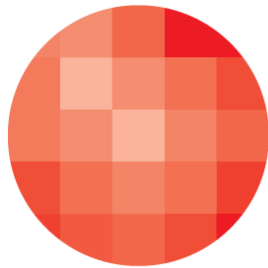


WARSZAWSKA WYŻSZA SZKOŁA INFORMATYKI
SYSTEMY OPERACYJNE



WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

SPRAWOZDANIE NR 5 TEMAT:

Instalacja i konfiguracja usługi FTP w
systemie Windows Server.

Wykonał
Wojciech Wiącek

1 Podstawy Teoretyczne

1.1 Protokoły transferu plików:

1.1.1 FTP

Protokół FTP (File Transfer Protocol) to protokół komunikacyjny pozwalający na przesyłanie plików z serwera do klienta lub z klienta do serwera. Jest to jeden z podstawowych protokołów sieciowych i jest często używany przez użytkowników internetowych do przesyłania plików w Internecie. Protokół FTP jest często używany przez administratorów sieci do bezpiecznego przesyłania plików między serwerem a klientem.

1.1.2 Zalety

- Łatwość użycia – FTP jest łatwy w użyciu, zwłaszcza dla użytkowników z małą wiedzą techniczną.
- Przenośność – FTP można używać na różnych platformach, takich jak Windows, Linux i Mac.
- Bezpieczeństwo – FTP używa protokołu TLS do ochrony twoich danych przed nieautoryzowanym dostępem.
- Prędkość – FTP może przesyłać duże pliki szybciej niż inne protokoły przesyłania plików.

1.1.3 Wady

- Niska wydajność – FTP ma niską wydajność w porównaniu do innych protokołów, takich jak SFTP i SCP.
- Brak bezpieczeństwa – FTP nie zapewnia silnego szyfrowania, co oznacza, że wszystkie dane przesyłane przez protokół są narażone na nieautoryzowane dostępy.
- Niska elastyczność – FTP jest stosunkowo trudny do skonfigurowania w porównaniu do innych protokołów.
- Brak automatyzacji – FTP nie ma wbudowanych opcji automatyzacji, takich jak monitorowanie, harmonogramowanie i tworzenie kopii zapasowych.

1.1.4 TFTP

TFTP (Trivial File Transfer Protocol) to protokół służący do przesyłania plików w sieciach komputerowych. Jest to łatwy w użyciu protokół, który jest stosowany w sieciach opartych na systemach UNIX, a także sieciach Ethernet. Protokół TFTP jest zazwyczaj stosowany do przesyłania plików zarządzania siecią, takich jak pliki konfiguracji, firmware, oprogramowanie, itp. Protokół TFTP jest bardzo prosty,

ale jest też bardzo ograniczony. Nie posiada wielu funkcji, takich jak kontrola poprawności, kompresja czy ochrona hasłem.

1.1.5 Zalety

- Prosty w użyciu, wymaga minimalnej konfiguracji;
- Szybki i lekki, idealny do transferu plików małych rozmiarów;
- Nie wymaga połączenia odwzajemnionego;
- Wsteczna kompatybilność z systemami DOS, Windows i Unix.

1.1.6 wady

- Niski limit transferu, maksymalne ograniczenie wynosi 512KB;
- Brak mechanizmów autoryzacji i uwierzytelniania;
- Brak szyfrowania, dane mogą być łatwo przechwytywane;
- Ograniczony zakres komend.

1.1.7 SFTP

SFTP (Secure File Transfer Protocol) to protokół bezpiecznego transferu plików, który jest zaszyfrowanym rozszerzeniem FTP. Oferuje wszystkie funkcje protokołu FTP, ale z dodatkową warstwą bezpieczeństwa, która ma na celu ochronę danych przed nieautoryzowanym dostępem. Protokół SFTP wykorzystuje SSH do wymiany komend i danych między klientem a serwerem.

1.1.8 Zalety

- Bezpieczeństwo: SFTP używa zaszyfrowanych połączeń, aby chronić dane przed nieupoważnionym dostępem.
- Użyteczność: SFTP może być wykorzystywany zarówno do przesyłania plików, jak i do zarządzania nimi. Może również umożliwiać edycję plików na miejscu.
- Integracja: SFTP może być łatwo zintegrowany z systemami operacyjnymi, takimi jak Windows, Linux i Mac OS, co pozwala użytkownikom na dostęp do plików ze wszelkich systemów.

1.1.9 Wady

- Ograniczony zasięg: SFTP ma ograniczony zasięg, co oznacza, że nie może zapewnić bezpiecznego przesyłania plików poza siecią lokalną.
- Ograniczony protokół: SFTP jest ograniczony do przesyłania plików i nie jest w stanie wykonywać innych zadań sieciowych.
- Utrudnienie w użyciu: SFTP może być trudny w użyciu dla użytkowników, którzy nie są dobrze zaznajomieni z technologią sieciową.

1.2 Tryby pracy serwera FTP

1.2.1 Tryb aktywny (Active Mode)

w tym trybie klient wysyła żądanie kontroli portu do serwera FTP, a serwer przesyła dane do klienta przez port, który został wcześniej ustalony.

1.2.2 Tryb pasywny (Passive Mode)

w tym trybie serwer nie wysyła żadnych żądań do klienta i przesyła dane do klienta za pośrednictwem portu, który został wcześniej ustalony. Klient musi wysłać żądanie do serwera, aby go połączyć z portem.

1.3 Rola IIS i jej możliwości

Internet Information Services (IIS) jest usługą serwera internetowego oferowaną przez Microsoft. Jest ona wykorzystywana do hostowania stron internetowych i aplikacji internetowych. IIS oferuje wiele możliwości, takich jak konfiguracja kont użytkowników, kontrola dostępu, zarządzanie plikami i zasobami, tworzenie i zarządzanie wirtualnymi folderami, tworzenie witryn internetowych i wiele innych. IIS jest łatwy w użyciu i posiada wbudowane narzędzia, które są przydatne do tworzenia i zarządzania witrynami i aplikacjami internetowymi. Ponadto IIS jest wysoce bezpiecznym systemem, który zapewnia wszystkim użytkownikom bezpieczeństwo i ochronę ich danych i kodu źródłowego.

1.4 System plików NTFS i prawa dostępu do zasobów w tym systemie plików;

NTFS (NT File System) to system plików, który jest używany przez system operacyjny Windows

do przechowywania i zarządzania plikami na dysku twardym. NTFS zapewnia szerokie

możliwości zarządzania plikami, takie jak:

- Możliwość tworzenia i usuwania plików i katalogów
- Możliwość zmiany nazw plików i katalogów
- Możliwość przenoszenia i kopiowania plików i katalogów
- Możliwość zabezpieczania plików hasłem

NTFS również umożliwia ustawianie praw dostępu do zasobów w systemie plików. Prawa

dostępu określają, które użytkownikom lub grupom użytkowników są udostępniane

określone uprawnienia do plików i katalogów. Uprawnienia mogą obejmować m.in.:

- Odczyt (Read) - uprawnienie do odczytu zawartości pliku lub katalogu
- Zapis (Write) - uprawnienie do zapisywania zmian w pliku lub katalogu
- Usuwanie (Delete) - uprawnienie do usuwania pliku lub katalogu
- Tworzenie (Create) - uprawnienie do tworzenia plików lub katalogów w danym katalogu

Można ustawić prawa dostępu do zasobów dla pojedynczych użytkowników lub grup

użytkowników, co pozwala na lepsze zarządzanie dostępem do plików i katalogów w

systemie. Ustawienie odpowiednich praw dostępu jest ważne w przypadku, gdy chce się

chronić poufne lub ważne pliki przed nieautoryzowanym dostępem.

2 Przebieg czynności do realizacji zadania

The screenshot shows the Windows Server 2016 Server Manager interface. A dialog box titled 'Zmiany nazwy komputera/domeny' (Change computer name/domain) is open. It allows changing the computer name and its membership. The current name is 'multiserver'. The 'Członkostwo' (Membership) section shows 'Grupa robocza: WORKGROUP' (Workgroup: WORKGROUP) selected. The background shows the 'Menedżer serwera' (Server Manager) console with various system settings and a list of events.

Właściwości systemu

Zmiany nazwy komputera/domeny

Możesz zmienić nazwę i członkostwo tego komputera. Zmiany mogą wpłynąć na możliwość uzyskiwania dostępu do zasobów sieciowych.

Nazwa komputera:
multiserver

Pełna nazwa komputera:
multiserver

Więcej...

Członkostwo

☐ Domena:

☒ Grupa robocza:
WORKGROUP

OK Anuluj

System

WIN-9OH7N587J3P
WORKGROUP

Publiczne: Włączone
Włączone
Wyłączone
Wyłączone
Adres IPv4 przypisany przez protokół DHCP, Protokół IPv6 włączony

Microsoft Windows Server 2016 Standard
innotek GmbH VirtualBox

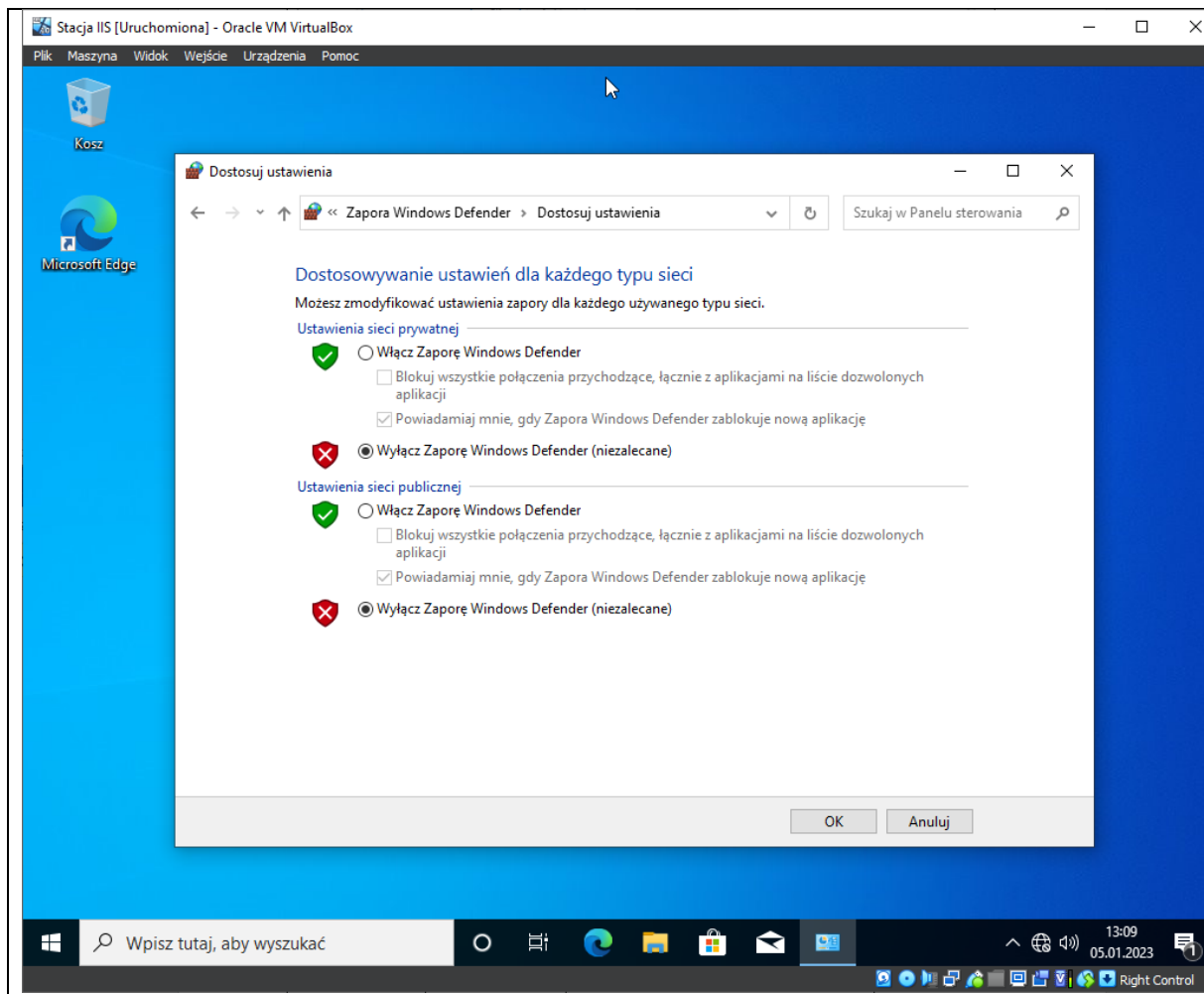
Procesory
Zainstalowana pamięć
Całkowite miejsce dyskowe

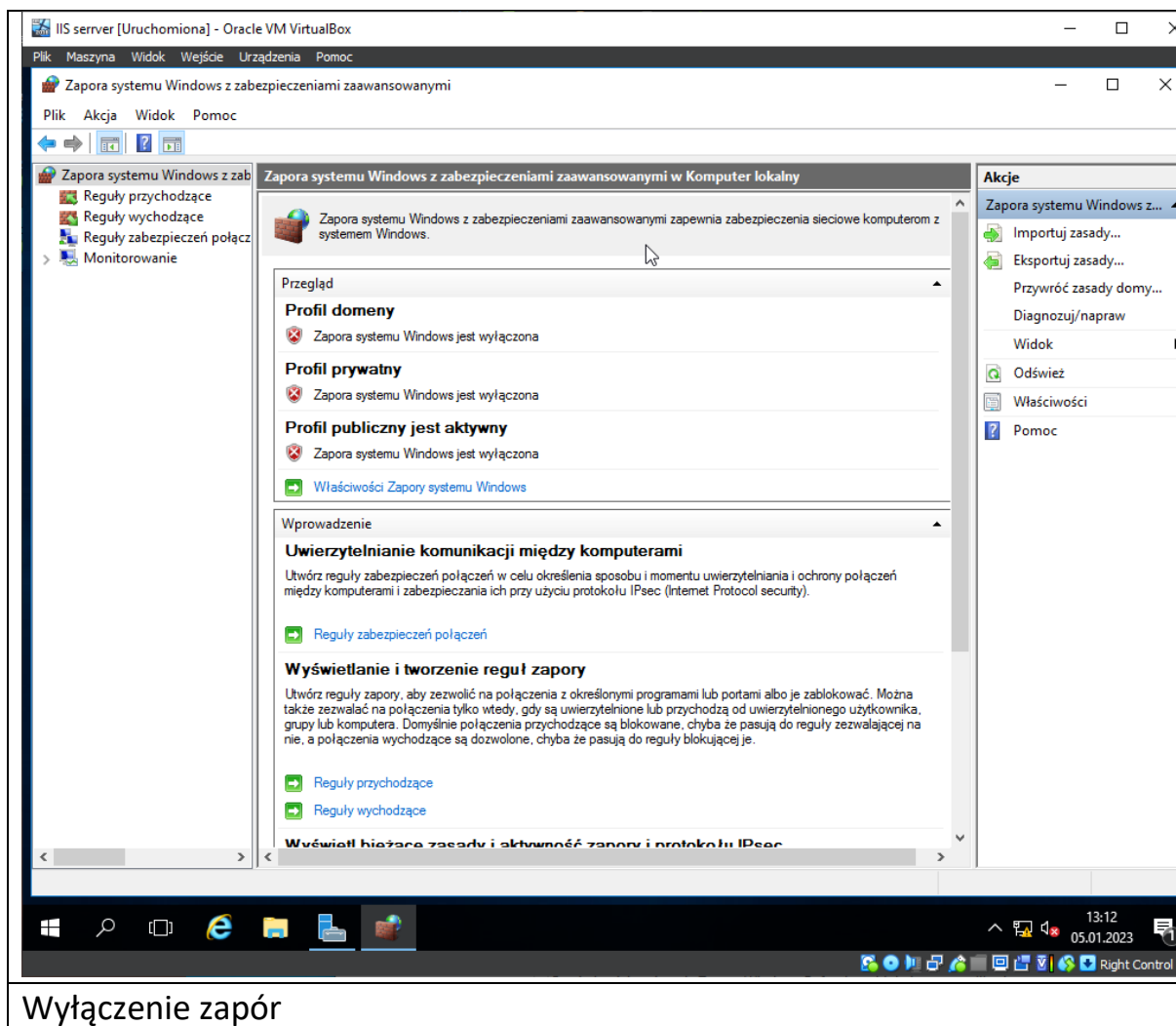
Wszystkie zdarzenia | Razem: 13

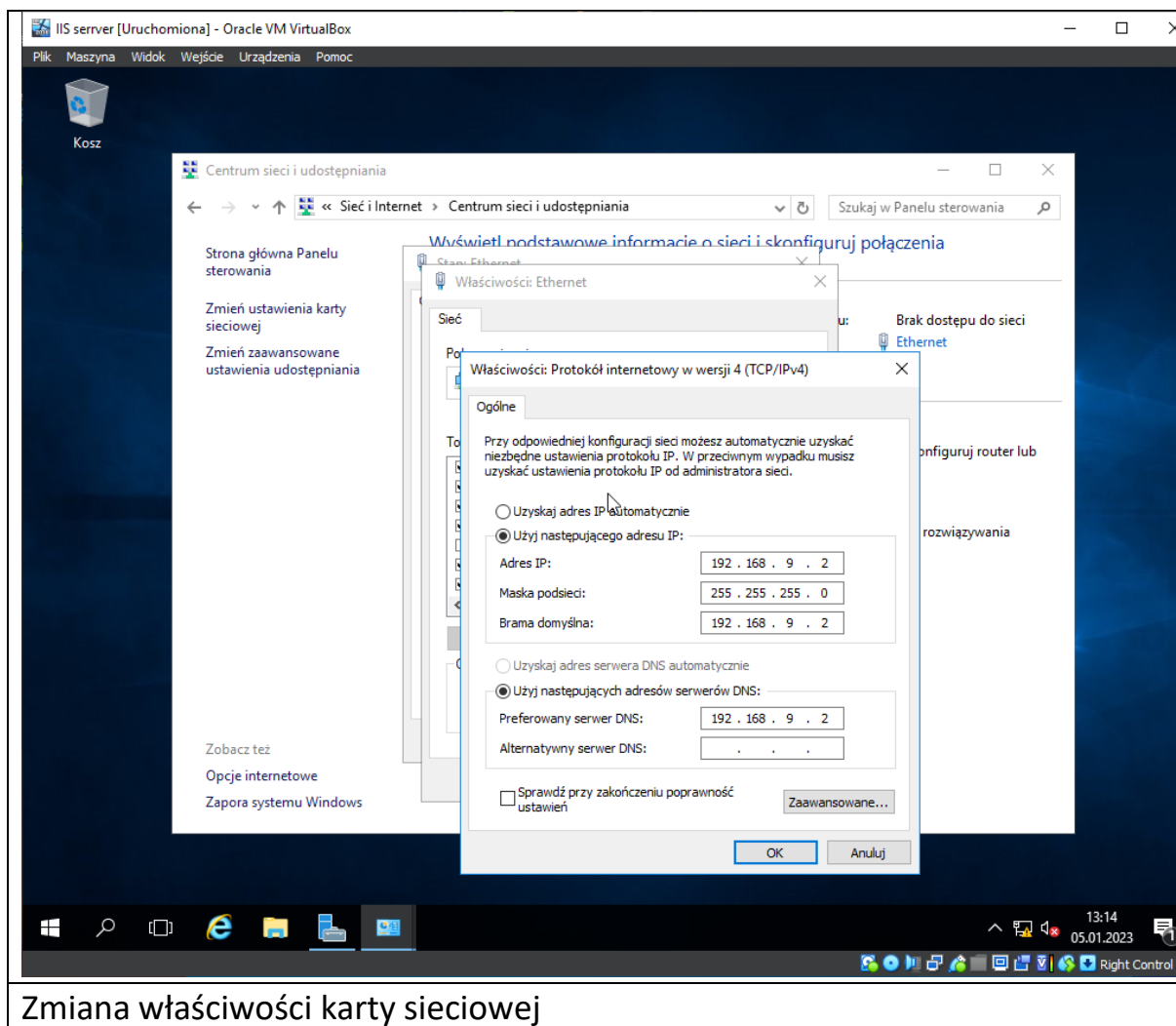
| Nazwa serwera | Identyfikator | Ważność | Źródło | Dziennik | Data i godzina |
|-----------------|---------------|-------------|--------------------------------|-----------|---------------------|
| WIN-9OH7N587J3P | 1076 | Ostrzeżenie | User32 | System | 05.01.2023 13:06:35 |
| WIN-9OH7N587J3P | 8198 | Błąd | Microsoft-Windows-Security-SPP | Aplikacja | 05.01.2023 13:06:35 |
| WIN-9OH7N587J3P | 134 | Ostrzeżenie | Microsoft-Windows-Time-Service | System | 05.01.2023 13:06:32 |

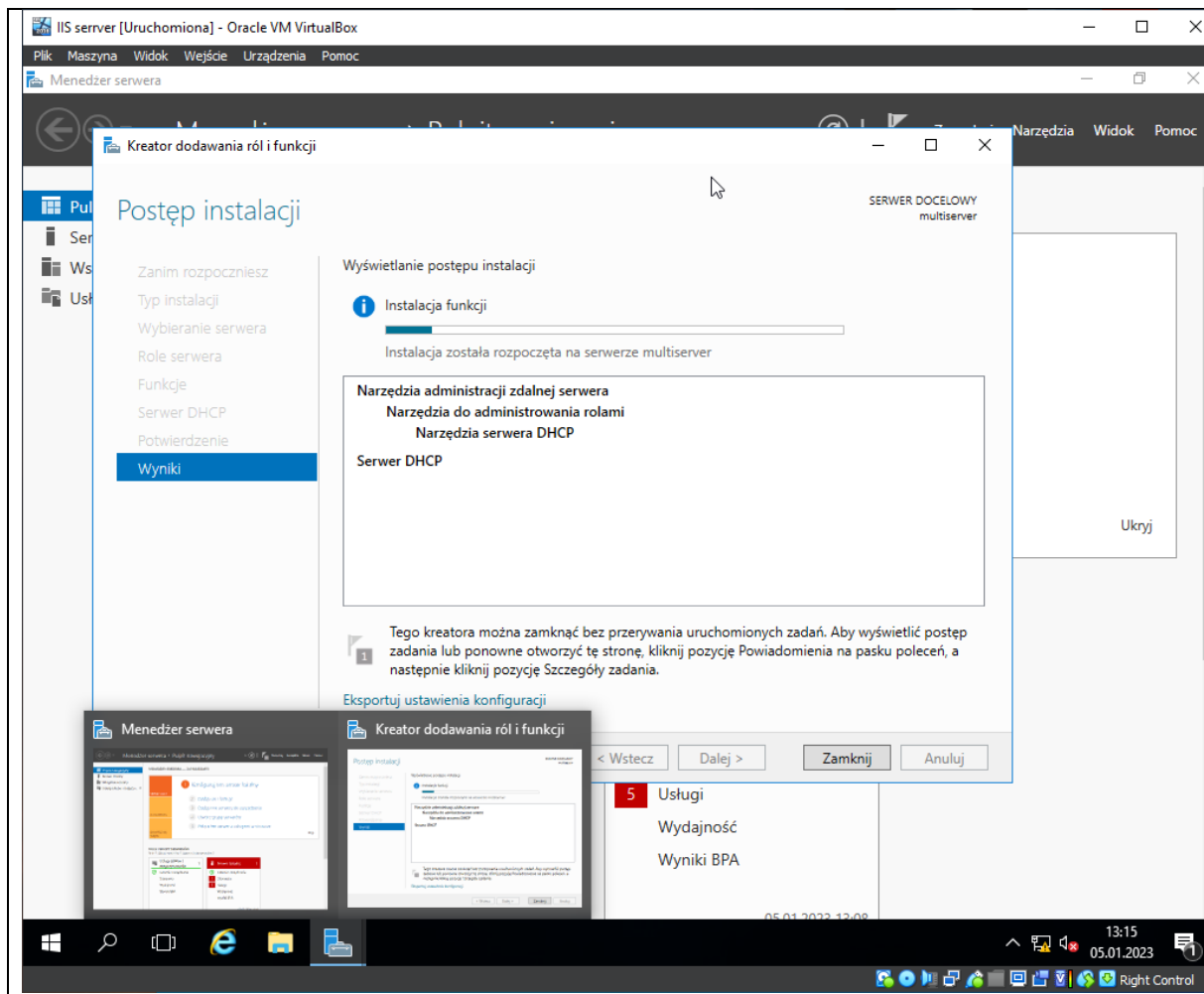
13:06
05.01.2023
Right Control

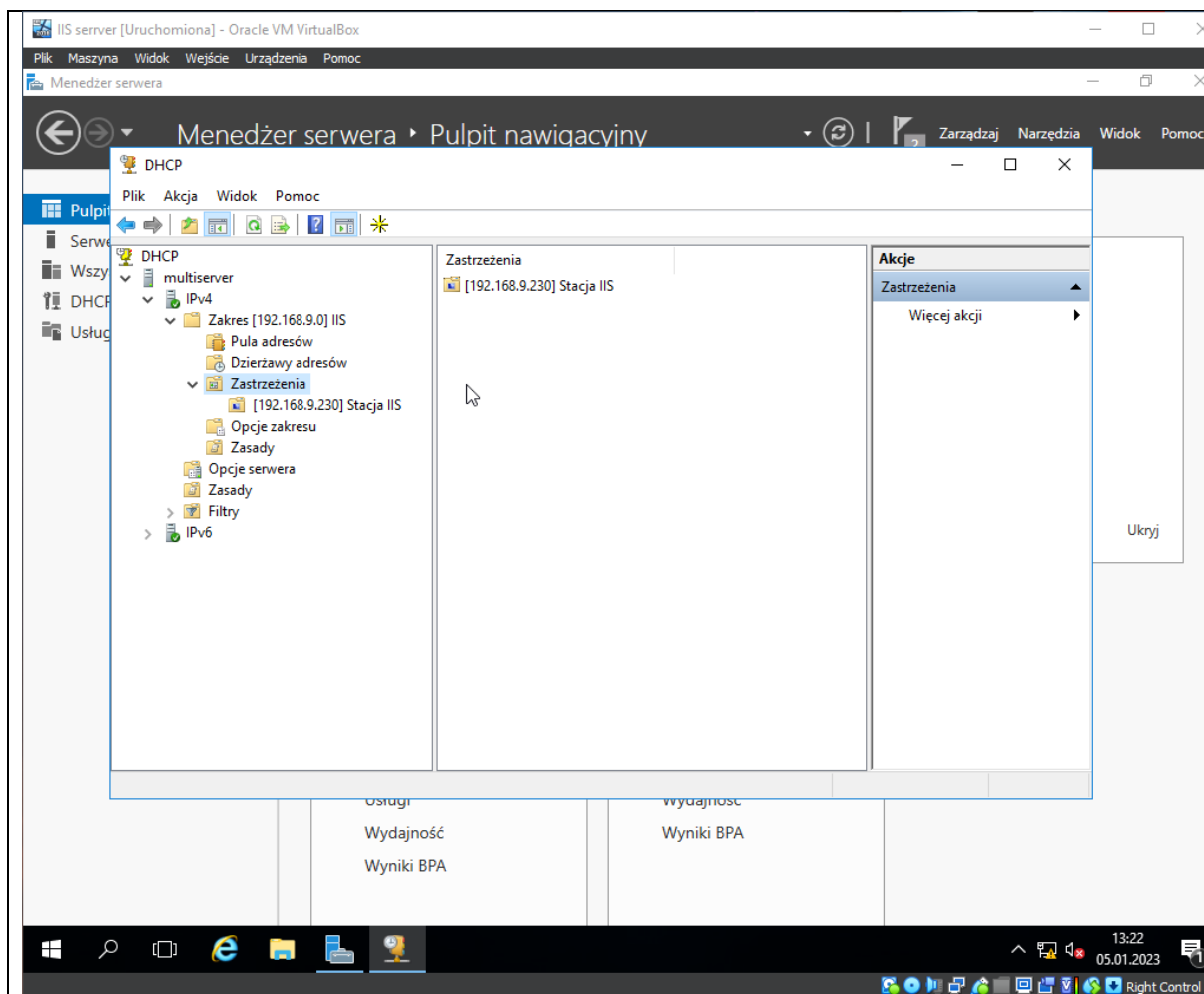
Zmiana nazw jednostek



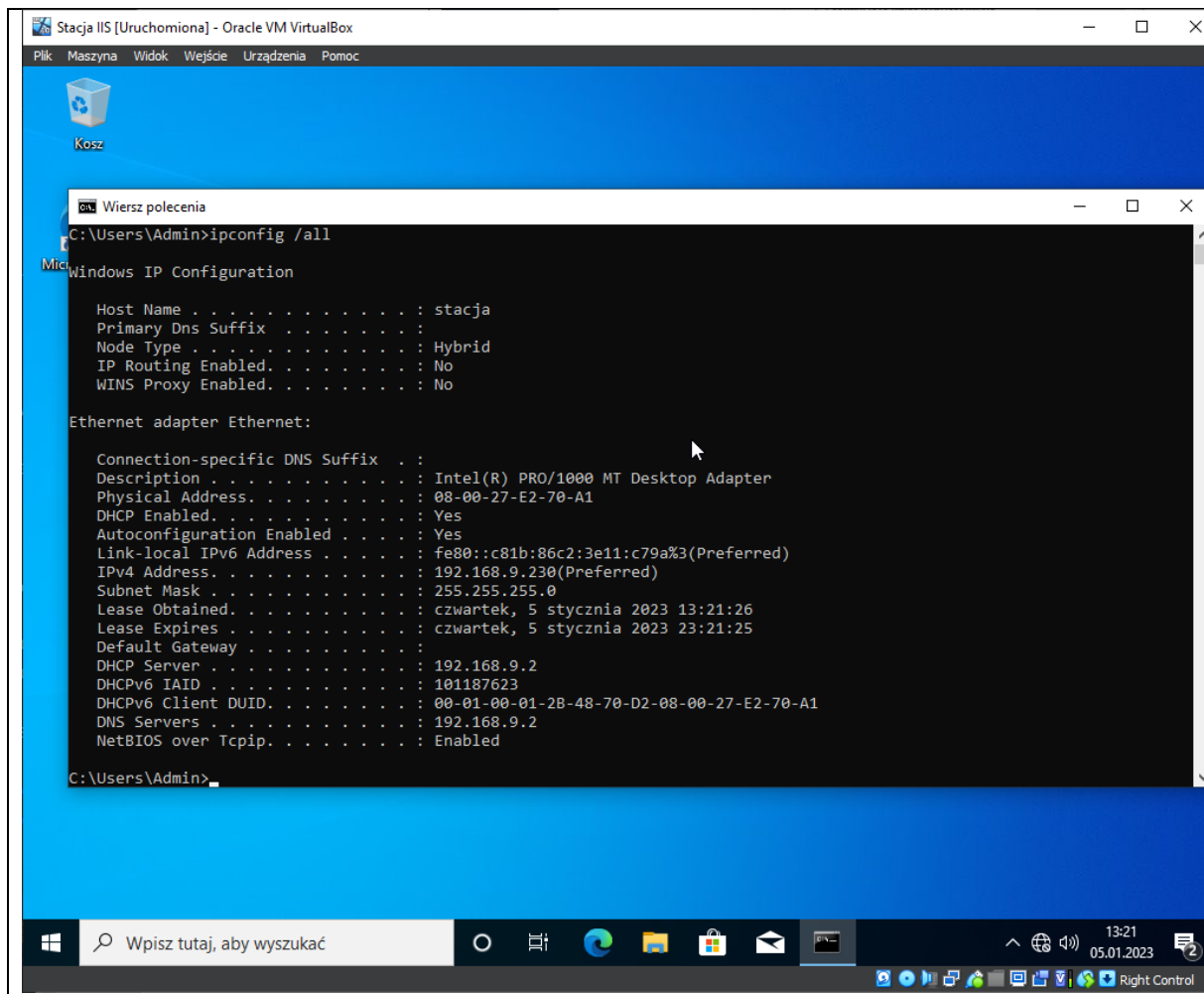


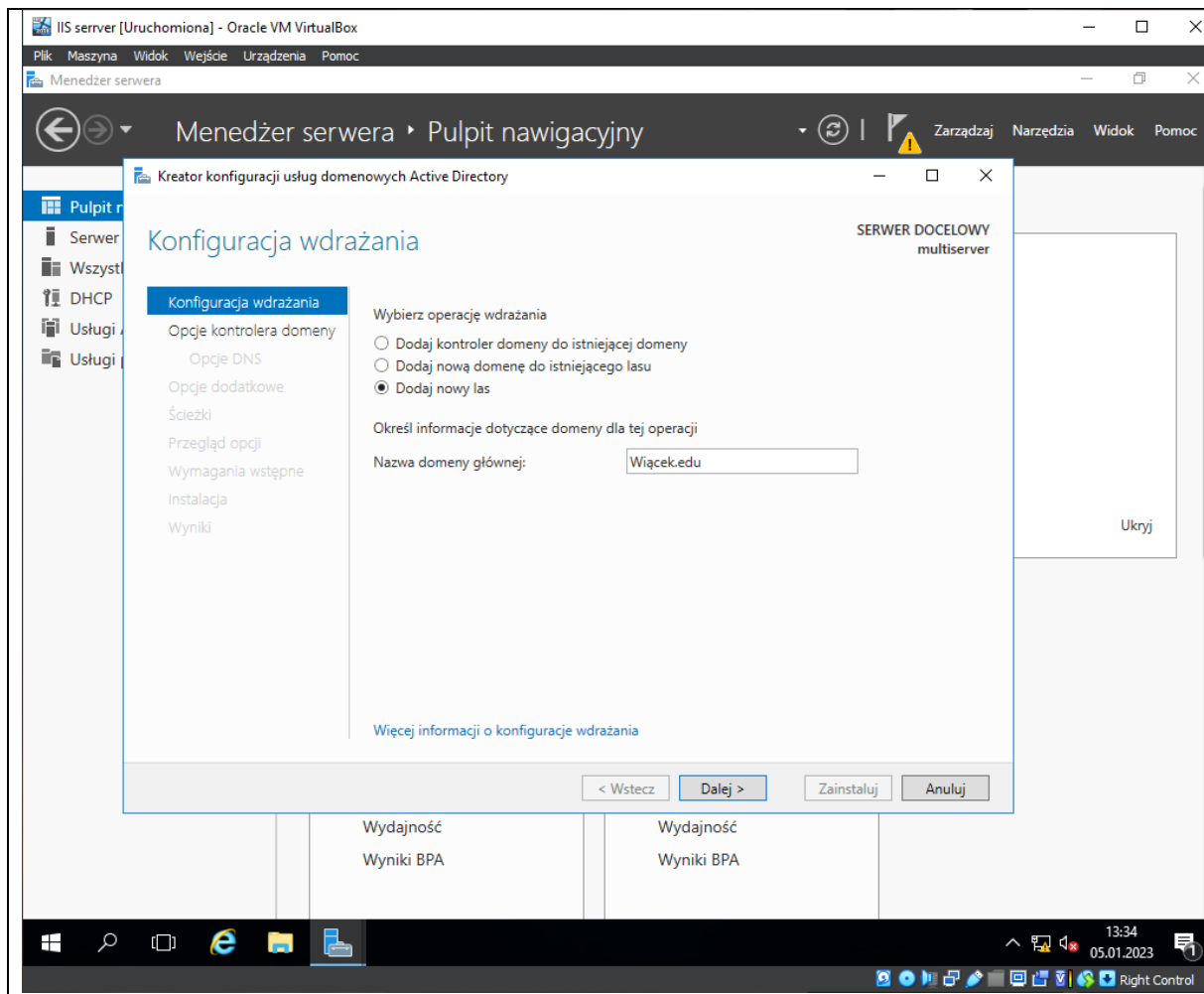


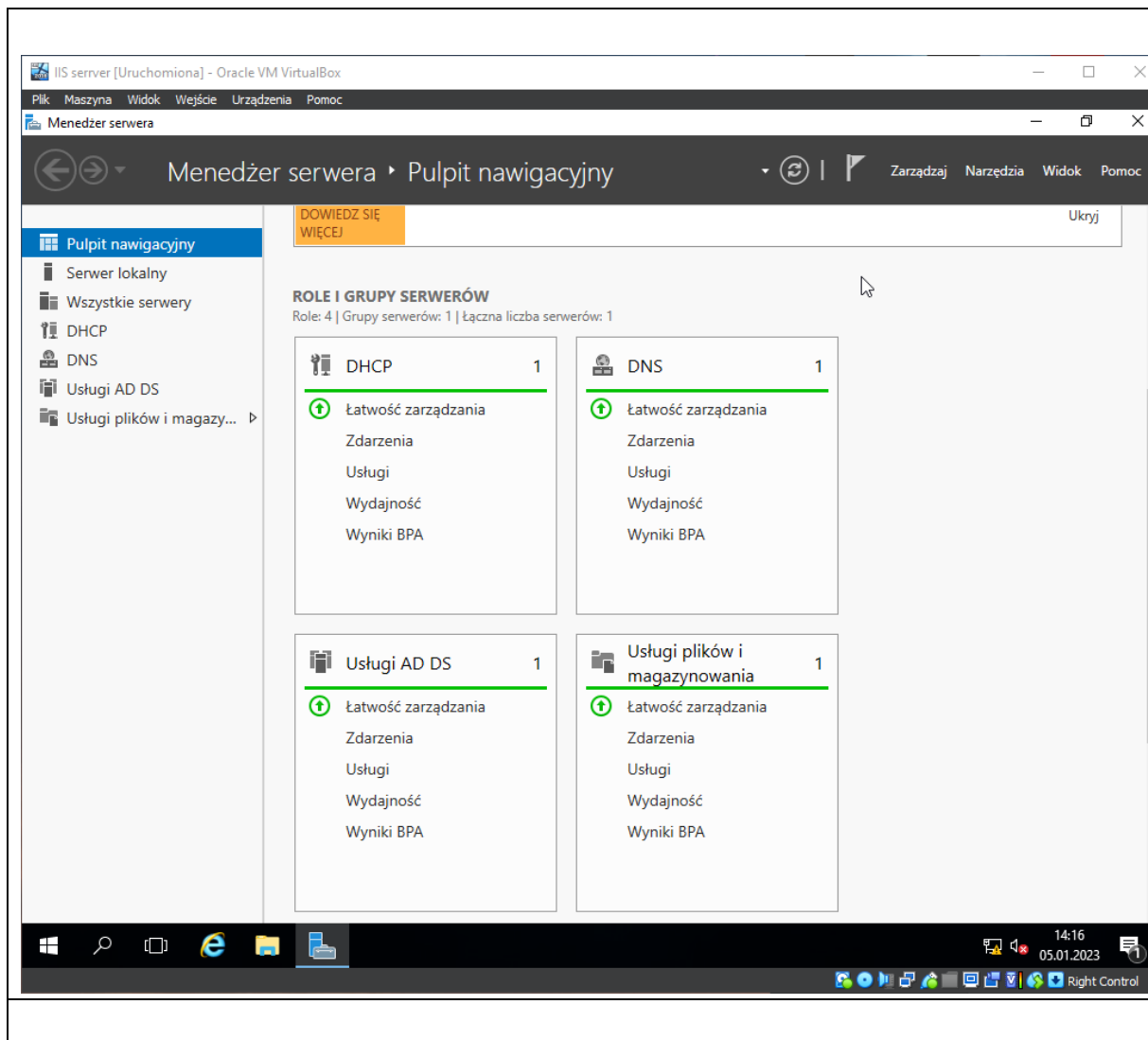


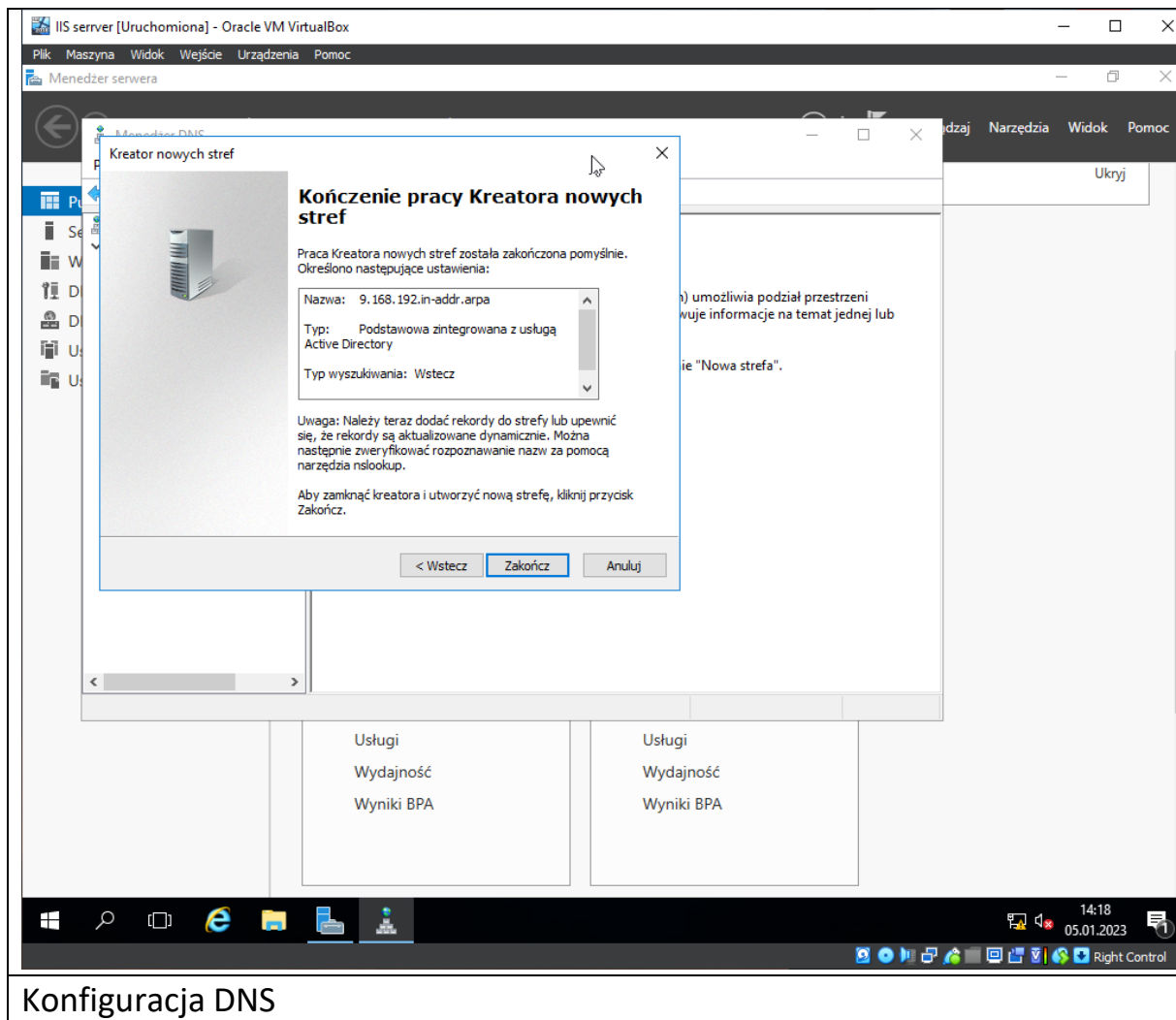


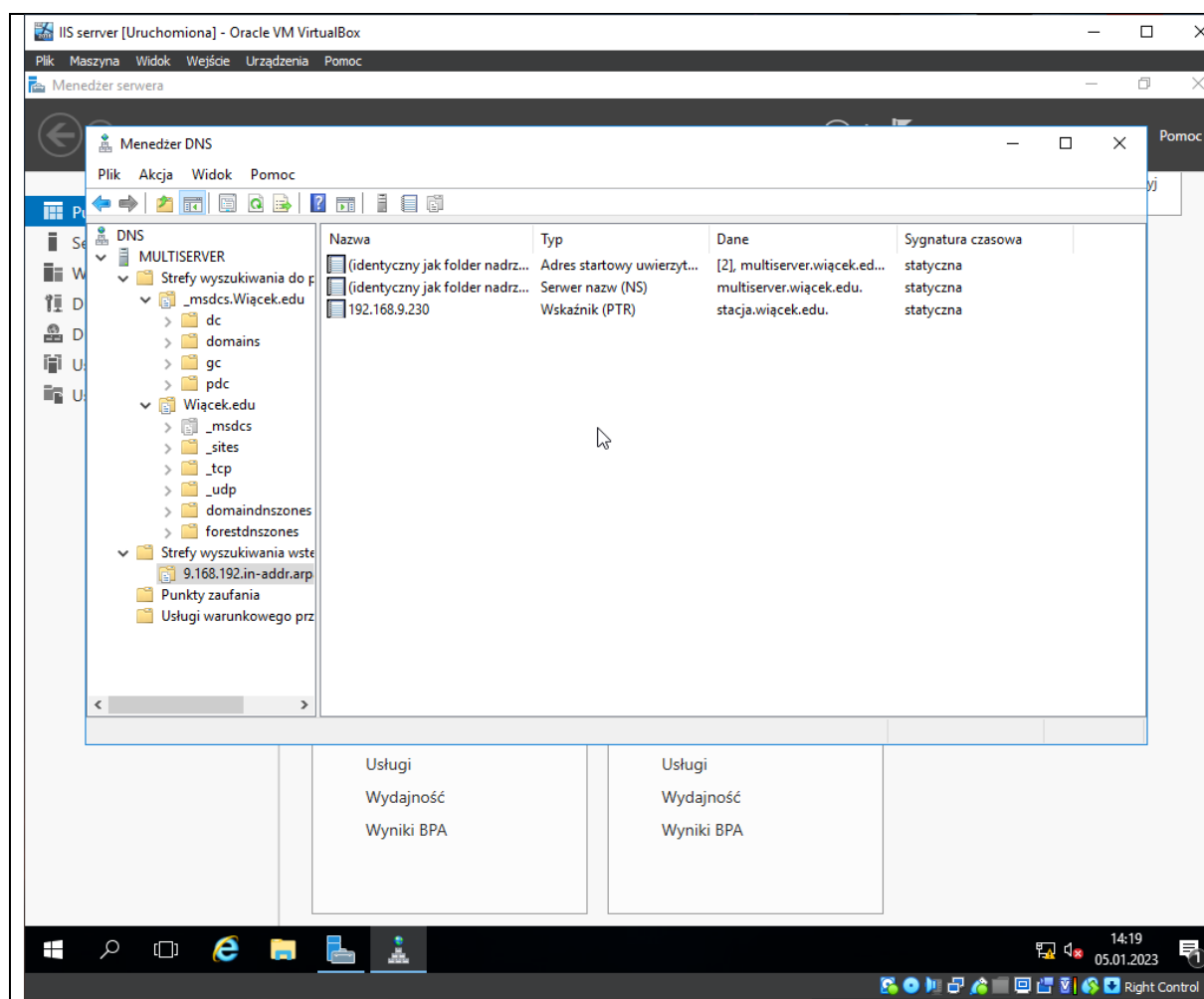
Poprawnie skonfigurowany DHCP

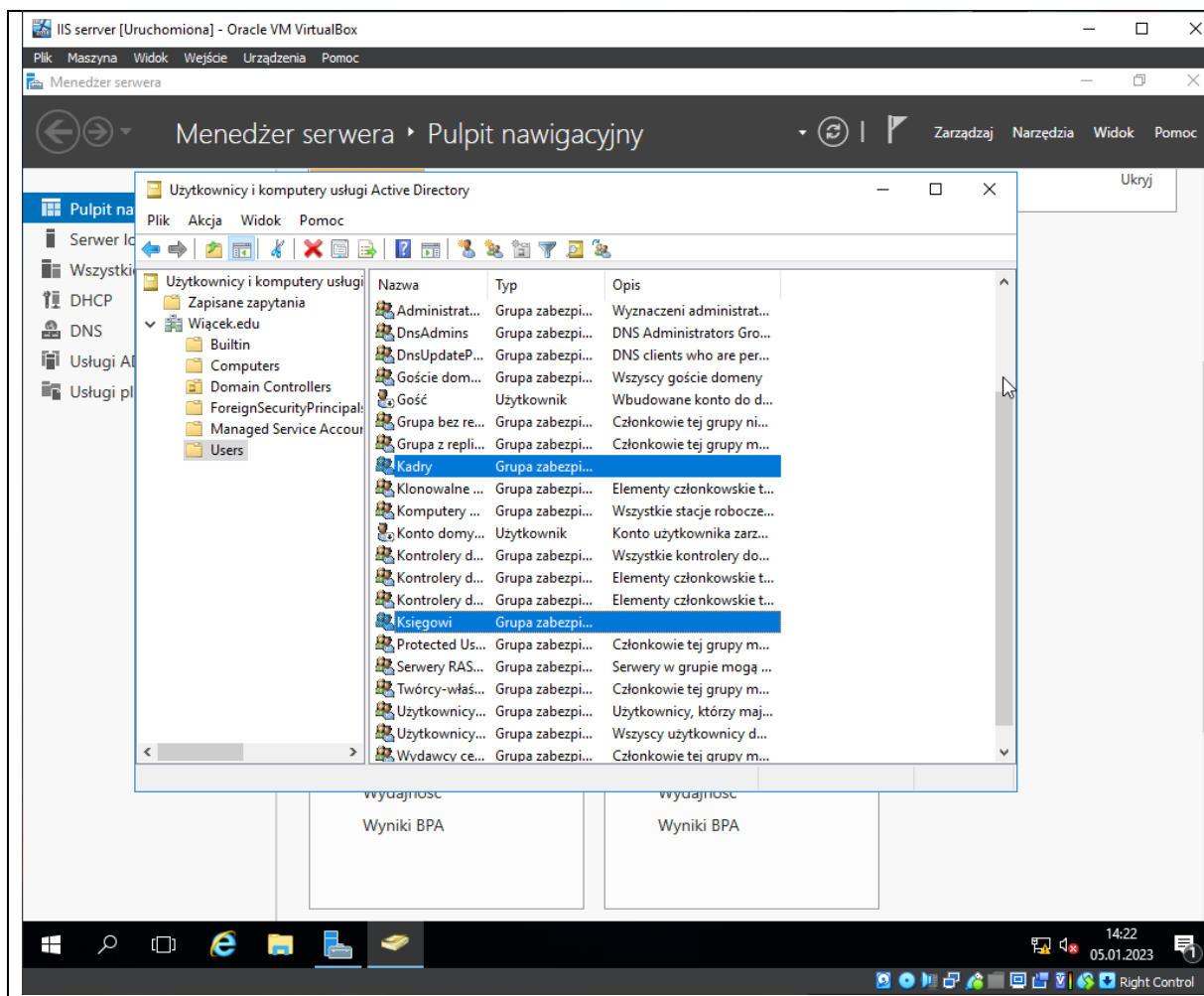


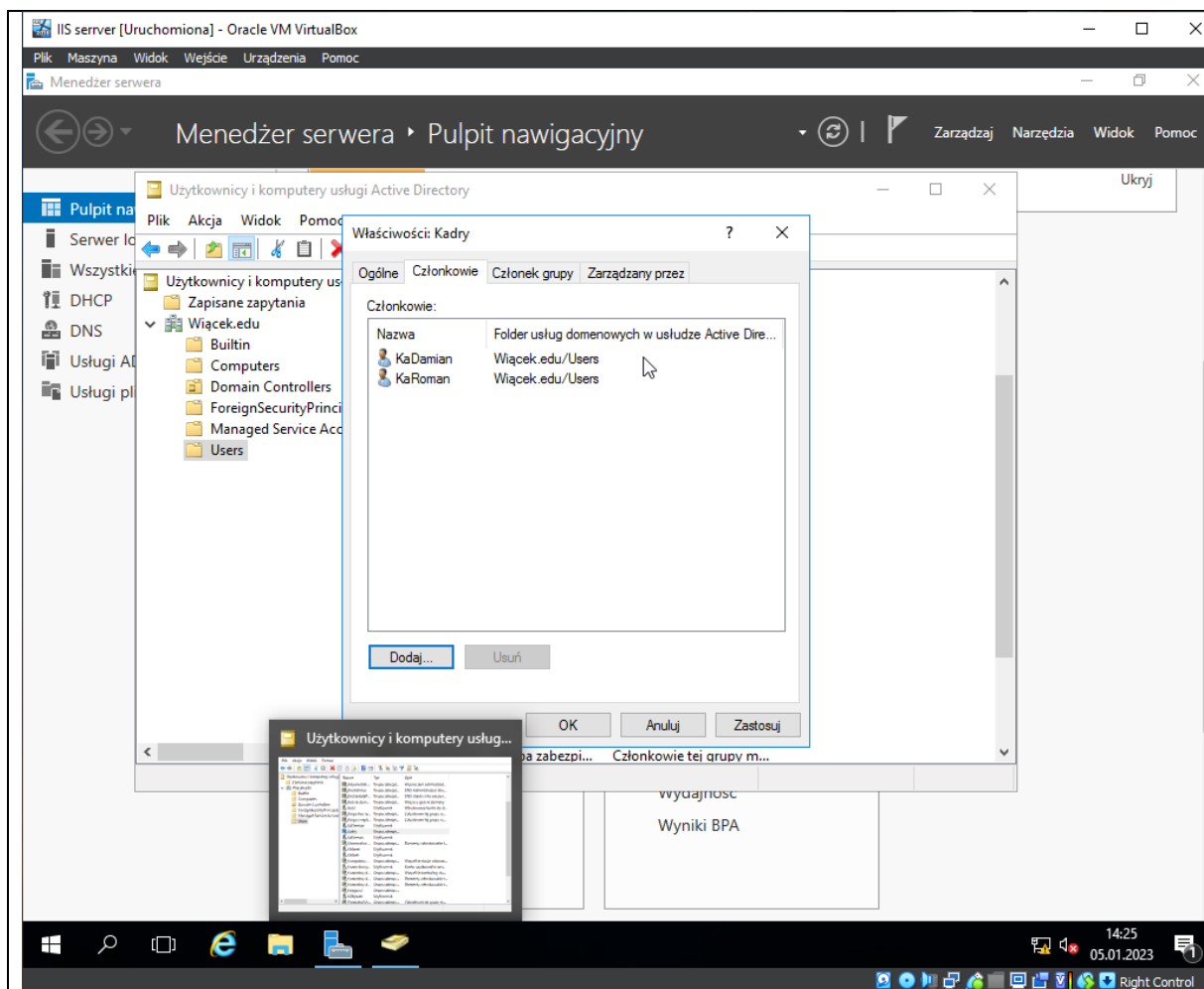




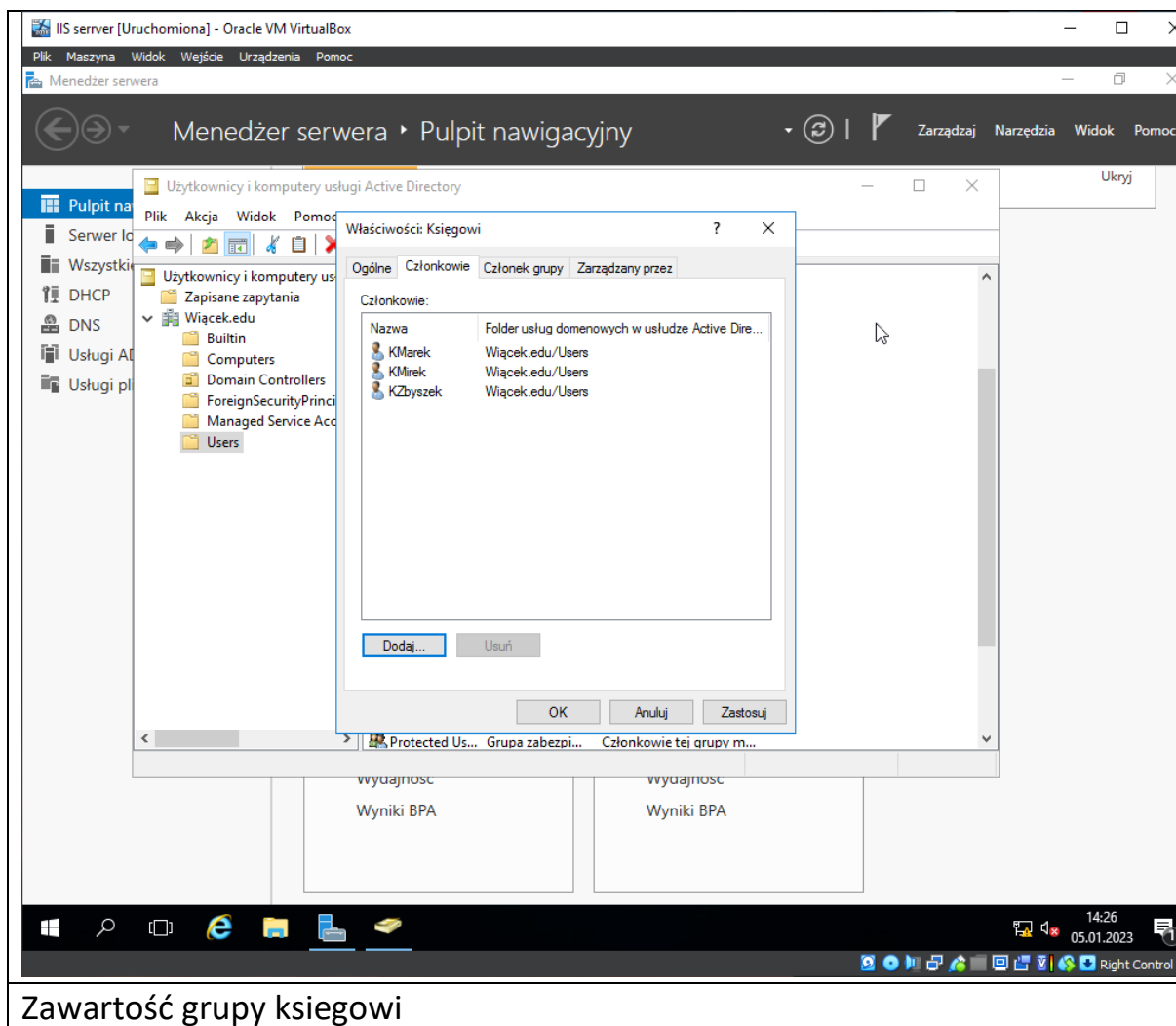




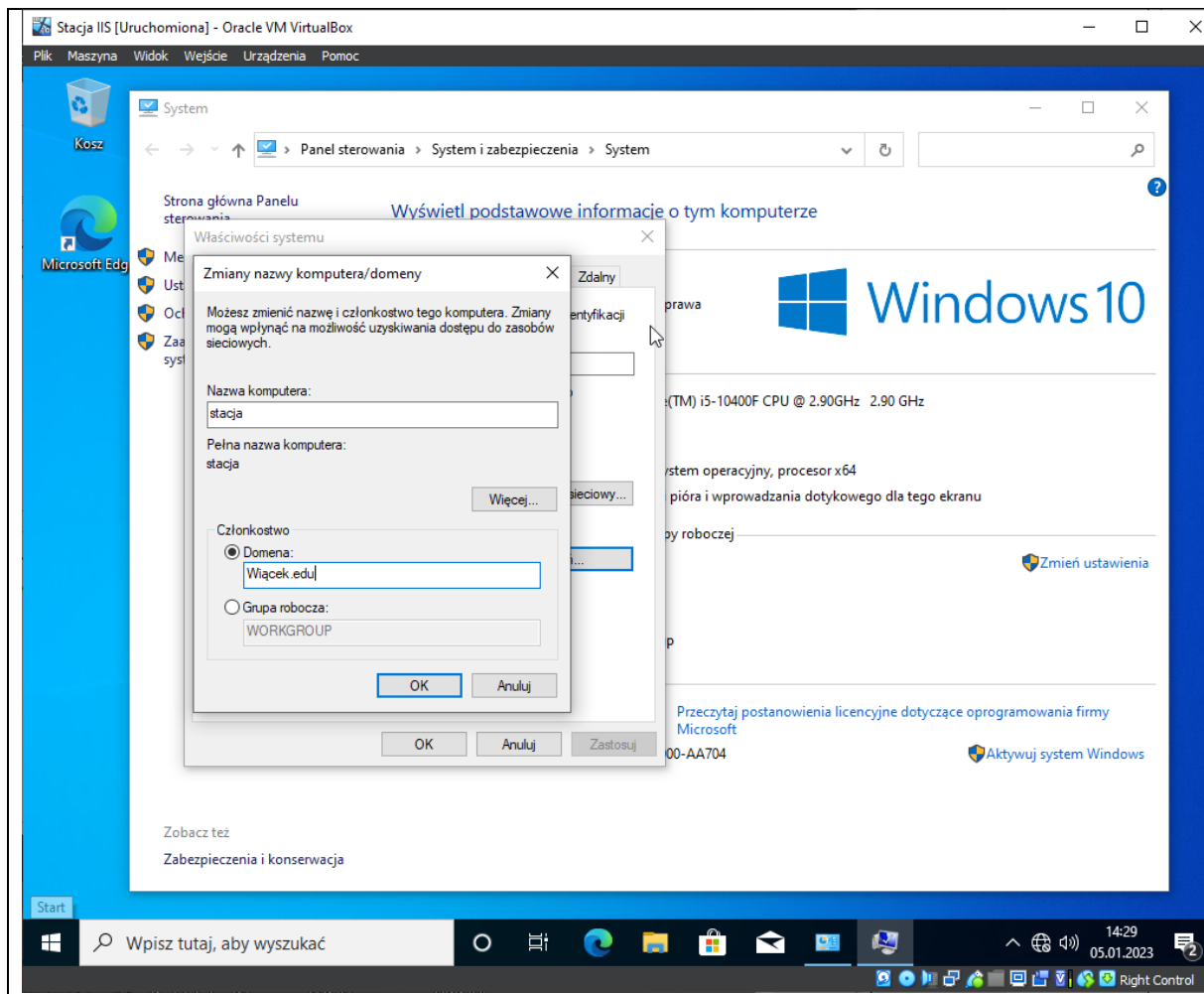


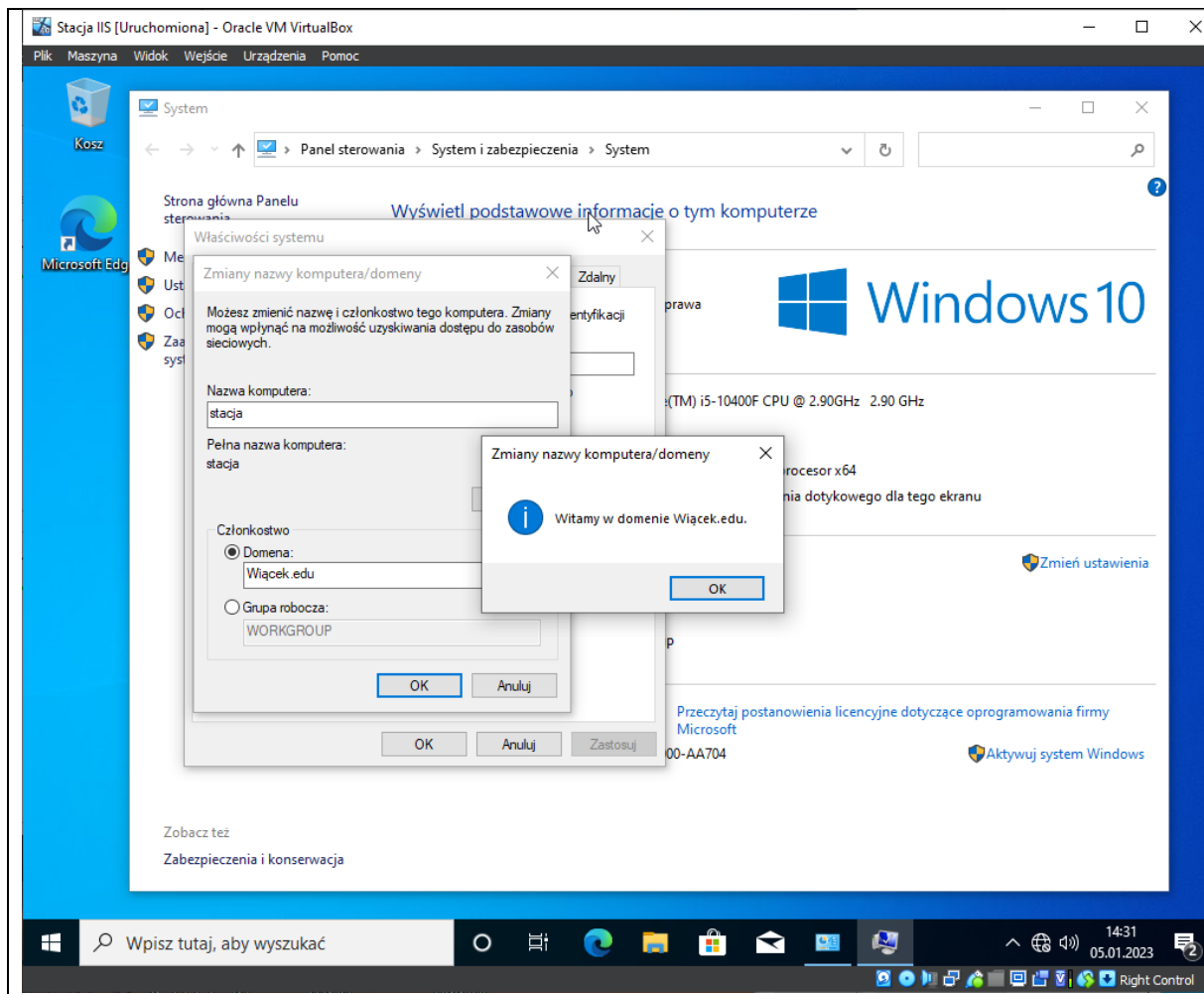


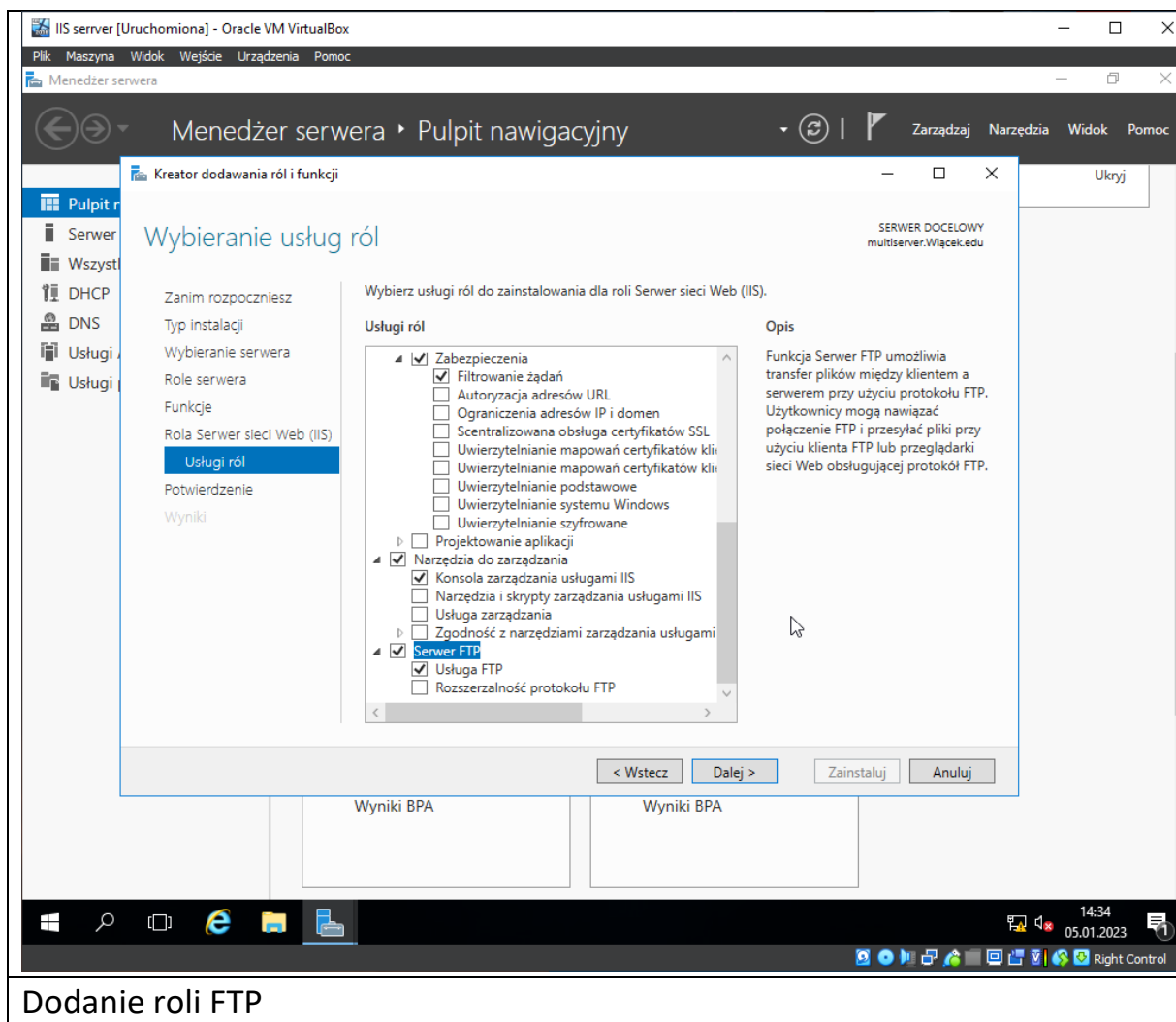
Zawartość grupy Kadry



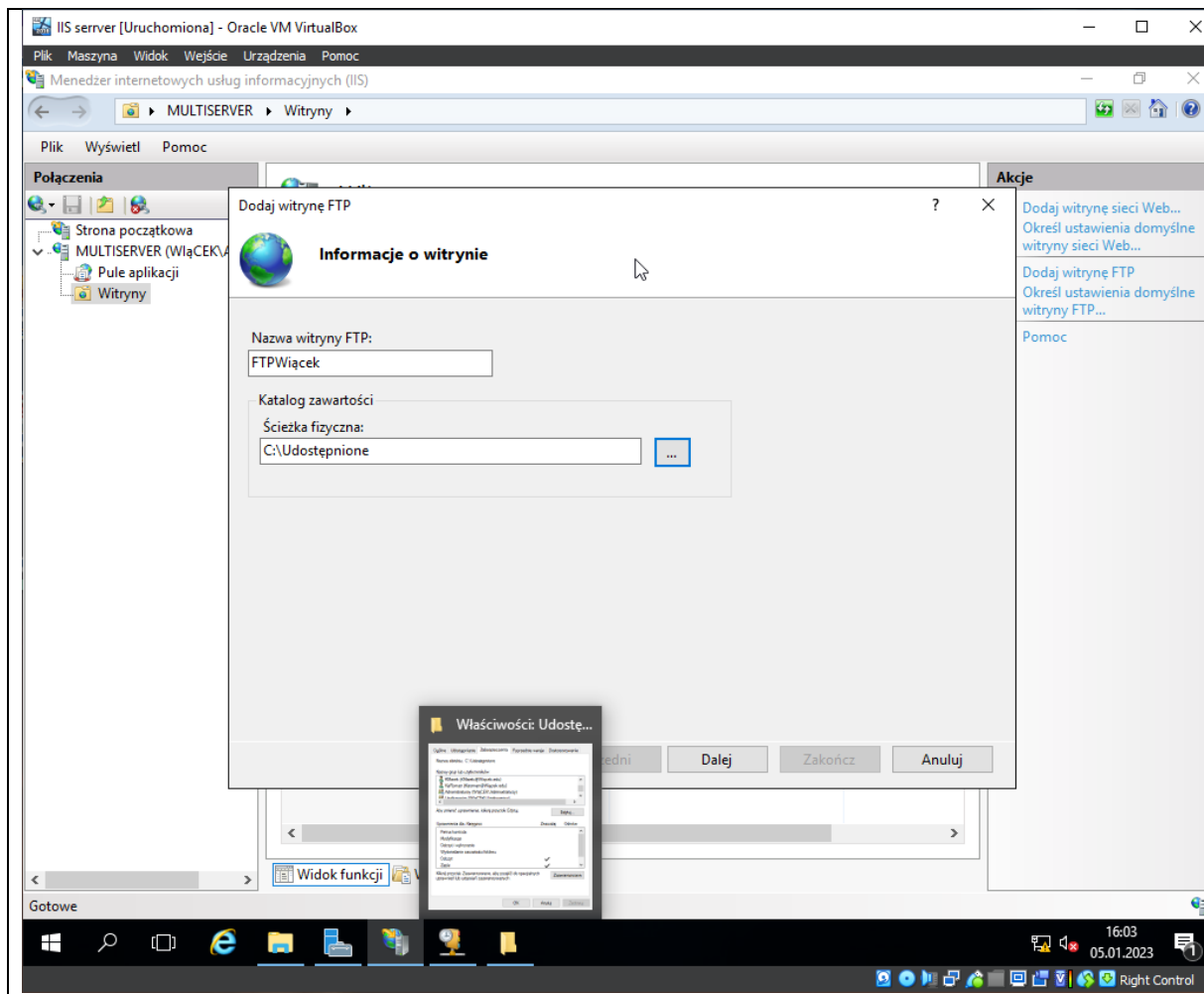
Zawartość grupy księgowi

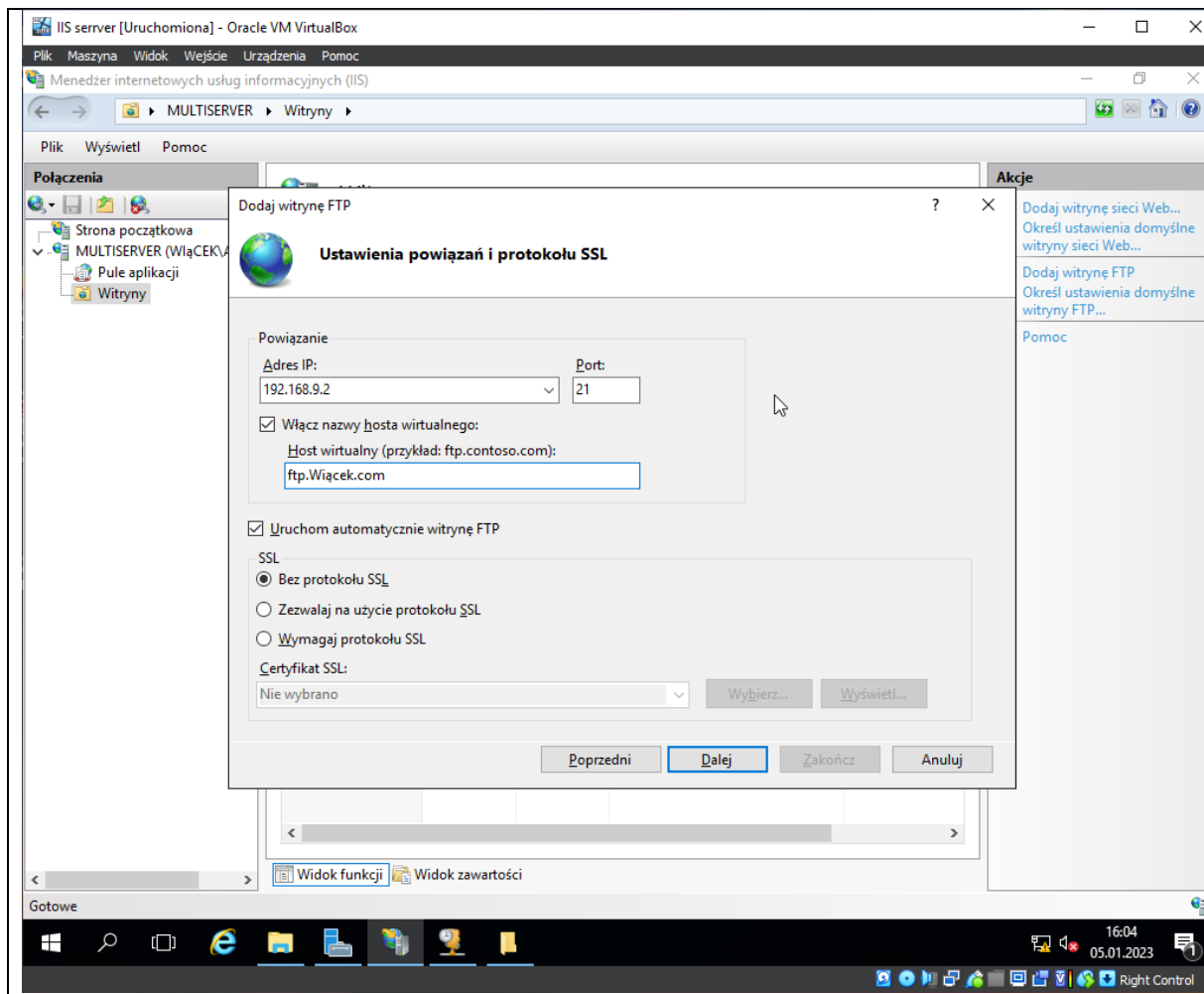


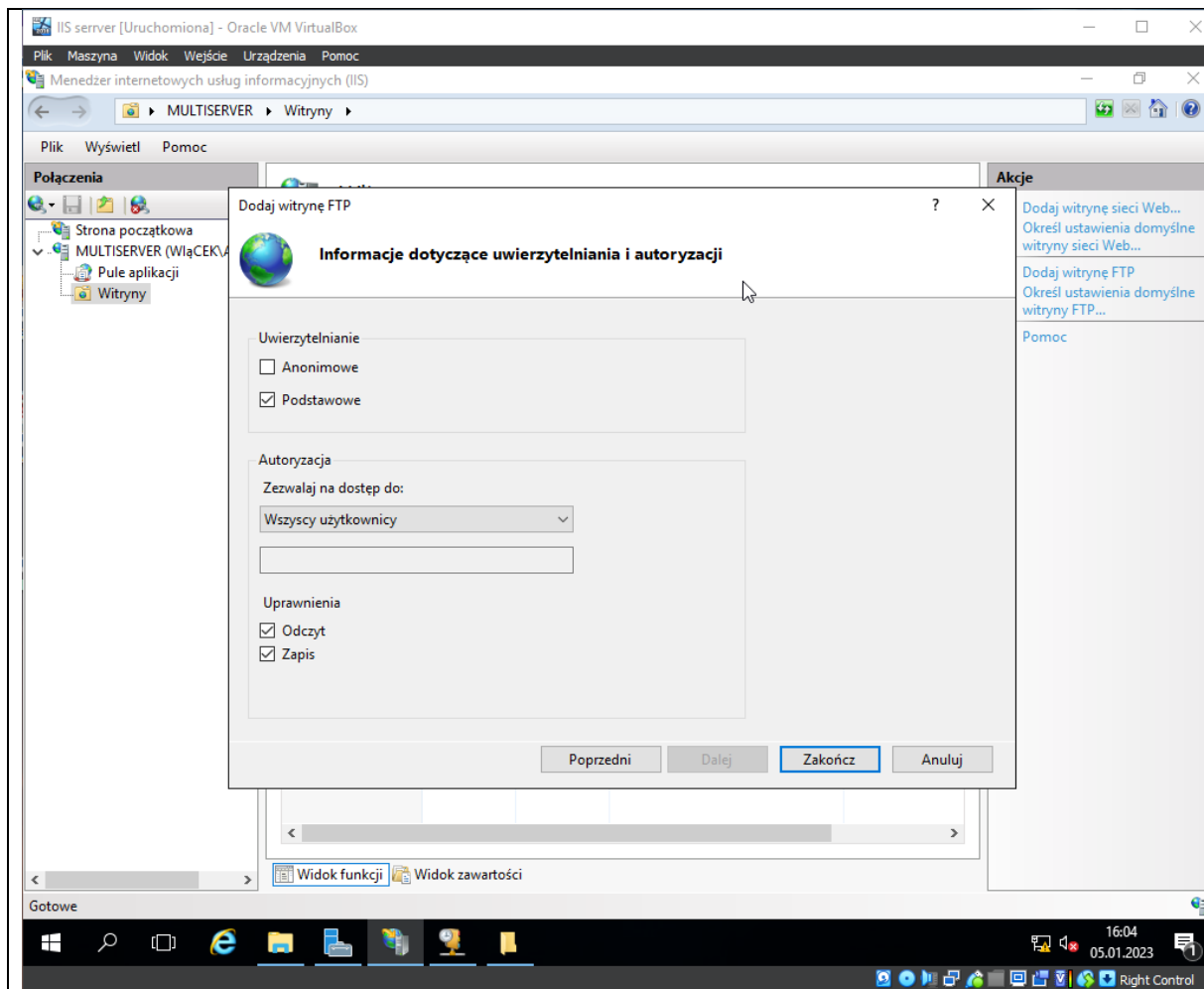




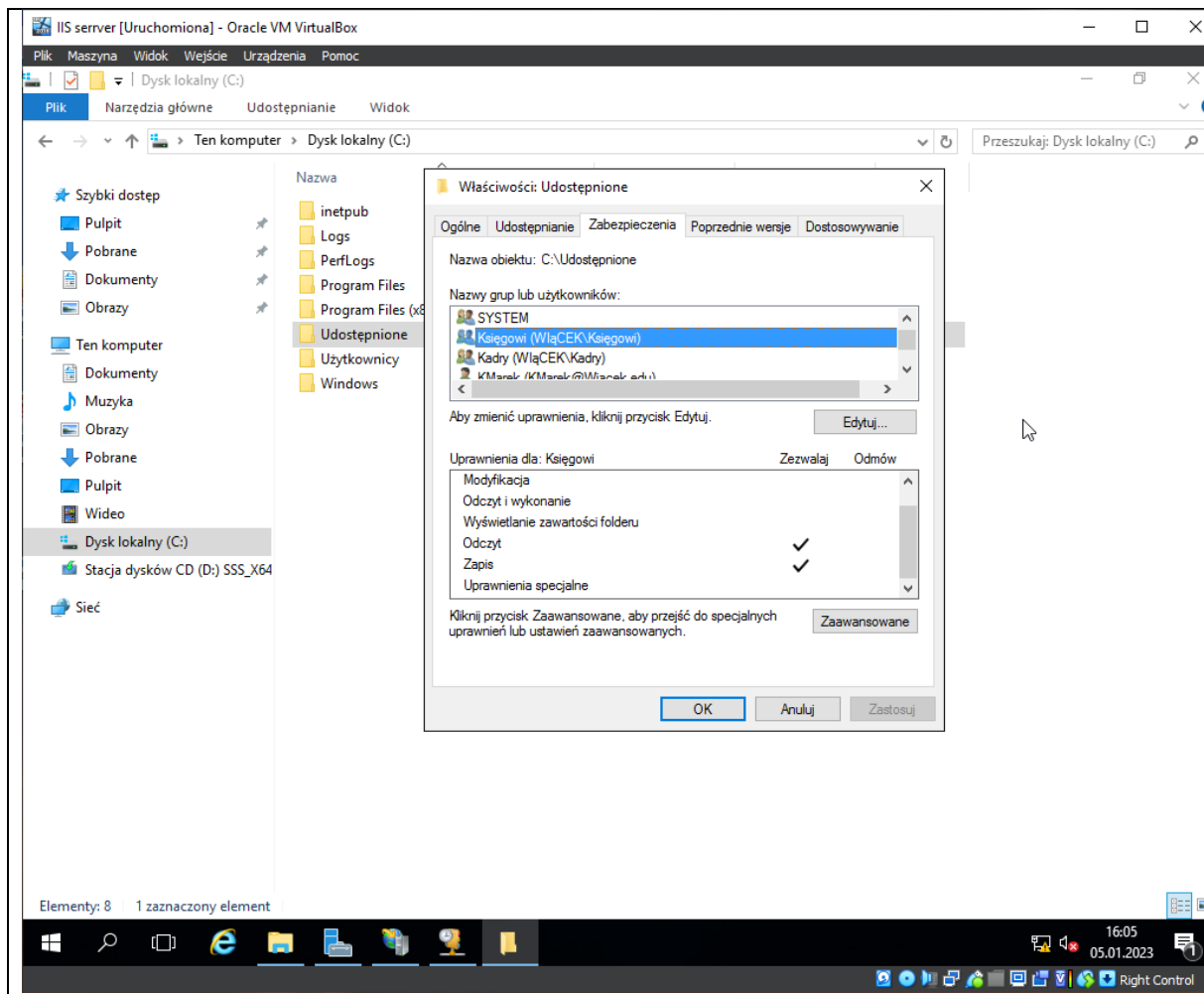
Dodanie roli FTP

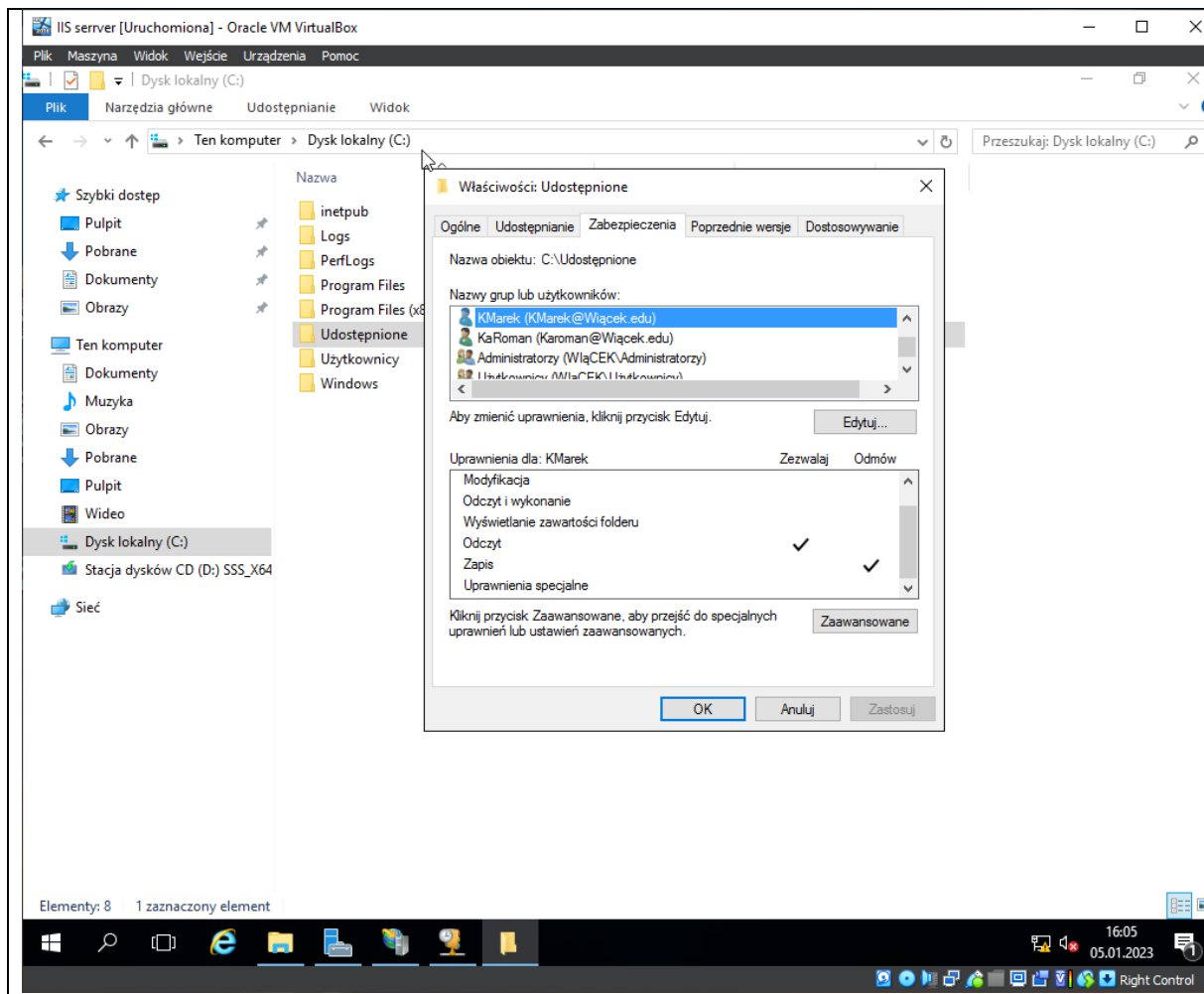


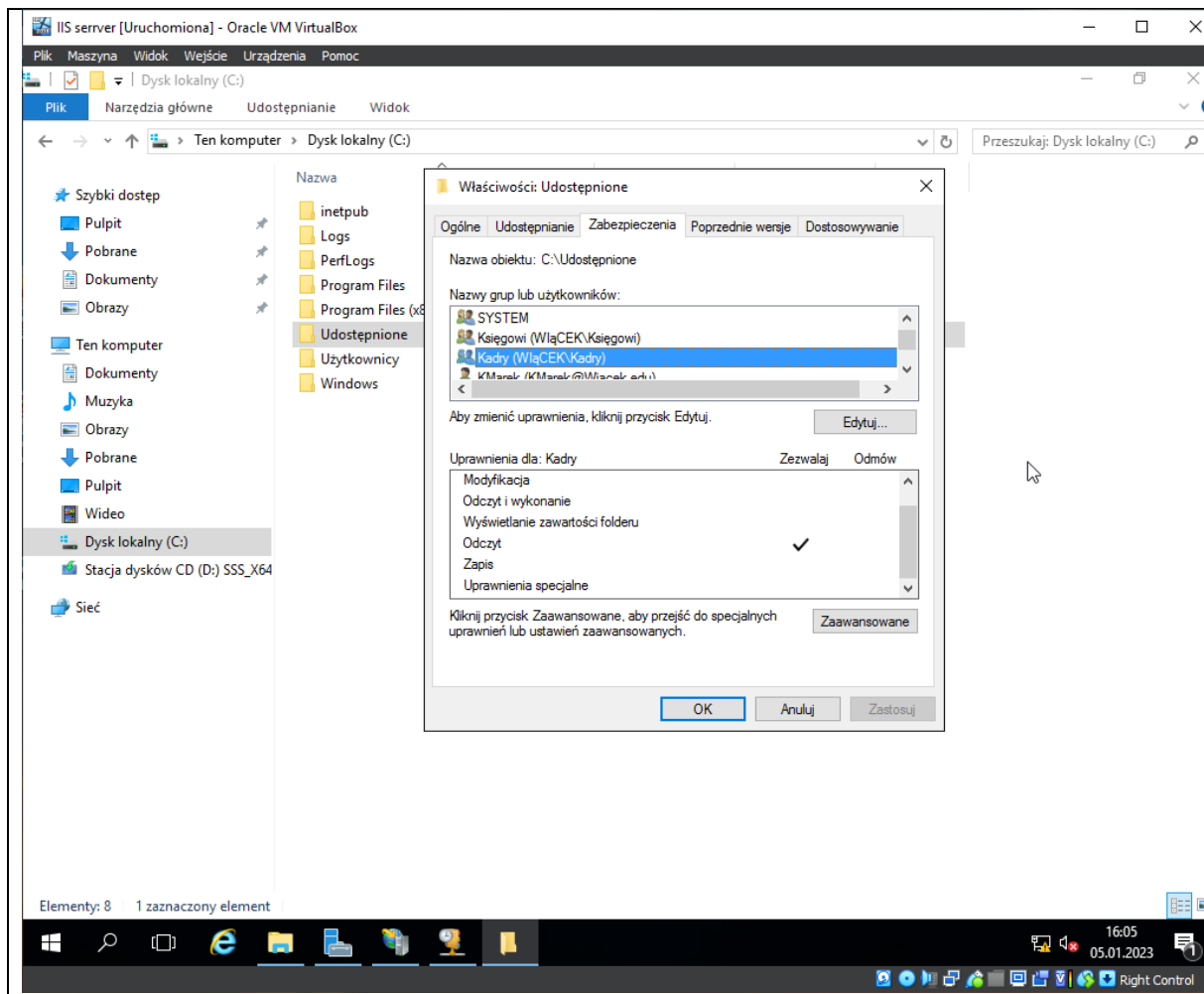


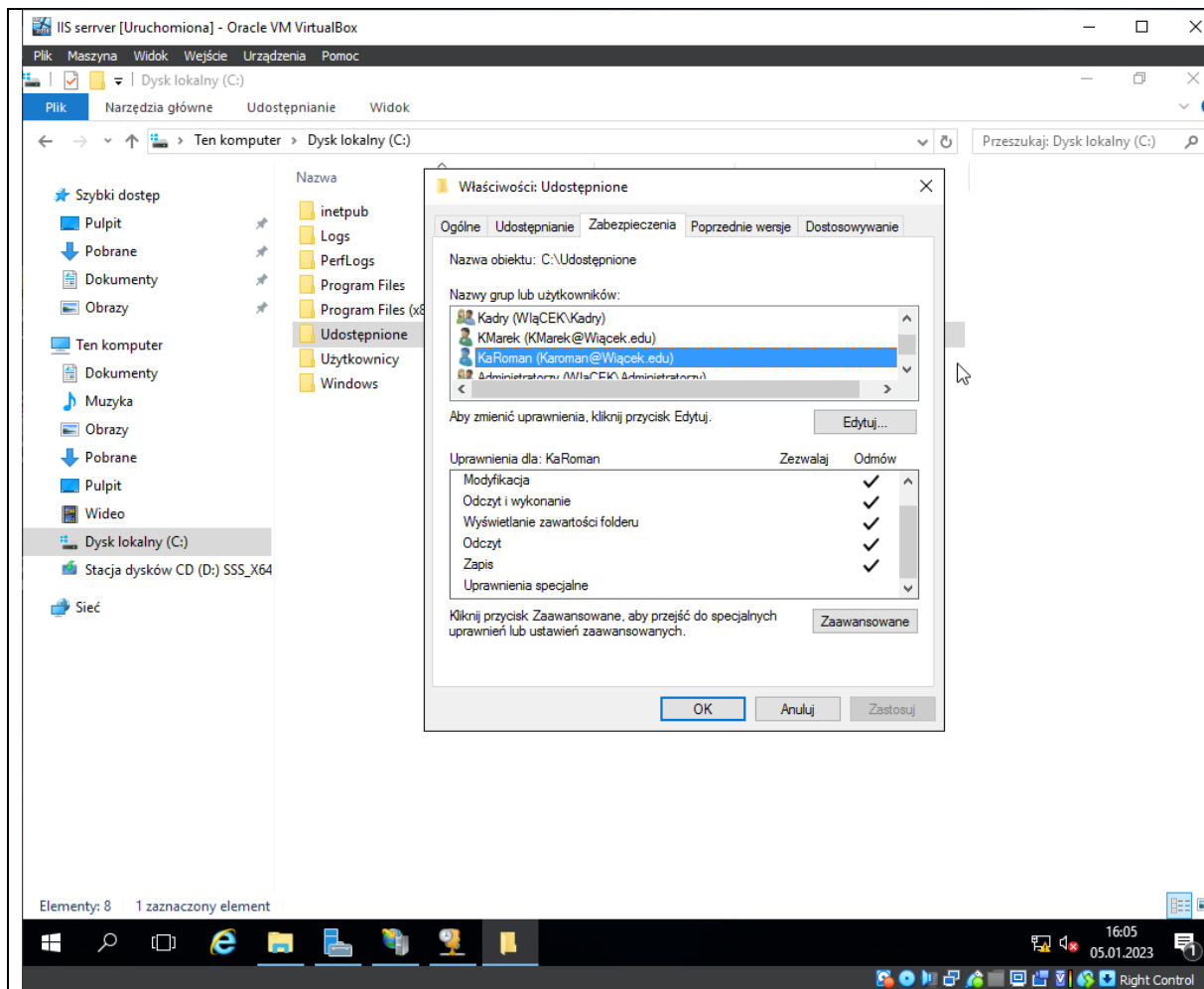


Konfiguracja witryny FTP

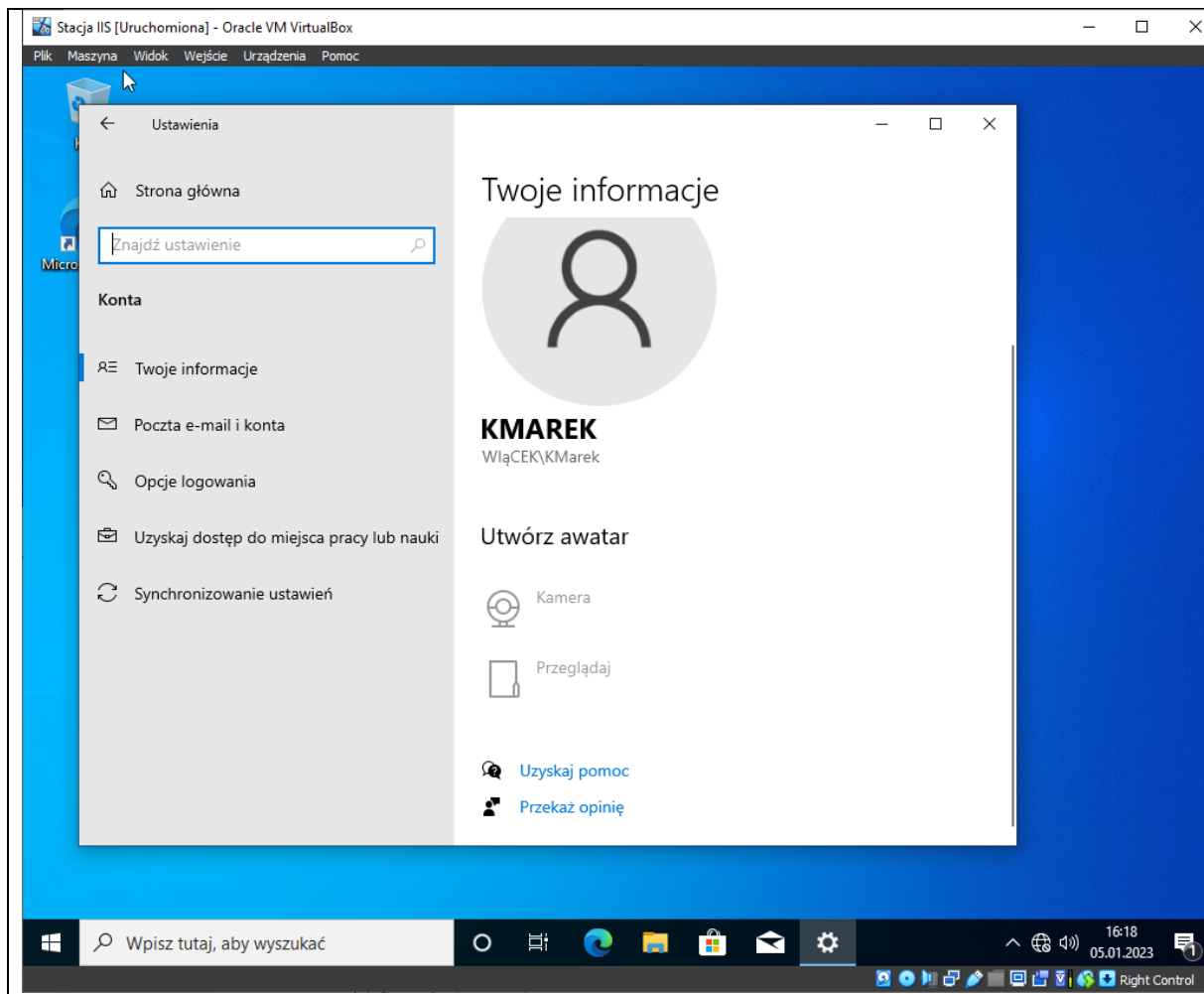


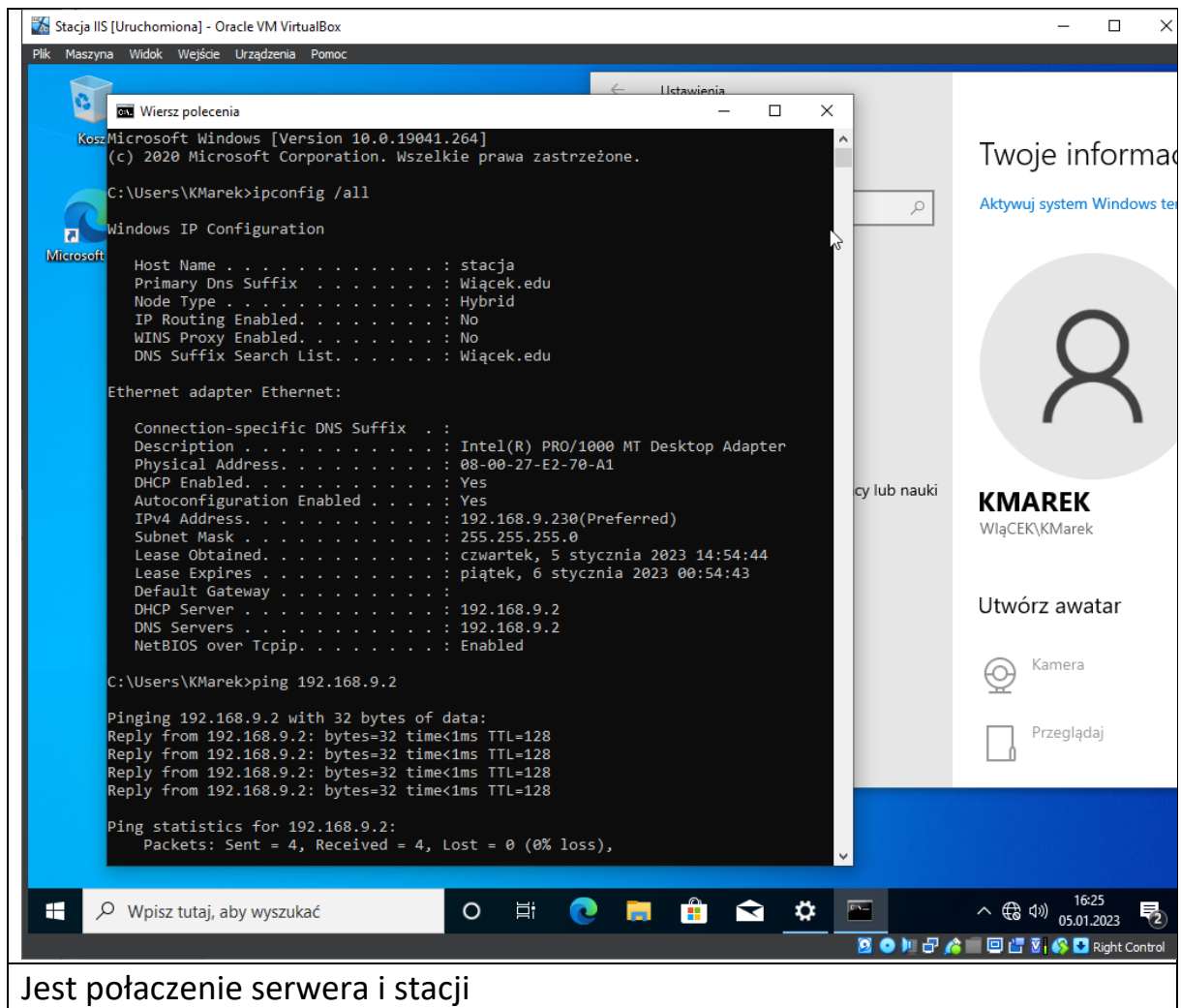




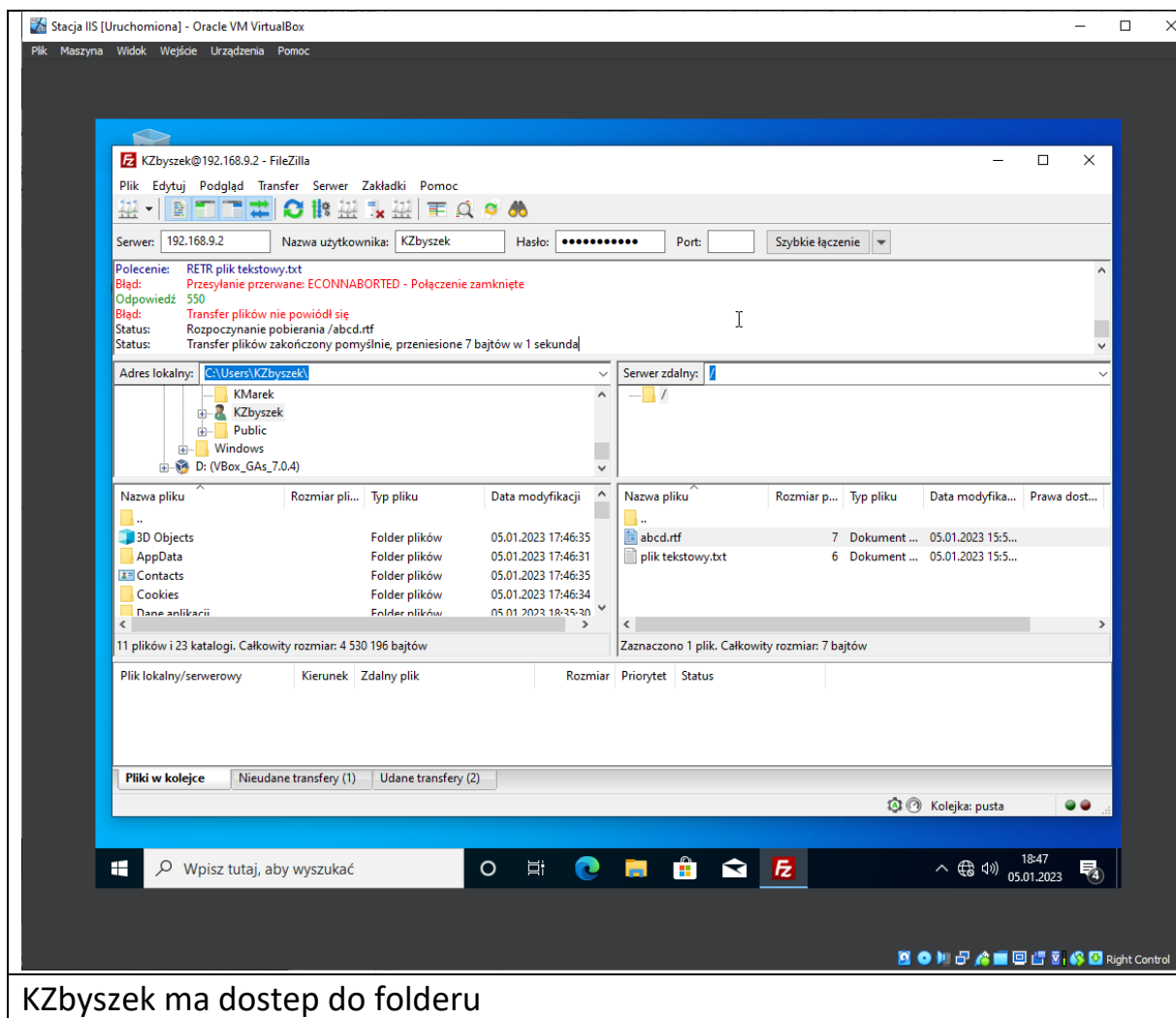


Utworzenie Uprawnień użytkownikom

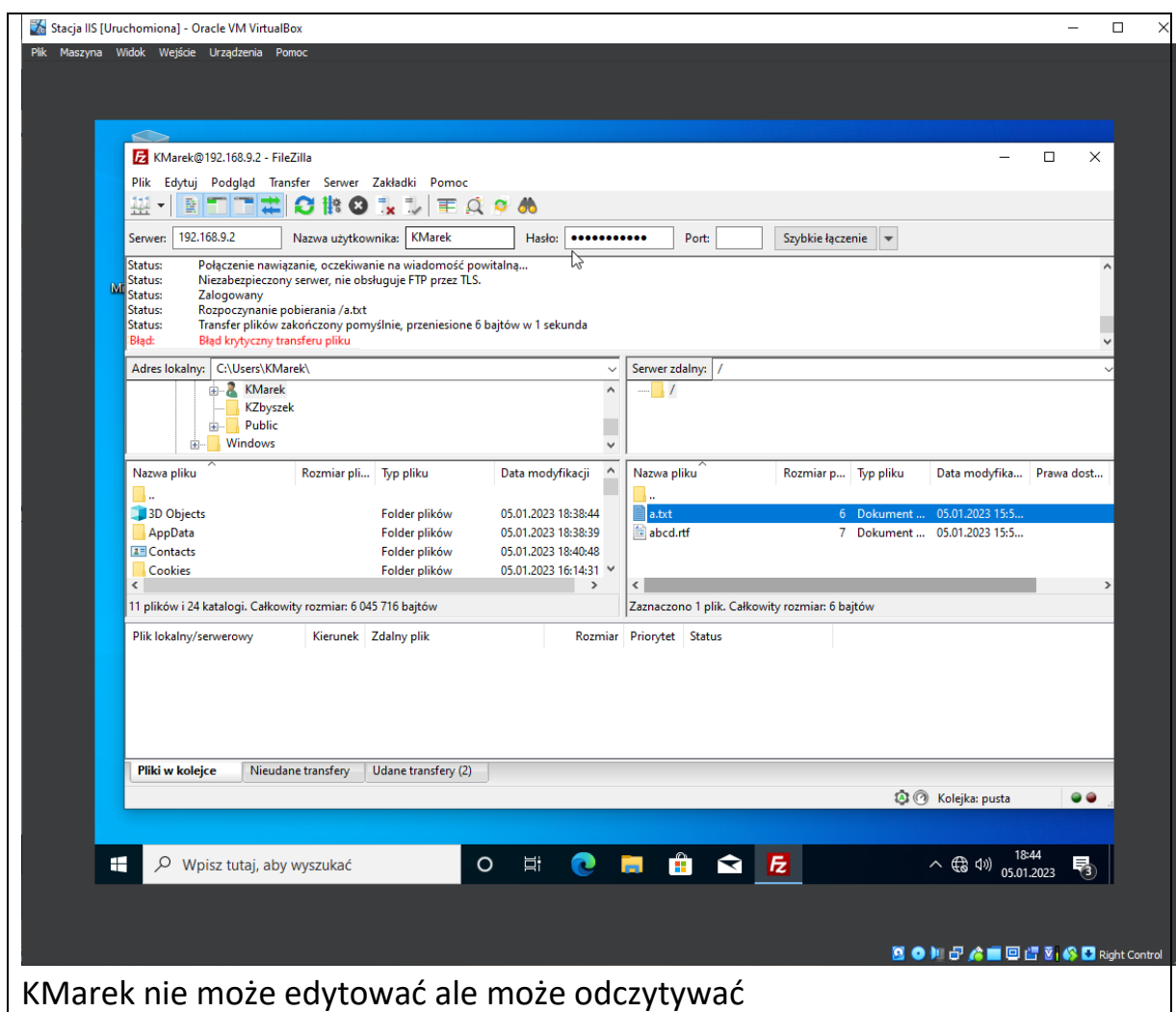




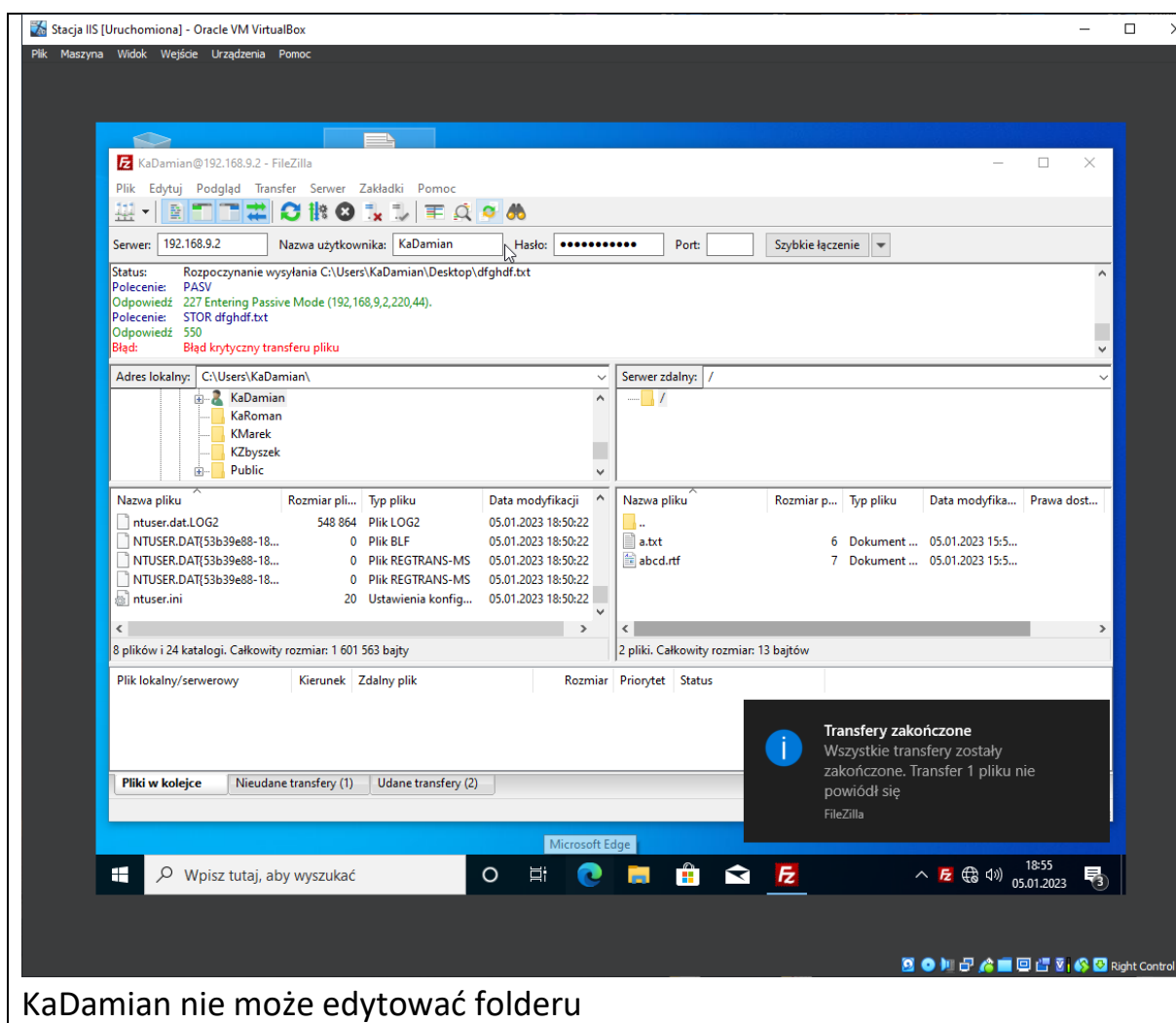
Jest połączenie serwera i stacji

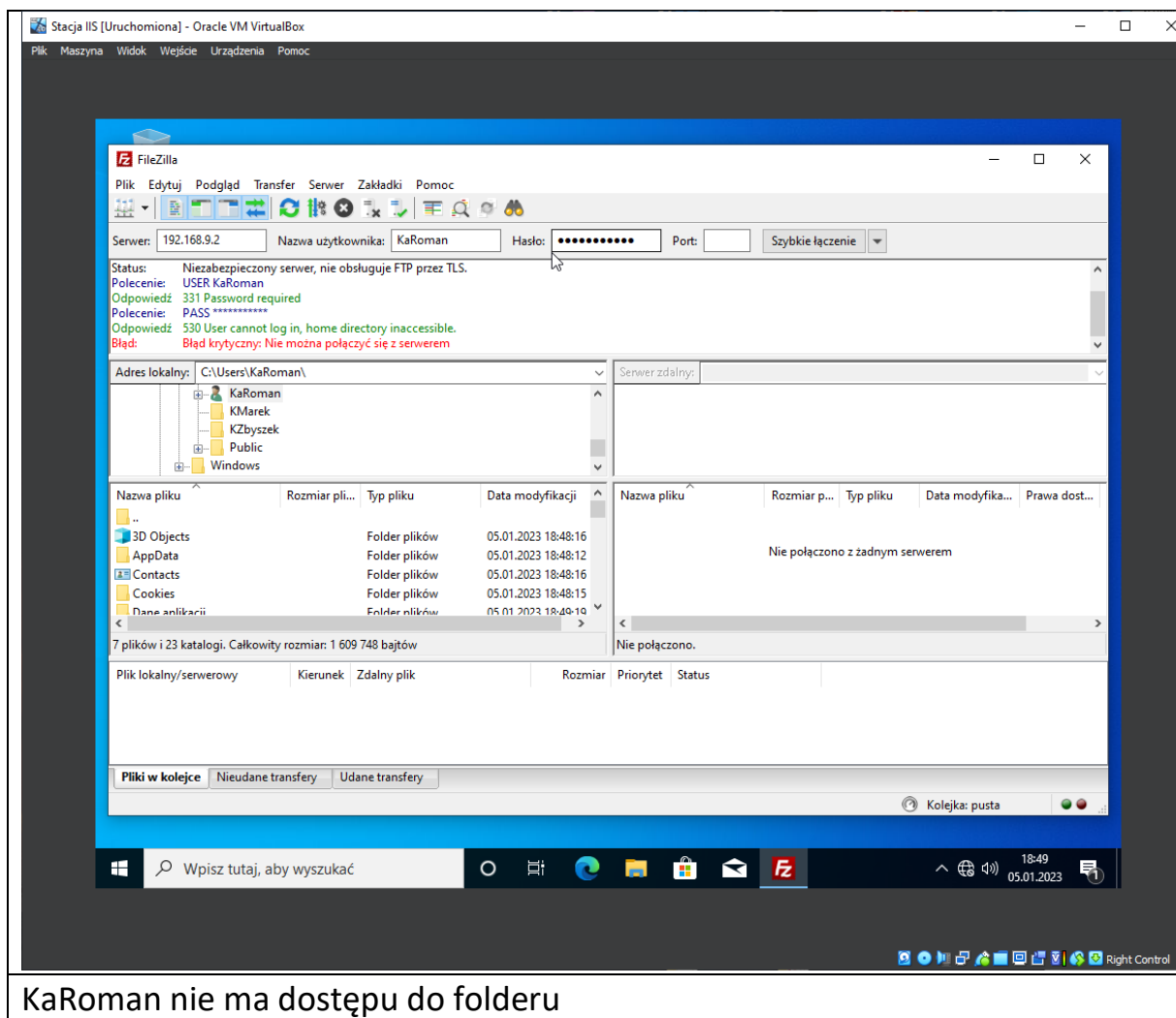


KZbyszek ma dostęp do folderu

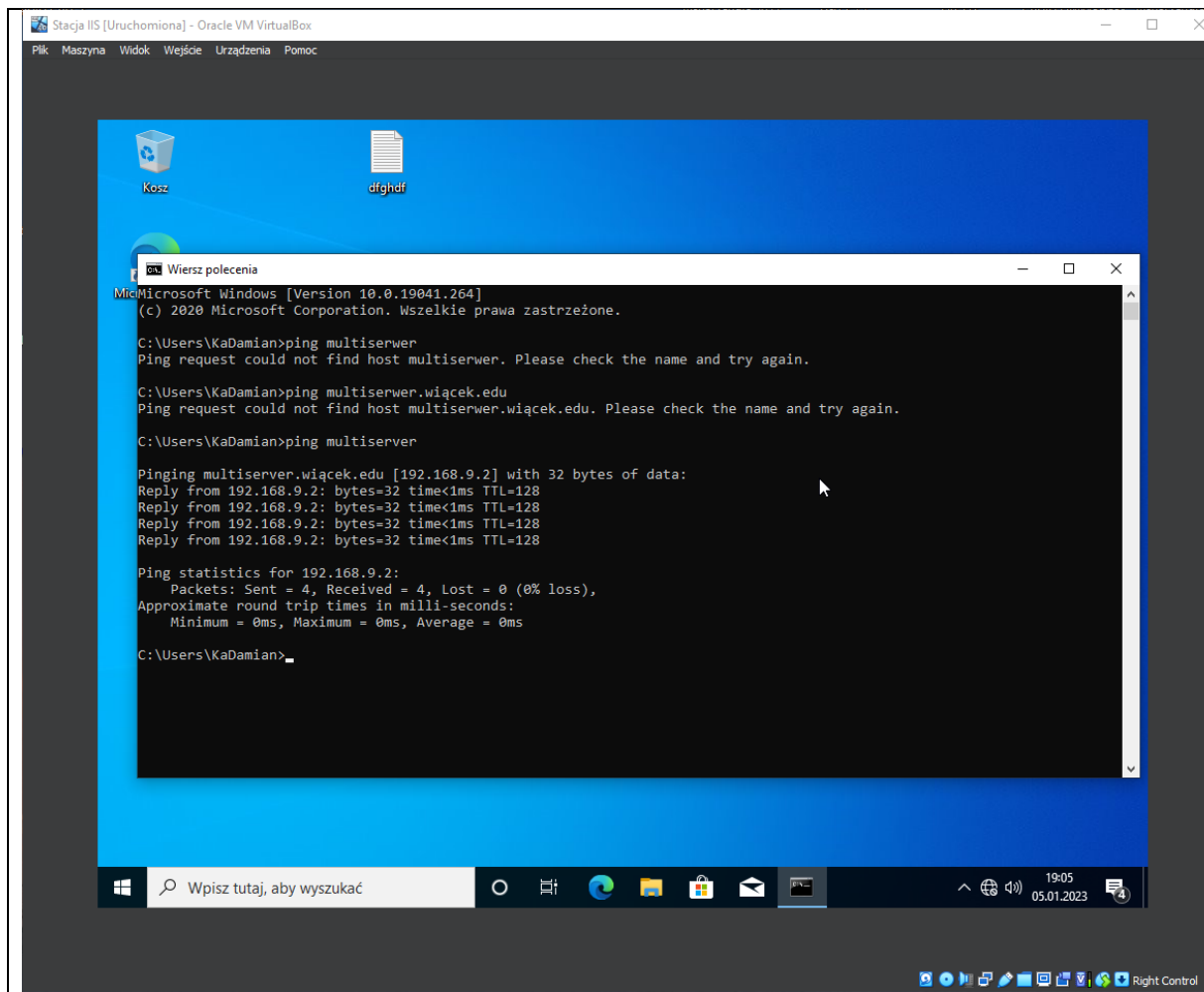


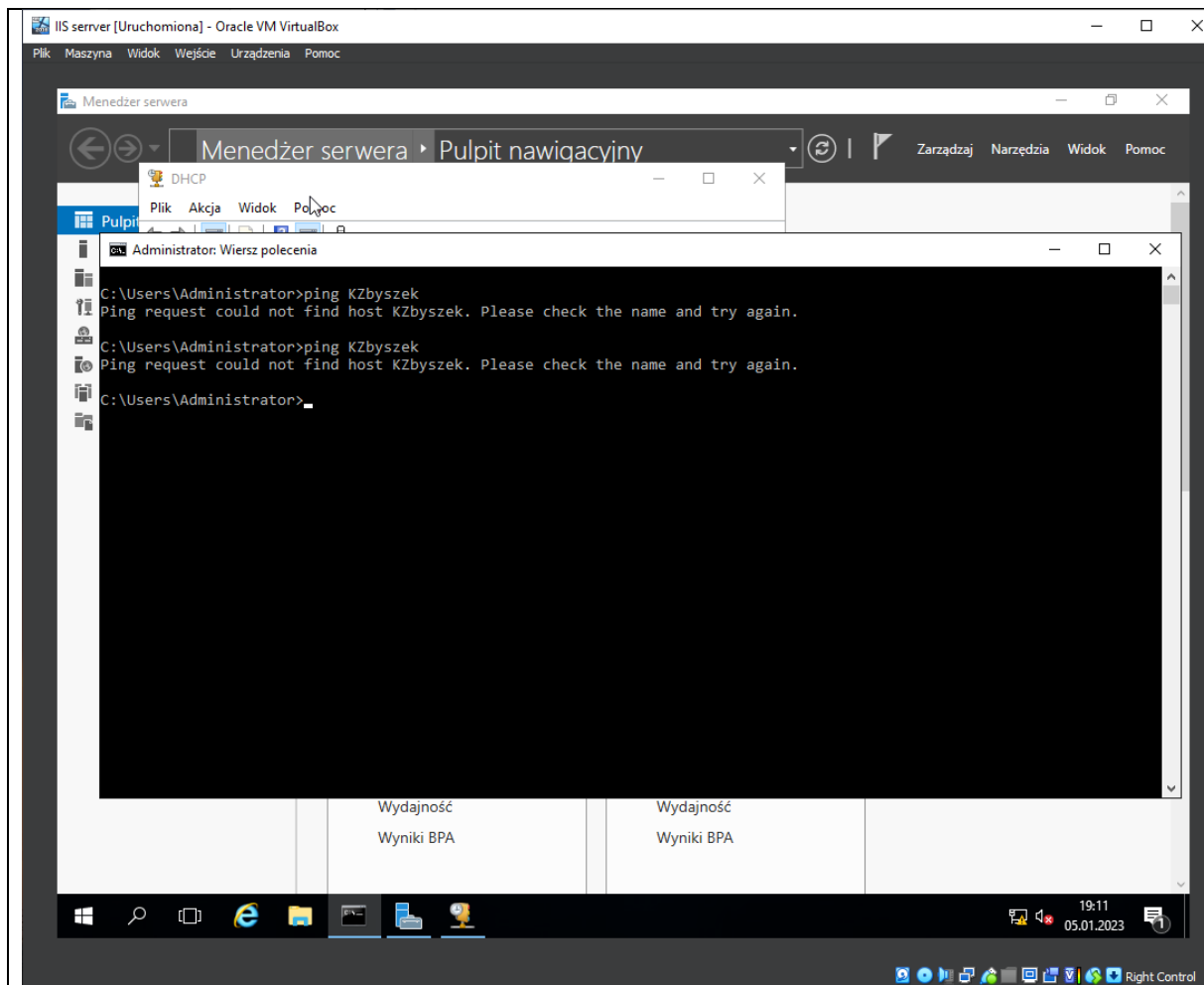
KMarek nie może edytować ale może odczytywać





KaRoman nie ma dostępu do folderu





Problemem jest że serwer nie jest w stanie spingować stacji po nazwie memonicznej a stacja jest w stanie to zrobić

3 Wnioski

Sprawozdanie numer 7 o serwerze FTP było najtrudniejsze do tej pory. Serwer DHCP nie sprawił trudności, ponieważ ćwiczyliśmy ten element w poprzednich sprawozdaniach. Z funkcją DNS było trochę trudniej. Po dodaniu stref wyszukiwania do przodu i do tyłu, a także rekordów A i PTR serwer DNS działał nieprawidłowo ponieważ serwer nie mógł odnaleźć stacji po nazwie memonicznej a po adresie IP już tak. Stacja robocza bez problemów dołączyła do domeny Wiącek.edu. Po utworzeniu kont użytkowników i dodaniu ich do odpowiednich grup zacząłem konfigurować serwer FTP. Dzięki posiadanej wiedzy na temat IIS z technikum nie miałem większych kłopotów z udostępnieniem folderu i ustawieniem odpowiednich ustawień dostępu, lecz sama usługa FTP była nowością bo wcześniej robiłem tylko plik HTML do odczytu. Problem pojawił się po stornie klienta, na stacji. Połączenie mogłem wykonać po zainstalowaniu filezilla który poznaliśmy na zajęciach, lecz ja pamiętałem również o Total comander którego nie wykorzystałem. Po wykonaniu tego sprawozdania utrwaliłem sobie wiedze na temat DHCP, DNS, AD, a także poznałem funkcje serwera FTP.