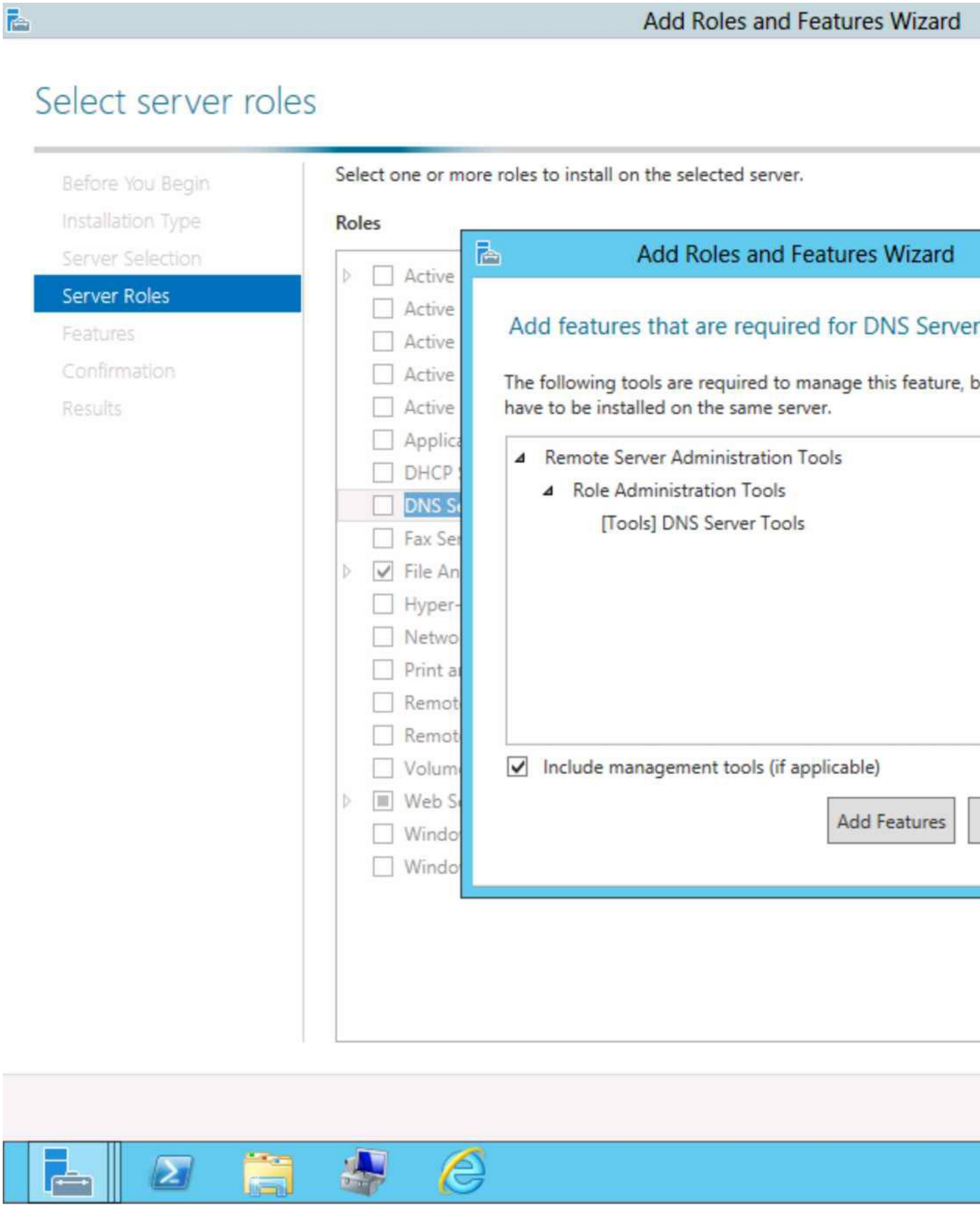
КАК - DNS - Domain Name System

DNS - Domain Name System. Одна из важнейших используемых ролей, отвечающих за сопоставление доменных имён IP адресам. С внедрением IPv6 её значимость ещё значительнее увеличивается. ДНС сервера делятся на кеширующие, перенаправляющие запросы и авторитарные. ДНС сервера, которым делегированы доменные зоны являются авторитарными, в противном случае вы получите Non-authoritative answer от nslookup. Настройка и управление ДНС на самом деле не является сложным делом. Однако, часто на форумах появляются темы о восстановление работы Active Directory, с которой ДНС сильно взаимосвязанны. Причинами некорректной работы Active Directory во многих случаях является "настройка"

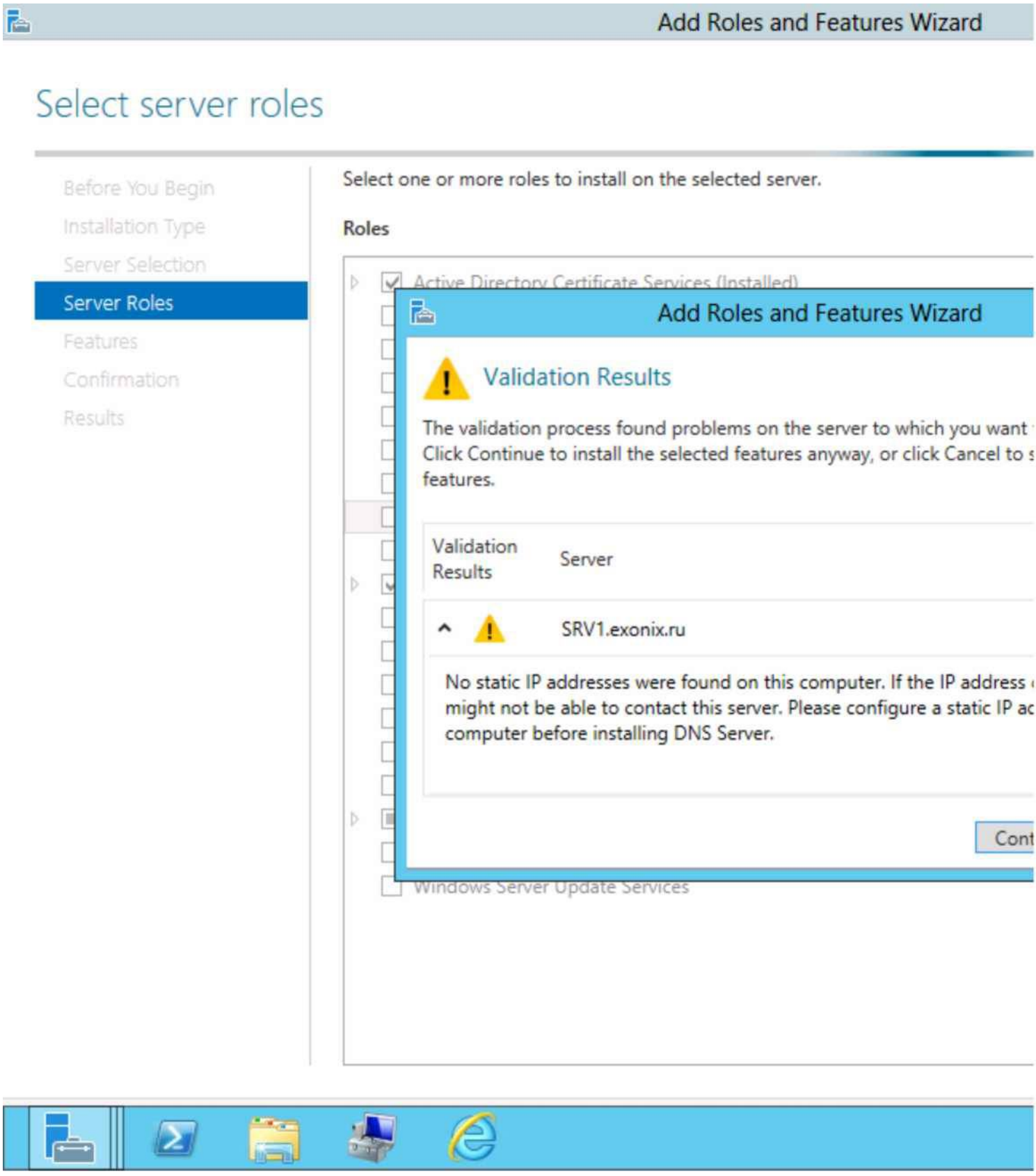
ДНС.
Немного истории операционных систем. В Windows Server 2003 необходимо (я рекомендую) выбирать и AD и ДНС. Я не знаю почему, но очень часто администраторы устанавливают сначала ДНС, настраивают и только потом устанавливают AD. Никогда так не поступал, а всегда устанавливал ДНС вместе с AD. У знакомого недавно был случай, когда он решил настроить второй контроллер домена, но по незнанию ДНС устанавливать не стал. Через некоторое время первый (по порядку) контроллер домена сломался, ну и ДНС вмести с ним. Восстановить контроллер домена не удалось. Вот они как-то и работали на втором контроллере домена без ДНС. В итоге пришлось устанавливать новый домен и импортировать пользователей. Не мигировать, а именно экспортировать и импортировать, так как для миграции нужны доверительные отношения, которым нужен кто? Правильно - ДНС.

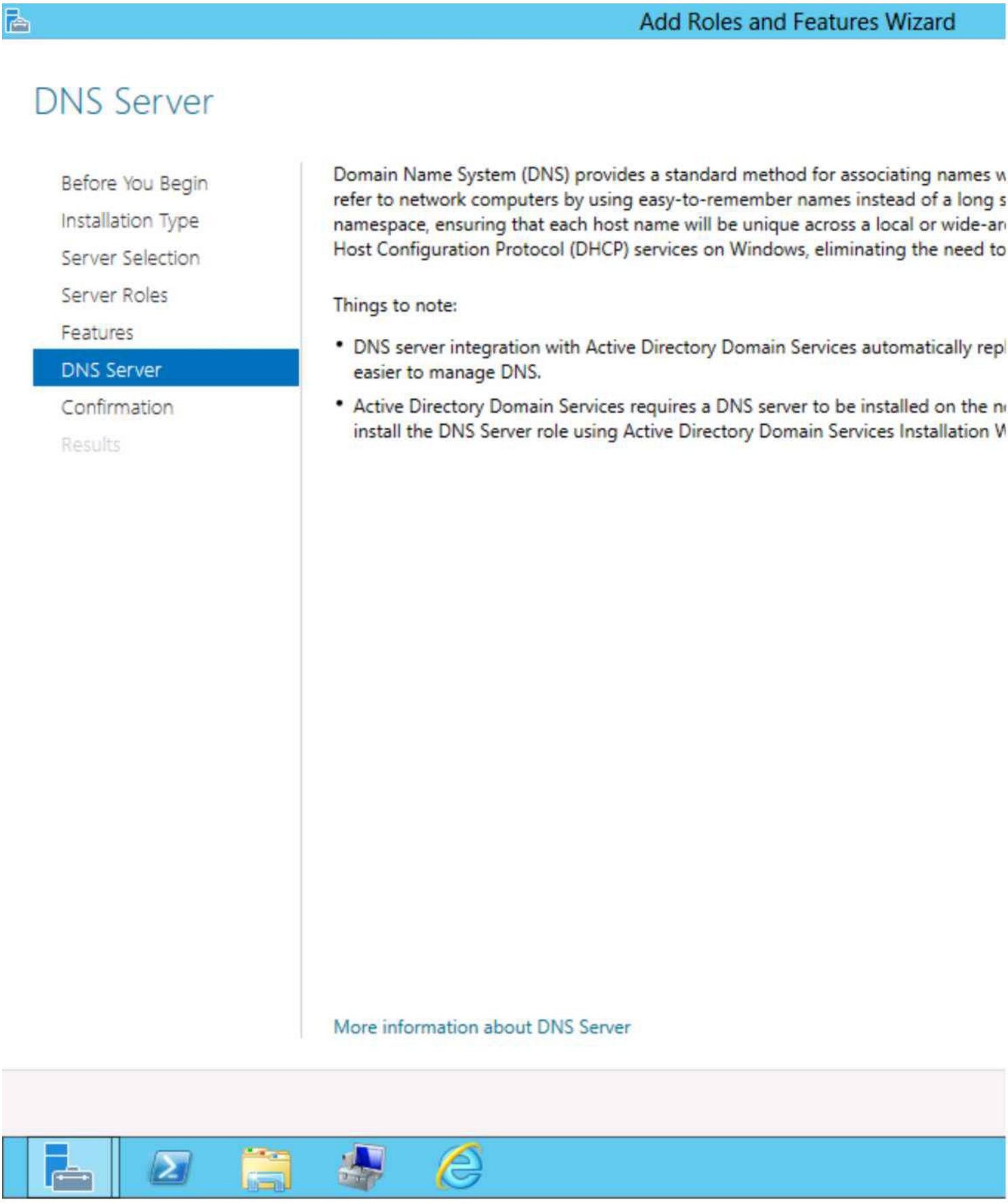
Конечно, бывают случаи когда ДНС нужен без AD, но через некоторое время компания может развернуть инфраструктуру AD. Вот почему важно планировать инфраструктуру с учётом расширения компании. Мне не приходилось работать с такой организацией. Если компании нужен ДНС для работы с сетью Интернет - я рекомендую использовать ДНС сервера предоставляемые провайдером или открытые ДНС Google, например 8.8.8.8. Если у вас есть веб-сайт я рекомендую использовать платные\бесплатные ДНС хостинговой компании. Так надёжнее.

Начиная с Windows Server 2008 ДНС по умолчанию устанавливается во время настройки AD DS через DCPROMO, и автоматически правильно настраивается. Единственное, что нужно в него будет добавить: *это адреса серверов пересылки (адресаДНС серверов вашего провайдера или Гугла) и Обратную зону.*
Установку роли ДНС 2012 я покажу на примере отдельной установки без AD, а настройку с AD. Если у вас контроллер домена имеет несколько сетевых интерфейсов, то предворительно рекомендую настроить сетевые интерфейсы в соответствии с данной статьёй. А именно - исключить недоменный интерфейс из регистрации в ДНС. Сетевые настройки самого недоменного интерфейса в этом случае не важны. Но бывают случаи (на моей практике это было один раз) когда и в случае отключённой регистрацией указанные ДНС в свойствах недоменной сетевой карты влияли на работу сервера. Ну и чтобы не было споров нужны там ДНС или нет - я не рекомендую использовать контроллеры домена в качестве маршрутизаторов. Если у вас просто Wndows Server 2012 в качестве маршрутизатора, то лично я настраиваю сеть как и на любом "аппаратном" маршрутизаторе, то есть с ДНС во внешнем интерфейсе. Вторая причина моего выбора: в случае отказа доменного ДНС, сам сервер будет использовать внешний ДНС автоматически. Установка начинается в Server Manager:

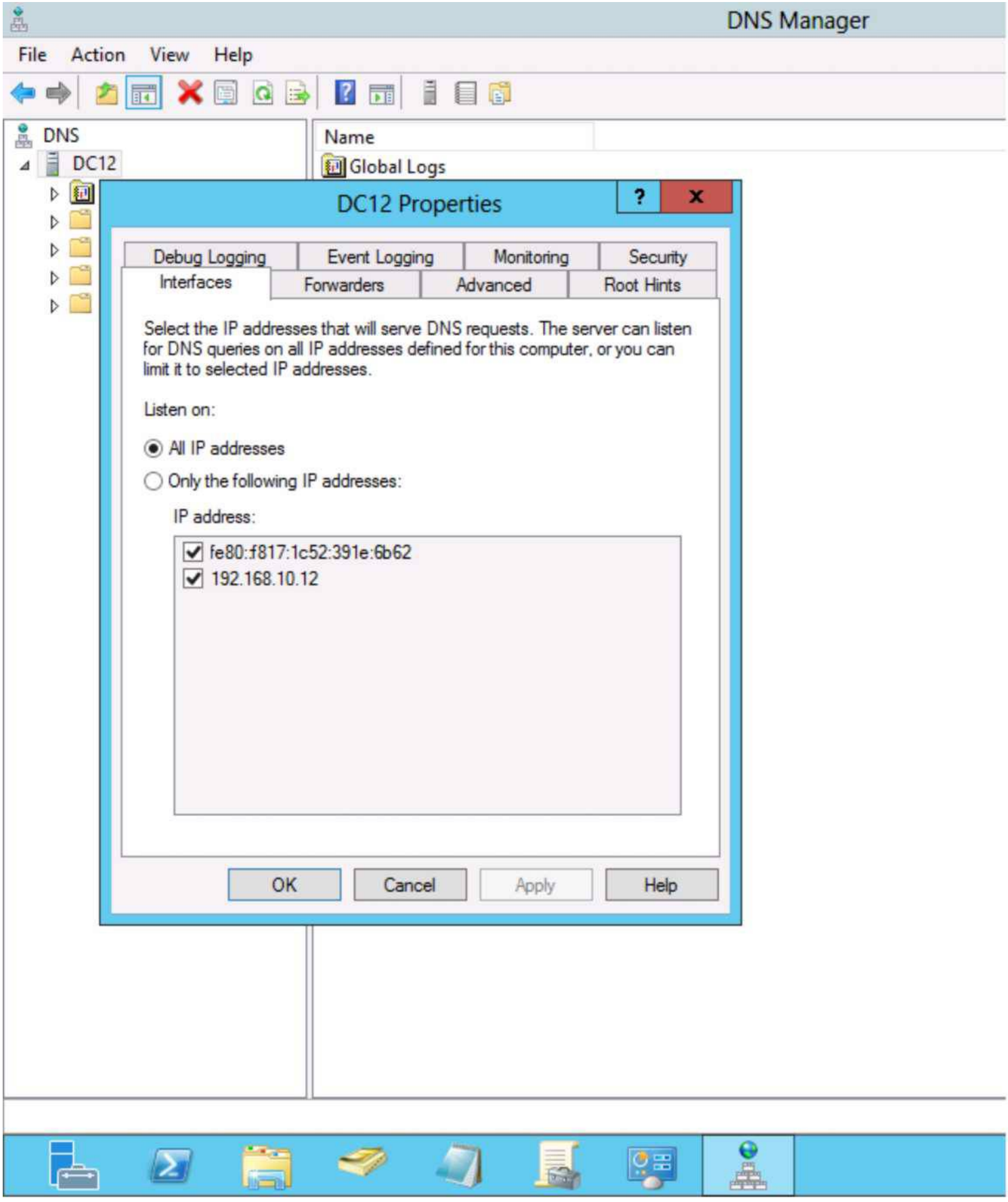


Предупреждение, что у нас не назначен статический IP адрес. Для тестов я позволю себе остаться на динамическом адресе.

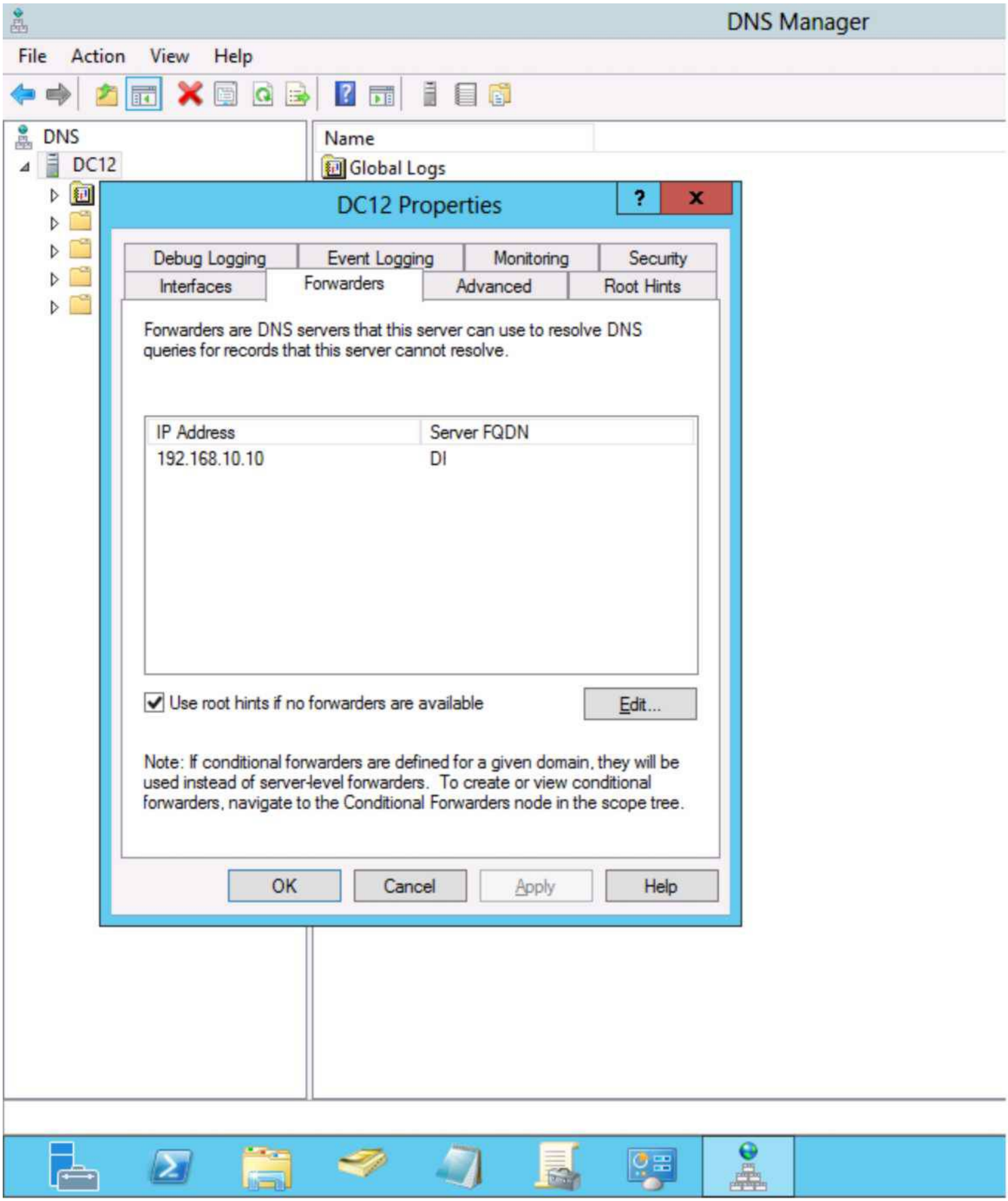

Add Roles and Features Wizard
Select server roles
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services (Installed)
Windows Server Update Services
Add Roles and Features Wizard
Validation Results
The validation process found problems on the server to which you want
Click Continue to install the selected features anyway, or click Cancel to s
features.
Validation Results
Server
SRV1.exonix.ru
No static IP addresses were found on this computer. If the IP address
might not be able to contact this server. Please configure a static IP ac
computer before installing DNS Server.
Cont



Теперь кратко о настройке. В свойствах сервера ДНС, первая вкладка определяет какие интерфейсы будет обслуживать данный ДНС сервер. По умолчанию выделены все.



Forwarders (Адреса пересылки) - здесь указываются вышестоящие ДНС сервера, на которые будет отправлять запросы ваш ДНС сервер, если не обнаружит записи у себя. Как правило это ДНС провайдера или открытые ДНС, например google 8.8.8.8. В примере я указал другой внутренний ДНС сервер.



Некоторые опции ДНС сервера. Если у вас кластер из веб-серверов и одно доменное имя имеет несколько IP адресов, то Round Robin позволяет поочередно выдавать разные IP адреса. Вот пример работы Round Robin:

C:\Users\user>nslookup ya.ru
Server: dc1.domain.local

Address: 192.168.10.10
Non-authoritative answer:
Name: ya.ru
Addresses: 87.250.251.3
93.158.134.3
93.158.134.203
213.180.193.3
213.180.204.3
77.88.21.3
87.250.250.3
87.250.250.203
C:\Users\user>ping ya.ru
Pinging ya.ru [93.158.134.3] with 32 bytes of data:
Reply from 93.158.134.3: bytes=32 time=35ms TTL=53
Reply from 93.158.134.3: bytes=32 time=42ms TTL=249
Reply from 93.158.134.3: bytes=32 time=48ms TTL=53
Reply from 93.158.134.3: bytes=32 time=38ms TTL=53
Ping statistics for 93.158.134.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 35ms, Maximum = 48ms, Average = 40ms

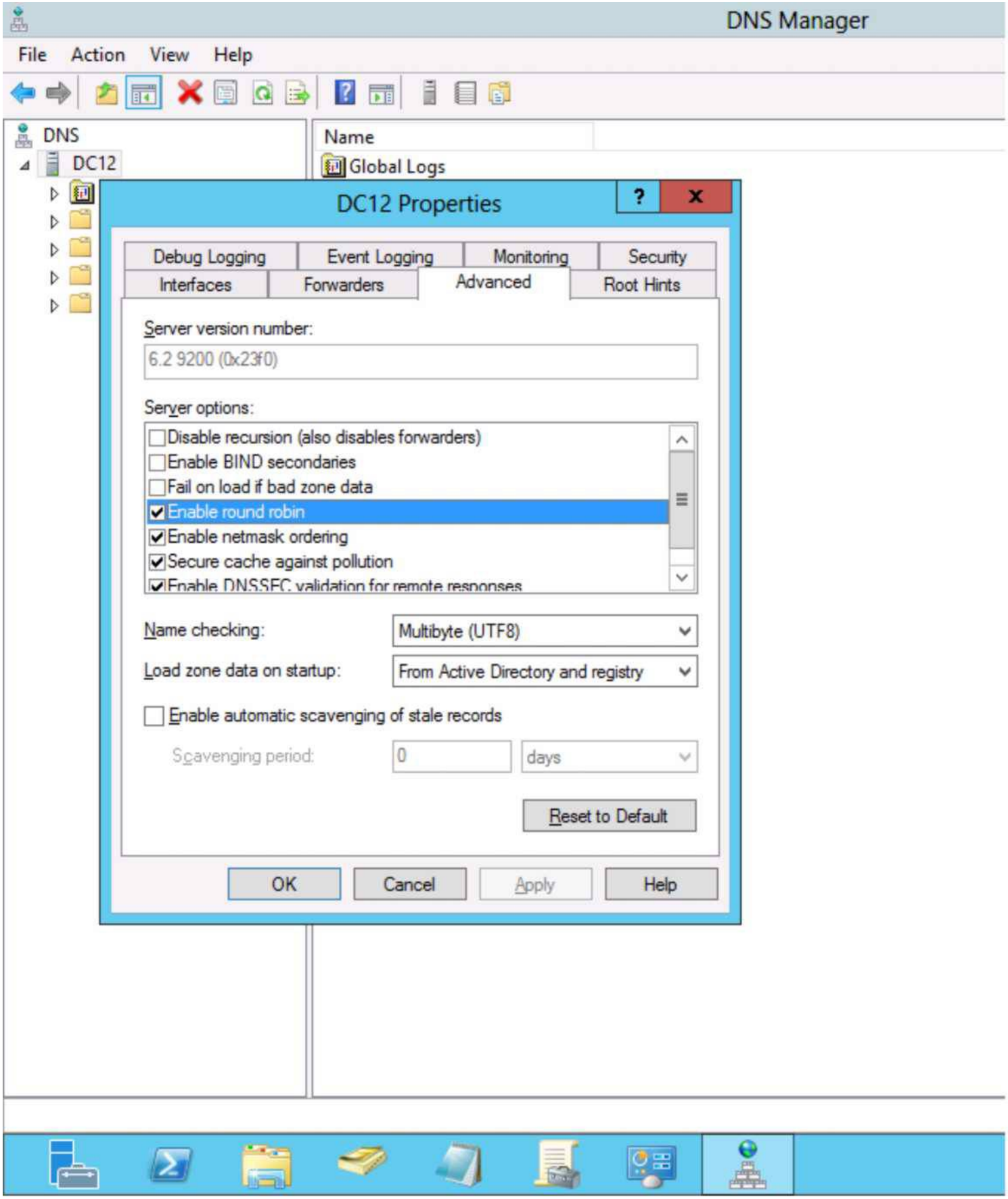
C:\Users\user>ipconfig /flushdns

Windows IP Configuration

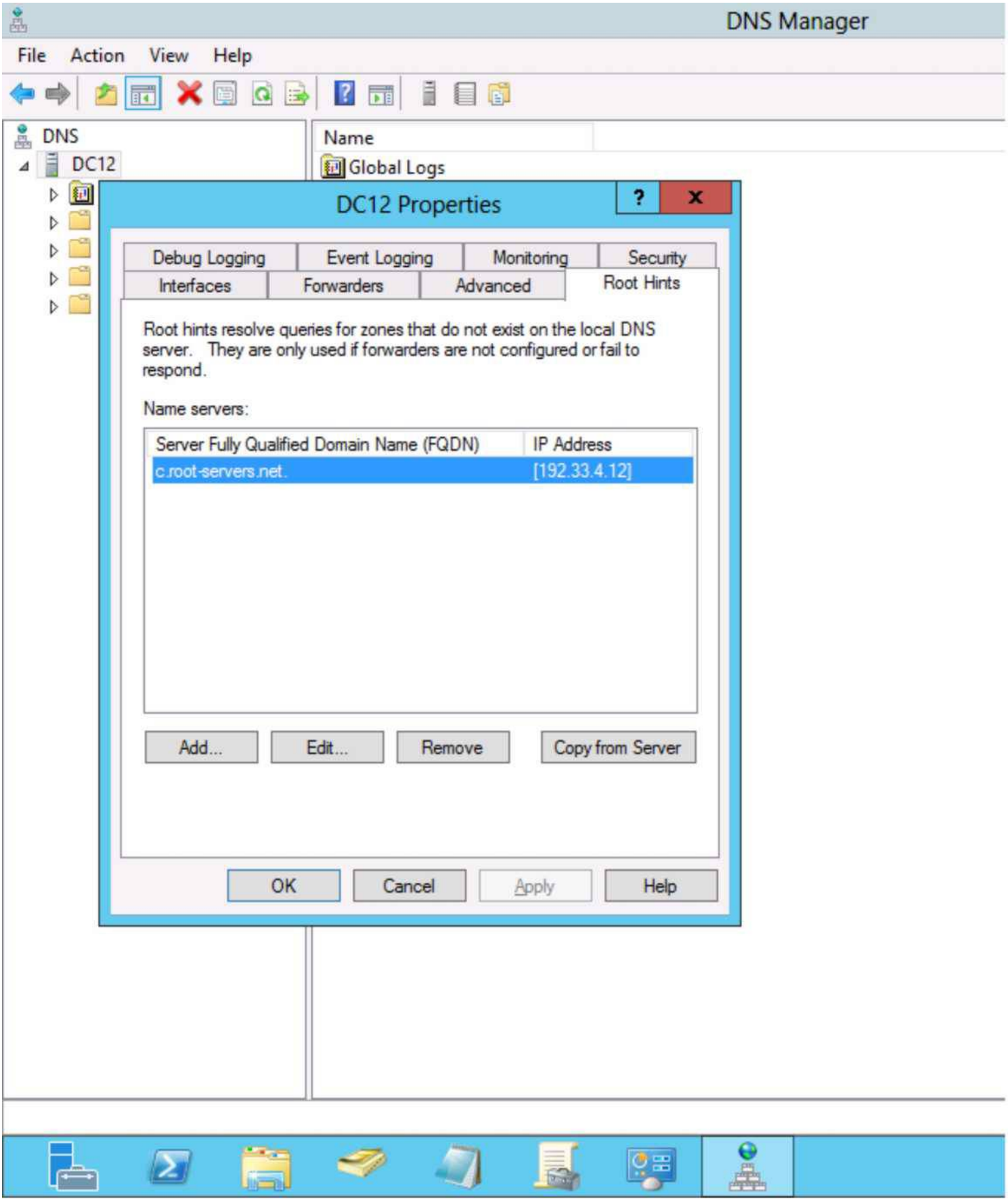
Successfully flushed the DNS Resolver Cache.

C:\Users\user>ping ya.ru

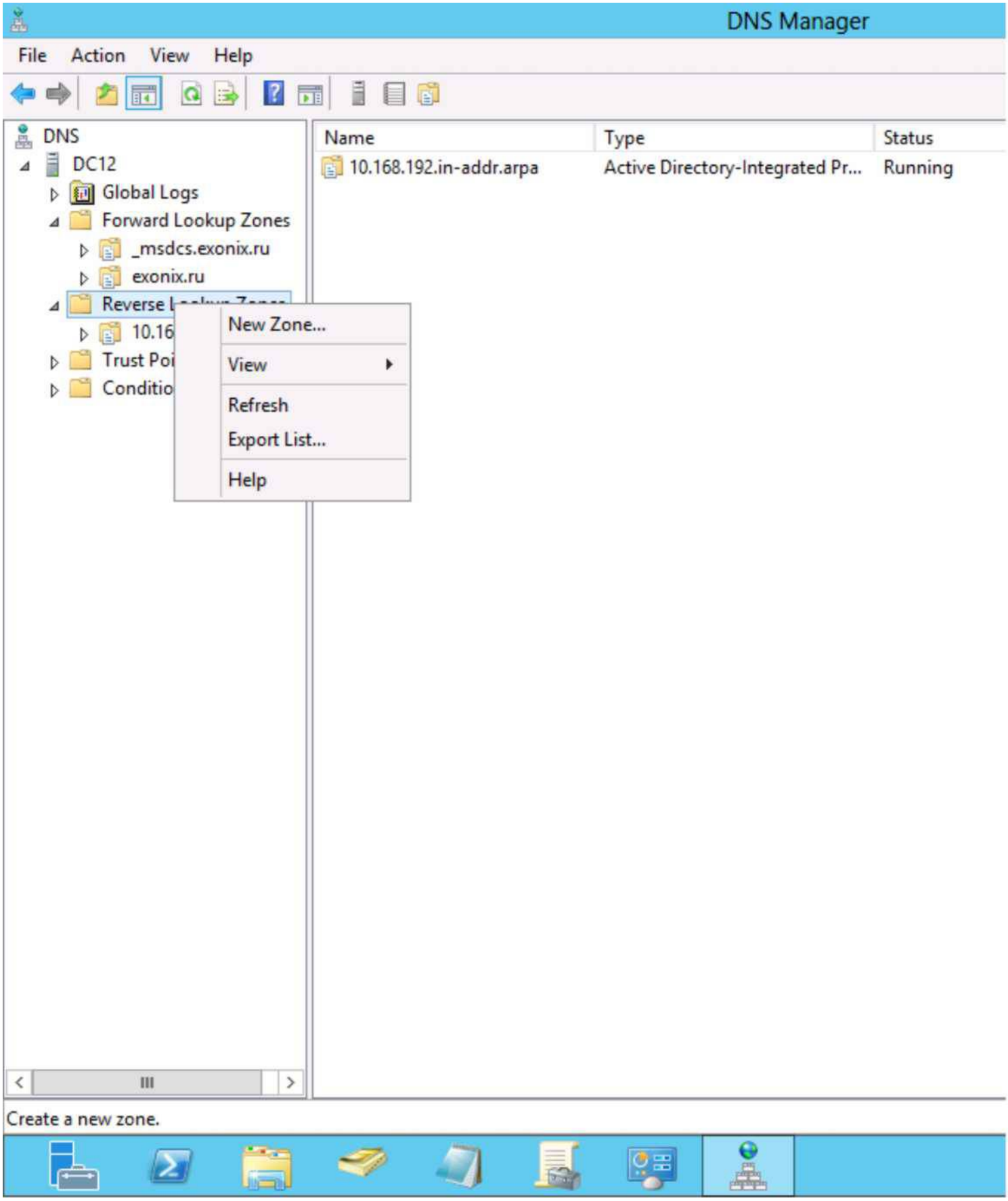
Pinging ya.ru [93.158.134.203] with 32 bytes of data:
Reply from 93.158.134.203: bytes=32 time=41ms TTL=249
Reply from 93.158.134.203: bytes=32 time=43ms TTL=249
Reply from 93.158.134.203: bytes=32 time=36ms TTL=53
Reply from 93.158.134.203: bytes=32 time=40ms TTL=53
Ping statistics for 93.158.134.203:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 36ms, Maximum = 43ms, Average = 40ms

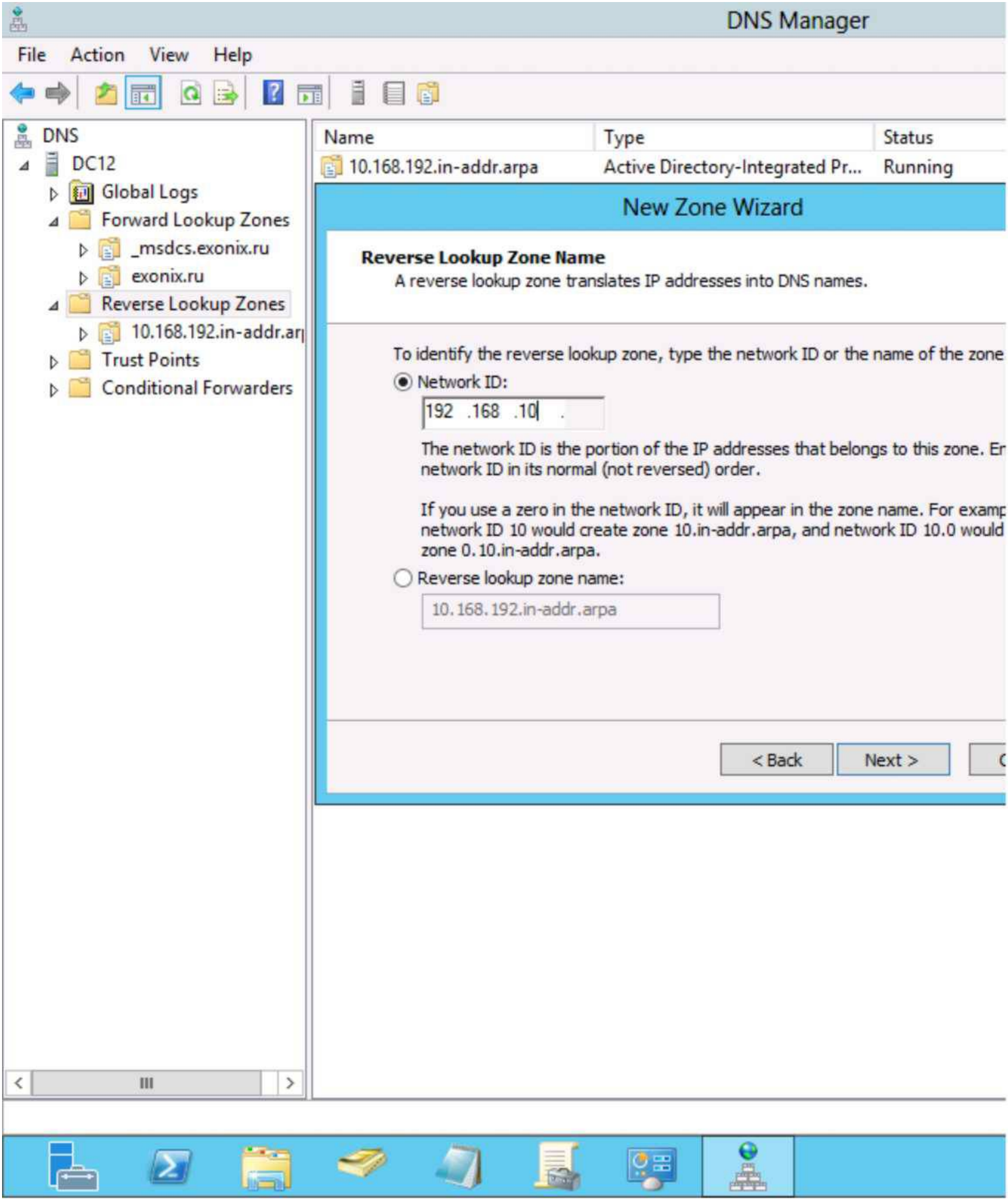


Root Hints - корневые ДНС сервера. Тоже самое что и сервера пересылке, только надёжность намного выше. Подразумевается, что root hints всегда доступны. Почему-то в ДНС 2012 прописан только один корневой сервер, обычно и там около десятка.

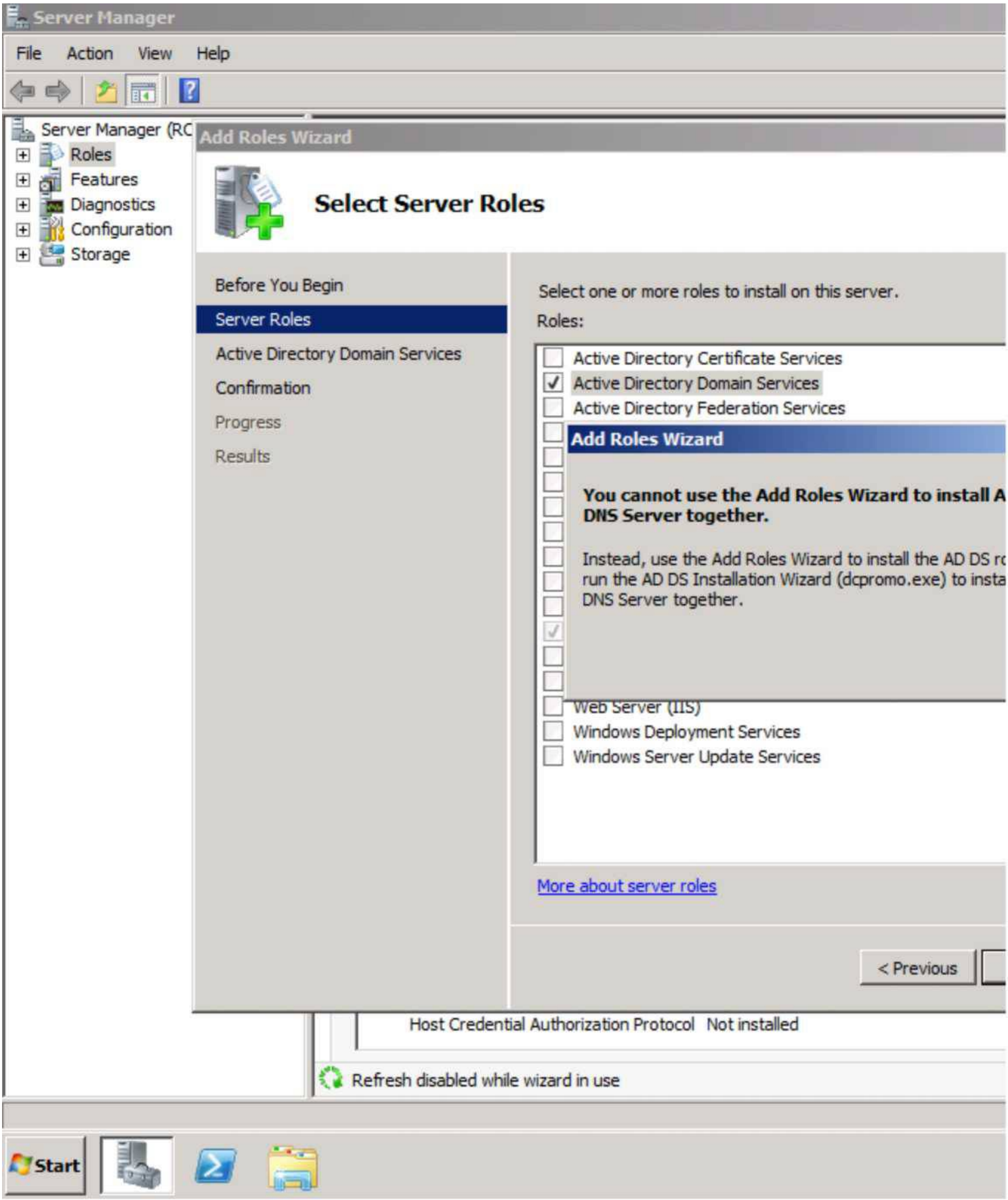


Создаём обратную зону. Без неё невозможно будет создать PTR записи. Все пункты по умолчанию. Вписать лишь нужно ID вашей сети. В моём примере обратная зона уже создана.


DNS Manager
File
Action
View
Help
DNS
DC12
Global Logs
Forward Lookup Zones
_msdcs.exonix.ru
exonix.ru
Reverse
10.16
Trust Poi
Conditio
Name
Type
Status
10.168.192.in-addr.arpa
Active Directory-Integrated Pr...
Running
New Zone...
View
Refresh
Export List...
Help
Create a new zone.



На этом базовая настройка завершена. ДНС сервер готов к обслуживанию клиентов.
Одно замечание по установке. Во время попытки установки AD DS и DNS одновременно на 2008 R2 можно было увидить следущее сообщение. В Windows Server 2012 можно одновременно выбрать AD DS и DNS роли.


Server Manager
File Action View Help
Server Manager (RC
Roles
Features
Diagnostics
Configuration
Storage
Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Add Roles Wizard
You cannot use the Add Roles Wizard to install A
DNS Server together.
Instead, use the Add Roles Wizard to install the AD DS ro
run the AD DS Installation Wizard (dcpromo.exe) to insta
DNS Server together.
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
More about server roles
< Previous
Host Credential Authorization Protocol Not installed
Refresh disabled while wizard in use
Start