

Otimização do Servidor DNS

Disciplina: Administração e Segurança de Sistemas de Computadores

Curso: Licenciatura em Engenharia Informática

Docentes: Doutor Eng. Lourino Chemane, engra. Ivone Cipriano e eng. Délcio Chadreca
DEEL, Faculdade de Engenharia, UEM

Agenda

- Configuracoes basicas do DNS
- Zona de Pesquisa Directa
- Zona de Pesquisa Inversa
- Teste de funcionamento

DNS

- Como é a comunicação entre os homens e como seria a comunicação entre *hosts* sem o DNS? Olá senhor 123456789.
- Sistema de comunicação entre computadores e bastante mais simples se forem identificados por números, isto é os endereços IP (http//: 196.3.96.206). Os utilizadores de computadores são pessoas, daí a necessidade de identificação alternativa, de acordo com a natureza humana , isto é, uma identificação baseada em nomes (Ex: www.uem.mz).
- Uma identificação por nome , permite agrupar logicamente os computadores com base numa estrutura organizacional. A identificação com base em endereço IP, reflete a estrutura física (rede) a qual o computador se encontra ligado ou conectado. Se o computador for deslocado para outra rede e receber um outro endereço IP, o nome (*hostname*) não será alterado e os seus utilizadores não se aperceberão facilmente desta alteração.

Cont.

- Serviço mais crítico da Internet, pois todos os demais serviços (E-mail, FTP, etc) dependem do seu funcionamento Efectivo.
- Principal Objectivo, Conversão de **Nomes em Endereço IP**. O seu papel na comunicação entre computadores a Internet é comparável ao da lista telefónica na comunicação entre os utilizadores dessa rede.
- Serviço de Suporte Fundamental, razão pela qual é o serviço cuja implementação é considerada em primeiro lugar, a quando do projecto de uma rede ou da ligação a Internet de uma rede isolada.

Componentes de suporte do DNS

- O espaço de nomeação de domínio, coordenado pela *Internet Corporation Assigned Names and Numbers* (ICANN), estruturado, hierarquicamente, em dominós e subdomínios, com identificação global única com gestão autónoma.
- Uma base de dados distribuída por servidores de nomes que para além de outra informação , armazena as correspondências entre os nomes dos computadores e os endereços IP
- Um protocolo de comunicação que permite aos clientes do serviço DNS (*Resolvers*) interrogarem os servidores de nomes.

Funcionamento do DNS

- O DNS é uma base de dados distribuída , contendo informação de mapeamos entre nomes de domínios e informação relativa a esses dominós e informação relativa a esses domínios. E, também , um protocolo de aplicação que permite a comunicação entre clientes **(que solicitam a conversão de um nome num ou mais endereços)** e servidores (que respondem com a informação disponível).
- O DNS define o processo de interrogação e de actualização da base de dados, os mecanismos de replicação da informação entre servidores e a organização da informação na base de dados.

Comunicação entre Clientes e Servidores

1- Questiona o *Resolver*, qual é o endereço IP correspondente a um determinado nome.

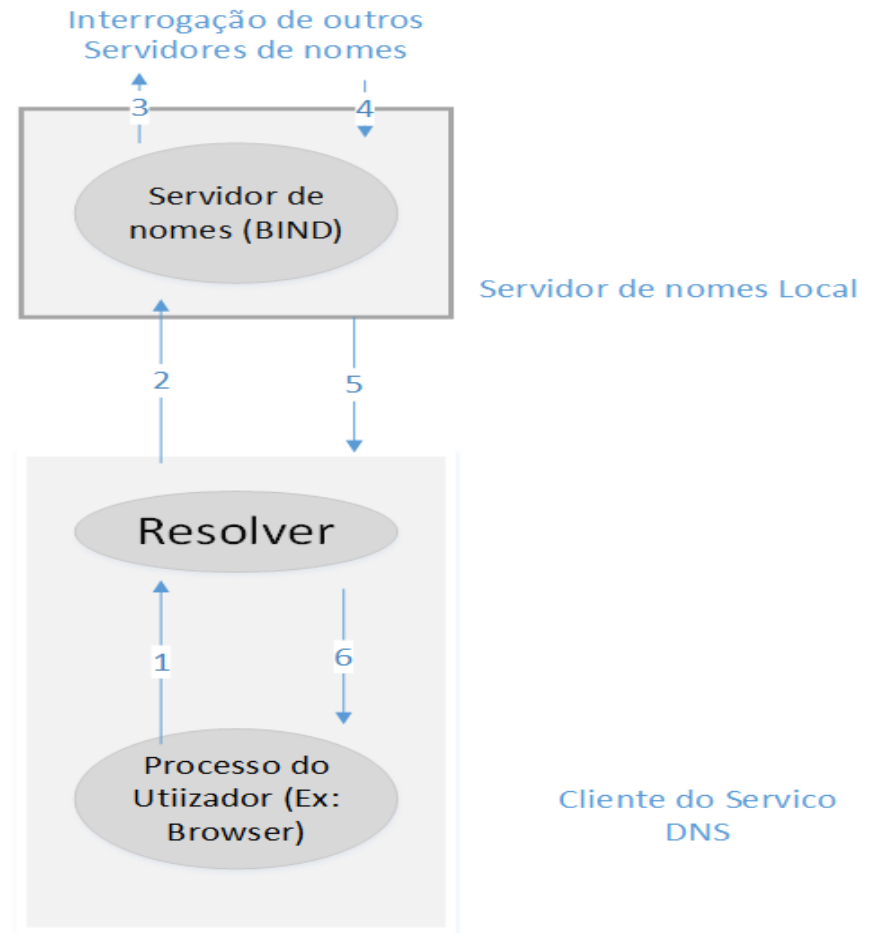
2- O Resolver solicita essa informação ao servidor de nomes mais próximo, conhecido pela configuração de TCP/IP do cliente.

3- Se o servidor de nomes solicitado não conhece o endereço IP do nome solicitado, interroga outros servidores de nomes.

4- O servidor de nome local recebe o endereço IP correspondente ao nome solicitado.

5- Devolve o resultado da *query* ao resolver

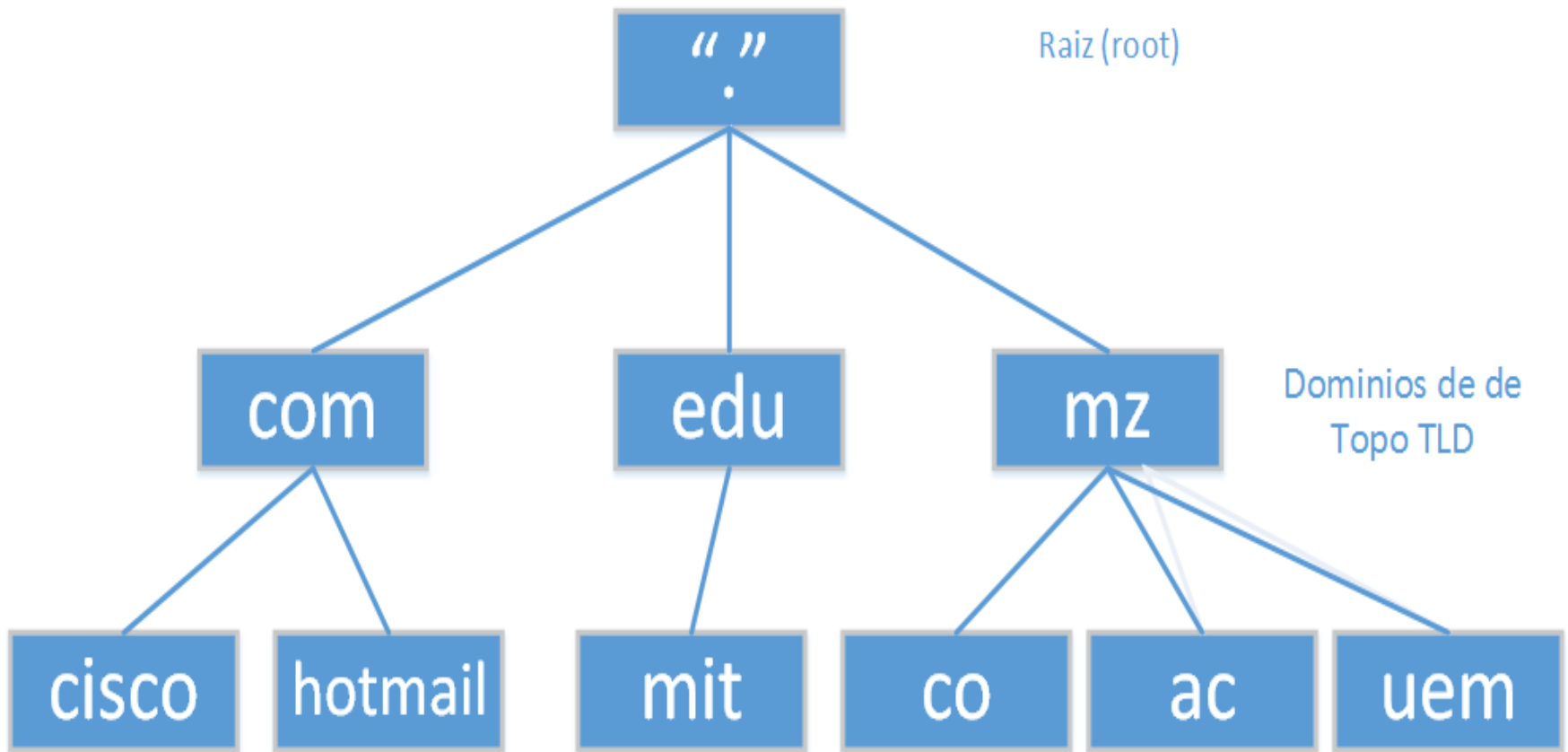
6- Finalmente, o resolver envia o endereço a aplicação do utilizador.



Espaços de Nomeação de Domínios

- DNS: repositório de informação que contém todas as correspondências entre nomes e endereços IP de todos os computadores na Internet.
- No espaço de nomeação temos cada dispositivo na rede associado a um nome único.
- Constitui um vasto e importante repositório de informação que define todas as correspondências entre nomes e endereços de dispositivos acessíveis na Internet.
- **Um servidor de DNS é suficiente para Internet?**
 - Um único ponto de falha
 - Capacidade de resposta para satisfazer todas as solicitações
 - Servidor geograficamente afastado da maioria dos clientes (Latência)
 - Esforço de manutenção inconcebível
- Dai a razão da sua implementação ter sido através de uma base de dados distribuída, escalável e com administração descentralizada, sua estrutura de nomes em árvore semelhante a uma estrutura administrativa hierárquica.

Fragmento de Espaço de Nomeação de Dominio



Fragmento de Espaço de Nomeação de Domínio

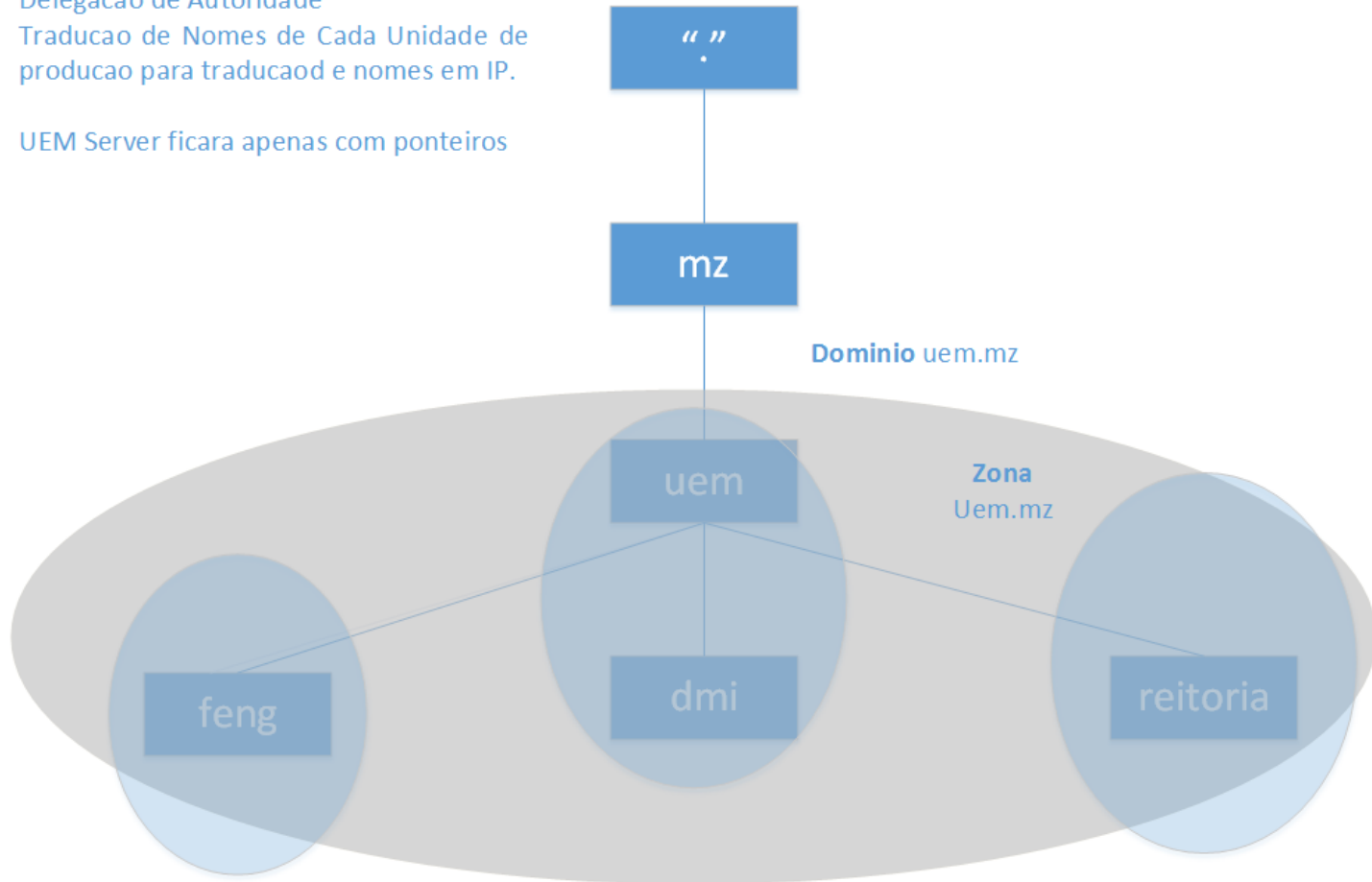
- Cada ramo corresponde um domínio, e pode ramificar-se em subdomínios. A cada organização é atribuída um espaço de nomeação, ficando responsável pela sua administração, subdivisão e atribuição de nomes, dentro desses espaço.
- Cada domínio tem um nome único, dependente da sua posição na árvore, O *Full Qualified Domain Name* (FQDN) de um computador inclui o nome do computador e os nomes de todos os subdomínios até a raiz.
- O DNS permite uma administração descentralizada da informação, através da delegação de autoridade.
- **Quem faz a administração do domínio .MZ?**

Zonas e Domínio

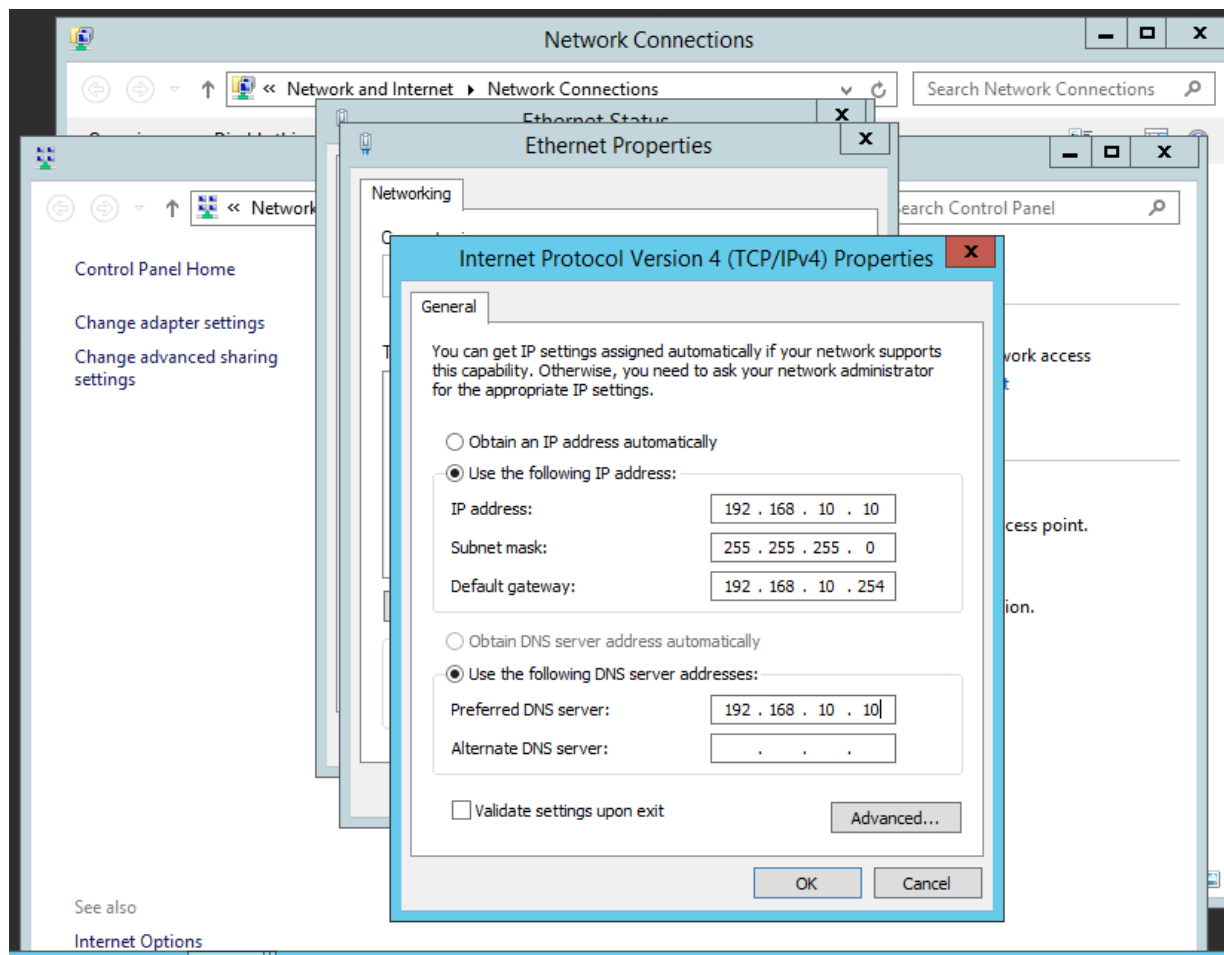
Delegação de Autoridade

Tradução de Nomes de Cada Unidade de produção para tradução e nomes em IP.

UEM Server ficará apenas com ponteiros



Reconfigurar a placa de rede



Verificação

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

Windows IP Configuration

    Host Name . . . . . : POMBO
    Primary Dns Suffix . . . . . : feuem.ac.mz
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : feuem.ac.mz

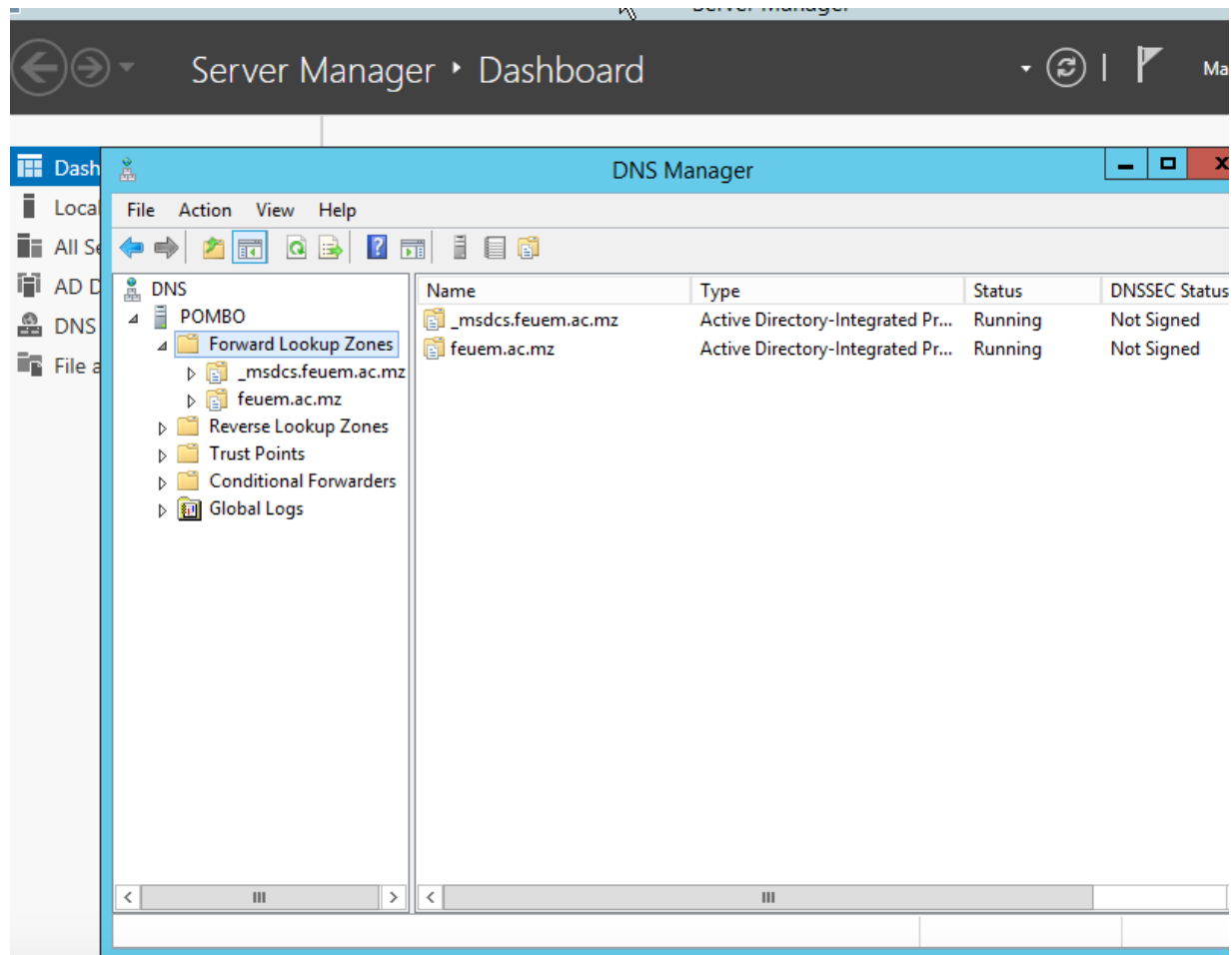
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Physical Address. . . . . : 08-00-27-57-53-13
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.10.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.254
    DNS Servers . . . . . : 192.168.10.10
    NetBIOS over Tcpip. . . . . : Enabled

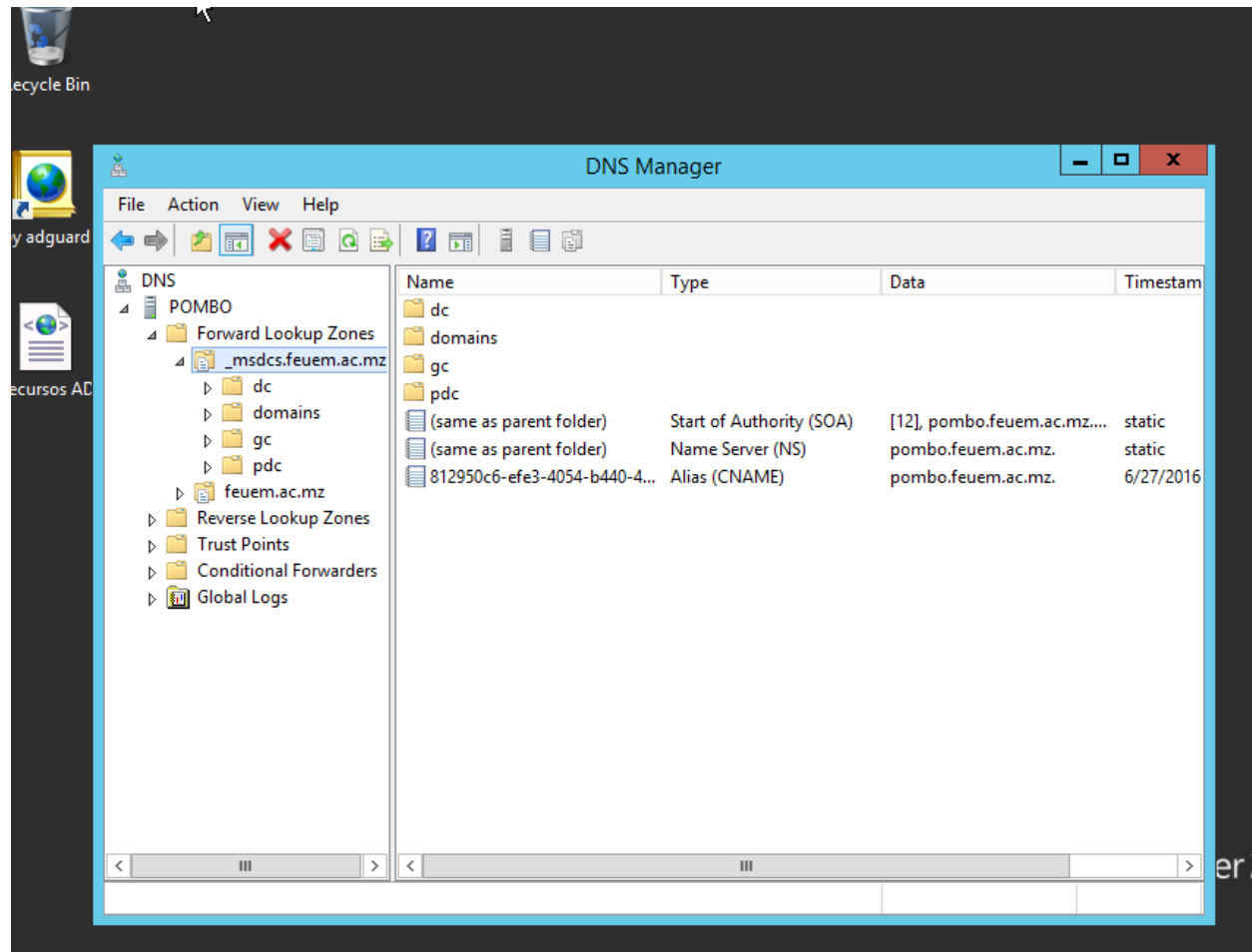
Tunnel adapter isatap.{A7A90ADA-F011-4DF8-BEB1-F20A254A2262}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft ISATAP Adapter #2
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
PS C:\Users\Administrator>
```

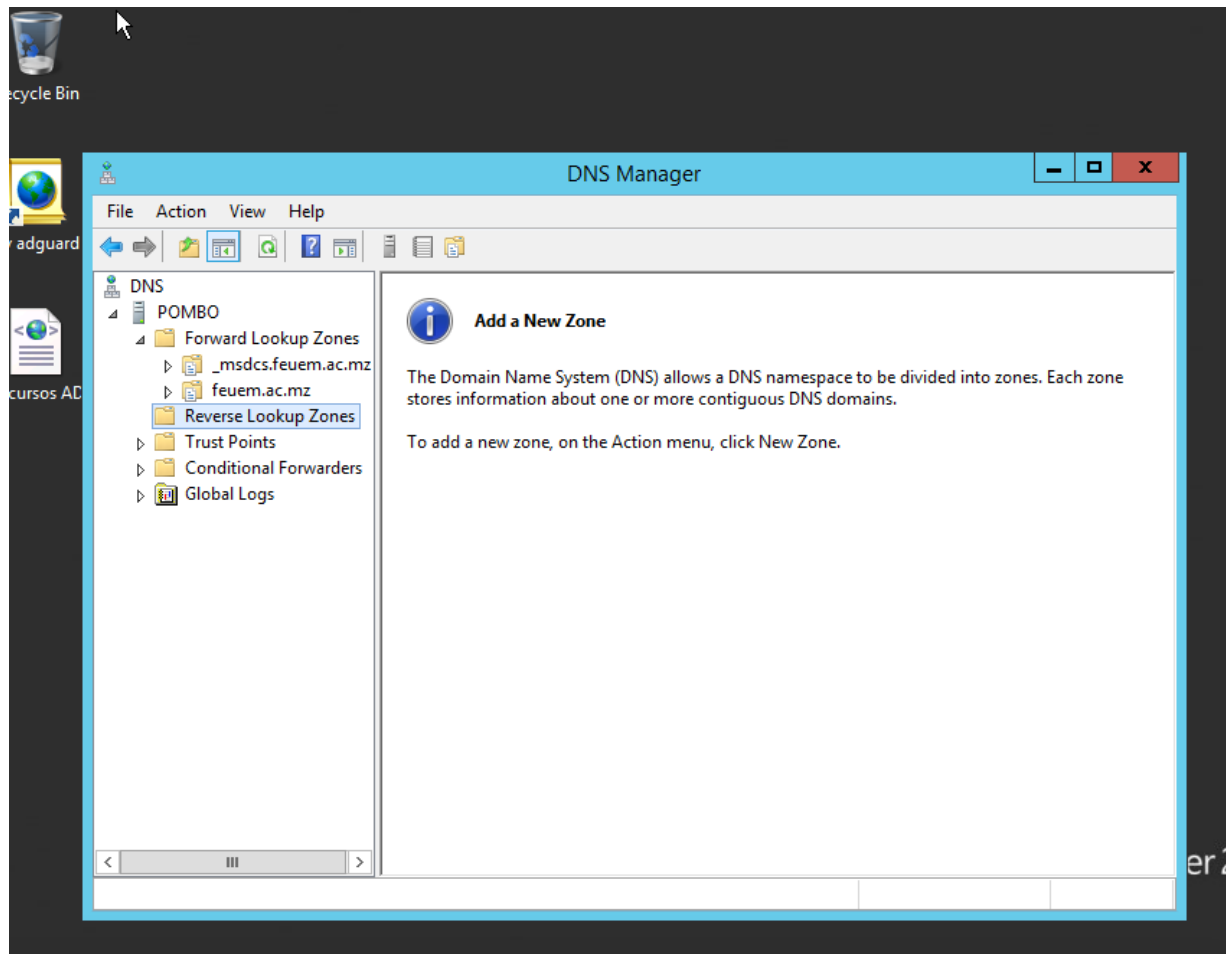
Serviço DNS



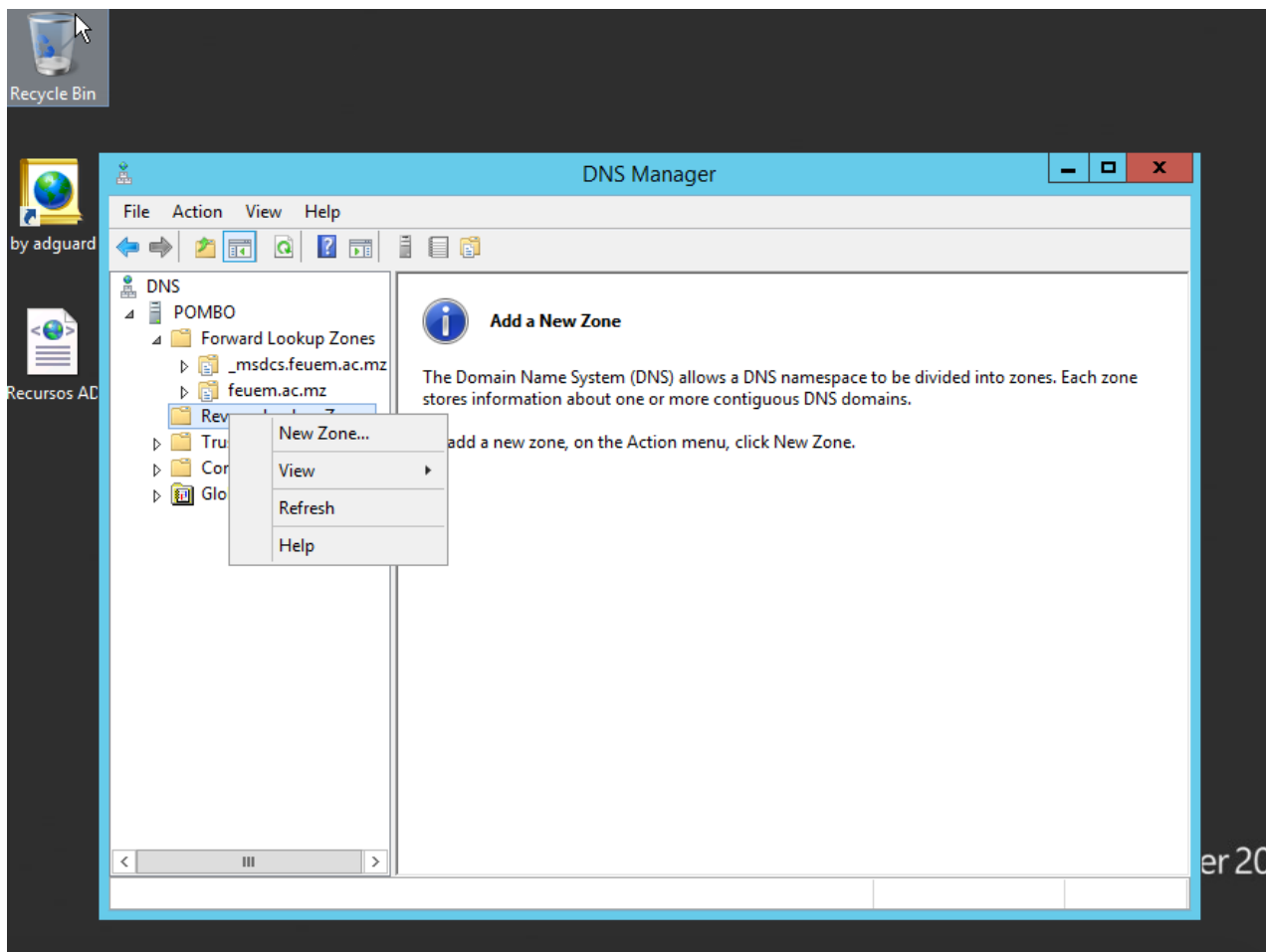
Zona de Pesquisa Directa



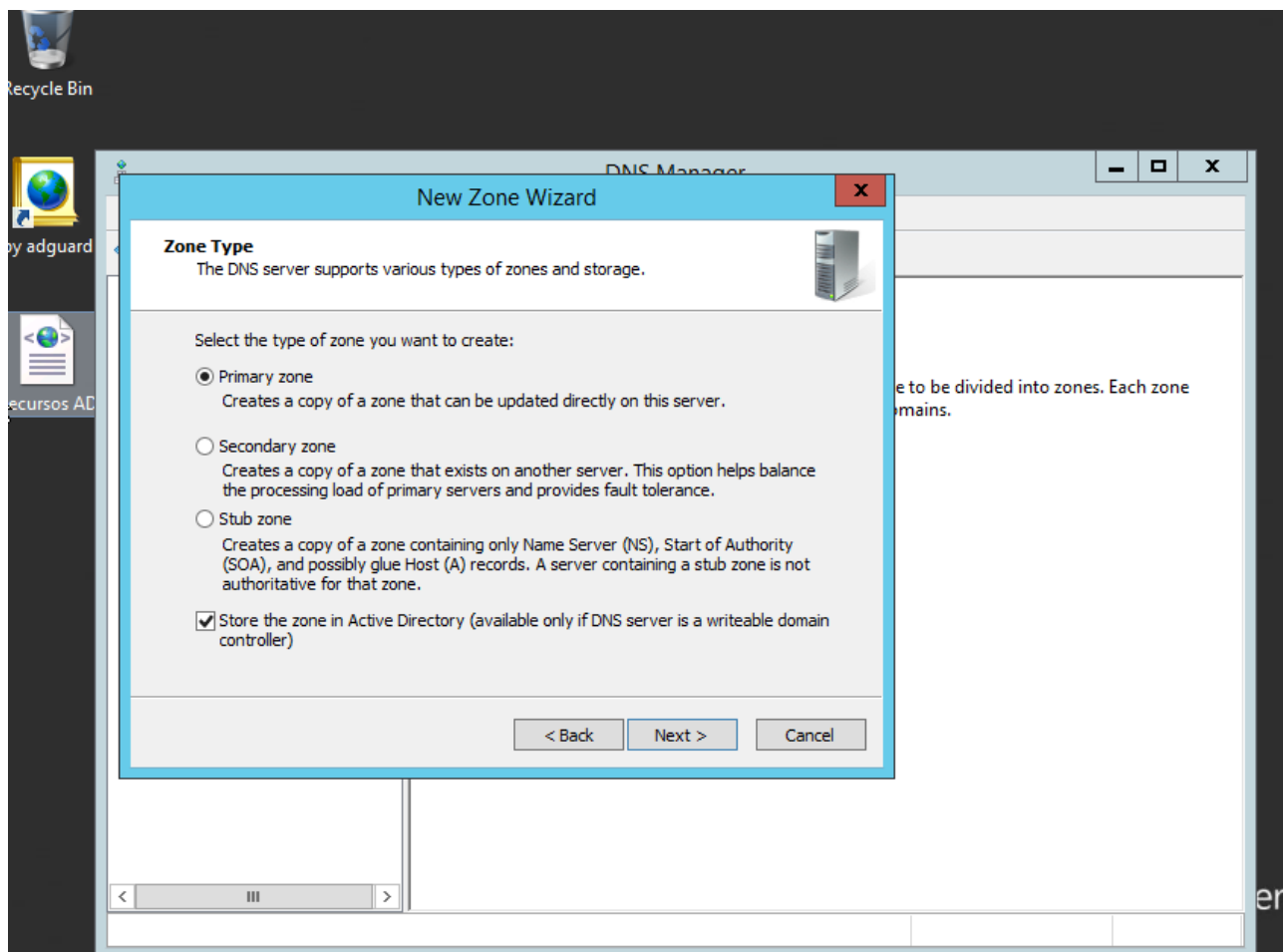
Zona de Pesquisa Inversa



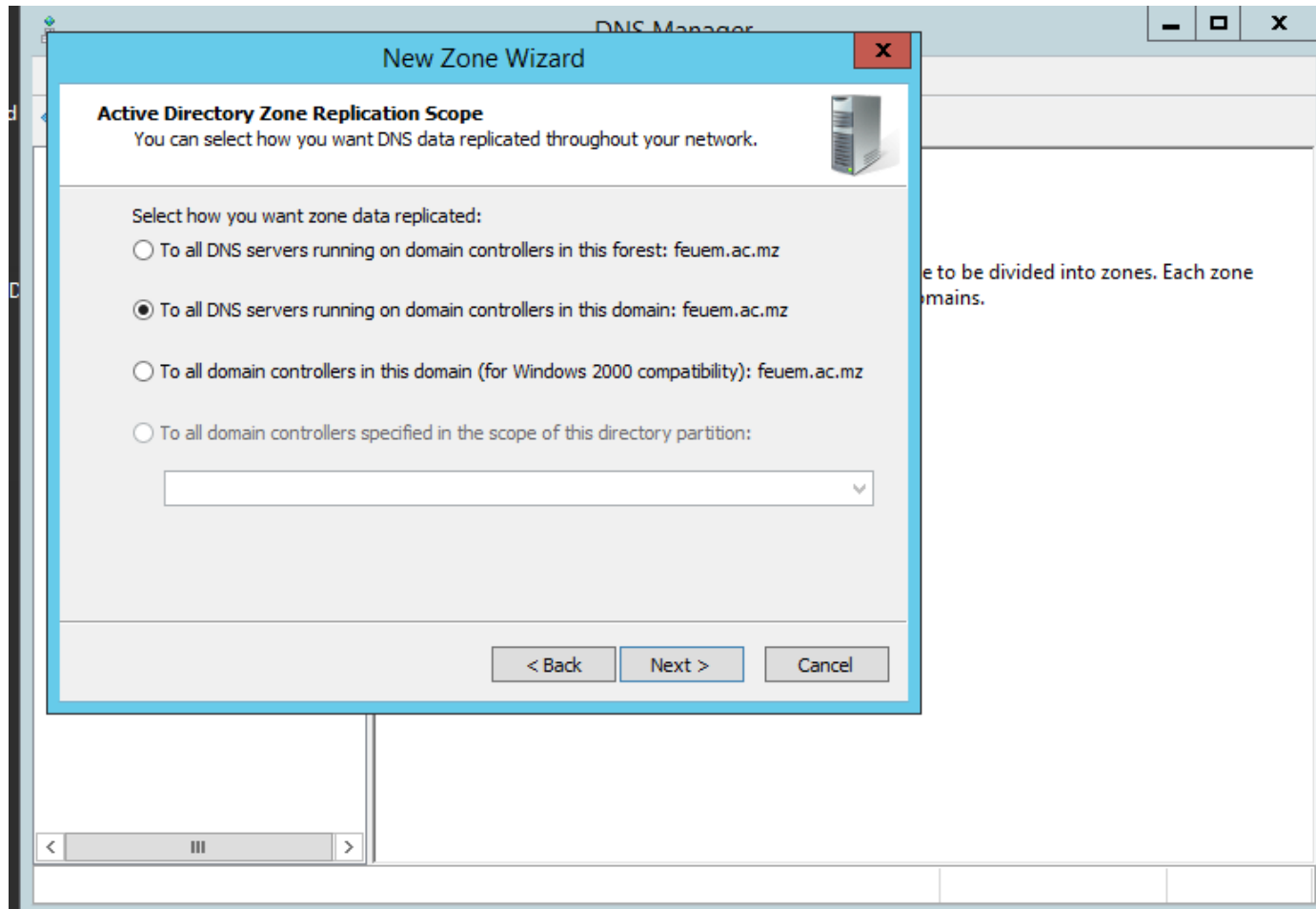
Criando Zona Inversa



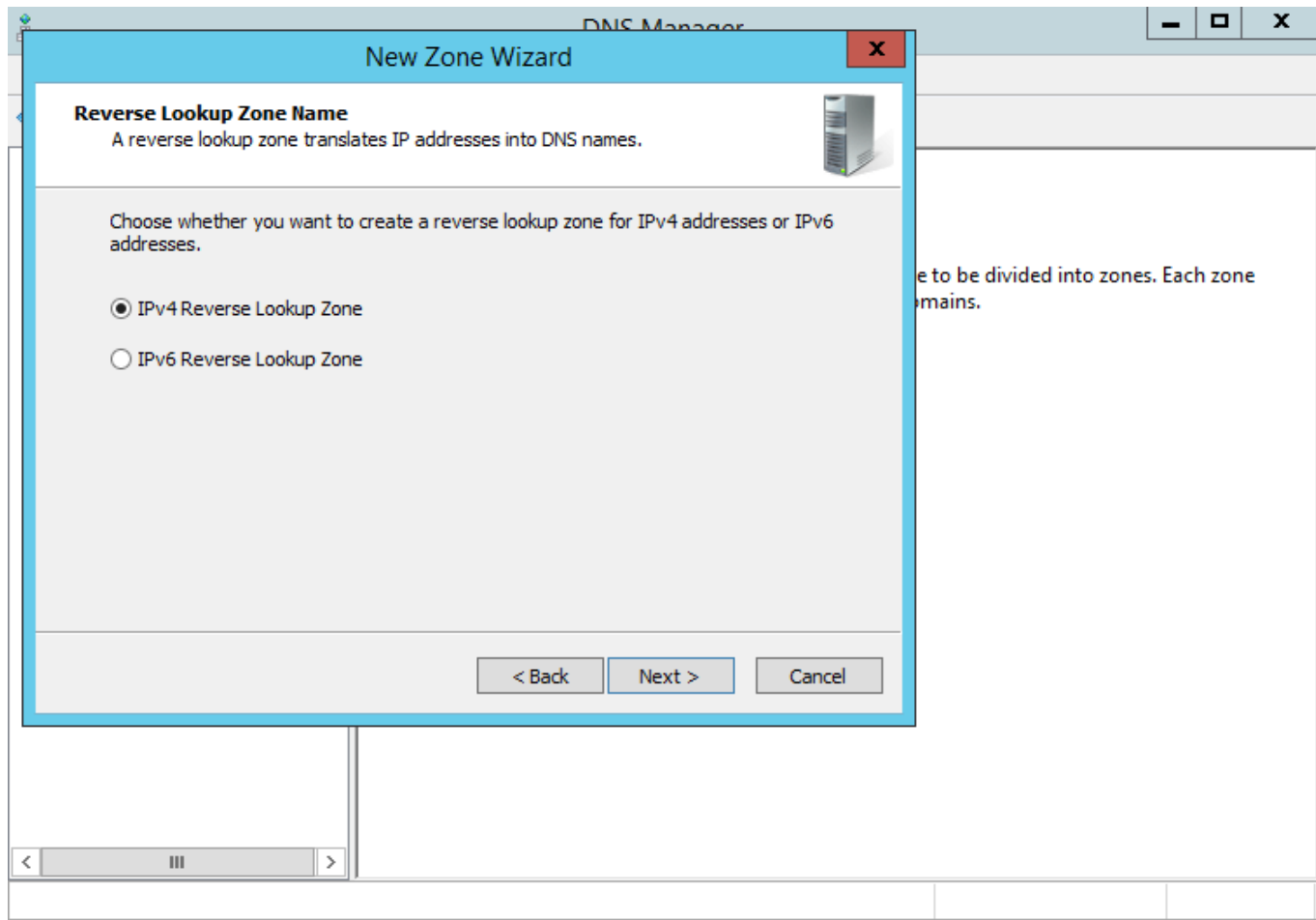
Tipo da Zona do DNS



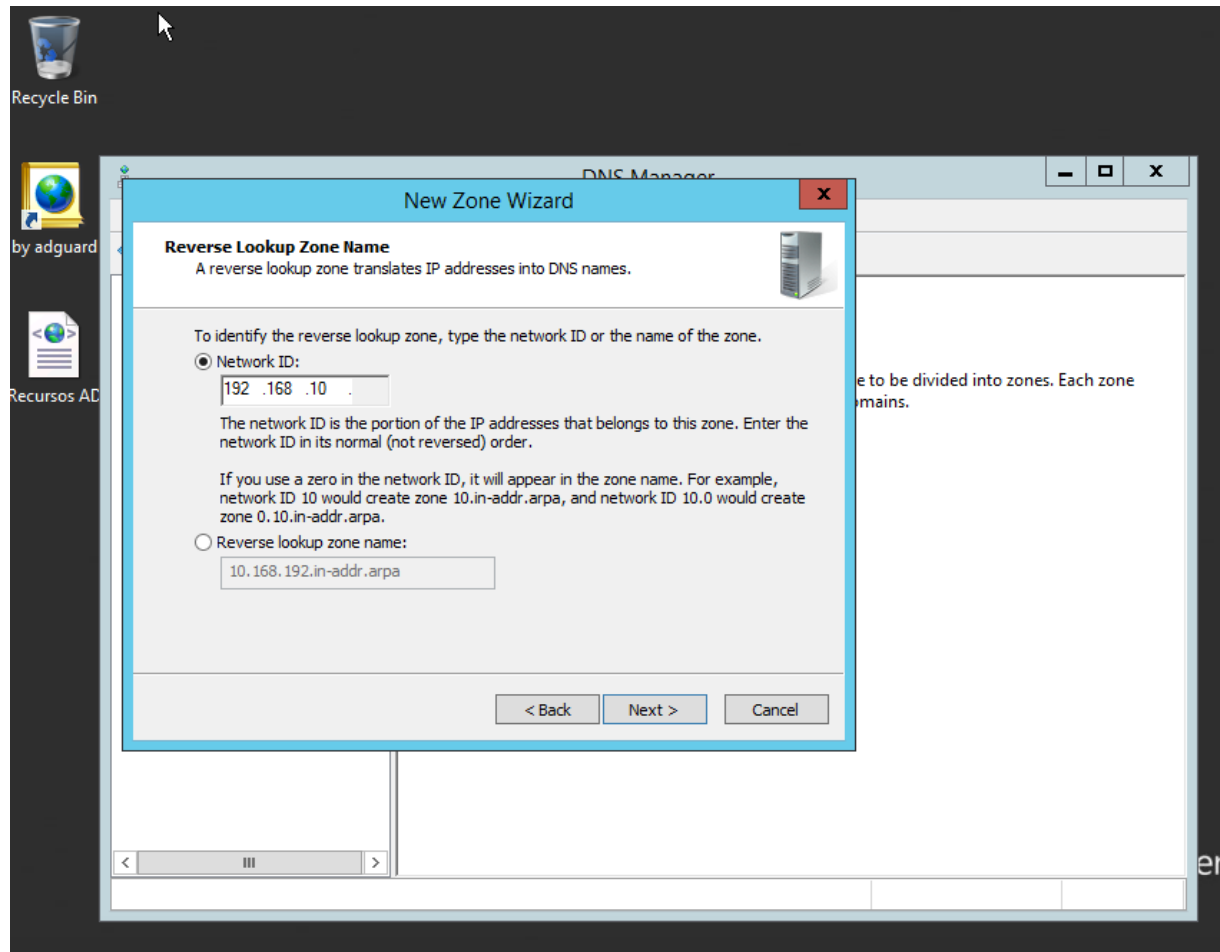
Escopo de Replicação da zona AD



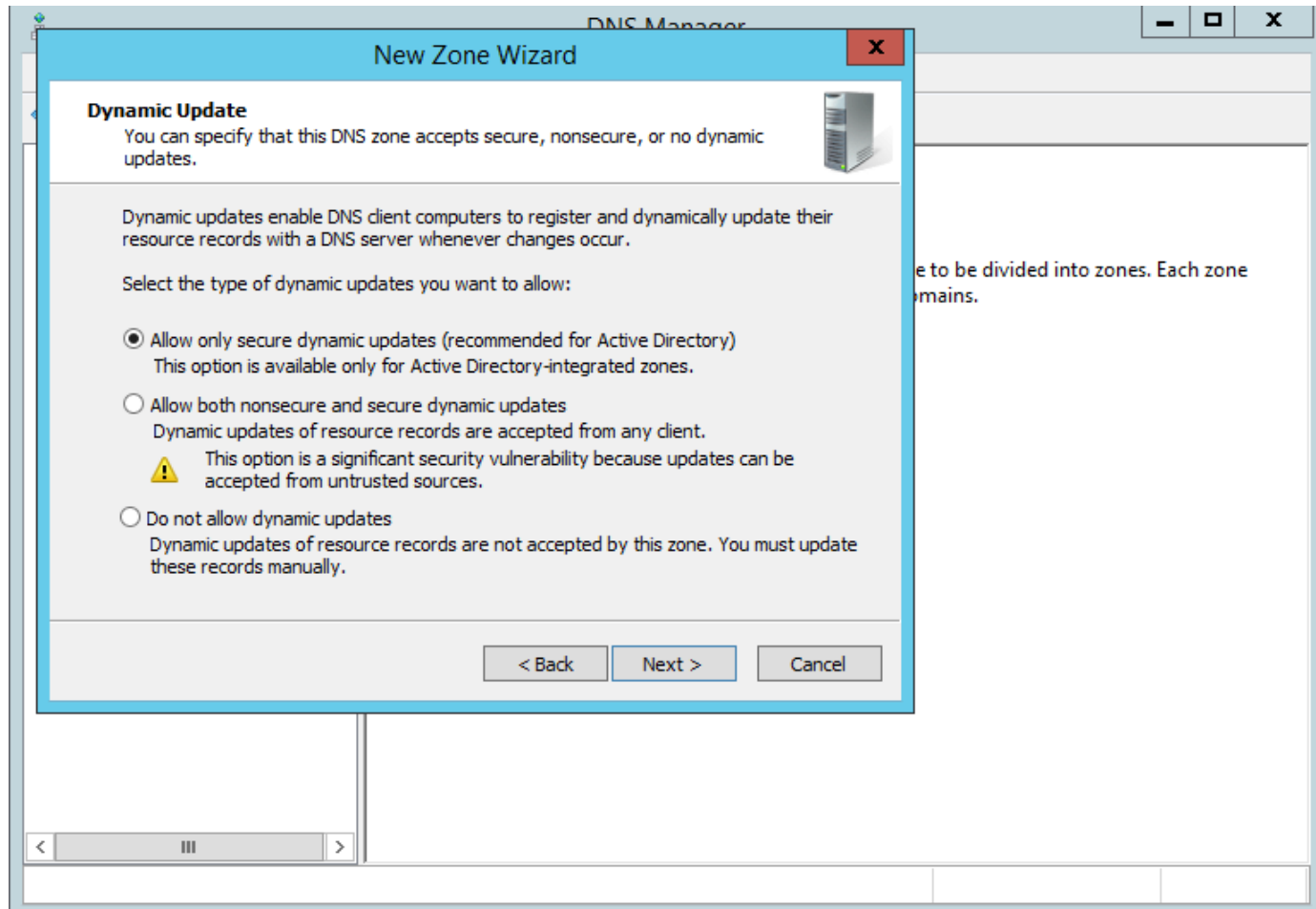
Nome da Zona de Pesquisa Inversa



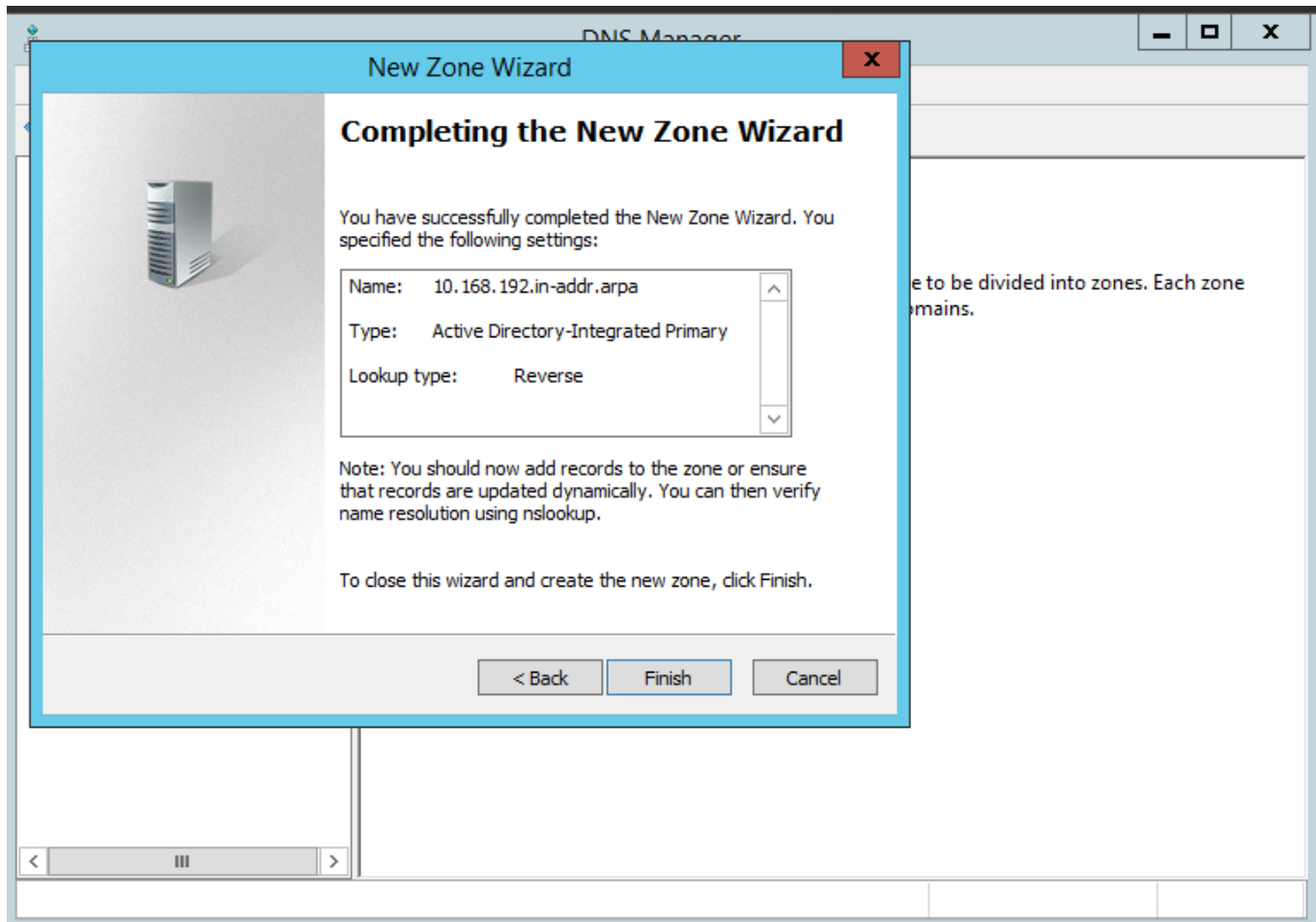
Nome da Zona de Pesquisa Inversa



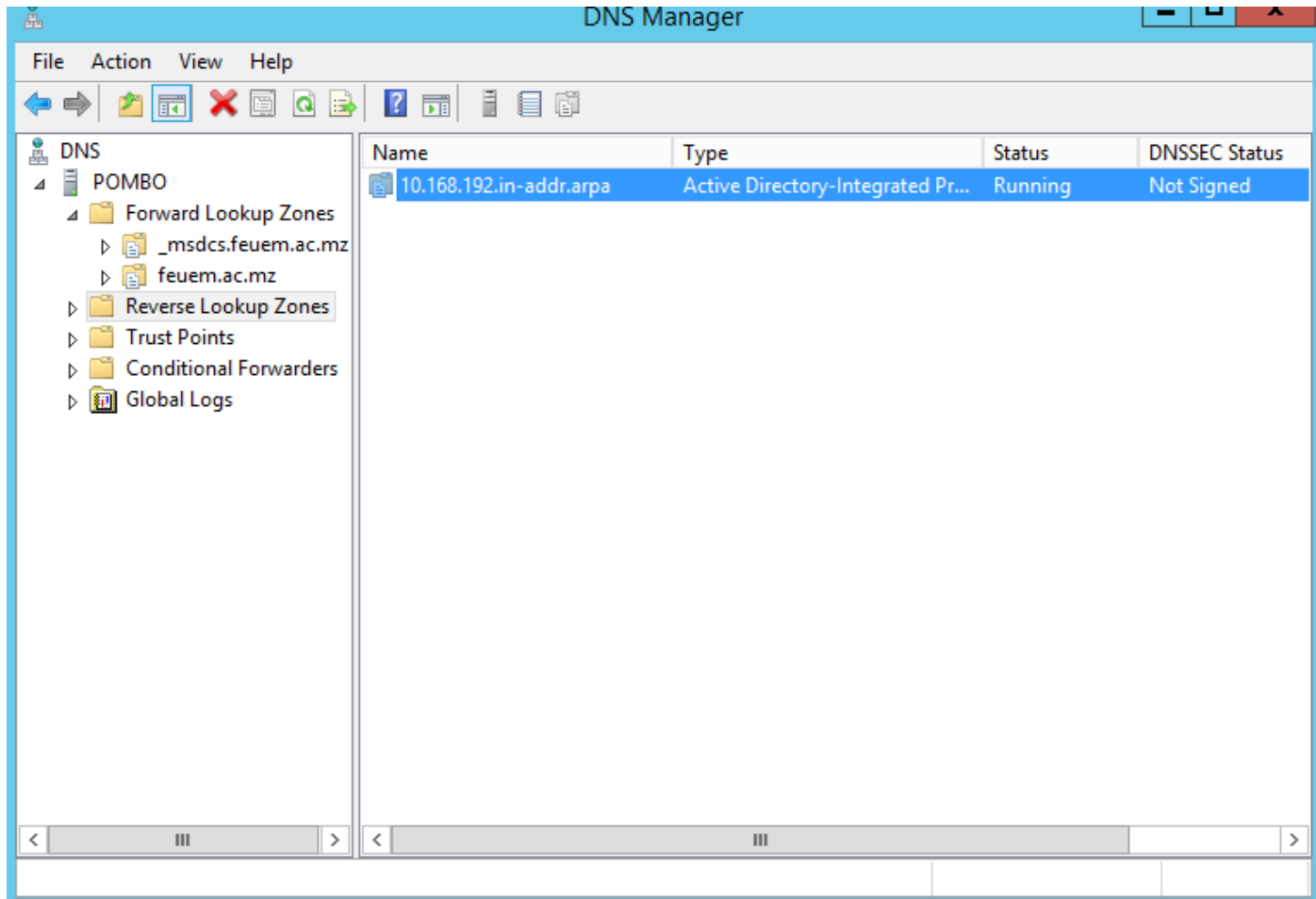
Actualização Dinamica



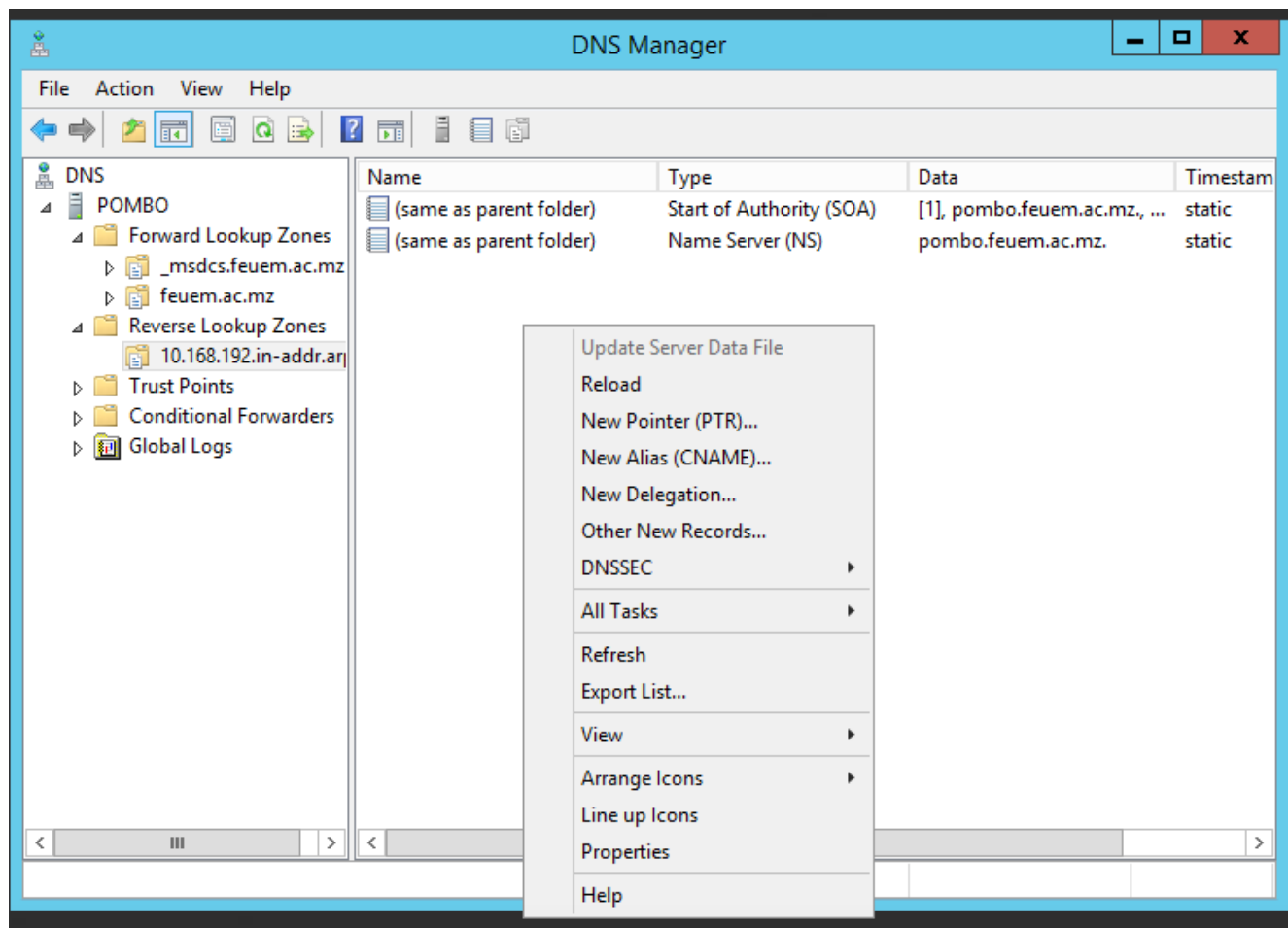
Configuração Concluída



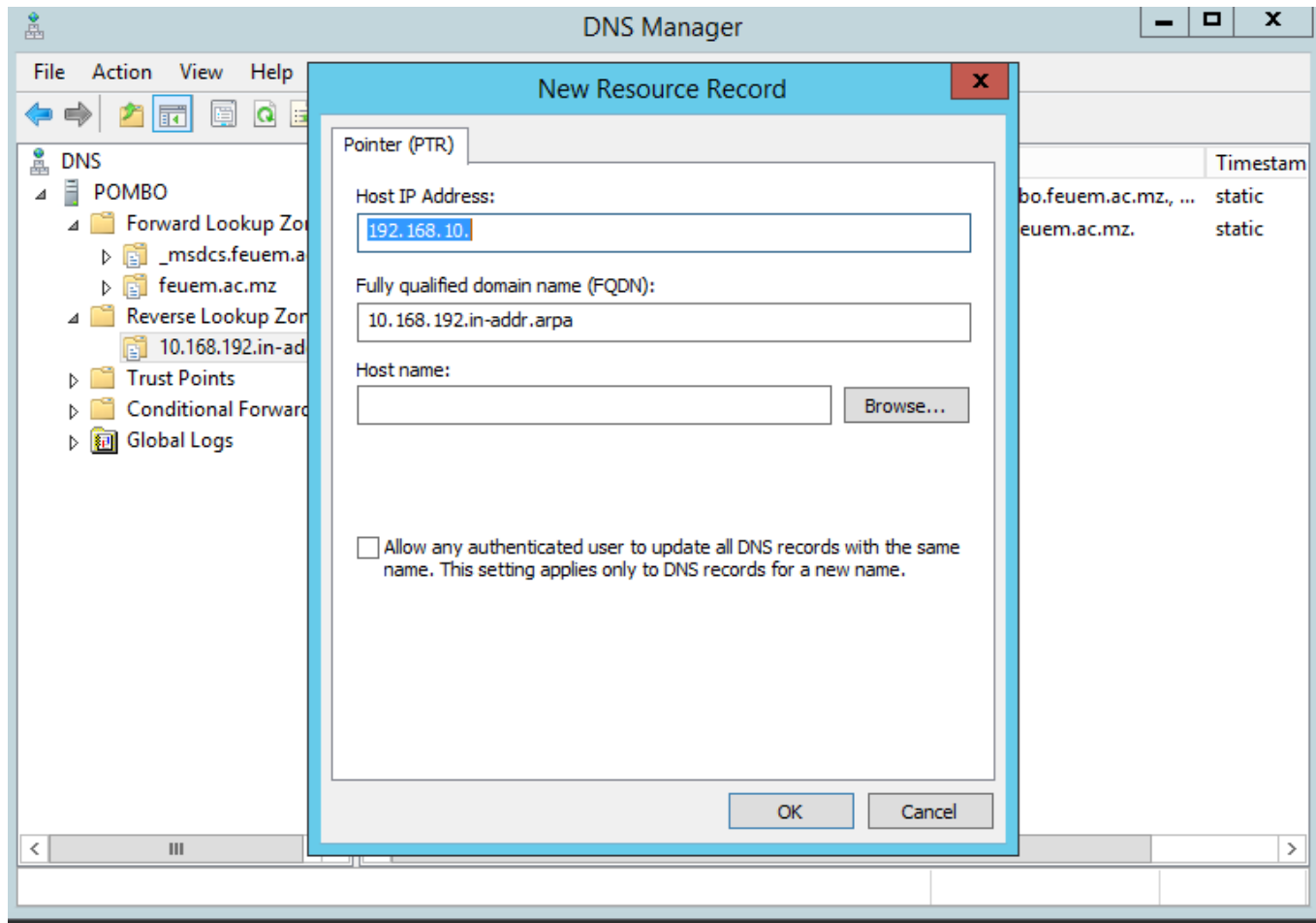
Zona de Pesquisa Inversa Criada



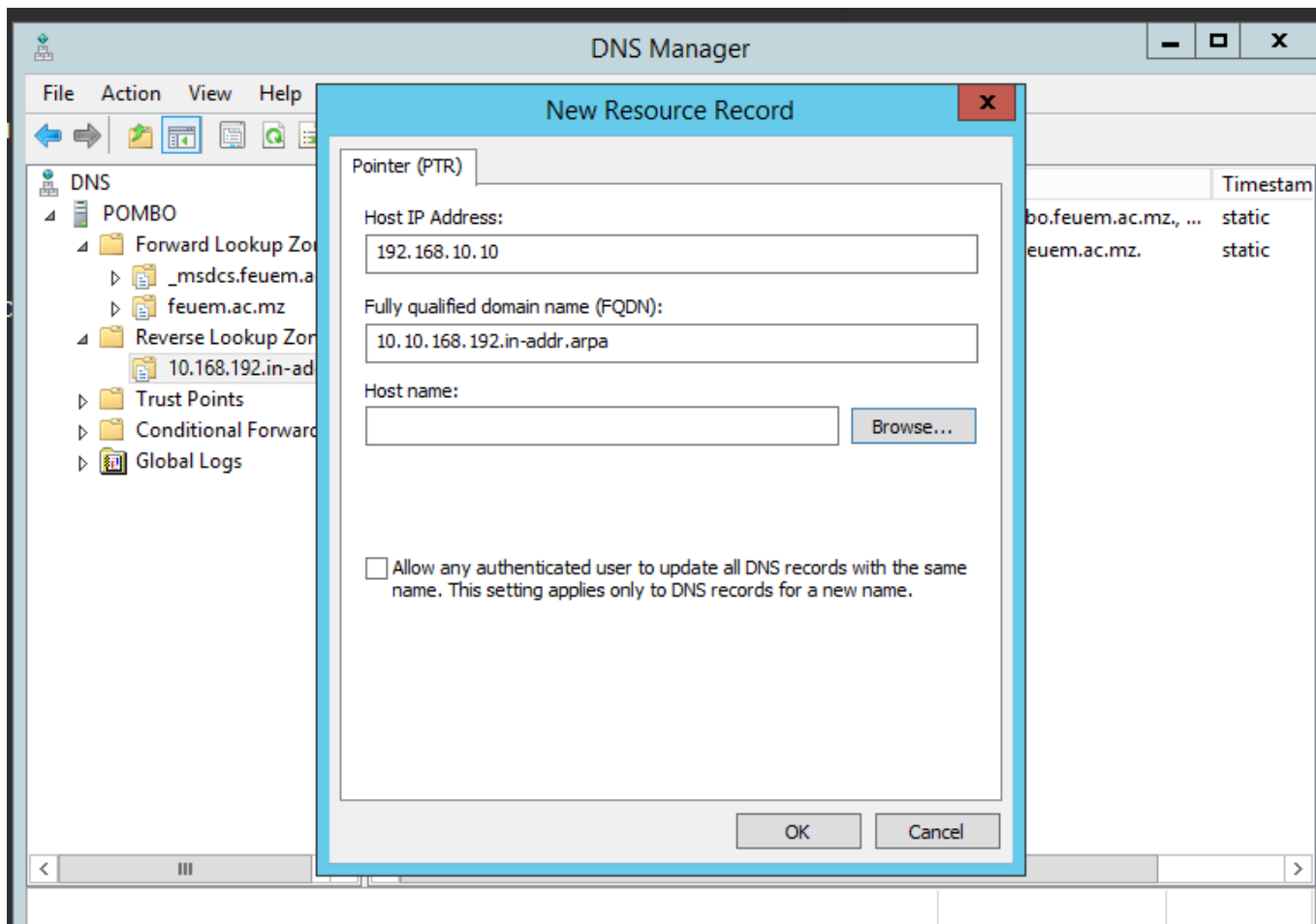
Criação do Ponteiro



Criação de Ponteiro



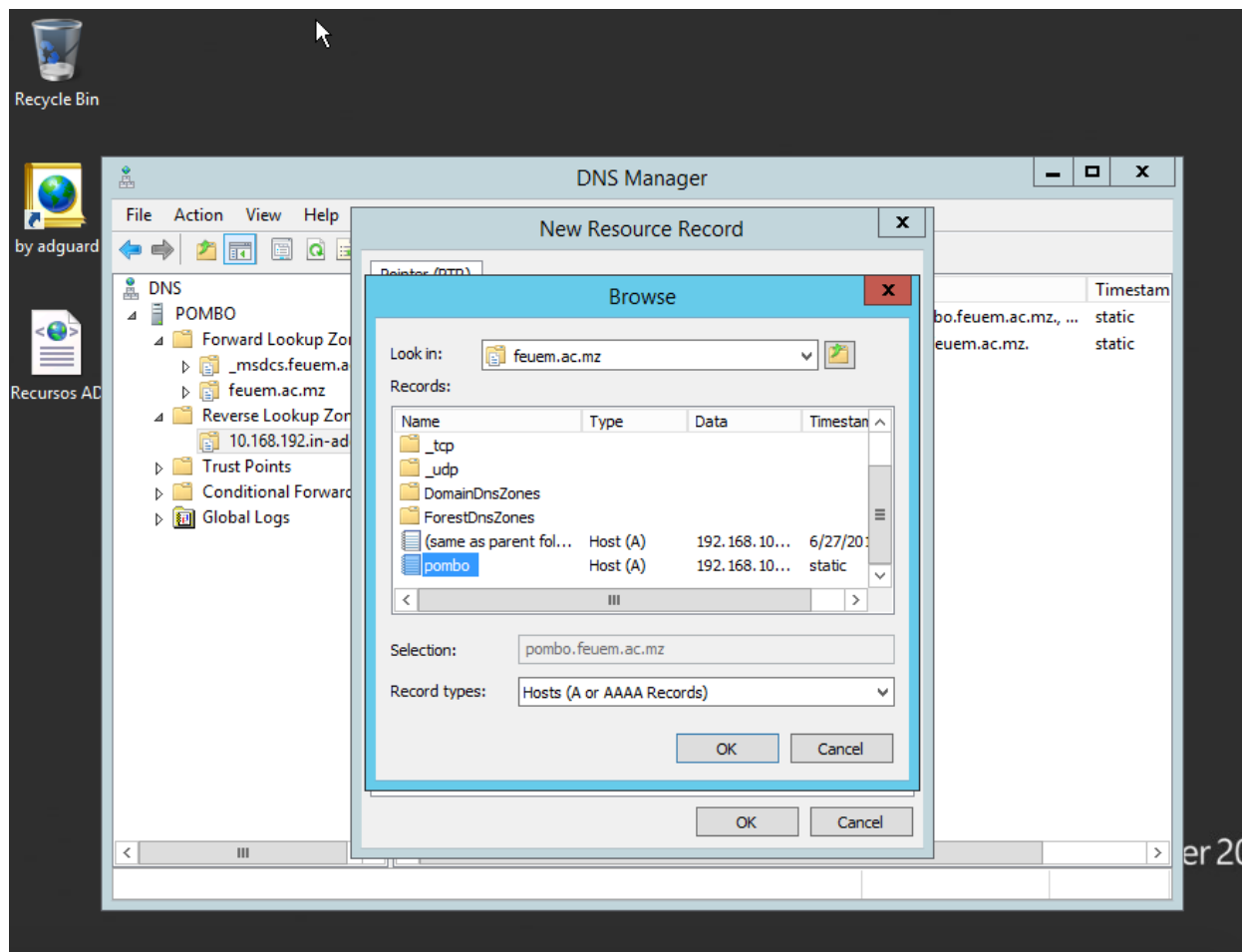
Criação de Ponteiro (Cont.)



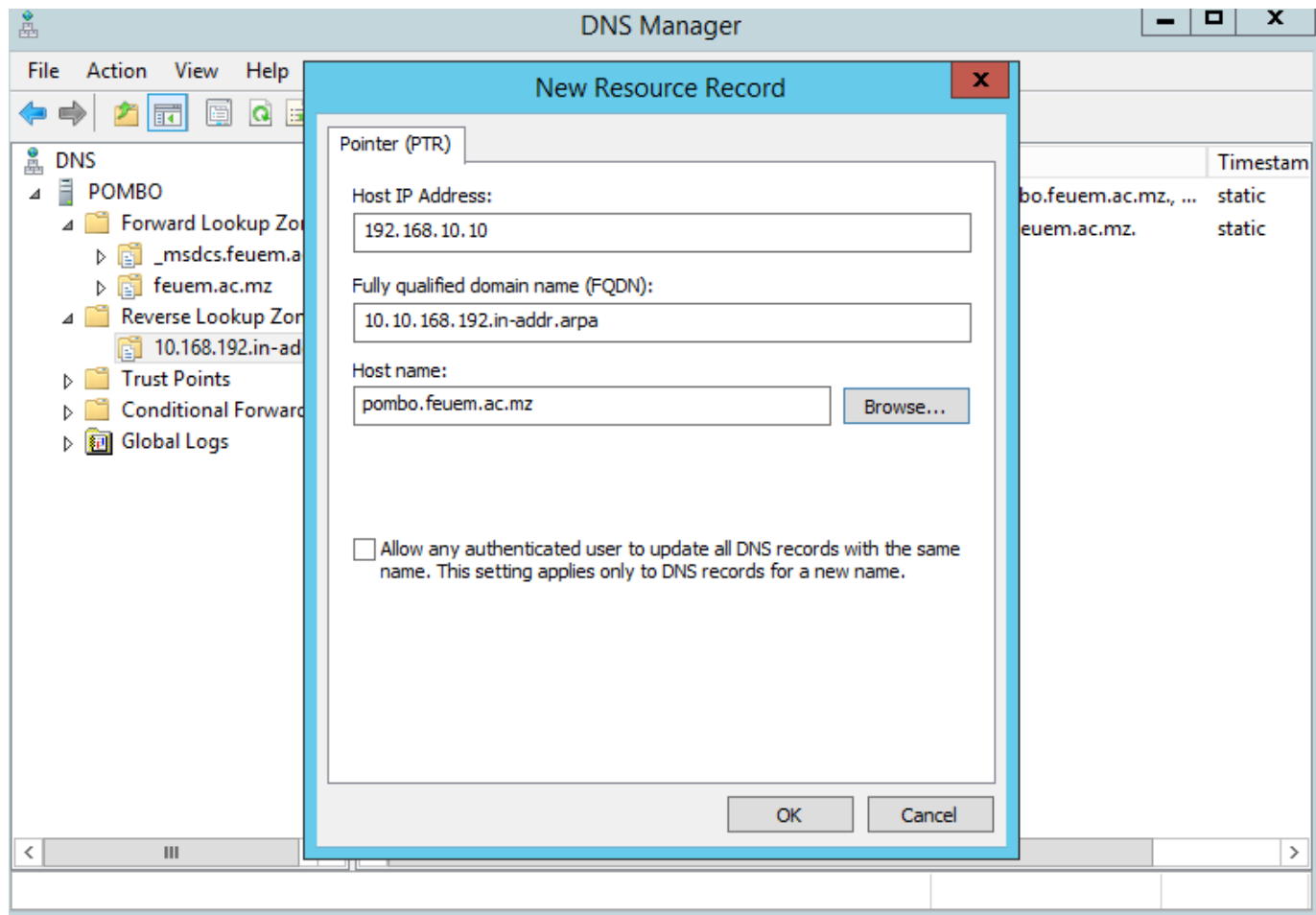
Criação de Ponteiro (Cont.)

- Para o hostname
 - Browser
 - Pombo
 - Forwardlookup Zone (Zona de Pesquisa Directa)
 - » Feuem.ac.mz
 - Pombo

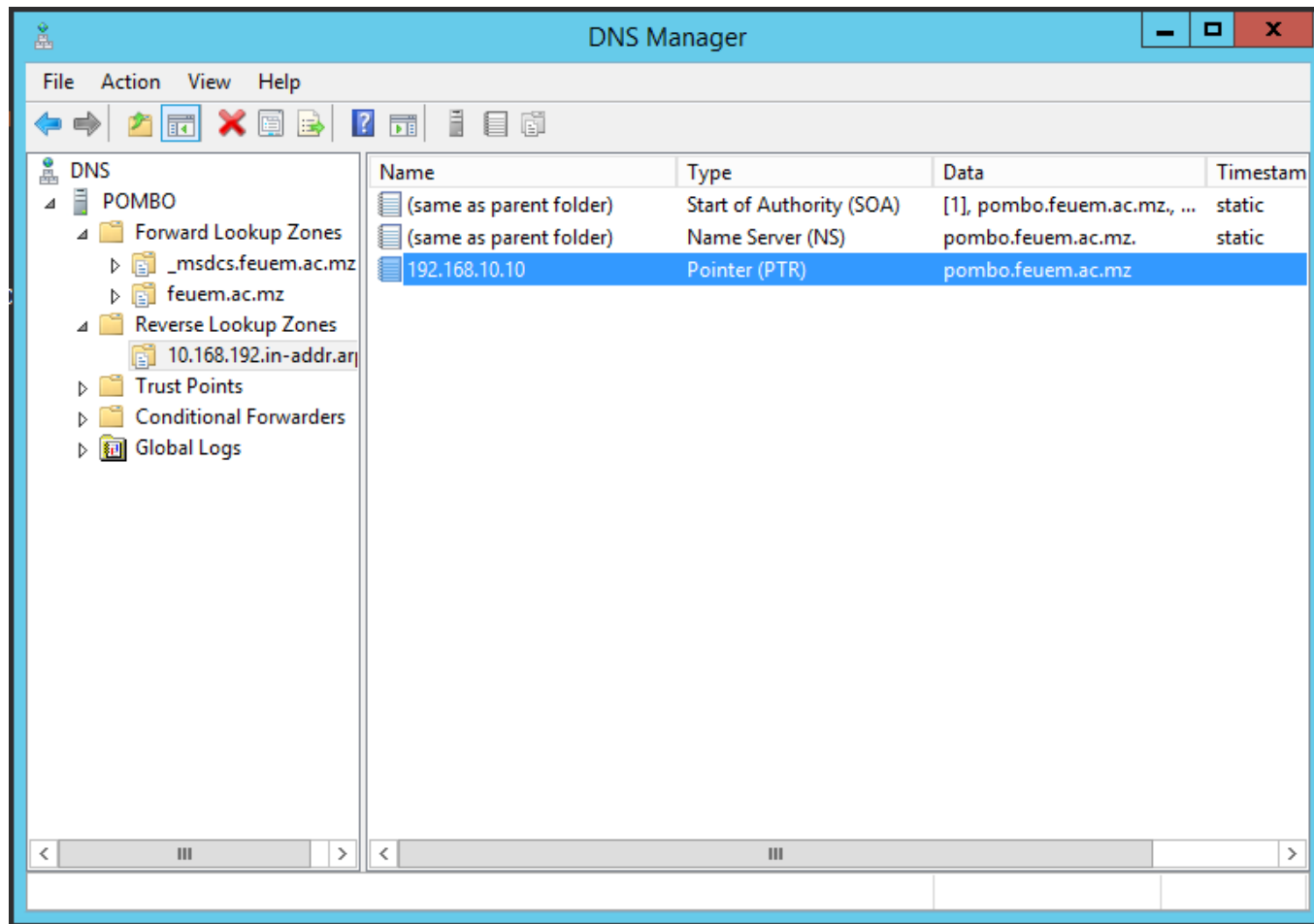
Criação de Ponteiro (Cont.)



Indicacao do endereco IP e do Hostname



Ponteiro Criado

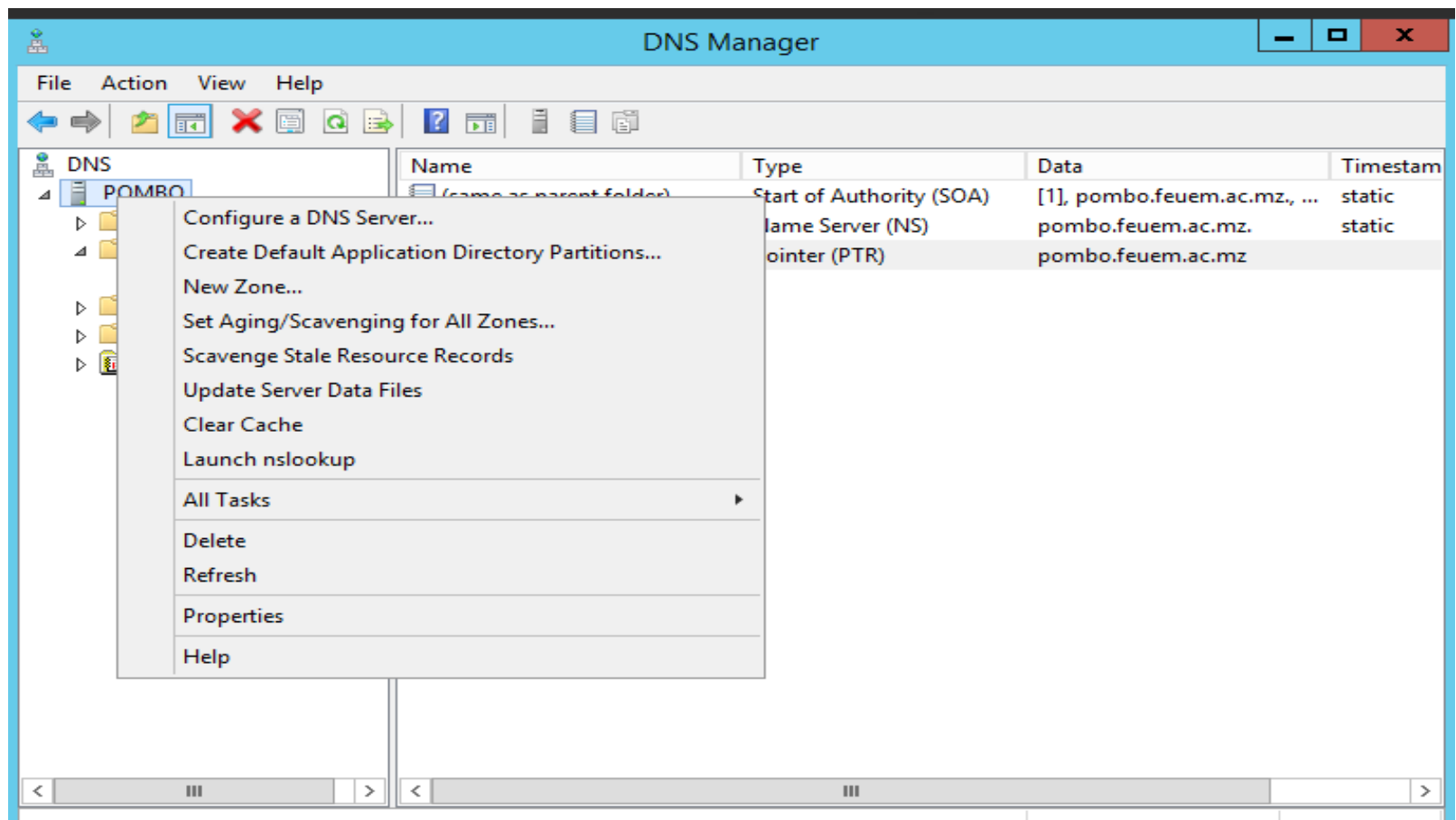


Zona de Pesquisa Directa e Inversa

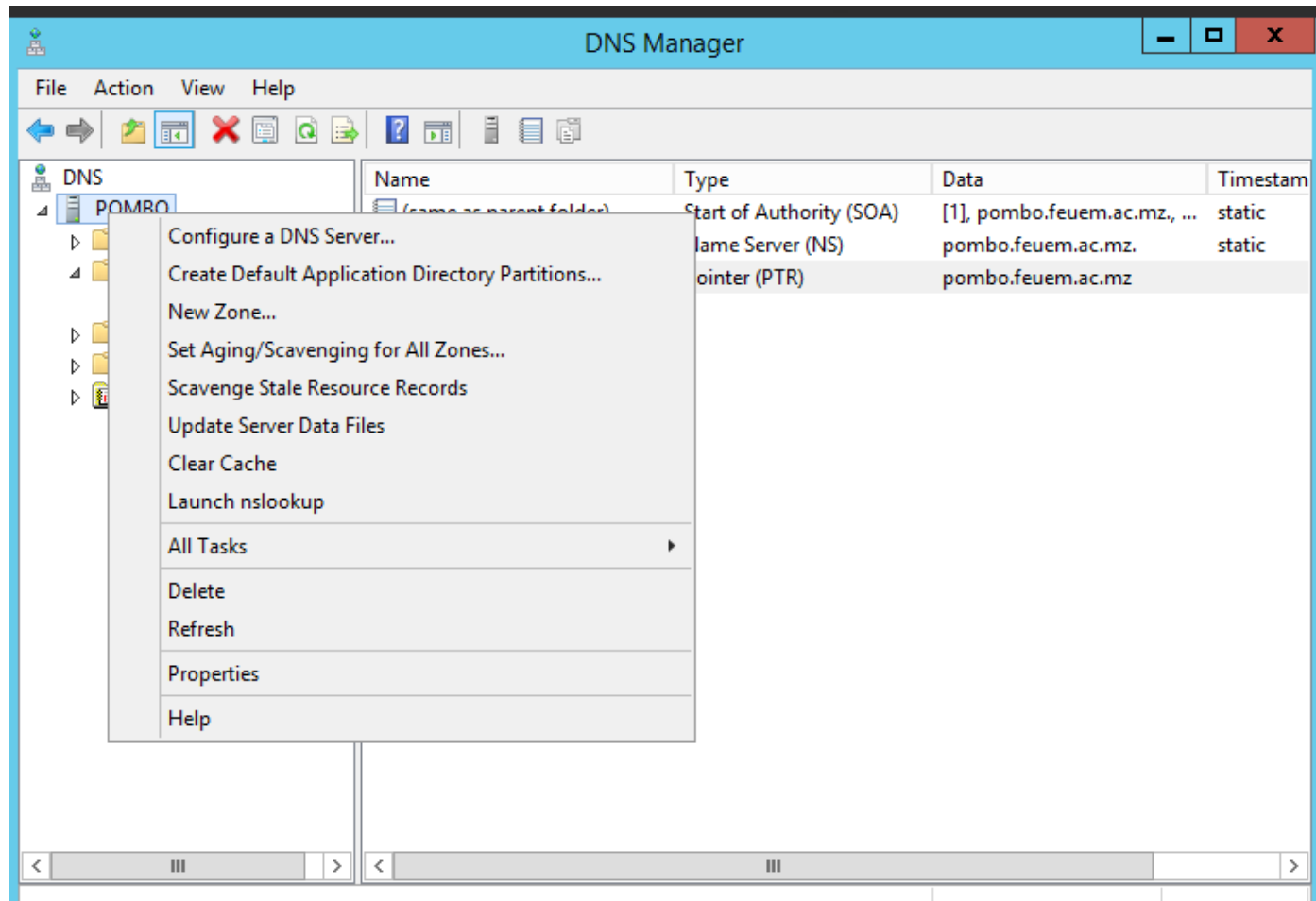
- Zona de Pesquisa Inversa:
 - Composto por um nome e a correspondência e de um endereço IP
- Zona de Pesquisa Inversa:
 - Composto um IP e a correspondência e um nome

Testando o Servidor

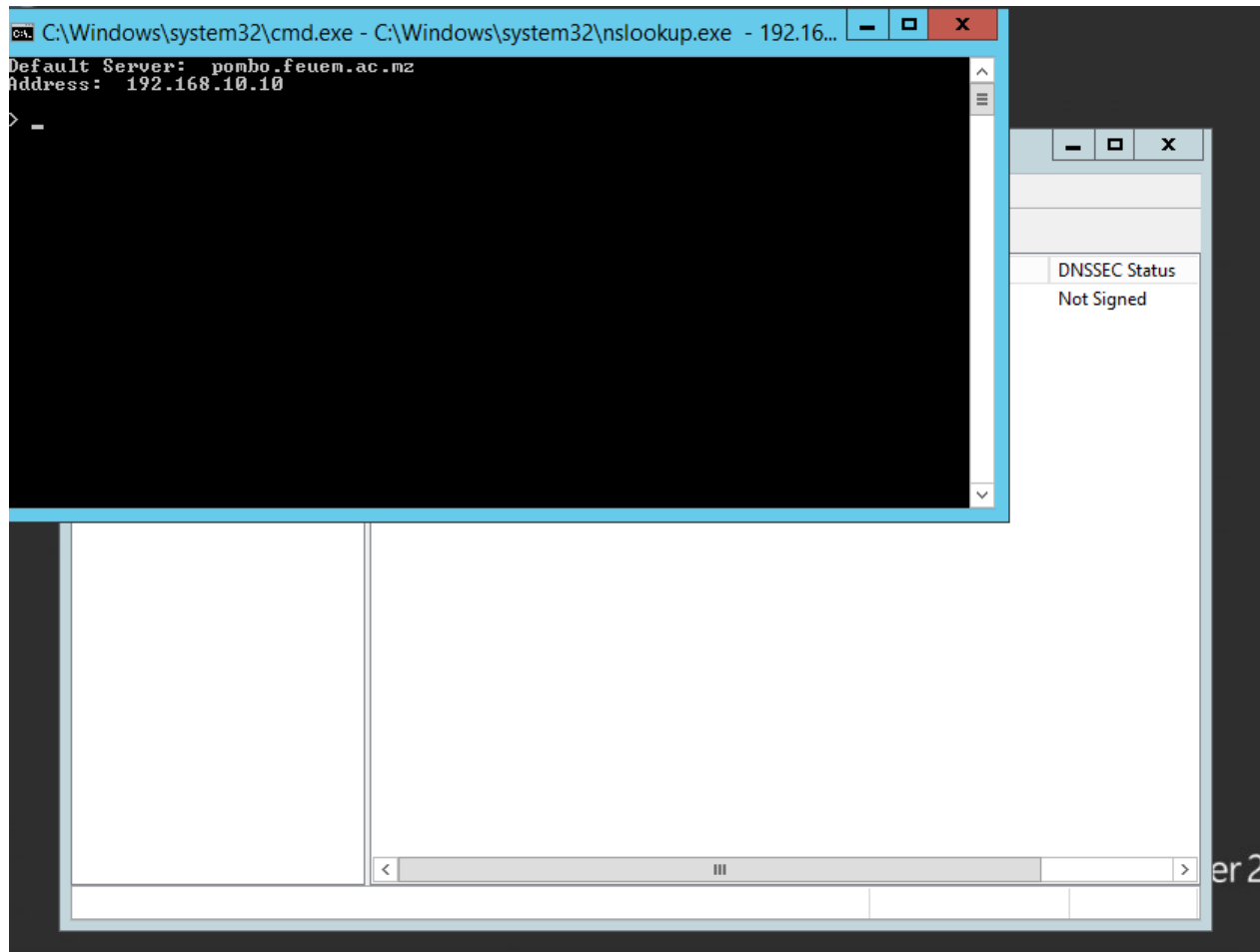
- Limpar o cache



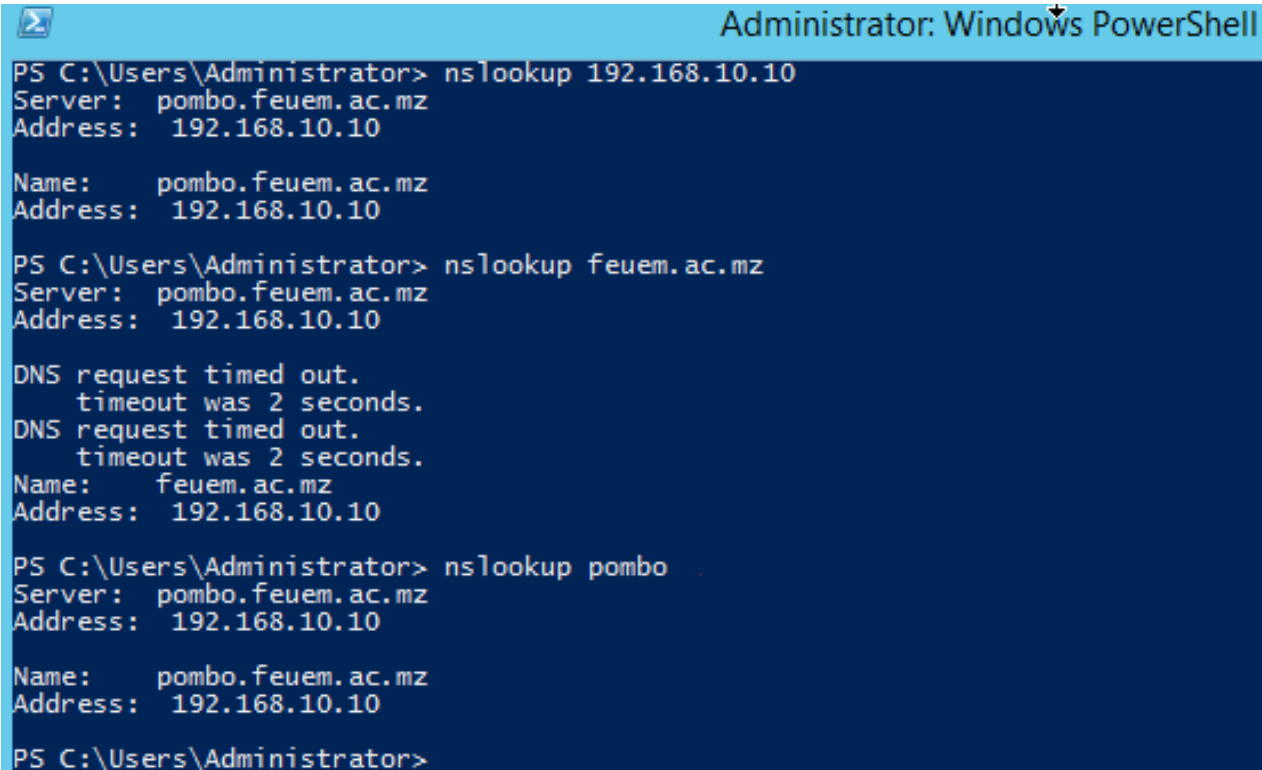
Iniciar o nslookup



Aba de teste do nslookup



Teste do funcionamento do DNS (Comando nslookup)



Administrator: Windows PowerShell

```
PS C:\Users\Administrator> nslookup 192.168.10.10
Server:  pombo.feuem.ac.mz
Address:  192.168.10.10

Name:     pombo.feuem.ac.mz
Address:  192.168.10.10

PS C:\Users\Administrator> nslookup feuem.ac.mz
Server:  pombo.feuem.ac.mz
Address:  192.168.10.10

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
Name:     feuem.ac.mz
Address:  192.168.10.10

PS C:\Users\Administrator> nslookup pombo
Server:  pombo.feuem.ac.mz
Address:  192.168.10.10

Name:     pombo.feuem.ac.mz
Address:  192.168.10.10

PS C:\Users\Administrator>
```

Teste do funcionamento do DNS (Comando PING)

```
Administrator: Windows PowerShell

PS C:\Users\Administrator> ping pombo

Pinging POMBO.feuem.ac.mz [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping feuem.ac.mz

Pinging feuem.ac.mz [192.168.10.10] with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator>
```

Teste do funcionamento do DNS (Comando dnscmd /info)

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> dnscmd /info

Query result:

Server info
server name           = POMBO.feuem.ac.mz
version               = 25800306 (6.3 build 9600)
DS container          = cn=MicrosoftDNS,cn=System,DC=feuem,DC=ac,DC=mz
forest name           = feuem.ac.mz
domain name           = feuem.ac.mz
builtin forest partition = ForestDnsZones.feuem.ac.mz
builtin domain partition = DomainDnsZones.feuem.ac.mz
read only DC          = 0
last scavenger cycle  = not since restart (0)

Configuration:
dwLogLevel            = 00000000
dwDebugLevel          = 00000000
dwRpcProtocol         = 00000005
dwNameCheckFlag       = 00000002
cAddressAnswerLimit   = 0
dwRecursionRetry      = 3
dwRecursionTimeout    = 8
dwDsPollingInterval  = 180

Configuration Flags:
fBootMethod           = 3
fAdminConfigured      = 1
fAllowUpdate           = 1
fDsAvailable          = 1
fAutoReverseZones     = 1
fAutoCacheUpdate      = 0
fSlave                = 0
fNoRecursion          = 0
fRoundRobin           = 1
fStrictFileParsing    = 0
fLooseWildcarding     = 0
fBindSecondaries      = 0
fWriteAuthorityNs     = 0
fLocalNetPriority      = 1

Aging Configuration:
ScavengingInterval    = 0
DefaultAgingState     = 0
DefaultRefreshInterval = 168
DefaultNoRefreshInterval = 168

ServerAddresses:

Ptr                  = 000000B83EB1E620
MaxCount             = 1
AddrCount            = 1
Addr[0] => af=2, salen=16, [sub=0, flag=00000000] p=13568, addr=192.168.10.10
```

Teste do funcionamento do DNS

(Comando dnscmd /zoneinfo feuem.ac.mz)

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> dnscmd /zoneinfo feuem.ac.mz

Zone query result:

Zone info:
    ptr                = 00000031C32FCB50
    zone name          = feuem.ac.mz
    zone type           = 1
    shutdown            = 0
    paused              = 0
    update              = 2
    DS integrated       = 1
    read only zone      = 0
    in DS loading queue = 0
    currently DS loading = 0
    data file           = (null)
    using WINS           = 0
    using Ntstat        = 0
    aging               = 0
        refresh interval = 168
        no refresh       = 168
        scavenger available = 0
    Zone Masters        NULL IP Array.
    Zone Secondaries    NULL IP Array.
    secure secs         = 3
    directory partition = AD-Domain      flags 00000015
    zone DN              = DC=feuem.ac.mz,cn=MicrosoftDNS,DC=DomainDnsZones,DC=feuem,DC=ac,DC=mz

Command completed successfully.

PS C:\Users\Administrator> _
```

Questões

- Para que ser a zona inversa?
- Liste cinco (03) comandos de rede para teste do servidor ou serviço DNS
- Explique o conceito de Delegação de DNS ou *“DNS Delegation”*