



INSTALANDO E CONFIGURANDO DNS SERVER NO WINDOWS 2008 R2

***Administrador saiba como implementar e administrar
corretamente o DNS Server***

Sumário

Autores.....	3
Visão geral	4
Hierarquia.....	5
Servidores de domínio de topo (Top-Level Domain)	5
Servidores autoritativos.....	6
Melhorias de Performance.....	7
Cache	7
Servidor Local.....	7
DNS resolvers	7
DNS Reverso	8
Obtenção de nomes de domínio e endereços IP	8
Instalando um servidor de DNS no Windows Server 2008 R2	9
Configurando DNS Server no Windows Server 2008 R2	17
Referências:	35

Autores

Erick Albuquerque: trabalha com infra-estrutura desde 2004, com foco em tecnologias Microsoft. Nomeado pela Microsoft como Most Valuable Professional (MVP), certificado em MCP, MCTS, MCITP System Administrator e MCITP Enterprise Administrator. Atualmente trabalha na RedeTV!, como responsável por toda infra-estrutura do portal (www.redetv.com.br).

Twitter: [@_ealbuquerque](https://twitter.com/_ealbuquerque)

email: erick.albuquerque@hotmail.com

Linkedin: <http://www.linkedin.com/in/easantos>

<http://iisbrasil.wordpress.com> | <http://erickalbuquerque.com.br>

Daniel Donda: Especializado em sistemas operacionais de rede e segurança. Atua no mercado de TI desde 1996. MVP Windows Expert-IT Pro possui as seguintes certificações MCP, MCT, MCITP-EA, MCSA+Security, MCSE+Security, MCSE+Messaging, EC-Council C|EH, C|HFI, C|EI autor de diversos artigos técnicos e autor dos livros "MCSE/MCSA Guia de Certificação Windows Server 2003" e "Administração do Windows Server 2008 R2 - Server Core". Lider do grupo MUGSS Mcsesolution.com e colaborador do MCPBrasil.com. Atua ainda como palestrante do Microsoft TechDay www.mstechday.com e colaborador ativo do TechNet Wiki www.technet.com/wiki. Beta-tester oficial de sistemas operacionais Microsoft. Twitter: @danieldonda

DNS é a abreviatura de Domain Name System, criado a partir da necessidade existente de traduzir os endereços IP para um tipo de mais alto nível, que poderia ser lembrando com maior facilidade por pessoas comuns, neste artigo será apresentado uma visão geral sobre o DNS bem como as boas práticas para instalação e configuração.

Visão geral

Um recurso da internet um site, por exemplo, pode ser identificado de duas maneiras: pelo nome de domínio “www.devmedia.com.br” ou pelo endereço IP dos equipamentos que o hospedam (por exemplo, 67.215.65.132 é o IP associado ao domínio www.devmedia.com.br). Endereços IP são usados pela camada de rede para determinar a localização física e virtual do equipamento. Nomes de domínio, porém, são mais fáceis de ser memorizados pelo usuário e empresas. É então necessário um mecanismo para traduzir um nome de domínio em um endereço IP. Esta é a principal função do DNS.

Nota: Domínio é um nome que serve para localizar e identificar conjuntos de computadores na Internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet. Sem ele, teríamos que memorizar uma sequência grande de números.

Nota: O endereço IP, de forma genérica, é um endereço que indica o local de um nó em uma rede local ou pública.

Para um melhor uso dos endereços de equipamentos em rede pelas pessoas, utiliza-se a forma de endereços de domínio, tal como “www.devmedia.com.br”. Cada endereço de domínio é convertido em um endereço IP pelo DNS. Este processo de conversão é conhecido como “resolução de nomes”.

Hierarquia

Devido ao tamanho da internet, armazenar todos os pares domínio - endereço IP em um único servidor DNS seria inviável, por questões de escalabilidade que incluem:

- **Confiabilidade:** se o único servidor de DNS falhasse, o serviço se tornaria indisponível para o mundo inteiro.
- **Volume de tráfego:** o servidor deveria tratar os pedidos DNS do planeta inteiro.
- **Distância:** grande parte dos usuários estaria muito distante do servidor, onde quer que ele fosse instalado, gerando grandes atrasos para resolver pedidos DNS.
- **Manutenção do banco de dados:** o banco de dados deveria armazenar uma quantidade de dados enorme e teria que ser atualizado com uma frequência muito alta, toda vez que um domínio fosse associado a um endereço IP.

A solução encontrada é fazer do DNS um banco de dados distribuído e hierárquico. Os servidores DNS se dividem nas seguintes categorias:

No topo da hierarquia estão os 13 servidores raiz. Um Servidor Raiz (**Root Name Server**) é um servidor de nome para a zona raiz do DNS (**Domain Name System**). A sua função é responder diretamente às requisições de registros da zona raiz e responder a outras requisições retornando uma lista dos servidores de nome designados para o domínio de topo apropriado. Os servidores raiz são parte crucial da internet por que eles são o primeiro passo em traduzir nomes para endereços IP e são usados para comunicação entre hosts.

Servidores de domínio de topo (Top-Level Domain)

Cada domínio é formado por nomes separados por pontos. O nome mais à direita é chamado de domínio de topo. Exemplos de domínios de topo são .com, .org, .net, .edu, mil e .gov. Cada servidor de domínio de topo conhece os endereços dos servidores autoritativos que pertencem àquele domínio de topo, ou o endereço de algum servidor DNS intermediário que conhece um servidor autoritativo. Veja a tabela com os descritivos do Top-Level-Domain:

Top-level-domain	Descrição
net	Diversos
com	Organizações comerciais

gov	Organizações governamentais
edu	Instituições educacionais
mil	Instituições militares
org	Organizações não comerciais

Servidores autoritativos

O servidor autoritativo de um domínio possui os registros originais que associam aquele domínio a seu endereço de IP. Toda vez que um domínio adquire um novo endereço, essa informação deve ser adicionada a pelo menos dois servidores autoritativos. Um deles será o servidor autoritativo principal e o outro, o secundário. Isso é feito para minimizar o risco de, em caso de erros em um servidor DNS, perder todas as informações originais do endereço daquele domínio.

Com essas três classes de servidores já é possível resolver qualquer requisição DNS. Basta fazer uma requisição a um servidor raiz, que retornará o endereço do servidor de topo responsável. Então se repete a requisição para o servidor de topo, que retornará o endereço do servidor autoritativo ou algum intermediário. Repete-se a requisição aos servidores intermediários (se houver) até obter o endereço do servidor autoritativo, que finalmente retornará o endereço IP do domínio desejado. Repare que essa solução não resolve um dos problemas de escalabilidade completamente: os servidores raiz tem que ser acessados uma vez para cada requisição que for feita em toda a internet. Esses servidores também podem estar muito longe do cliente que faz a consulta.

Além disso, para resolver cada requisição, são precisas várias consultas, uma para cada servidor na hierarquia entre o raiz e o autoritativo. Esta forma de resolver consultas é chamada não-recursividade: cada servidor retorna ao cliente (ou ao servidor local requisitante, como explicado adiante) o endereço do próximo servidor no caminho para o autoritativo, e o cliente ou servidor local fica encarregado de fazer as próximas requisições. Há também o método recursivo: o servidor pode se responsabilizar por fazer a requisição ao próximo servidor, que fará a requisição ao próximo, até chegar ao autoritativo, que retornará o endereço desejado, e esse endereço será retornado para cada servidor no caminho até chegar ao cliente. Esse método faz com que o cliente realize apenas uma consulta e receba diretamente o endereço desejado, porém

aumenta a carga dos servidores no caminho. Por isso, servidores podem se recusar a resolver requisições recursivas.

Melhorias de Performance

Dois recursos são usados em conjunto para reduzir a quantidade de requisições que os servidores raiz devem tratar e a quantidade de requisições feitas para resolver cada consulta:

Cache

Toda vez que um servidor retorna o resultado de uma requisição para a qual ele não é autoridade (o que pode acontecer no método de resolução recursivo), ele armazena temporariamente aquele registro. Se, dentro do tempo de vida do registro, alguma requisição igual for feita, ele pode retornar o resultado sem a necessidade de uma nova consulta. Note que isso pode provocar inconsistência, já que se um domínio mudar de endereço durante o tempo de vida do cache, o registro estará desatualizado. Apenas o servidor autoritativo tem a garantia de ter a informação correta. É possível exigir na mensagem de requisição DNS que a resposta seja dada pelo servidor autoritativo.

Servidor Local

Esse tipo de servidor não pertence a hierarquia DNS, mas é fundamental para o seu bom funcionamento. Em vez de fazer requisições a um servidor raiz, cada cliente faz sua requisição a um servidor local, que geralmente fica muito próximo do cliente fisicamente. Ele se encarrega de resolver a requisição. Com o uso de cache, esses servidores podem ter a resposta pronta, ou ao menos conhecer algum servidor mais próximo ao autoritativo que o raiz (por exemplo, o servidor de topo), reduzindo a carga dos servidores raiz.

DNS resolvers

O lado do cliente é chamado de DNS resolvers, é responsável por iniciar e sequenciar as consultas que levam a uma resolução máxima do recurso procurado, por exemplo, a tradução de um nome de domínio em um endereço IP.

Uma consulta DNS pode ser uma consulta de não-recursiva ou uma consulta recursiva:\

Uma consulta não-recursiva é aquela no qual o servidor DNS fornece um registro de um domínio para o qual é autorizada em si, ou que proporciona um resultado parcial sem consultar outros servidores.

Uma consulta recursiva é aquela para a qual o servidor DNS irá responder plenamente a consulta (ou dar um erro), consultando outros servidores de nome conforme necessário. Servidores DNS não são necessários para suportar consultas recursivas.

Os resolvers, ou outro servidor DNS agindo de forma recursiva, em nome do resolver, negocia uso do serviço de recursividade usando bits nos cabeçalhos de consulta.

Resolver geralmente implica iterar servidores de nome para encontrar as informações necessárias. No entanto, alguns resolvers tem a função mais simples, comunicando apenas com um único servidor de nomes. Esses resolvers simplesmente (chamado de "stub resolvers") dependem de um servidor de nomes recursivo para executar o trabalho de encontrar informações para eles.

DNS Reverso

Normalmente o DNS atua resolvendo o nome do domínio de um host qualquer para o endereço IP correspondente. O DNS Reverso resolve o endereço IP, buscando o nome de domínio associado ao host. Ou seja, quando temos disponível o endereço IP de um host e não sabemos o endereço do domínio(nome dado à máquina ou outro equipamento que acesse uma rede), tentamos resolver o endereço IP através do DNS reverso que procura qual nome de domínio está associado aquele endereço. Os servidores que utilizam o DNS Reverso conseguem verificar a autenticidade de endereços, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS.

Isto evita que alguém utilize um domínio que não lhe pertence para enviar spam, por exemplo.

Obtenção de nomes de domínio e endereços IP

O espaço de nomes de domínio e endereços IP são recursos críticos para a internet, no sentido que requerem coordenação global. Cada endereço IP deve identificar um único equipamento, de forma que não é possível atribuir

endereços IP de maneira descentralizada. Da mesma forma, um nome de domínio deve identificar o conjunto de computadores que o mantém. A organização responsável por atribuir nomes de domínio e endereços IP em nível global é a ICANN.

Nota: ICANN é uma entidade internacional sem fins lucrativos, responsável pela alocação do espaço de endereços do Protocolo da Internet (IP), pela atribuição de identificadores de protocolo, pela administração do sistema de nomes de domínio de primeiro nível genéricos (gTLDs) e com códigos de países (ccTLDs), assim como as funções de gerenciamento do sistema de servidores-raiz.

Instalando um servidor de DNS no Windows Server 2008 R2

Antes de iniciarmos a instalação do DNS é necessário configurar um IP estático, assegurar que todas as atualizações do servidor estão em dia, uma boa prática é monitorar o Event Viewer.

Nota: A configuração do IP estático é necessária para que não tenha problemas futuros com conectividade, performance da rede e resolução de nomes.

Nota: No event viewer são gravados logs de aviso e erros que podem ajudar a resolver diversos problemas antes e depois da instalação do DNS.

Para definir um IP estático siga os passos:

- a) Clique em **Start, Network, Network and Sharing center**
- b) Clique em **Change adapter settings**
- c) Selecione a **placa de rede**, clique com o **botão direito** em **Properties**
- d) Selecione **Internet Protocol Version 4 (TCP/IPv4)**, Clique em **Properties**

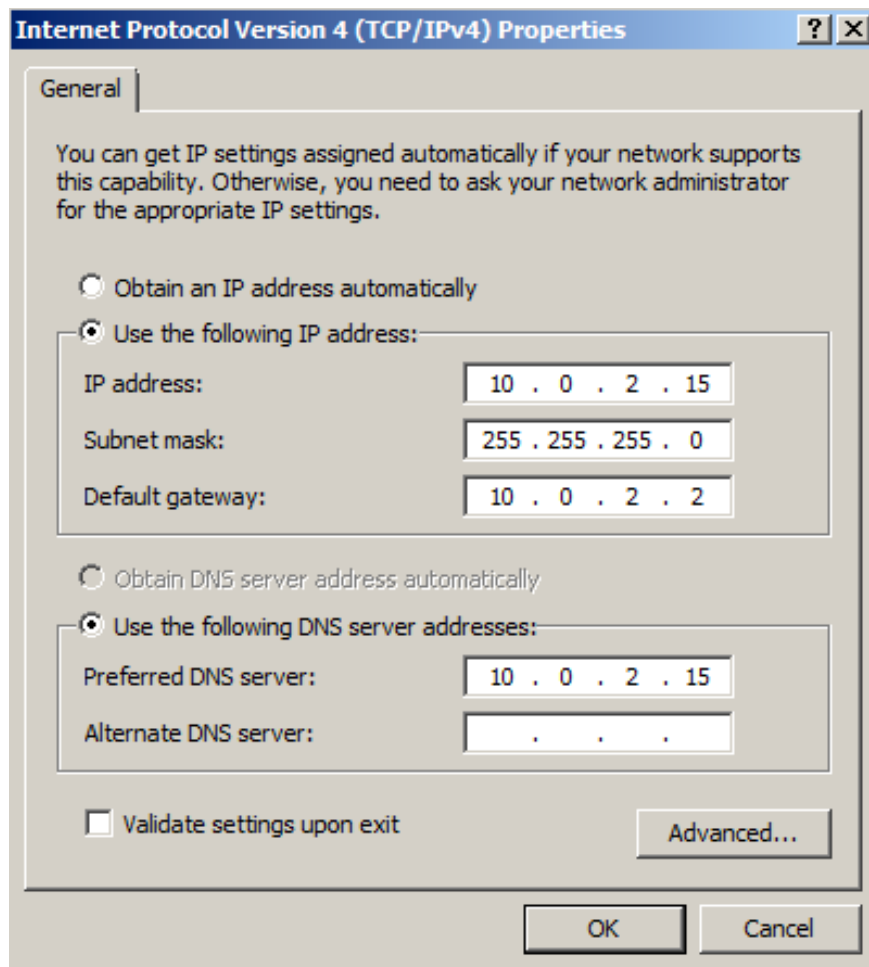


Figura 1: Propriedades da placa de rede

Na **Figura 1** podemos visualizar a configuração de **IP address** e **Subnet mask**, apenas salientando que em **Preferred DNS server** deve ser configurado o mesmo endereço IP do servidor que está sendo instalado o DNS, em **Alternate DNS server** devemos configurar o DNS secundário, se existir.

Após as validações, prosseguiremos com a instalação do servidor de DNS, para isso devemos estar com o Server Manager aberto, clicando em Start, Administrative Tools, Server Manager, em seguida, selecione Roles, no painel a direita clique em Add Roles. (Figura 2)

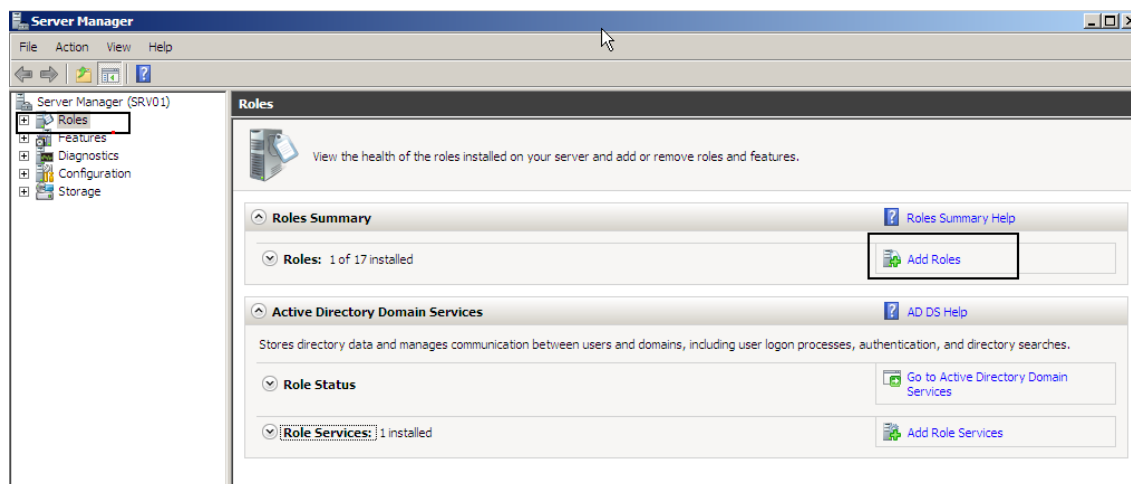


Figura 2: Server Manager

Ao clicar em **Add Roles**, iniciará uma janela chamada **Add Roles Wizard** (**Figura 3**), explicando que antes de seguir com a instalação é necessário verificar alguns itens, como:

- O usuário administrador precisa ter uma senha forte, isto é, com comprimento mínimo de 8 caracteres, letras maiúsculas e minúsculas, caracteres e alfanuméricos.
- Na configuração de rede é necessário configurar o IP estático.
- Todas as atualizações de segurança do Windows Update precisam estar instaladas.

Se os passos acima estiverem sido completados com sucesso, podemos prosseguir com a instalação clicando em next, caso contrario devemos cancelar e corrigir o problemas.

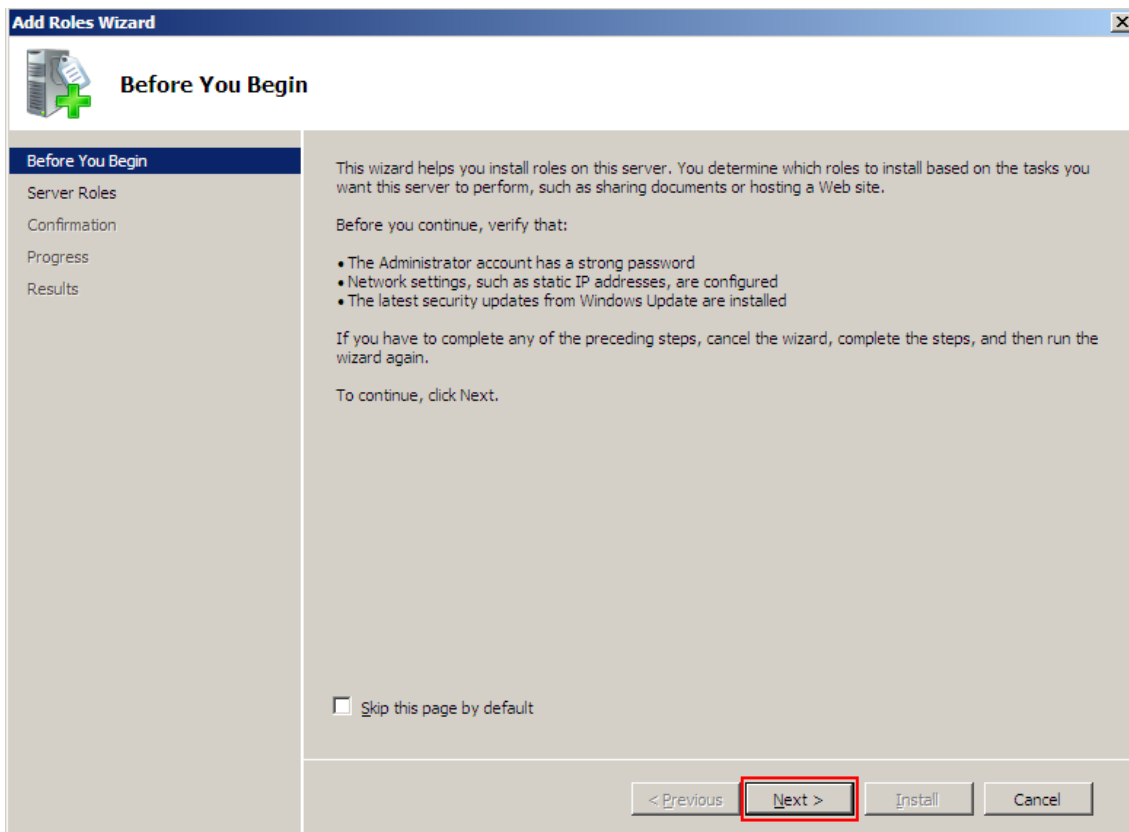


Figura 3: Antes de começar

Na próxima janela serão exibidos vários serviços o qual poderemos instalar para fazer um determinado papel no servidor, neste caso abortaremos apenas o DNS Server, para isso selecione o serviço **DNS Server** (Figura 4) e clique em next.

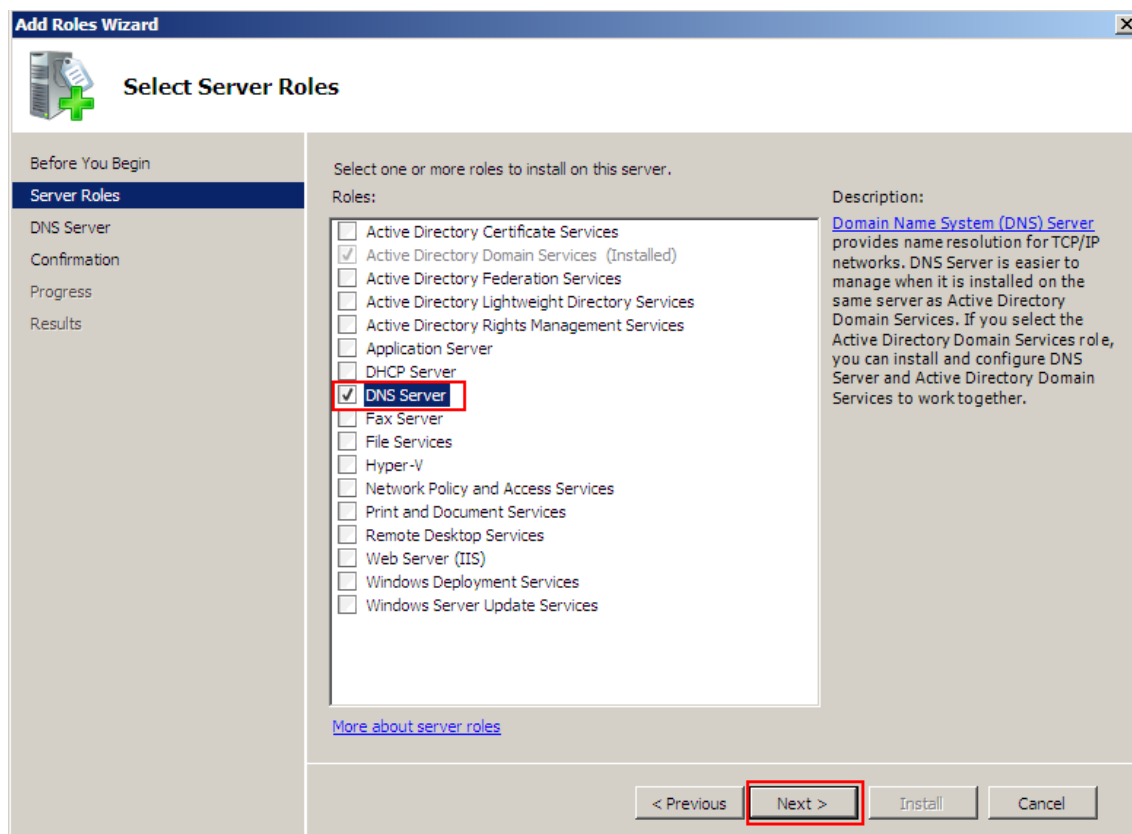


Figura 4: Selecionar Papel

Na próxima janela temos uma introdução ao DNS Server o qual fizemos neste artigo e alguns pontos que precisamos nos atentar, como:

- A integração do DNS Server com o ADDS (Active Directory Domain Services) adiciona automaticamente a replica de dados do DNS com o ADDS, tornando o gerenciamento muito mais fácil.
- Active Directory Domain Services requer que o DNS Server esteja instalado na rede, se você estiver instalando o Domain Controller, você pode também instalar o DNS Server utilizando a role Active Directory Domain Services Installation Wizard.

Resumindo se você estiver instalando um Domain Controller é possível instalar o DNS Server na mesma instalação, até porque o Domain Controller necessita que exista um DNS Server.

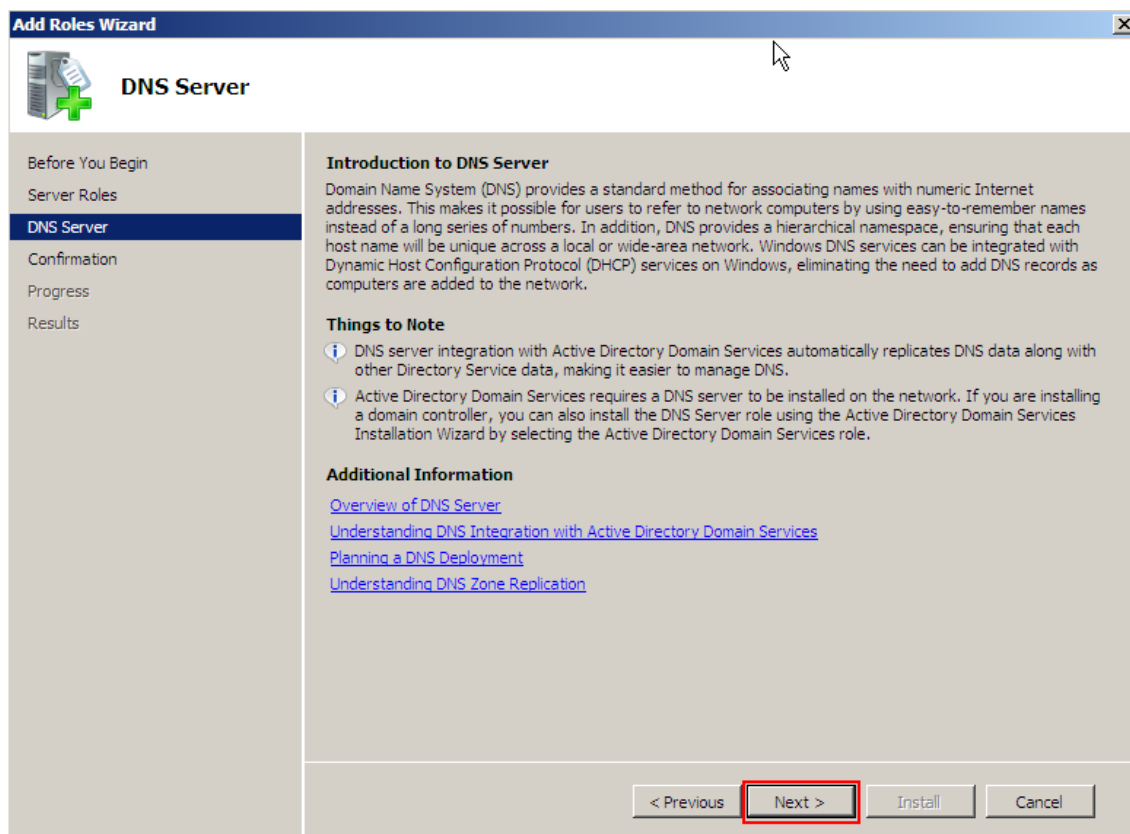


Figura 5: Introdução ao DNS Server

Na próxima janela temos informações sobre as roles e features que estamos prestes a instalar, vale fazer uma revisão para que não sejam instalado nada errado, confirmado os dados, prosseguiremos clicando em **Install** (Figura 6).

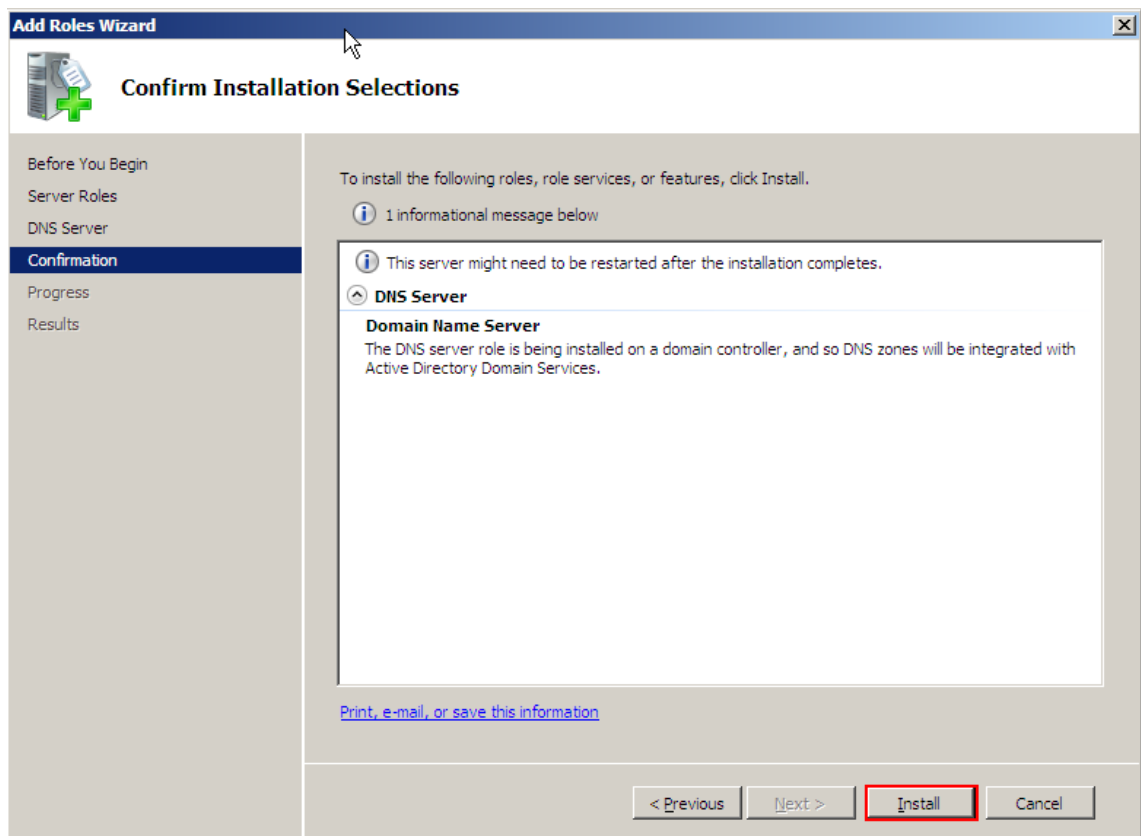


Figura 6: Confirme a instalação

Na próxima janela (Figura 7) temos a verificação dos pré-requisitos que vimos anteriormente e o progresso da instalação dos componentes e serviços necessários para o funcionamento do DNS Server.

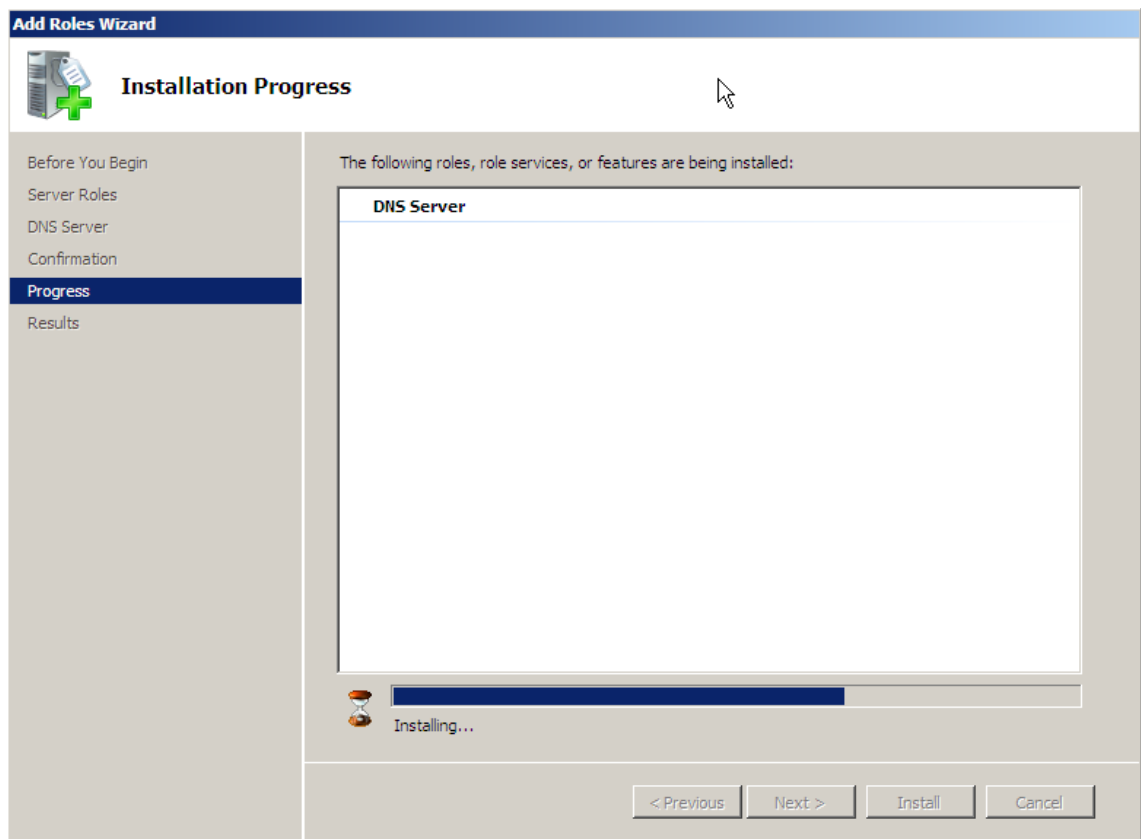


Figura 7: Progresso da instalação

Ao finalizar a instalação é gerado um relatório o qual pode conter alguns avisos de falha, erros ou recomendações, se nós tivermos seguido toda a recomendação não haverá problemas, apenas visualizaremos o aviso para que seja feito o Windows Update e instalado as atualizações de segurança, para isso clicamos em Start, Control Panel e selecionamos o Windows Update, seguida clique em Turn On.

Finalizamos a instalação do DNS Server, para finalizar o Wizard clique em close. (Figura 8)

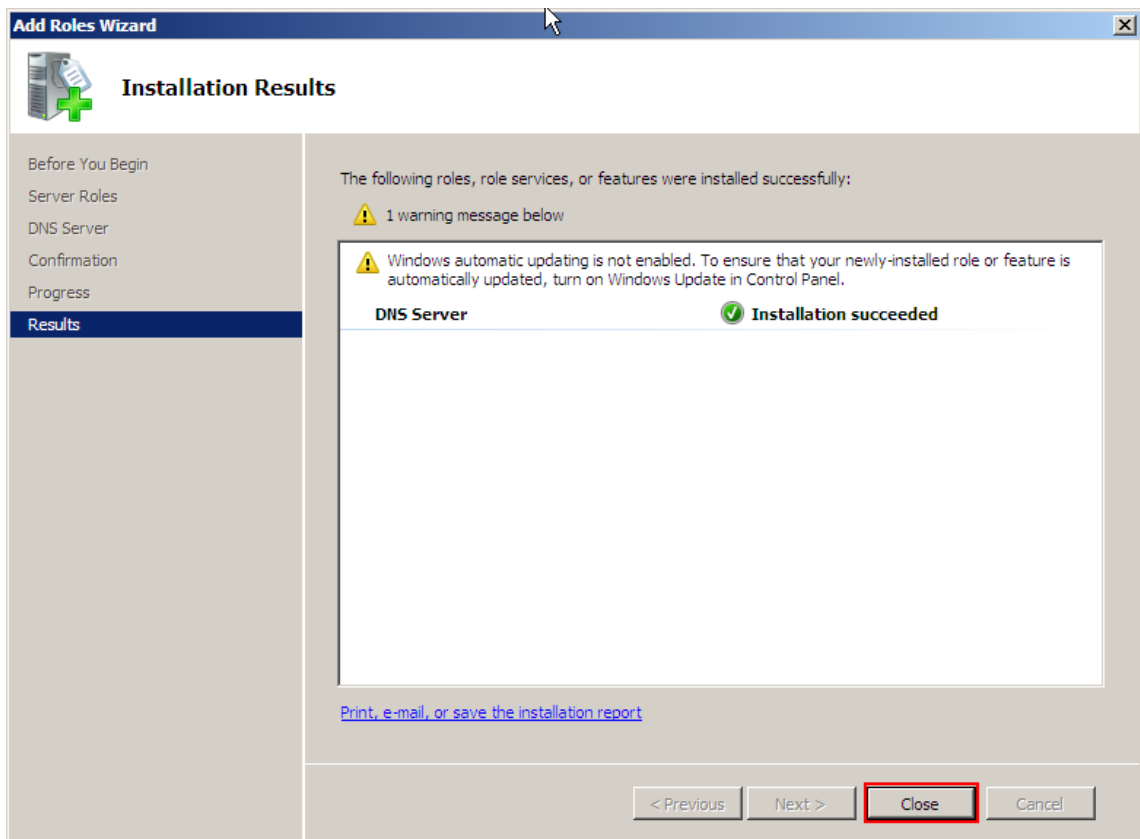


Figura 8: Resultado da instalação

Configurando DNS Server no Windows Server 2008 R2

Antes de configurar o servidor DNS, você deve estar familiarizado com os seguintes conceitos:

- Forward lookup zone
- Reverse lookup zone
- Zone types

Uma zona de pesquisa direta (Forward lookup zone) é simplesmente uma maneira de resolver nomes de host para endereços IP. A zona de pesquisa inversa (Reverse lookup zone) permite que um servidor DNS descubra o host a partir do endereço IP. Basicamente, o oposto de uma zona de pesquisa direta.

Ao selecionar um tipo de zona DNS, você tem as seguintes opções:

Primary Zone, Secondary Zone e Stub Zone.

Zona Primária (Primary Zone) armazena o banco de dados em um arquivo de texto com a extensão “.dns”. Pode ser compartilhado com outros

servidores DNS, que por sua vez também armazenam suas informações em um arquivo de texto.

Zona Secundária (Secondary Zone) simplesmente cria uma cópia do banco de dados existente de outro servidor DNS. Isso é usado principalmente para balanceamento de carga entre servidores.

Stub Zone é uma cópia de uma zona primária que só contém os registros de recursos necessários para identificar os servidores DNS autoritativos para a zona. Uma zona de stub é usada para resolver nomes entre namespaces de DNS separados. Este tipo de resolução pode ser necessária quando uma fusão de empresas exigir que os servidores DNS de dois namespaces separados resolvam nomes para clientes em ambos os namespaces.

Store the Zone In Active Directory armazena as informações de banco de dados do DNS dentro de uma partição do domínio ou diretório de aplicativos do Active Directory. Cada zona integrada ao Active Directory é armazenada dentro de um recipiente chamado *dnsZone* identificado pelo nome que você escolheu para a zona ao criá-la. Quando selecionada esta opção facilita a replicação e segurança na transferência de dados entre servidores DNS.

Nota: A opção Store the Zone In Active Directory, apenas está disponível quando existe uma instalação do Active Directory no mesmo servidor.

Agora que conhecemos os conceitos sobre Zona, vamos à prática, para isso é necessário estar com o DNS Manager aberto, clicando em Start Administrative Tools e por fim DNS Manager (Figura 9).

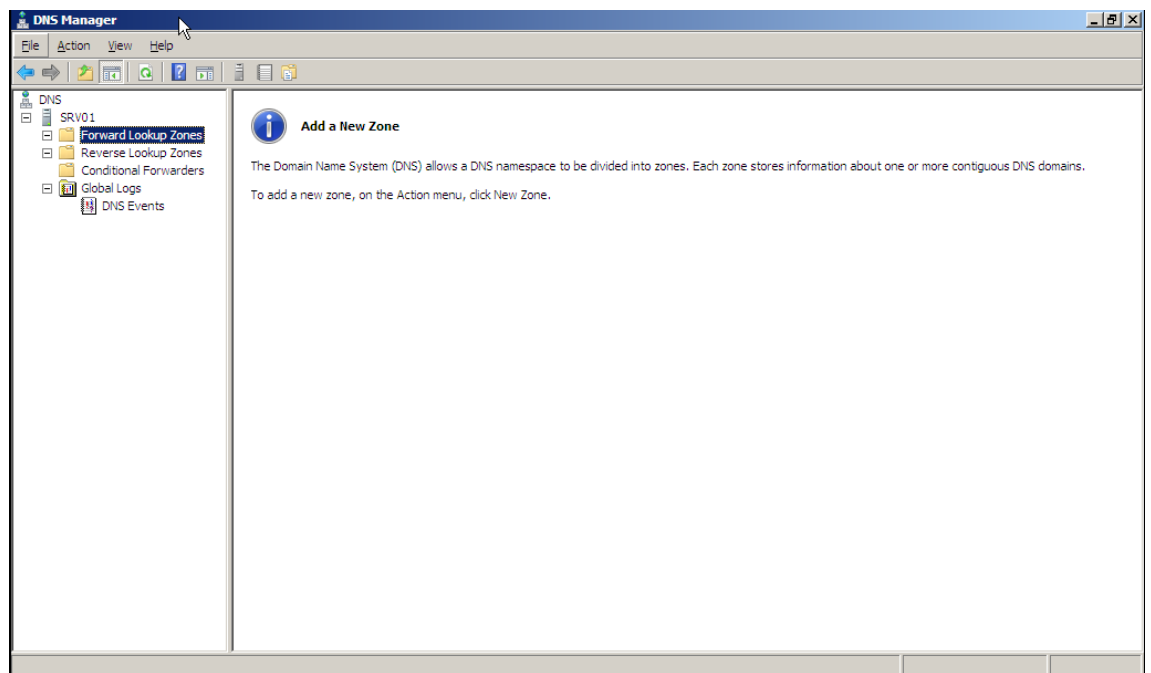


Figura 9: DNS Manager

Clique com o botão direito em Forward Lookup Zones, selecione New Zone, com o Wizard (Figura 10), marque a opção Primary Zone e clique em Next.

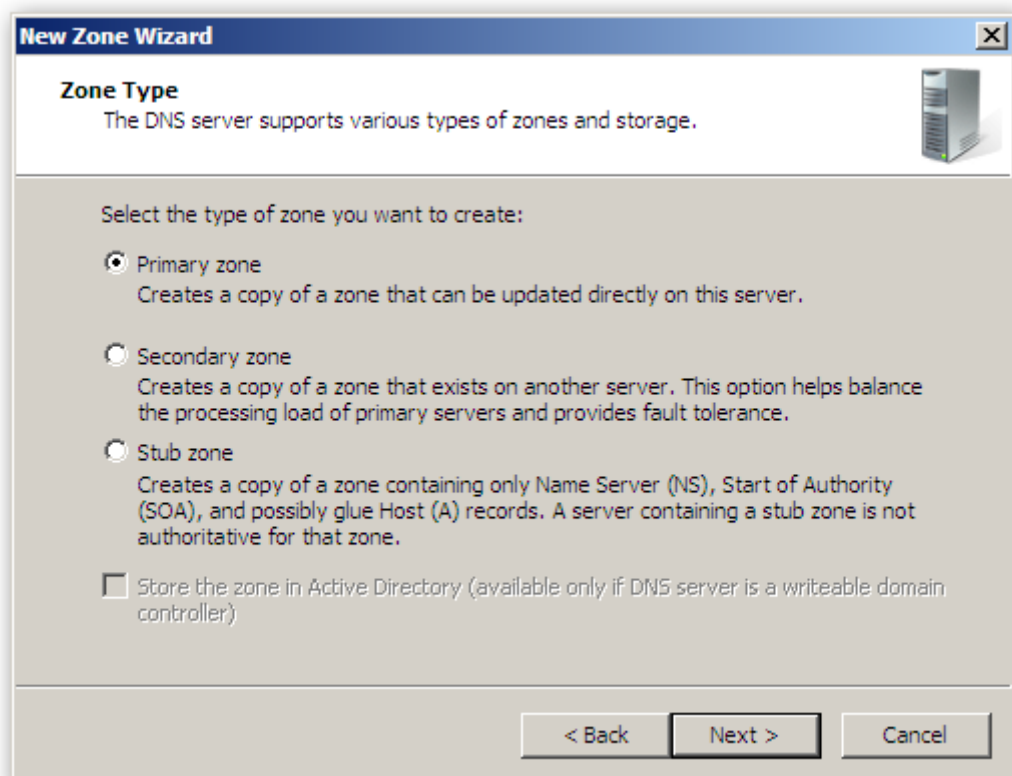


Figura 10: Nova zona

Em Zone Name definimos o nome da zona para o servidor DNS autoritativo. Podemos usar o nome da organização como exemplo: empresa.com.br, dns1.empresa.com.br, dns1.empresa.local e assim por diante.

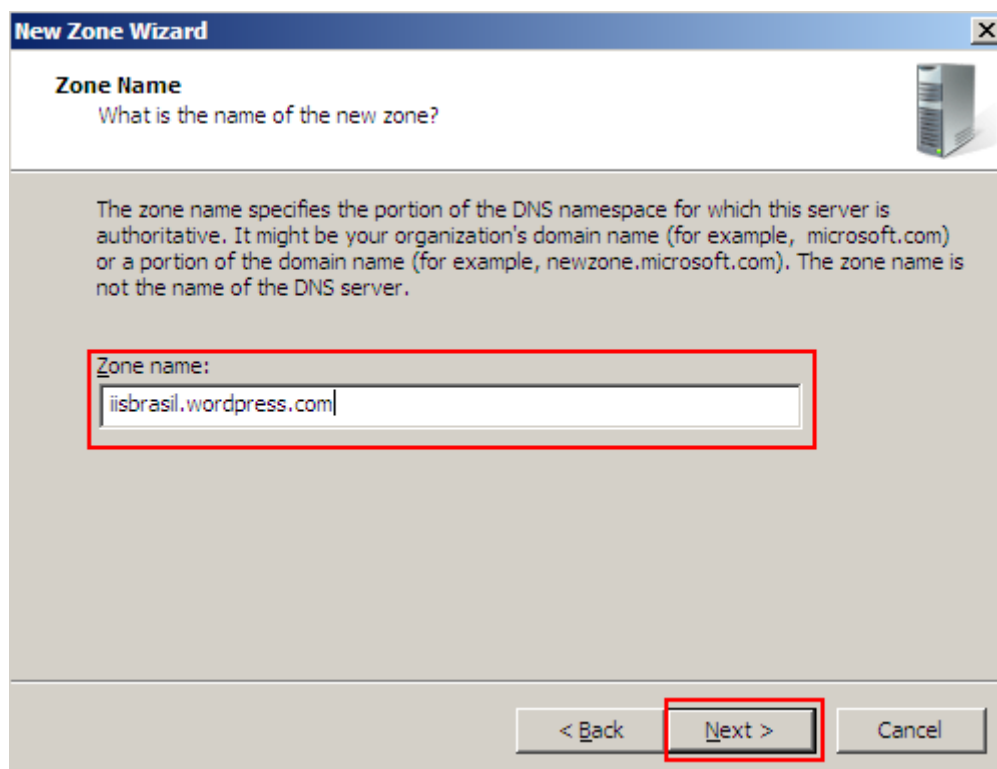


Figura 11: Nome da zona

Em Zone file (Figura 12) colocamos o nome do arquivo de banco de dados, por padrão ele pega o nome zona que definimos no passo anterior, mas pode ser alterado para o nome que desejar. Outra opção seria utilizar um arquivo já existente, como é uma instalação nova de DNS, nós não temos este arquivo, portanto devemos criar um novo selecionando Create a new file with this file name, em seguida clique em Next.

Nota: O arquivo de banco de dados do dns está localizado dentro da pasta %SystemRoot%\System32\dns

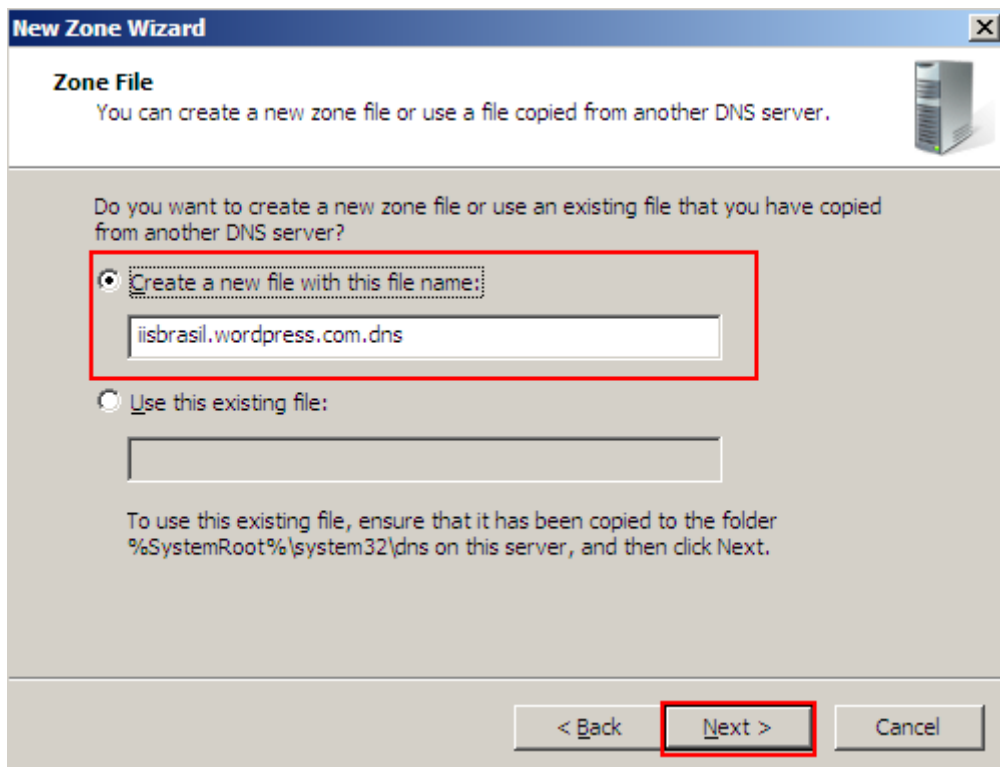


Figura 12: Arquivo de zona

Na janela Dynamic Update é habilitado para que os computadores clientes se registrem e atualizem dinamicamente os registros no DNS Server, isso minimiza a administração manual de registros no DNS Server, existem alguns tipos de atualizações dinâmicas, veja:

- **Allow only secure dynamic updates:** Atualização dinâmica segura é suportada apenas para Zonas integradas ao Active Directory.
- **Allow both nonsecure and secure dynamic updates:** Muito cuidado ao selecionar esta opção, pois não é seguro, atualizações podem ser aceitas, mesmo a partir de fontes que não são confiáveis, ou seja, não estão em nosso domínio.
- **Do not allow dynamic updates:** Não aceita atualizações dinâmicas, necessário que seja feito manualmente.

Prosseguindo com a configuração marque Do not allow dynamics updates, em seguida Next.

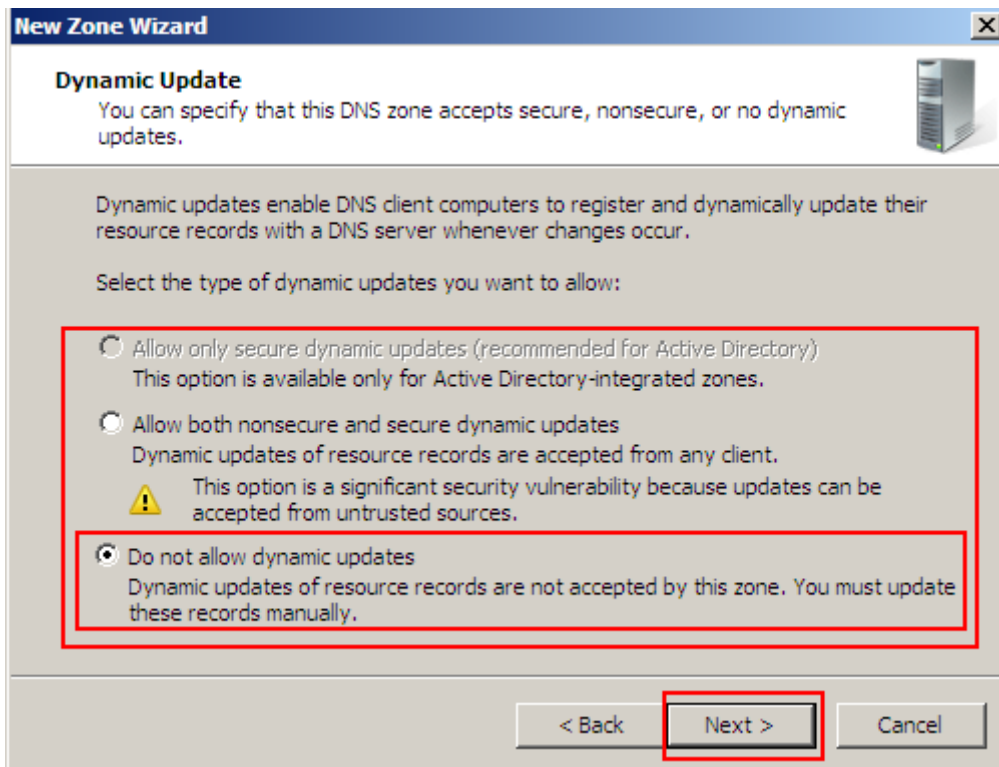


Figura 13: Atualizações dinâmicas

Na próxima janela, é mostrado que completamos a configuração da nova zona e algumas informações como, nome, tipo, tipo de pesquisa e o nome do arquivo de banco de dados. Clique em finish, para finalizar a janela de Wizard e voltar para a janela do DNS Manager.

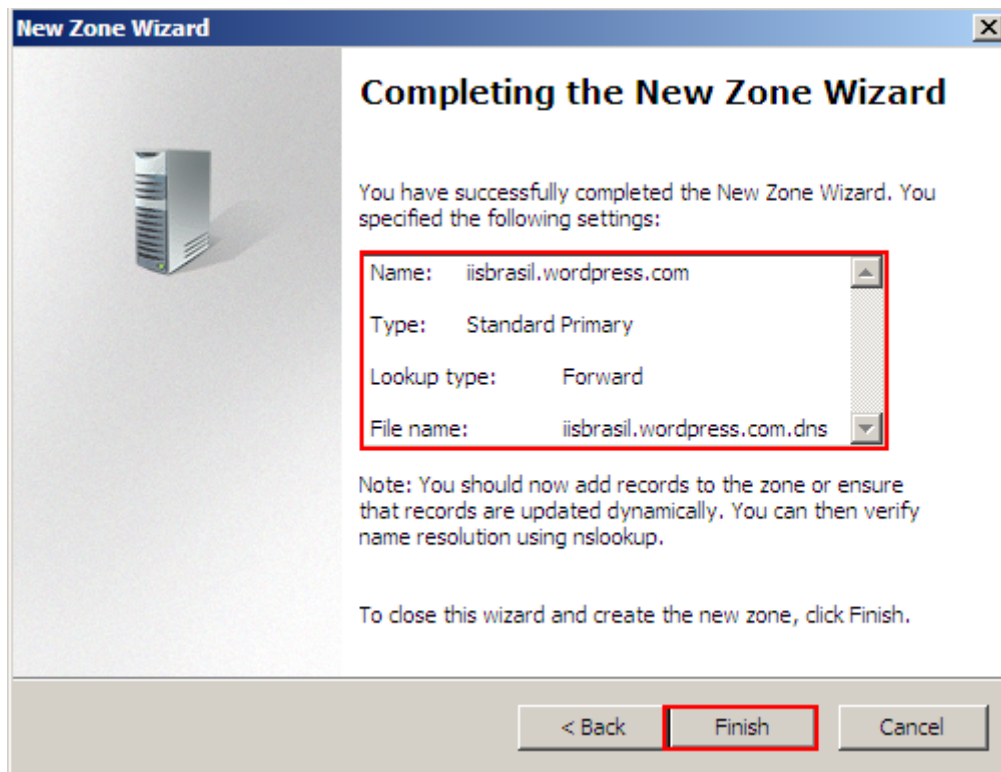


Figura 14: Finalizando a instalação

Notem que na janela do DNS Manager foi criada a Zona Direta e alguns registros do tipo SOA e NS.

SOA: Start of Authority (SOA) Primeiro registro de uma zona primaria, indica que este servidor de DNS é a melhor fonte de informações para os dados nesse domínio DNS.

NS: Especificam quais são os servidores DNS para o domínio.

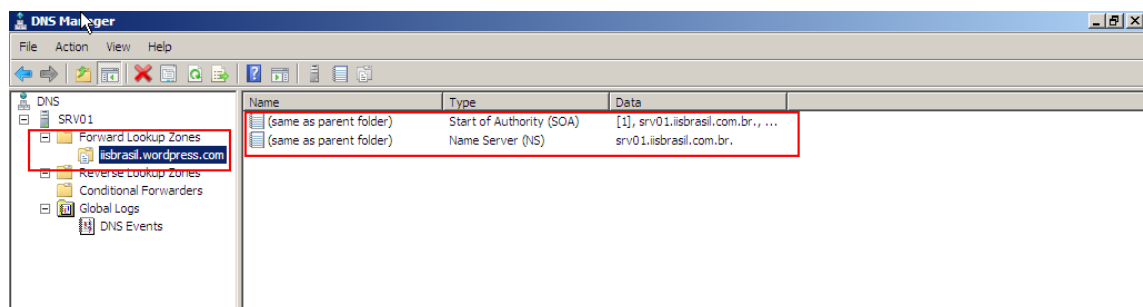


Figura 15: Registros NS e SOA

É necessário criar registros A (também conhecidos como registros host) são os registros centrais de DNS. Esses registros vinculam um domínio, ou subdomínio, a um endereço IP.

Na zona direta iisbrasil.wordpress.com, clique com o botão direito e selecione New host (A or AAAA).

Em Name coloque o nome correspondente ao servidor.

Em IP Address digite o endereço correspondente ao servidor.

Desmarque a checkbox “Create associated pointer (PTR) record”, esta opção é utilizada para criar automaticamente o registro PTR quando existe a zona reversa.

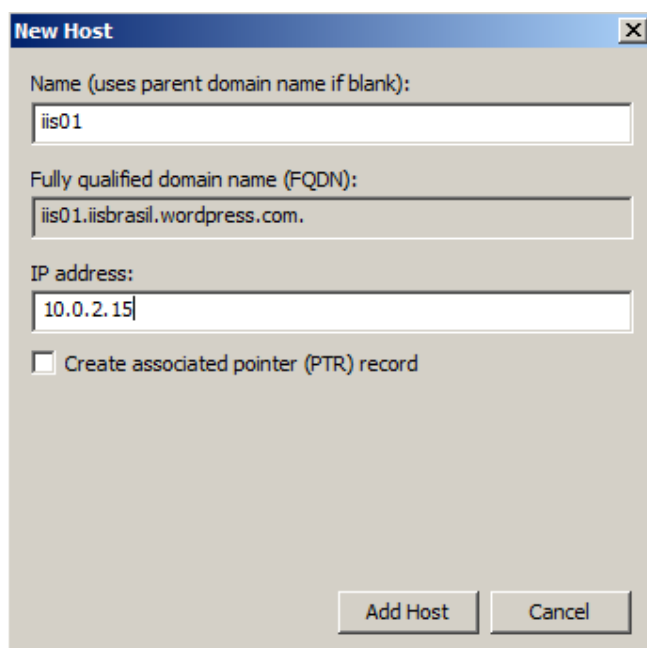


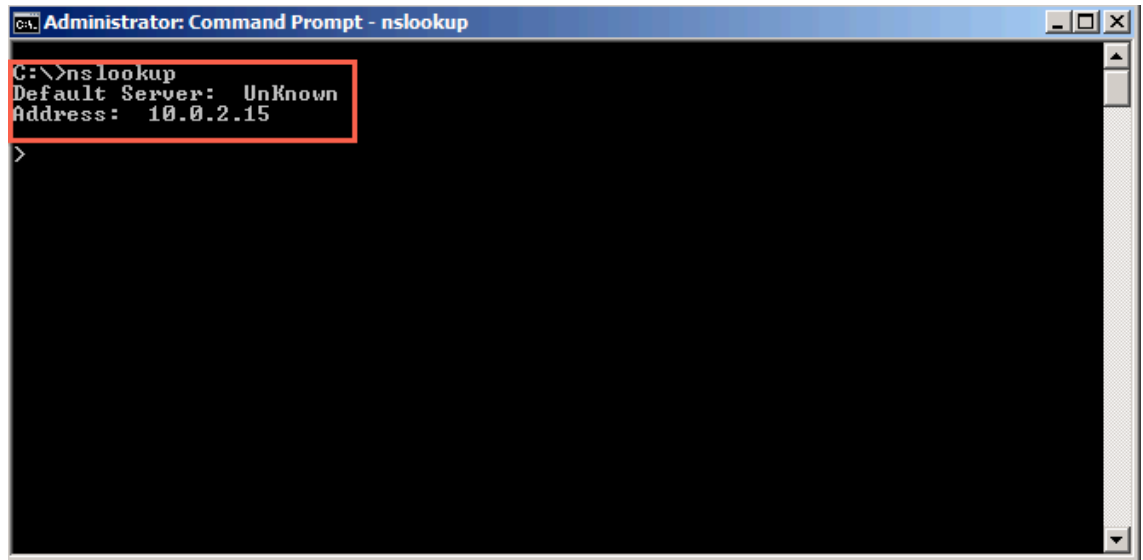
Figura 16: Configurando registro A

OBS: Registro A é utilizado no protocolo IPv4 e o AAAA é utilizado no IPv6.

Para validarmos a instalação utilizaremos o comando *nslookup*, que é muito utilizado para resolução de problemas no DNS, para isto é necessário acessar o prompt de comandos, seguindo os passos:

Clique em Start > All Programs > Accessories > Selecione Command Prompt

Com a janela do prompt de comandos aberta, digite nslookup e tecle enter.

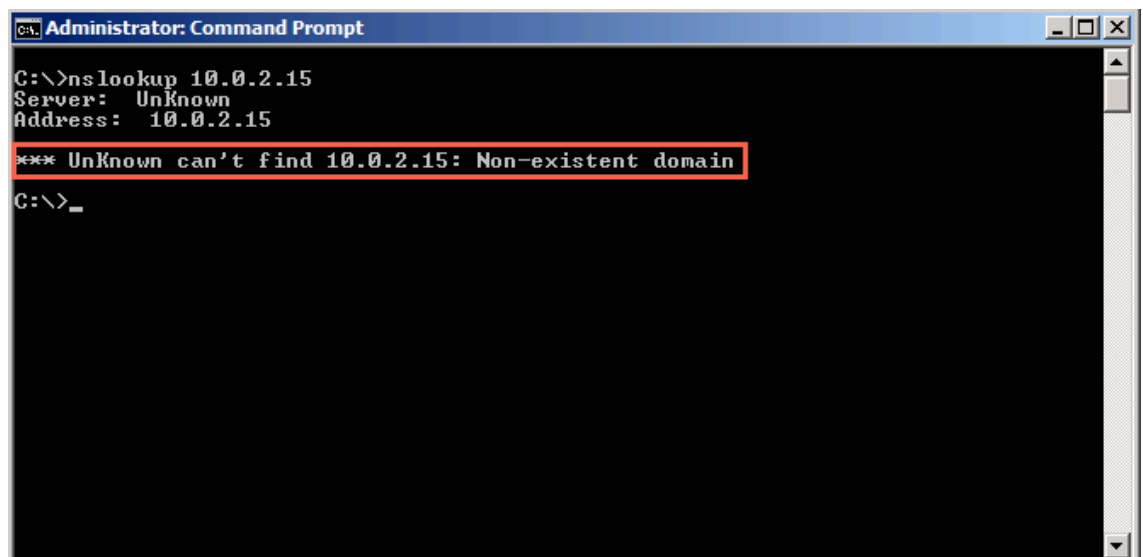
A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt - nslookup". The command prompt shows the command "C:\>nslookup" entered. The output is "Default Server: UnKnown" and "Address: 10.0.2.15". The output text is highlighted with a red rectangular box.

```
C:\>nslookup
Default Server:  UnKnown
Address:  10.0.2.15
>
```

Figura 17: Validando instalação

Notem, que em *Default Server* está definido como *Unknown*, pois não está criada a zona reversa (Reverse Lookup Zones).

A zona reversa é utilizada para resolução de IP para nome, ou seja, tenho o IP 10.0.2.15, mas gostaria de saber qual é o nome, neste caso pode ser feita a pergunta para o DNS da seguinte forma, com o prompt de comandos aberto, digite: nslookup 10.0.2.15 e tecle enter.

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The command prompt shows the command "C:\>nslookup 10.0.2.15" entered. The output is "Server: UnKnown" and "Address: 10.0.2.15". Below this, a red rectangular box highlights the error message: "*** UnKnown can't find 10.0.2.15: Non-existent domain". The prompt ends with "C:\>_".

```
C:\>nslookup 10.0.2.15
Server:  UnKnown
Address: 10.0.2.15
*** UnKnown can't find 10.0.2.15: Non-existent domain
C:\>_
```

Figura 18: Validando resolução de endereço IP para host

O DNS não pode encontrar o nome correspondente ao IP 10.0.2.15, por dois motivos.

1. Não existe a zona reversa
2. Não existe o registro PTR

Registro PTR é conhecido também como *Pointer*, sua função é mapear o IP para o nome.

Para fazer a configuração da zona reversa selecione *Reverse Lookup Zones*, clique com o botão direito e Selecione *New Zone*.

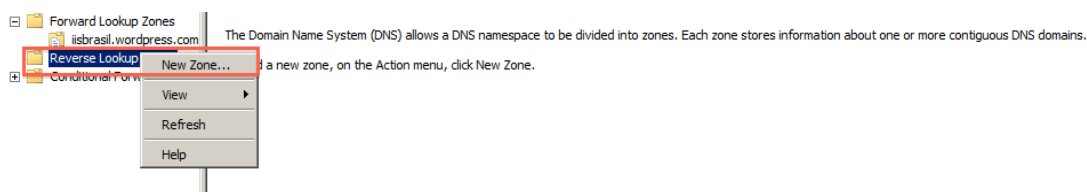


Figura 19: Configurando Zona reversa

Na janela do Wizard clique em next para iniciar a configuração da zona



Figura 20: Bem vindo ao Wizard

Na próxima janela vamos definir o tipo de zona, o conceito é o mesmo abortado no começo da configuração do DNS Server, selecione Primary Zone e clique em next.

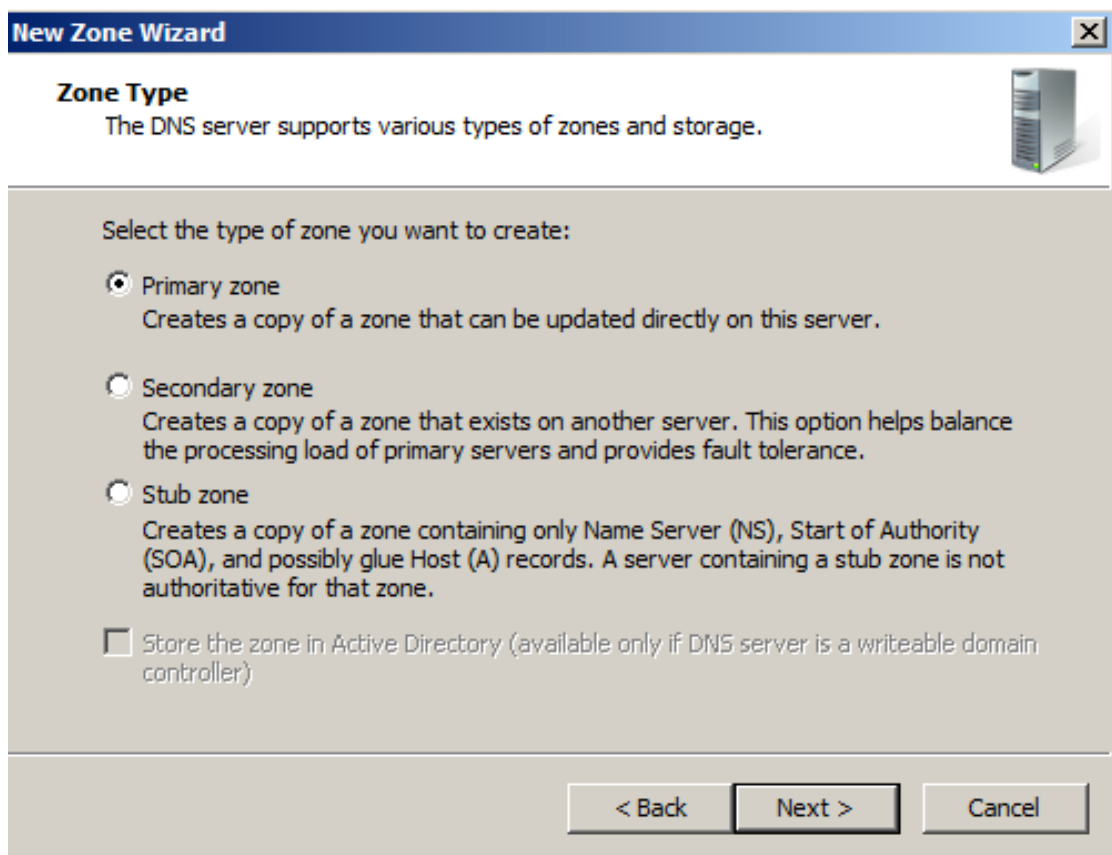


Figura 21: Selecionando zona primária

Na próxima janela selecione *IPv4 Reverse Lookup Zone* e clique em *next*.

O protocolo IPv4 foi definido no momento que configuramos o endereço IP na placa de rede.

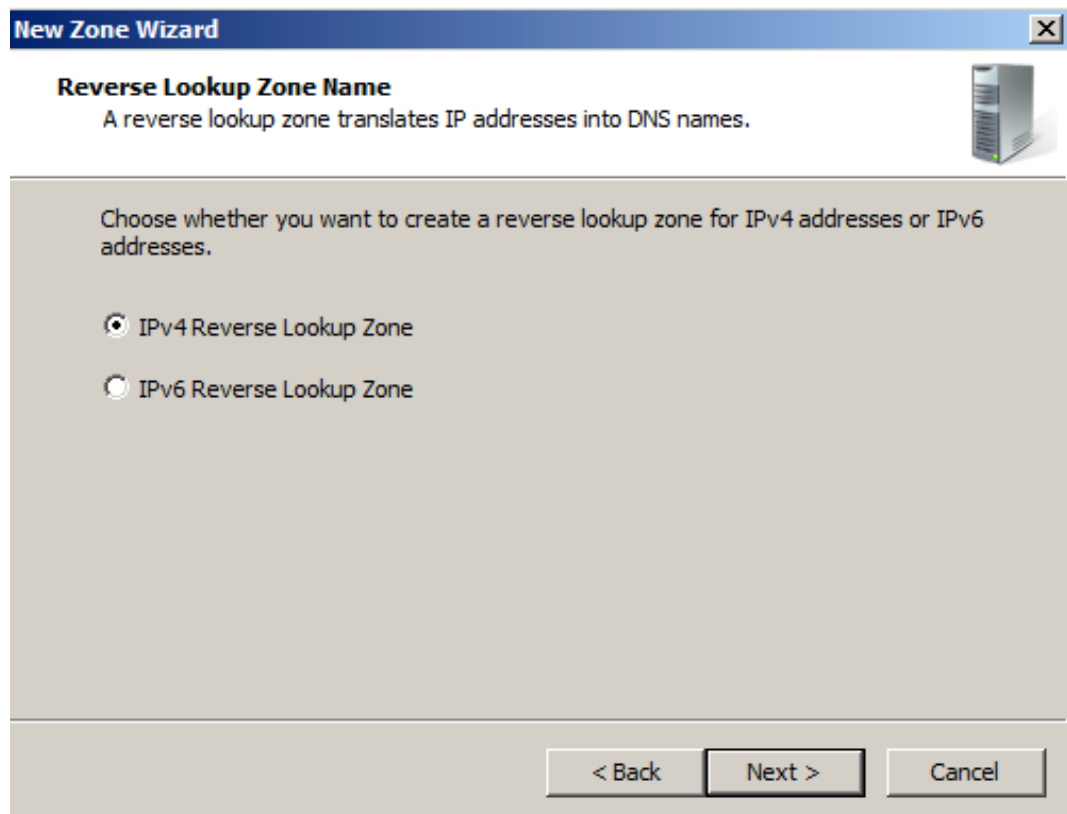


Figura 22: Selecionando protocolo IPv4

Na próxima janela definiremos a identidade de rede, também conhecido como Network ID, para conhecer mais detalhes consulte a referência. Digite 10.0.2 e cliquem em next.

The screenshot shows a Windows-style dialog box titled "New Zone Wizard" with a close button (X) in the top right corner. The main heading is "Reverse Lookup Zone Name" in bold. Below it, a subtitle reads: "A reverse lookup zone translates IP addresses into DNS names." To the right of this text is a small icon of a server tower. The main content area has a light gray background and contains the following text: "To identify the reverse lookup zone, type the network ID or the name of the zone." Below this, there are two radio button options. The first option, "Network ID:", is selected (indicated by a filled circle). It is followed by a text input field containing three dots "...". Below the input field, there is explanatory text: "The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order." and "If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa." The second option, "Reverse lookup zone name:", is not selected (indicated by an empty circle) and is followed by an empty text input field. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Figura 23: Configurando Network IP

Na próxima janela definiremos o nome do arquivo de banco de dados, você pode utilizar um arquivo já existente, ou criar um novo, como abortado anteriormente na criação de zona direta, clique em next para continuar com a configuração.

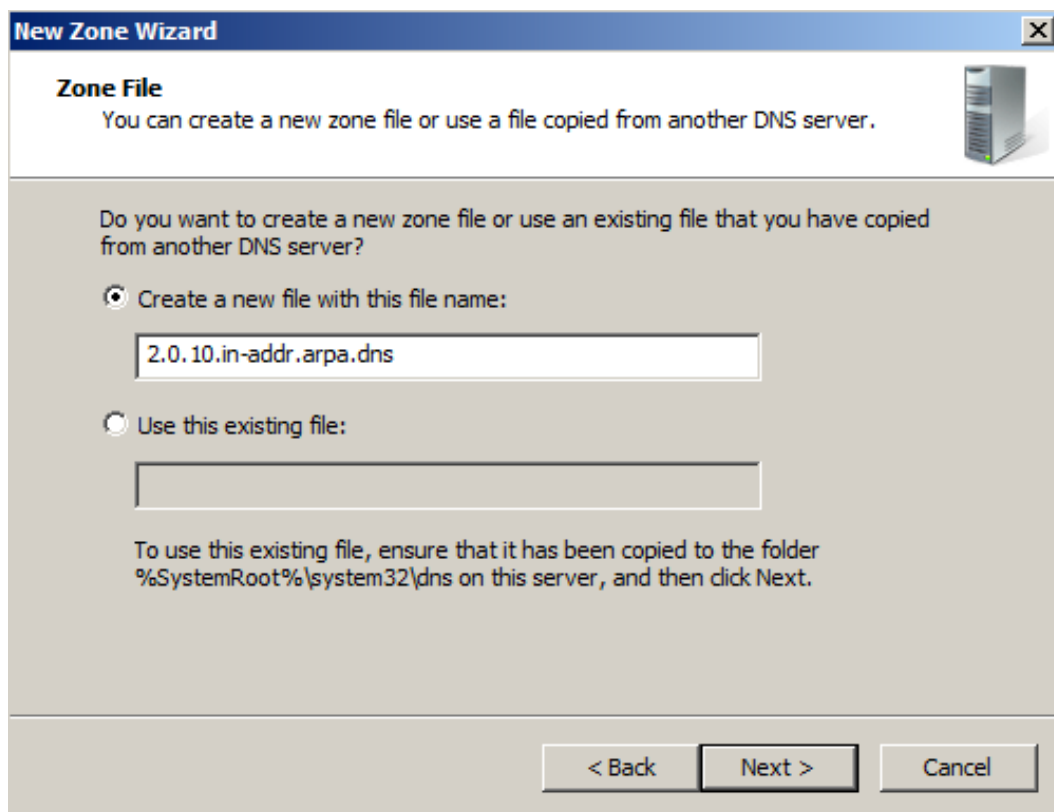


Figura 24: Configurando novo arquivo de banco de dados

Na próxima janela selecione *Do not allow dynamics updates*, apenas lembrando o que vimos anteriormente, está opção necessita que o registro PTR seja criado manualmente.

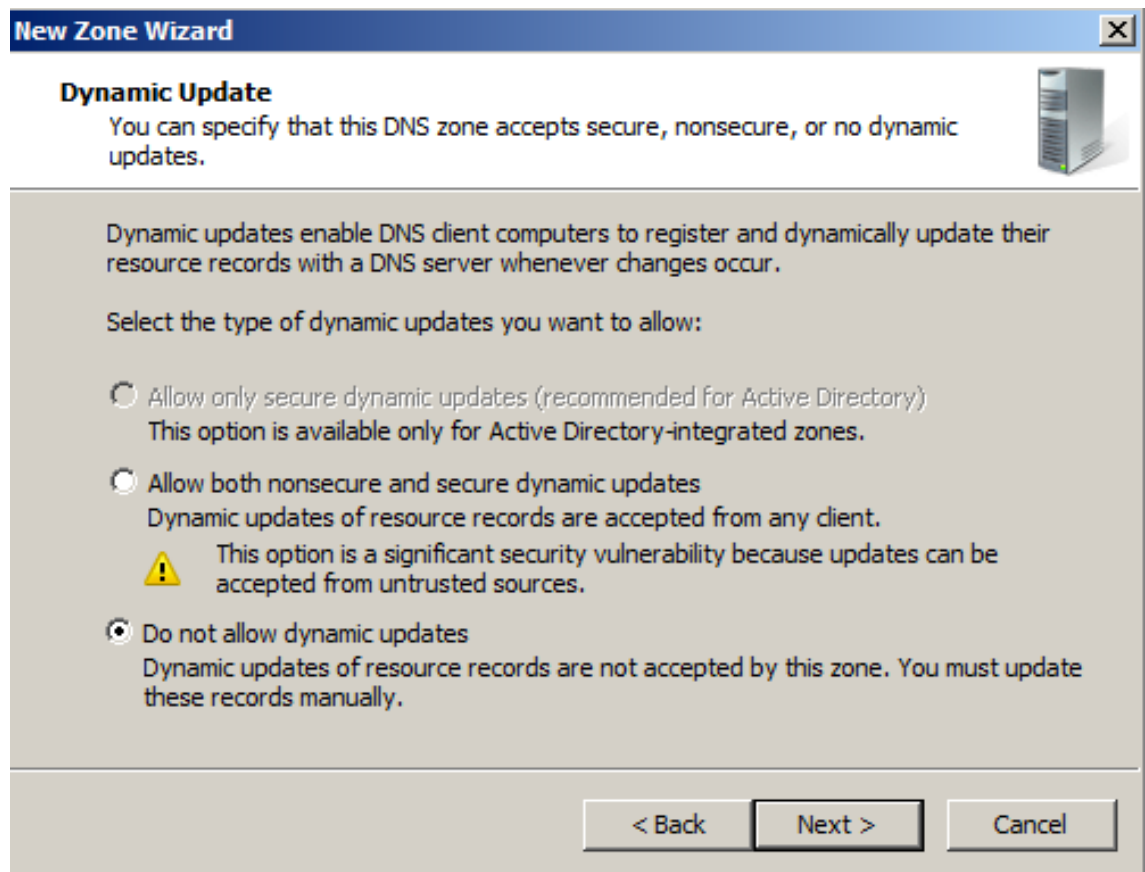


Figura 25: Configurando atualizações dinâmicas

Na próxima janela temos um resumo do que foi configurado anteriormente, configura se está de acordo e, clique em Finish.

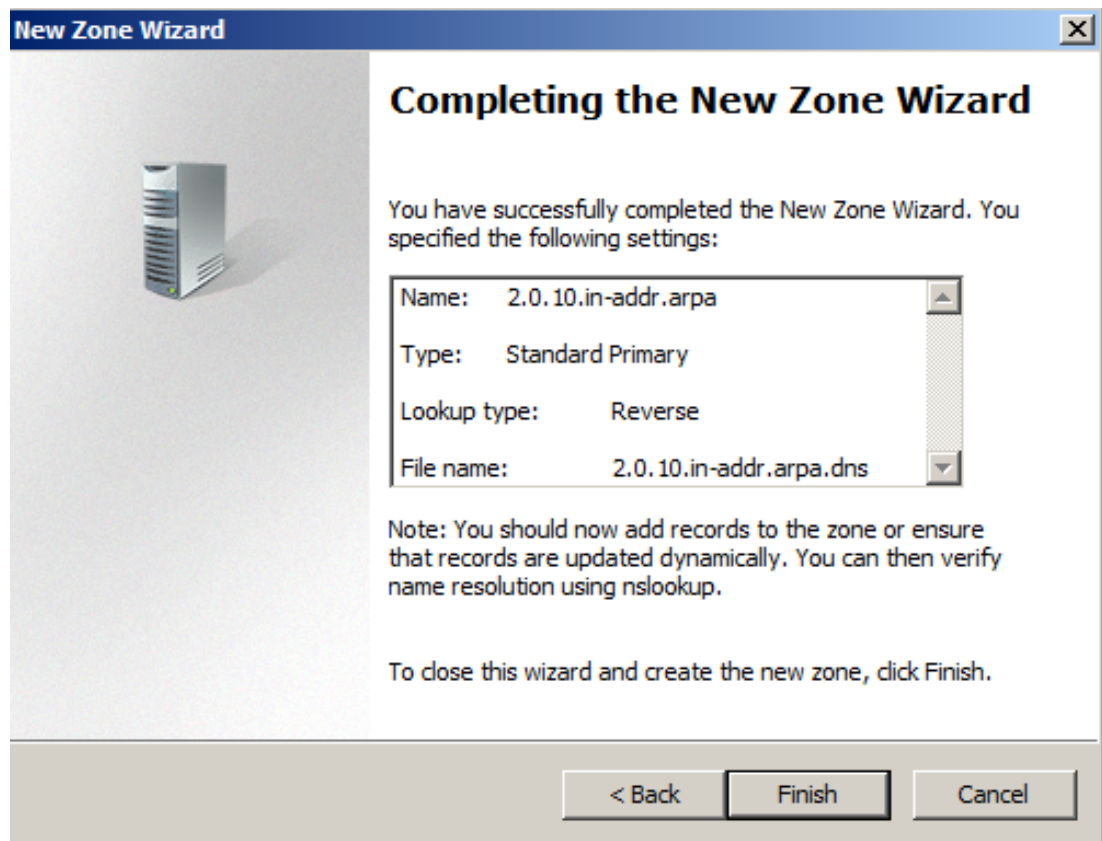


Figura 26: Finalizando a configuração

Temos a zona reversa criada, mas ainda falta configurar o Registro PTR, selecione a zona correspondente, clique com o botão e em seguida “New Pointer PRT”

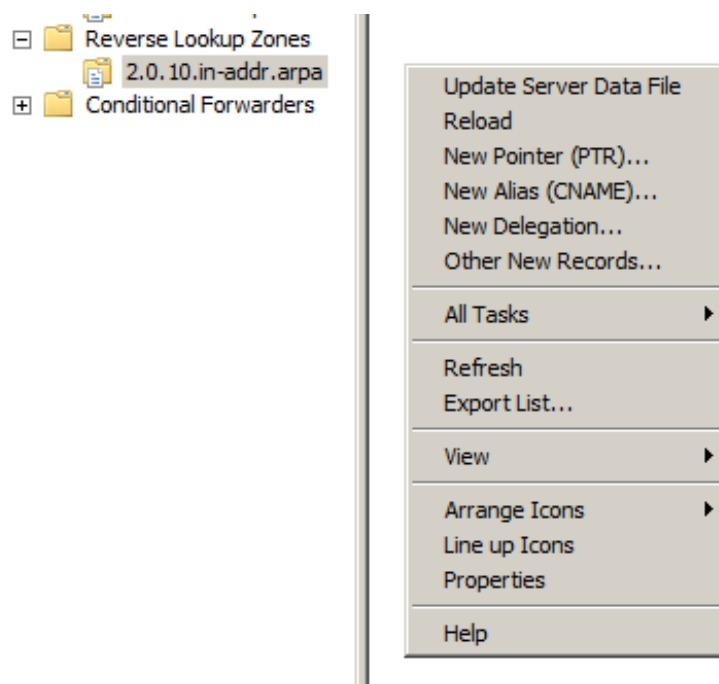


Figura 27: Zona reversa

Com a janela aberta insira os dados.

Host IP Address: Endereço IP do Servidor

Host name: Selecione browser e o registro A correspondente.

New Resource Record

Pointer (PTR)

Host IP Address:
10.0.2.15

Fully qualified domain name (FQDN):
15.2.0.10.in-addr.arpa

Host name:
iis01.iisbrasil.wordpress.com Browse...

OK Cancel

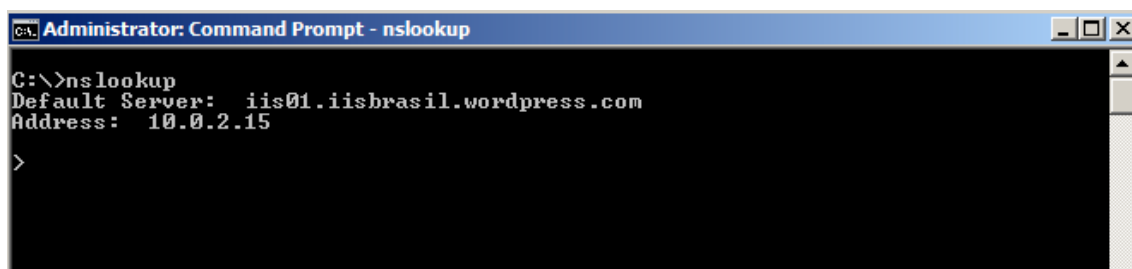
Figura 28: Criando registro PTR

Global Logs	(same as parent folder)	Name Server (NS)	iis01.iisbrasil.local.
Forward Lookup Zones	10.0.2.15	Pointer (PTR)	iis01.iisbrasil.wordpress.com.
iisbrasil.wordpress.com			
Reverse Lookup Zones			
2.0.10.in-addr.arpa			
Conditional Forwarders			

Figura 29: Registro PTR criado.

Agora que temos tudo configurado, vamos testar novamente o comando nslookup e se certificar que não existe nenhum problema de resolução de nomes tanto na zona direta como na zona reversa.

Com o prompt de comandos aberto digite: nslookup



```
Administrator: Command Prompt - nslookup
C:\>nslookup
Default Server: iis01.iisbrasil.wordpress.com
Address: 10.0.2.15
>
```

Figura 29: Validando configuração

Notem que agora temos o resultado correto do Default Server, se caso apareça qualquer coisa diferente de nome_do_servidor.nome_da_zona verifique os passos anteriores para a criação do Registro A, Zona reversa e Registro PTR.

Conclusão

Neste artigo conhecemos o serviço de DNS e vimos a importância deste pilar na internet, sem o qual, por sites seria algo completamente desagradável, pois teríamos que gravar inúmeros endereços IP para poder acessar um site em qualquer lugar da rede mundial de computadores, aprendemos a instalar e configurar o DNS de forma correta e possíveis problemas que podem acontecer durante este percurso.

Referências:

<ftp://ftp.registro.br/rfc/rfc882.txt>

<ftp://ftp.registro.br/rfc/rfc883.txt>

<ftp://ftp.registro.br/rfc/rfc1034.txt>

<ftp://ftp.registro.br/rfc/rfc1035.txt>

http://en.wikipedia.org/wiki/Domain_Name_System

http://pt.wikipedia.org/wiki/Domain_Name_System

[http://technet.microsoft.com/en-us/library/cc728412\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc728412(W.S.10).aspx)

http://pt.wikipedia.org/wiki/Máscara_de_rede