from 192.168.239.132: icmp_seq=2 ttl=128 time=0.540 ms
^C
--- 192.168.239.132 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.540/0.728/0.917/0.188 ms
root@debian:~#
```

Zrzut ekranu 25 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Debian.

```
root@ubuntuserver:~# ping google.com
PING google.com (142.251.98.101) 56(84) bytes of data.
64 bytes from nt-in-f101.1e100.net (142.251.98.101): icmp_seq=1 ttl=128 time=13.7 ms
64 bytes from nt-in-f101.1e100.net (142.251.98.101): icmp_seq=2 ttl=128 time=13.3 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 13.312/13.510/13.709/0.198 ms
root@ubuntuserver:~# ping 192.168.239.1
PING 192.168.239.1 (192.168.239.1) 56(84) bytes of data.
64 bytes from 192.168.239.1: icmp_seq=1 ttl=128 time=0.426 ms
64 bytes from 192.168.239.1: icmp_seq=2 ttl=128 time=0.302 ms
^C
--- 192.168.239.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1053ms
rtt min/avg/max/mdev = 0.302/0.364/0.426/0.062 ms
root@ubuntuserver:~# ping 192.168.239.128
PING 192.168.239.128 (192.168.239.128) 56(84) bytes of data.
64 bytes from 192.168.239.128: icmp_seq=1 ttl=64 time=0.412 ms
64 bytes from 192.168.239.128: icmp_seq=2 ttl=64 time=0.381 ms
^C
--- 192.168.239.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 0.381/0.396/0.412/0.015 ms
root@ubuntuserver:~# ping 192.168.239.129
PING 192.168.239.129 (192.168.239.129) 56(84) bytes of data.
64 bytes from 192.168.239.129: icmp_seq=1 ttl=64 time=0.152 ms
64 bytes from 192.168.239.129: icmp_seq=2 ttl=64 time=0.037 ms
^C
--- 192.168.239.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.037/0.094/0.152/0.057 ms
root@ubuntuserver:~# ping 192.168.239.130
PING 192.168.239.130 (192.168.239.130) 56(84) bytes of data.
64 bytes from 192.168.239.130: icmp_seq=1 ttl=64 time=0.416 ms
64 bytes from 192.168.239.130: icmp_seq=2 ttl=64 time=0.467 ms
^C
--- 192.168.239.130 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1060ms
rtt min/avg/max/mdev = 0.416/0.441/0.467/0.025 ms
root@ubuntuserver:~# ping 192.168.239.131
PING 192.168.239.131 (192.168.239.131) 56(84) bytes of data.
64 bytes from 192.168.239.131: icmp_seq=1 ttl=128 time=0.475 ms
64 bytes from 192.168.239.131: icmp_seq=2 ttl=128 time=0.536 ms
^C
--- 192.168.239.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1017ms
rtt min/avg/max/mdev = 0.475/0.505/0.536/0.030 ms
root@ubuntuserver:~#
```

Zrzut ekranu 26 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Ubuntu.

```
[root@localhost ~]# ping google.com
PING google.com (142.251.98.102) 56(84) bytes of data.
64 bytes from nt-in-f102.1e100.net (142.251.98.102): icmp_seq=1 ttl=128 time=12.9 ms
64 bytes from nt-in-f102.1e100.net (142.251.98.102): icmp_seq=2 ttl=128 time=12.9 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 12.885/12.889/12.893/0.004 ms
[root@localhost ~]# ping 192.168.239.1
PING 192.168.239.1 (192.168.239.1) 56(84) bytes of data.
64 bytes from 192.168.239.1: icmp_seq=1 ttl=128 time=0.356 ms
64 bytes from 192.168.239.1: icmp_seq=2 ttl=128 time=0.316 ms
^C
--- 192.168.239.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 0.316/0.336/0.356/0.020 ms
[root@localhost ~]# ping 192.168.239.128
PING 192.168.239.128 (192.168.239.128) 56(84) bytes of data.
64 bytes from 192.168.239.128: icmp_seq=1 ttl=64 time=0.395 ms
64 bytes from 192.168.239.128: icmp_seq=2 ttl=64 time=0.345 ms
^C
--- 192.168.239.128 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1063ms
rtt min/avg/max/mdev = 0.345/0.370/0.395/0.025 ms
[root@localhost ~]# ping 192.168.239.129
PING 192.168.239.129 (192.168.239.129) 56(84) bytes of data.
64 bytes from 192.168.239.129: icmp_seq=1 ttl=64 time=0.950 ms
64 bytes from 192.168.239.129: icmp_seq=2 ttl=64 time=0.334 ms
^C
--- 192.168.239.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.334/0.642/0.950/0.308 ms
[root@localhost ~]# ping 192.168.239.131
PING 192.168.239.131 (192.168.239.131) 56(84) bytes of data.
64 bytes from 192.168.239.131: icmp_seq=1 ttl=128 time=0.468 ms
64 bytes from 192.168.239.131: icmp_seq=2 ttl=128 time=0.495 ms
^C
--- 192.168.239.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1042ms
rtt min/avg/max/mdev = 0.468/0.481/0.495/0.013 ms
^C[root@localhost ~]# ping 192.168.239.132
PING 192.168.239.132 (192.168.239.132) 56(84) bytes of data.
64 bytes from 192.168.239.132: icmp_seq=1 ttl=128 time=0.514 ms
64 bytes from 192.168.239.132: icmp_seq=2 ttl=128 time=0.475 ms
^C
--- 192.168.239.132 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1030ms
rtt min/avg/max/mdev = 0.475/0.494/0.514/0.019 ms
[root@localhost ~]#
```

Zrzut ekranu 27 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Fedora.

```

Administrator: Win+P PS C:\Users\Administrator> ping google.com
Pinging google.com [142.251.98.138] with 32 bytes of data:
Reply from 142.251.98.138: bytes=32 time=8ms TTL=128
Reply from 142.251.98.138: bytes=32 time=11ms TTL=128

Ping statistics for 142.251.98.138:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 11ms, Average = 9ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.1

Pinging 192.168.239.1 with 32 bytes of data:
Reply from 192.168.239.1: bytes=32 time<1ms TTL=128
Reply from 192.168.239.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.128

Pinging 192.168.239.128 with 32 bytes of data:
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.128:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator>

Administrator: Windows Pow+ PS C:\Users\Administrator> ping 192.168.239.129
Pinging 192.168.239.129 with 32 bytes of data:
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.129:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.130

Pinging 192.168.239.130 with 32 bytes of data:
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.132

Pinging 192.168.239.132 with 32 bytes of data:
Reply from 192.168.239.132: bytes=32 time<1ms TTL=128
Reply from 192.168.239.132: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.132:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator>

```

Zrzut ekranu 28 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Windows Server.

```

Administrator: Windows Pow+ PS C:\Users\Administrator> ping google.com
Pinging google.com [142.251.98.139] with 32 bytes of data:
Reply from 142.251.98.139: bytes=32 time=8ms TTL=128
Reply from 142.251.98.139: bytes=32 time=12ms TTL=128

Ping statistics for 142.251.98.139:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 12ms, Average = 10ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.1

Pinging 192.168.239.1 with 32 bytes of data:
Reply from 192.168.239.1: bytes=32 time<1ms TTL=128
Reply from 192.168.239.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.128

Pinging 192.168.239.128 with 32 bytes of data:
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.128:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator>

Administrator: Windows Pow+ PS C:\Users\Administrator> ping 192.168.239.129
Pinging 192.168.239.129 with 32 bytes of data:
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.129:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.130

Pinging 192.168.239.130 with 32 bytes of data:
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping 192.168.239.131

Pinging 192.168.239.131 with 32 bytes of data:
Reply from 192.168.239.131: bytes=32 time<1ms TTL=128
Reply from 192.168.239.131: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.239.131:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator>

```

Zrzut ekranu 29 Weryfikacja możliwości komunikacji sieciowej z poziomu maszyny wirtualnej z systemem Windows 11.

Aby ułatwić sobie komunikację między systemami serwerowymi, możemy dokonać w każdym z nich konfiguracji prostej zamiany *nazwy mnemonicznej na adres IP* z wykorzystaniem pliku */etc/hosts*. Poprawność wprowadzonej konfiguracji możemy ponownie sprawdzić poleceniem *ping*.

```
127.0.0.1      localhost
127.0.1.1      debian
192.168.239.129 ubuntuBieniek
192.168.239.130 fedoraBieniek
192.168.239.131 windowsBieniek

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
~
~
~
```

Zrzut ekranu 30 Konfiguracja prostych nazw DNS na serwerze z systemem Debian.

```
root@debian:~# ping ubuntuBieniek
PING ubuntuBieniek (192.168.239.129) 56(84) bytes of data.
64 bytes from ubuntuBieniek (192.168.239.129): icmp_seq=1 ttl=64 time=0.766 ms
64 bytes from ubuntuBieniek (192.168.239.129): icmp_seq=2 ttl=64 time=0.365 ms
^C
--- ubuntuBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.365/0.565/0.766/0.200 ms
root@debian:~# ping fedoraBieniek
PING fedoraBieniek (192.168.239.130) 56(84) bytes of data.
64 bytes from fedoraBieniek (192.168.239.130): icmp_seq=1 ttl=64 time=0.442 ms
64 bytes from fedoraBieniek (192.168.239.130): icmp_seq=2 ttl=64 time=0.304 ms
^C
--- fedoraBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1028ms
rtt min/avg/max/mdev = 0.304/0.373/0.442/0.069 ms
root@debian:~# ping windowsBieniek
PING windowsBieniek (192.168.239.131) 56(84) bytes of data.
64 bytes from windowsBieniek (192.168.239.131): icmp_seq=1 ttl=128 time=0.471 ms
64 bytes from windowsBieniek (192.168.239.131): icmp_seq=2 ttl=128 time=0.449 ms
^C
--- windowsBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.449/0.460/0.471/0.011 ms
root@debian:~#
```

Zrzut ekranu 31 Weryfikacja możliwości komunikacji z pozostałymi systemami serwerowymi z wykorzystaniem krótkich nazw mnemonicznych na serwerze z systemem Debian.

W analogiczny sposób skonfigurujemy i sprawdzimy poprawność komunikacji z wykorzystaniem krótkich nazw w pozostałych systemach Linux.

```
root@ubuntuserver:~# cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu_server
192.168.239.128 debianBieniek
192.168.239.130 fedoraBieniek
192.168.239.131 windowsBieniek

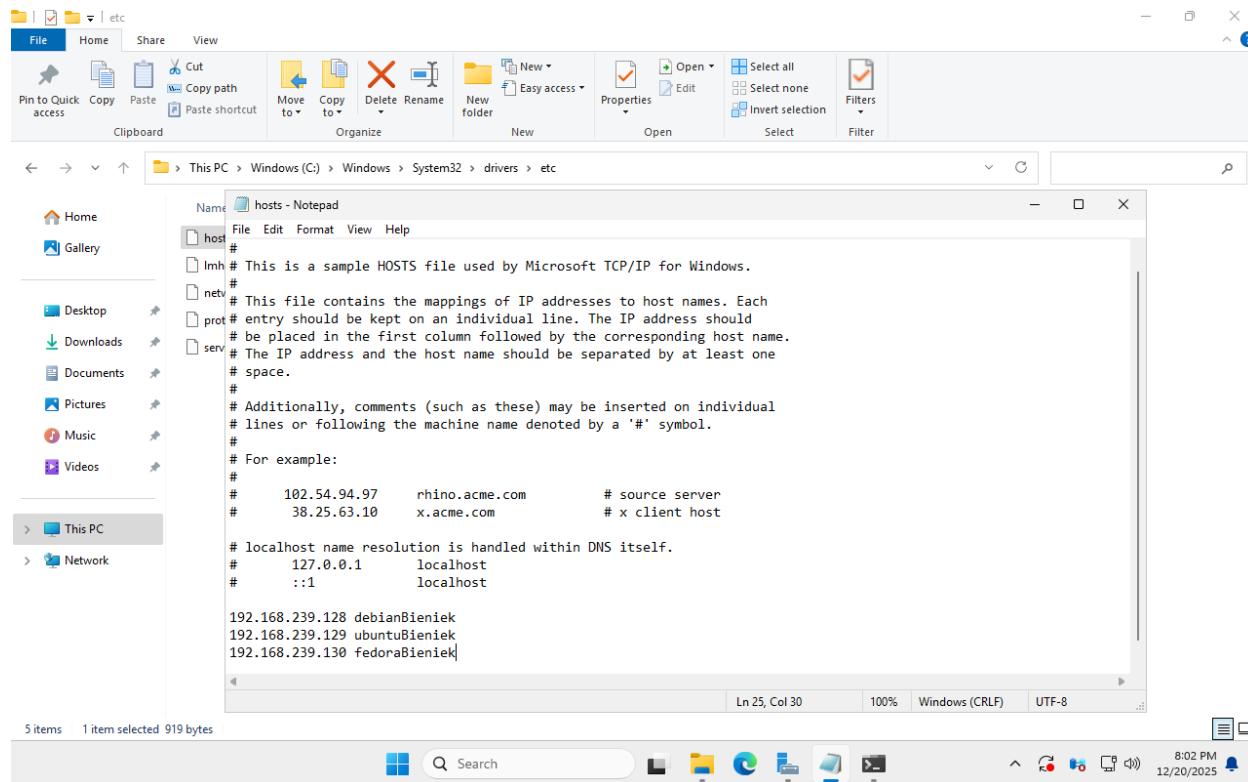
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
root@ubuntuserver:~# ping debianBieniek
PING debianBieniek (192.168.239.128) 56(84) bytes of data.
64 bytes from debianBieniek (192.168.239.128): icmp_seq=1 ttl=64 time=0.388 ms
64 bytes from debianBieniek (192.168.239.128): icmp_seq=2 ttl=64 time=0.380 ms
^C
--- debianBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1045ms
rtt min/avg/max/mdev = 0.380/0.384/0.388/0.004 ms
root@ubuntuserver:~# ping fedoraBieniek
PING fedoraBieniek (192.168.239.130) 56(84) bytes of data.
64 bytes from fedoraBieniek (192.168.239.130): icmp_seq=1 ttl=64 time=0.361 ms
64 bytes from fedoraBieniek (192.168.239.130): icmp_seq=2 ttl=64 time=0.375 ms
^C
--- fedoraBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1023ms
rtt min/avg/max/mdev = 0.361/0.368/0.375/0.007 ms
root@ubuntuserver:~# ping windowsBieniek
PING windowsBieniek (192.168.239.131) 56(84) bytes of data.
64 bytes from windowsBieniek (192.168.239.131): icmp_seq=1 ttl=128 time=0.454 ms
64 bytes from windowsBieniek (192.168.239.131): icmp_seq=2 ttl=128 time=0.394 ms
^C
--- windowsBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1012ms
rtt min/avg/max/mdev = 0.394/0.424/0.454/0.030 ms
root@ubuntuserver:~# _
```

Zrzut ekranu 32 Konfiguracja krótkich nazw DNS i weryfikacja poprawności komunikacji z ich wykorzystaniem na serwerze z systemem Ubuntu.

```
[root@localhost ~]# cat /etc/hosts
# Loopback entries; do not change.
# For historical reasons, localhost precedes localhost.localdomain:
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1          localhost localhost.localdomain localhost6 localhost6.localdomain6
# See hosts(5) for proper format and other examples:
# 192.168.1.10 foo.mydomain.org foo
# 192.168.1.13 bar.mydomain.org bar
192.168.239.128 debianBieniek
192.168.239.129 ubuntuBieniek
192.168.239.131 windowsBieniek
[root@localhost ~]# ping debianBieniek
PING debianBieniek (192.168.239.128) 56(84) bytes of data.
64 bytes from debianBieniek (192.168.239.128): icmp_seq=1 ttl=64 time=0.489 ms
64 bytes from debianBieniek (192.168.239.128): icmp_seq=2 ttl=64 time=0.365 ms
^C
--- debianBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1044ms
rtt min/avg/max/mdev = 0.365/0.427/0.489/0.062 ms
[root@localhost ~]# ping ubuntuBieniek
PING ubuntuBieniek (192.168.239.129) 56(84) bytes of data.
64 bytes from ubuntuBieniek (192.168.239.129): icmp_seq=1 ttl=64 time=0.414 ms
64 bytes from ubuntuBieniek (192.168.239.129): icmp_seq=2 ttl=64 time=0.335 ms
^C
--- ubuntuBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1064ms
rtt min/avg/max/mdev = 0.335/0.374/0.414/0.039 ms
[root@localhost ~]# ping windowsBieniek
PING windowsBieniek (192.168.239.131) 56(84) bytes of data.
64 bytes from windowsBieniek (192.168.239.131): icmp_seq=1 ttl=128 time=0.459 ms
64 bytes from windowsBieniek (192.168.239.131): icmp_seq=2 ttl=128 time=0.474 ms
^C
--- windowsBieniek ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1055ms
rtt min/avg/max/mdev = 0.459/0.466/0.474/0.007 ms
[root@localhost ~]# _
```

Zrzut ekranu 33 Konfiguracja krótkich nazw DNS i weryfikacja poprawności komunikacji z ich wykorzystaniem na serwerze z systemem Fedora.

Plik hosts znajdziemy również na komputerze z systemem Windows Server w folderze C:\Windows\System32\drivers\etc\.



Zrzut ekranu 34 Konfiguracja prostych nazw DNS na maszynie z systemem Windows Server.

```
Administrator: Windows PowerShell + 
PS C:\Users\Administrator> ping debianBieniek

Pinging debianBieniek [192.168.239.128] with 32 bytes of data:
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64
Reply from 192.168.239.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.128:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping ubuntuBieniek

Pinging ubuntuBieniek [192.168.239.129] with 32 bytes of data:
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64
Reply from 192.168.239.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.129:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator> ping fedoraBieniek

Pinging fedoraBieniek [192.168.239.130] with 32 bytes of data:
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64
Reply from 192.168.239.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.239.130:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
PS C:\Users\Administrator>
```

Zrzut ekranu 35 Weryfikacja możliwości komunikacji z pozostałymi systemami serwerowymi z wykorzystaniem krótkich nazw DNS na komputerze z systemem Windows Server.

Zadanie 1.2. Konfiguracja połączeń SSH.

Przed przystąpieniem do zadania utwórzmy na każdym serwerze użytkownika testowego. W systemach Linux wykorzystuje się do tego polecenie *adduser*, a na Windows – aplikację *Computer Management*.

```
root@debian:~# adduser --allow-bad-names BartoszBieniek
Allowing use of questionable username.
Adding user 'BartoszBieniek' ...
Adding new group `BartoszBieniek' (1000) ...
Adding new user `BartoszBieniek' (1000) with group `BartoszBieniek (1000)' ...
Creating home directory '/home/BartoszBieniek' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for BartoszBieniek
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
Adding new user `BartoszBieniek' to supplemental / extra groups `users' ...
Adding user `BartoszBieniek' to group `users' ...
root@debian:~# tail -n 1 /etc/passwd
BartoszBieniek:x:1000:1000:,,,:/home/BartoszBieniek:/bin/bash
root@debian:~#
```

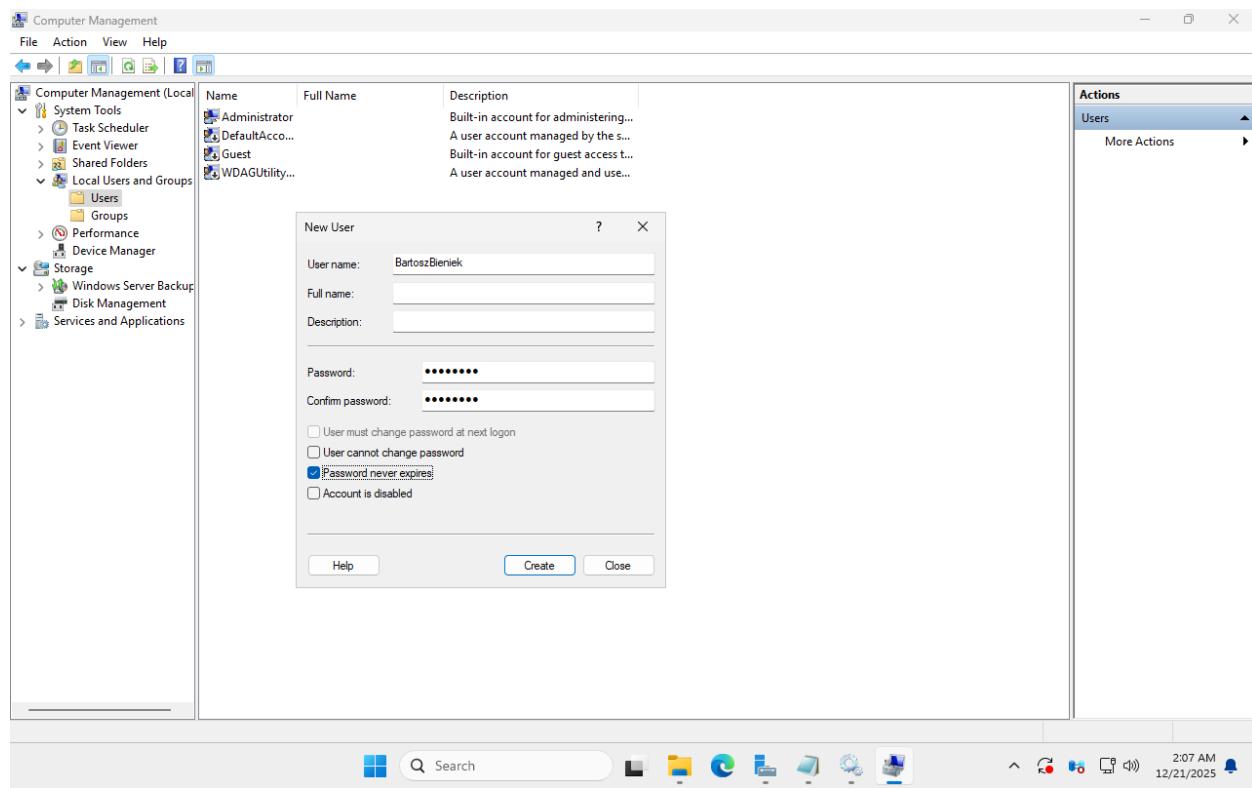
Zrzut ekranu 36 Utworzenie testowego użytkownika w systemie Debian.

```
[root@localhost ~]# adduser BartoszBieniek
[root@localhost ~]# passwd BartoszBieniek
Changing password for user BartoszBieniek.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

Zrzut ekranu 37 Utworzenie testowego użytkownika w systemie Fedora.

```
root@ubuntuserver:~# adduser --allow-bad-names BartoszBieniek
info: Allowing use of questionable username.
info: Adding user 'BartoszBieniek' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `BartoszBieniek' (1000) ...
info: Adding new user `BartoszBieniek' (1000) with group `BartoszBieniek (1000)' ...
info: Creating home directory '/home/BartoszBieniek' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for BartoszBieniek
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []
Is the information correct? [Y/n]
info: Adding new user `BartoszBieniek' to supplemental / extra groups `users' ...
info: Adding user `BartoszBieniek' to group `users' ...
root@ubuntuserver:~# tail -n 1 /etc/passwd
BartoszBieniek:x:1000:1000:,,,:/home/BartoszBieniek:/bin/bash
root@ubuntuserver:~#
```

Zrzut ekranu 38 Utworzenie testowego użytkownika w systemie Ubuntu.



Zrzut ekranu 39 Utworzenie testowego użytkownika w systemie Windows Server.

Ponieważ do uwierzytelniania będziemy chcieli wykorzystać klucz asymetryczny systemu klienckiego *Windows 11*, musimy go najpierw wygenerować. W tym celu skorzystamy z polecenia *ssh-keygen* wypełniając zgodnie z instrukcją kolejne pola. Domyślnie użyty zostanie nowszy algorytm *ED25519*, uznawany za równie bezpieczny co *RSA* przy znacznie krótszych kluczach.

The screenshot shows a Windows PowerShell window titled "Administrator: Windows Pow" with the following command and output:

```
PS C:\Users\Administrator> ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:/Users/Administrator/.ssh/id_ed25519):
Created directory 'C:/Users/Administrator/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:/Users/Administrator/.ssh/id_ed25519
Your public key has been saved in C:/Users/Administrator/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:xpB0WLkActhQlnAspHQ3hAAUgYlqnMVeBgls0grDYXk administrator@DESKTOP-T4CP00U
The key's randomart image is:
+--[ED25519 256]--+
|@&*+..|
|0=Eo*o.|
|*.0 +.|
|+B . o.o|
|+. . . S|
|.|.
+---[SHA256]---+
PS C:\Users\Administrator> ls ~/.ssh

Directory: C:/Users/Administrator/.ssh

Mode                LastWriteTime         Length Name
----                -----          ---- -
-a---       12/20/2025 11:57 PM           464 id_ed25519
-a---       12/20/2025 11:57 PM          112 id_ed25519.pub

PS C:\Users\Administrator>
```

The taskbar at the bottom shows icons for Cloud, Weather (3°C), Search, File Explorer, Task View, and others, along with the date and time (11:58 PM, 12/20/2025).

Zrzut ekranu 40 Generowanie klucza asymetrycznego na maszynie z systemem klienckim *Windows 11*.

Na dysku w folderze `~/.ssh` zostaną utworzone dwa pliki – klucz prywatny i klucz publiczny (z końcówką `.pub`). Aby móc skorzystać z mechanizmu uwierzytelniania kluczem asymetrycznym do logowania się po *SSH*, konieczne będzie skopiowanie tego ostatniego na każdy z serwerów.

Możemy teraz przejść do instalacji i konfiguracji serwera *SSH* w każdym systemie serwerowym.

Aby zainstalować wymagane oprogramowanie, w systemie *Debian* wykonamy polecenie *apt update && apt install openssh-server -y*, które zaktualizuje najpierw lokalną bazę pakietów, a dopiero potem przejdzie do instalacji *openssh-server*.

```
root@debian:~# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Sat 2025-12-20 20:07:55 CET; 47s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 1866 (sshd)
    Tasks: 1 (limit: 4610)
   Memory: 1.4M
      CPU: 16ms
     CGroup: /system.slice/ssh.service
             └─1866 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 20 20:07:55 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 20 20:07:55 debian sshd[1866]: Server listening on 0.0.0.0 port 22.
Dec 20 20:07:55 debian sshd[1866]: Server listening on :: port 22.
Dec 20 20:07:55 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@debian:~# _
```

Zrzut ekranu 41 Uruchomiona usługa sshd.

Usługa *sshd* (serwer SSH) wystartuje natychmiast po instalacji oprogramowania. Aby ustawić niestandardowy port **1022** wystarczy zmienić w pliku konfiguracyjnym */etc/ssh/sshd_config* odpowiednią linię.

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 1022 ←
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
```

Zrzut ekranu 42 Konfiguracja niestandardowego portu serwera SSH w pliku */etc/ssh/sshd_config* na maszynie z systemem *Debian*.

Do wprowadzenia zmian konieczne jest zrestartowanie usługi *sshd* poleceniem *systemctl restart sshd*.

```
root@debian:~# systemctl restart sshd
root@debian:~# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-12-21 14:21:10 CET; 6s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 1475 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 1477 (sshd)
   Tasks: 1 (limit: 4610)
  Memory: 1.4M
    CPU: 15ms
   CGroup: /system.slice/ssh.service
           └─1477 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 21 14:21:10 debian systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 21 14:21:10 debian sshd[1477]: Server listening on 0.0.0.0 port 1022.
Dec 21 14:21:10 debian sshd[1477]: Server listening on :: port 1022.
Dec 21 14:21:10 debian systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
root@debian:~# _
```

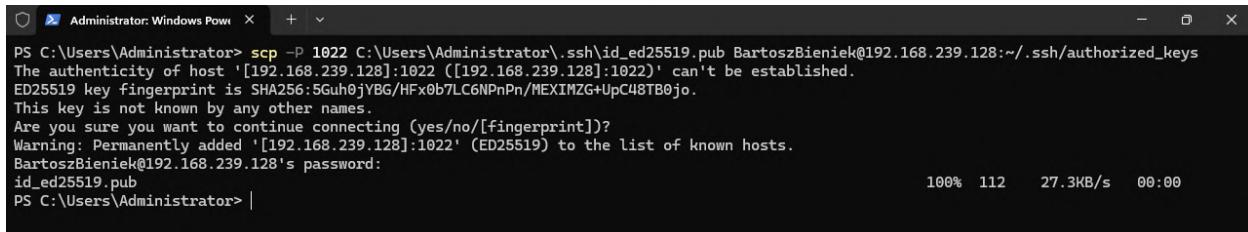
Zrzut ekranu 43 Restart usługi sshd. Serwer nastuchujący na niestandardowym porcie 1022.

Następnie przekopiujemy na konto użytkownika docelowego (*BartoszBieniek*) klucz *publiczny* z systemu klienckiego, wykorzystując do tego polecenie *scp*, które wykorzystuje pod spodem SSH. Przed tym konieczne jest jednak utworzenie katalogu docelowego – */home/BartoszBieniek/.ssh*.

```
BartoszBieniek@debian:~$ ls -la
total 24
drwx----- 2 BartoszBieniek BartoszBieniek 4096 Dec 21 00:07 .
drwxr-xr-x 3 root          root        4096 Dec 20 20:05 ..
-rw------- 1 BartoszBieniek BartoszBieniek  549 Dec 20 23:43 .bash_history
-rw-r--r-- 1 BartoszBieniek BartoszBieniek  220 Dec 20 20:05 .bash_logout
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 3526 Dec 20 20:05 .bashrc
-rw-r--r-- 1 BartoszBieniek BartoszBieniek  807 Dec 20 20:05 .profile
BartoszBieniek@debian:~$ mkdir ~/.ssh/
BartoszBieniek@debian:~$ chmod 700 ~/.ssh/
BartoszBieniek@debian:~$ ls -la
total 28
drwx----- 3 BartoszBieniek BartoszBieniek 4096 Dec 21 00:07 .
drwxr-xr-x 3 root          root        4096 Dec 20 20:05 ..
-rw------- 1 BartoszBieniek BartoszBieniek  549 Dec 20 23:43 .bash_history
-rw-r--r-- 1 BartoszBieniek BartoszBieniek  220 Dec 20 20:05 .bash_logout
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 3526 Dec 20 20:05 .bashrc
-rw-r--r-- 1 BartoszBieniek BartoszBieniek  807 Dec 20 20:05 .profile
drwx----- 2 BartoszBieniek BartoszBieniek 4096 Dec 21 00:08 .ssh
BartoszBieniek@debian:~$
```

Zrzut ekranu 44 Utworzenie katalogu *~/.ssh* z odpowiednimi uprawnieniami.

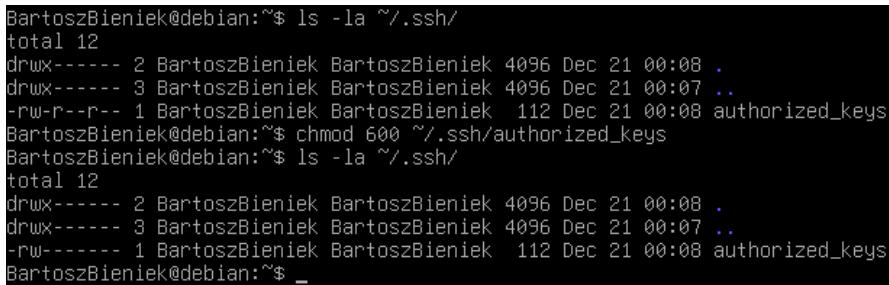
Ponieważ łączymy się po raz pierwszy z *maszyny klienckiej Windows 11* do serwera *Debian*, jesteśmy proszeni o potwierdzenie chęci połączenia się z nim. Zwróćmy uwagę, że przed przesłaniem pliku konieczne będzie podanie hasła.



```
Administrator: Windows Pow X + 
PS C:\Users\Administrator> scp -P 1022 C:\Users\Administrator\.ssh\id_ed25519.pub BartoszBieniek@192.168.239.128:~/ssh/authorized_keys
The authenticity of host '[192.168.239.128]:1022 ([192.168.239.128]:1022)' can't be established.
ED25519 key fingerprint is SHA256:5Guuh0jYBG/HFx0b7LC6NPnPn/MEXIMZG+UpC48TB0jo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added '[192.168.239.128]:1022' (ED25519) to the list of known hosts.
BartoszBieniek@192.168.239.128's password: id_ed25519.pub
PS C:\Users\Administrator> | 100% 112 27.3KB/s 00:00
```

Zrzut ekranu 45 Przeniesienie klucza publicznego z komputera z klienckim systemem Windows 11.

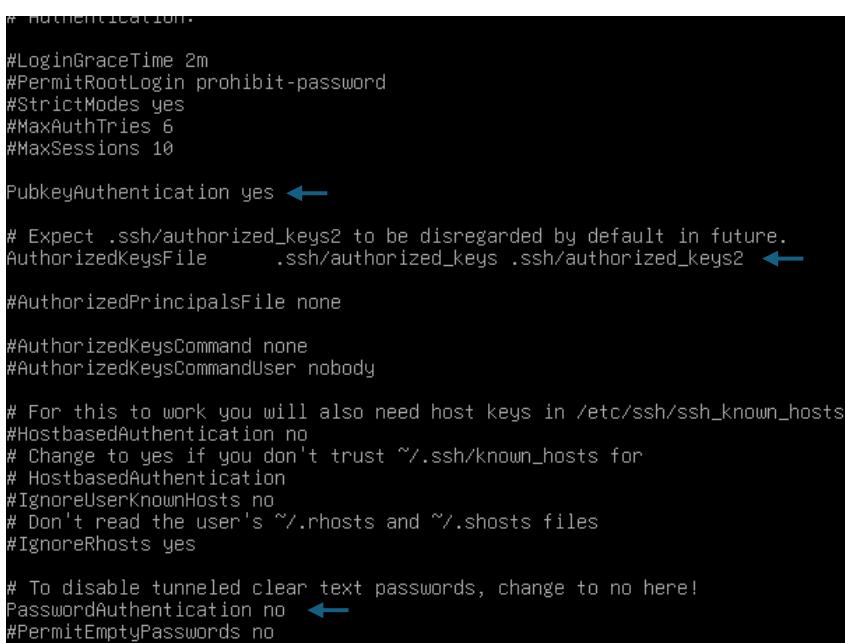
Możemy także nadać odpowiednie uprawnienia dostępu do pliku, tak, aby dostęp do tego klucza miał tylko użytkownik *BartoszBieniek*.



```
BartoszBieniek@debian:~$ ls -la ~/.ssh/
total 12
drwx----- 2 BartoszBieniek BartoszBieniek 4096 Dec 21 00:08 .
drwx----- 3 BartoszBieniek BartoszBieniek 4096 Dec 21 00:07 ..
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 112 Dec 21 00:08 authorized_keys
BartoszBieniek@debian:~$ chmod 600 ~/.ssh/authorized_keys
BartoszBieniek@debian:~$ ls -la ~/.ssh/
total 12
drwx----- 2 BartoszBieniek BartoszBieniek 4096 Dec 21 00:08 .
drwx----- 3 BartoszBieniek BartoszBieniek 4096 Dec 21 00:07 ..
-rw----- 1 BartoszBieniek BartoszBieniek 112 Dec 21 00:08 authorized_keys
BartoszBieniek@debian:~$ _
```

Zrzut ekranu 46 Zmiana uprawnień dostępu do skopiowanego z komputera klienckiego klucza publicznego.

Możemy teraz wrócić do pliku konfiguracyjnego, aktywować uwierzytelnianie kluczem asymetrycznym i wyłączyć logowanie hasłem.



```
# Authentication:
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes ←

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2 ←

#AuthorizedPrincipalsFile none

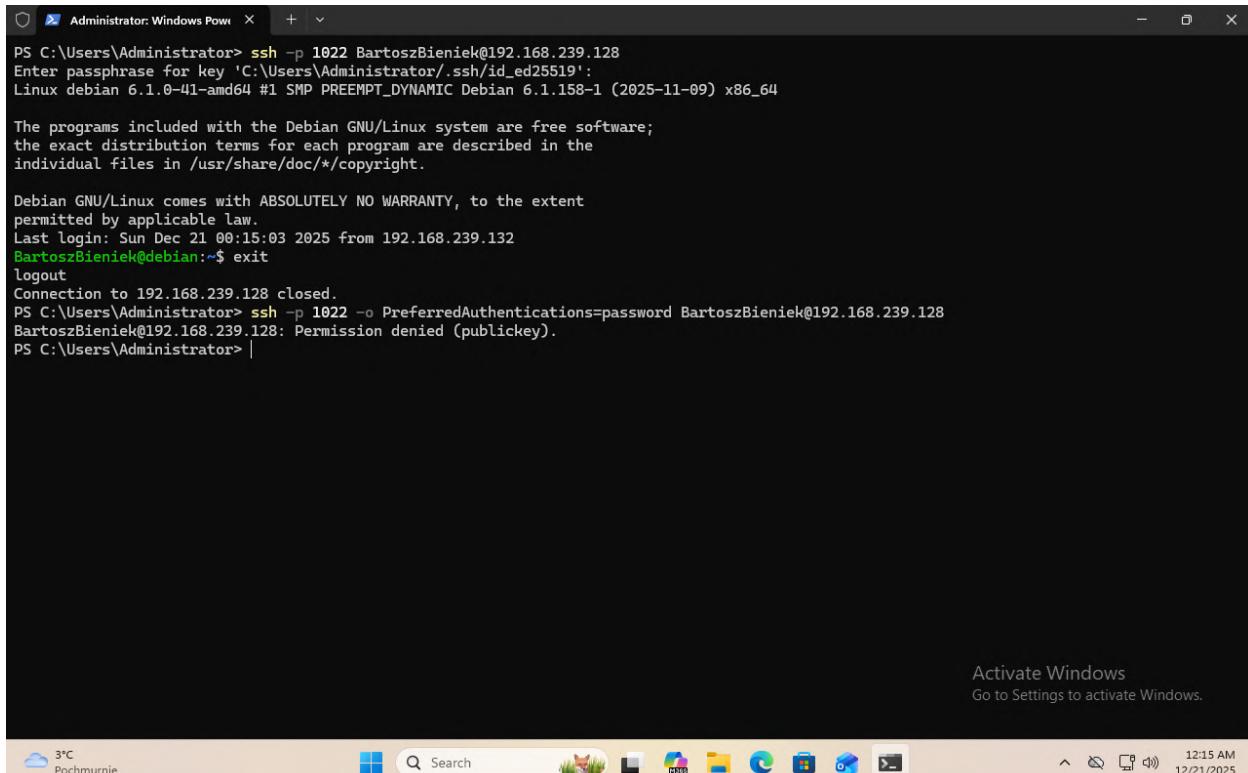
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no ←
#PermitEmptyPasswords no
```

Zrzut ekranu 47 Włączenie mechanizmu uwierzytelniania kluczem asymetrycznym i wyłączenie logowania hasłem dla serwera ssh w systemie Debian.

Po wprowadzeniu zmian spróbujmy zalogować się ponownie z komputera klienckiego.



```
Administrator: Windows Pow PS C:\Users\Administrator> ssh -p 1022 BartoszBieniek@192.168.239.128 Enter passphrase for key 'C:\Users\Administrator/.ssh/id_ed25519': Linux debian 6.1.0-41-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.158-1 (2025-11-09) x86_64 The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright. Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Sun Dec 21 00:15:03 2025 from 192.168.239.132 BartoszBieniek@debian:~$ exit logout Connection to 192.168.239.128 closed. PS C:\Users\Administrator> ssh -p 1022 -o PreferredAuthentications=password BartoszBieniek@192.168.239.128 BartoszBieniek@192.168.239.128: Permission denied (publickey). PS C:\Users\Administrator>
```

Zrzut ekranu 48 Poprawne logowanie z wykorzystaniem klucza asymetrycznego z systemu klienckiego. Nieudana próba zalogowania z wykorzystaniem hasła.

Jak widać, logując się przez SSH nie jesteśmy teraz proszeni o hasło użytkownika, ale o hasło do utworzonego wcześniej klucza asymetrycznego. Po jego podaniu następuje poprawne zalogowanie. Próba zalogowania się z uwierzytelnianiem na podstawie hasła (podanie opcji *-o PreferredAuthentications=password*) została przez serwer odrzucona.

Powyższe czynności analogicznie powtarzamy dla pozostałych systemów Linux.

W przypadku maszyny z systemem Ubuntu proces ten będzie wyglądał następująco.

```
root@ubuntuserver:~# apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libwrap0 ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  libwrap0 ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 5 newly installed, 0 to remove and 59 not upgraded.
Need to get 1,786 kB of archives.
After this operation, 6,853 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://pl.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-client amd64 1:9.6p1-3ubuntu13.14 [906 kB]
Get:2 http://pl.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-3ubuntu13.14 [37.3 kB]
Get:3 http://pl.archive.ubuntu.com/ubuntu noble/main amd64 libwrap0 amd64 7.6.q-33 [47.9 kB]
Get:4 http://pl.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubuntu13.14 [510 kB]
Get:5 http://pl.archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [275 kB]
Get:6 http://pl.archive.ubuntu.com/ubuntu noble-updates/main amd64 ssh-import-id all 5.11-0ubuntu2.24.04.1 [10.1 kB]
Fetched 1,786 kB in 1s (3,103 kB/s)
Preconfiguring packages ...
(Reading database ... 85%
```

Zrzut ekranu 49 Instalacja serwera open-ssh na serwerze z systemem Ubuntu.

```
# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
Port 1022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#PkeyAlg none
```

Zrzut ekranu 50 Konfiguracja niestandardowego portu serwera SSH w pliku /etc/ssh/sshd_config na maszynie z systemem Ubuntu.

Restartujemy serwer SSH poleceniem `systemctl restart sshd`.

```

root@ubuntuserver:~# su -l BartoszBieniek
BartoszBieniek@ubuntuserver:~$ ls -la ~
total 24
drwxr-x--- 2 BartoszBieniek BartoszBieniek 4096 Dec 20 23:54 .
drwxr-xr-x 3 root         root        4096 Dec 20 23:53 ..
-rw----- 1 BartoszBieniek BartoszBieniek 10 Dec 20 23:54 .bash_history
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 220 Dec 20 23:53 .bash_logout
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 8771 Dec 20 23:53 .bashrc
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 807 Dec 20 23:53 .profile
BartoszBieniek@ubuntuserver:~$ mkdir ~/.ssh/
BartoszBieniek@ubuntuserver:~$ ls -la ~
total 32
drwxr-x--- 4 BartoszBieniek BartoszBieniek 4096 Dec 21 00:31 .
drwxr-xr-x 3 root         root        4096 Dec 20 23:53 ..
-rw----- 1 BartoszBieniek BartoszBieniek 10 Dec 20 23:54 .bash_history
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 220 Dec 20 23:53 .bash_logout
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 8771 Dec 20 23:53 .bashrc
drwx----- 2 BartoszBieniek BartoszBieniek 4096 Dec 21 00:31 .cache
-rw-r--r-- 1 BartoszBieniek BartoszBieniek 807 Dec 20 23:53 .profile
drwxrwxr-x 2 BartoszBieniek BartoszBieniek 4096 Dec 21 00:31 .ssh

```

Zrzut ekranu 51 Utworzenie katalogu `~/.ssh`.

```

PS C:\Users\Administrator> scp -P 1022 C:\Users\Administrator\.ssh\id_ed25519.pub BartoszBieniek@192.168.239.129:~/ssh/authorized_keys
The authenticity of host '[192.168.239.129]:1022 ([192.168.239.129]:1022)' can't be established.
ED25519 key fingerprint is SHA256:J7jKIDJm94MzUOP8S4K5v6SFnu4wX1OrYPLX/H5+LYs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added '[192.168.239.129]:1022' (ED25519) to the list of known hosts.
BartoszBieniek@192.168.239.129's password:
id_ed25519.pub                                         100%   112    27.3KB/s  00:00
PS C:\Users\Administrator>

```

Zrzut ekranu 52 Przeniesienie klucza publicznego z komputera z klienckim systemem Windows 11.

```

BartoszBieniek@ubuntuserver:~$ ls -la ~/ssh/
total 12
drwxrwxr-x 2 BartoszBieniek BartoszBieniek 4096 Dec 21 00:31 .
drwxr-x--- 4 BartoszBieniek BartoszBieniek 4096 Dec 21 00:31 ..
-rw-rw-r-- 1 BartoszBieniek BartoszBieniek 112 Dec 21 00:31 authorized_keys
BartoszBieniek@ubuntuserver:~$ chmod 700 ~/ssh/
BartoszBieniek@ubuntuserver:~$ chmod 600 ~/ssh/authorized_keys
BartoszBieniek@ubuntuserver:~$ 

```

Zrzut ekranu 53 Zmiana uprawnień dostępu do folderu `~/ssh` oraz skopiowanego z komputera klienckiego klucza publicznego.

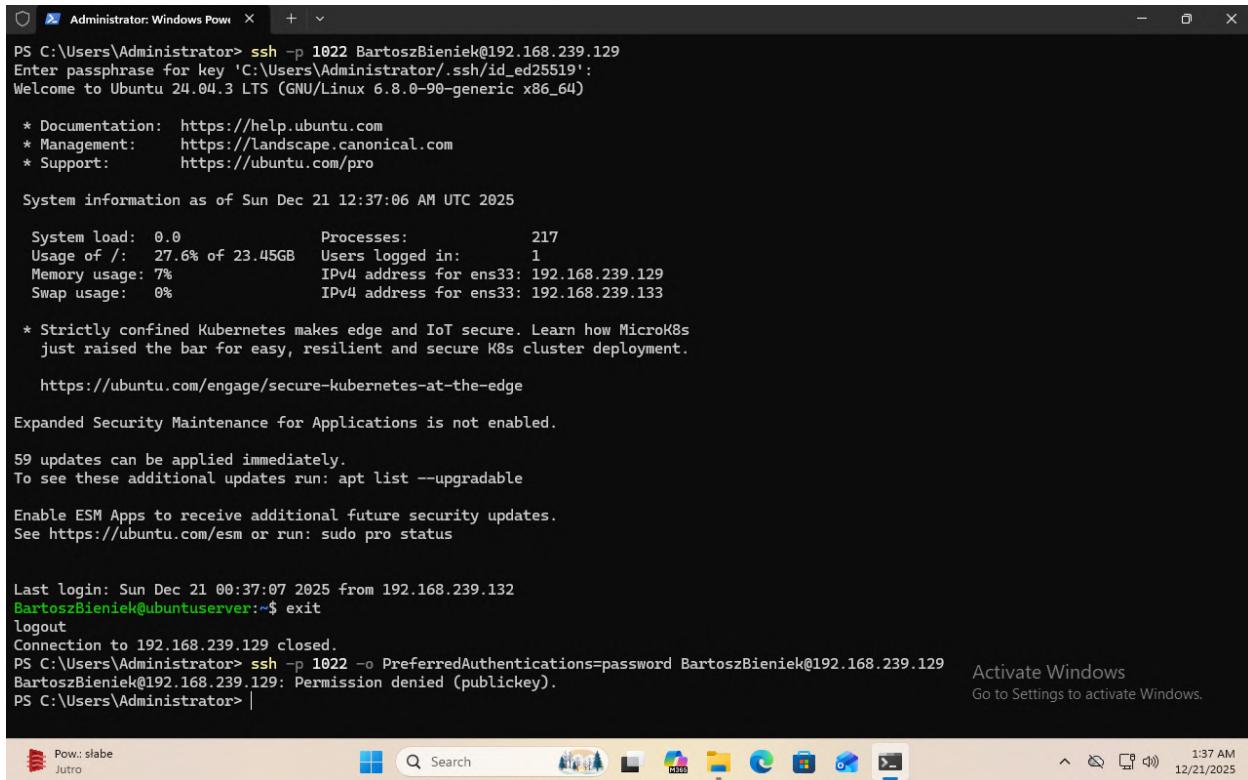
```

#MaxSessions 10
PubkeyAuthentication yes
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
# change to yes to enable challenge-response passwords (beware issues with

```

Zrzut ekranu 54 Włączenie mechanizmu uwierzytelniania kluczem asymetrycznym i wyłączenie logowania hasłem dla serwera ssh w systemie Ubuntu.

Restartujemy następnie usługę `sshd` i weryfikujemy możliwość zalogowania się na serwer z systemu klienckiego Windows 11 z wykorzystaniem klucza asymetrycznego.



```
Administrator: Windows Pow C:\Users\Administrator> ssh -p 1022 BartoszBieniek@192.168.239.129
Enter passphrase for key 'C:\Users\Administrator/.ssh/id_ed25519':
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Sun Dec 21 12:37:06 AM UTC 2025

System load: 0.0 Processes: 217
Usage of /: 27.6% of 23.45GB Users logged in: 1
Memory usage: 7% IPv4 address for ens33: 192.168.239.129
Swap usage: 0% IPv4 address for ens33: 192.168.239.133

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

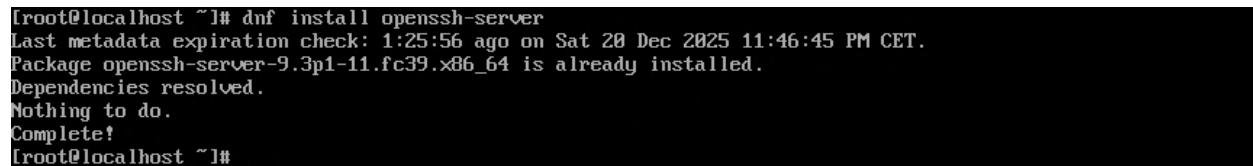
59 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun Dec 21 00:37:07 2025 from 192.168.239.132
BartoszBieniek@ubuntuserver:~$ exit
logout
Connection to 192.168.239.129 closed.
PS C:\Users\Administrator> ssh -p 1022 -o PreferredAuthentications=password BartoszBieniek@192.168.239.129
BartoszBieniek@192.168.239.129: Permission denied (publickey).
PS C:\Users\Administrator> |
```

Zrzut ekranu 55 Poprawne logowanie z wykorzystaniem klucza asymetrycznego z systemu klienckiego. Nieudana próba zalogowania z wykorzystaniem hasła.

Dla maszyny wirtualnej z systemem Fedora postąpimy w podobny sposób, jednak ze względu na włączony podsystem bezpieczeństwa konieczne będzie otwarcie niestandardowego portu dla serwera SSH w SELinux i zaporze ognioowej.



```
[root@localhost ~]# dnf install openssh-server
Last metadata expiration check: 1:25:56 ago on Sat 20 Dec 2025 11:46:45 PM CET.
Package openssh-server-9.3p1-11.fc39.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@localhost ~]# _
```

Zrzut ekranu 56 Serwer SSH jest domyślnie zainstalowany w systemie Fedora.

```
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 1022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
```

Zrzut ekranu 57 Konfiguracja niestandardowego portu serwera SSH w pliku `/etc/ssh/sshd_config` na maszynie z systemem Fedora. Informacja o konieczności otwarcia portu w SELinux.

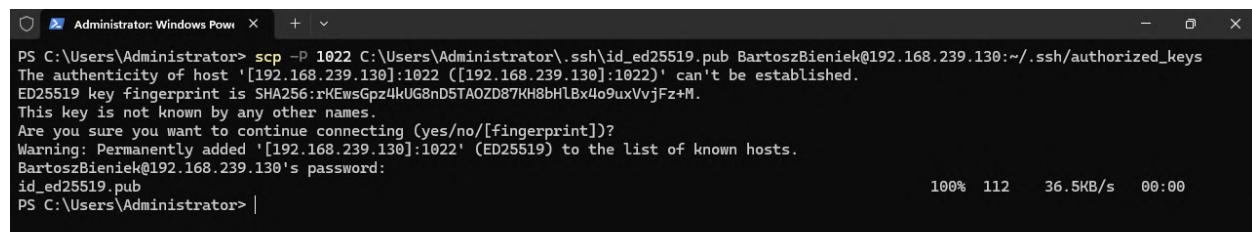
```
[root@localhost ~]# semanage port -l | grep ssh
ssh_port_t          tcp      22
[root@localhost ~]# semanage port -a -t ssh_port_t -p tcp 1022
[root@localhost ~]# semanage port -l | grep ssh
ssh_port_t          tcp      1022, 22
[root@localhost ~]# firewall-cmd --get-active-zones
FedoraServer (default)
  interfaces: ens160
[root@localhost ~]# firewall-cmd --zone=FedoraServer --add-port=1022/tcp --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# systemctl restart sshd
[root@localhost ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
  Drop-In: /usr/lib/systemd/system/service.d
            └─10-timeout-abort.conf
  Active: active (running) since Sun 2025-12-21 01:57:04 CET; 4s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 2510 (sshd)
    Tasks: 1 (limit: 4580)
   Memory: 1.3M
      CPU: 16ms
     CGroup: /system.slice/sshd.service
             └─2510 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 21 01:57:04 localhost.localdomain (sshd)[2510]: sshd.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS
Dec 21 01:57:04 localhost.localdomain systemd[1]: Starting sshd.service - OpenSSH server daemon...
Dec 21 01:57:04 localhost.localdomain sshd[2510]: Server listening on 0.0.0.0 port 1022.
Dec 21 01:57:04 localhost.localdomain sshd[2510]: Server listening on :: port 1022.
Dec 21 01:57:04 localhost.localdomain systemd[1]: Started sshd.service - OpenSSH server daemon.
[root@localhost ~]# _
```

Zrzut ekranu 58 Dodanie wyjątku w podsystemie SELinux i zaporze sieciowej dla niestandardowego portu.

```
[root@localhost ~]# su -l BartoszBieniek
[BartoszBieniek@localhost ~]$ pwd
/home/BartoszBieniek
[BartoszBieniek@localhost ~]$ mkdir .ssh/
[BartoszBieniek@localhost ~]$ chmod 700 .ssh/
[BartoszBieniek@localhost ~]$ ls -la .ssh/
total 0
drwx-----. 2 BartoszBieniek BartoszBieniek 6 Dec 21 01:38 .
drwx-----. 3 BartoszBieniek BartoszBieniek 74 Dec 21 01:38 ..
[BartoszBieniek@localhost ~]$ _
```

Zrzut ekranu 59 Utworzenie katalogu `~/.ssh` z odpowiednimi uprawnieniami.



```
PS C:\Users\Administrator> scp -P 1022 C:\Users\Administrator\.ssh\id_ed25519.pub BartoszBieniek@192.168.239.130:~/ssh/authorized_keys
The authenticity of host '[192.168.239.130]:1022 ([192.168.239.130]:1022)' can't be established.
ED25519 key fingerprint is SHA256:rKEwsGpz4kUG8nD5TA0ZD87KH8bHlBx4o9uxVvjFz+M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added '[192.168.239.130]:1022' (ED25519) to the list of known hosts.
BartoszBieniek@192.168.239.130's password:                                     100% 112    36.5KB/s  00:00
id_ed25519.pub
PS C:\Users\Administrator> |
```

Zrzut ekranu 60 Przeniesienie klucza publicznego z komputera z klienckim systemem Windows 11.

```
[BartoszBieniek@localhost ~]$ ls -la ~/.ssh/
total 4
drwx-----. 2 BartoszBieniek BartoszBieniek 29 Dec 21 01:57 .
drwx-----. 3 BartoszBieniek BartoszBieniek 95 Dec 21 01:39 ..
-rw-r--r--. 1 BartoszBieniek BartoszBieniek 112 Dec 21 01:57 authorized_keys
[BartoszBieniek@localhost ~]$ chmod 600 ~/.ssh/authorized_keys
[BartoszBieniek@localhost ~]$ ls -la ~/.ssh/
total 4
drwx-----. 2 BartoszBieniek BartoszBieniek 29 Dec 21 01:57 .
drwx-----. 3 BartoszBieniek BartoszBieniek 95 Dec 21 01:39 ..
-rw-r--r--. 1 BartoszBieniek BartoszBieniek 112 Dec 21 01:57 authorized_keys
[BartoszBieniek@localhost ~]$ _
```

Zrzut ekranu 61 Zmiana uprawnień dostępu do skopiowanego z komputera klienckiego klucza publicznego.

```
#sshdessions 10
PubkeyAuthentication yes
# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to no to disable s-key passwords
```

Zrzut ekranu 62 Włączenie mechanizmu uwierzytelniania kluczem asymetrycznym i wyłączenie logowania hasłem dla serwera ssh w systemie Fedora.

Po wprowadzeniu zmian restartujemy usługę serwera SSH polecienniem `systemctl restart ssh`, a następnie weryfikujemy możliwość zalogowania się na serwer z systemu klienckiego z wykorzystaniem klucza asymetrycznego.

A screenshot of a Windows Command Prompt window titled "Administrator: Windows Pow". The window shows the following command and its output:

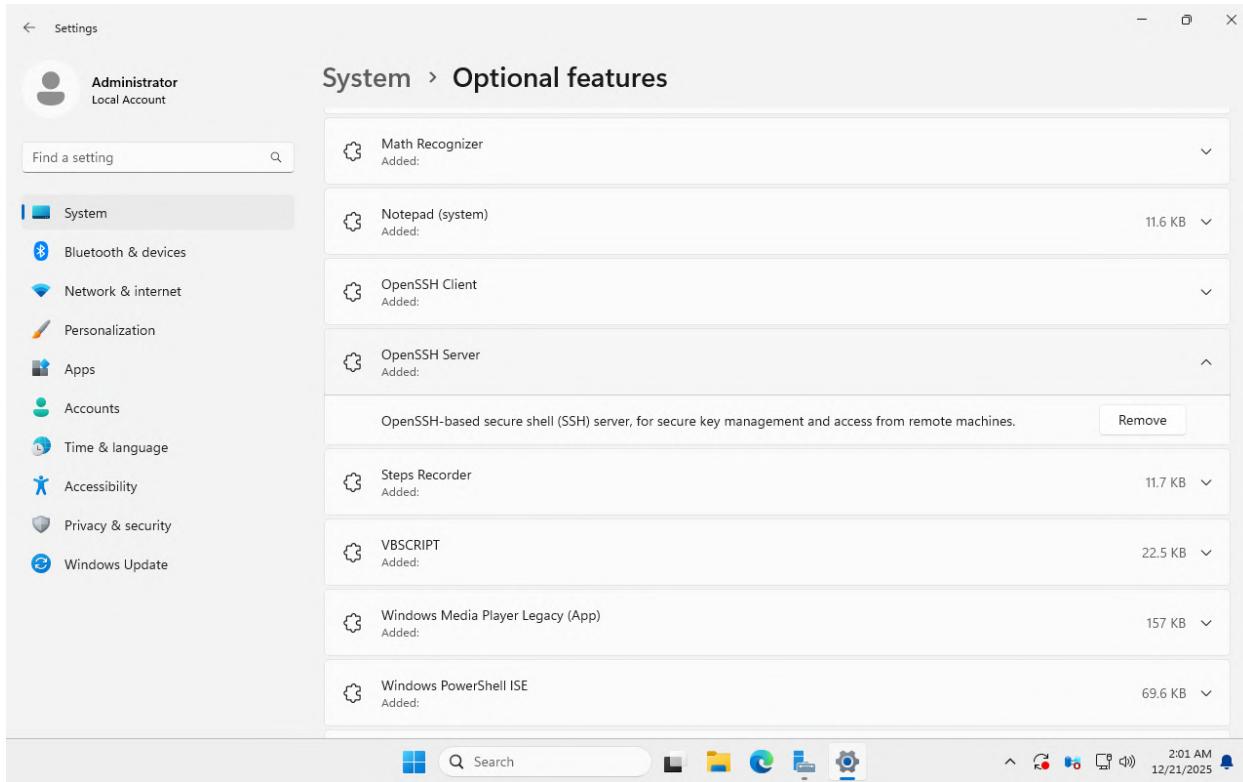
```
PS C:\Users\Administrator> ssh -p 1022 BartoszBieniek@192.168.239.130
Enter passphrase for key 'C:\Users\Administrator/.ssh/id_ed25519':
Last login: Sun Dec 21 01:58:14 2025
BartoszBieniek@localhost: $ exit
logout
Connection to 192.168.239.130 closed.
PS C:\Users\Administrator> ssh -p 1022 -o PreferredAuthentications=password BartoszBieniek@192.168.239.130
BartoszBieniek@192.168.239.130: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
PS C:\Users\Administrator>
```

The taskbar at the bottom of the screen includes icons for weather (3°C Pochmurnie), search, and various system applications. The system tray shows the date and time as "2:00 AM 12/21/2025".

Zrzut ekranu 63 Poprawne logowanie z wykorzystaniem klucza asymetrycznego z systemu klienckiego. Nieudana próba zalogowania z wykorzystaniem hasła.

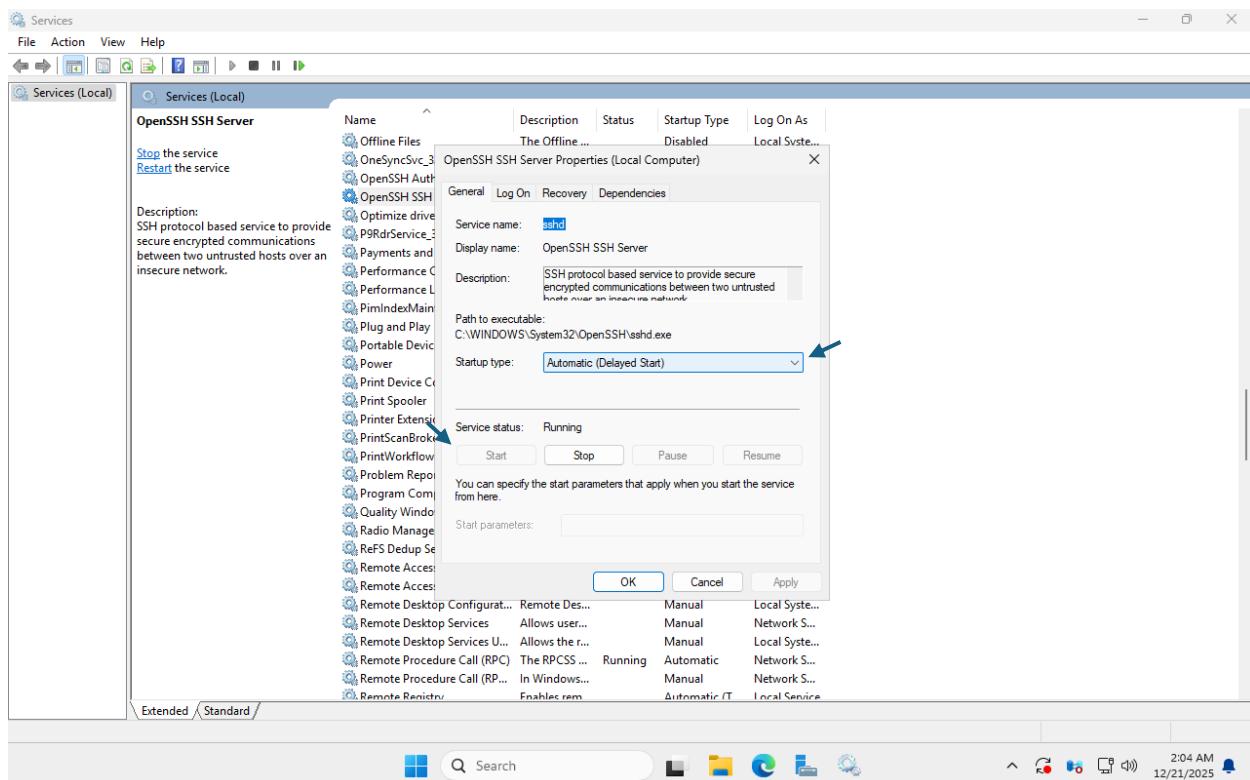
Proces instalacji i uruchomienia serwera SSH wygląda zupełnie inaczej w systemie Windows Server.

Aby zainstalować pakiet należy przejść do ustawień i w zakładce *System* → *Optional features* wyszukać i dodać pakiet *OpenSSH Server*.



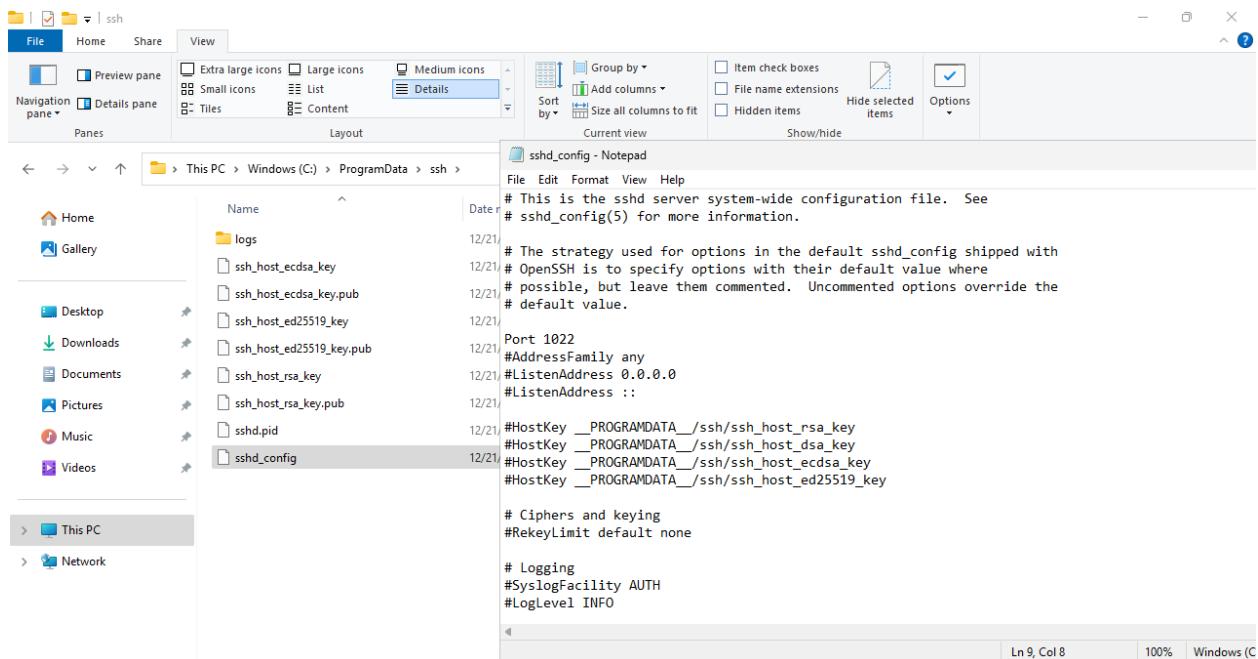
Zrzut ekranu 64 Instalacja serwera SSH w systemie Windows Server.

Serwer można następnie uruchomić w aplikacji *Services* poprzez włączenie usługi *OpenSSH SSH Server*. Warto również zaznaczyć tryb automatycznego startu wraz z systemem, co umożliwi zdalny dostęp po jego restarcie.



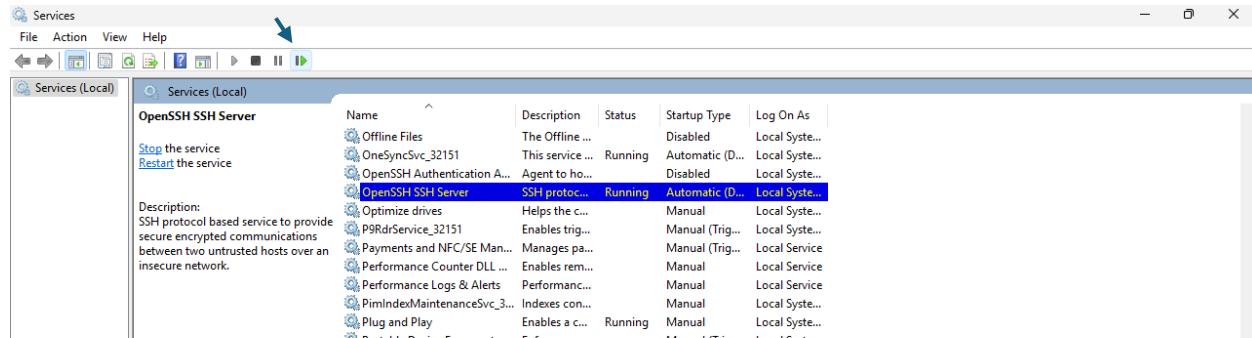
Zrzut ekranu 65 Włączenie usługi serwera SSH w systemie Windows.

W celu ustawienia niestandardowego portu, należy zmienić konfigurację programu.
Znajduje się ona w pliku C:\ProgramData\ssh\sshd_config.

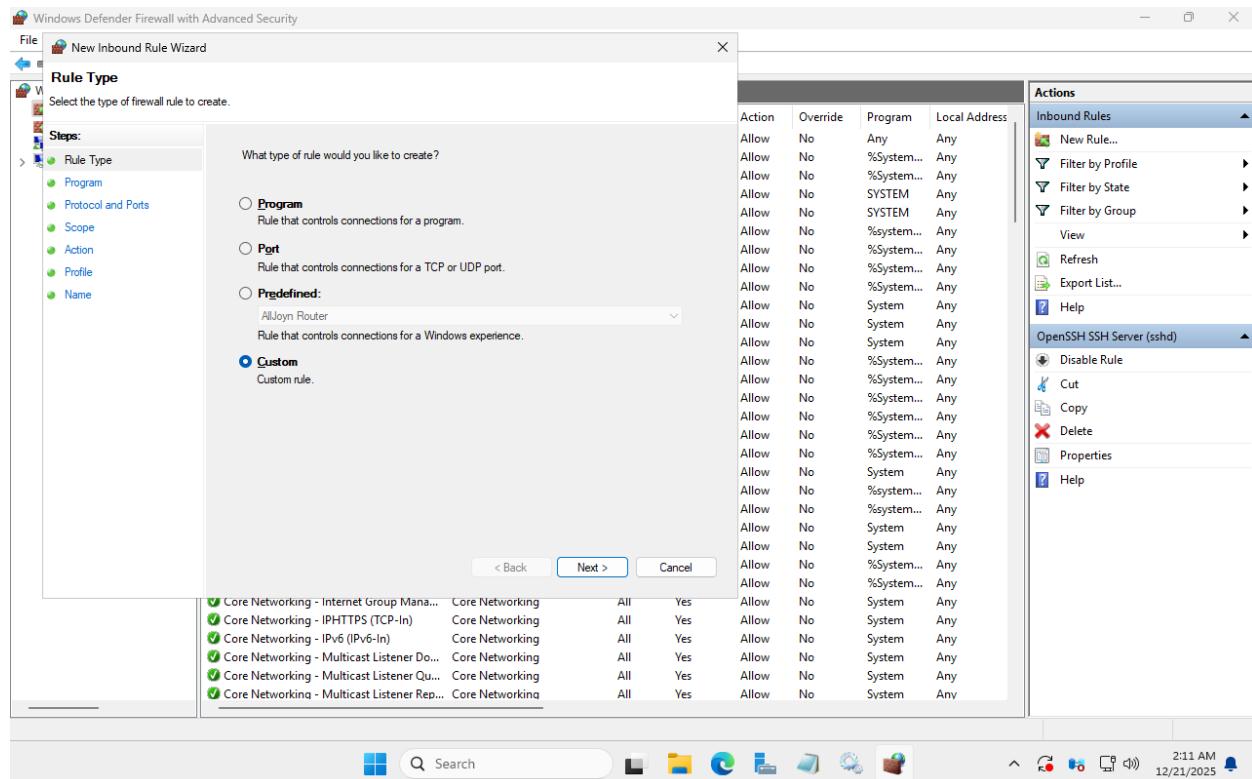


Zrzut ekranu 66 Konfiguracja niestandardowego portu serwera SSH na maszynie z systemem Windows Server.

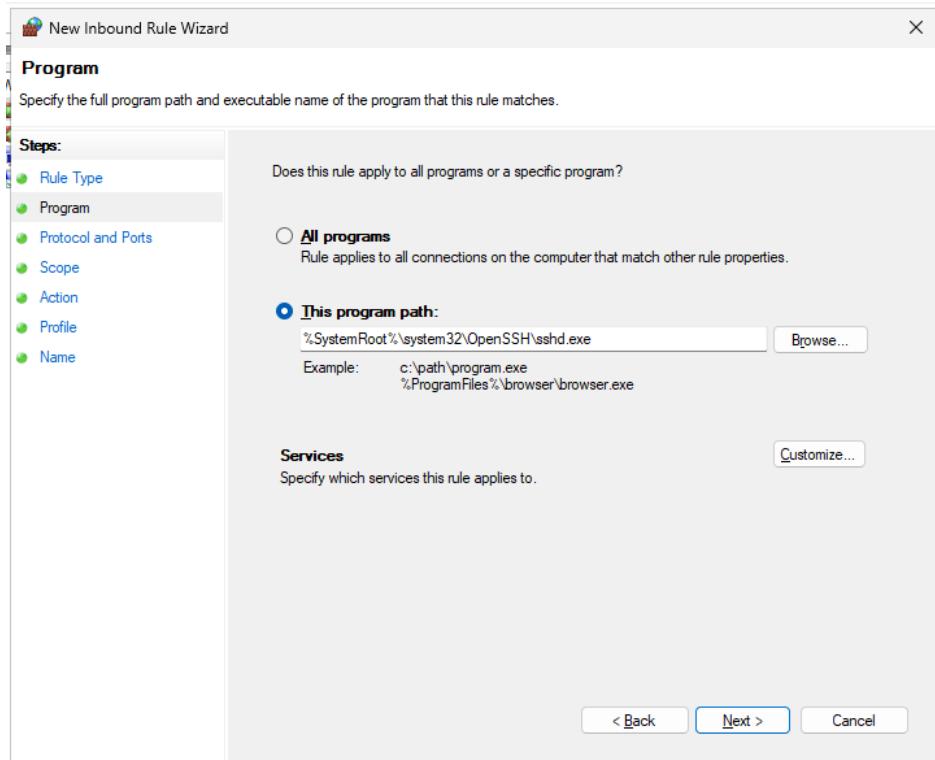
Po wprowadzeniu zmian konieczny jest restart usługi, a także utworzenie wyjątku w zaporze sieciowej.



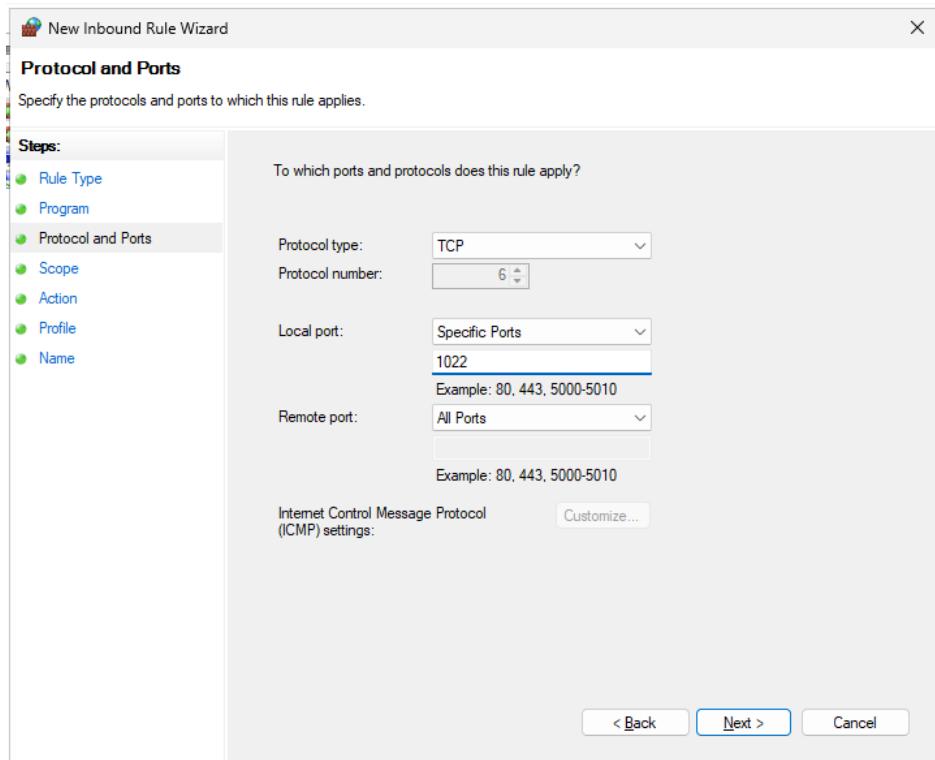
Zrzut ekranu 67 Restart usługi serwera SSH w systemie Windows Server.



Zrzut ekranu 68 Tworzenie wyjątku w zaporze sieciowej systemu Windows na potrzeby serwera SSH działającego na niestandardowym porcie (krok 1).

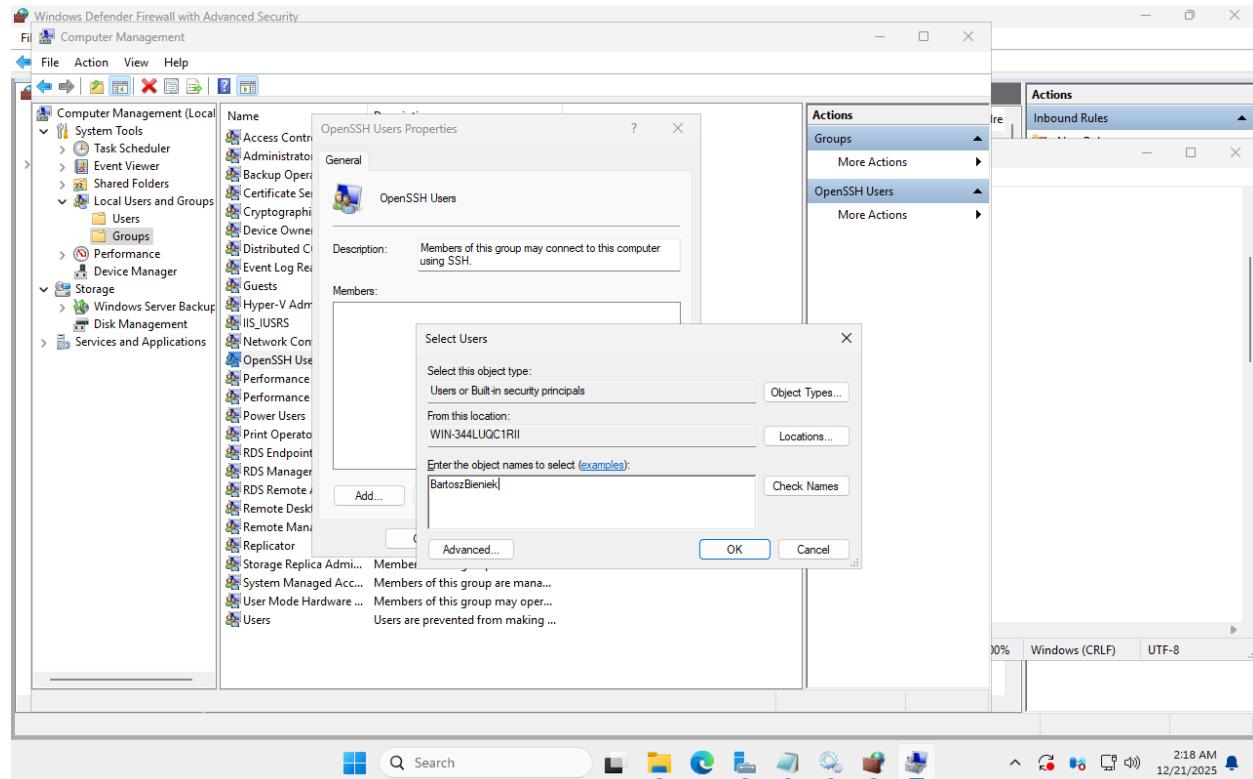


Zrzut ekranu 69 Wskazanie programu (serwera SSH), który będzie mógł korzystać z tworzonej reguły.



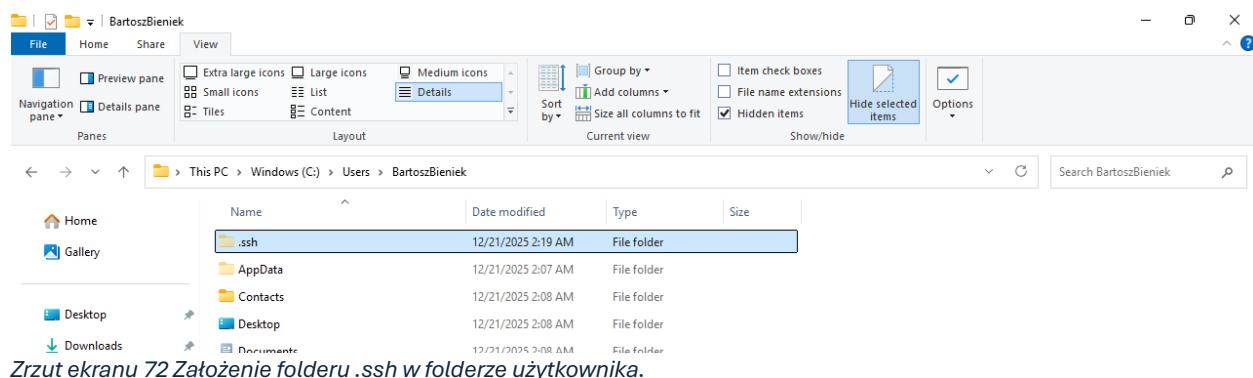
Zrzut ekranu 70 Wskazanie protokołu i portu, na którym będzie nastuchiwiał serwer SSH.

Zanim możliwe będzie jeszcze logowanie się przez SSH na założone na nim konta użytkowników, konieczne jest dodanie ich do specjalnie utworzonej w tym celu grupy – OpenSSH Users.



Zrzut ekranu 71 Dodanie użytkownika do grupy OpenSSH Users, aby umożliwić mu logowanie przez SSH.

Od teraz wskazani użytkownicy będą mogli łączyć się przez SSH. Wykorzystajmy to, tak jak w przypadku systemów *Linux*, do pobrania klucza publicznego komputera klienckiego.



Zrzut ekranu 72 Założenie folderu .ssh w folderze użytkownika.

```
Administrator: Windows Pow + x
PS C:\Users\Administrator> scp -P 1022 C:\Users\Administrator\.ssh\id_ed25519.pub BartoszBieniek@192.168.239.131:~\.ssh\authorized_keys
The authenticity of host '[192.168.239.131]:1022 ([192.168.239.131]:1022)' can't be established.
ED25519 key fingerprint is SHA256:0la1wgTpZX7tR6Wc9mza8EMGcsi+3bgNPMfyfD8cg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added '[192.168.239.131]:1022' (ED25519) to the list of known hosts.
BartoszBieniek@192.168.239.131's password:
id_ed25519.pub
PS C:\Users\Administrator>
```

Zrzut ekranu 73 Przeniesienie klucza publicznego z komputera z klienckim systemem Windows 11.

```
sshd_config - Notepad
File Edit Format View Help
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes ←

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysfile      .ssh/authorized_keys ←

#AuthorizedPrincipalsFile none

# For this to work you will also need host keys in %programData%ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no ←
#PermitEmptyPasswords no

# GSSAPI options
#GSSAPIAuthentication no

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
```

Zrzut ekranu 74 Włączenie mechanizmu uwierzytelniania kluczem asymetrycznym i wyłączenie logowania hasłem dla serwera ssh w systemie Windows Server.

Po wprowadzeniu zmian należy ponownie uruchomić usługę serwera SSH.

Administrator: Windows Pow

```
PS C:\Users\Administrator> ssh -p 1022 BartoszBieniek@192.168.239.131
Enter passphrase for key 'C:\Users\Administrator/.ssh/id_ed25519': |
```

Administrator: Windows Pow

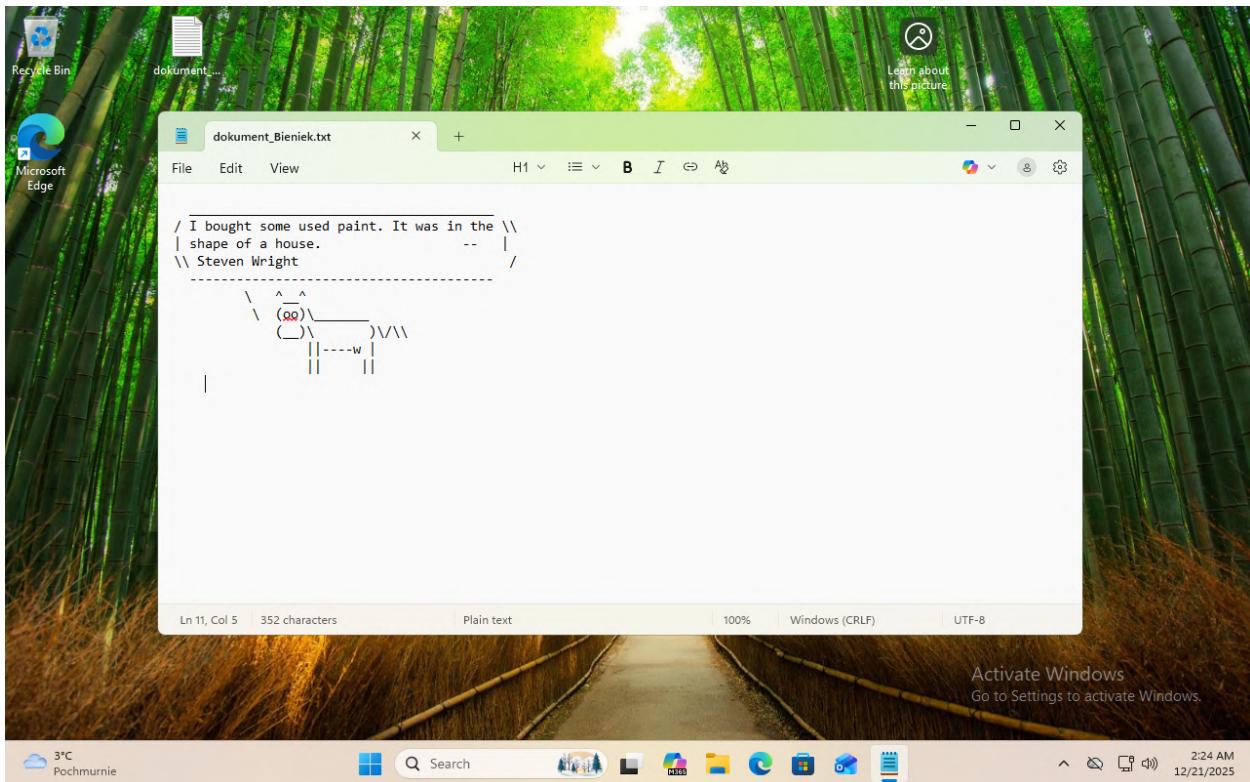
```
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserved.

bartoszbieniek@WIN-344LUQC1RII C:\Users\BartoszBieniek>exit
Connection to 192.168.239.131 closed.
PS C:\Users\Administrator> ssh -p 1022 -o PreferredAuthentications=password BartoszBieniek@192.168.239.130
BartoszBieniek@192.168.239.130: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
PS C:\Users\Administrator> |
```

Activate Windows
Go to Settings to activate Windows.

Zrzut ekranu 75 Poprawne logowanie z wykorzystaniem klucza asymetrycznego z systemu klienckiego. Nieudana próba zalogowania z wykorzystaniem hasła.

Przetestowaliśmy już możliwość logowania z wykorzystaniem klucza asymetrycznego. Warto jeszcze zweryfikować działanie programu *scp*, przesyłającego pliki z wykorzystaniem SSH. W tym celu utworzę na pulpicie komputera klienckiego plik, a następnie roześle go na wszystkie maszyny z systemami serwerowymi.



Zrzut ekranu 76 Utworzenie testowego pliku tekstuowego na komputerze klienckim.

```
BartoszBieniek@debian:~$ ls
dokument_Bieniek.txt
BartoszBieniek@debian:~$ cat dokument_Bieniek.txt

/ I bought some used paint. It was in the \\
| shape of a house.          -- |
\\ Steven Wright
-----
\ ^ ^
 \(oo)\_____
 (__) \      )\\\\
    ||----w |
    || |||
```

Zrzut ekranu 77 Sprawdzenie zawartości skopiowanego pliku na maszynie wirtualnej z systemem Debian.

```
BartoszBieniek@ubuntuserver:~$ ls
dokument_Bieniek.txt
BartoszBieniek@ubuntuserver:~$ cat dokument_Bieniek.txt

/ I bought some used paint. It was in the \\ 
| shape of a house.          -- |
\\ Steven Wright           / 

\   ^__^
 \  (oo)\_____
   (__)\       )\/\
     ||----w |
     ||     ||
```

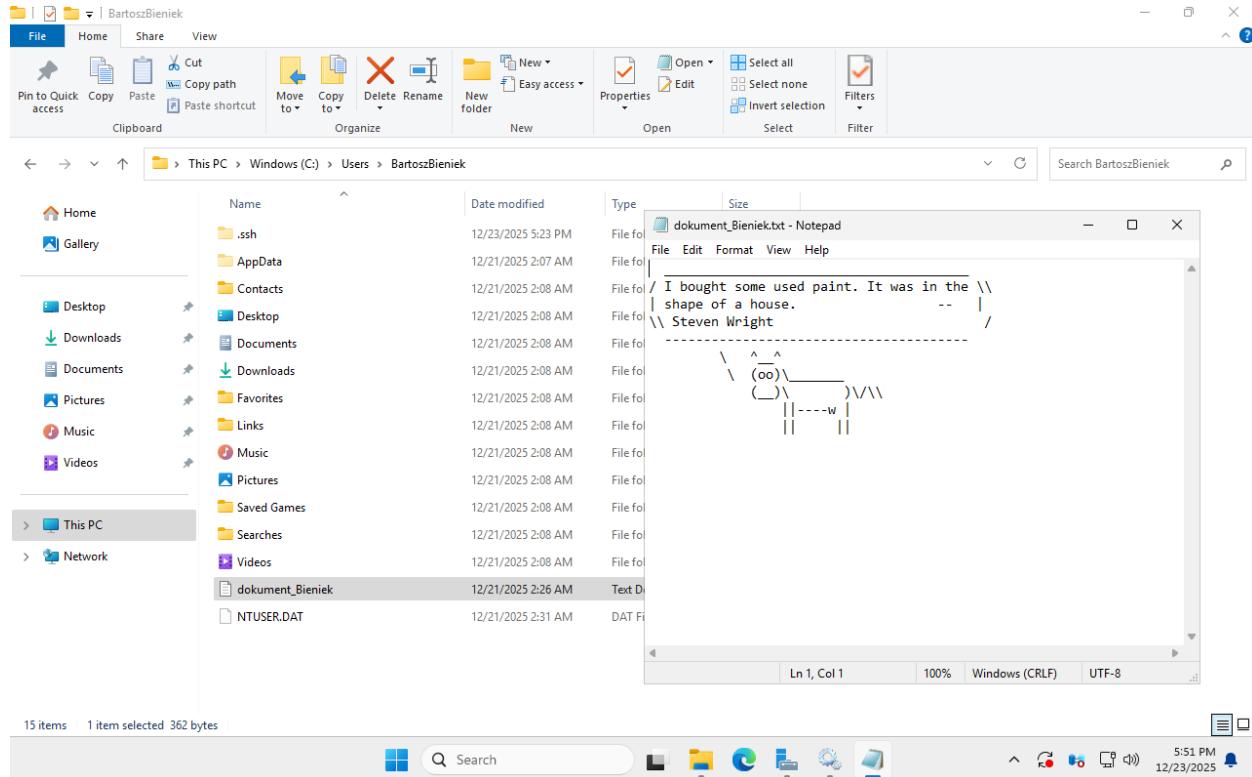
Zrzut ekranu 78 Sprawdzenie zawartości skopowanego pliku na maszynie wirtualnej z systemem Ubuntu.

```
[BartoszBieniek@localhost ~]$ ls
dokument_Bieniek.txt
[BartoszBieniek@localhost ~]$ cat dokument_Bieniek.txt

/ I bought some used paint. It was in the \\ 
| shape of a house.          -- |
\\ Steven Wright           / 

\   ^__^
 \  (oo)\_____
   (__)\       )\/\
     ||----w |
     ||     ||
```

Zrzut ekranu 79 Sprawdzenie zawartości skopowanego pliku na maszynie wirtualnej z systemem Fedora.



Zrzut ekranu 80 Sprawdzenie zawartości skopowanego pliku na maszynie wirtualnej z systemem Windows Server.

Poziom bezpieczeństwa można podnieść konfigurując mechanizm uwierzytelniania dwuetapowego, na przykład z wykorzystaniem kodów czasowych. W systemach Linux wystarczy w tym celu doinstalować i skonfigurować odpowiedni *moduł PAM* (*Pluggable Authentication Modules*) – w naszym przypadku *libpam-google-authenticator*. Wbrew swojej nazwie, kody będzie można generować w dowolnej aplikacji, na przykład *Proton Authenticator*.

```
root@debian:~# apt install libpam-google-authenticator
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libqrencode4
The following NEW packages will be installed:
  libpam-google-authenticator libqrencode4
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 85.9 kB of archives.
After this operation, 229 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://deb.debian.org/debian bookworm/main amd64 libqrencode4 amd64 4.1.1-1 [40.4 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 libpam-google-authenticator amd64 20191231-2 [45.5 kB]
Fetched 85.9 kB in 0s (991 kB/s)
Selecting previously unselected package libqrencode4:amd64.
(Reading database ... 33415 files and directories currently installed.)
Preparing to unpack .../libqrencode4_4.1.1-1_amd64.deb ...
Unpacking libqrencode4:amd64 (4.1.1-1) ...
Selecting previously unselected package libpam-google-authenticator.
Preparing to unpack .../libpam-google-authenticator_20191231-2_amd64.deb ...
Unpacking libpam-google-authenticator (20191231-2) ...
Setting up libqrencode4:amd64 (4.1.1-1) ...
Setting up libpam-google-authenticator (20191231-2) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u13) ...
root@debian:~#
```

Zrzut ekranu 81 Instalacja modułu *libpam-google-authenticator*.

Następnie w *pliku konfiguracyjnym PAM dla SSH*, */etc/pam.d/sshd*, należy umieścić wpis dodający zainstalowany przed chwilą moduł *libpam-google-authenticator*.

```
session optional pam_deny.so
# Standard Unix password updating.
@include common-password
# Multi-factor authentication.          ↛
auth required pam_google_authenticator.so
```

Zrzut ekranu 82 Dodanie modułu *libpam-google-authenticator* do pliku konfiguracyjnego */etc/pam.d/sshd*.

Ponieważ wyłączyliśmy możliwość logowania hasłem, konieczne będzie także usunięcie (zakomentowanie) linijki dotyczącej ten rodzaj autentykacji.

```
# PAM configuration for the Secure Shell service
# Standard Unix authentication.
#@include common-auth
# Disallow non-root logins when /etc/pam.d/login exists.
```

Zrzut ekranu 83 Wyłączenie modułu odpowiedzialnego za mechanizm logowania z hasłem.

Aby aktywować mechanizm *PAM* i hasła typu „zadanie-odpowiedź” (czyli między innymi mechanizm MFA z kodami czasowymi) konieczne jest także dokonanie zmian w pliku konfiguracyjnym serwera *SSH*.

```
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication yes ←
AuthenticationMethods publickey,keyboard-interactive ←

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetFSToken no

# GSSAPI options
#gssapiAuthentication no
#gssapiCleanupCredentials yes
#gssapiStrictAcceptorCheck yes
#gssapiKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin prohibit-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes ←

#AllowAgentForwarding yes
```

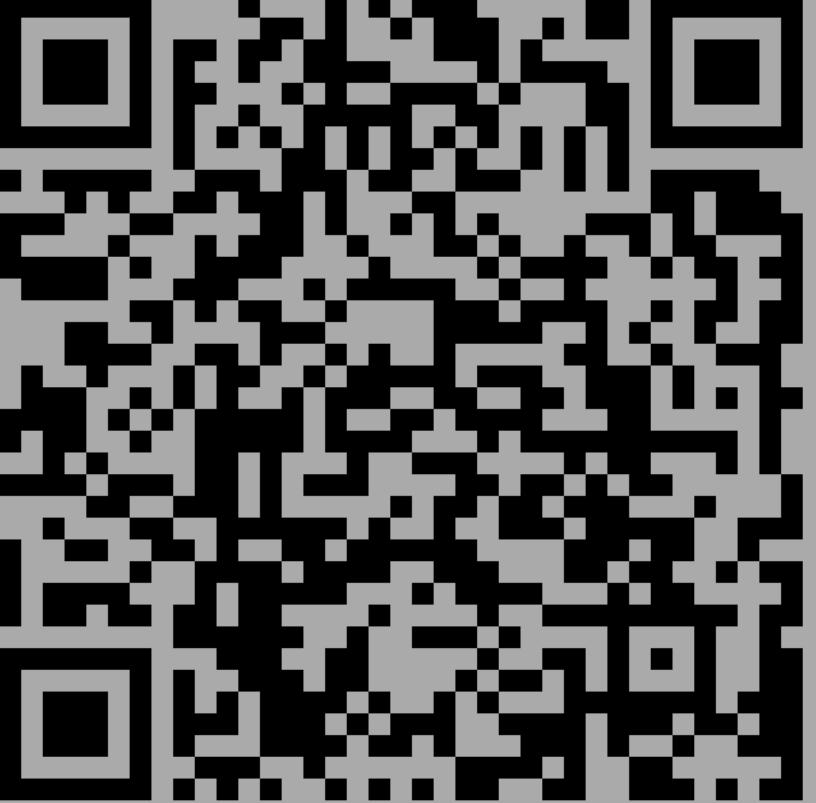
Zrzut ekranu 84 Aktywacja mechanizmu PAM oraz włączenie obsługi haseł typu "zadanie-odpowiedź".

Po wprowadzeniu zmian konieczne jest zrestartowanie serwera SSH polecienniem *systemctl restart sshd*.

Możemy teraz przejść do wygenerowania sekretu OTP, przechodząc na konto użytkownika docelowego i wykonując polecenie *google-authenticator*.

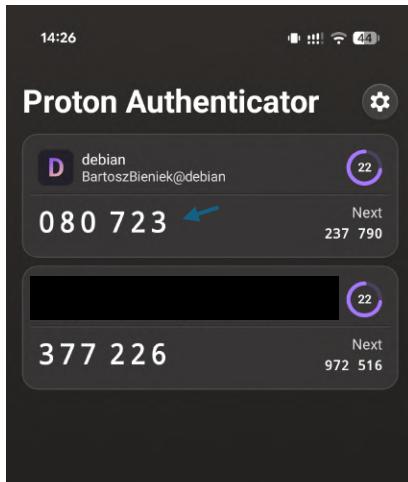
```
root@debian:~# su -l BartoszBieniek
BartoszBieniek@debian:~$ google-authenticator

Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/BartoszBieniek@debian%3Fsecret%3Dj

  
Your new secret key is: JDLCDQMC6EVWC3AFC7R3B7QDM4
Enter code from app (-1 to skip): _
```

Zrzut ekranu 85 Efekt wywołania komendy `google-authenticator`.

Otrzymany kod skanujemy teraz w aplikacji generującej kody czasowe *TOTP*, na przykład *Proton Authenticator*, a następnie przepisujemy na komputerze odczytany w niej kod, aby upewnić się, że proces przebiegł pomyślnie.



Zrzut ekranu 86 Kod czasowy wygenerowany w aplikacji Proton Authenticator.

```
Your new secret key is: JDLCDQMC6EVWC3AFC7R3B7QDM4
Enter code from app (-1 to skip): 080723
Code confirmed
Your emergency scratch codes are:
26806178
81604310
14780625
17387961
60481912

Do you want me to update your "/home/BartoszBieniek/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) n

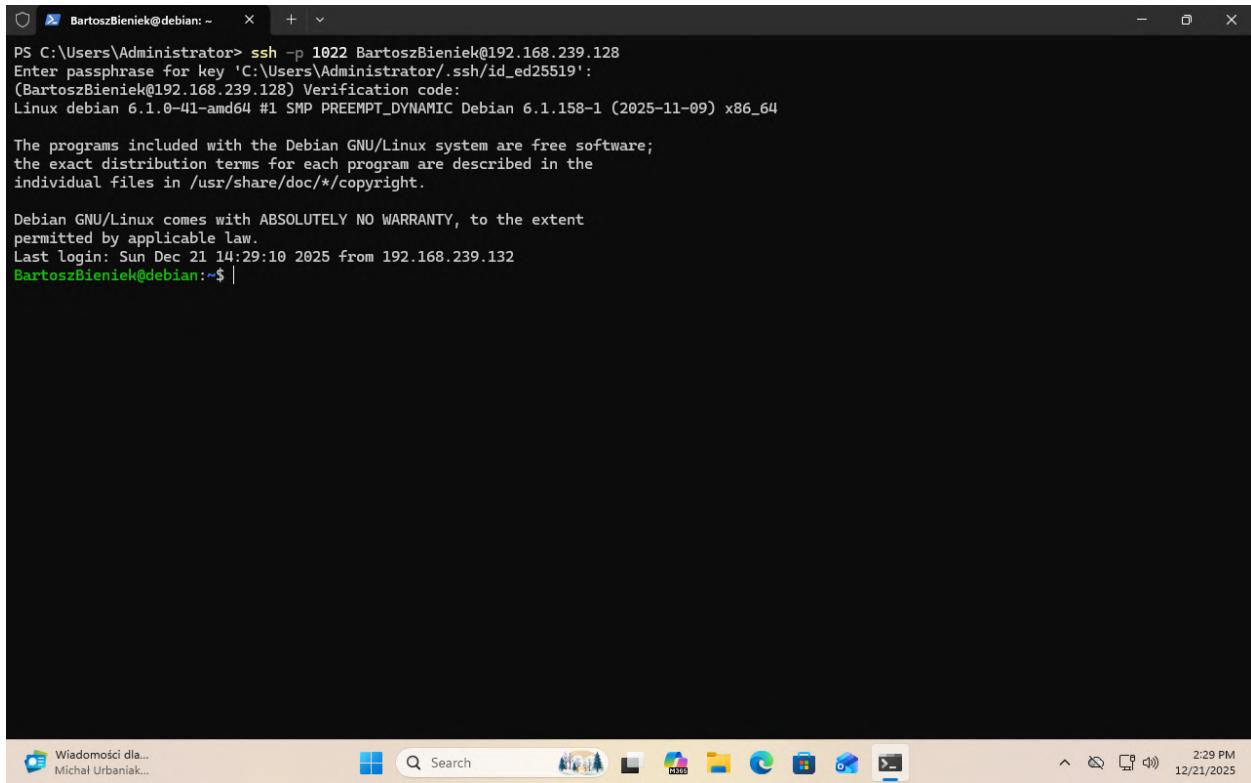
By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) n
BartoszBieniek@debian:~$
```

Zrzut ekranu 87 Dokończenie konfiguracji kodów czasowych.

Po wpisaniu poprawnego kodu z aplikacji, na ekranie zostają wypisane hasła zapasowe, które mogą przydać się w przypadku utraty do niej dostępu. Jesteśmy także pytani o dodatkowe ustawienia tego mechanizmu, które konfigurujemy zgodnie z polityką bezpieczeństwa.

Skonfigurowane uwierzytelnianie dwuetapowe możemy teraz przetestować.



A screenshot of a Windows desktop environment. At the top is a dark terminal window titled "BartoszBieniek@debian: ~". It displays a command-line session where a user has logged in via SSH from a Windows host. The session includes prompts for a passphrase, the Debian license, and a warning about the lack of warranty. The terminal ends with a prompt "\$". Below the terminal is a standard Windows taskbar. On the left side of the taskbar, there's a notification for "Wiadomości dla..." from "Michał Urbaniak...". The taskbar also features icons for the Start button, Search, File Explorer, Task View, Edge browser, File Explorer, Task View, and File Explorer. On the right side of the taskbar, there are system icons for battery status, signal strength, and the date and time ("2:29 PM 12/21/2025").

```
PS C:\Users\Administrator> ssh -p 1022 BartoszBieniek@192.168.239.128
Enter passphrase for key 'C:\Users\Administrator/.ssh/id_ed25519':
(BartoszBieniek@192.168.239.128) Verification code:
Linux debian 6.1.0-41-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.158-1 (2025-11-09) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

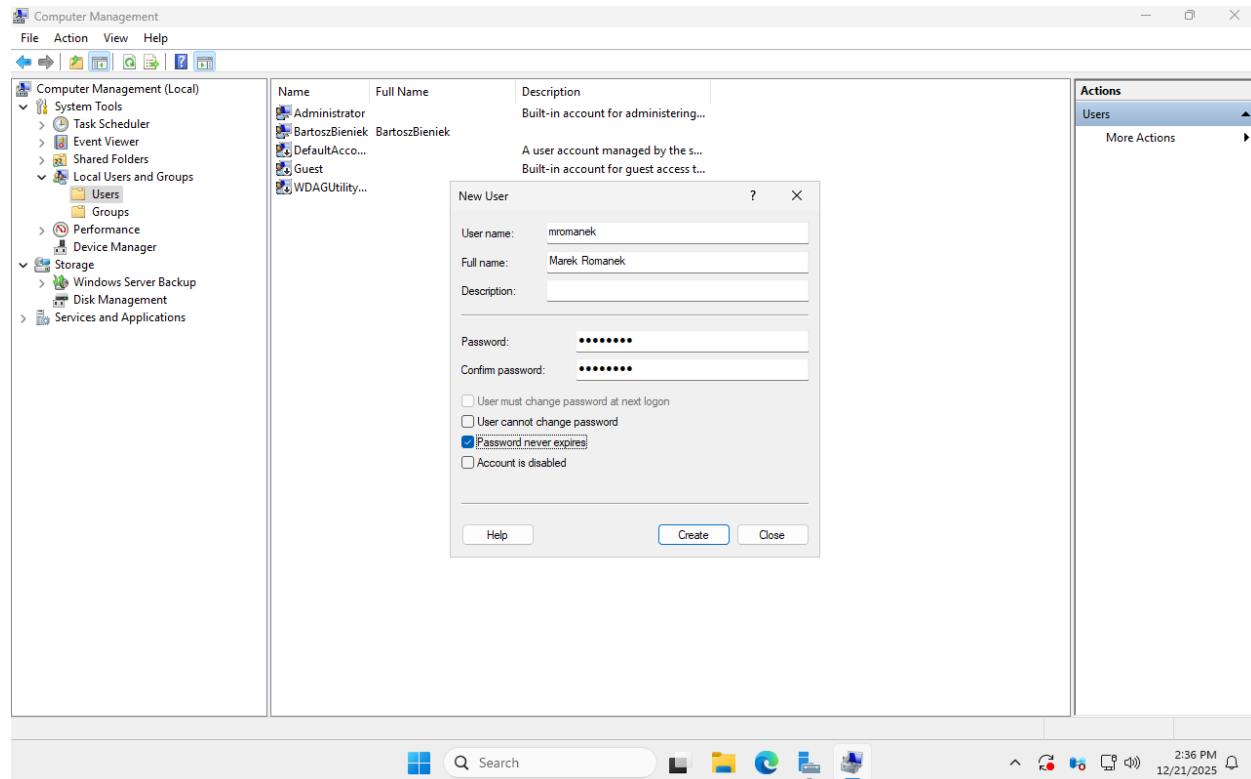
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec 21 14:29:10 2025 from 192.168.239.132
BartoszBieniek@debian:~$ |
```

Zrzut ekranu 88 Udane logowanie przez SSH po podaniu kodu czasowego z aplikacji.

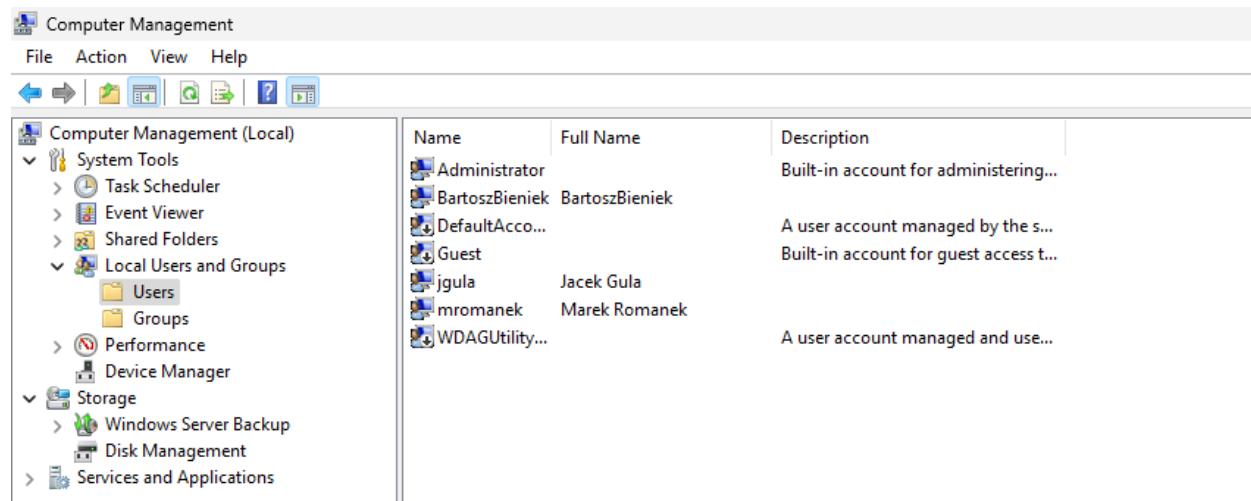
Jak widać, po uwierzytelnieniu się kluczem asymetrycznym, do zalogowania konieczne było także podanie kodu odczytanego z aplikacji.

Zadanie 2. Zarządzanie użytkownikami i grupami, zasoby sieciowe.

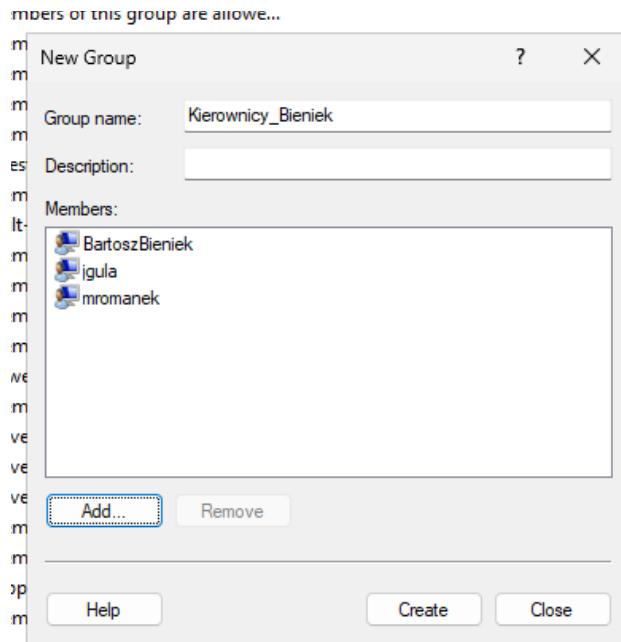
Na samym początku utwórzmy dwóch dodatkowych użytkowników, a następnie przypiszmy ich do wspólnej grupy. Wykorzystamy do tego celu aplikację *Computer Management*.



Zrzut ekranu 89 Tworzenie nowych użytkowników w systemie Windows Server.

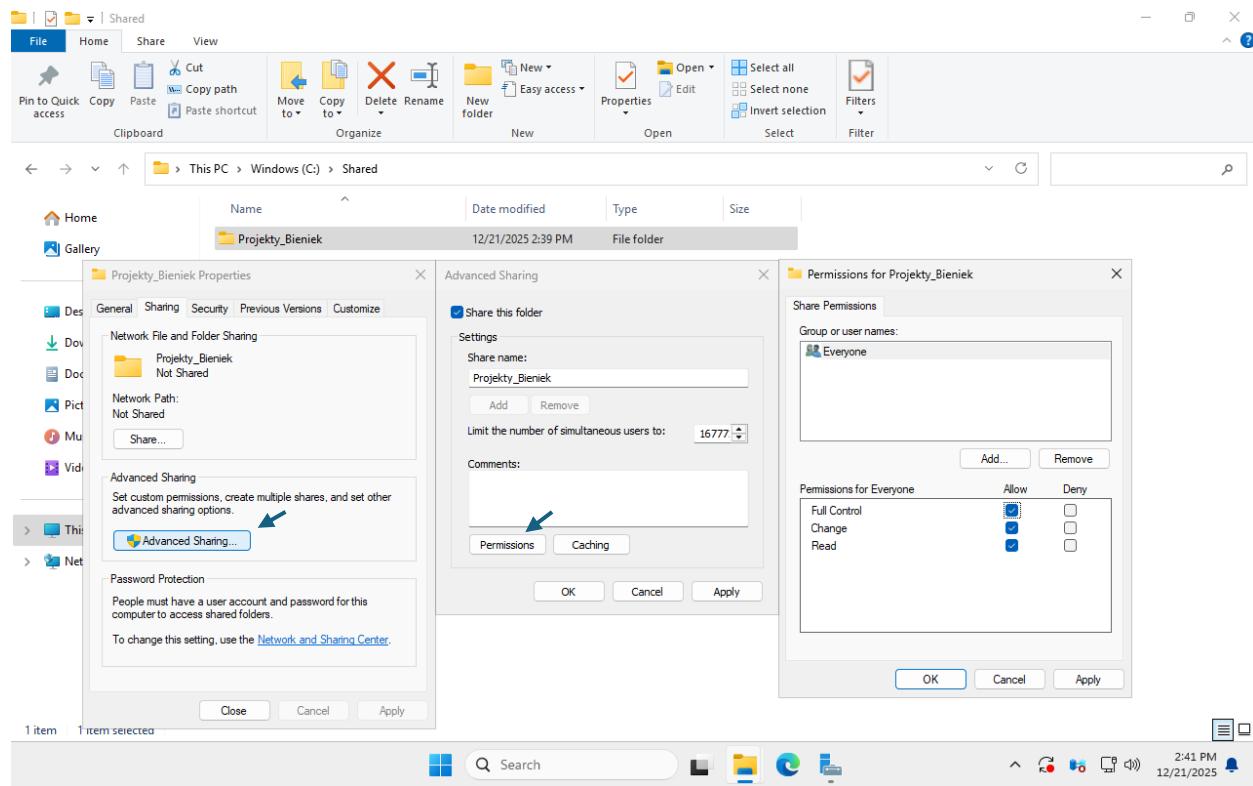


Zrzut ekranu 90 Lista użytkowników na maszynie wirtualnej z systemem Windows Server.



Zrzut ekranu 91 Przypisywanie użytkowników do grupy.

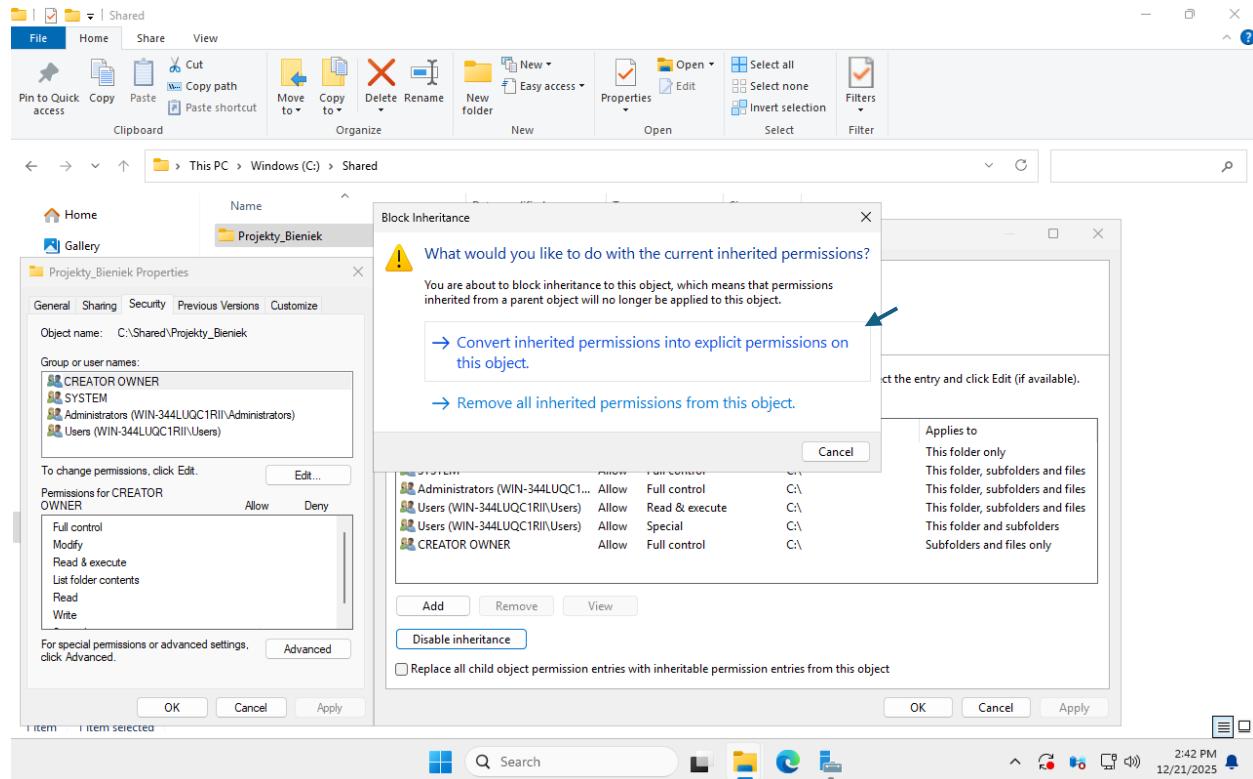
Możemy teraz udostępnić w sieci katalog, do którego dostęp będą mieli kierownicy z wyłączeniem pana Marka Romanka. W tym celu należy najpierw utworzyć na dysku nowy folder i z menu właściwości, w zakładce *Sharing* przydzielić wszystkim pełną kontrolę.



Zrzut ekranu 92 Udostępnianie folderu w sieci.

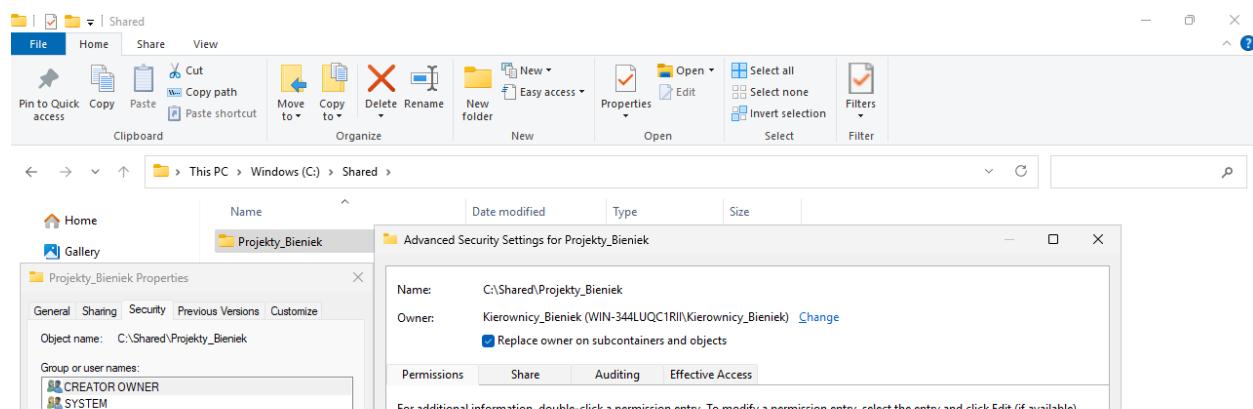
Gdyby dysk nie był sformatowany jako *NTFS*, już na tym etapie musielibyśmy przydzielić odpowiednie prawa dostępu dla użytkowników zdalnych. Ponieważ jest inaczej, mamy dostęp do zakładki *Security*, w której te prawa nadamy.

Przechodząc do zaawansowanych ustawień bezpieczeństwa, musimy w pierwszej kolejności wyłączyć dziedziczenie uprawnień, aby móc je modyfikować.



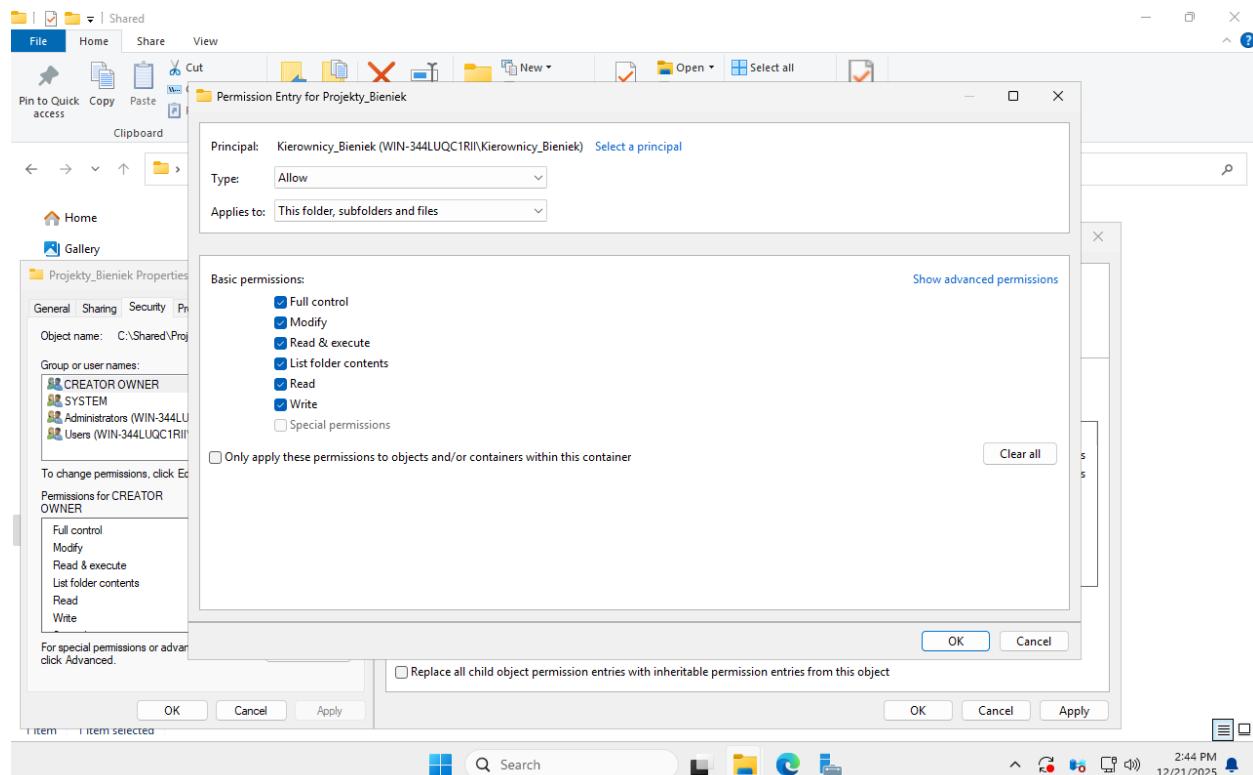
Zrzut ekranu 93 Wyłączenie dziedziczenia uprawnień.

Ponieważ będzie to folder użytkowany przez grupę Kierowników, możemy nadać jej do niego własność.



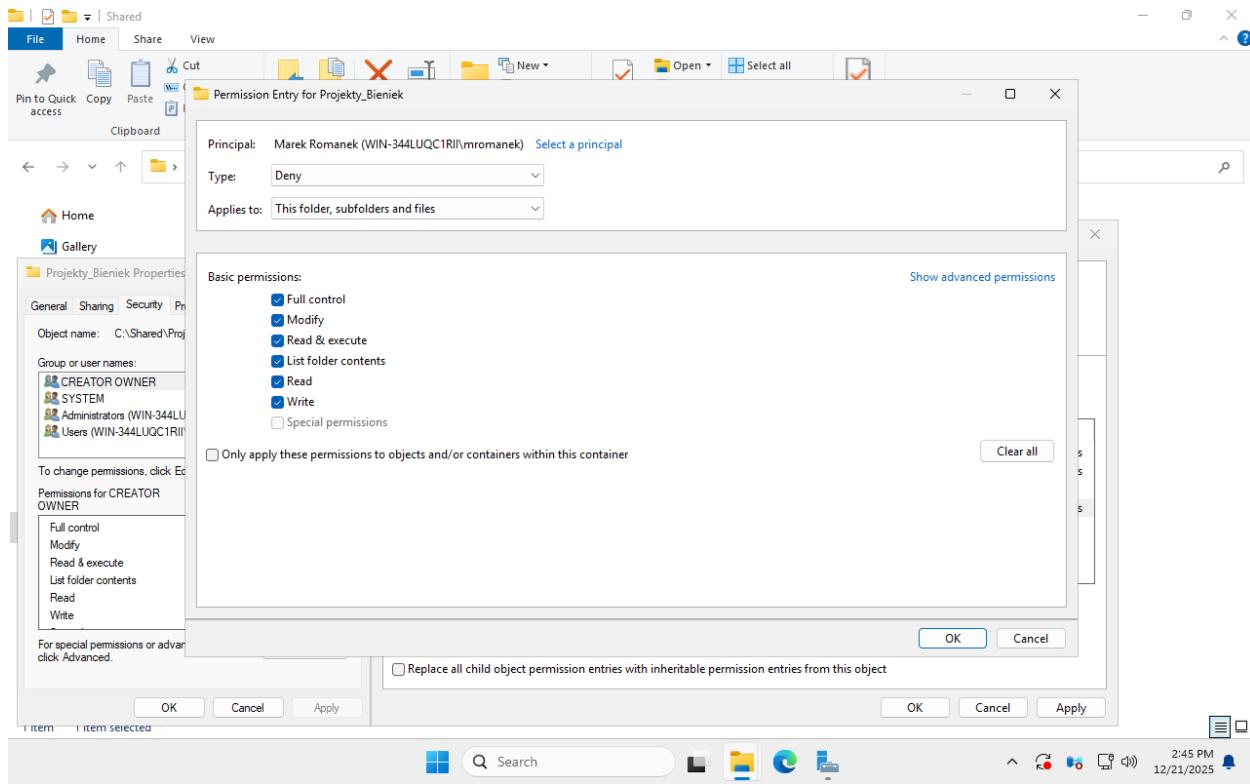
Zrzut ekranu 94 Nadanie grupie Kierownicy własności do folderu Projekty.

Przydzielmy im teraz prawa pełnej kontroli nad folderem.



Zrzut ekranu 95 Przydzielenie pełnej kontroli nad katalogiem użytkownikom należącym do grupy

Celem zadania było także ograniczenie dostępu dla wybranego użytkownika należącego do grupy kierowników. W tym celu dodamy kolejny wpis z uprawnieniami – tym razem typu *Deny*. Wskazując pełne prawa dostępu, całkowicie zablokujemy mu możliwość wykonywania jakichkolwiek operacji (w tym odczytu) na katalogu.



Zrzut ekranu 96 Odebranie wszelkich praw do folderu wybranemu użytkownikowi.

Może się zdarzyć, że awarii ulegnie serwer lub sieć komputerowa. Aby użytkownicy mogli dalej pracować na plikach zawartych w modyfikowanym przed chwilą katalogu, konieczne będzie wcześniejsze włączenie „plików trybu offline”. Opcję tę można aktywować przechodząc do właściwości folderu → Advanced Sharing → Caching i zaznaczając *All files and programs that users open from the shared folder are automatically available offline*. Dla poprawy wydajności warto zaznaczyć *Optimize for performance*.

Aby przetestować działanie mechanizmu, przyjmijmy, że z komputera klienckiego korzystają ci sami użytkownicy co z serwera i mają na nim utworzone swoje konta z identycznymi hasłami (nie będzie wówczas konieczności manualnego logowania się przy podłączaniu dysku sieciowego).

The screenshot shows the Windows Computer Management console window. The left sidebar lists various management tools: System Tools (Task Scheduler, Event Viewer, Shared Folders), Local Users and Groups (with sub-folders for Users and Groups), Performance, Storage (Disk Management), and Services and Applications. The main pane displays a table of user accounts:

Name	Full Name	Description
Administrator	Bartosz Bieniek	Built-in account for administering...
BartoszBieniek	Bartosz Bieniek	A user account managed by the s...
DefaultAcco...		Built-in account for guest access t...
Guest	Jacek Gula	Built-in account for guest access t...
jgula	Jacek Gula	A user account managed and use...
mromanek	Marek Romanek	
WDAGUtility...		

The Actions ribbon tab is selected, and the 'More Actions' dropdown is visible.

Zrzut ekranu 97 Utworzono na komputerze klienckim konta użytkowników.

Do testów wykorzystam konto Jacka Guli.

W pierwszej kolejności, aby móc w ogóle skorzystać z mechanizmu „plików trybu offline”, konieczne będzie włączenie tej usługi z poziomu panelu sterowania → *All Control Panel Items* → *Sync Center* → *Manage offline files* i kliknięcie na przycisk *Enable offline files*.

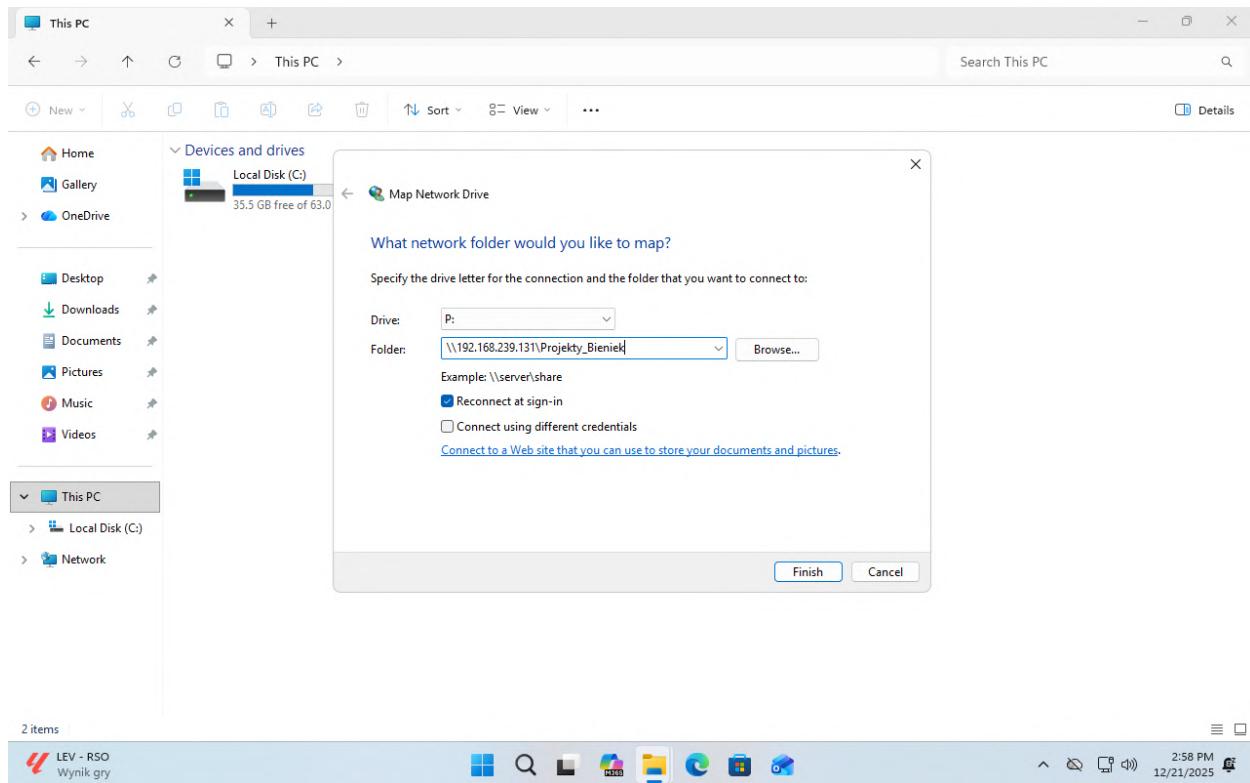
The screenshot shows the Windows Control Panel Sync Center. The address bar indicates the path: Control Panel > All Control Panel Items > Sync Center. The main area displays the 'Keep your information in sync' section with links for View sync partnerships, View sync conflicts, View sync results, Set up new sync partnerships, and Manage offline files. A callout arrow points to the 'Manage offline files' link.

A modal dialog box titled 'Offline Files' is open. It contains the following text: "Use offline files to keep copies of files stored on the network. This allows you to work with them even when you are not connected or a server is unavailable." Below this is a button labeled "Disable offline files". A message at the bottom states: "Offline Files is currently enabled." There are also buttons for "Open Sync Center", "View your offline files", "OK", "Cancel", and "Apply".



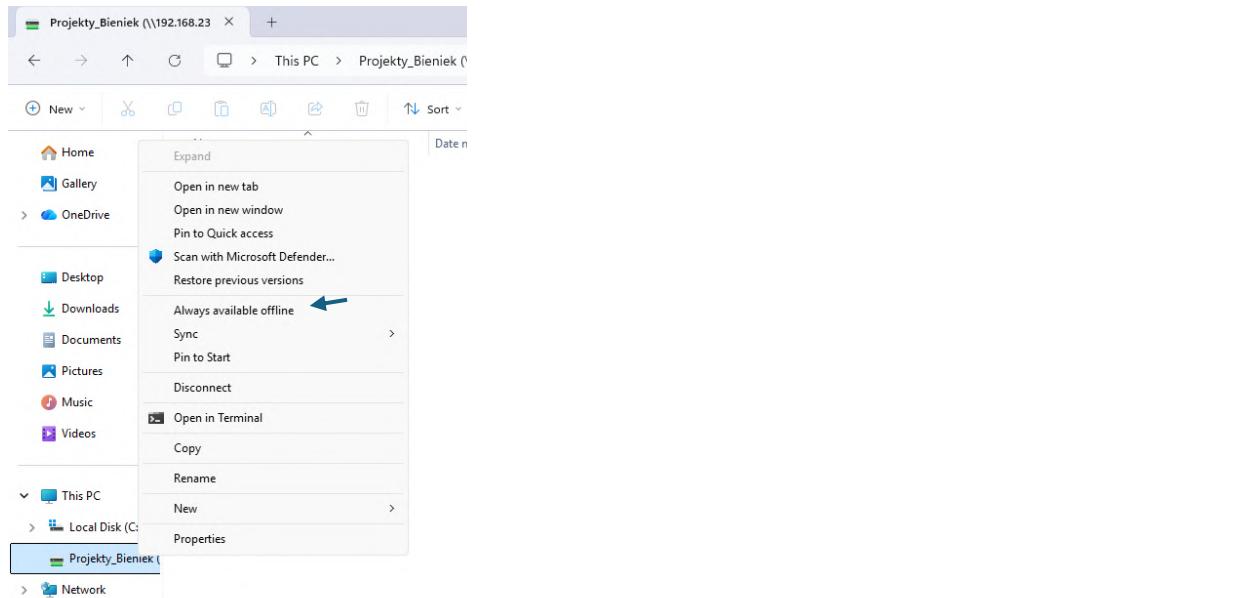
Zrzut ekranu 98 Włączenie plików trybu offline.

Dalej, podłączę folder Projekty jako dysk sieciowy.



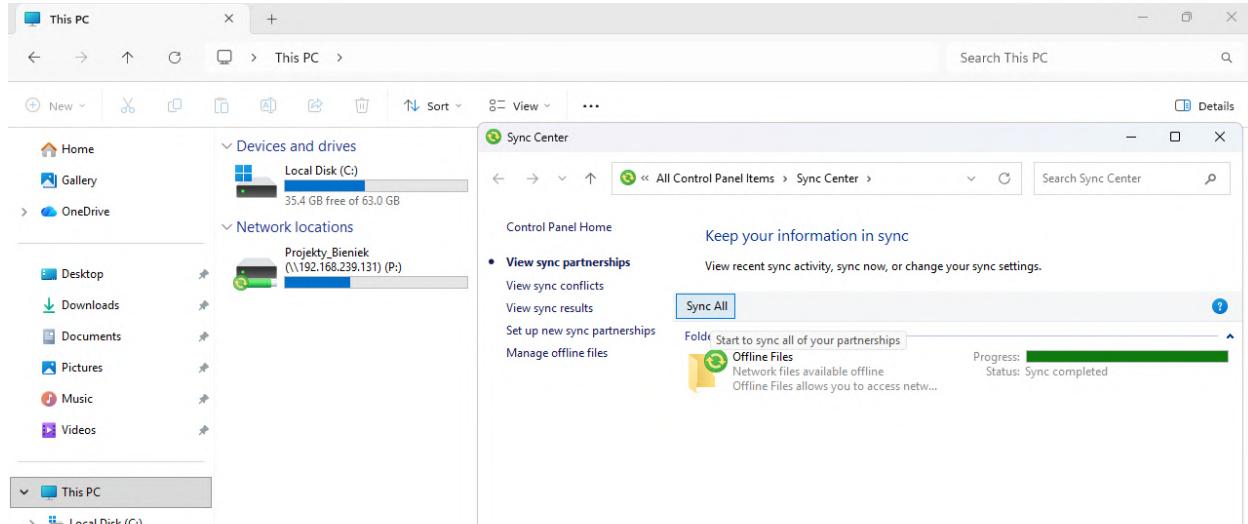
Zrzut ekranu 99 Podłączanie dysku sieciowego.

Na koniec włączę dla wybranego folderu możliwość korzystania z mechanizmu „plików trybu offline” wybierając stosowną opcję z menu kontekstowego.



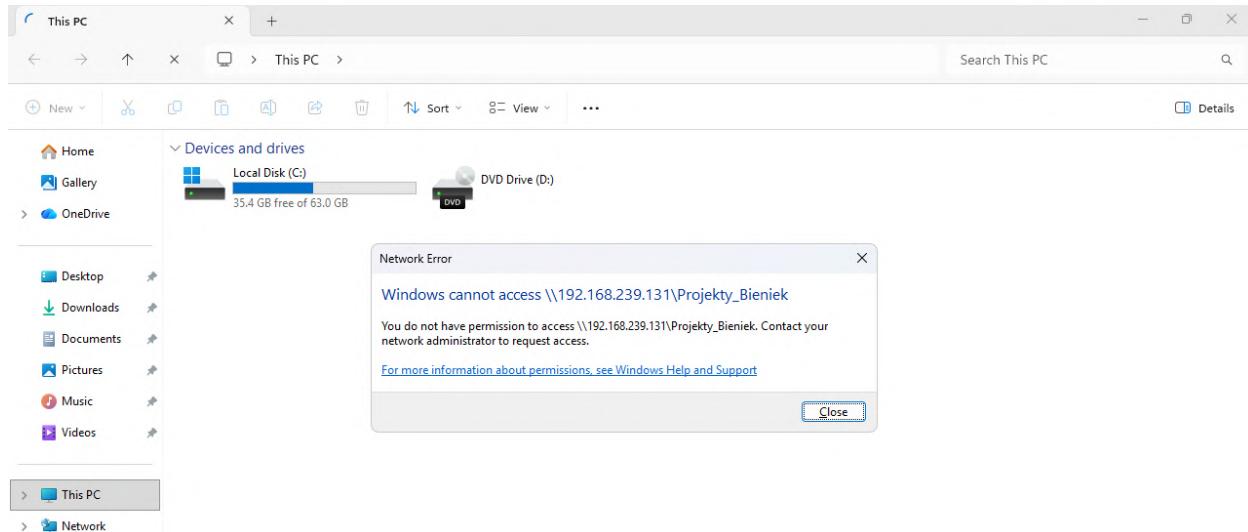
Zrzut ekranu 100 Aktywacja opcji plików trybu offline.

Zmiany zostaną zasygnalizowane pojawieniem się na katalogu (dysku sieciowym) ikonki synchronizacji. Z poziomu centrum synchronizacji w panelu sterowania można ręcznie wymusić synchronizację i rozwiązać ewentualne konflikty.



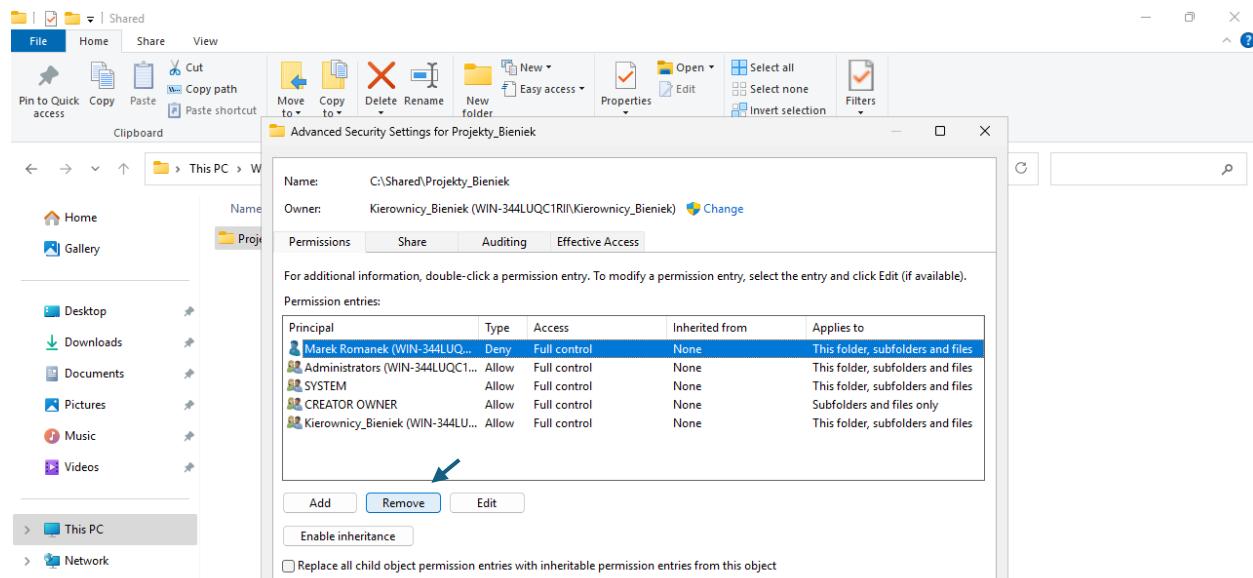
Zrzut ekranu 101 Centrum synchronizacji w panelu sterowania.

Sprawdźmy również, czy pan Marek Romanek należący do grupy Kierownicy (któremu zablokowaliśmy dostęp do folderu) rzeczywiście nie ma do niego dostępu. Logując się na jego konto możemy wpisać w pasku adresu lokalizację sieciową katalogu.



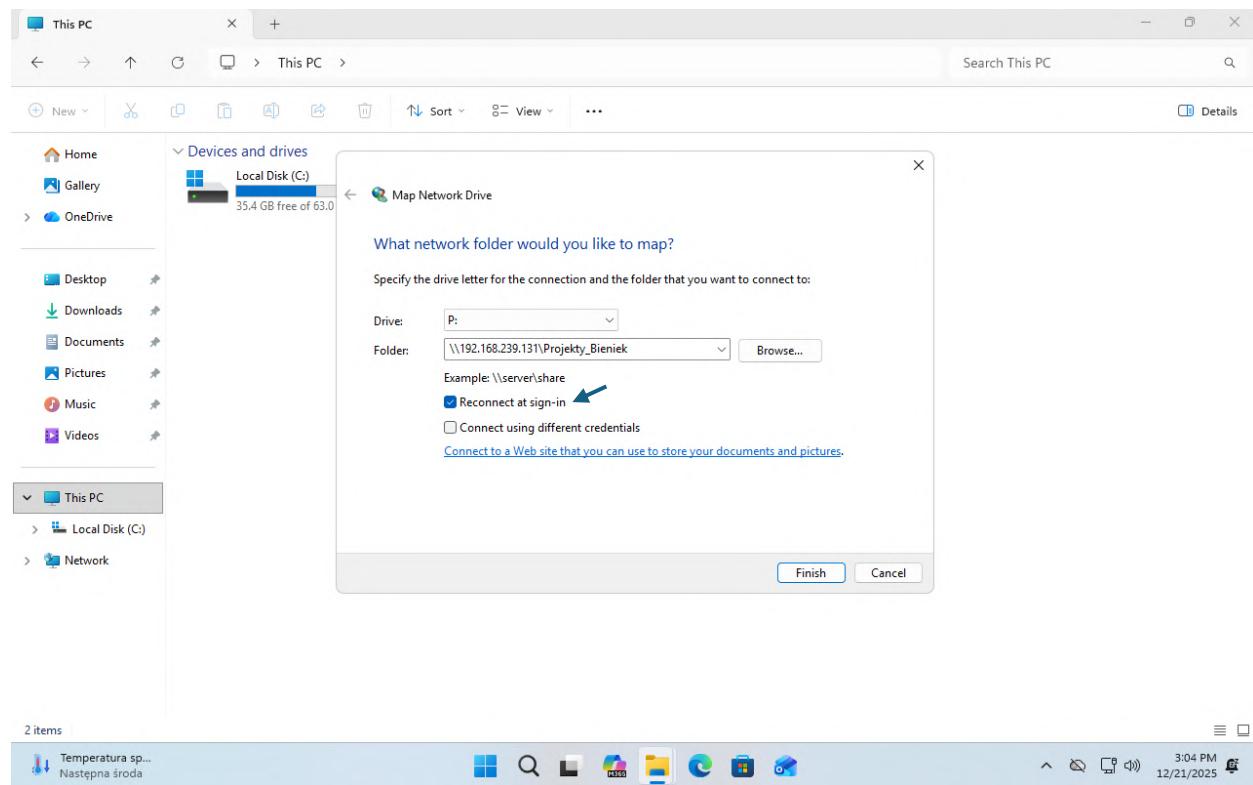
Zrzut ekranu 102 Brak możliwości uzyskania dostępu do folderu Projekty przez wskazanego użytkownika.

Zgodnie z przewidywaniami, dostęp do folderu jest niemożliwy. Gdyby jednak nastąpiła konieczność przywrócenia go panu Romankowi, w pierwszej kolejności trzeba by było usunąć wpis blokujący z *listy ACL* dla folderu *Projekty*.



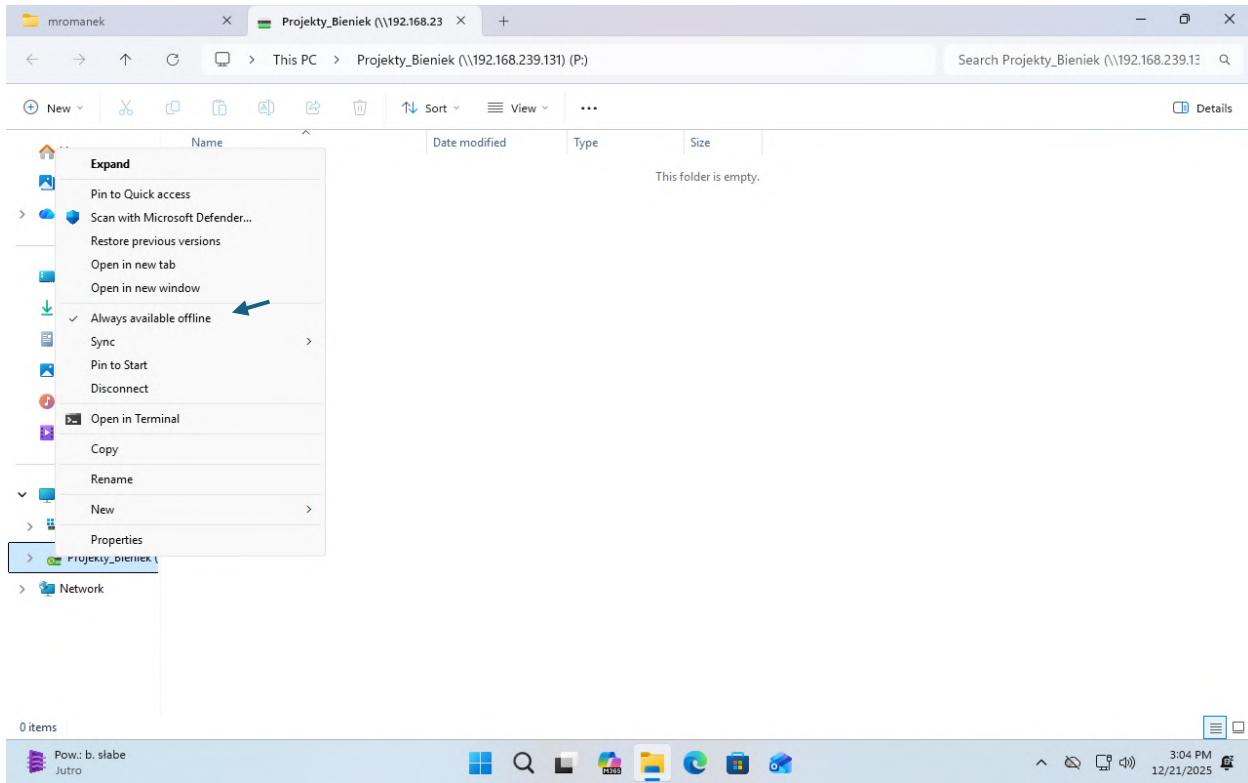
Zrzut ekranu 103 Usunięcie użytkownika z odebranymi uprawnieniami dostępu do folderu z listy ACL.

Po odblokowaniu dostępu, warto byłoby podłączyć dysk sieciowy, opcjonalnie zaznaczając opcję automatycznego łączenia w momencie logowania.



Zrzut ekranu 104 Podłączanie dysku sieciowego z opcją automatycznego nawiązywania połączenia przy logowaniu.

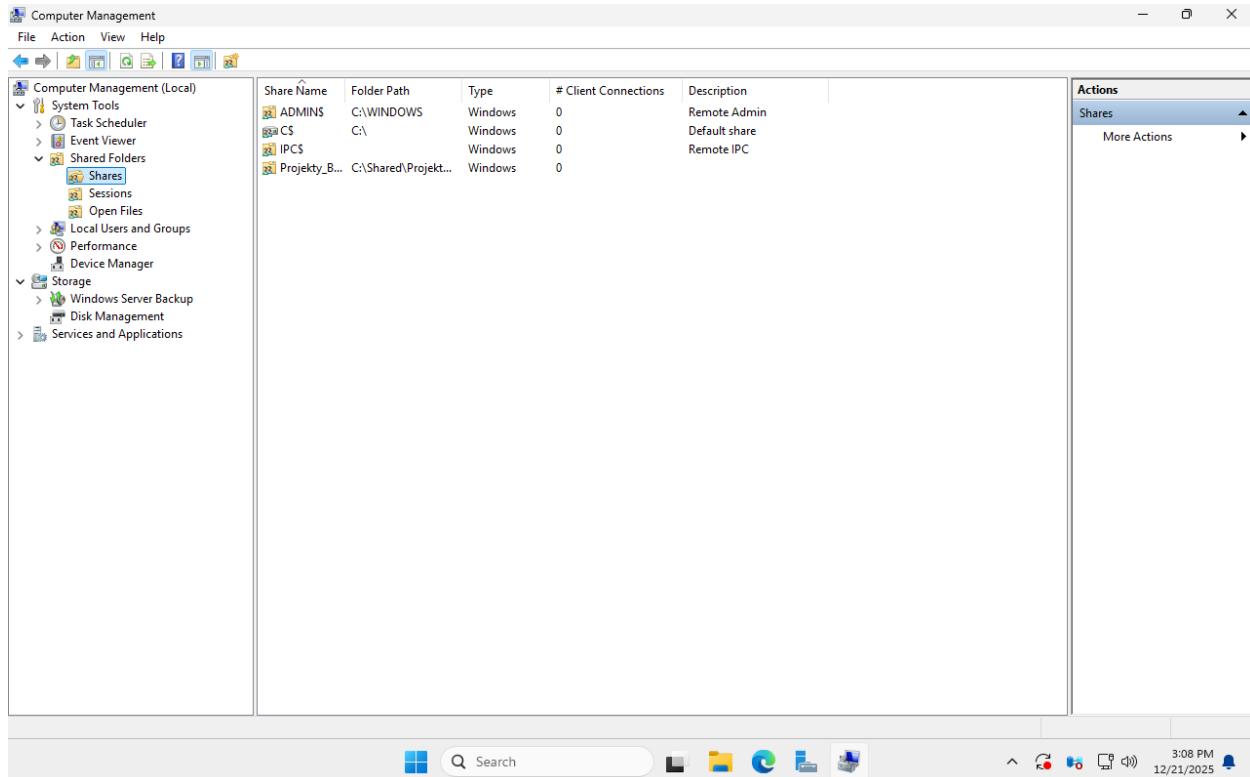
Aby użytkownik mógł korzystać z plików nawet w trakcie awarii serwera lub sieci, konieczne byłoby włączenie usługi *plików trybu offline* w panelu sterowania, a następnie aktywacja tej opcji dla wybranego folderu.



Zrzut ekranu 105 Aktywacja plików trybu offline dla wybranego folderu.

Zadanie 3. Ukryte zasoby sieciowe.

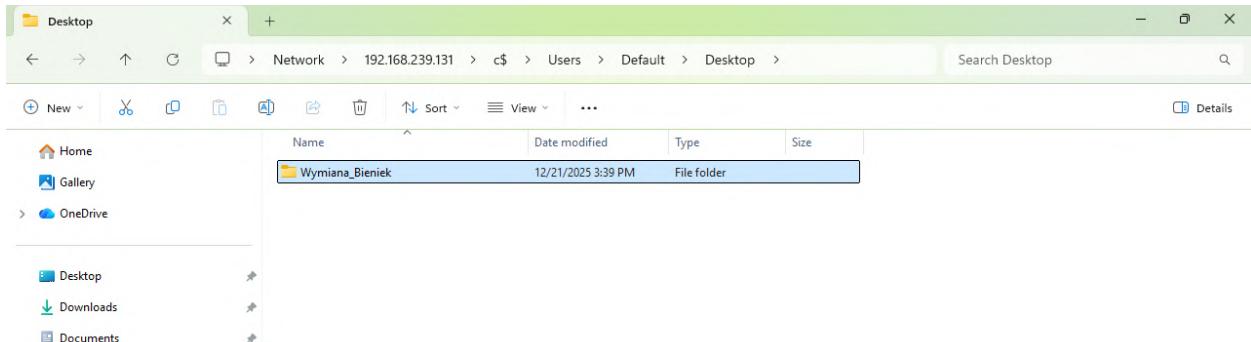
W systemie Windows domyślnie tworzone są ukryte zasoby sieciowe, które umożliwiają między innymi na bezpośredni dostęp do dysków. Mechanizm ten można wykorzystać, na przykład, aby zdalnie umieścić plik na pulpitach nowotworzonych użytkowników.



Zrzut ekranu 106 Wyświetlenie wszystkich udostępnianych udziałów sieciowych.

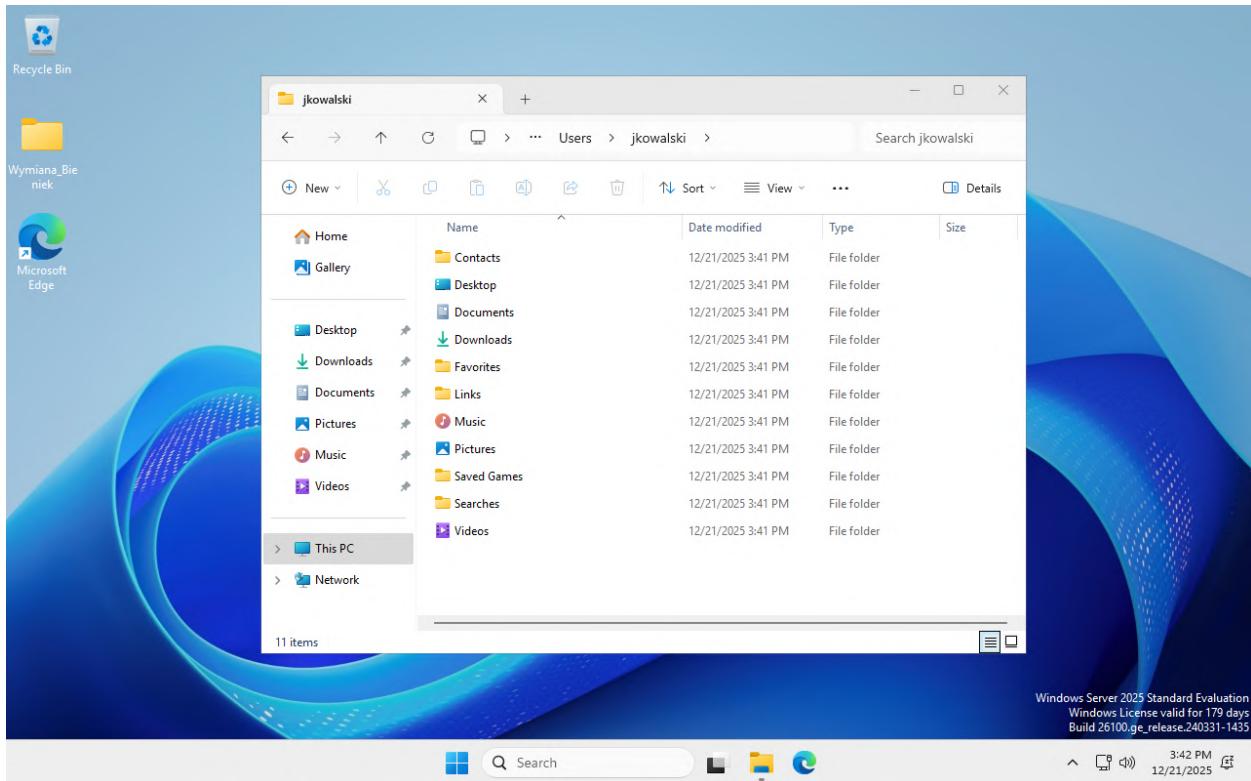
W przypadku dystrybucji Windows Server, zasoby te udostępniane są domyślnie i nie wymagają dodatkowej konfiguracji. Dzięki temu możemy podłączyć się do serwera z dowolnego komputera w sieci, zalogować na konto z odpowiednimi uprawnieniami i modyfikować zawartość dysku.

Aby nowotworzeni użytkownicy mieli na pulpicie katalog o nazwie Wymiana, należy dodać go do folderu użytkownika domyślnego – szablonu wykorzystywanego do tworzenia katalogów domowych użytkowników.

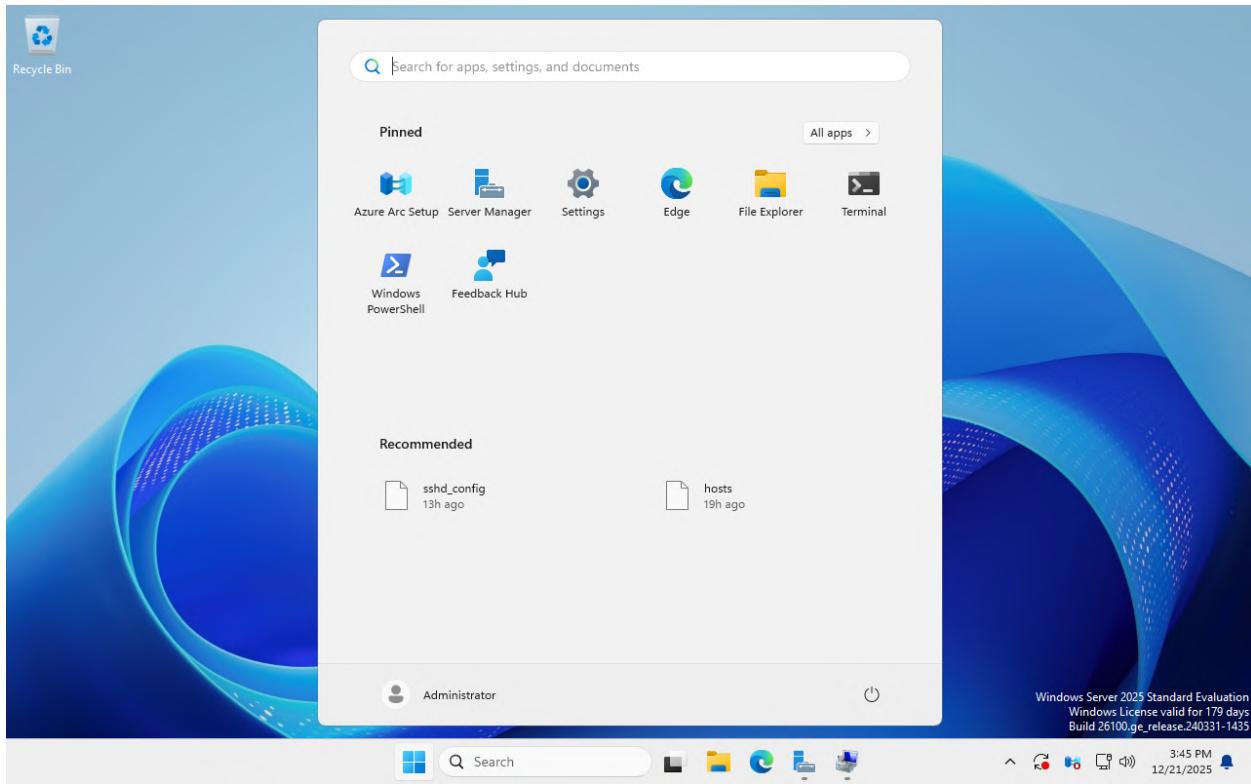


Zrzut ekranu 107 Utworzenie katalogu w folderze na pulpicie użytkownika domyślnego (szablonu dla nowych kont).

Możemy teraz zweryfikować poprawność działania mechanizmu.



Zrzut ekranu 108 Folder Wymiana znajdujący się na pulpicie nowoutworzonego użytkownika jkowalski.



Zrzut ekranu 109 Brak folderu na pulpicie istniejącego użytkownika (Administratora).

Zadanie 4. Listy ACL w systemach Linux.

Mechanizm *list ACL* znany z systemu Windows nie jest domyślnie dostępny w systemach Linux. Aby z nich skorzystać konieczne jest uprzednie doinstalowanie pakietu *acl*, a następnie jego aktywacja we właściwościach dysku (pliku *fstab*).

```
root@debian:~# apt update && apt install acl
Hit:1 http://deb.debian.org/debian bookworm InRelease
Get:2 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:4 http://security.debian.org/debian-security bookworm-security/main Sources [195 kB]
Get:5 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [290 kB]
Fetched 588 kB in 0s (1,259 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  acl
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 61.2 kB of archives.
After this operation, 215 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 acl amd64 2.3.1-3 [61.2 kB]
Fetched 61.2 kB in 0s (734 kB/s)
Selecting previously unselected package acl.
(Reading database ... 38437 files and directories currently installed.)
Preparing to unpack .../archives/acl_2.3.1-3_amd64.deb ...
Unpacking acl (2.3.1-3) ...
Setting up acl (2.3.1-3) ...
Processing triggers for man-db (2.11.2-2) ...
root@debian:~# -
```

Zrzut ekranu 110 Instalacja pakietu *acl*.

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point> <type> <options>      <dump> <pass>
# / was on /dev/sda1 during installation
UUID=c3958d6a-ba05-4ec4-9a83-eb402c885ef6 /          ext4    errors=remount-ro,acl 0           1
# swap was on /dev/sda5 during installation
UUID=0e73fb18-aid2-412e-b71a-5eab9068abfd none        swap    sw            0           0
/dev/sr0      /media/cdrom0  udf,iso9660 user,noauto     0           0
~
~
~
~
~
```

Zrzut ekranu 111 Włączenie mechanizmu *acl* dla dysku systemowego przez dodanie go do listy opcji.

Po wprowadzeniu zmian konieczny jest restart systemu, aby mechanizm *acl* został aktywowany.

Aby przetestować jego działanie, możemy utworzyć folder współdzielony, do którego pełny dostęp będzie miało jednocześnie tylko kilka wybranych grup. Zadanie rozpoczniemy od utworzenia trzech testowych grup i nowego folderu, do którego dostęp będzie miał jedynie właściciel.

```
root@debian:~# groupadd Produkcja
root@debian:~# groupadd Kadry
root@debian:~# groupadd IT
root@debian:~# mkdir /home/dokumenty_Bieniek
root@debian:~# ls -la /home/dokumenty_Bieniek/
total 8
drwxr-xr-x 2 root root 4096 Dec 21 17:24 .
drwxr-xr-x 4 root root 4096 Dec 21 17:24 ..
root@debian:~# chmod 700 /home/dokumenty_Bieniek/
root@debian:~# ls -la /home/dokumenty_Bieniek/
total 8
drwx----- 2 root root 4096 Dec 21 17:24 .
drwxr-xr-x 4 root root 4096 Dec 21 17:24 ..
root@debian:~# getfacl /home/dokumenty_Bieniek/
getfacl: Removing leading '/' from absolute path names
# file: home/dokumenty_Bieniek/
# owner: root
# group: root
user::rwx
group::---
other::---
```

Zrzut ekranu 112 Utworzenie testowych grup i folderu współdzielonego.

Możemy następnie skorzystać z polecenia *setfacl -m*, aby dodać do listy nowe pozycje, zapisane w formacie *formacie <typ>:<nazwa>:<maska>*. Na pierwszej pozycji podstawi się *u* dla zwykłych użytkowników lub *g* dla grup, a ostatnia pozycja stanowi maskę nadającą odpowiednie uprawnienia, na przykład *r-x* dla odczytu i wykonania lub *---* oznaczający całkowity brak uprawnień.

Aby nadać pełne prawa dostępu do folderu dla grup *Produkcja*, *Kadry* oraz *IT*, a także zdefiniować domyślne prawa nadawane nowym plikom, wykonamy poniższe polecenia.

```
root@debian:~# setfacl -m g:Produkcja:rwx,g:Kadry:rwx,g:IT:rwx /home/dokumenty_Bieniek/
root@debian:~# setfacl -d -m g:Produkcja:rwx,g:Kadry:rwx,g:IT:rwx /home/dokumenty_Bieniek/
root@debian:~# getfacl /home/dokumenty_Bieniek/
getfacl: Removing leading '/' from absolute path names
# file: home/dokumenty_Bieniek/
# owner: root
# group: root
user::rwx
group::---
group:Produkcja:rwx
group:Kadry:rwx
group:IT:rwx
mask::rwx
other::---
default:user::rwx
default:group:---
default:group:Produkcja:rwx
default:group:Kadry:rwx
default:group:IT:rwx
default:mask::rwx
default:other:---
```

Zrzut ekranu 113 Nadanie praw dostępu do katalogu współdzielonego.

Aby przetestować mechanizm, dodam w systemie nowego użytkownika i przydzielę go do jednej z wymienionych grup, a następnie utworzę w folderze współdzielonym kilka podkatalogów i plików, aby odczytać automatycznie nadane uprawnienia.

```
root@debian:~# adduser --allow-bad-names marek.romanek
Allowing use of questionable username.
Adding user `marek.romanek' ...
Adding new group `marek.romanek' (1004) ...
Adding new user `marek.romanek' (1004) with group `marek.romanek (1004)' ...
adduser: The home directory `/home/marek.romanek' already exists. Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for marek.romanek
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
Adding new user `marek.romanek' to supplemental / extra groups `users' ...
Adding user `marek.romanek' to group `users' ...
root@debian:~# usermod -a -G Kadry marek.romanek
root@debian:~# cat /etc/group | grep -i "kadry"
Kadry:x:1002:marek.romanek
root@debian:~# _
```

Zrzut ekranu 114 Utworzenie użytkownika testowego i przypisanie go do grupy wymienionej na liście ACL.

```
marek.romanek@debian:~$ cd /home/dokumenty_Bieniek/
marek.romanek@debian:/home/dokumenty_Bieniek$ ls -la
total 12
drwxrwx---+ 2 root root 4096 Dec 21 17:44 .
drwxr-xr-x  5 root root 4096 Dec 21 17:36 ..
marek.romanek@debian:/home/dokumenty_Bieniek$ touch a.txt
marek.romanek@debian:/home/dokumenty_Bieniek$ mkdir b
marek.romanek@debian:/home/dokumenty_Bieniek$ touch b/c.txt
marek.romanek@debian:/home/dokumenty_Bieniek$ mkdir b/d
marek.romanek@debian:/home/dokumenty_Bieniek$ touch b/d/e.txt
marek.romanek@debian:/home/dokumenty_Bieniek$ getfacl a.txt
# file: a.txt
# owner: marek.romanek
# group: marek.romanek
user::rw-
group::---
group:Produkcja:rw-
group:Kadry:rw-
group:IT:rw-
mask::rw-
other::---

marek.romanek@debian:/home/dokumenty_Bieniek$ getfacl b
# file: b
# owner: marek.romanek
# group: marek.romanek
user::rwx
group::---
group:Produkcja:rw-
group:Kadry:rw-
group:IT:rw-
mask::rw-
other::---
default:user::rwx
default:group::---
default:group:Produkcja:rw-
default:group:Kadry:rw-
default:group:IT:rw-
default:mask::rw-
default:other::---
```

```
marek.romanek@debian:/home/dokumenty_Bieniek$ getfacl b/d
# file: b/d
# owner: marek.romanek
# group: marek.romanek
user::rwx
group::---
group:Produkcja:rw-
group:Kadry:rw-
group:IT:rw-
mask::rw-
other::---
default:user::rwx
default:group::---
default:group:Produkcja:rw-
default:group:Kadry:rw-
default:group:IT:rw-
default:mask::rw-
default:other::---

marek.romanek@debian:/home/dokumenty_Bieniek$ getfacl b/d/e.txt
# file: b/d/e.txt
# owner: marek.romanek
# group: marek.romanek
user::rw-
group::---
group:Produkcja:rw-
group:Kadry:rw-
group:IT:rw-
mask::rw-
other::---

marek.romanek@debian:/home/dokumenty_Bieniek$ _
```

Zrzut ekranu 115 Utworzenie plików testowych i sprawdzenie uprawnień nadawanych automatycznie nowym obiektom.

Jak widać, prawa odczytu i zapisu do utworzonych plików, wynikające z domyślnych uprawnień, przysługują wyłącznie wskazanym grupom. Użytkownik testowy, będący właścicielem i należący do jednej z tych grup, otrzymał takie same uprawnienia.

W przypadku folderów sytuacja jest analogiczna. Na liście pojawiają się także odziedziczone wpisy domyślne, dzięki czemu uprawnienia propagują się w dół drzewa plików. Warto zwrócić uwagę, że prawo do wykonywania zostało nadane wyłącznie właścicielowi, co oznacza, że tylko on ma dostęp do utworzonego folderu.