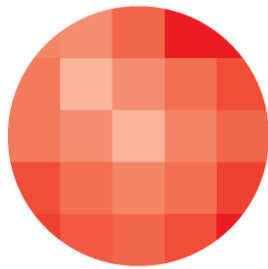


WARSZAWSKA WYŻSZA SZKOŁA INFORMATYKI

SYSTEMY OPERACYJNE



WARSZAWSKA
WYŻSZA SZKOŁA
INFORMATYKI

SPRAWOZDANIE NR 3 TEMAT:

Instalacja i konfiguracja roli DNS w systemie Windows Server

Wykonał/a

Wojciech Wiącek

1 Podstawy teoretyczne

1.1 Pojęcie roli DNS:

System nazw domen (DNS) to hierarchiczny system nazewnictwa zbudowany na rozproszonej bazie danych dla komputerów, usług lub dowolnego zasobu podłączonego do Internetu lub sieci prywatnej. Co najważniejsze, tłumaczy czytelne dla człowieka nazwy domen na identyfikatory numeryczne związane ze sprzętem sieciowym, umożliwiając lokalizowanie i podłączanie urządzeń na całym świecie. Analogicznie do sieciowej „książki telefonicznej”, DNS to sposób, w jaki przeglądarka może przetłumaczyć nazwę domeny (np. „facebook.com”) na rzeczywisty adres IP serwera, który przechowuje informacje żądane przez przeglądarkę.

System nazw domen (tj. „DNS”) jest odpowiedzialny za tłumaczenie nazw domen na określony adres IP, aby klient inicjujący mógł załadować żądane zasoby internetowe. System nazw domen działa podobnie jak książka telefoniczna, w której użytkownicy mogą wyszukać żadaną osobę i pobrać jej numer telefonu. Serwery DNS tłumaczą żądania dotyczące określonych domen na adresy IP, kontrolując, którzy użytkownicy serwera mają dostęp po wprowadzeniu nazwy domeny do przeglądarki.

1.2 Pojęcie przestrzeni nazw:

Przestrzeń nazw w systemie DNS jest zorganizowana w postaci drzewa. Nazwy poszczególnych węzłów mają postać sekwencji etykiet rozdzielonych kropką, poczynwszy od etykiety najniższej w hierarchii a skończywszy na etykiecie najwyższej w hierarchii. Ponieważ hierarchia jest drzewem, to nazwy krawędzi tego drzewa wykorzystuje się do etykietowania samych węzłów. Korzeń jest oznaczany po prostu „.”, choć w zapisie nazw węzłów jest to z reguły pomijane. Nazwy nie rozróżniają małych i wielkich liter. Przykładowa nazwa *put.poznan.pl*. oznacza węzeł *put* będący podrzędnym węzłem w stosunku do węzła *poznan*, który z kolei jest podrzędny w stosunku do *pl*. Węzeł *pl* podlega bezpośrednio korzeniowi hierarchii.

Poddrzewa przestrzeni nazw w systemie DNS są nazywane domenami. Nazwa ścieżki od korzenia całej przestrzeni nazw do korzenia domeny nazywamy nazwą domeny

1.3 Klasyfikacje serwerów DNS:

1.3.1 Główne (root) serwery:

Podstawowym typem serwerów DNS są serwery główne. Z praktycznego punktu widzenia każdy serwer przechowujący dane źródłowe jest traktowany jako serwer główny dla danego poziomu w hierarchii nazw domenowych. Wśród tego typu serwerów szczególną funkcję pełnią tzw. „root serwery”, czyli serwery przechowujące informacje o serwerach głównych, obsługujących domeny pierwszego poziomu. Ze względu na dość specyficzną rolę, która ma krytyczne znaczenie dla sprawnego działania całego systemu nazw w Internecie, serwery te realizują tylko i wyłącznie tę jedną funkcjonalność. Wszystkie inne serwery DNS muszą znać adresy „root serwerów”, co jest podstawowym warunkiem umożliwiającym rozwiązywanie wszystkich poprawnych nazw.

1.3.2 Master serwer:

Na każdym poziomie systemu nazw instalowane są tzw. „master serwery”, przechowujące dane źródłowe dla konkretnego poddrzewa danego poziomu. W zależności od możliwości firmy, serwery te mogą ograniczać się jedynie do tej jednej funkcjonalności albo mogą świadczyć szerszy zakres usług w sieci, np. udzielać odpowiedzi bezpośrednio stacjom klienckim. Na ogół, w celu podniesienia poziomu bezpieczeństwa sieci, serwery te oprócz przechowywania danych źródłowych, świadczą jedynie usługi polegające na transferze pełnych danych do serwerów zapasowych oraz udzielaniu odpowiedzi dotyczących domen zależnych.

1.3.3 Slave serwer:

Serwery zapasowe także zaliczane są do serwerów głównych. W praktyce, klient jednakowo traktuje odpowiedzi uzyskane od serwera typu slave co i master. Zgodnie z normami, dopuszczalna liczba oficjalnych serwerów głównych (master i slave) wynosi pięć. Praca serwera typu slave polega na transferowaniu informacji z serwera typu master zawsze wtedy, gdy serwer typu slave nie ma odpowiednich danych albo gdy dane uległy zmianie. Serwer typu slave okresowo porównuje wersję danych, które posiada z wersją danych znajdujących się na serwerze typu master. Jeżeli wersje różnią się między sobą (wersja master jest nowsza niż wersja slave), serwer typu slave dokonuje transferu danych z serwera typu master. Najnowsze serwery DNS umożliwiają bardziej efektywny sposób synchronizacji danych poprzez informowanie serwerów pomocniczych o zmianie wersji oraz transfer tylko tych danych, które uległy zmianie.

1.3.4 Cache serwer:

Jedną z funkcji serwerów DNS jest buforowanie danych, które zostały uzyskane w wyniku procesu wyszukiwania. Jeżeli serwer nie został skonfigurowany do przechowywania danych dla konkretnego fragmentu systemu nazw jako serwer typu master lub slave, to taki serwer nazywa się serwerem buforującym. Jego jedynym zadaniem jest wyszukiwanie danych i ich buforowanie. Podstawową informacją, na podstawie której serwer buforujący poszukuje danych jest baza adresów serwerów typu root.

1.3.5 Forward serwer:

Funkcjonalność serwera typu forward nie wynika z konfiguracji, a ze sposobu jego użytkowania. Serwerem typu forward może być zarówno serwer typu master jak i slave, czy cache, który komunikuje się z serwerami zewnętrznymi w imieniu serwerów wewnętrznych. Jeżeli serwer wewnętrzny otrzyma zapytanie, które wymaga wyszukiwania w Internecie, przekazuje to zapytanie do konkretnego serwera, a ten dokonuje standardowego wyszukiwania danych komunikując się z serwerami zewnętrznymi. Tego typu konstrukcje stosuje się najczęściej w przypadku, gdy sieć wewnętrzna odseparowana jest od Internetu za pomocą FireWall'a i ze względów bezpieczeństwa serwery wewnętrzne komunikują się jedynie z serwerem typu forward, którego rolę pełni zwykły serwer DNS zainstalowany na hoście bastionowym w strefie zdemilitaryzowanej.

1.4 Budowa serwerów DNS:

1.4.1 DOMAIN NAME SPACE, RESOURCE RECORDS

Specyfikują strukturę drzewa przestrzeni nazw i danych związanych z tymi nazwami. Każda gałąź i każdy liść drzewa DNSPACE zawiera pewien zbiór informacji i sposoby (rodzaje zapytań - *queries*) potrzebne do uzyskania chcianej informacji z całego zbioru. Zapytanie wyszczególnia domenę, która go interesuje, oraz określa rodzaj informacji, jakiej potrzebuje.

1.4.2 NAME SERVERS

są programami, które przechowują informacje o drzewie struktury domeny i zbiorach informacji. *Name server* może cache'ować jakiś dowolny fragment struktury sieci, ale generalnie *Name Sever* zawiera kompletną informację na temat fragmentu przestrzeni nazw i wskaźniki do innych *name server'ów*, które zapewniają informacje dla pozostałych części lub innych domen. *Name*

Server zna całą część domeny, o której ma kompletną informację i mówi się, że jest autorytatywny dla niej (*authoritative*). Miarodajne (autorytatywne) informacje są organizowane w jednostki zwane dalej strefami (*zones*).

1.4.3 RESOLVERS

są również programami, które wyciągają informację od *name server'ów* w celu udzielenia informacji na pytania żądane przez komputery - klientów. *Resolver* musi mieć dostęp do co najmniej jednego *name server'a*, by móc odpowiedzieć na pytanie bezpośrednio, lub wymóc żądanie odpytania innych *name server'ów*. Żaden protokół nie jest potrzebny do komunikacji między programem użytkownika a *Resolver'em*, ponieważ ten ostatni jest zwykle wywołaniem systemowym dostępnym bezpośrednio z programów.

1.5 Rekordy:

1.5.1 A:

Przedstawia adres domeny w postaci IP (w systemie Ipv4 jest to 32-u bitowa liczba), np. 195.149.224.42. Jest jednym z głównych rekordów dla domeny – bez niego system nie potrafiłby poprawnie rozwiązać adresu domeny.

1.5.2 AAAA:

Rekord AAAA przypisuje Twojej domenie 128-bitowy adres IPv6. Rekord ten odpowiedzialny jest za to samo co rekord A z tym, że stosuje nowocześniejszy protokół (IP wersja 6).

1.5.3 PTR:

Rekord DNS PTR jest wskaźnikiem do adresu IP nazwy domeny. System DNS utrzymuje te rekordy, które pomagają połączyć nazwę domeny z adresem IP.

1.5.4 NX:

Rekord NS określa autorytatywne serwery nazw dla domeny. Autorytatywne serwery nazw to serwery, które są używane do rozwiązywania zapytań do nazw hostów i określania, które adresy IP powinny być używane do uzyskania dostępu do danego serwera.

1.5.5 MX:

MX wskazuje położenie serwera obsługującego pocztę dla domeny. Poczta przekazywana jest do serwera mającego najwyższy priorytet, jeśli serwer ten nie odpowie, poczta przekazywana jest do serwera backupowego. Rekord MX może wskazywać na nazwę kanoniczną, czyli jako jego wartość wpisujemy nazwę domeny.

Jako przykład podana zostanie konfiguracja rekordów MX dla domeny , której poczta obsługiwana jest na serwerze Google.

1.5.6 SOA:

SOA oznacza początek danych dotyczących domeny. Każda domena może posiadać jeden taki rekord. Znajdziemy w nim takie informacje jak nazwa domeny, mail administratora DNS autorytatywnego dla domeny oraz adres serwerów autorytatywnych. czyli serwera przechowującego konfigurację domeny.

1.5.7 TXT:

TXT pozwala wpisać dowolne informacje tekstowe opisujące domenę. Ostatnio jest on wykorzystywany w systemie anty-spamowych SPF (*Sender Policy Framework*) – w takim przypadku jako wartość domeny wpisujemy adresy, które są uprawnione do wysyłania poczty dla danej domeny.

1.5.8 strefy w których się je umieszcza:

Strefy wyszukiwania do przodu	Strefy wyszukiwania wstecznego
A	PTR
AAAA	NS
SOA	
MX	
CNAME	
TXT	

1.6 Rodzaje zapytań i odpowiedzi na zapytania DNS

1.6.1 Autorytatywne:

dotyczące domeny w strefie, nad którą dany serwer ma zarząd, pochodzą one bezpośrednio z bazy danych serwera; jest to pozytywna odpowiedź zwracana do klienta, która w komunikacie DNS zawiera ustawiony bit uwierzytelniania (AA – *Authoritative Answer*) wskazujący, że odpowiedź została uzyskana z serwera dokonującego bezpośredniego uwierzytelnienia poszukiwanej nazwy

1.6.2 Nieautorytatywne:

dane które zwraca serwer pochodzą spoza zarządzanej przez niego strefy; odpowiedzi nieautorytatywne są buforowane przez serwer przez czas TTL, wyspecyfikowany w odpowiedzi, później są usuwane.

1.7 PowerShell polecenia grupy Add-DnsServer:

1.7.1 Add-DnsServerClientSubnet:

Dodaje podsieć klienta do serwera DNS.

1.7.2 Add-DnsServerConditionalForwarderZone:

Dodaje warunkową usługę przesyłania dalej do serwera DNS.

1.7.3 Add-DnsServerDirectoryPartition:

Tworzy partycję katalogu aplikacji DNS.

1.7.4 Add-DnsServerForwarder:

Dodaje usługi przesyłania dalej na poziomie serwera do serwera DNS.

1.7.5 Add-DnsServerPrimaryZone:

Dodaje strefę podstawową do serwera DNS.

1.7.6 Add-DnsServerQueryResolutonPolicy:

Dodaje zasady rozpoznawania zapytań do serwera DNS.

1.7.7 Add-DnsServerRecursionScope:

Dodaje zakres rekursji na serwerze DNS.

1.7.8 Add-DnsServerResourceRecord:

Dodaje rekord zasobu określonego typu do określonej strefy DNS.

1.7.9 Add-DnsServerResourceRecordA:

Dodaje rekord zasobu typu A do strefy DNS.

1.7.10Add-DnsServerResourceRecordAAAA:

Dodaje rekord zasobu typu AAAA do serwera DNS.

1.7.11Add-DnsServerResourceRecordCName:

Dodaje rekord zasobu typu CNAME do strefy DNS.

1.7.12Add-DnsServerResourceRecordDnsKey:

Dodaje rekord zasobu typu DNSKEY do strefy DNS.

1.7.13Add-DnsServerResourceRecordDS:

Dodaje rekord zasobu typu DS do strefy DNS.

1.7.14Add-DnsServerResourceRecordMX:

Dodaje rekord zasobu MX do serwera DNS.

1.7.15Add-DnsServerResourceRecordPtr:

Dodaje rekord zasobu typu PTR do serwera DNS.

1.7.16Add-DnsServerResponseRateLimitingExceptionlist:

Dodaje listę wyjątków RRL na serwerze DNS.

1.7.17Add-DnsServerRootHint:

Dodaje wskazówki dotyczące serwerów głównych na serwerze DNS.

1.7.18Add-DnsServerSecondaryZone:

Dodaje strefę pomocniczą serwera DNS.

1.7.19Add-DnsServerSigningKey:

Dodaje KSK lub ZSK do podpisanej strefy.

1.7.20Add-DnsServerStubZone:

Dodaje strefę skrótu DNS.

1.7.21Add-DnsServerTrustAnchor:

Dodaje kotwicę zaufania do serwera DNS.

1.7.22Add-DnsServerVirtualizationInstance:

Dodaje instancję wirtualizacji.

1.7.23Add-DnsServerZoneDelegation:

Dodaje nową delegowaną strefę DNS do istniejącej strefy.

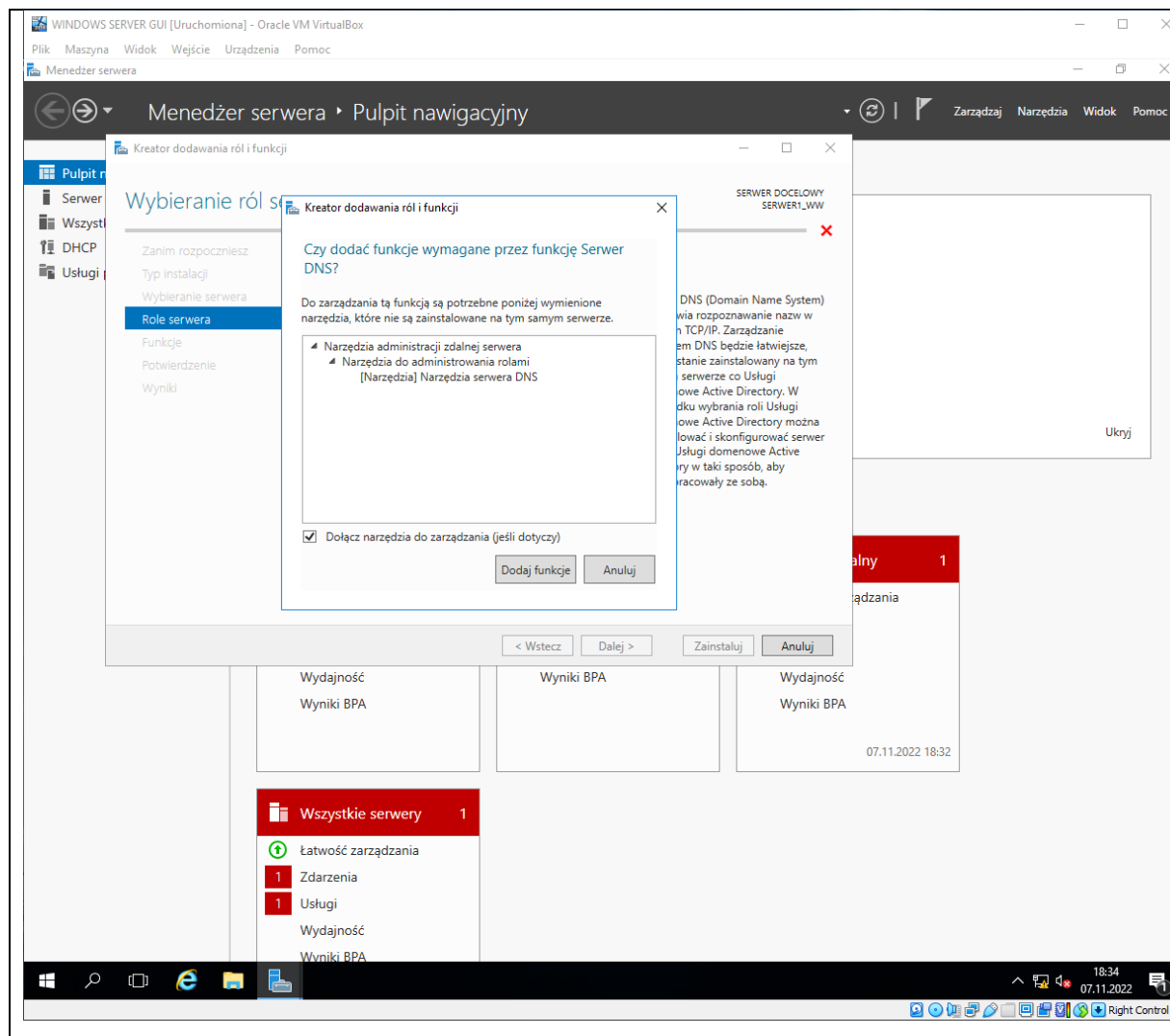
1.7.24Add-DnsServerZoneScope:

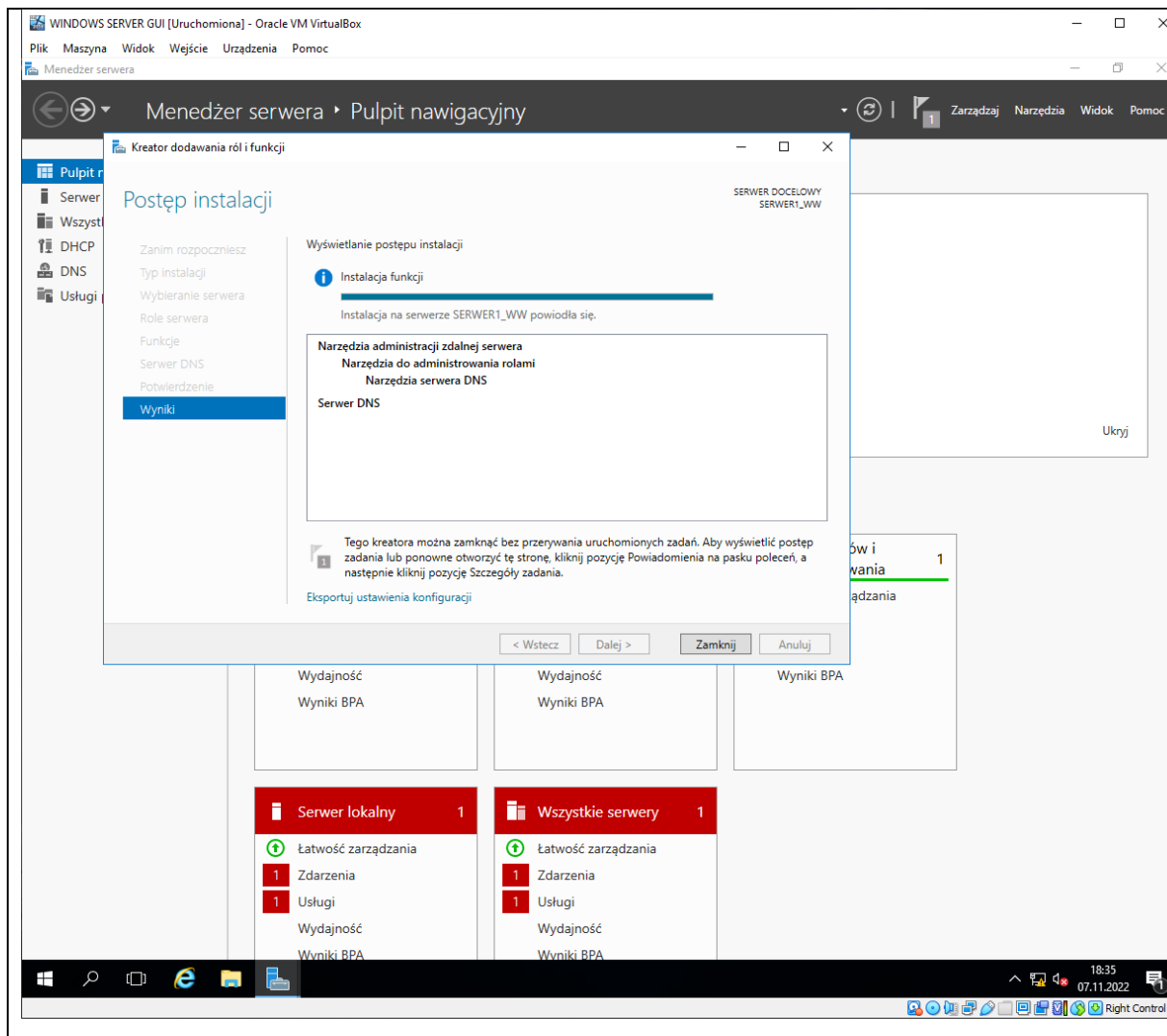
Dodaje zakres strefy do istniejącej strefy.

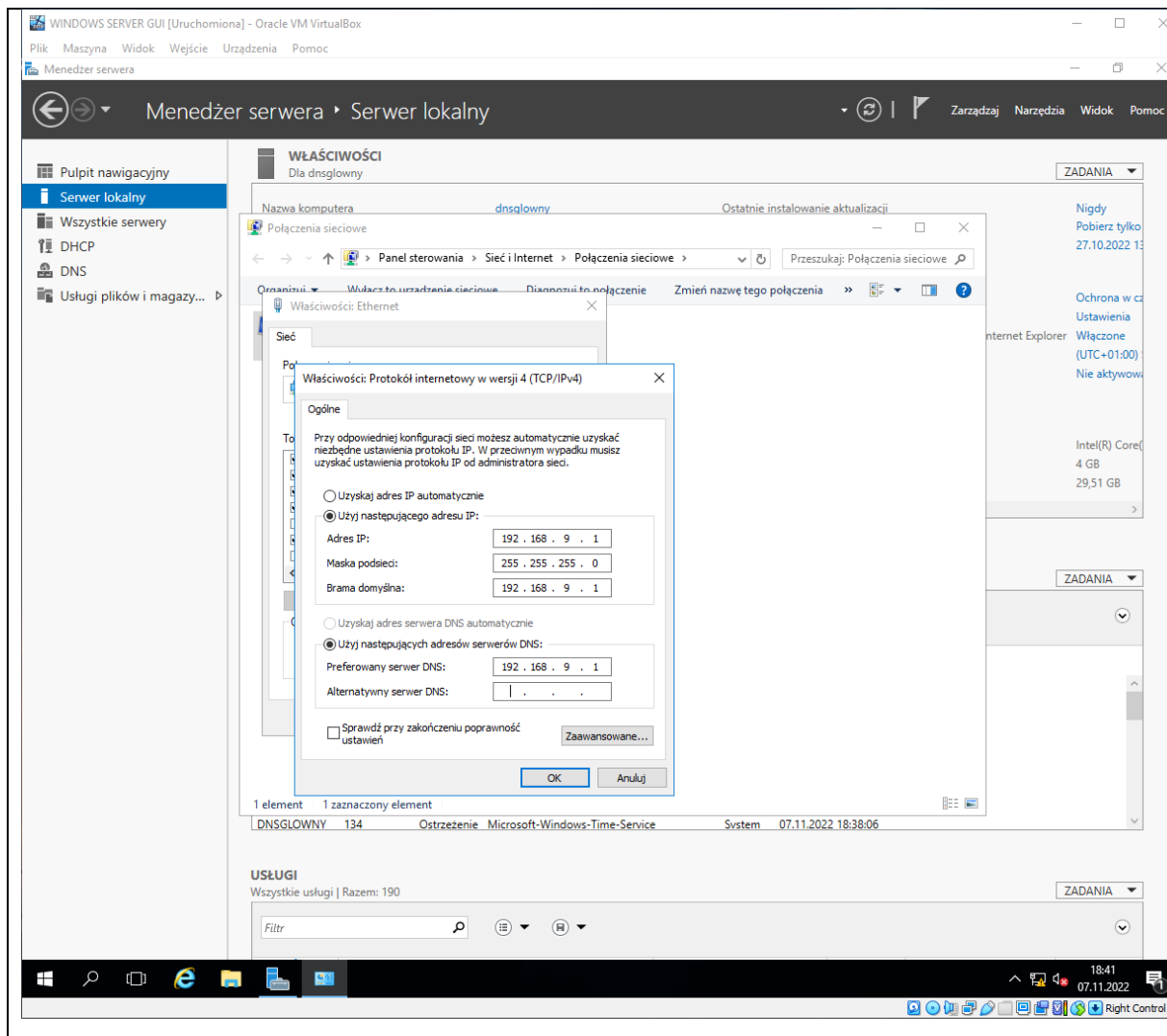
1.7.25Add-DnsServerZoneTransferPolicy:

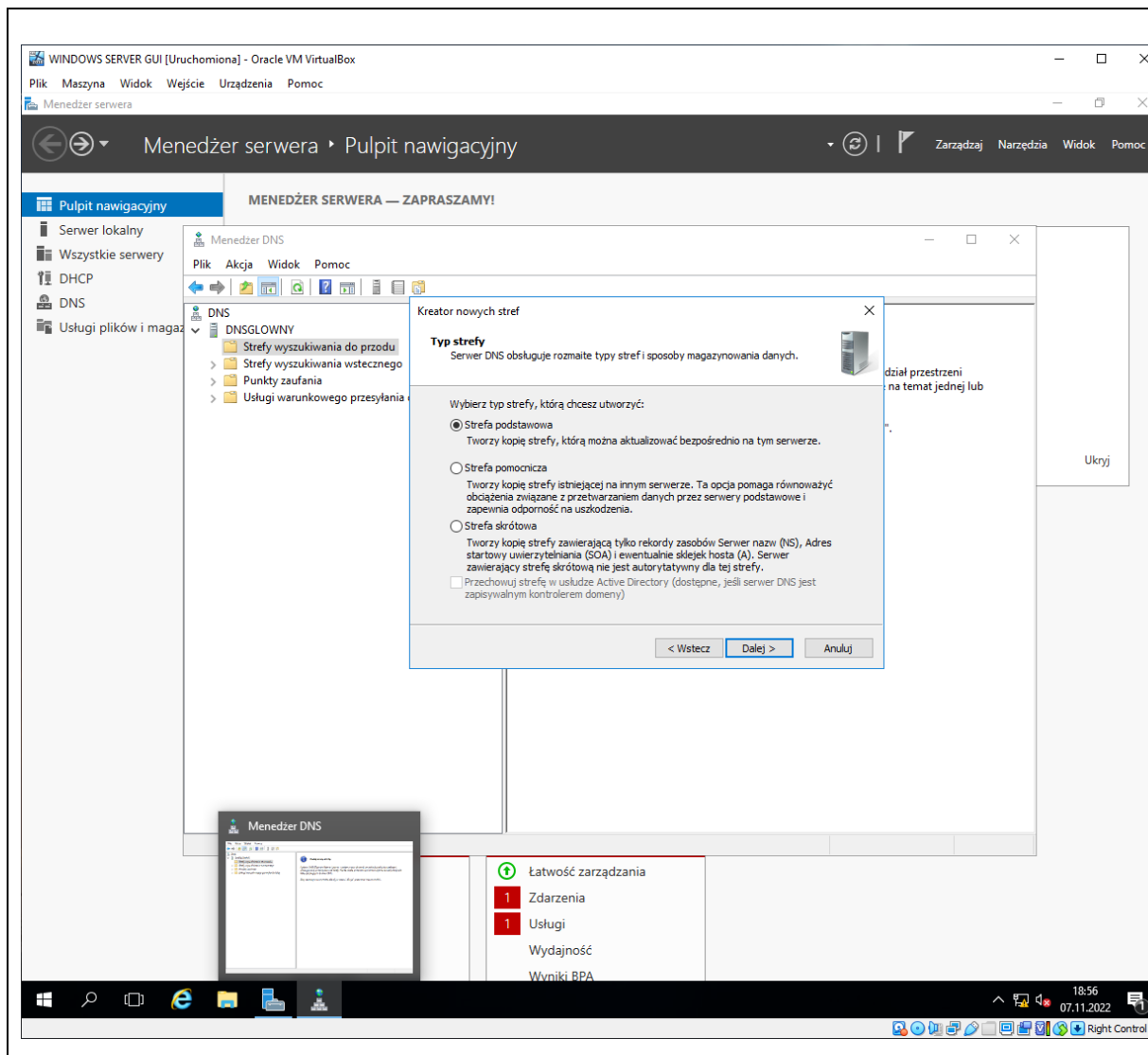
Dodaje zasadę transferu stref do serwera DNS.

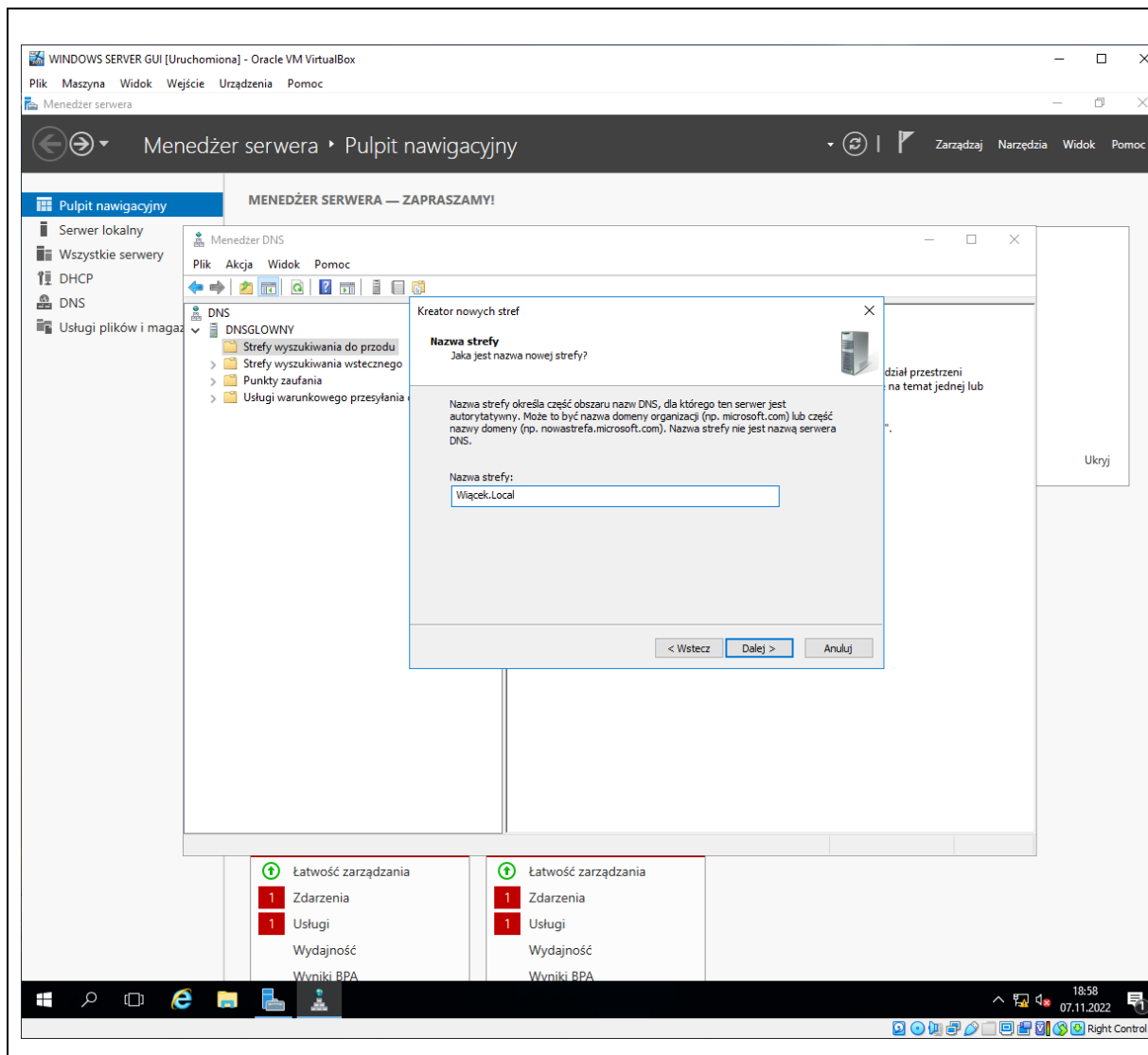
2 Przebieg czynności prowadzący do realizacji zadania

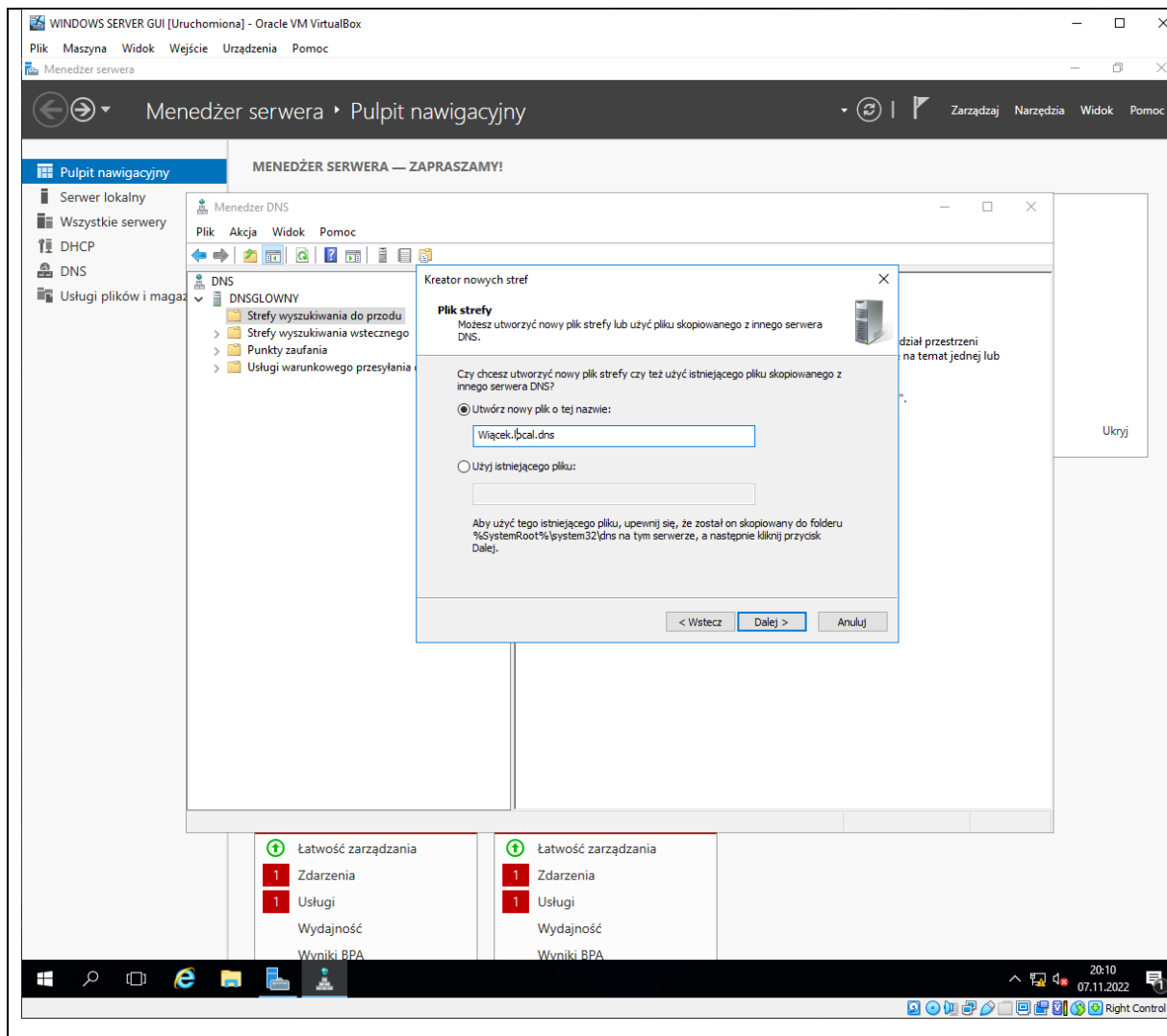


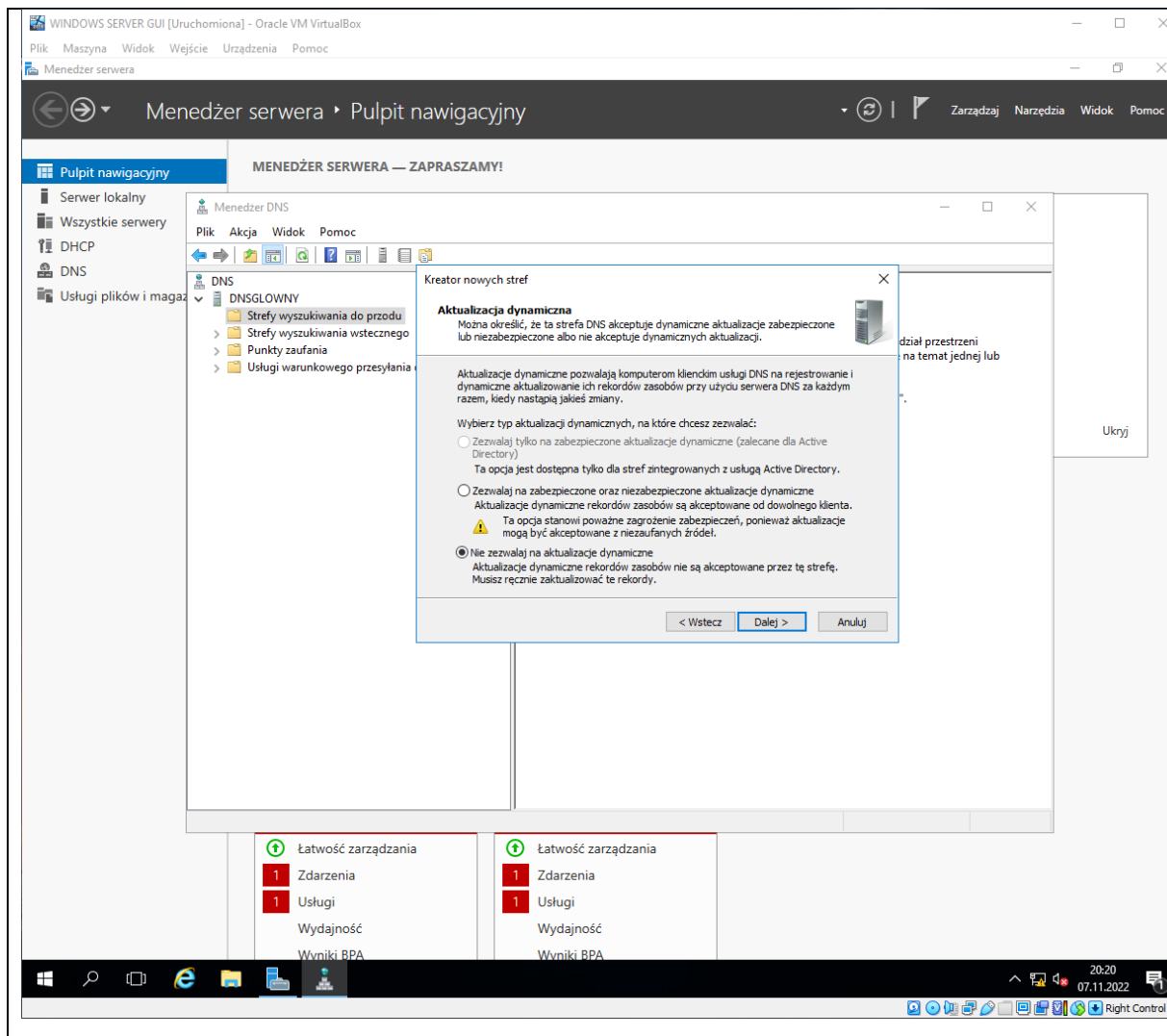


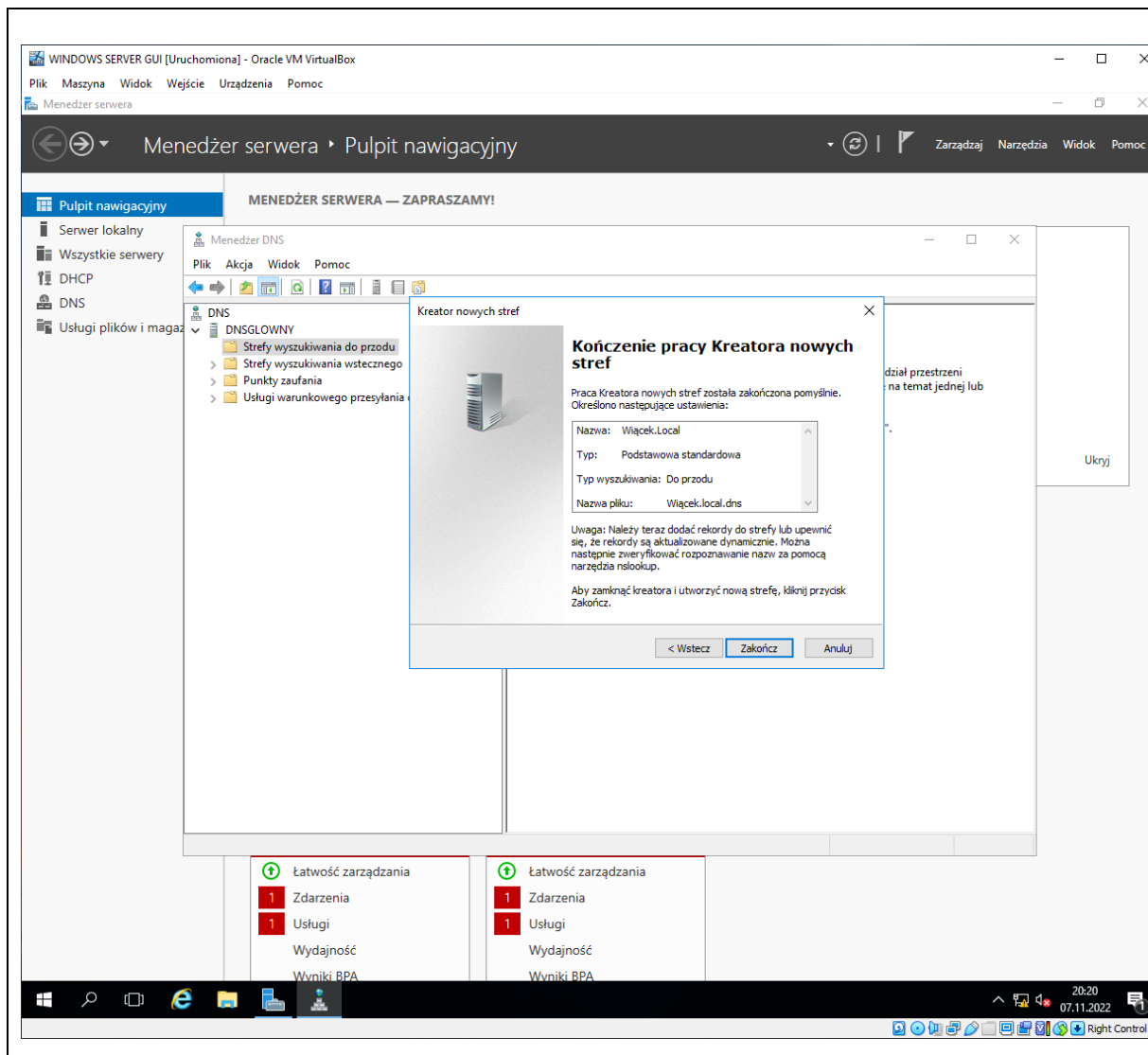


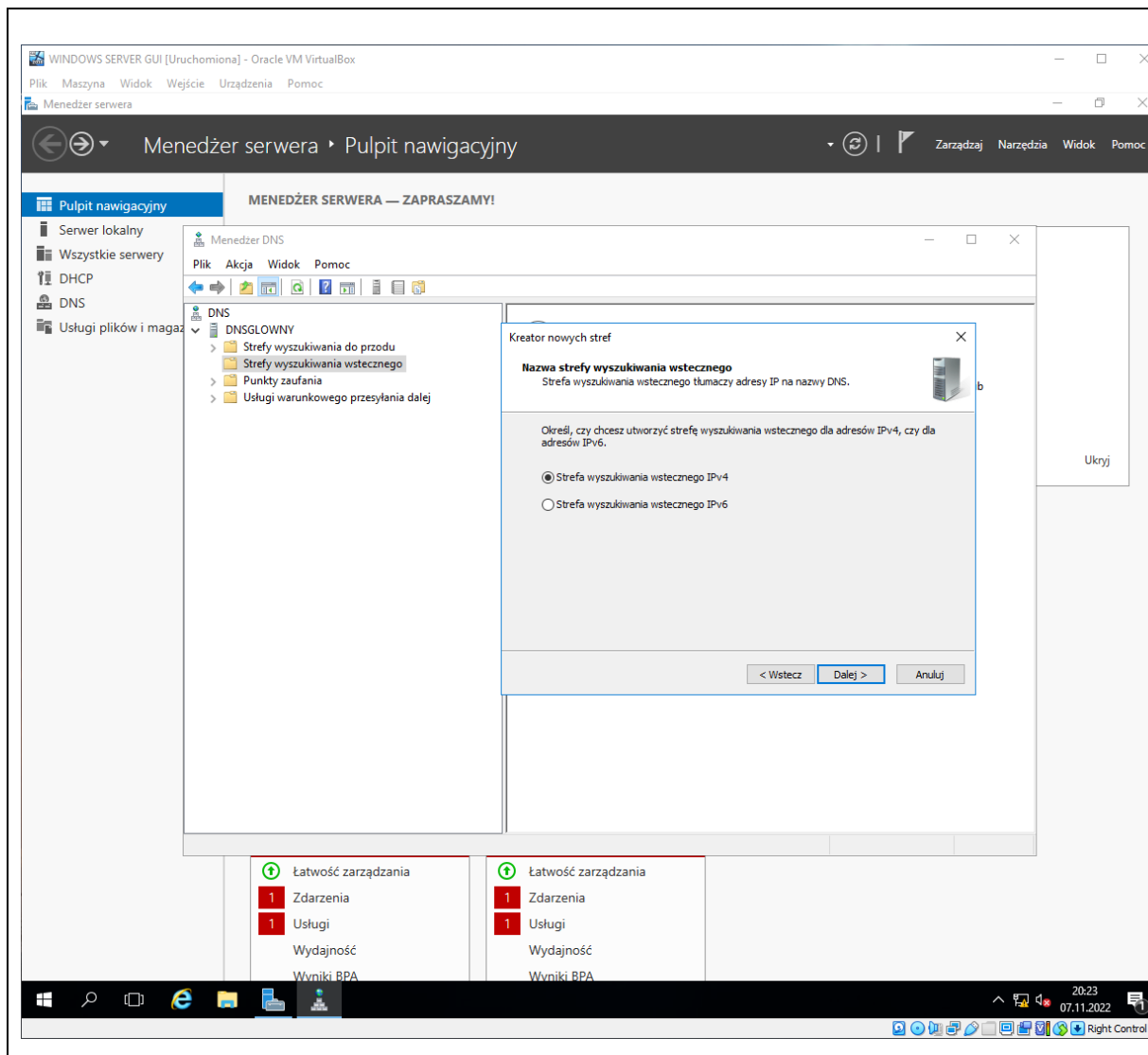


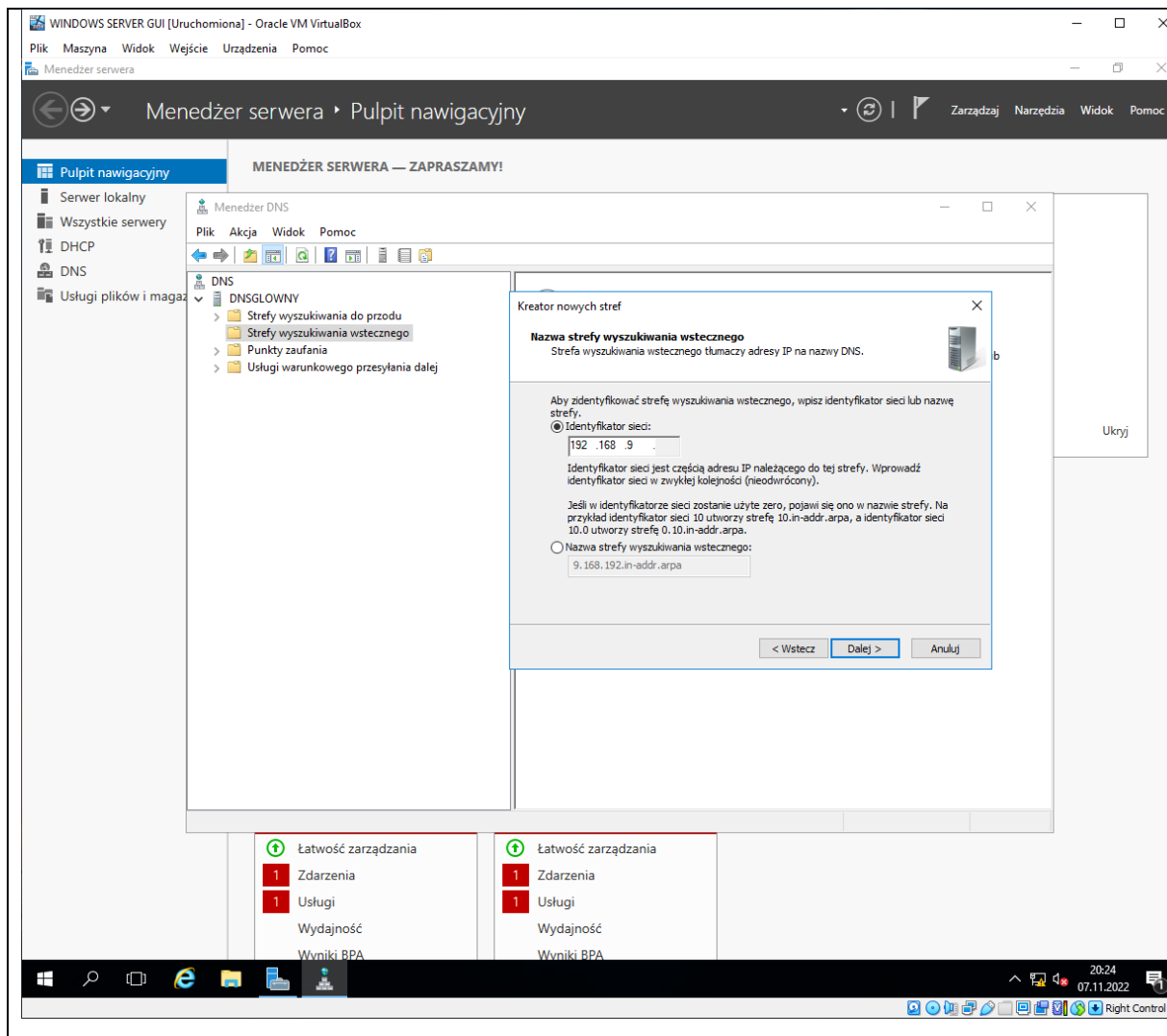


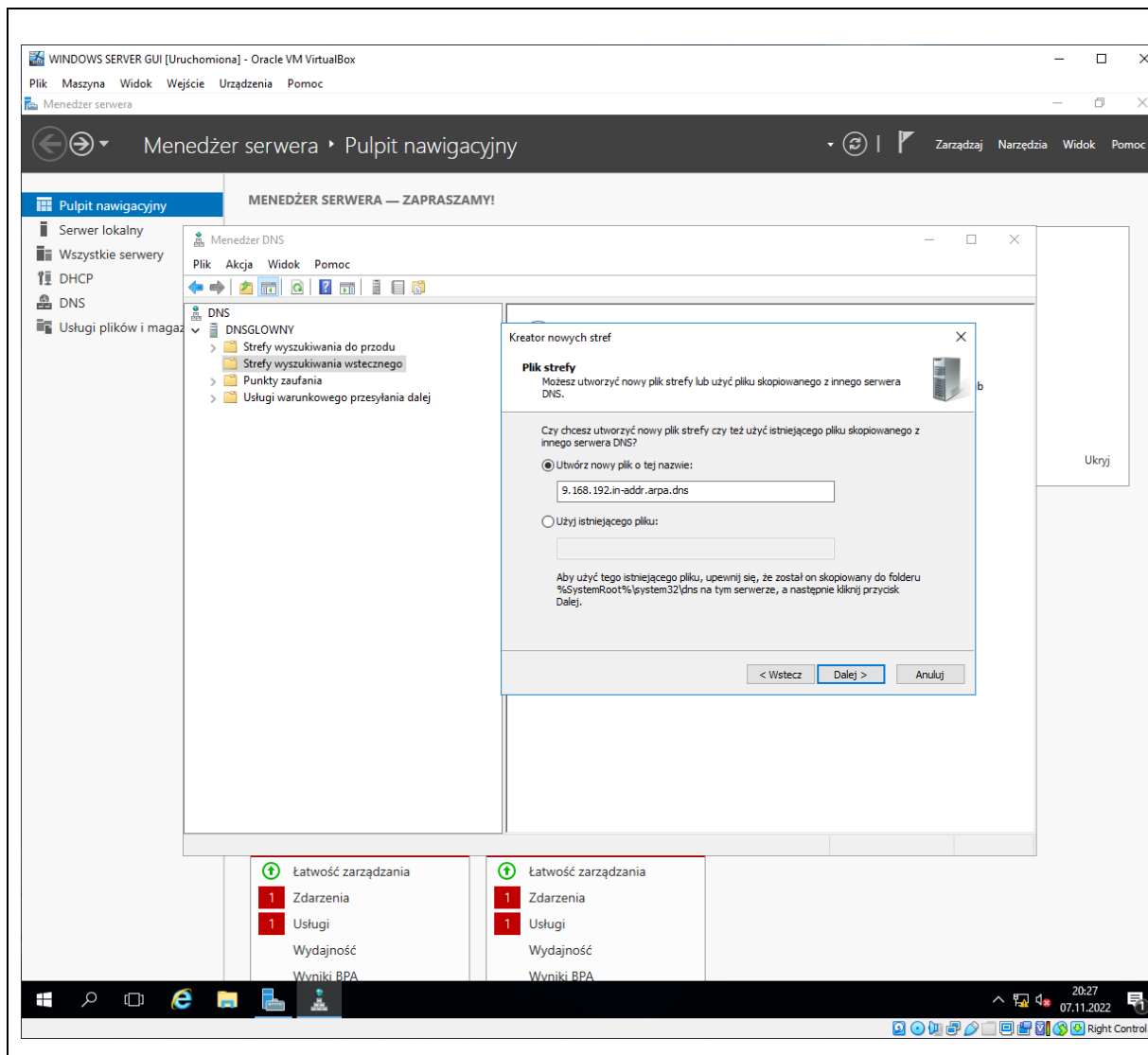


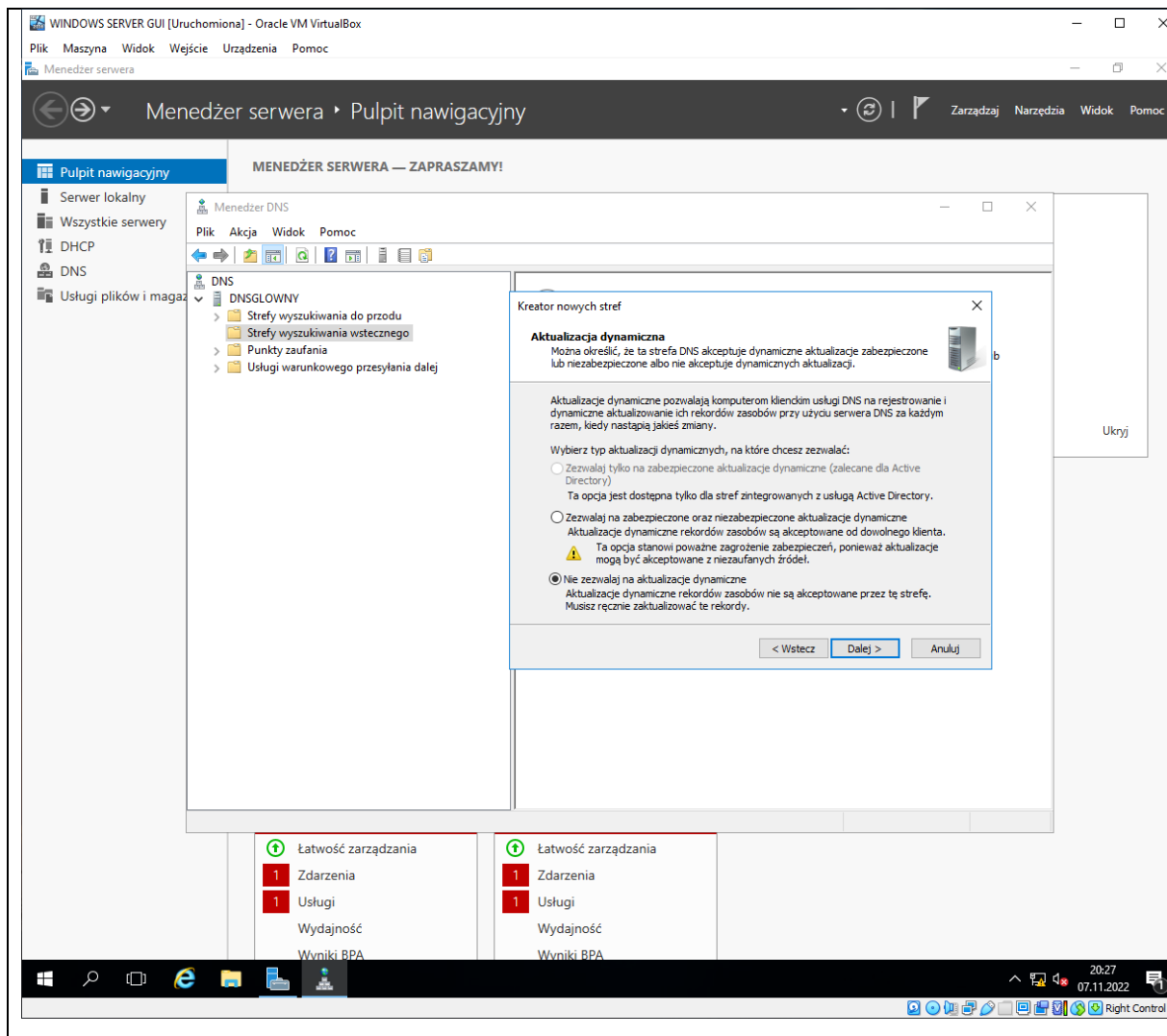


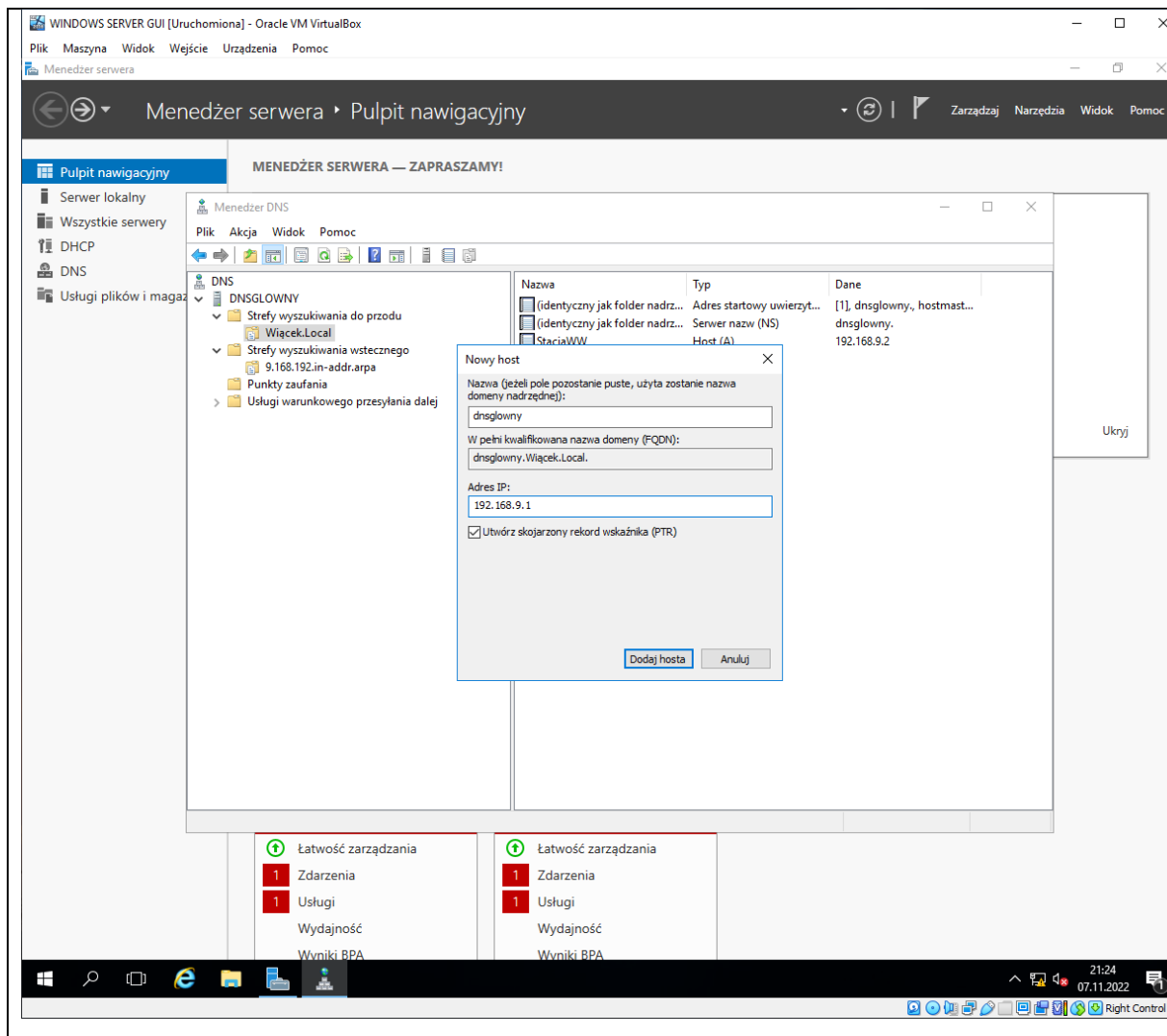


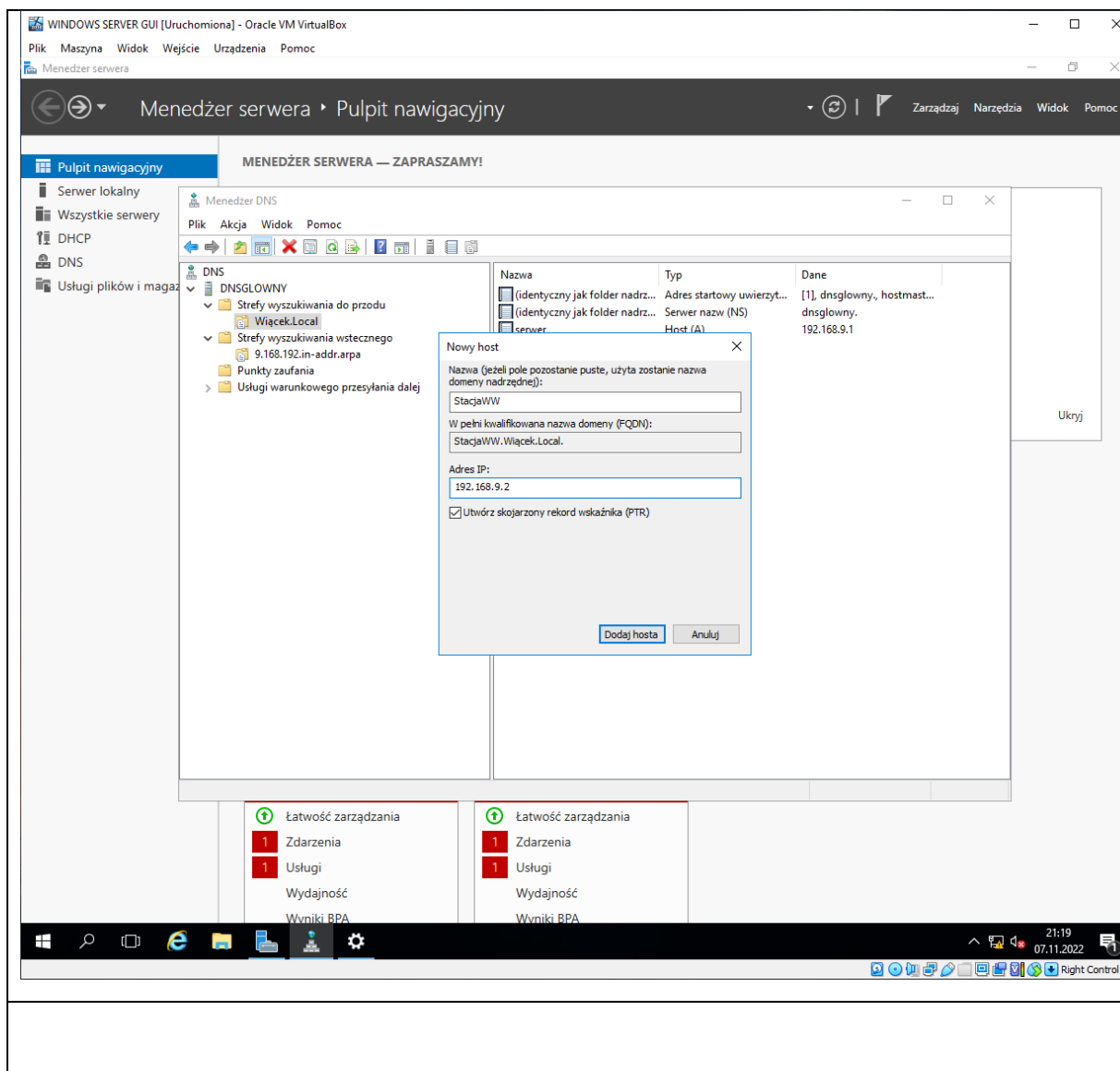


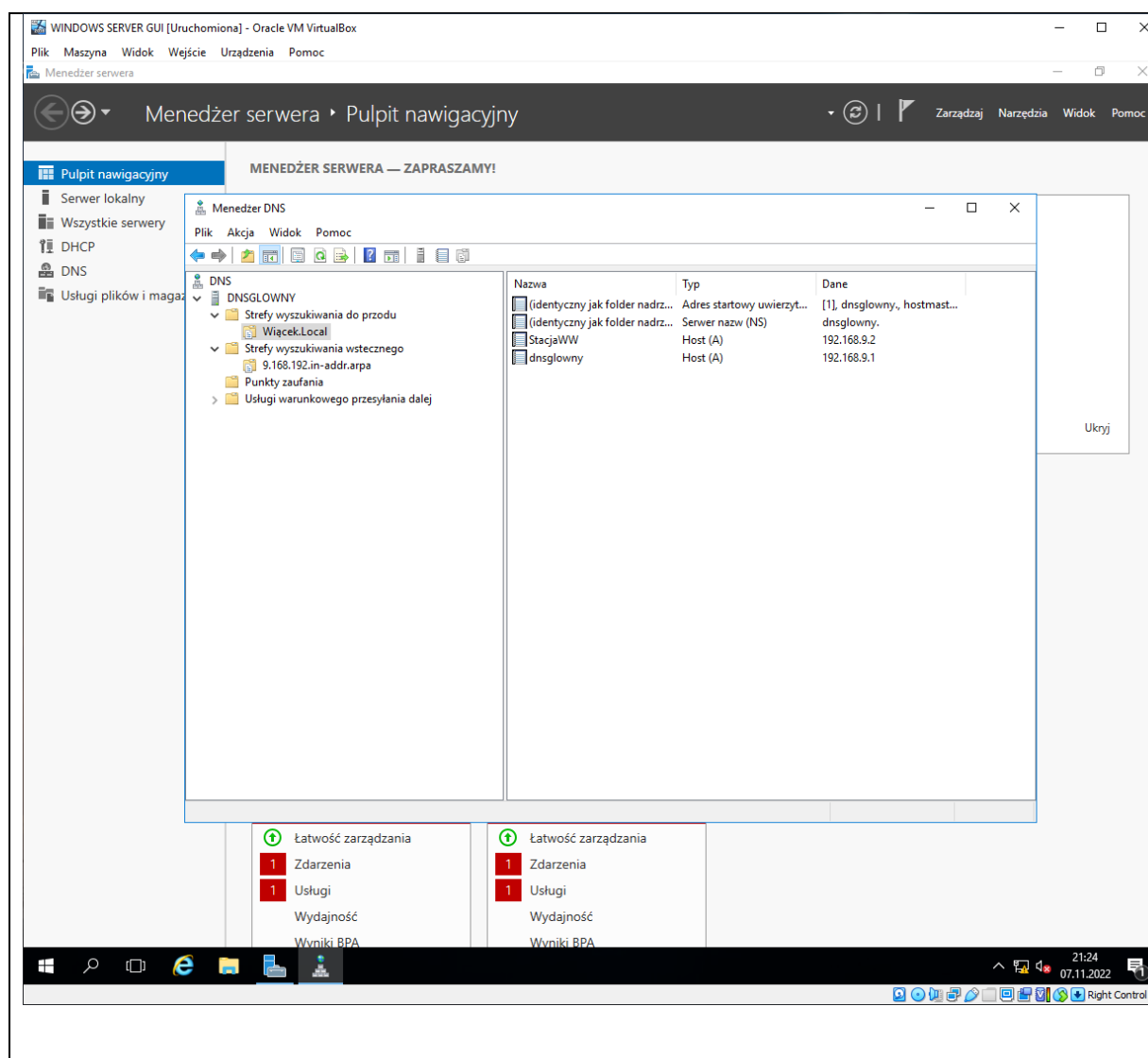


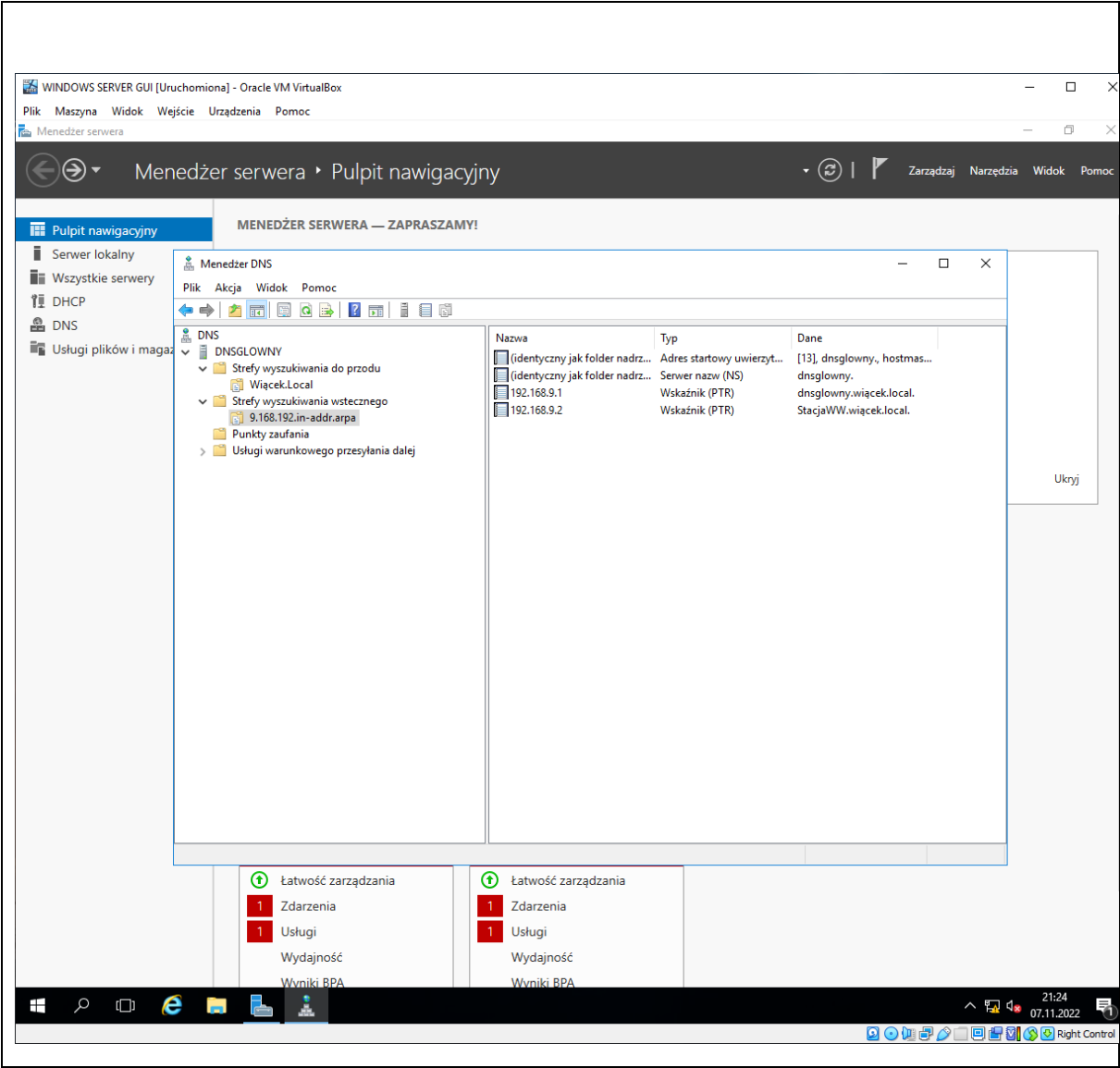


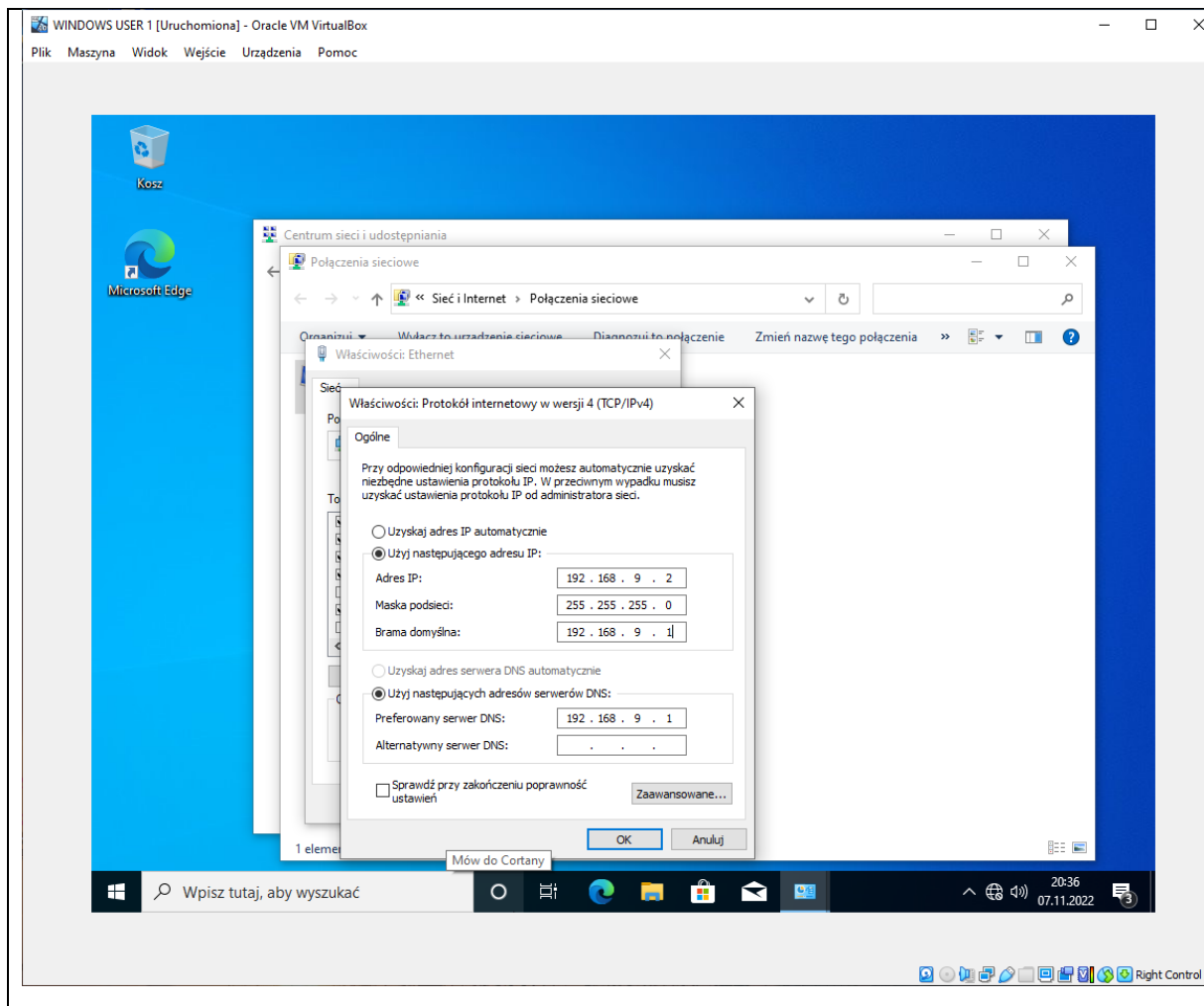


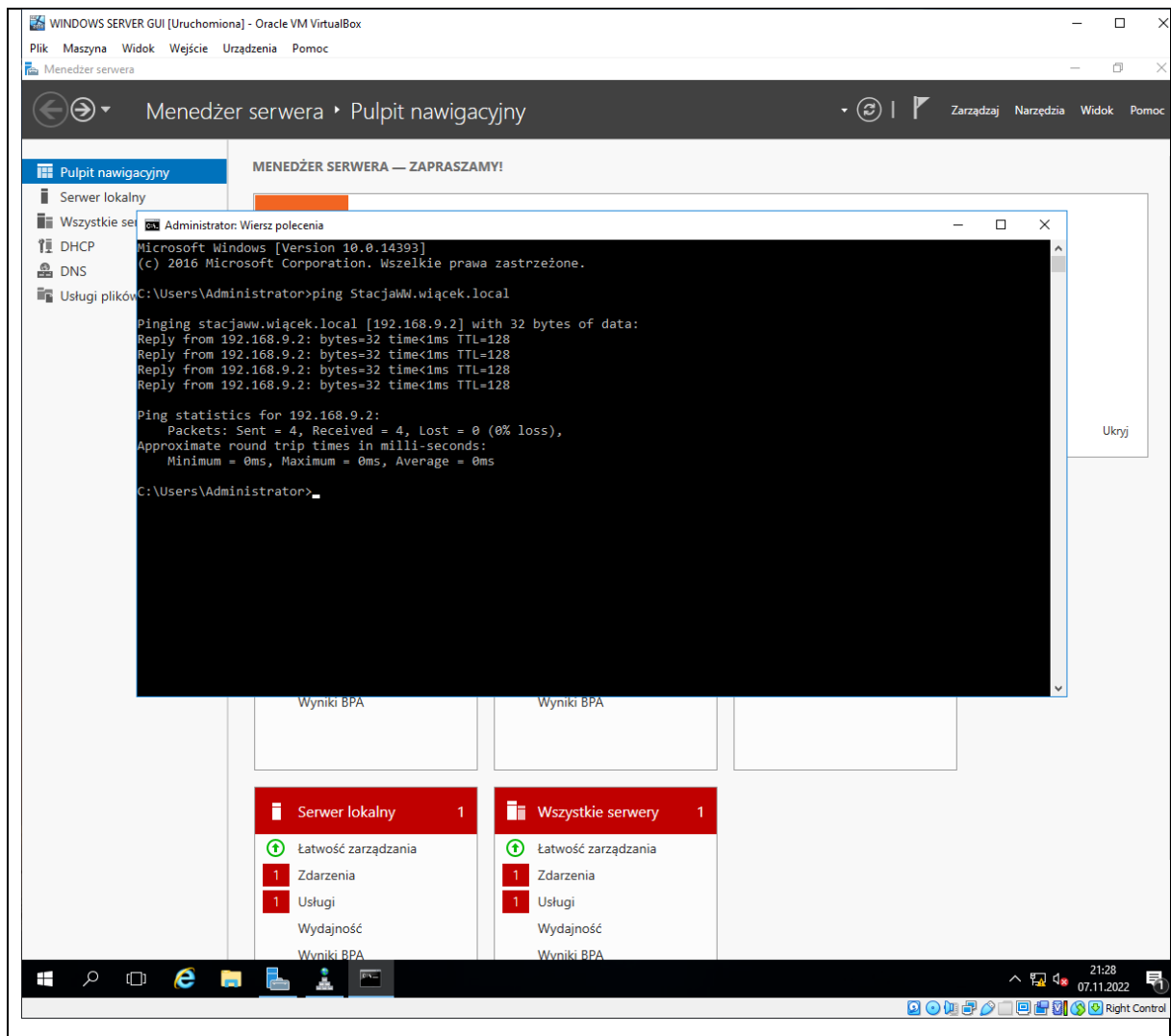


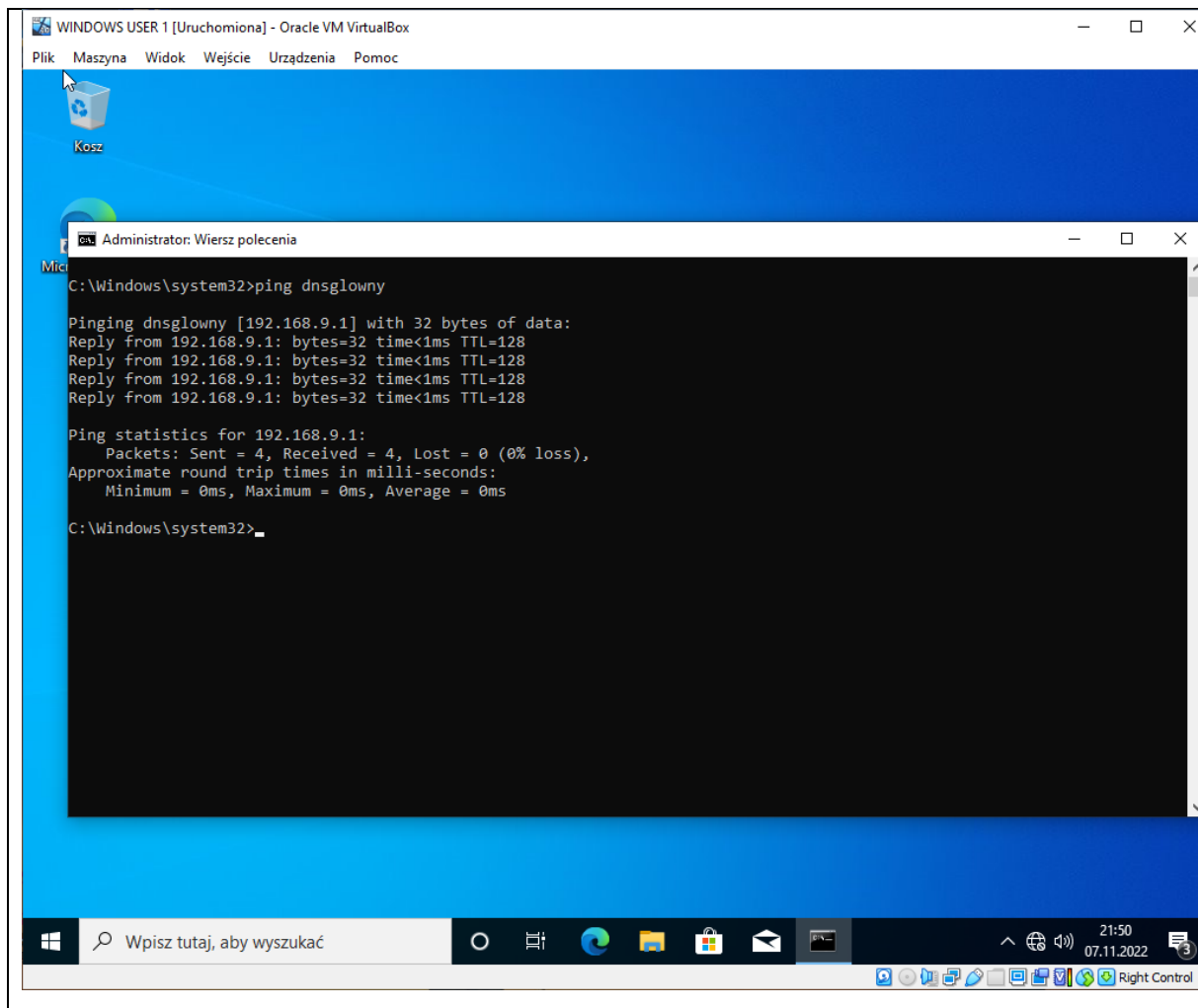


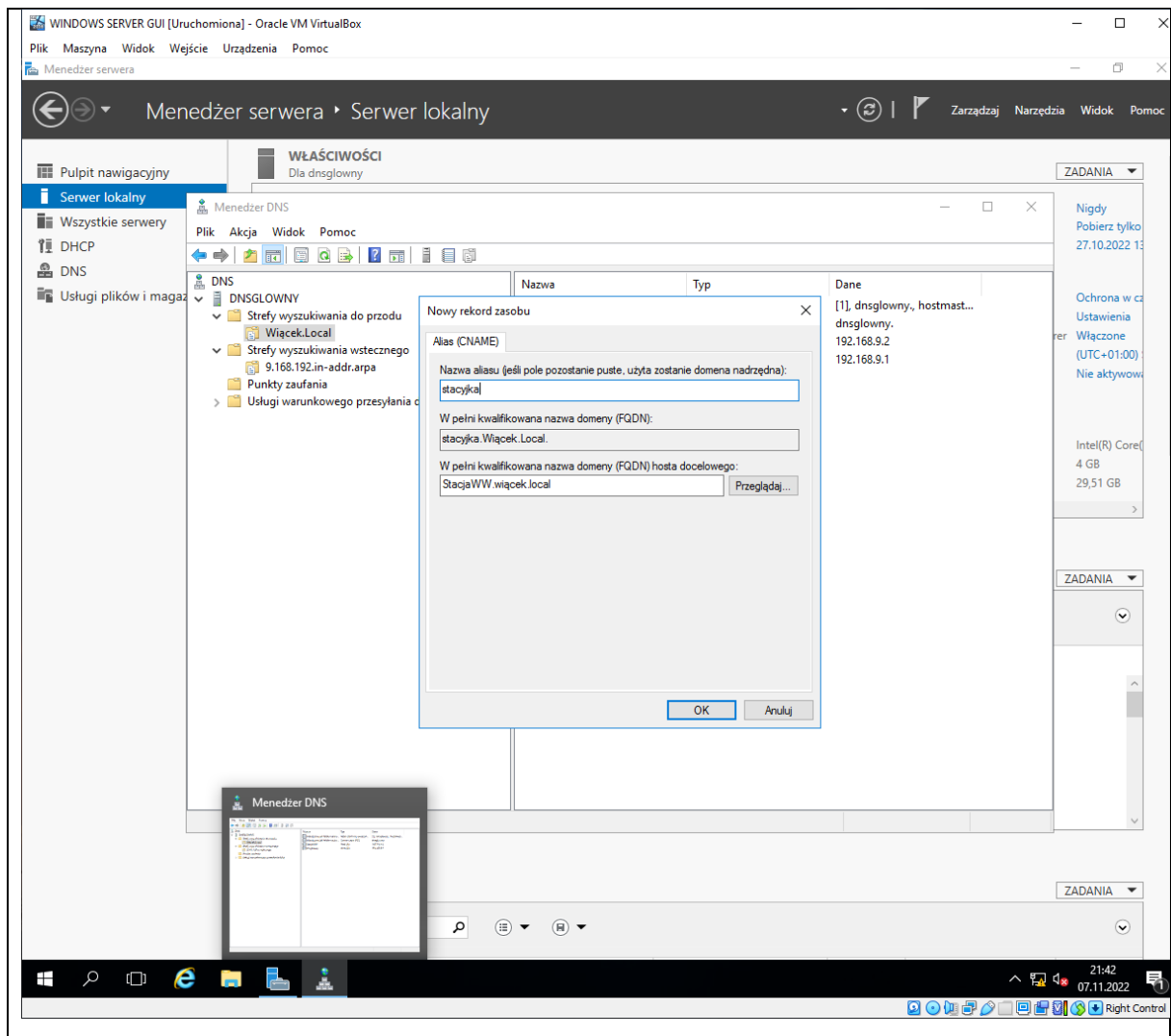


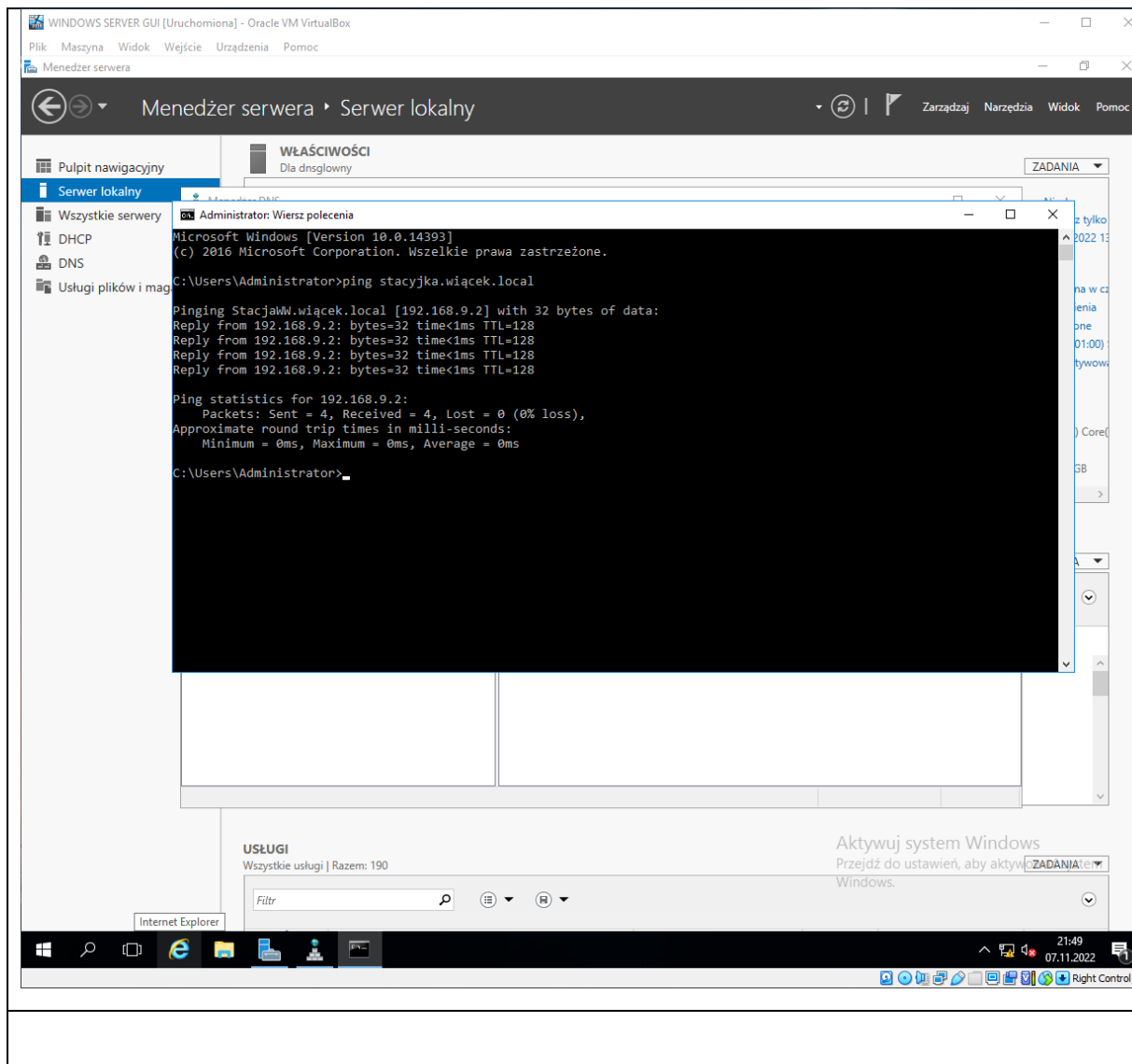












3 Wnioski

Tworząc serwer DNS poszerzyłem swoją wiedzę o teoretyczne pojęcia roli, typów, rekordów, przestrzeni nazw, jak zbudowany jest serwer DNS oraz comandletów wykorzystywanych w Powershellu w celu utworzenia i skonfigurowania serwera nazw domenowych.

Po wykonanym zadaniu praktycznym jestem w stanie stwierdzić że dam rade samodzielnie stworzyć i skonfigurować serwer DNS dostosowując go do potrzeb własnych lub klienta.