DNS REVERSO

Operação e Manutenção Remota Redes Multiserviço

Gerência de Operação e Manutenção Remota

Elaborado pela Equipe de Segurança N3 IP

Sumário

Especificações Funcionais:

➔ **Classes C (máscara igual a /24):**

É feita a designação junto (Registro.Br) da faixa de IP's e registrada a faixa sob responsabilidade do cliente. Após a OI executar a designação é necessário que o cliente acesse o site registro.Br e faça a devida delegação para os seus servidores de DNS.

- **Dados necessários:**

- Número do Circuito ou Terminal:
- Razão Social:
- CNPJ:
- ID do Registro.br/ Domínio:
- Responsável Técnico (Nome e Telefone):
- Faixa do Cliente:

- **Exemplo:**

- Número do Circuito ou Terminal: 0458647
- Razão Social: Empresa Fictícia S.A.
- CNPJ: 001.234.567/0004-89
- ID do Registro.Br/ Domínio: JDG786 / domínio.com.br
- Responsável Técnico (Nome e Telefone): Fulano (61) 305-1234
- Faixa do Cliente: 200.181.23.0/24 (200.181.23.0 a 200.181.23.255)

Ao recebermos o formulário acima, devidamente preenchido, será efetuada a configuração. No caso acima, a faixa 200.181.23.0/24 será designada no (Registro.Br) para o domínio domínio.com.br.

Para o correto funcionamento será necessário que o cliente faça a delegação no registro.br para seus servidores e que estes tenham a zona 23.181.200.in-addr.arpa. corretamente configurada.

➔ **Menores que classe C (máscara maior que /24 e menor que /32):**

A designação é feita junto ao (Registro.Br) somente para fins administrativos. As requisições de resolução serão enviadas para os servidores da OI, que por sua vez irão repassar a solicitação para os servidores do cliente. Neste caso o cliente não necessita fazer configuração junto ao Registro.Br.

- Dados necessários:

- Numero do Circuito ou Terminal:
- Razão Social:
- CNPJ:

- ID do Registro.Br/ Domínio:
- Responsável Técnico (Nome e Telefone):
- Faixa do Cliente: 200.181.23.0/29
- DNS Primário (IP e Nome): ola.com.br
- DNS Secundário (IP e Nome): tchau.com.br

Ao recebermos o formulário acima, devidamente preenchido, será efetuada a configuração. No caso acima, a faixa 200.181.23.0/29 será designado no (Registro.Br) para o domínio domínio.com.br.

Para o correto funcionamento será necessário que o cliente faça a configuração em seus servidores e que estes tenham a zona 7-0.23.181.200.in-addr.arpa. Corretamente configurada de acordo com a RFC2317.

É necessário que o cliente possua um cadastro (ID) no resgistro.br que é gratuito e não é de responsabilidade da OI.

Exemplos de Configuração:

➔ Linux:

As configurações dos servidores do cliente devem seguir a RFC 2317 (http://www.faqs.org/rfcs/rfc2317.html).

Segue exemplo de arquivo de configuração do servidor DNS do cliente para faixas menores que classe C.

Bloco 200.181.23.128/26 (200.181.23.128 a 200.181.23.191)

Arquivo de zone para 128-191.23.181.200.in-addr.arpa.

```
@ IN SOA dns.dominio.com.br. postmaster.dominio.com.br. (YYYYMMDDHH) ; serial number
28800 ; refresh
7200 ; retry
3600000 ; expire
86400 ) ; minimum TTL
;
; Zone NS records
;
IN NS dns.dominio.com.br. ; servidor primário do cliente
IN NS dns2.dominio.com.br. ; servidor secundário do cliente
;
; Zone MX records (mail exchange)
;
IN MX 10 mail
;
; Zone records
;
n1 IN PTR server1.dominio.com.br.
n2 IN PTR server2.dominio.com.br.
n3 IN PTR server3.dominio.com.br.
...
```

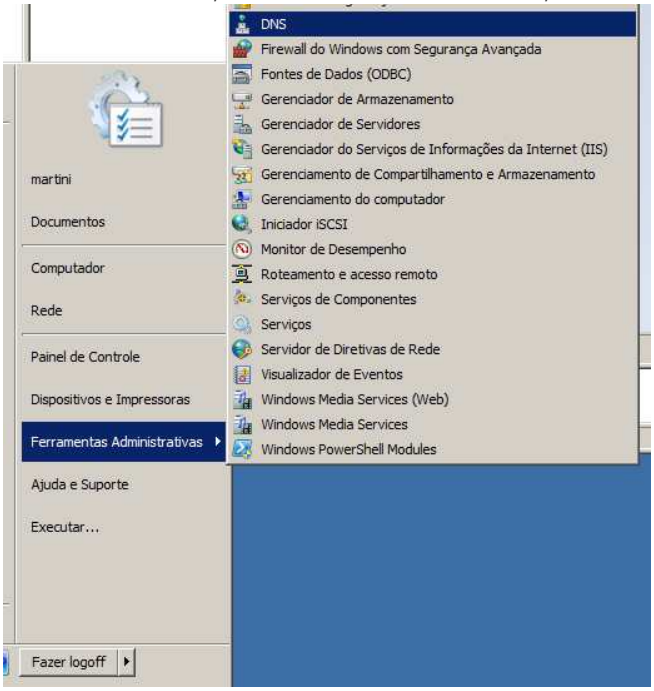
nnn IN PTR serverN.dominio.com.br.
;
;* n1, n2 ... nnn: indicam números dentro da faixa 128 a 191 em uso pelo cliente.
;-

Este arquivo de configuração é valido para os servidores DNS BIND. Caso o cliente utilize outro servidor DNS deve observar a mesma regra, ou seja, criar a zona somente para a sua faixa (i.e. 128-191.23.181.200.in-addr.arpa.), conforme determina a RFC 2317.
Caso o cliente configure a classe C completa (i.e. 23.181.200.in-addr.arpa.) as requisições não serão resolvidas.

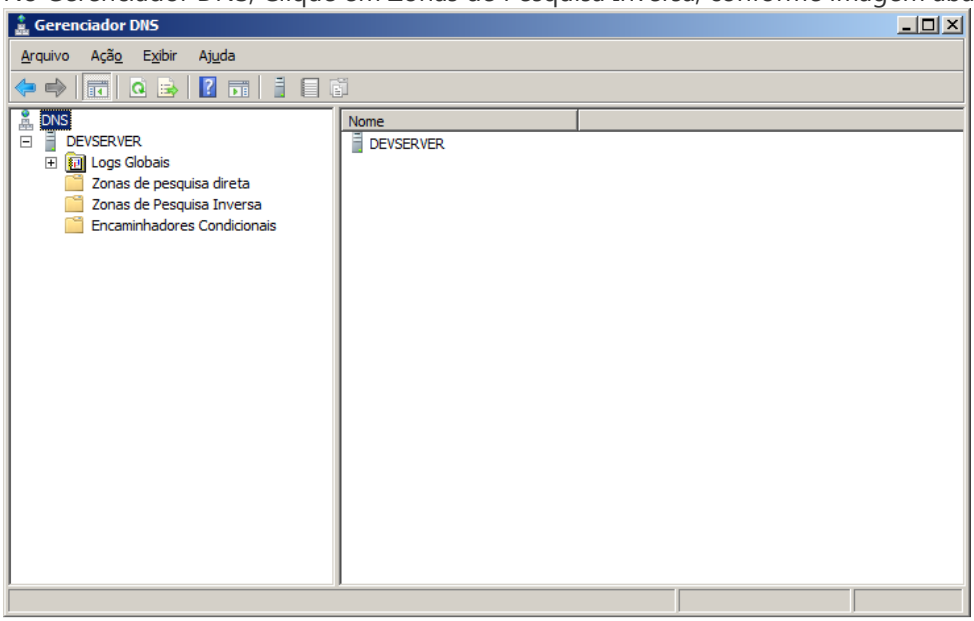
- ➔ **Windows 2k/2k3/2k8:**

Configurando um DNS Reverso no Windows Server: (para dns reverso /24)

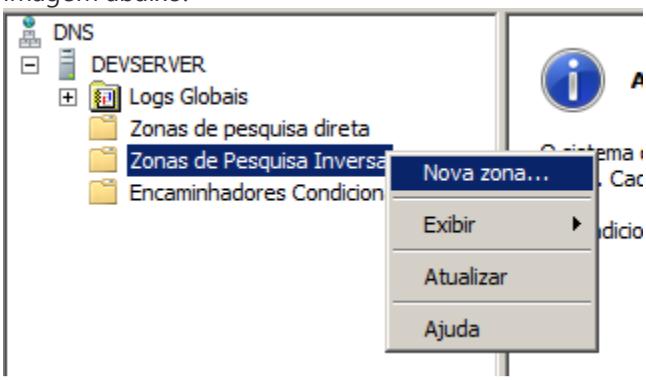
Para iniciar o DNS, você deve entrar em Iniciar, Ferramentas Administrativas e DNS, conforme imagem abaixo:



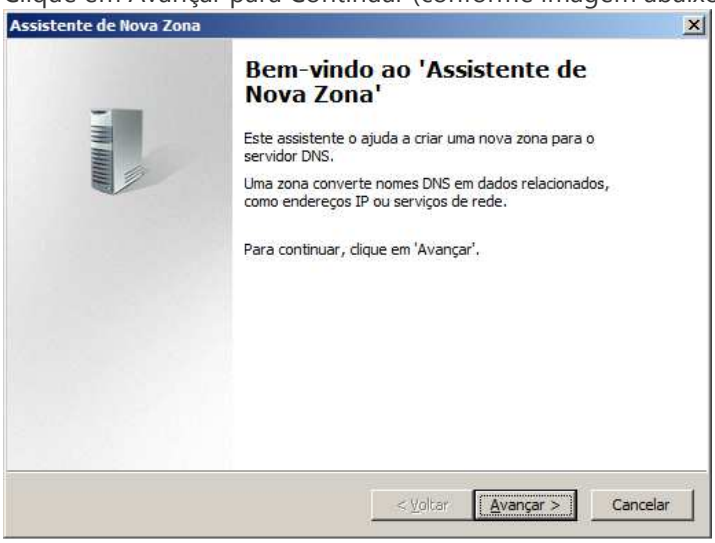
No Gerenciador DNS, Clique em Zonas de Pesquisa Inversa, conforme imagem abaixo:



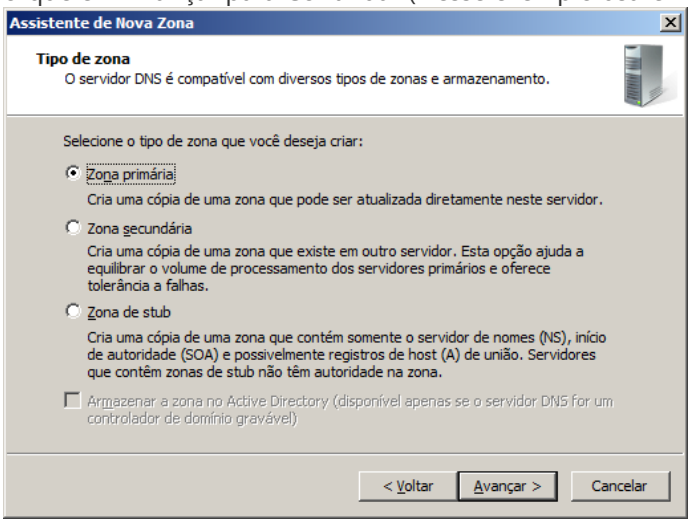
Clique com o Botão Direito em Zonas de Pesquisa Inversa (Ou no Menu Ações) e Clique em Nova Zona..., conforme imagem abaixo:



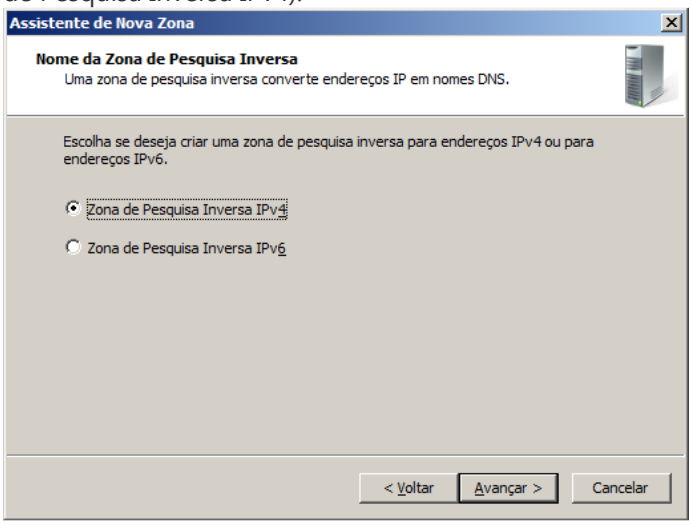
Agora é aberto o Wizard para adicionar a Zona de DNS Reverso.
Clique em Avançar para Continuar (conforme imagem abaixo):



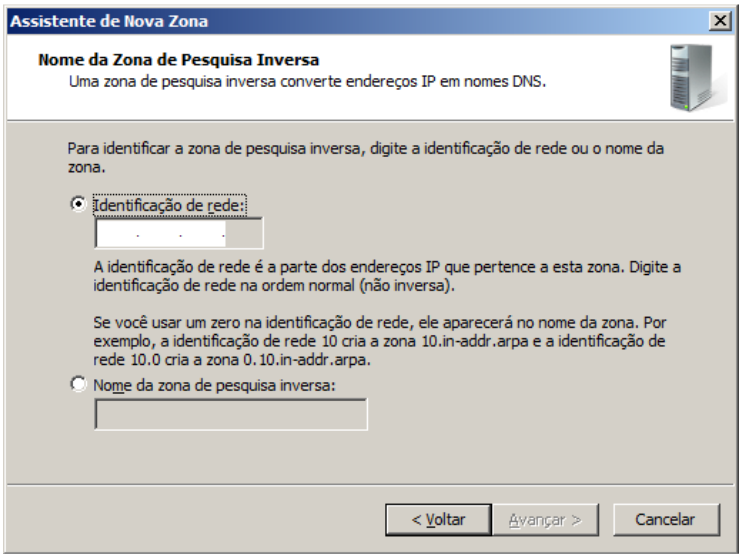
Selecione o Tipo de Zona do DNS Reverso (Se for Primária = Primeira | Secundária = Uma cópia de uma zona já existente em outro servidor | Zona de stub = Uma cópia de uma zona de servidor de nomes (NS). Após a Seleção clique em Avançar para Continuar (Nesse exemplo usaremos a opção Zona primária):



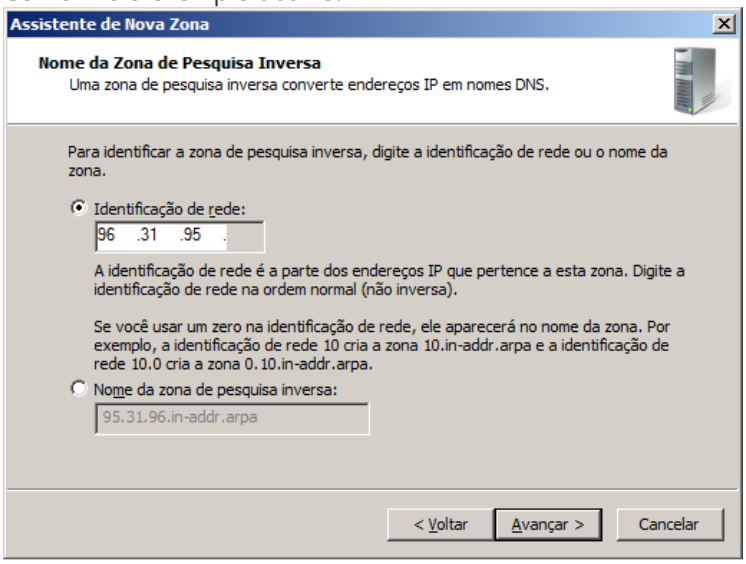
Selecione o tipo de IP da Zona. (IPv4 ou IPv6) – e clique em Avançar para continuar (Nesse exemplo usaremos a Zona de Pesquisa Inversa IPv4):



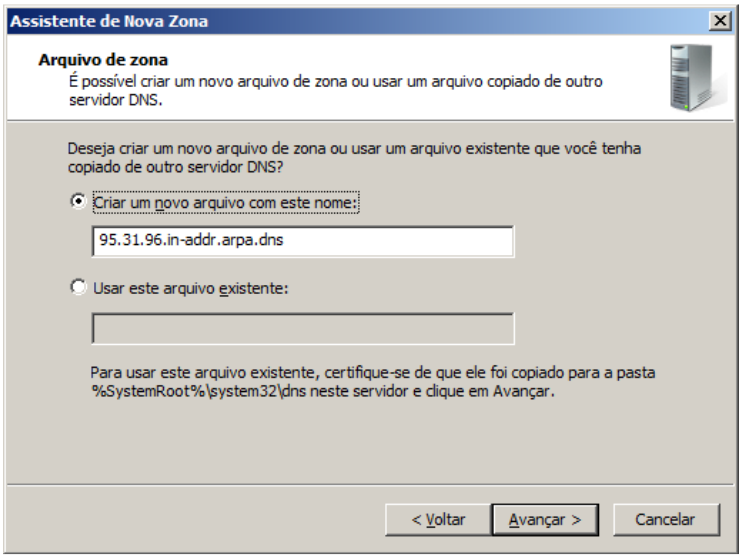
Agora nesse ponto, você deve informar o Endereço IP (Em Identificação de rede), Lembre-se que você apenas vai poder informar os 3 primeiros conjuntos do IP. (Você também pode usar o Nome da Zona de Pesquisa inversa – Para Usuários Avançados). Após informar o seu IP (primeiros 3 conjuntos de números) clique em Avançar para continuar:



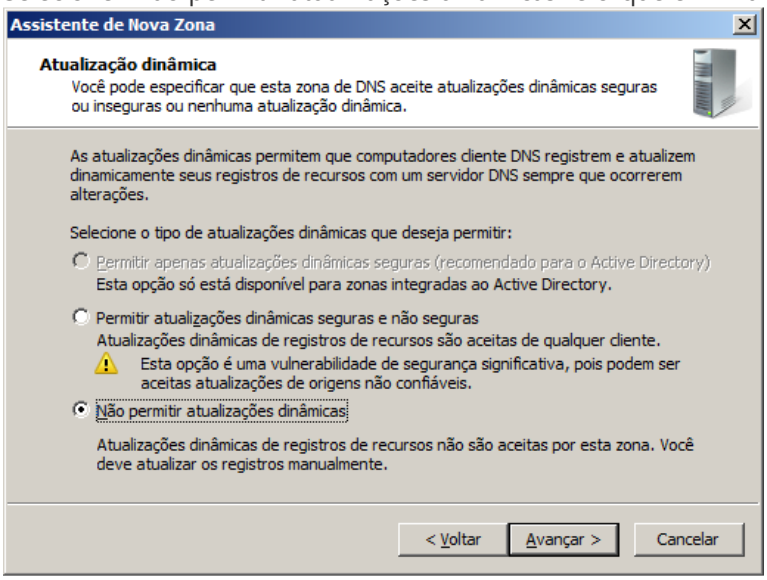
Conforme o exemplo abaixo:



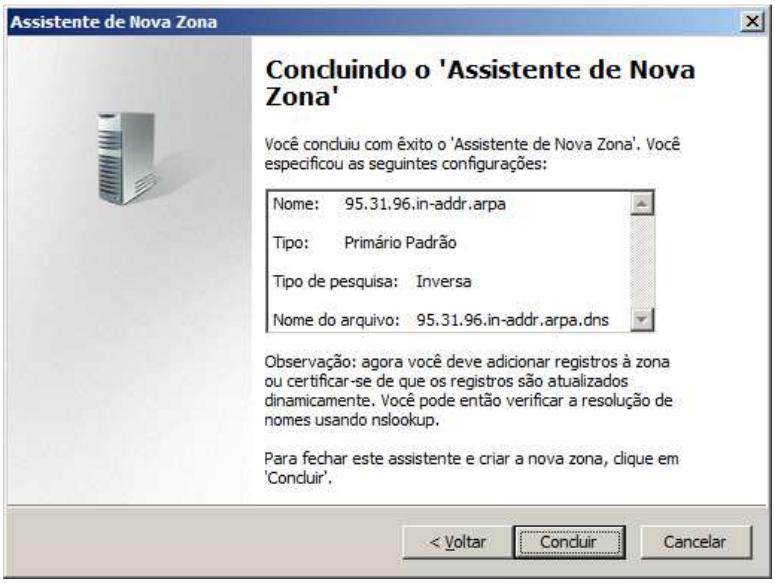
Agora informe o nome do Arquivo da Zona que você acaba de adicionar (Recomendo que deixe a padrão do DNS Server, conforme imagem abaixo) e clique em Avançar para continuar:



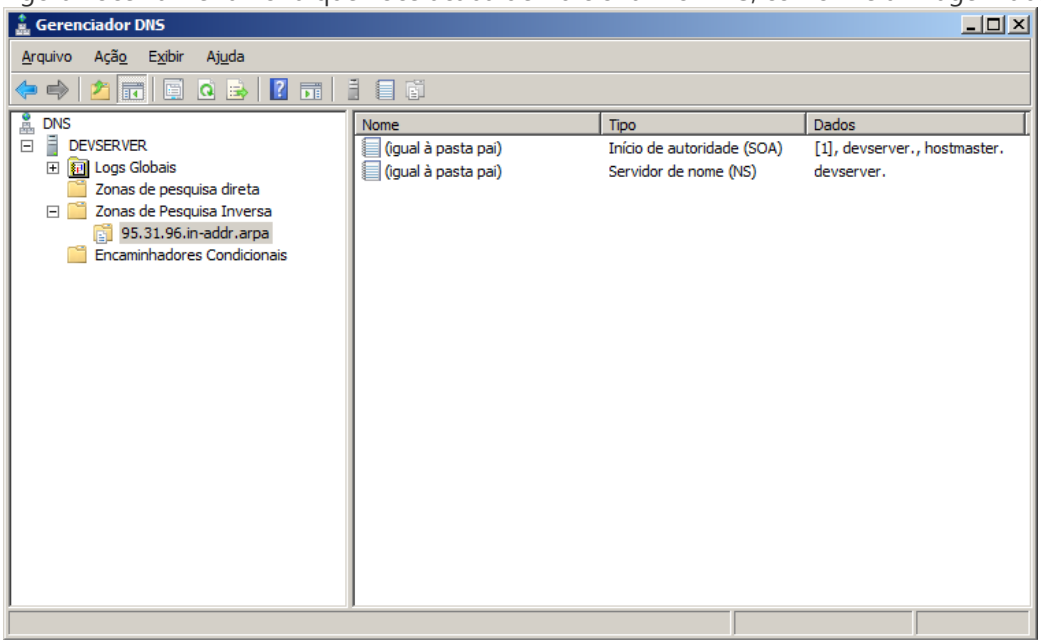
Selecione "Não permitir atualizações dinâmicas" e clique em Avançar para continuar:



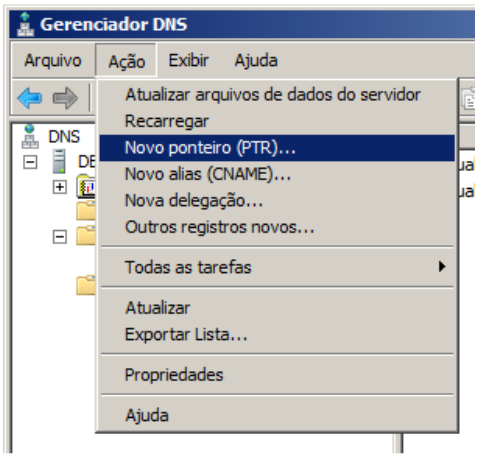
A Zona foi adicionada com Sucesso. Clique em Concluir para Fechar a Janela de Wizard.



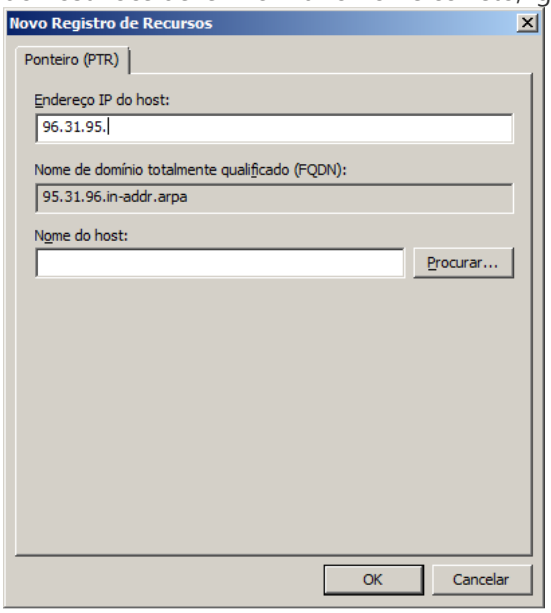
Agora você vai ver a Zona que você acaba de Adicionar no DNS, conforme a imagem abaixo:



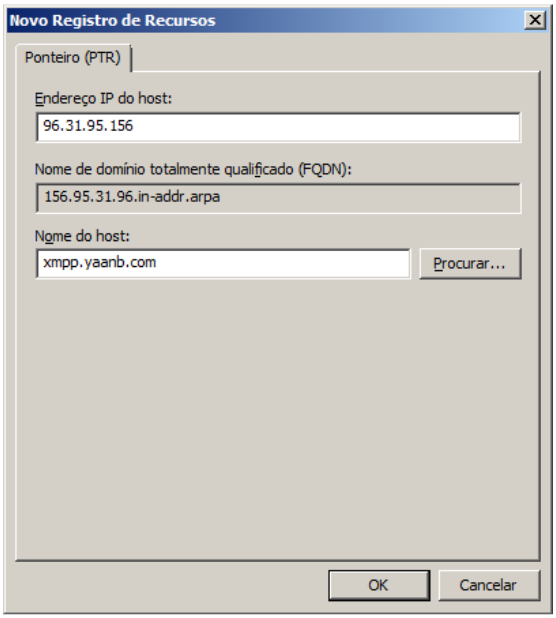
Agora vamos adicionar os Endereços IPs e seus nomes, clicando em Ação e Novo ponteiro (PTR), conforme imagem abaixo:



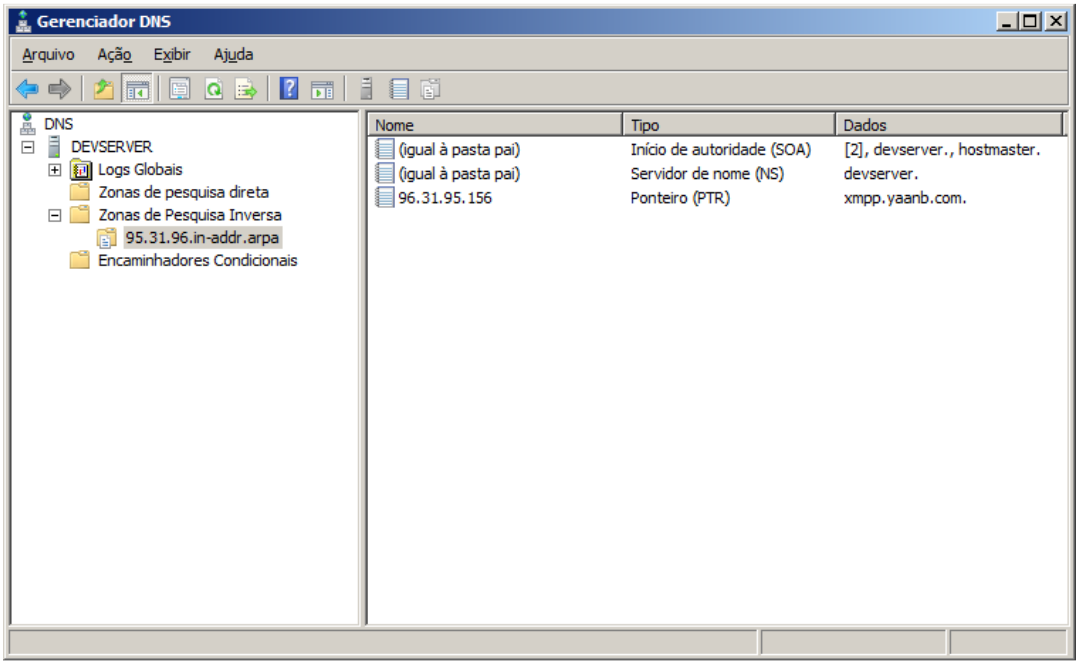
Na Tela de "Novo Registro de Recursos", informe em Endereço IP do Host (No caso o último bloco do IP), e em Nome do host você deve informar o nome correto, igual ao que você apontou o nome do host no DHCP:



Conforme exemplo abaixo:



E clique em OK para Adicionar o Registro do Recurso.
Agora faça o mesmo processo de Adicionar o "Novo Ponteiro (PTR)" para cada IP que você deseje fazer o DNS reverso.



Configurando um DNS Reverso no Windows Server: (para dns reverso /25, /26, /27, /28, /29)

Um esquema de endereçamento IP "classes" é aquele que não pode dividir uma rede IP em segmentos menores. Por exemplo, um endereço classe c de 192.168.1.0 com uma máscara de sub-rede de 255.255.255.0 é um esquema de endereçamento IP com classes.

Um esquema de endereçamento IP "sem classe" é aquele que usa uma máscara de sub-rede para dividir um endereço IP em segmentos menores. Por exemplo, um endereço classe c de 192.168.1.0 com uma máscara de sub-rede de 255.255.255.192 é um esquema de endereçamento IP classless. Com essa rede, você também terá os seguintes endereços de rede IP: 192.168.1.64, 192.168.1.128 e 192.168.1.192.

Quando sub-redes de redes IP, bits adicionais são tiradas da parte do host do endereço IP e para a parte de rede. Isso é definido pela adição de bits adicionais para a máscara de sub-rede. O valor 11111111.11111111.11111111.00000000 nos mostra uma máscara de sub-rede em classes para uma rede classe c 255.255.255.0, enquanto o valor 11111111.11111111.11111111.11000000 ilustra a classless máscara de sub-rede 255.255.255.192. Portanto, no exemplo acima, sabemos que:

```
If the subnet mask is   The subnet mask bit-count is
   --------------------   ----------------------------
   255.255.255.128          25
   255.255.255.192          26
   255.255.255.224          27
   255.255.255.240          28
   255.255.255.248          29
   255.255.255.252          30
   255.255.255.254          31
```

A sintaxe:

Delegado pesquisa inversa em sub-rede zonas podem ser usadas para transferir o controle administrativo entre qualquer pai e filho IN-ADDR.Zona ARPA no DNS. Configurações comuns envolvem um ISP (pai) delegar a um Site do cliente (filho) ou uma delegação da sede (pai) para um Site remoto corporativo (filho). Como o cenário do provedor é mais comum, será usado no exemplo a seguir.

Ao criar zonas de pesquisa inversa classless, você pode usar a notação a seguinte:

<subnet>-< contagem de bits de máscara de sub-rede >. 100.168.192.in-addr.arpa ou

<subnet> / < contagem de bits de máscara de sub-rede >. 100.168.192.in-addr.arpa ou

<subnet>. < contagem de bits de máscara de sub-rede >. 100.168.192.in-addr.arpa ou

SubnetX <subnet>. 100.168.192.in-addr.arpa (onde x é o número de sub-rede atribuído pelo pai) ou

<subnet>. 100.168.192.in-addr.arpa

Por exemplo:

64-26.100.168.192.in-arpa ou

64/26.100.168.192.in-addr.arpa ou

64.26.100.168.192.in-addr.arpa ou

Arpa Subnet3.100.168.192.in ou

64.100.168.192.in-addr.arpa

Isso indica que a zona de pesquisa inversa em sub-rede 64 sub-rede que está usando 26 bits para a máscara de sub-rede.

Observação: Se você executará as transferências de zona, entre pai e filho você precisa verificar a sintaxe dos arquivos que serão transferidos entre servidores DNS. Nem todas as versões de servidores DNS oferecerá suporte os vários métodos de sintaxe definidos na RFC (hífen, a barra, etc.). Microsoft DNS oferecem suporte qualquer desses métodos.

Observação: A sintaxe é escolhida no domínio pai deve ser idêntico à sintaxe usada no domínio filho.

A lista de verificação:

Preenchendo a seguinte lista de verificação fará a movimentação por meio deste documento.

```
Parent Checklist                          Child Checklist
 ----------------                          ---------------
 <Parent DNS server name>                  <Child DNS server name>
 <Parent DNS server IP>                    <Child DNS server IP>
 <subnet mask>                             <subnet mask>
 <subnet><syntax><subnet mask bit count>   <subnet><syntax><subnet  mask bit
                                           count>
```

Aqui está o exemplo de um ISP que tenha levado um intervalo de classe c e em sub-redes em 4 sub-redes, usando o 255.255.255.192, usaremos a máscara de sub-rede. 4 Sub-redes são 192.168.100.0, 192.168.100.64, 192.168.100.128 e 192.168.100.192. A sub-rede local do cliente sendo delegada é o segundo intervalo, que é a rede 64 usando 126 65 para os endereços IP de host.

```
Parent Checklist       Child Checklist
   ----------------       ---------------
   NS.microsoft.com       NS1.msn.com
   192.168.43.8           192.168.100.126
   255.255.255.192        255.255.255.192
   0-26                   64-26
   64-26
   128-26
   192-26
```

Explicação para ambientes Windows 2000 e Windows Server 2003:

1. Inicie o MMC (Console de gerenciamento Microsoft) do DNS.
2. Em Exibir, altere de modo de exibição padrão para Avançado.
3. Realce zonas de pesquisa inversa, clique com botão direito e selecione nova zona.
4. Selecione zona tipo integrado ao Active Directory ou primária padrão, clique em **Avançar**.
5. Selecione a opção para o "nome de zona de pesquisa inversa". Digite o nome da zona de pesquisa inversa (por exemplo, 64-26.100.168.192.in-addr. arpa) para a sub-redes endereço classe C. Certifique-se de usar a convenção de nomes fornecida pelo administrador do domínio pai, clique em Avançar.
6. Se você selecionou primária padrão, você pode criar um novo arquivo de zona ou se houver um arquivo de zona existente, você pode colocá-lo no diretório %systemroot%\winnt\system32\dns e o servidor lê-lo do diretório.
7. Adicione manualmente o PTR (registros de ponteiro) como faria em qualquer zona de pesquisa inversa.

   Por exemplo:
   65 Host65.msn.com PTR

8. Talvez você precise configurar os servidores DNS que hospedam a zona delegada, filho para encaminhar para servidores DNS pai. Isso permite que os servidores DNS filhos resolver registros em zonas hospedadas por servidores DNS pai.

Explicação para ambiente Windows NT 4.0:

1. Aplica o Service Pack mais recente do Microsoft Windows NT.
2. Reinicie o computador quando solicitado.
3. Clique em **Iniciar**, selecione **programas**, selecione **Ferramentas administrativas** e clique em **Gerenciador de DNS**.
4. No menu **DNS** , clique em **Novo servidor**, digite o nome de host ou endereço IP do servidor DNS e clique em **OK**.
5. Crie uma zona de pesquisa inversa em sub-rede usando as seguintes etapas:
   a. Clique em seu servidor DNS e, em seguida, no menu **DNS** , clique em **Nova zona** ..
   b. Clique no botão de rádio **principal** na caixa de diálogo **Criar nova zona** e clique em **Avançar**.
   c. Acordo com a sintaxe escolhida no pai selecione um dos pares abaixo. Em nosso exemplo podemos digitar "64-26.100.168.192.in-addr. arpa" (sem as aspas) na caixa de texto Nome da zona e pressione Tab.

```
d. Zone Name: 64-26.100.168.192.in-addr.arpa
e.          Zone File: 64-26.100.168.192.in-addr.arpa.dns or
f.
g.          Zone Name: 64/26.100.168.192.in-addr.arpa
h.          Zone File: 64.26.100.168.192.in-addr.arpa.dns or
i.
j.          Zone Name: 64.26.100.168.192.in-addr.arpa
k.          Zone file: 64.26.100.168.192.in-addr.arpa.dns or
l.
m.          Zone Name: 64.100.168.192.in-addr.arpa
n.          Zone file: 64.100.168.192.in-addr.arpa.dns or
o.
p.          Zone Name: Subnet64.100.168.192.in-addr.arpa
            Zone file: Subnet64.100.168.192.in-addr.arpa.dns or
```

   Observação: Administrador de DNS da Microsoft automaticamente preencherá o campo nome do arquivo ao criar zonas. Se você usar a sintaxe "/" certifique-se alterar o nome do arquivo e substituir o caractere "/" porque o sistema de arquivos subjacente não permitirá uma "/" no nome do arquivo. Basta substituir o caractere de barra no nome do arquivo com outro caractere como sugerido no segundo exemplo acima (64.26.100.168.192.in-addr.arpa.dns).

   q. A caixa de texto do arquivo de zona deve ser preenchida automaticamente com 64-26.100.168.192.in-addr.arpa.dns.
   r. Clique em **Concluir**.
   s. Repita as etapas a até e para as sub-redes adicionais sendo delegada a você.
6. Quando tiver terminado de criar as zonas, pare o servidor DNS usando um dos seguintes métodos:
   - Clique em **Iniciar**, selecione **configurações**, **painel de controle** e clique duas vezes no ícone **Serviços**. Selecione o servidor DNS da Microsoft na lista **serviço** e clique em **Parar**.
   - Digite o seguinte comando no prompt e pressione Enter:

```
NET STOP DNS
```

7. **Observação:** É importante parar o serviço DNS antes de editar os arquivos de zona ou você poderá perder informações registradas manualmente.
8. Abra o arquivo de zona de pesquisa inversa em sub-rede usando um editor de texto. Agora é necessário criar registros PTR para cada endereço no intervalo de sub-redes delegado. Adicione o seguinte ao final do arquivo:

```
9.       65                      PTR     host65.msn.com.
```

```
10.       66                      PTR     host66.msn.com.
11.       67                      PTR     host67.msn.com.
12.       ...
          126                     PTR     host126.msn.com.
```

Observação: A elipse "...", indica os endereços IP e hosts entre 67 e 126 exclusivos. Reticências não são válidas no arquivo.

13. Após inserir os registros PTR, salvar e sair do arquivo.
14. Reinicie o servidor DNS usando um dos seguintes métodos:
    - Clique em Iniciar, aponte para configurações, clique em Painel de controle e clique duas vezes no ícone **Serviços**. Selecione o servidor DNS da Microsoft na lista serviço e clique em **Iniciar**.
    - Digite o seguinte comando no prompt de comando e pressione Enter:
      `NET START DNS`
15. Agora devem ser capazes de realizar uma pesquisa inversa para endereços IP na zona de pesquisa inversa delegada hosts na Internet. Uma última série de etapas é necessária para hosts que usam o Site de cliente DNS para executar corretamente as inversas. É necessário que uma cópia da zona em sub-redes não estar presente no servidor DNS do domínio filho. A maneira mais fácil de fazer isso se tornará uma zona secundária para o ISP. Crie a zona secundária usando as seguintes etapas:
    . Clique em seu servidor DNS e, em seguida, no menu **DNS** , clique em **Nova zona** ..
    a. Clique no botão de rádio **secundária** na caixa de diálogo **Criar nova zona** ..
    b. Para **zona:** digite 100.168.192.in-addr.arpa e **Server:** digite o < IP do servidor DNS pai >. Para nosso exemplo, é 192.168.43.8. Clique em **Avançar**.
    c. Para **o nome de zona:** digite 100.168.192.in-addr.arpa e **arquivo de zona:** digite 100.168.192.in-addr.arpa.dns.Clique em **Avançar**.
    d. No campo IP mestres, insira novamente o < IP do servidor DNS pai >. Nosso exemplo é 192.168.43.8. Clique em **Adicionar**, clique em **Avançar**e, em seguida, clique em **Concluir**.
16. Talvez você precise configurar os servidores DNS que hospedam a zona delegada, filho para encaminhar para servidores DNS pai. Isso permite que os servidores DNS filhos resolver registros em zonas hospedadas por servidores DNS pai.

Exemplo de arquivo de zona:

Arquivo de zona de pesquisa inversa em sub-rede filho

```
;
;  Database file 64-26.100.168.192.in-addr.arpa.dns for 64-26.100.168.192.in-addr.arpa zone.
;      Zone version:  1
;

@                       IN  SOA NS1.msn.com. administrator.msn.com. (
                         1           ; serial number
                         3600        ; refresh
                         600         ; retry
                         86400       ; expire
                         3600      ) ; minimum TTL

;
;  Zone NS records
;

@                       NS       NS1.msn.com.

;
;  Zone records
```

```
;

65                      PTR     host65.msn.com.
66                      PTR     host66.msn.com.
67                      PTR     host67.msn.com.
...
126                    PTR     host126.msn.com.
```

Observação Novamente, nos exemplos acima, as elipses indicam os endereços IP omitidos entre 67 e 126. Reticências não são válidas no arquivo.

Abaixo seguem alguns links que podem ajudar na configuração do servidor DNS do cliente.

Servidor BIND, para LINUX e UNIX

- http://info.matik.com.br/modules.php?op=modload&name=News&file=article&sid=47&mode=thread&order=0&thold=0
- http://br-linux.org/tutoriais/001970.html
- http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=1667
- http://www.inf.ufes.br/~proinfo/docs/dns/tarefa7/tarefa7.html

Servidor DNS Windows NT/2000

- http://www.fernandomartini.com/blog/configurando-um-dns-reverso-no-windows-2k2k32k8/
- http://support.microsoft.com/kb/174419/pt-br
- http://www.baboo.com.br/absolutenm/anmviewer.asp?a=4153
- http://www.w2k.com.br/images/curso/ImplementandoResolucaoNomesUsandoDNS/ImplementandoResolucaoNomesUsandoDNS.htm
- http://www.clubedasredes.eti.br/soft0004.htm
- http://support.microsoft.com/default.aspx?scid=kb;pt-br;308201