Grupo

iPED

Material de apoio

Sumário

Institucional

O iPED, Instituto Politécnico de Ensino a Distância, é um centro de educação on-line que oferece informação, conhecimento e treinamento para profissionais, educadores e qualquer um que queira evoluir profissionalmente e culturalmente.

Nosso objetivo é torná-lo uma base forte de conhecimento e expandir cada vez mais o seu nível intelectual e cultural.

Oferecemos uma quantidade enorme de informação, além de diversos cursos on-line, onde você se mantém atualizado em qualquer lugar e a qualquer hora.

Educação à Distância

Aulas online ou a prática de aprendizagem à distância, através de ambientes virtuais e redes de computadores interligadas para fins educacionais e culturais, nada mais é do que o meio mais prático e inteligente de proliferação de conhecimento.

Através de ambientes virtuais e sistemas inteligentes, é possível adquirir conhecimento de forma total ou gradativa.

Esse é nosso conceito de educação, em tempo real, total ou gradativo, quando quiser e onde quiser e acima de tudo, da forma que quiser!

Nossa Missão

O Grupo iPED foi lançado com o intuito de aprimorar e disseminar o conceito de ensino a distância.

Com a implantação do ensino a distância, pesquisas recentes registram que as pessoas alavancam os resultados dos módulos de treinamento em até 70%, eliminando as distâncias geográficas e proporcionando a melhoria da gestão do conhecimento e dos recursos humanos por competências.

Pensando nisso o iPED presta esse serviço a todos, para que a exclusão digital seja cada vez menor e com o passar do tempo ela desapareça completamente.

Esse é nosso objetivo, essa é nossa missão, e esteja certo que vamos conseguir!

Fabio Neves de Sousa
Diretor Geral - Grupo iPED

Introdução

Bem-vindo ao curso de gerenciamento e configuração do windows server 2012, última versão do sistema operacional servidor de rede da Microsoft. Apesar de ter sido lançado em 2012, as empresas demoram cerca de 2 a 3 anos para implantar em suas infraestruturas, pois seria uma "irresponsabilidade" utilizar qualquer sistema operacional recém-lançado, o que colocaria em risco toda informação da empresa.

Desta maneira, voce é a pessoa certa, no local certo, no momento certo, pois é neste período que as empresas iniciam suas migrações de versões anteriores, tais como o Windows server 2003 e 2008 para esta última versão, tornando você, que vai adquirir o conhecimento necessário, um profissional indispensável.

Boa sorte!

Unidade 1 - Conhecendo o Windows Server 2012

Olá!

Nesta unidade você irá conhecer a finalidade do Windows Server 2012 , suas versões e também como fazer sua instalação adequadamente.

Você entenderá a importância da conectividade e disponibilidade de um servidor de rede. E, ainda, os modos de funcionamento do NIC teaming. Além disso, estudará a interface de gerenciamento de um servidor de rede nessa versão 2012.

E por fim, você aprenderá a função, as unidades organizacionais, a finalidade dos grupos de usuários e o GPOs do Active Directory.

Bom estudo!

1.1 Edições e Finalidade do Windows Server 2012

O windows server 2012 vem em 4 tipos diferentes, cuja finalidade é se adequar às diferentes necessidades dos diversos tipos de clientes. Pois alguns precisam de um sistema operacional mais completo, com mais ferramentas e serviços que atendam a mais usuáriso em sua rede, enquanto outros não precisam de tantas ferramentas, nem precisam de um sistema para tantos funcionários, a exemplo de uma pequena empresa, bem como outras diferenças.

Motivada por estas razões, a microsoft disponibiliza as seguintes edições de windows server 2012:

1. Windows server 2012 datacenter:
    a. Feita para servidores poderosos;
    b. Suporte até 64 processadores;
    c. Suporta a troca a quente de processadores;
    d. Todas ferramentas (Funções) nativas disponíveis para instalação.
2. Windows server 2012 standard:
    a. A única diferença entre esta versão e a datacenter, é a quantidade de máquinas virtuais que podem ser rodadas, pois na versão datacenter a quantidade é ilimitada, nesta é de 2 instâncias apenas.
3. Windows server 2012 essentials:
    a. No tocante às funções, é semelhante às versão anteriores, com exceção das funcionalidades server core, hyper-V e serviços de federação do active directory;
    b. Limitada ao número máximo de 25 usuários.
4. Windows server 2012 foundation:
    a. Para pequenas empresas, que precisem de poucos serviços de rede, tais como serviços básicos de autenticação, servidor de impressão e arquivos;
    b. Limitada ao número máximo de 15 usuários;
    c. Não suporta virtualização.

Apesar do que foi dito, acredite que a decisão sobre qual edição adquirir, irá se basear mais na questão da virtualização, não sendo tão importante a quantidade de usuários ou funções disponíveis.

Uso e virtualização do windows server 2012

No tocante a licenciamento e virtualização, existem dois pontos a serem observados, que são:

1. POSE (Phisical Operational System Enviroment): É quando o windows Server 2012 será instalado em uma máquina física real.
2. VOSE (Virtual Operational System Enviroment): É quando o windows Server 2012 será instalado em uma máquina virtual.

Com base nestes 2 termos, verifique o quadro abaixo:

	Quantidade de instalações físicas (POSE)	Quantidade de instalações virtuais (VOSE)
Datacenter	1	Ilimitada
Standard	1	2
Essencials	1 (pose ou vose)	1 (pose ou vose)
Foundation	1	0

Requisitos de hardware

No tocante aos requisitos de hardware, estes devem ter:

Processador: 1.4Ghz
Ram: 512mb
HD: 38 GB livres
Arquitetura: 64 bits

Windows server 2012 core edition

A versão server core do Windows server 2012 é uma opção interessante para aqueles que desejam economizar alguns recursos de hardware e diminuir a superfície de ataque resultante de falhas de segurança e facilidade de operação, patrocinada pela interface gráfica.

Na versão server core não há menu iniciar, barras de tarefas ou qualquer tipo de interface gráfica que possa ajudar na operação do sistema, sendo necessária que todo gerenciamento da máquina ocorra via linha de comando.

Ainda vale lembrar que na versão 2008 deste sistema a instalação da versão server core era irremediável, ou seja, caso após a instalação e configuração de todo ambiente, caso o administrador resolvesse mudar para versão gráfica, toda configuração seria perdida, o que não acontece na versão 2012. Desta forma, utilizando a versão 2012, e possível reverter entre a edição gráfica ou server core sem perda de configuração.

No mais a versão core não dispõe das seguintes ferramentas:

Active directory federativo	Serviço de ativação de volumes	Host de sessão de desktop remoto
Servidor de aplicação	Serviços de entrega windows	Acesso web a desktop remoto
Servidor de fax	Servicos de desktop remoto	
Diretivas de rede e serviços de acesso	Gateway de desktop remoto	

Por fim, não iremos abordar em detalhes a versão server core, continuando o curso apenas abordando a versão gráfica.

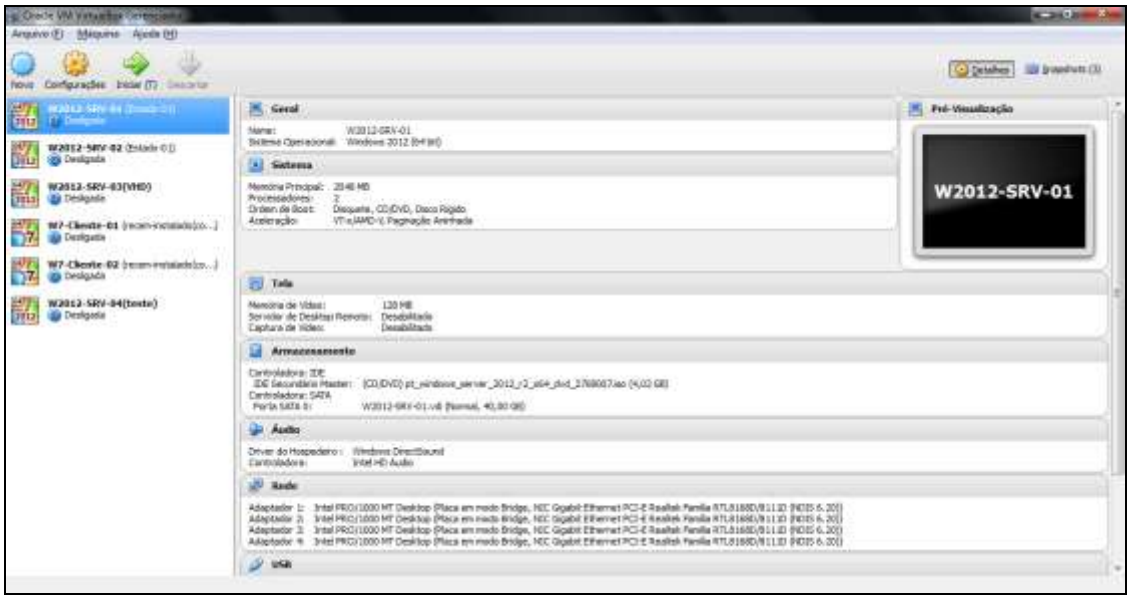
Funções de servidor sobre demanda

Como já não é novidade, no Windows server 2012 a instalação das funções que o Windows server irá desempenhar pode ser escolhida a qualquer momento do funcionamento do sistema operacional, resguardada a ciência de que, em alguns casos, é necessário reiniciar o sistema operacional para que as modificações entrem plenamente em vigor, o que não é muito aconselhável em momentos de pleno horário de funcionamento, o que pode vir a causar transtornos aos usuários.

No entanto, é importante saber que durante a instalação do Windows 2012 server, um diretório é criado no disco rígido da máquina, onde ficam depositados todos os arquivos necessários para futuras modificações no sistema, sem a necessidade de ter em mãos a mídia de instalação do

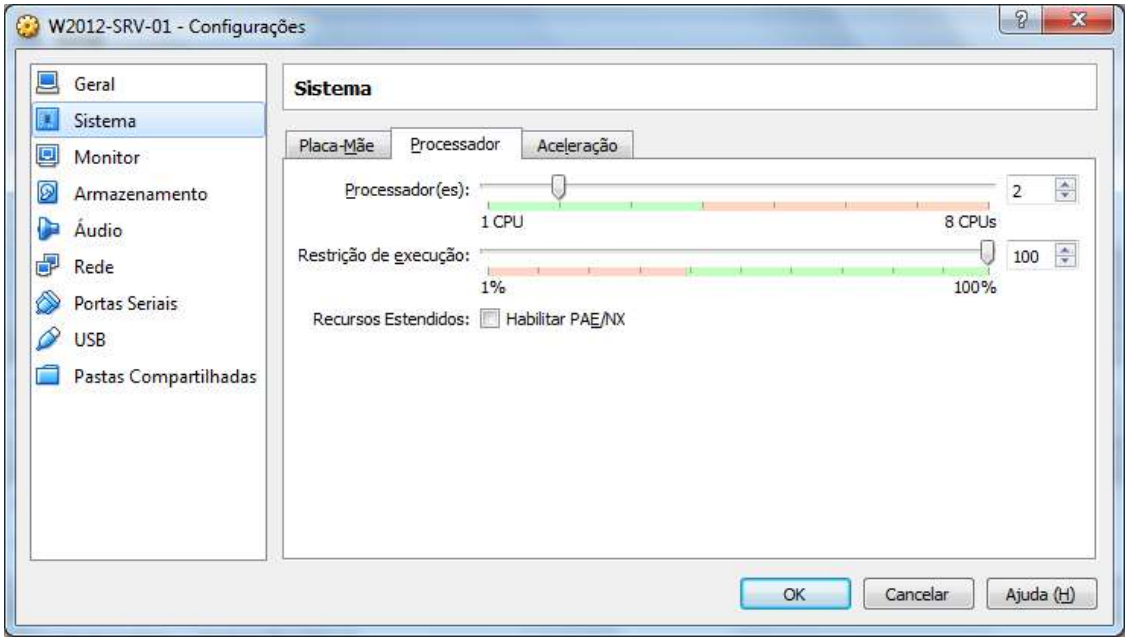
sistema. Este diretório é conhecido como winSxS e, se desejar, pode ser removido do disco sem causar problemas futuros, economizando espaço de armazenamento. Caso os arquivos deletados sejam necessários no futuro, o sistema automaticamente irá fazer download dos arquivos da internet ou recuperá-los da mídia de instalação facilmente.

1.2 Virtualbox

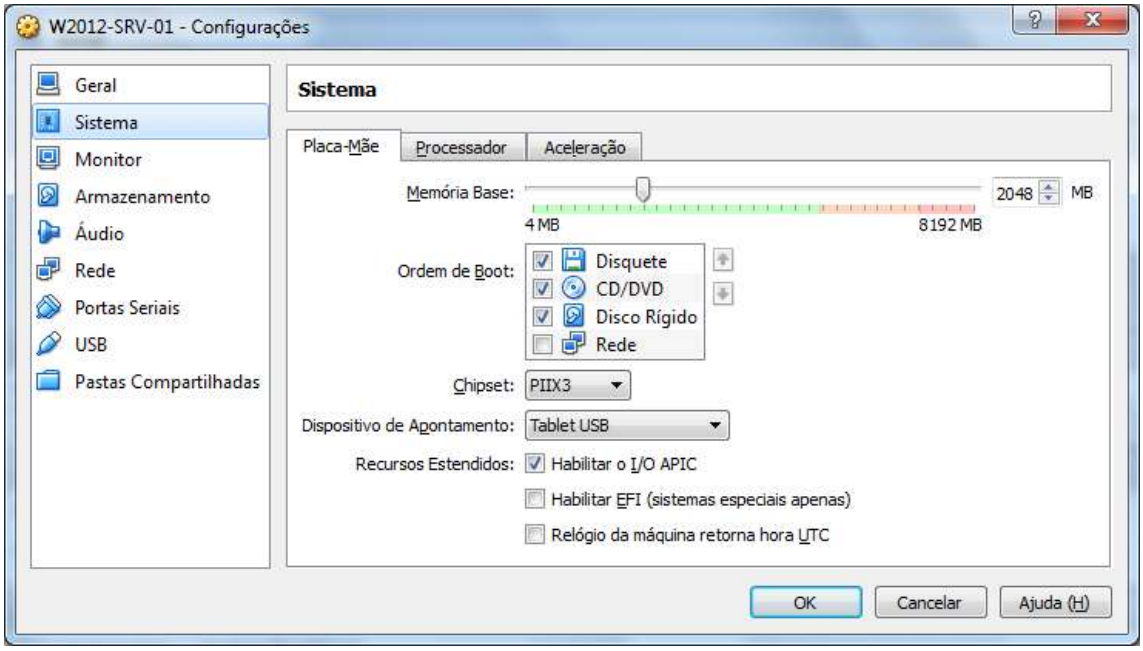


Acima nosso ambiente de trabalho no virtualbox, onde é possível ver as máquinas virtuais à esquerda e os resumos dos dados de configuração de uma delas à direita.

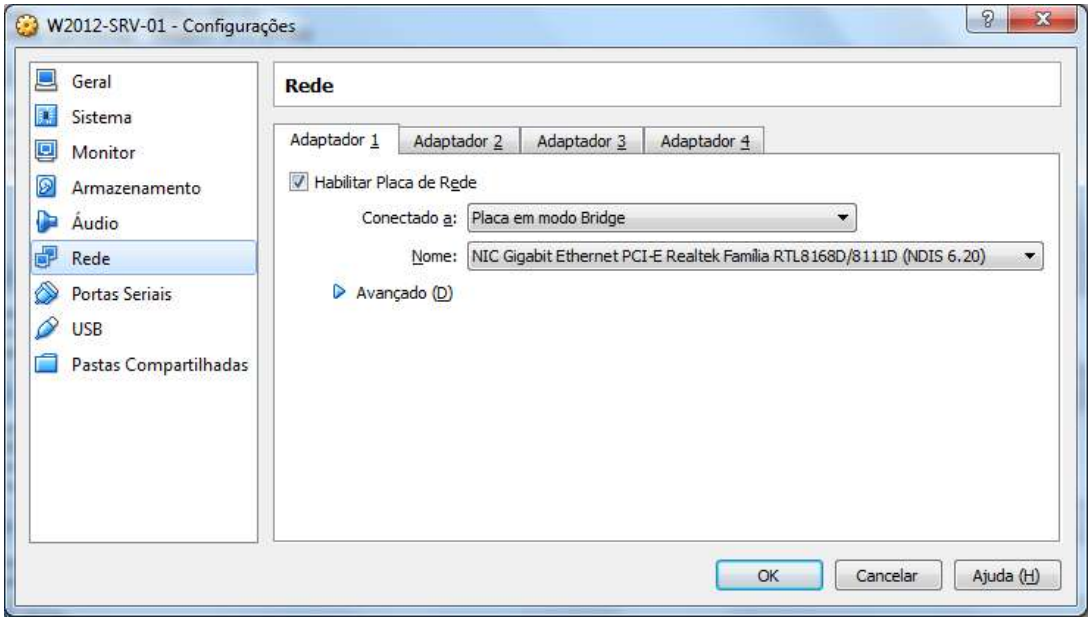
Para atingir esta tela, basta selecionar a máquina virtual que se deseja configurar, e clicar em “configurações”.



Na opção sistema, aba processador, defina quantos processadores terá sua VM, em muitos casos 2 processadores já é numero satisfatório.



Observe a quantidade de memória RAM disponível em seu computador e, com base nesta informação, veja quanto de memória RAM você poderá disponibilizar para sua máquina virtual, lembrando que para sistema operacional cliente, bastam 768 MB de memória RAM e para um servidor Windows 2012, ofereça 2048 MB de memória RAM.



Tela de configuração da máquina virtual W2014-SRV-01, que é uma das máquinas virtuais que serão utilizadas como controlador de domínio do ambiente virtualizado, onde vemos a área de configuração de rede, que possibilita a adição de até 4 adaptadores de rede, os quais serão necessários para a configuração do NIC teaming. Observe a existência de 4 abas “adaptadores”, bastando habilitar o campo “habilitar placa de rede”, para dar novo adaptador à máquina virtual.

1.3 NIC teaming (Agrupamento de adaptadores de rede)

Obviamente a conectividade e disponibilidade de um servidor de rede e algo tão importante que,neste curso, chega a ser assunto abordado antes mesmo de termos falado o mínimo sobre o windows server 2012.

Nesta versão existe a possibilidade de agregar duas ou mais interfaces de rede da máquina com a finalidade de aumentar o fluxo de dados desta, unindo os throughput das interfaces ou criando um funcionamento tolerante a falhas. Apesar de ser uma técnica que anteriormente era vinculada a uma ou outra característica do hardware da placa de rede, nesta versão 2012 e completamente independente.

Resumidamente quando se agrega diversos adaptadores de rede, em caso de falha de um deles todo o trafego de dados é redirecionado para os adaptadores restantes, sem grandes impactos na performance da rede.

Os modos de funcionamento do NIC teaming são:

1. Modo independente: As interfaces de rede são ligadas em switches diferentes.
2. Modo dependente: As interfaces de rede são ligadas ao mesmo switch.

No modo independente é possível escolher entre duas configurações, deixando as interfaces em modo ativo/ativo, onde as interfaces trabalham juntas, somando suas bandas de dados, causando a diminuição da largura de banda, caso uma delas deixe de funcionar e o modo ativo/standby, onde uma interface funciona e a outra fica em standby, entrando em atividade caso a interface ativa deixe de funcionar, neste caso, como uma delas já não estava funcionando, a largura de banda permanece a mesma. Em todo caso a queda de uma das interfaces não impacta visivelmente na troca de dados entre o servidor e os computadores clientes.

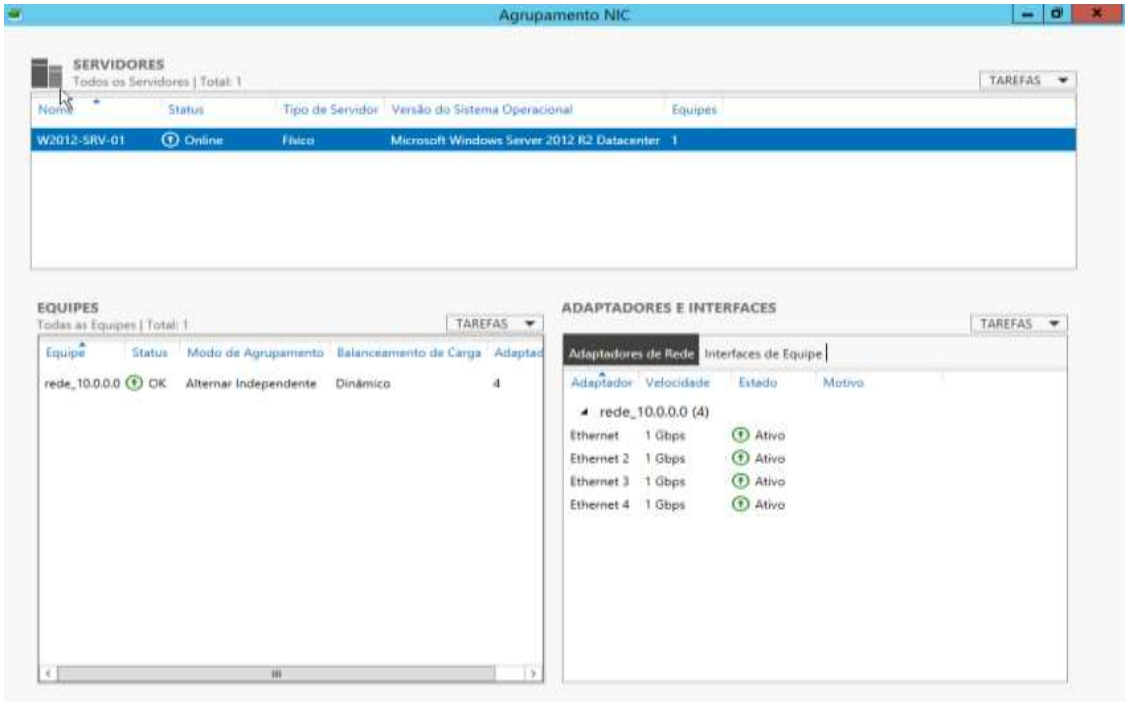
Modo independente:

É possível escolher entre duas configurações, deixando as interfaces em modo ativo/ativo, onde as interfaces trabalham juntas, somando suas bandas de dados, causando a dimunicão da largura de banda, caso uma delas deixe de funcionar e o modo ativo/standby, onde uma interface funciona e a outra fica em standby, entrando em atividade caso a interface ativa deixe de funcionar, neste caso, como uma delas já não estava funcionando, a largura de banda permanece a mesma. Em todo caso, a queda de uma das interfaces não impacta visivelmente na troca de dados entre o servidor e os computadores clientes.

Modo dependente:

É possível utilizar o balanceamento de carga utilizando o modo estático, que é um modo genérico, ou o modo LACP (Link Aggregation Control Protocol – 802.3ax), que já necessita que o adaptador tenha suporte a este modo.

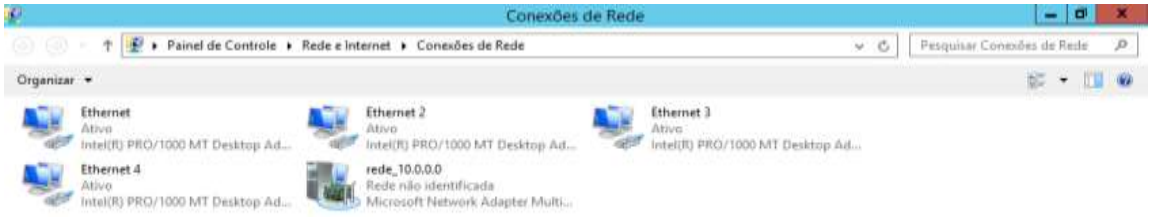
Visualização do NIC teaming



Acima um exemplo de agrupamento de interfaces de rede já configurado. Na área “equipes” é possível ver que só existe um grupamento formado, cujo nome é “rede_10.0.0.0”, para ficar claro que este grupamento atende a rede IP 10.x.x.x. Na área “adaptadores e interfaces” é listada a quantidade e quais os adaptadores que fazem parte do grupamento, bem como seu estado. Caso houvessem mais adaptadores disponíveis (por exemplo, mais quatro), seria possível criar um outro grupamento e colocar todos os quatro restantes, ou apenas dois deles, neste novo grupamento, para criar uma outra interface.

Obs.: Para se chegar nesta tela basta seguir o passos abaixo:

1. Abrir o gerenciador de servidores (Server manager)
2. Clicar em “servidor local”
3. Clicar em "habilitado" ou "desabilitado", na opção nicteaming.



Após a criação do nicteaming é possível visualizar que um novo ícone aparece, cujo nome é idêntico ao que foi dado ao agrupamento “rede_10.0.0.0”. O citado ícone representa a aglomeração dos quatro adaptadores de rede presentes na ilustração, com nome “ethernet x”. Neste caso, a configuração de IP e DNS deve ser executada sobre o ícone do nicteaming, e ficará válido para todos adaptadores que fizerem parte do grupamento.

Não faça configuração individual em um adaptador que faz parte de um grupamento!

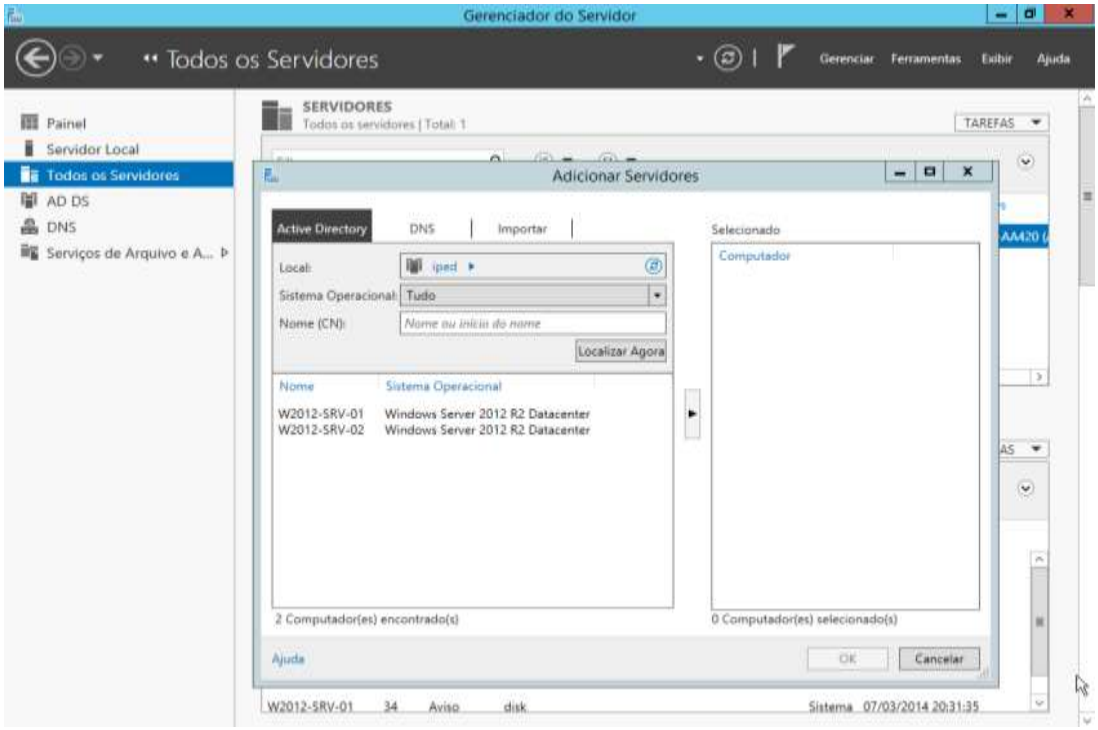
Atenção: para o laboratório a seguir, crie um snapshot da máquina virtual e dê a ele o nome de VM-ORIGINAL, ao final deste laboratório, crie outro com nome VM-NIC-TEAMING.

1.4 Gerenciamento de Servidores Centralizado

Uma das mais evidentes inovações do Windows server 2012 é a interface de gerenciamento centralizada de servidores, através da qual é possível gerenciar todos os servidores da rede sem a necessidade de acessar fisicamente o servidor e/ou remotamente. Com esta interface todo o trabalho de instalação de funções ou ferramentas ficam acessíveis para manipulação, desde que com uma conta com privilégios de administração.

Através da interface de administração, é possível criar grupos de servidores, organizando-os por localidade, funções, ou da forma como quiser, sendo possível, também, Adicionar servidores Windows server 2003, 2008 ou 2012, bem como instalar serviços e ferramentas em várias maquinas remotas de uma única vez, utilizando o Windows powershell.

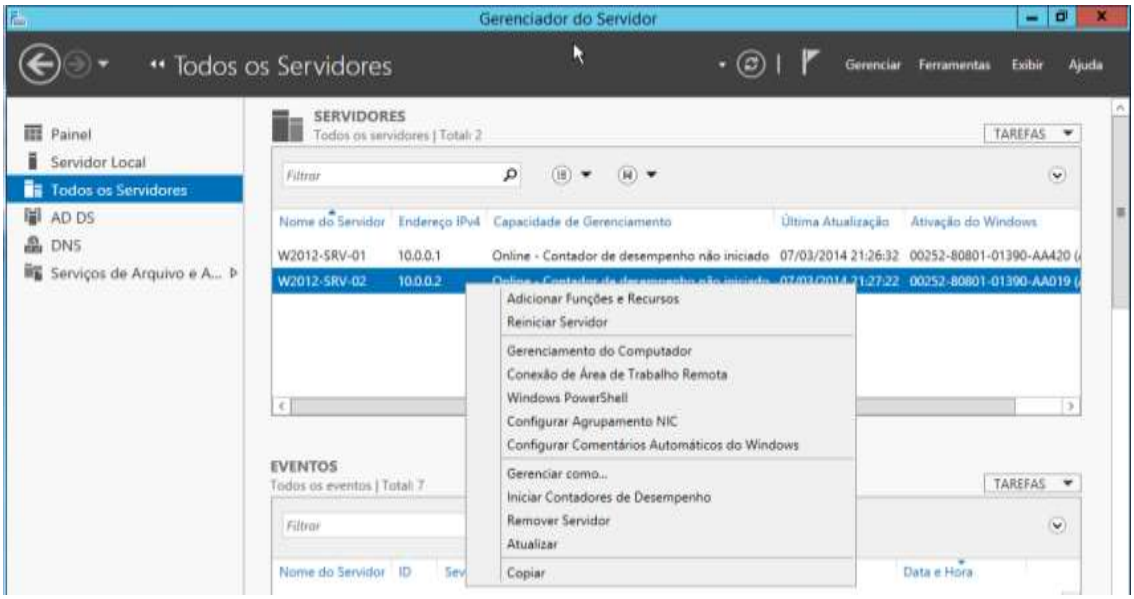
Outra novidade é que, em caso de máquinas virtuais, não é necessário que a VM esteja ligada para que suas propriedades sejam alteradas, uma vez que e possível modificar os arquivos diretamente dentro do próprio disco virtual (arquivo VHD), mesmo com a máquina virtual desligada.



Como é possível ver na ilustração acima, a adição de servidores ao painel “gerenciamento de servidor” (Server manager) é muito simples, sendo necessário que o computador que será adicionado já pertença ao domínio, feito isto, siga os seguintes passos:

1. Abra o gerenciador de servidores;
2. Clique com o botão direito sobre “todos os servidores”;
3. Clique em “adicionar servidores”;

4. A janela “adicionar servidores” abrirá, conforme a janela acima, mostrando todos os computadores com sistemas operacionais servidores pertencentes ao domínio, que poderão ser adicionados à interface de gerenciamento única;
5. Selecione o computador desejado, clique na seta para que passe ao estado de “selecionado”;
6. Clique em “OK”.



Adicionado o servidor, é possível gerenciá-lo remotamente através do painel de gerenciamento, conforme mostra a figura acima, inclusive adicionando funções e recursos ao computador.

O funcionamento de um domínio

Um domínio é uma área de segurança gerenciada por um sistema operacional servidor de rede, seja Windows ou qualquer outro sistema operacional, ao qual os demais computadores integrantes estarão submetidos às diretivas de segurança. Obviamente que tal “obediência” apenas é concretizada quando o computador ingressa no domínio.

Em todo caso, o fato de um computador não estar no domínio, não significa que ele não possa trocar informações IP com computadores que estejam dentro do domínio, tais como conteúdo HTML, impressão de documentos, etc.

No entanto, para se ter um domínio Windows é necessário que haja um computador na rede com requisitos de hardware suficientes para suportar Windows server 2012 e, além disso, que ele tenha a função de Active Directory instalada adequadamente.

1.5 Active Directory

O active directory é um recipiente cuja finalidade é armazenar informações referentes às entidades de segurança que compõem a rede. Estas entidades de segurança são outros computadores, clientes ou servidores, contas de usuários, aplicações e serviços diversos.

Quando estes objetos passam a existir no AD (Active Directory), uma entidade é criada para o objeto, com um SID exclusivo (Security IDentification – Identificação de segurança), que é a informação que identifica o objeto no domínio e perante os demais integrantes da rede. Este SID é exclusivo e único. Isto significa que, caso o objeto ingresse, receba um SID e saia do domínio, caso regresse já receberá uma nova identificação, completamente diferente da anterior. O AD é instalado e executado no servidor que recebe o nome de controlador de domínio, podendo existir outros sobressalentes com cópias do AD, atualizadas automaticamente, para caso de pane em um dos servidores.

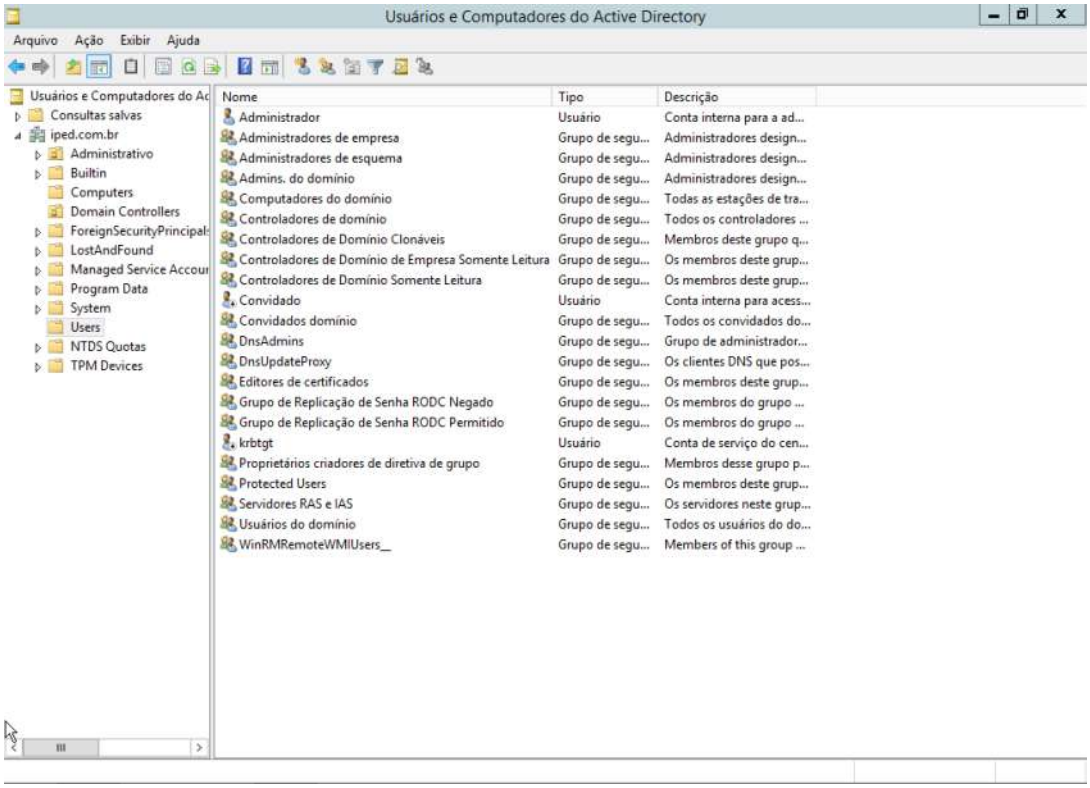
Active Directory – Unidades organizacionais

O active directory é dividido em OUs (unidades organizacionais), cuja finalidade é manter cada objeto agrupado de acordo com sua função ou importância para a rede de computadores.

Algumas OUs já são criadas por padrão quando se instala e configura o AD, podendo o administrador de rede criar outras várias, tantas quantas forem necessárias para organizar sua infraestrutura de acordo com seu planejamento.

É sempre importante manter alguns objetos em Ous diferentes, como é o caso de computadores e contas de usuários, uma vez que as diretivas de segurança da rede (GPOs – Group Policie Objects) são aplicadas sob as OUs, afetando diretamente os objetos contidos nelas, lembrando que existem GPOs específicas para computadores e usuários, motivo pelo qual é aconselhável que estes sejam mantidos em OUs diferentes.

Outro ponto é separar contas de usuários de acordo com sua relevância e privilégios dentro da rede, mantendo, por exemplo, contas de usuários administradores em uma OU e contas de usuários normais em outras, facilitando a utilização de GPOs específicas para cada grupo.



Acima um exemplo da interface de gerenciamento do activedirectory, onde é possível ver o domínio e sua estrutura original de Unidades

Organizacionais (Em modo de visualização avançado), bem como os grupos e usuários que já são criados por padrão.

Com o decorrer do uso o administrador da rede tem a possibilidade de criar novas unidades organizacionais (sugere-se seguir o organograma da empresa), grupos e alocar os usuários dentro de suas respectivas OUs e grupos, facilitando a aplicação de regras de acesso e políticas de segurança.

Ingressando com uma máquina no domínio

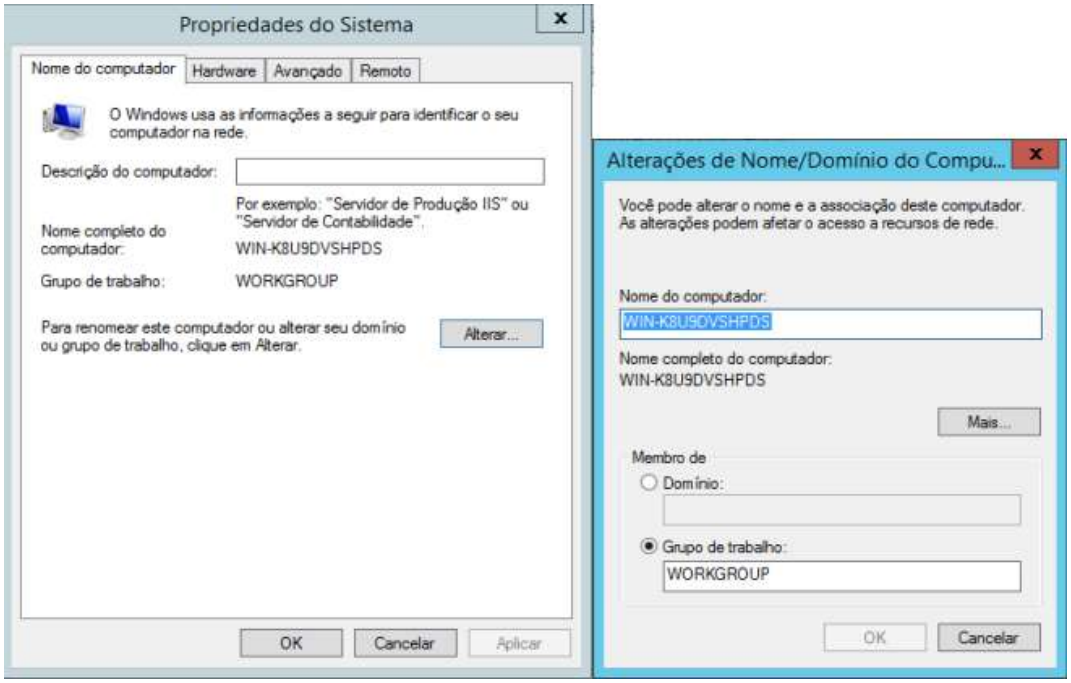
Inicialmente, vale lembrar que passa a existir um domínio em sua rede a partir do momento em que um dos computadores com sistema operacional Windows server 2012 passa a integrar a rede, com o active directory instalado e tenha sido elevado a controlador de domínio. Mesmo assim, o fato de existir um controlador de domínio da rede, não significa que as demais máquinas que pertençam à rede já estejam submetidas às regras de segurança e banco de dados de autenticação do domínio. Para que isto seja possível, é necessário que cada um dos computadores que integram a rede ingressem no domínio pelo qual o servidor responde que, no nosso caso, é o domínio iped.com.br.

Uma rede pode ter mais de um controlador de domínio, pode ter vários, o que não vai aumentar a segurança da rede, mas irá prover redundância de serviços de autenticação de contas, uma vez que o banco de dados do active directory será replicado entre todos eles.

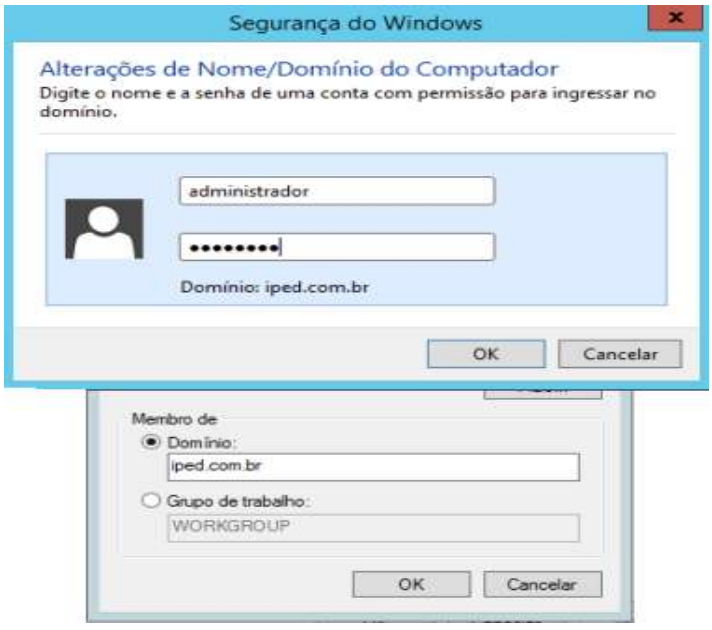
Para ingressar com uma máquina no domínio, basta acessá-la com a senha de administração, a qual será autenticada no banco de dados local do computador, uma vez que este ainda não está no domínio.

Uma vez utilizando usuário com privilégios de administração local, execute o seguinte procedimento:

1. Abra o Windows explorer
2. Clique com o botão direito sobre o ícone “computador”
3. Clique em “propriedades”
4. Na janela que aparecer, clique em “alterar configurações”
5. Na próxima janela, clique no botão “alterar” (a janela abaixo aparecerá)



Observe na janela acima que o nome do computador também não está adequado, e este é um dos servidores que serão usados no laboratório. No que diz respeito a servidores, um das primeiras ações que você deve tomar, antes de qualquer configuração, é providenciar a mudança do nome do computador. No caso acima, portanto, mudamos o nome do computador para W2012-SRV-03, reiniciamos o computador, voltamos para esta tela, e ingressamos no domínio iped.com.br, fornecendo as credenciais de administração do domínio, para que fosse possível tal ação.

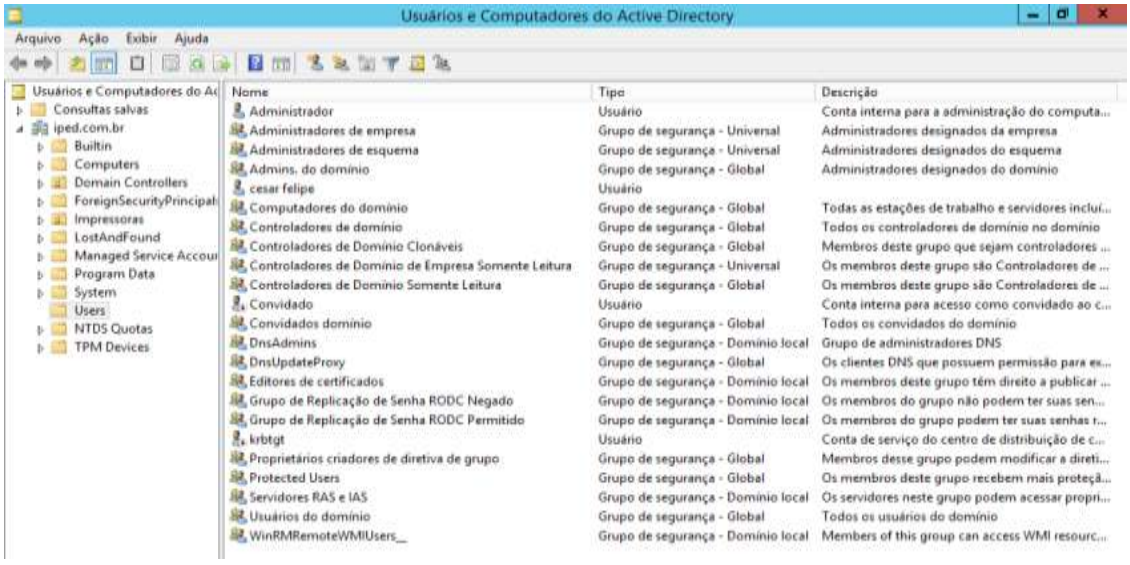


Assim que concluída esta ação, o computador será reiniciado e já retornará carregando as diretrizes de segurança do domínio, bem como irá constar no activedirectory, como uma entidade de segurança, que ficará disponível na OU “computadores”, caso no futuro este computador passe a controlador de domínio, automaticamente ele passará para a OU “controladores de domínios”.

Active Directory – Grupos de usuários

Uma das entidades mais importantes do AD, e que fará toda diferença na vida do administrador de rede, é a entidade conhecida como “grupo”.

Um grupo tem, grosseiramente falando, a finalidade de aglomerar contas de usuários de acordo com sua relevância. Assim, caso uma conta de usuário precise ter privilégios de acesso total, ele deve estar na conta de administradores de domínio, caso seja uma conta de usuário com acesso remoto, no grupo de usuário com acesso remoto, e assim respectivamente. Já existem diversos grupos criados, bastando ao administrador apenas ingressar com as contas dos usuários em cada um deles de acordo com os privilégios que o usuário terá. No entanto, também é possível criar novos grupos e dar a eles os direitos que se fizerem necessários para atender seu planejamento, tais como permissões de acessos a compartilhamento, exceções de aplicação de GPO’s, entre vários outros benefícios.



A ilustração mostra grupos que já são predefinidos e criados automaticamente. Cada um destes grupos reúne um conjunto específico de direitos sobre as máquinas do domínio. Também existe a possibilidade de criar novos grupos e definir privilégios personalizados ao grupo e seus componentes, de forma a atender as necessidades de seu projeto.

Ainda é importante saber que, no tocante a grupos de usuários, existem dois tipos, que são:

1. Grupos de distribuição: não são usados para fins de segurança. Tem por finalidade servirem para envio de informações, tais como e-mails.
2. Grupos de segurança: são para fins de segurança e permissão de acesso, afetando todos os usuários que pertencerem ao grupo. Dos vários grupos que existem, diversos podem ser do tipo segurança e os demais de distribuição.

Quanto à abrangência, chamada de escopo, estes podem ser:

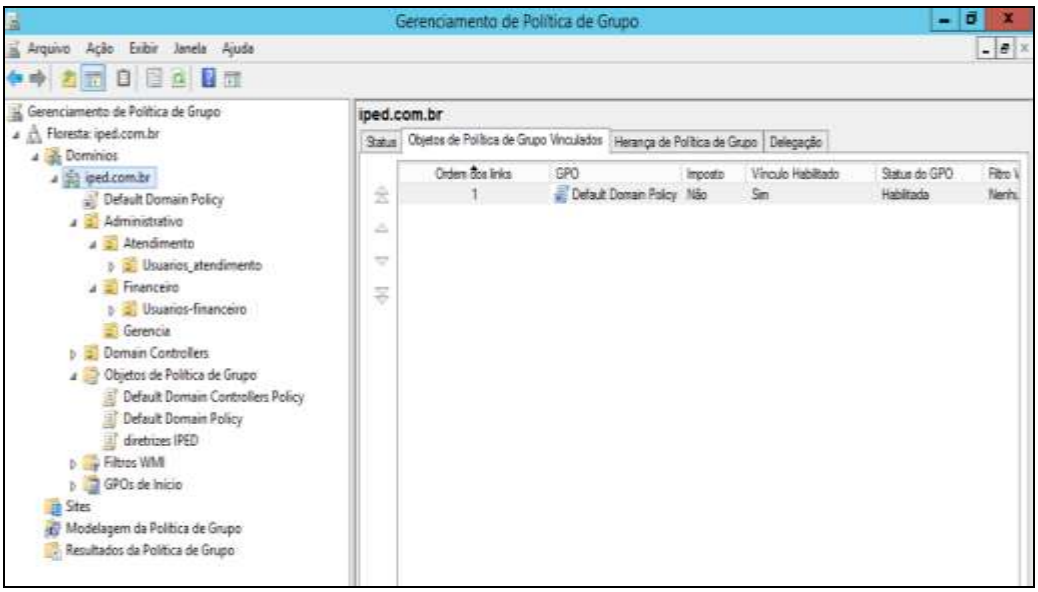
1. Grupos de domínio local: são reconhecidos apenas no mesmo domínio ao qual pertencem.
2. Grupos globais: são utilizados para dar acesso a contas em qualquer domínio na floresta.
3. Grupos universais: são utilizados para dar acesso a contas em qualquer domínio na floresta.

Active Directory – Group Policy Objects (GPOs)

GPOs são entidades que controlam e entregam diretivas de sistema e segurança para todos os computadores e usuários pertencentes a um domínio. Tais diretivas consistem em regras e ações que são aplicadas durante o carregamento do sistema operacional, durante seu desligamento e/ou durante o logon de um usuário, uma vez que são aplicáveis a computadores e/ou usuários.

Uma boa dica é evitar criar, dentro de uma única GPO, duas ou mais regras para finalidades distintas, sendo aconselhável que a GPO tenha um nome que faça referência à sua finalidade, o que se torna complicado se ela tiver diversas finalidades.

A GPO, inicialmente, aplicada em uma unidade organizacional existente, afetando todos os objetos que existam nela. No entanto escopo de aplicabilidade desta GPO pode ser reduzido, bastando indicar a qual grupo ele será aplicado, motivo pelo qual o bom planejamento na criação das unidades organizacionais e grupos terá impacto direto no trabalho do administrador da rede.



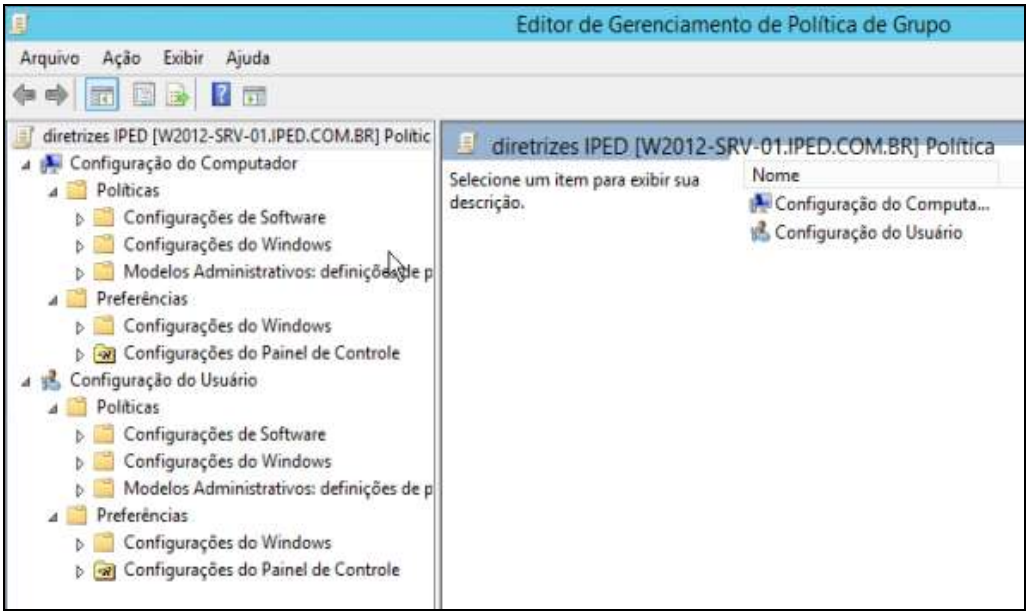
Por fim, uma GPO pode ser aplicada ao domínio, atingindo todas as unidades organizacionais e seus objetos, ou pode ser aplicada a uma ou várias destas de uma única vez, tudo fica a critério do administrador.

As GPOs são divididas em dois grupos com três subgrupos cada, cuja finalidade é facilitar encontrar regras de maneira facilitada. Estes grupos são:

1. Configurações de usuários
2. Configurações de computadores

E os subgrupos são:

1. Configurações de software: tem opções configuráveis referentes à instalação de programas.
2. Configurações do windows: tem opções de scripts e segurança para computadores e usuários e redirecionamento de pastas para usuários.
3. Modelos administrativos: tem opções extras de segurança baseadas em registro.



Acima a tela de edição de uma GPO.

Quando uma GPO é criada, ela recebe um número de versão, conforme esta GPO vai sofrendo modificações, seu número de versão vai sendo modificado, o que permite ao “client side extension”, que roda do lado do cliente, verificar se a GPO sofreu alteração, para que seja reaplicada com as modificações feitas.

Desta forma, o sistema cliente sempre verifica se houve modificação na GPO, caso o número da versão tenha mudado, o sistema entende que é necessário fazer a leitura do novo conteúdo da GPO para que esta seja aplicada com as novas mudanças.

Como já sabemos, as GPOs são aplicadas às unidades organizacionais e recebem um número de ordem de aplicação, cuja finalidade é definir qual GPO será aplicada primeiro. Para desabilitar uma GPO em uma determinada unidade organizacional, não é necessário desvincular a GPO, sendo suficiente desabilitar a GPO, deixando-a vinculada, sem efeitos.

Explicando mais profundamente o que foi passado anteriormente, a aplicação das GPOs nos clientes, é feita através do confrontamento da versão da GPO presente do cliente com a versão da GPO existente no controlador de domínio. O serviço responsável por isto é conhecido como client-sideextention. Apesar de ser possível atribuir nomes às GPOs, estas são identificadas por um numerador exclusivo em hexadecimal.

Unidade 2 - Endereços de IPs

Nesta unidade abordaremos algumas funções do serviço de DHCP que entre elas está a distribuição de endereços de IPs para os computadores clientes. Além de entender como é feita a instalação desse serviço em um computador que tenha a versão 2012 server.

Em seguida iremos mostrar como é possível atrelar um nome e um endereço de IP para cada host de rede.

E por último, veremos como configurar o DNS no cliente e no servidor também.

Bom estudo!

2.1 Distribuindo endereços IPs com DHCP

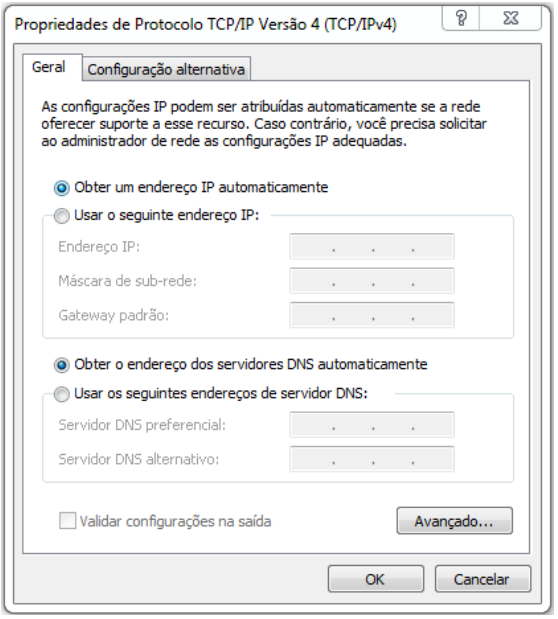
O serviço de DHCP funciona para distribuir automaticamente endereços IPs dentro de uma faixa pré-definida para computadores clientes, desde que estejam configurados para receber endereço IP de forma automática.

No entanto o serviço de DHCP, aprimorado no decorrer do tempo, não tem por função apenas fornecer endereços IPs. Ele também fornece, junto desta informação, os endereços de servidores DNS, gateway, servidor NTP, dentre outros dados.

A configuração e funcionamento do DHCP são simples. Basicamente basta definir o escopo de endereços IPs que o servidor irá fornecer, informando o endereçamento IP e sua máscara de subrede, lembrando que é importante que o administrador tenha conhecimento antecipado da quantidade de equipamentos que irão solicitar endereços ao DHCP e bom conhecimento de cálculo de endereçamento, pois podemos citar como exemplo o fato de que se a rede tem previsão de ter 500 clientes que precisarão de endereço IP, o escopo do servidor DHCP jamais poderá ser

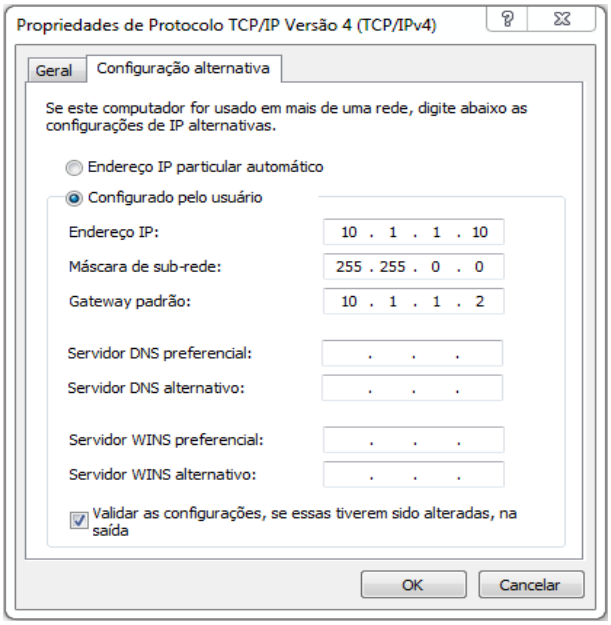
rede 192.168.1.0 com máscara 255.255.255.0, pois esta rede só terá disponíveis 254 endereços IPs válidos, quando o necessário seria um escopo com mais de 500.

Pelo exposto, se fôssemos levar o estudo de endereçamento IP a sério, a configuração correta seria rede 192.168.1.0 com máscara de subrede 255.255.254.0, que forneceria 510 endereços IPs válidos.



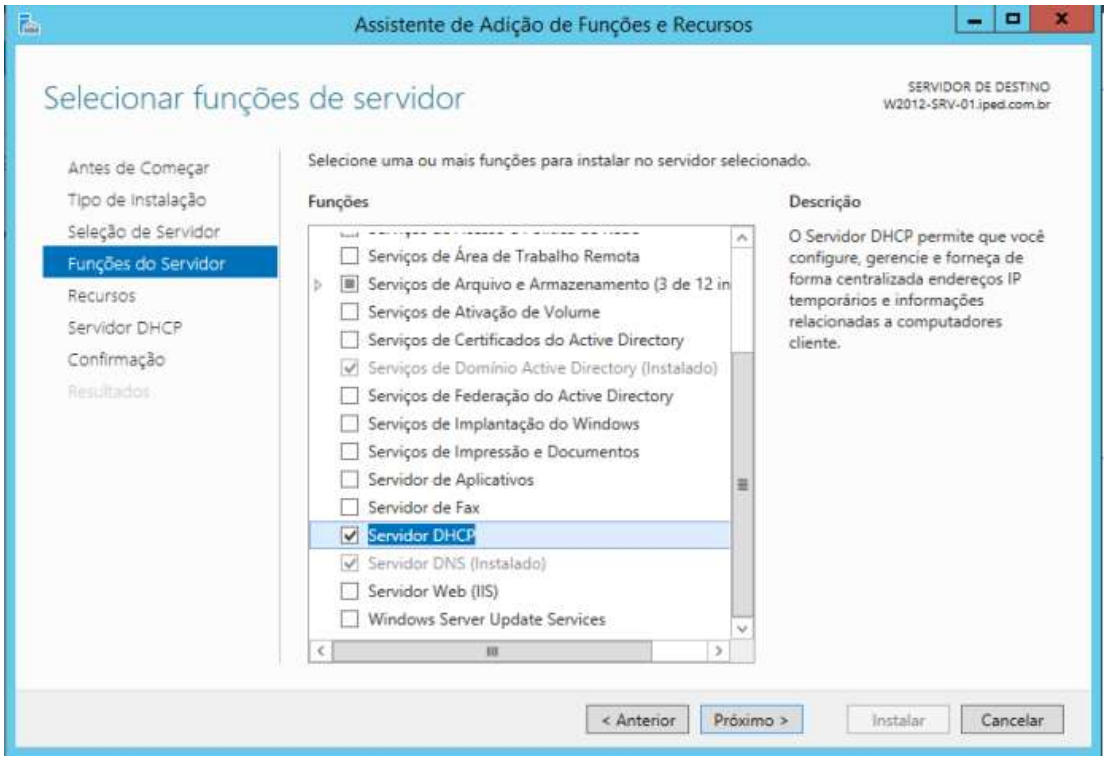
A figura acima ilustra a correta configuração do adaptador de rede para aquisição de endereço IP através de DHCP.

No entanto é bom que você saiba que um computador só pode fazer parte de um único domínio, mas que pode pertencer a várias redes IPs diferentes, uma vez que o endereçamento IP fica atrelado ao adaptador de rede. Desta forma, já que um computador pode ter diversos dispositivos de rede, cada um deles pode receber endereços IPs de redes diferentes, já que há a possibilidade de configurar um endereço IP “extra”, na aba “configuração alternativa” da janela de propriedades do endereço IP da opção “propriedades” do adaptador de rede, conforme figura abaixo.



Para que a solução de serviço DHCP funcione, é necessário que o serviço seja instalado em um computador com sistema operacional servidor de rede, no nosso caso, rodando a versão 2012 server.

A instalação de serviço é iniciada através da interface do gerenciador de servidor, clicando em “adicionar funções e recursos”, avançando pelas telas iniciais, até se chegar a janela abaixo.

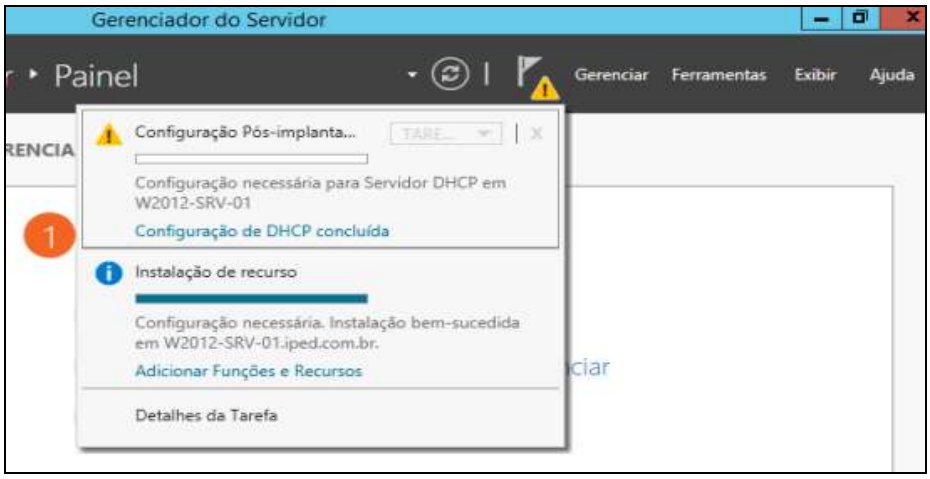


Onde a opção “servidor DHCP”, clicando-se posteriormente em “próximo”.

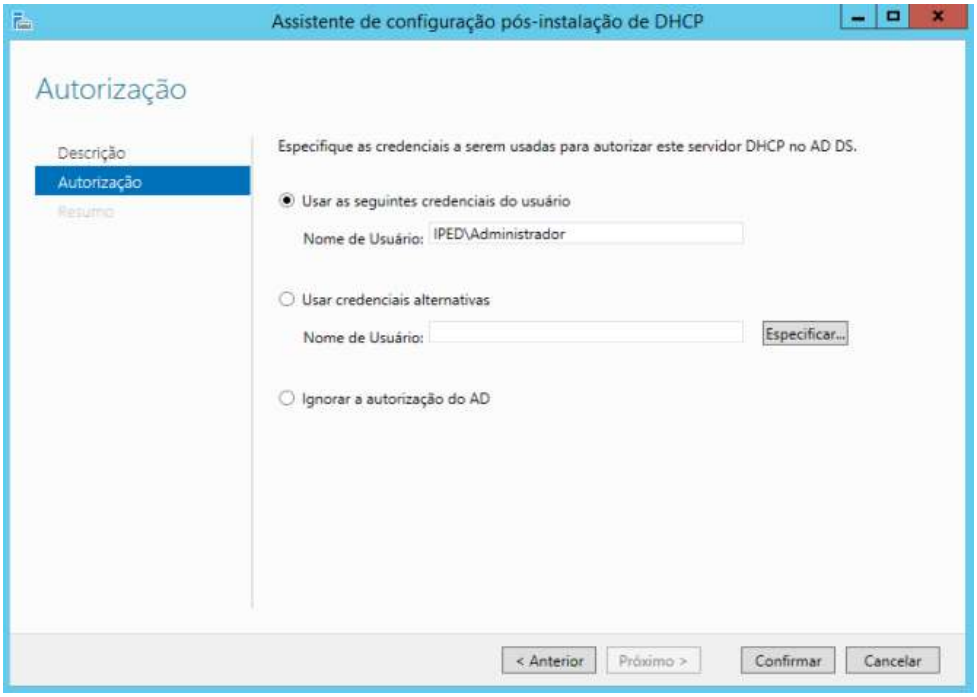
Como sempre, caso haja pendência de outras ferramentas para que o serviço que está sendo instalado funcione, a seguinte janela aparecerá.

É suficiente clicar em “adicionar recursos” e prosseguir pelas janelas seguintes até que seja iniciada a instalação.

Assim que for concluída a instalação, o notificador da janela do gerenciador de servidor irá indicar que há pendências para que o serviço rode adequadamente, basta clicar na notificação e no link sugerido pela janela, conforme ilustração.

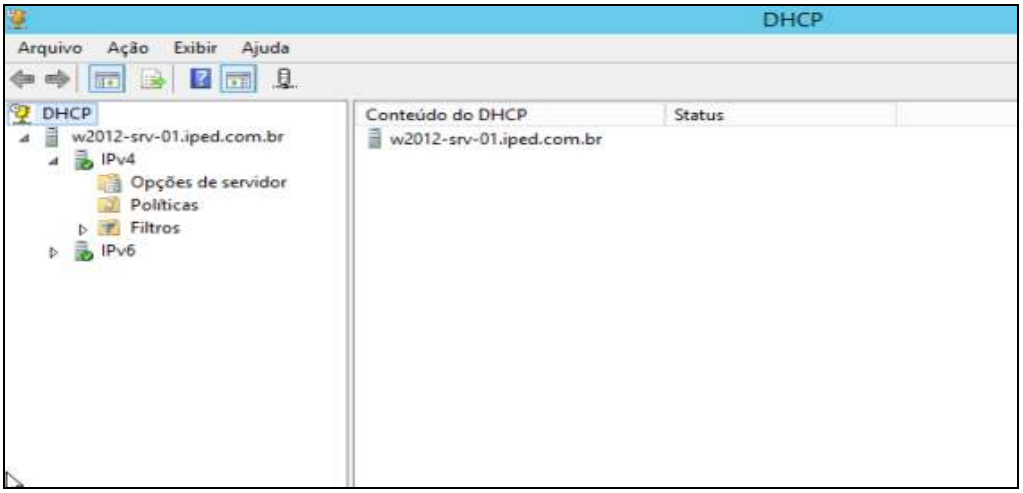


Na janela que será aberta, é suficiente avançar alguns passos, confirmando a conta de administração que será usada para a configuração, lembrando que a janela a seguir poderá não estar presente em todos os processos de configuração de outros serviços.

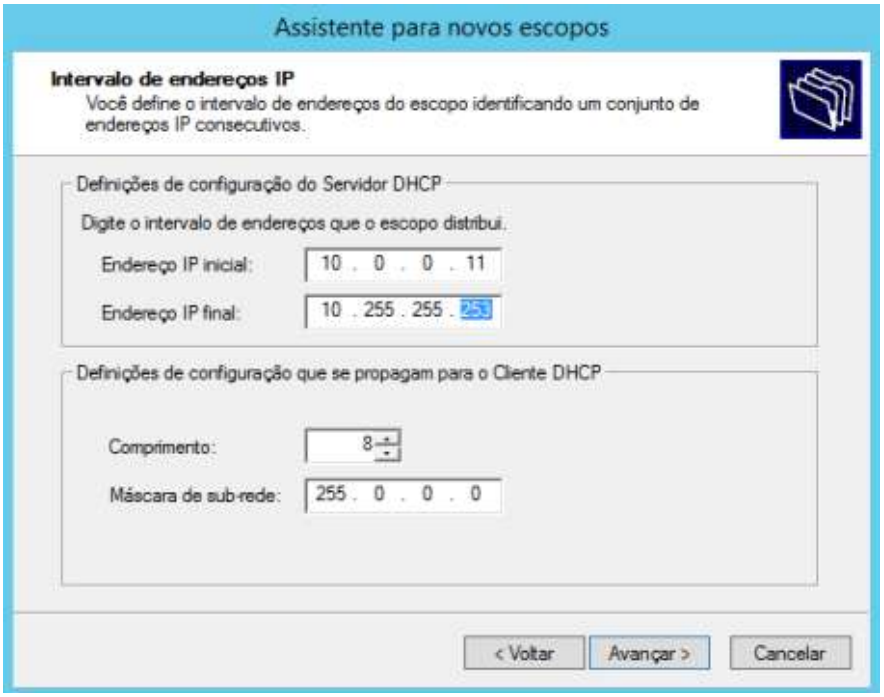


Clique em confirmar, e pronto. No entanto, não ache que o serviço de DHCP já está rodando, pois ainda será preciso criar o escopo de endereços, que veremos a seguir.

A configuração do DHCp é simples, basta clicar no menu “ferramentas”, na janela do gerenciador de servidores, e clicar em “DHCP”.

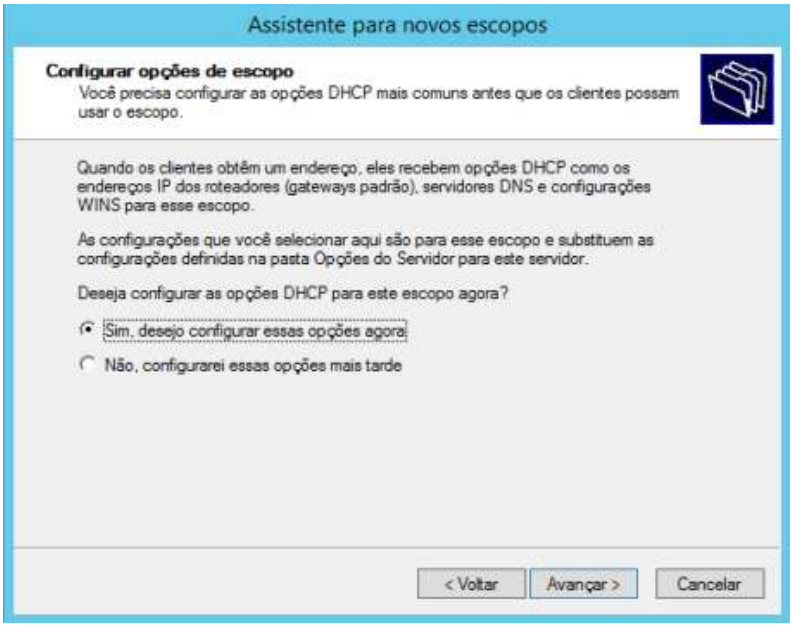


Observe que ainda não há escopo criado. Para fazê-lo, basta clicar com o botão direito sobre IPv4 e escolher a opção “novo escopo...”, avance algumas janelas e defina o nome e uma descrição para o escopo, clicando em “avançar”, a janela abaixo irá aparecer.

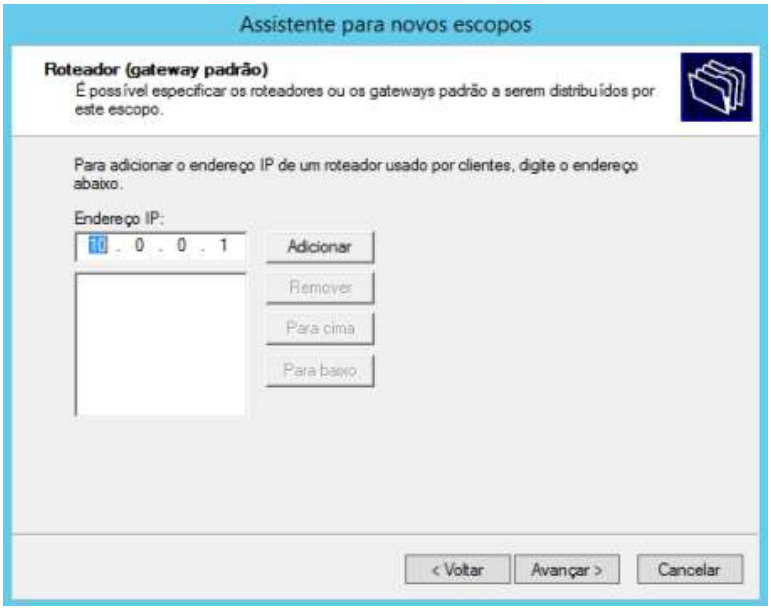


Nela, preencha os dados de endereçamento de acordo com o projeto de sua rede. Em nosso ambiente virtual, a “previsão” é de que existam 10 servidores (dado fictício), portanto o endereço IP inicial disponível para distribuição, será o IP 10.0.0.11, deixando os endereços iniciais, para que sejam atribuídos manualmente aos servidores, uma vez que as boas práticas de TI sugerem que servidores de rede tenham endereços configurados de forma fixa e manual.

Observe o endereçamento que foi preenchido na janela acima e cuidado! Os valores que serão colocados ali devem ser adequados e respeitar as regras de endereçamento. Para o bom uso de endereços IPs, é aconselhável que o administrador tenha um bom conhecimento a respeito do assunto. Clique em próximo e, na janela de “exclusão e atraso” e “duração da concessão”, clique em próximo novamente, pois não serão necessárias estas configurações.

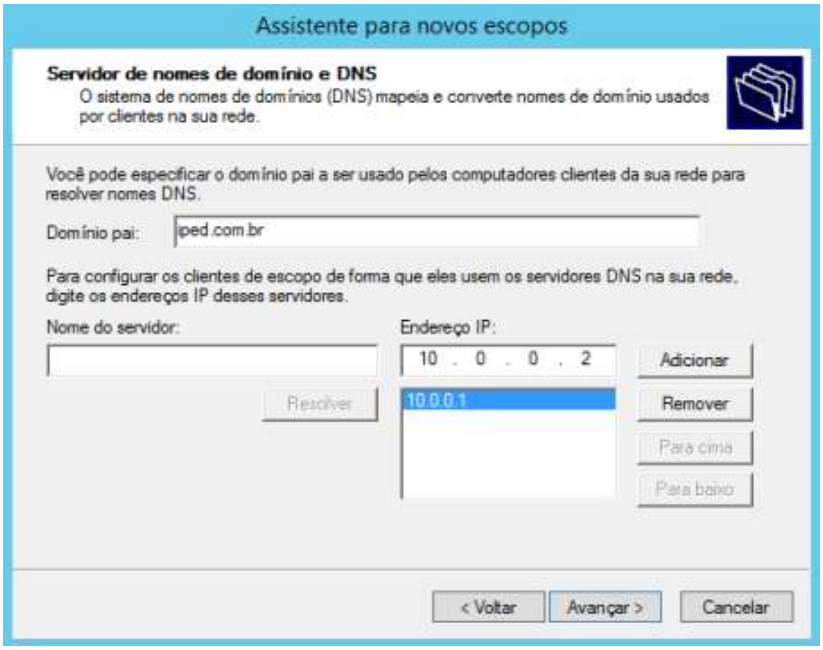


Na janela “configurar opções de escopo” marque a opção “Sim, desejo configurar estas opções agora” e clique em “avançar”.



Na janela de configuração do roteador, informe o endereço IP do equipamento que faz a conectividade entre a rede interna de sua empresa com outras redes IPs diferentes. Em nosso cenário, conforme vimos em vídeo aula passada, este papel está sendo exercido pelo próprio servidor de domínio, o que não é muito aconselhável, mas assim o fizemos por limitações do laboratório. O correto é utilizar um equipamento específico, no caso um roteador dedicado, para tal tarefa.

Assim que definido o endereço do roteador, clique em “adicionar” e siga para a próxima janela de configuração.

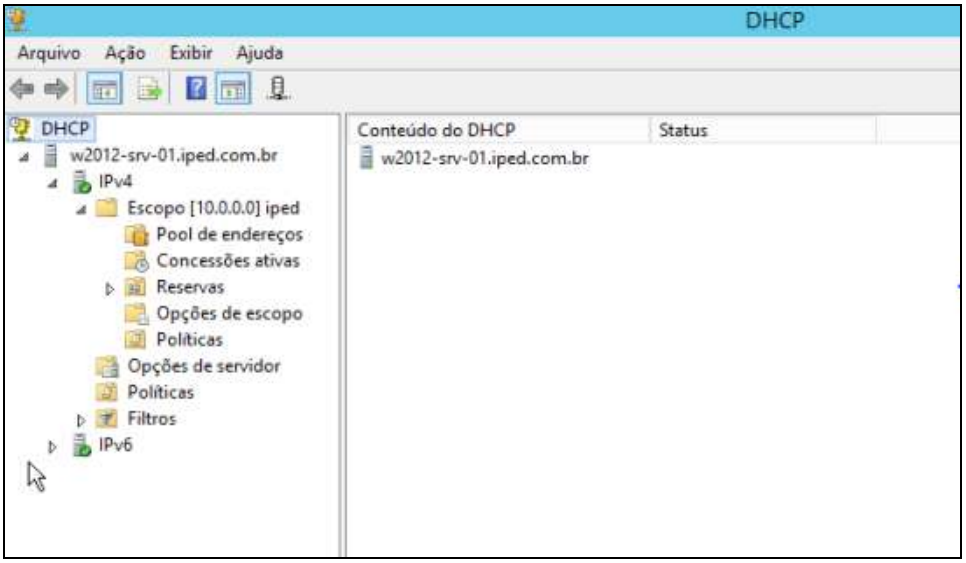


Nesta janela, tenha em mente que estará preenchendo uma das informações mais importantes do DHCP, que são os dados referentes aos servidores de DNS de sua rede. Na janela acima é possível ver que existem dois servidores de DNS, o 10.0.0.1 e o 10.0.0.2.

Tais informações são importantes para que computadores possam ingressar no domínio e resolver nomes de serviços, aplicações e demais recursos. Após o preenchimento, clique em avançar.

Na janela seguinte, é oferecida a possibilidade de configuração de servidores de nomes WINS, cuja finalidade é resolver nomes netbios, que há tempos caiu em desuso. Pelo exposto, não precisa ser configurado, a menos que você tenha em sua rede algum sistema legado.

Prosseguindo nas telas, ative o serviço DHCP e finalize a configuração.



A figura acima mostra o serviço DHCP devidamente configurado.

Agora é possível visualizar as concessões ativas, onde são mostrados os nomes dos computadores da rede e qual o endereço IP que lhes foi atribuído, fazer reserva de endereço IP para um computador específico da rede, impedindo que um determinado endereço IP seja fornecido para outro computador, que não o especificado, lembrando que tal reserva é feita com base no endereço MAC do computador cliente, informação que pode ser obtida com o comando ipconfig /all no prompt de comando do computador cliente.

2.2 Serviço de nomes de domínio (DNS)

No início da história das redes de computadores, as referências aos hosts pertencentes à rede de computadores eram feitas através de referências numéricas. Estamos nos referindo ao endereço IP!

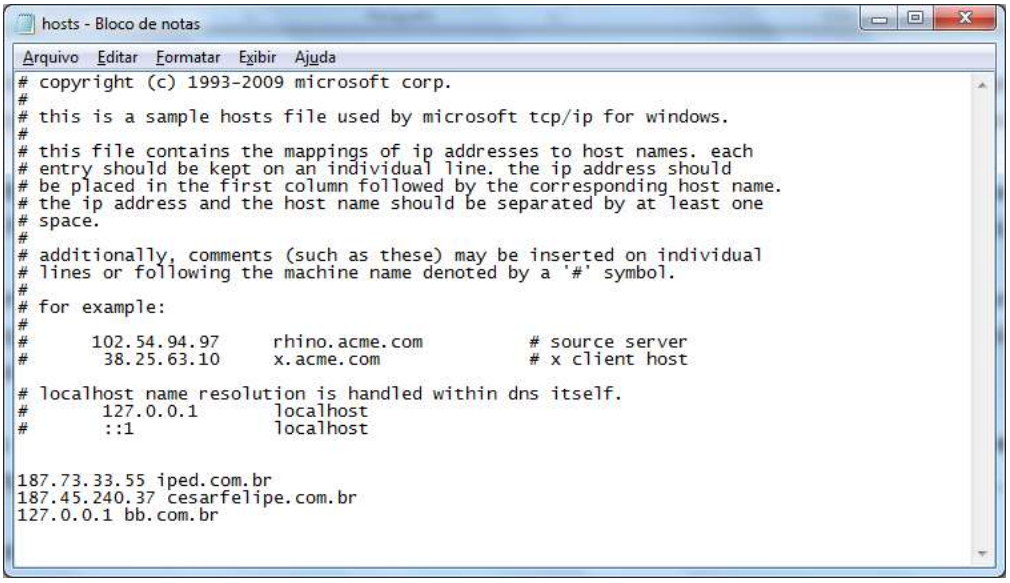
Contudo, com o passar do tempo, houve a necessidade de tornar estas referências mais palpáveis ao uso humano através do uso de nomes, ao invés de números, que são menos inteligíveis aos humanos.

Assim iniciou-se a utilização de nomes ficando, cada um, vinculado ao respectivo endereço IP de cada computador. Desta forma, para cada host da

rede, um nome e um endereço IP atrelado, tornando possível que aplicação encontrasse seu destino utilizando nome ou número.

Mas este registro de vínculo nome<>endereço IP, inicialmente era feito localmente, em cada computador, em um arquivo de texto bastante conhecido, cujo nome é “hosts”, presente em: %systemroot%\System32\drivers\etc

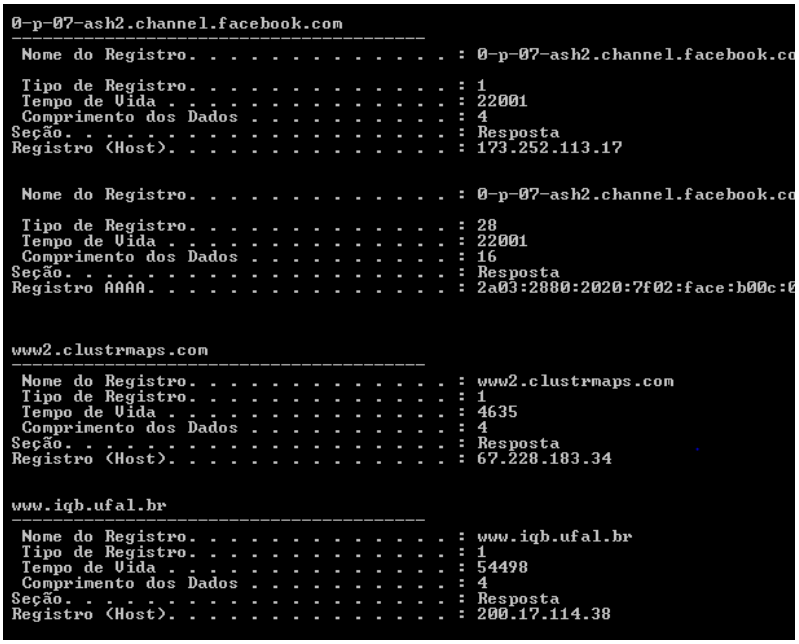
O qual pode ser aberto com o bloco de notas do Windows.



A ilustração acima mostra o arquivo HOSTS de um computador, onde vemos uma vinculação manual e estática do domínio cesarfelipe.com.br e iped.com.br aos seus respectivos endereços IPs e uma referência para o site do banco do brasil apontando para o endereço de loopback do próprio computador. Neste último caso, como efeito, o site do banco do brasil nunca será carregado, pois aponta para o próprio computador do usuário, que não tem serviço de IIS rodando, nem conteúdo algum do banco do brasil. Está prática pode ser utilizada para se evitar o acesso a determinados sites.

Toda vez que um computador cliente tenta acessar um recurso através de um nome, o “resolvedor”, nome do serviço de resolução que roda do lado do cliente, pesquisa por registros locais de nomes que estejam armazenados no arquivo hosts, que é um arquivo estático, cuja modificação do conteúdo deve ser manual. Caso não encontre registros, procura no cache DNS armazenado localmente, que pode ser visto quando se digita o

comando “ipconfig /displaydns” no prompt de comando e, não havendo registro, faz a pesquisa para o servidor DNS que foi informado pelo DHCP, ou que tenha sido configurado manualmente. Abaixo o resultado da saída do comando displaydns:



Imaginando uma infraestrutura partindo do zero, quando um servidor DNS recebe uma consulta, a resposta para esta consulta é respondida e, também, fica armazenada no cache do servidor DNS, uma vez que as consultas seguintes podem fazer referência ao mesmo conteúdo, evitando que reiteradas pesquisas referentes ao mesmo conteúdo sejam feitas ao banco de dados DNS, o que sobrecarregaria o servidor DNS, ou qualquer outro servidor DNS hierarquicamente superior aquele que recebeu a consulta.

No entanto, você pode estar pensando que armazenar um resultado DNS em cache pode ser arriscado, uma vez que o vínculo nome<>ip pode mudar com alguma frequência, fazendo com que o servidor DNS que tem a informação em cache possa enviar resultados imprecisos aos clientes. Para isto existe o TTL (Time To Live – tempo de vida) da informação, que por padrão é de uma hora, fazendo com que o servidor DNS verifique de tempo em tempo se aquela informação em cache ainda é valida.

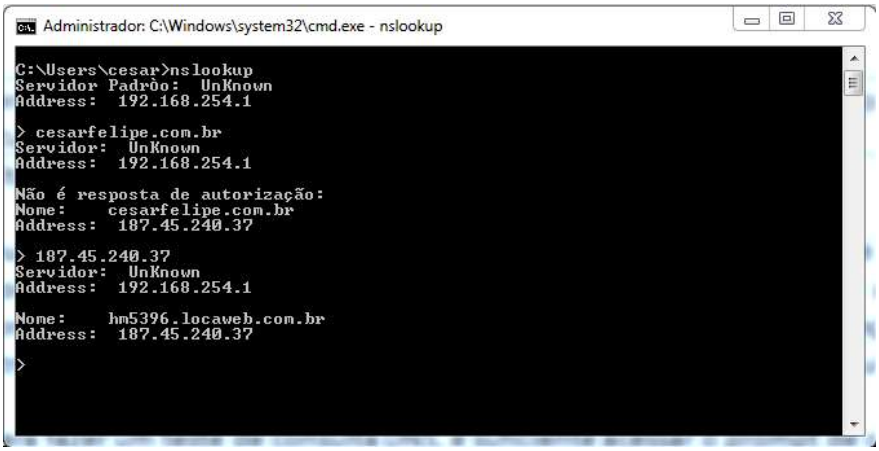
Caso o computador cliente, por qualquer falha que seja, esteja se baseando nas informações de seu cache, é importante verificar se não há algum registro dentro do arquivo hosts e, também, limpar o cache dinâmico do utilizando o comando ipconfig /flushdns.

No tocante ao assunto DNS, ainda existe o servidor DNS do tipo “encaminhador”, cuja finalidade não é ter uma base de dados relacional de nomes e endereços IPS mas, sim, de encaminhar pesquisas feitas por outros computadores para servidores DNS específicos. Este tipo de “servidor DNS” não recebe registros DNS, servindo apenas para fazer consultas em nome de outros computadores, retornando para estes os resultados. É importante saber disto, para que você entenda que um servidor DNS, de fato, tem registro de todos os computadores da rede e seus respectivos endereços IPS, uma vez que estes são informados para ele automaticamente, pelos próprios computadores quando do momento em que recebem seus endereços IPs pelo DHCP, ou este banco de dados é criado manualmente pelo administrador de rede. Tudo depende do planejamento de sua rede e da camada de segurança extra que você pretende colocar, quando evita que seu banco de dados DS seja atualizado pelos próprios computadores de forma automática.

Outro ponto interessante, que encerra o assunto referente a DNS, é o fato de que o servidor DNS pode receber um nome de máquina, querendo saber o IP vinculado a ele, o que é feito através de consulta a base de dados da “zona direta”, ou receber um endereço IP querendo saber o nome atrelado a este, o que é feito nos registros existentes na zona de pesquisa reversa.

Para fazer um teste de consulta DNS, é suficiente acessar o prompt de comando de seu computador e digitar o comando “nslookup”. Feito isto, digite o nome de um domínio qualquer, como “CESARFELIPE.COM.BR” e veja que será informado qual o IP do computador que atende pelo domínio. Feito isto, utilize o mesmo IP que te foi enviado como resposta e veja que será obtida como resposta o nome do computador que atender pelo domínio.

Respectivamente você fez uma pesquisa para uma “zona de pesquisa direta” e, depois, uma pesquisa para uma “zona de pesquisa reversa”, conforme mostra a figura abaixo.



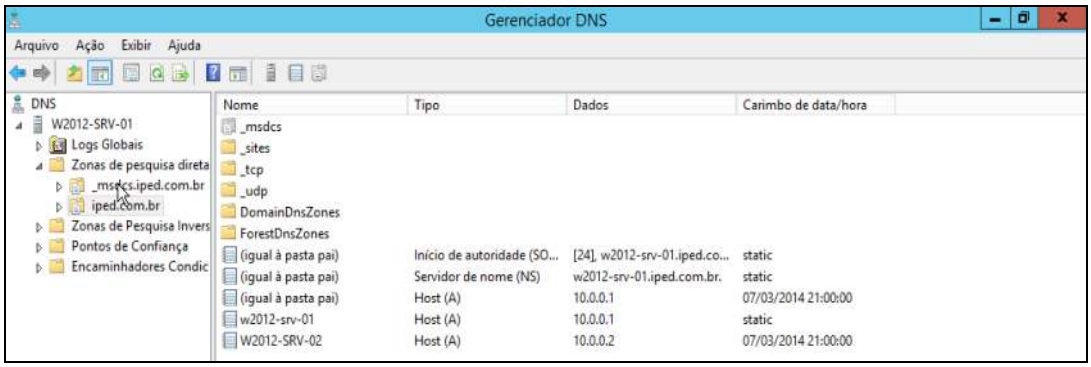
Observe também que para toda pesquisa feita, existe uma linha que informa quem é o servidor que está sendo responsável por responder às pesquisas feitas, que neste caso é o computador de IP 192.168.254.1

O serviço de DNS contém diversos tipos diferentes de registros, estes são:

1. SOA (Start Of Authority) – Cada zona DNS pode ter apenas uma autoridade deste tipo e indica que ele é o melhor recurso de DNS da zona.
2. NS (Name Server) –Os IPs registrados sobre esta identificação são reconhecidos como servidores DNS para a zona em questão, e podem ser os servidores primários ou secundários desta.
3. A (IPv4 Address) – Registro de relação nome-para-IP na versão IPv4
4. AAAA (IPv6 Address) - Registro de relação nome-para-IP na versão IPv6.
5. PTR (Pointer) - Registro de relação IP-para-nome que são criados e armazenados na zona de pesquisa reversa.
6. CNAME (Canonical Name) –São alias (Apelidos) que pode ser usados como nomes alternativos para um registro “A”.

MX (Mail Exchange) – Identifica que o IP informado neste registro é servidor de e-mail.

2.3 Conhecendo o DNS

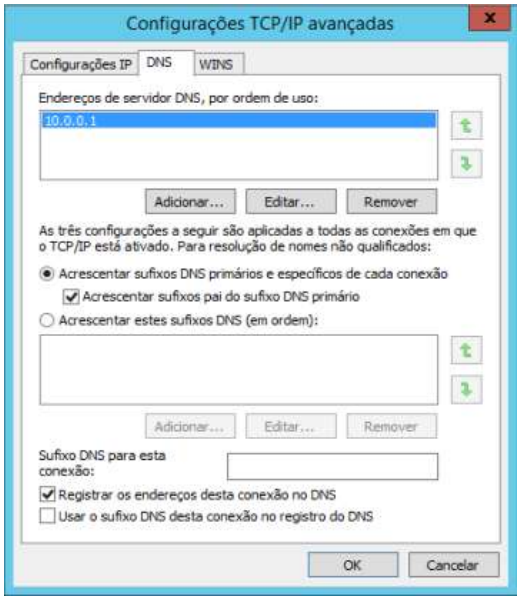


Acima a ilustração mostra o banco de dados DNS, contendo dois computadores. W2012-SRV-01, que é servidor DNS para o domínio IPED e W2012-SRV-02, que acabou de ingressar no domínio e, está com a configuração IP definida manualmente, inclusive o endereço do servidor DNS (configuração IP feita antes de ele ingressar).

Observe que W2012-SRV-01 e W2012-SRV-02 contém registros do tipo “A” e do tipo “NS”, que representam, respectivamente:

1. Vinculo do nome da maquina com endereço IP v4
2. Informe de que os computadores são servidores de DNS

Configuração do DNS no cliente



Por padrão W2012-SRV-02, como qualquer outro computador, vem configurado para informar ao seu servidor DNS seu nome e IP, permitindo

ser encontrado através de consultas DNS posteriores, conforme configuração apresentada na ilustração acima. (Observe a opção “registrar os endereços desta conexão no DNS” marcada, o que confirma as informações repassadas anteriormente.)

Esta tela foi alcançada clicando-se no botão “avançado” na janela de configuração do endereço IP do computador cliente.

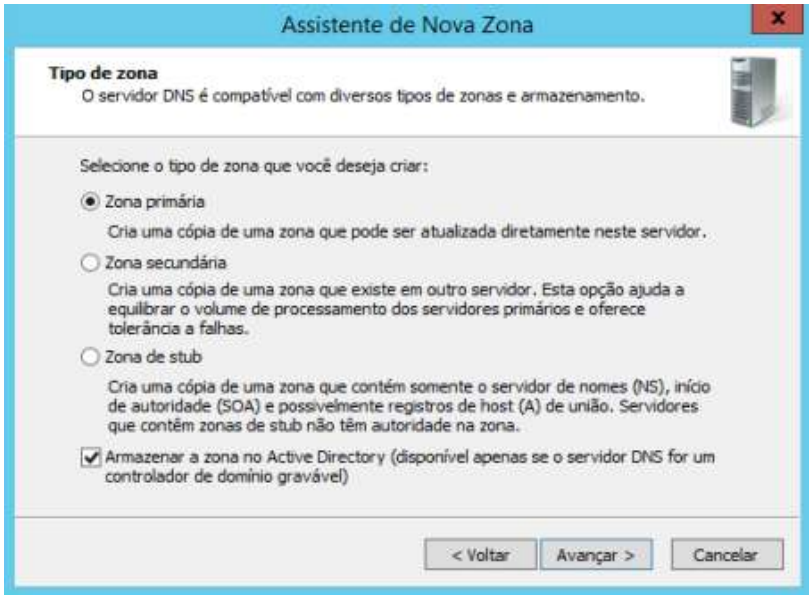
Configuração do DNS no servidor

O fato de instalar o serviço de DNS no servidor, não significa que ele esteja devidamente configurado. Desta forma, é necessário abrir a gerência do DNS, disponível no menu “ferramentas” do gerenciador de servidores.

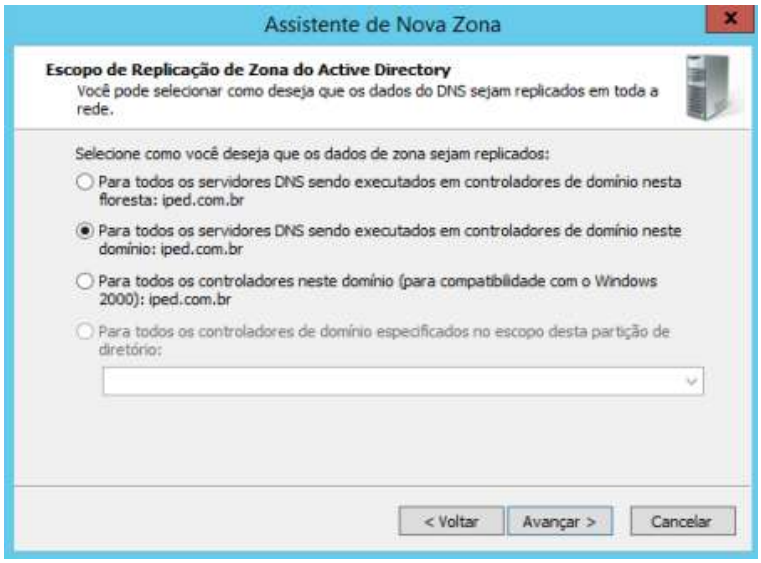
Uma vez aberto o gerenciador, veremos a seguinte janela:

Inicialmente é possível ver a existência de duas zonas distintas, a zona de pesquisa direta, responsável pela resolução de nomes em endereços IPs, e a zona de pesquisa inversa, responsável pela resolução de endereços Ips em nomes de computadores.

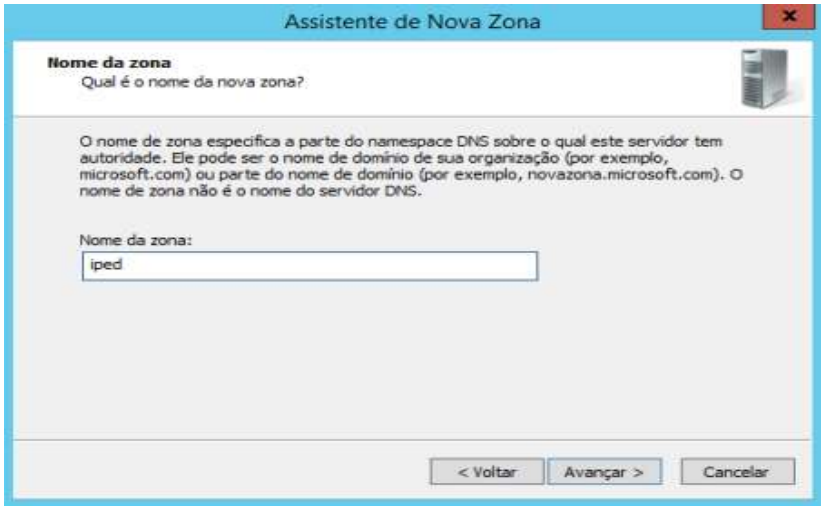
Para começar a configuração, clique com o botão direito sobre “zonas de pesquisa direta” e clique em “nova zona”, avançando pela tela de boas vindas.



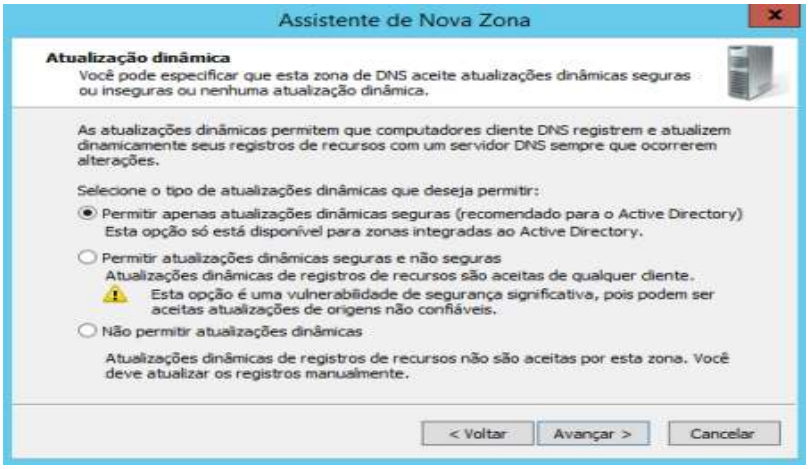
Nesta janela, marque a opção “zona primária” e avance.



Na janela acima, você poderá escolher se as informações que serão recebidas por este servidor de DNS será replicada para computadores apenas dentro do domínio iped.com.br, ou se será replicada para quais outros servidores DNS que, por ventura, estejam na mesma floresta que o domínio IPED. Esta decisão vai depender de sua infraestrutura e de suas diretrizes de segurança.



Nesta janela, digite o nome da zona de pesquisa, lembrando que o comportamento padrão neste passo é utilizar o nome do domínio.



A janela acima é uma das etapas mais sensíveis, pois nela será definido que se computadores que ingressarem na rede terão permissão de informar ao DNS seus nomes e IPs, para que fiquem disponíveis para resolução.

Caso você queira segurança máxima na atualização de seu banco de dados DNS, escolha a opção “não permitir atualizações automáticas”, onde você terá de registrar manualmente todas, ou parte, das máquinas que integram sua rede, o que pode ser um grande e contínuo trabalho.

Em geral a escolha é pela primeira opção, impedindo que computadores que não façam parte do domínio registrem-se no DNS, o que pode ser visto como uma falha de segurança.

Após este passo, basta avançar e concluir. De agora em diante, para cada computador que ingressar na rede, seja com IP dinâmico, ou manual, ocorrerá o registro no banco de dados do servidor DNS.

Unidade 3 - Compartilhamento de recursos

Olá,

Nesta unidade você irá conhecer os dois tipos de compartilhamento de recursos: o básico e o avançado. E qual deve ser a forma correta de aplicar permissões de usuários nesse processo.

Também conhecerá a função do sistema de arquivo distribuído (DFS), além de como fazer sua instalação e configuração afim de facilitar o acesso de usuários em vários compartilhamentos espalhados pela rede.

Bom estudo!

3.1 Compartilhamento e permissão de acesso

Depois da possibilidade de que computadores trocassem dados através de uma rede, um benefício importante tornou-se possível: o compartilhamento de recursos.

Atualmente é possível compartilhar pastas, arquivos, impressoras e scanners e, em um nível mais avançado, compartilhar até o processamento do equipamento, para que seja usado por outro.

Quando queremos compartilhar algum recurso, devemos ter as seguintes informações:

1. Qual recurso será compartilhado;
2. Quais usuários terão acesso ao recurso compartilhado;
3. Quais serão as permissões destes usuários.

É importante saber que existem dois tipos de compartilhamento, sendo um básico e o outro avançado. O modo simples é obtido quando um usuário limitado cria uma pasta, tornando-se proprietário desta, razão pela

qual ele terá acesso ao modo básico de compartilhamento, onde é possível, apenas, indicar os usuários e se estes terão as seguintes permissões:

1. Sem acesso
2. Somente leitura
3. Leitura e gravação

Já no modo avançado, disponível para administradores, é possível definir permissões mais detalhadas, tais como apagar, criar ou modificar arquivos, executar, listar conteúdo, dentre outras.

No entanto, saiba que as permissões podem ser aplicadas a usuários de forma individual, o que não é aconselhável, salvo se for um caso muito específico, sendo correto aplicar permissões diretamente nos grupos de usuários.

Assim, se um grupo obtém permissão de criar arquivos dentro de uma pasta, mas um de seus usuários recebe uma permissão negativa de poder criar arquivos, é a permissão negativa que irá prevalecer sobre este usuário, mesmo que ele pertença a um grupo com permissões positivas.

Então saiba que, existindo contradição entre permissões sobre um mesmo objeto, as permissões que serão aplicadas são as de negação de privilégios.

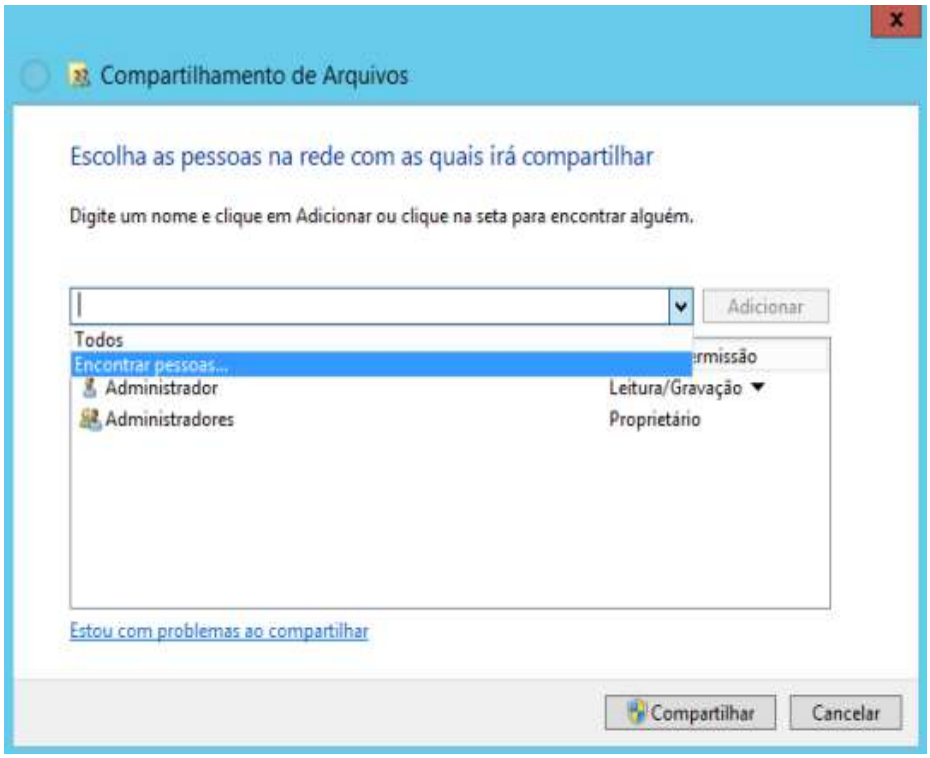
No mais as permissões permissivas são acumulativas, o que significa que é possível dar privilégios de leitura e, em outro momento futuro, dar permissão de escrita para um mesmo usuário, fazendo com que o usuário em questão tenha as duas permissões.

Herança de permissões é outro assunto importante, para isto imagine o seguinte cenário:

Então vamos compartilhar a pasta “publica, dando acesso aos grupos de domínio criados (do tipo domínio local) para esta pasta.

Para isto, faça:

1. Clique com o botão direito sobre a pasta “publica”
2. Clique em “propriedades”
3. Clique na aba “compartilhamento”
4. Clique no botão “compartilhar”
5. Clique na seta do campo indicado na figura abaixo



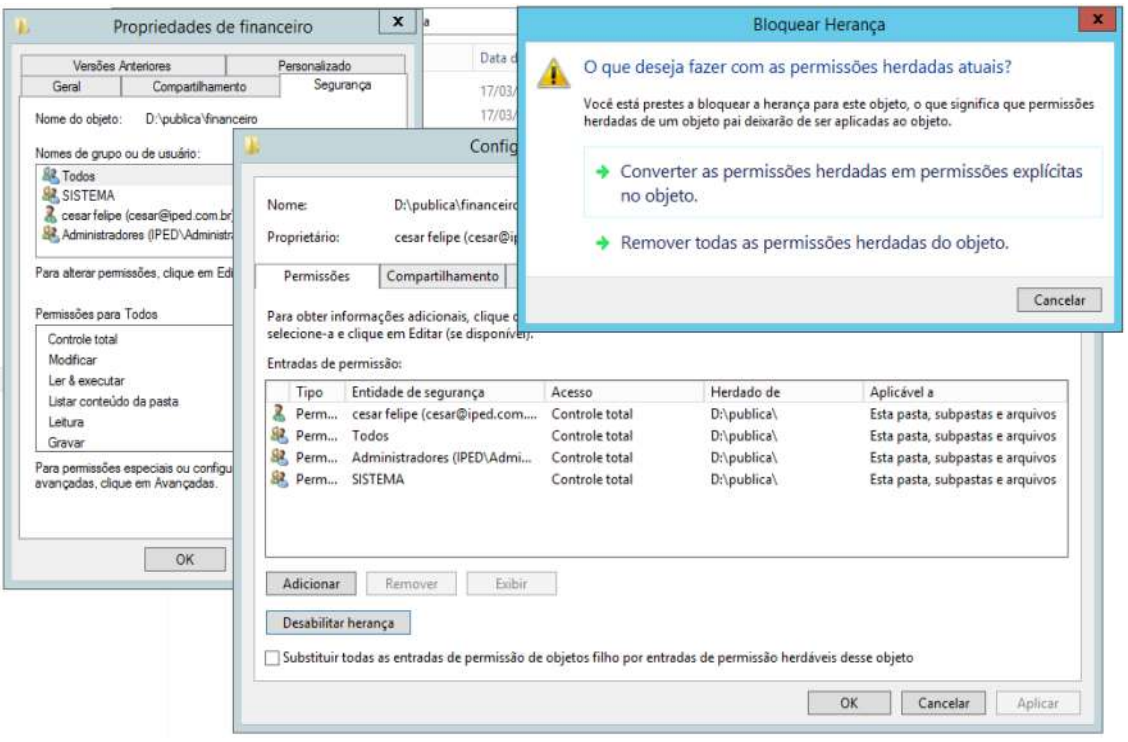
6. Clique em “encontrar pessoas”
7. Digite o nome do grupo que deseja adicionar, no nosso caso, GRP_financeiro, GRP_diretoria e GRP_atendimento
8. De para eles acesso de “leitura”

Se dermos permissão de acesso “somente leitura” à pasta “publica”, por padrão todas as pastas filhas (atendimento, diretoria e financeiro) herdarão a permissão. No entanto, é possível quebrar a herança padrão, com o seguinte procedimento (utilizaremos a pasta financeiro como exemplo):

1. Clicar com botão direito na pasta “financeiro”
2. Clicar em “propriedades”
3. Na janela que abrir, clicar na aba “segurança”
4. Clicar no botão “avançado”
5. Clicar no botão “desabilitar herança”
6. Clicar em “converter as permissões herdadas em permissões explícitas no objeto”

Faça o mesmo nas demais pastas!

Executando o procedimento descrito anteriormente, a herança é quebrada com a pasta pai, e cópias das permissões são definidas diretamente na pasta, permitindo que sejam aplicadas permissões específicas para cada pasta.



Deste ponto em diante é hora de iniciar todo o processo de definição dos privilégios adequados para cada pasta, no nosso caso, a pasta “financeiro”.

Assim, para darmos privilégio total ao grupo “financeiro” (GRP_financeiro) sobre a pasta “financeiro”, basta fazer o seguinte:

1) Acesse o computador que contêm a pasta compartilhada (neste caso o Servidor w2012-srv-02)
2) Clique com o botão direito sobre a pasta “financeiro”
3) Clique em “propriedades”
4) Clique na aba “segurança”

Observe a presença dos três grupos citados anteriormente com privilégios sobre esta pasta.

5) Clique no botão “avançado”
6) Clique em “desfazer herança” e confirme de acordo com instrução repassada anteriormente
7) Marque o GRP_financeiro
8) Clique em “editar”
9) Na janela que aparecer, marque a opção “controle total”
10) De OK em todas as janelas.
11) Como passo extra, caso queira, você poderá excluir os outros 2 grupos dos privilégios da pasta financeiro, impedindo-os, inclusive, de acessar a pasta.

3.2 Sistema de arquivos distribuídos

Também conhecido como DFS, tem por função permitir que arquivos sejam encontrados de maneira mais fácil pelos usuários, sem a necessidade de que tenham de se lembrar do nome ou IP do computador que detém a pasta compartilhada, caso não tenha a pasta mapeada. Também é utilizado para agrupar sobre um único caminho diversas pastas compartilhadas, para que possam ser visualizadas de maneira mais fácil pelo usuário, sem a necessidade de várias ações para se alcançar os compartilhamentos necessários, bastando apenas digitar o namespace referente ao agrupamento de todos estes recursos.

Outra funcionalidade importante do DFS, é que as pastas compartilhadas e seus conteúdos podem ser replicados para outras áreas da rede, criando um ambiente de alta disponibilidade e de tolerância a falhas, tudo de maneira transparente para o usuário.

Resumidamente podemos utilizar como exemplo, o seguinte cenário:

Imagine 3 computadores diferentes, chamados de servidor-01, servidor-02 e servidor-03. Cada um, respectivamente, com as seguintes pastas compartilhadas: documentos, cálculos e multimidias.

Sem DFS, estes recursos deveriam ser acessados da seguinte maneira:

\\servidor-01\documentos

\\servidor-02\calculos

\\servidor-03\multimidias

Com DFS o acesso fica assim:

\\iped.com.br\documentos

\\iped.com.br\calculos

\\iped.com.br\multimidia

Veja que antes tínhamos três origens diferentes (o nome dos computadores). Agora temos apenas uma origem, que aglomera todos os compartilhamentos em um local único, mesmo que venham de computadores diferentes. Facilitar o acesso. Esta é a função do DFS!

Vale lembrar que namespace é o nome que se dá ao identificador que irá concentrar em um único alvo todos os compartilhamentos distribuídos através da rede.

Existem dois tipos de namespace DFS, que são:

1. Namespace baseados em domínio: se registram no Active Directory e podem pertencer a diversos servidores DFS, criando um ambiente de alta disponibilidade e aglomerando pastas originadas de mais de 50 mil computadores diferentes.

2. Namespace stand-alone: não se registram no Active Directory e não suportam que dois sistemas DFS suportem o mesmo namespace, o que impossibilita a criação de um ambiente de alta disponibilidade, pois se o computador que presta o serviço de DFS se tornar indisponível, o namespace também se tornará inoperante.

3.3 Instalação e configuração do DFS

A seguir vamos aprender a configurar o DFS, visando facilitar o acesso de usuários em diversos compartilhamentos espalhados pela rede.

Neste cenário temos dois computadores:

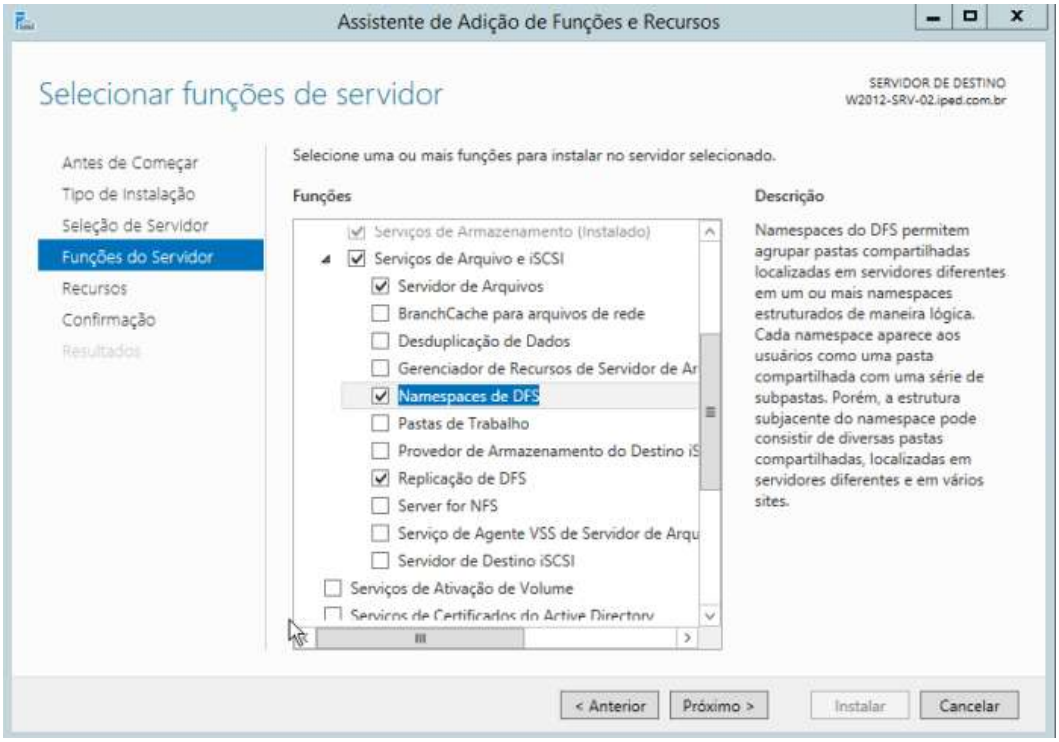
1. W2012-SRV-01 – Controlador de domínio
2. W2012-SRV-02 – Servidor standalone com Windows server 2012 instalado
3. W2012-SRV-03 – Servidor standalone com Windows server 2012 instalado

O computador W2012-SRV-02 e W2012-SRV-03 acabaram de ingressar no domínio, desta forma permitindo que as configurações de DFS que serão feitas em W2012-SRV-02 possam surtir efeitos sobre W2012-SRV-03, uma vez que as diretivas de segurança do domínio permitirão que as ações executadas em W2012-SRV-02 afete W2012-SRV-03.

Devido à replicação DFS, ambos os computadores terão o serviço DFS instalado, visando que o conteúdo que tenha no namespace, seja replicado para o outro, provendo tolerância à falha.

O processo de instalação do DFS é idêntico para W2012-SRV-02 e para W2012-SRV-03, portanto vamos apresentar as telas referentes ao W2012-SRV-02.

Para começar, clique em painel e, depois, em “adicionar funções e recursos”, avançando alguns passos, até chegar à tela ilustrada abaixo.



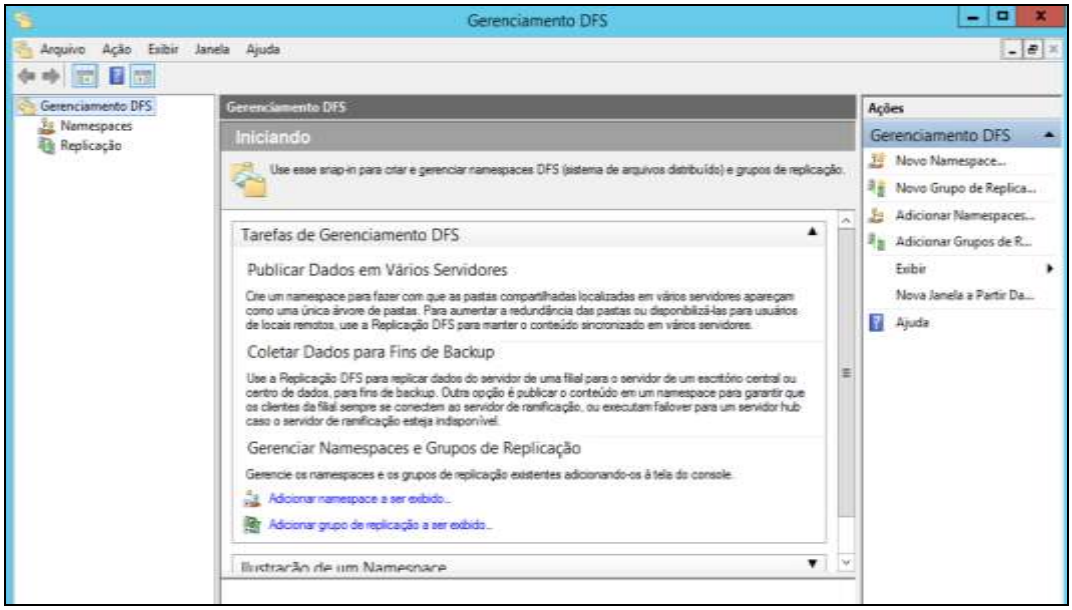
Marque as caixas acima confirmando, na janela de pendências, a adição de recursos necessários ao funcionamento do DFS. Assim que marcadas as caixas, avance pelo processo de instalação, até que seja concluído. Faça a mesma coisa no servidor W2012-SRV-03.

Após a instalação, ambos os servidores terão disponível a opção “gerenciamento DFS”, no menu ferramentas da janela gerenciador de servidor.

Observação: Lembre-se de que todo o processo de instalação deve ser feito com o uso de uma conta de administração.

Com o processo de instalação concluído vamos executar em W2012-SRV-02 o processo de configuração DFS. Para isto clique no menu ferramentas e clique em “gerenciamento DFS”.

A seguinte janela aparecerá:

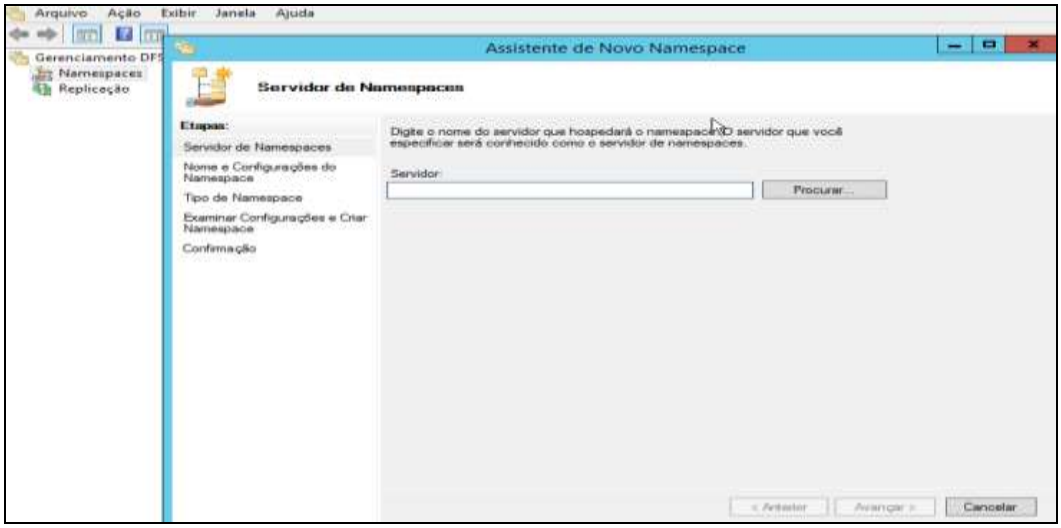


A ilustração mostra as opções “namespaces” e “replicação”.

A primeira é a opção onde agregamos os compartilhamentos espalhados pela rede sob um único namespace, nome dado o “caminho” utilizado pelo usuário para acessar todos os compartilhamentos de uma única vez.

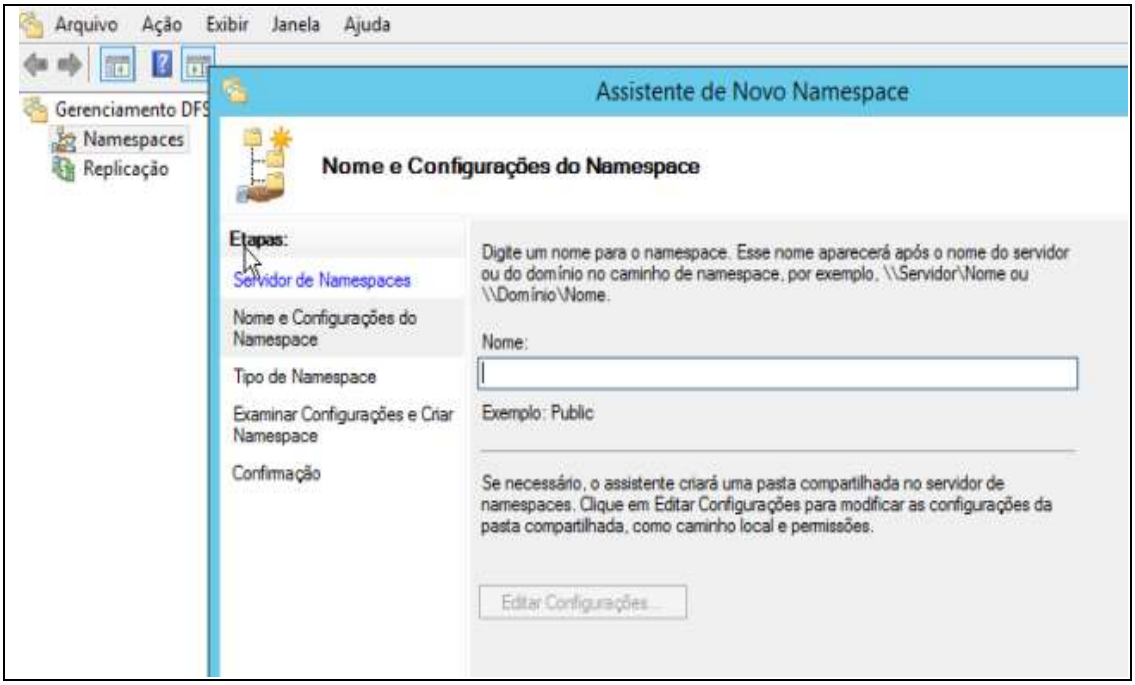
A segunda opção é onde iremos configurar a replicação, que funcionará replicando os dados entre os servidores de DFS, garantindo que o serviço permaneça ativo mesmo se um dos servidores se tornar indisponível.

Para continuar o processo, clique com o botão direito do mouse sobre “namespace” e clique em “novo namespace”, a janel abaixo será exibida.



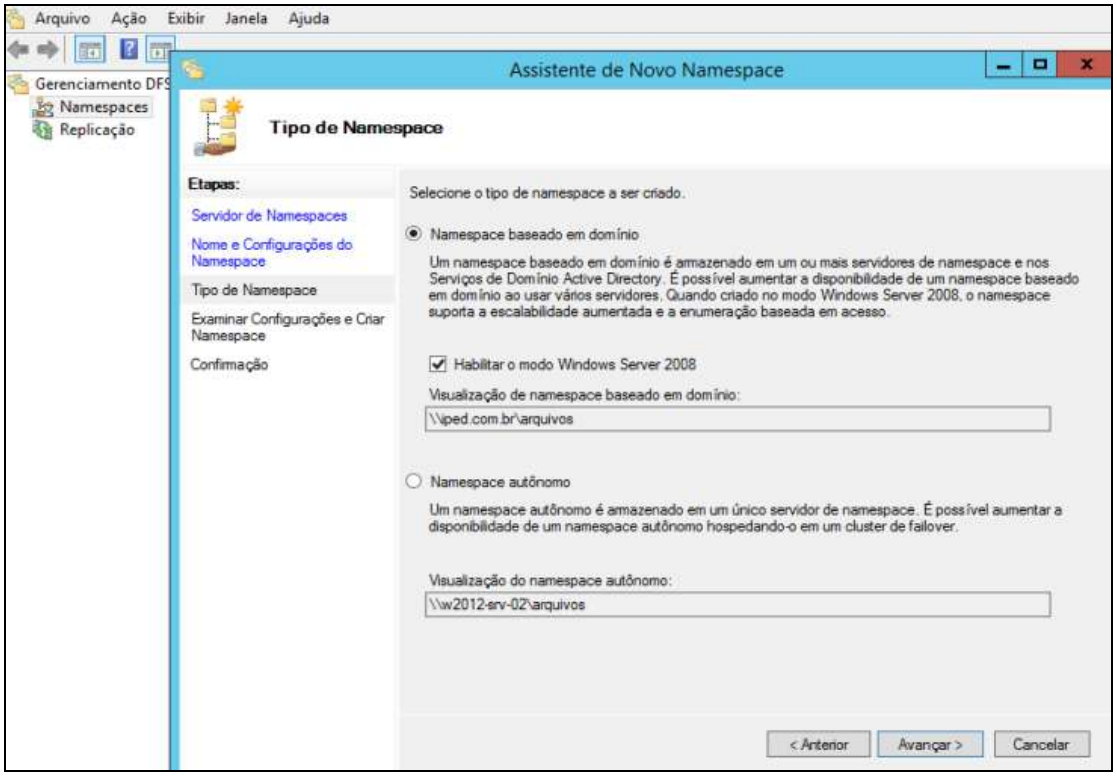
No campo “servidor”, clique em “procurar” e localize o computador que será o servidor de namespace conhecido do domínio, no nosso caso: W2012-SRV-02, e clique em avançar. Vale lembrar que o servidor de namespace, também poderia ser o w2012-srv-03, caso assim quiséssemos, ou qualquer outro computador.

Nesta etapa, vamos configurar o nome da pasta principal.



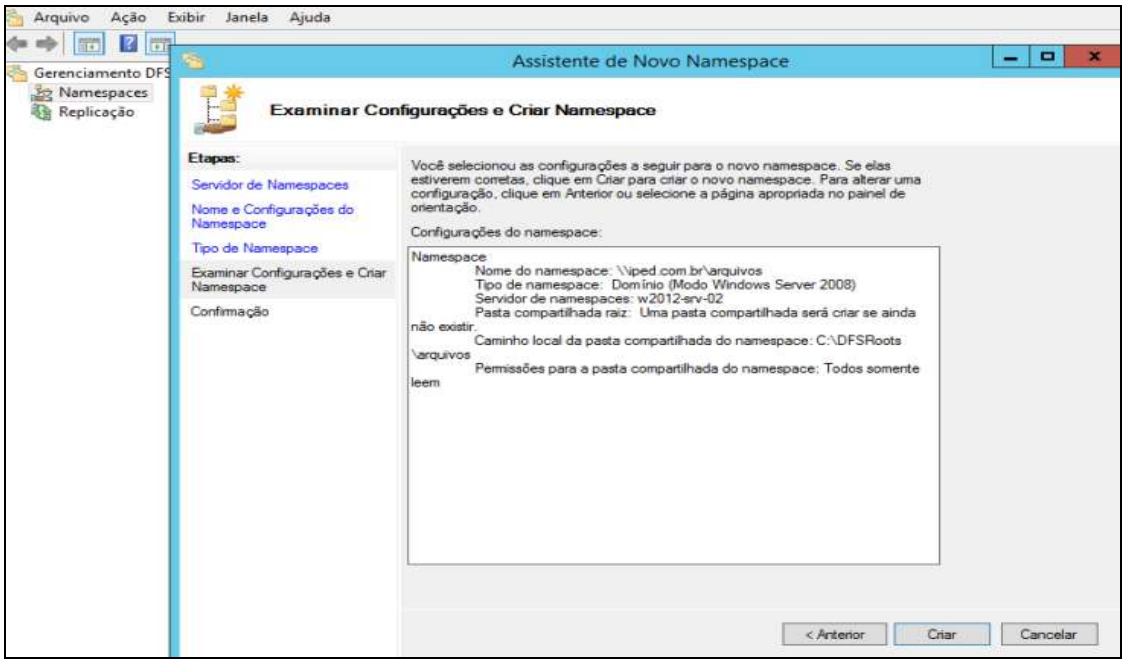
Na janela acima, digite o nome da “pasta alvo”, que será chamada de “arquivos”, neste laboratório.

Agora é chegada a hora de definir se o serviço DFS será baseado em domínio ou será um DFS autônomo. Vale lembrar que, em nosso caso, é mais aconselhável utilizar DFS baseado em domínio, para usufruir de um suporte maior à quantidade de pastas compartilhadas e diretivas de segurança, já que temos as máquinas ingressadas em um domínio Microsoft.

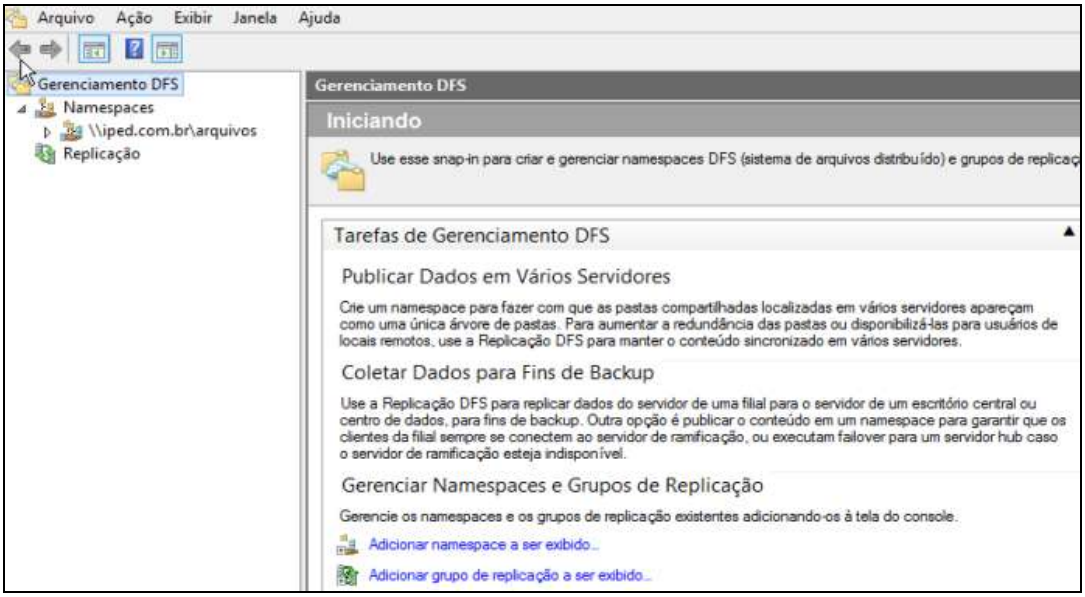


Nesta etapa deixe a opção “namespace baseado em domínio” selecionada e avance ao próximo passo.

Nesta fase verifique o resumo das configurações definidas durante o processo inicial de configuração, e clique em “criar”. Assim que concluído, uma janela informando sobre o êxito da configuração será exibida, bastando clicar em “fecha” para finalizar a etapa inicial de configuração.



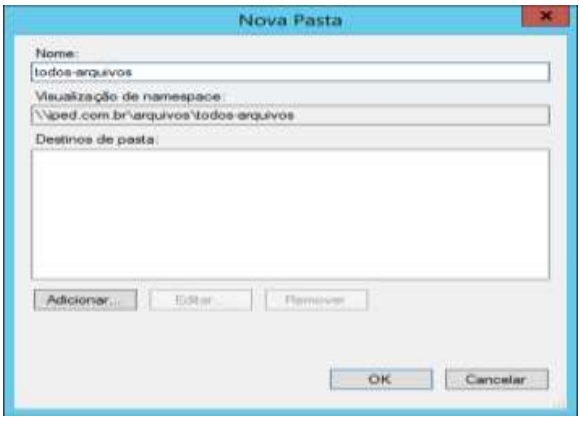
Apesar de finalizada a configuração de funcionamento, agora é necessário iniciar a configuração do namespace e informar quais as pastas compartilhadas ao longo da rede que serão agrupadas sobre um único namespace.



Na parte superior esquerda da janela, note a existência do namespace //iped.com.br/arquivos, sendo o caminho que os usuários deverão acessar para ter acesso aos diversos compartilhamentos espalhados ao longo da rede em diversos computadores diferentes.

Agora vamos à configuração do grupamento de pastas distribuídas através da rede.

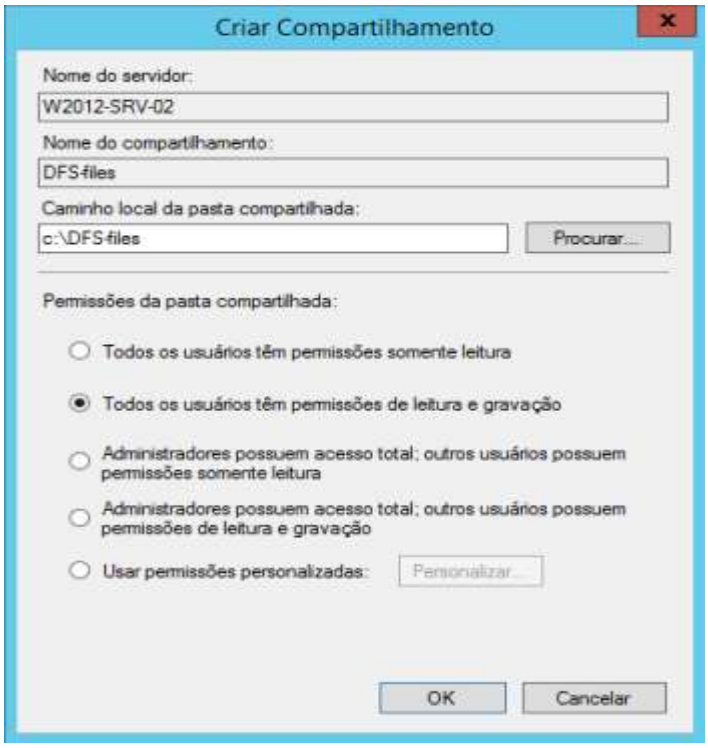
Neste nosso cenário, iremos criar duas pastas compartilhadas na rede, na unidade (c:) de W2012-SRV-02 e W2012-SRV-03, ambas com o nome “DFS-files” para padronizar.



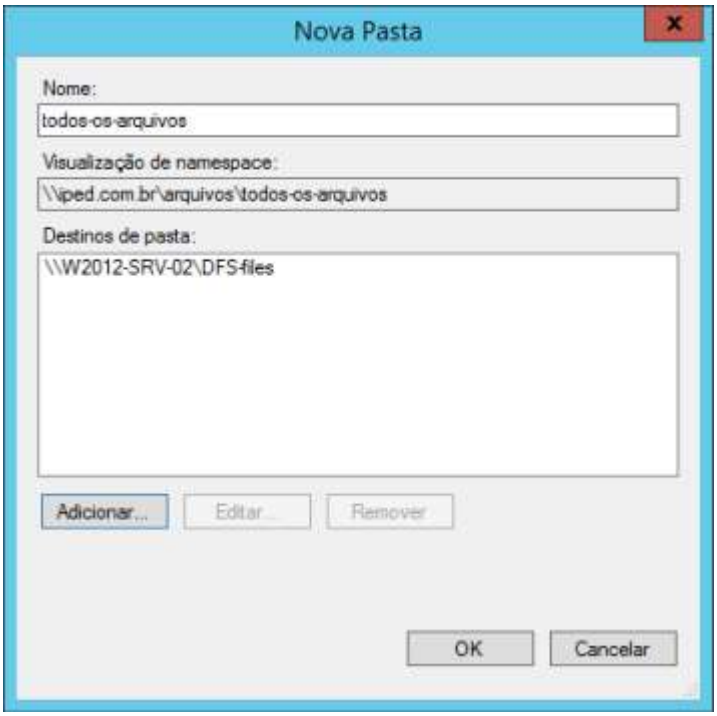
Para iniciar o processo das pastas compartilhadas “DFS-files”, faça o seguinte:

1. Clique com o botão direito sobre o namespace\\iped.com.br\arquivos
2. Clique em “nova pasta”
3. No campo “nome” coloque o nome “todos-arquivos” (A janela acima aparecerá.)
4. Clique no botão “adicionar” (a janela abaixo aparecerá)
5. No campo “caminho para a pasta de destino”, digite \\W2012-SRV-02\DFS-files

6. Na janela que aparecer, confirme a criação da pasta (a janela abaixo aparecerá)



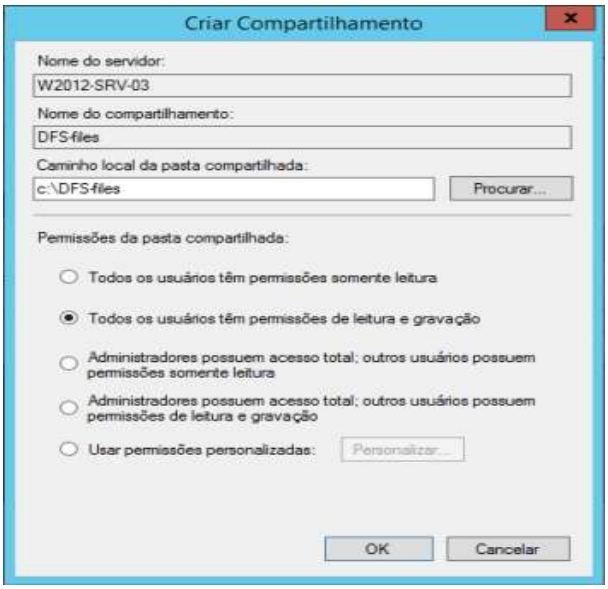
7. Nela preencha o campo “caminho local da pasta compartilhada”
8. Em “permissões da pasta compartilhada, marque “todos os usuários de permissão de leitura e gravação”
9. Dê OK
10. Na janela que aparecer, confirme a criação da pasta. (a janela abaixo aparecerá)



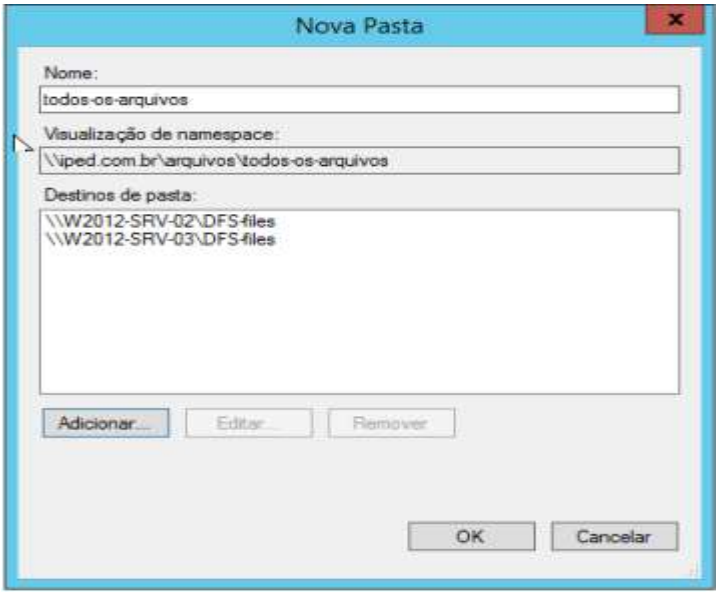
Neste passo, o compartilhamento já está criado em W2012-SRV-02, agora vamos executar o mesmo passo para W2012-SRV-03.

1. Clique no botão “adicionar” (a janela abaixo aparecerá)
2. No campo “caminho para a pasta de destino”, digite \\W2012-SRV-03\DFS-files\documentos
3. De “OK”

4. Na janela que aparecer, confirme a criação da pasta (a janela abaixo aparecerá)



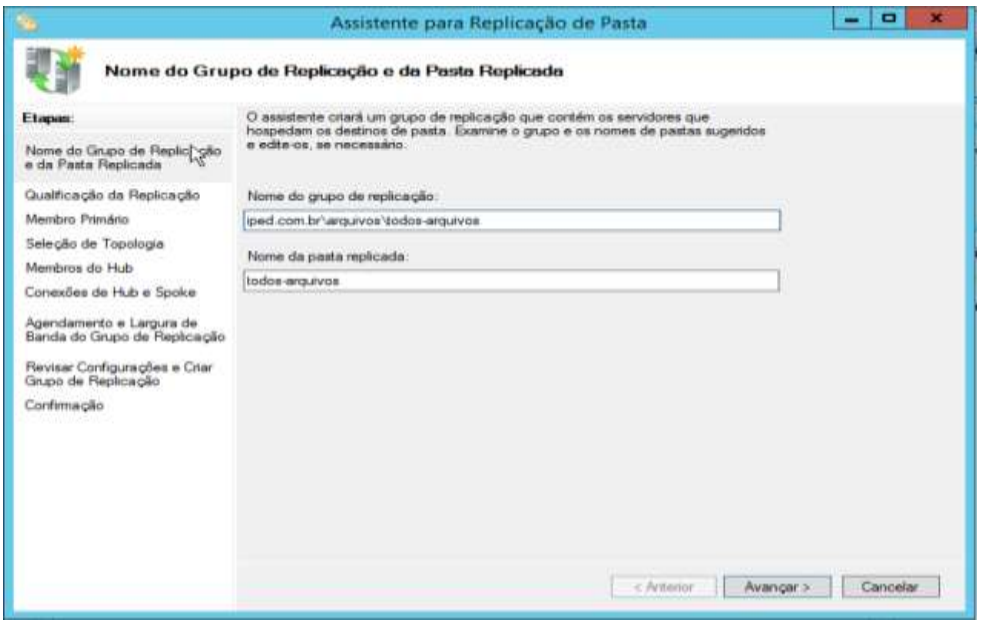
1. Nela preencha o campo “caminho local da pasta compartilhada”
2. Em “permissões da pasta compartilhada, marque “todos os usuários de permissão de leitura e gravação”
3. Dê OK
4. Na janela que aparecer, confirme a criação da pasta. (a janela abaixo aparecerá)



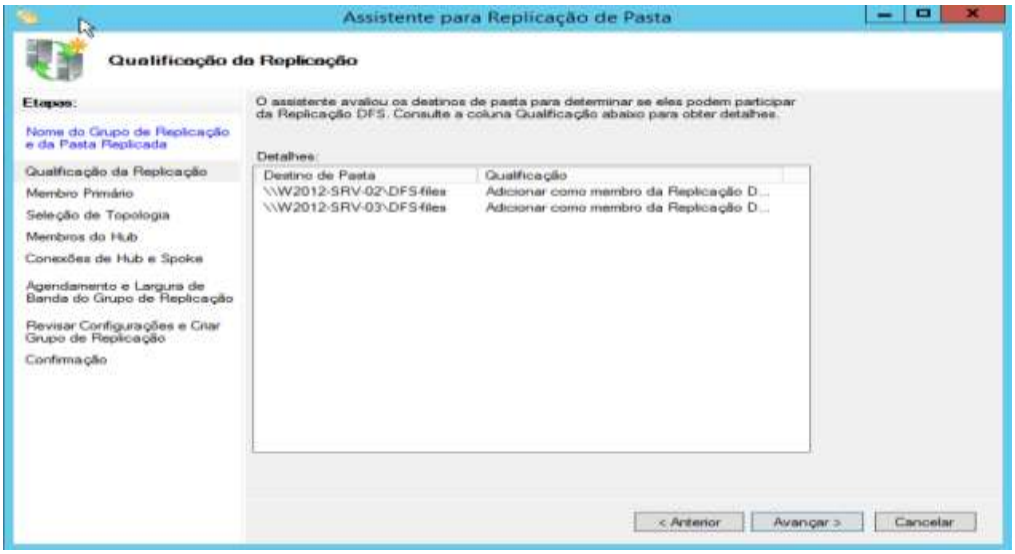
5. Clique em “OK”
6. A janela do assistente de replicação aparecerá, clique em “SIM”

Agora vamos iniciar o processo de replicação, que irá “espelhar” os diferentes conteúdos existentes nos compartilhamentos através dos servidores de DFS, garantindo a disponibilidade do serviço, caso algum dos servidores venha a falhar. Vamos iniciar o processo de criação da replicação...

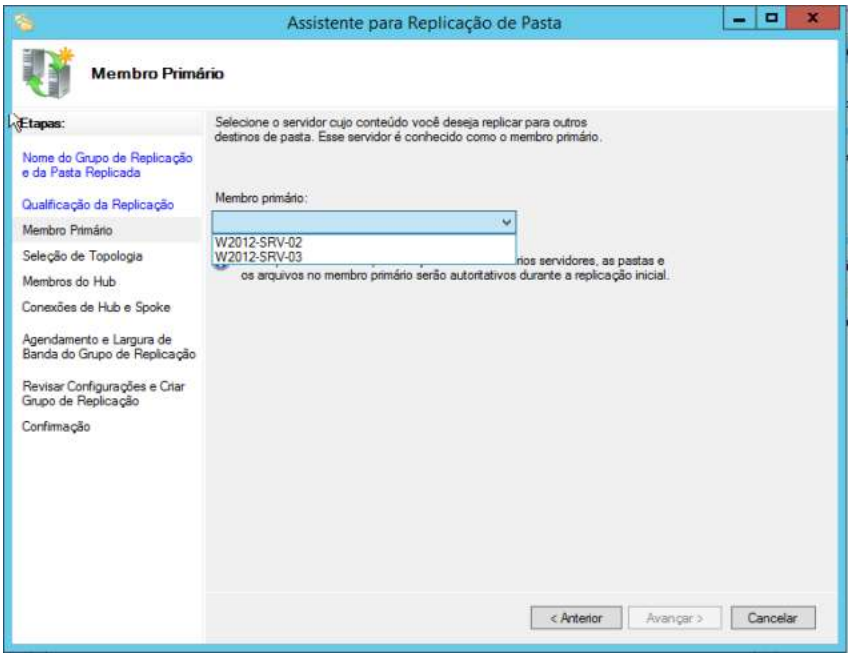
Assim que o processo de conexão entre os servidores DFS iniciar, a seguinte janela aparecerá:



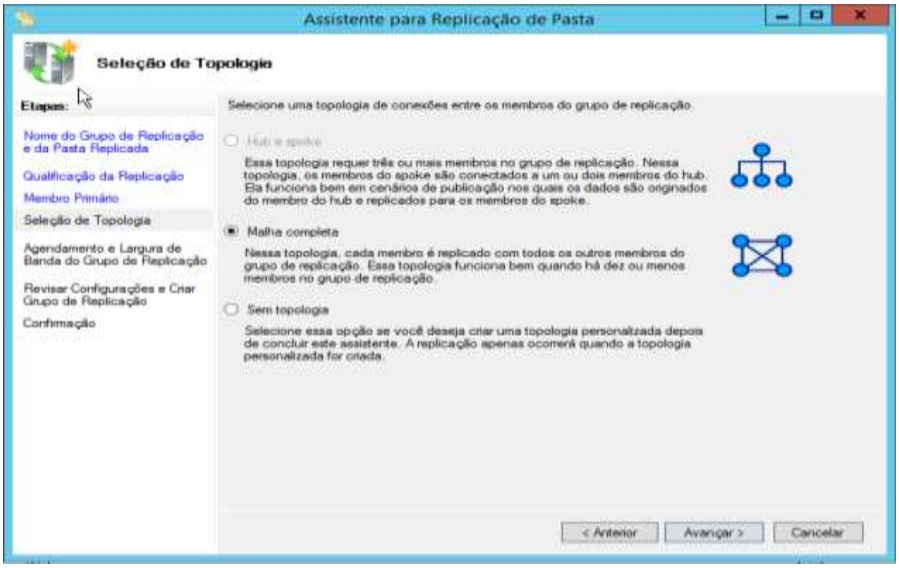
Observe que o sistema DFS já identificou o namespace criado anteriormente e já indica qual é o caminho que será replicado entre os servidores DFS. Nesta janela, clique em “avançar”.



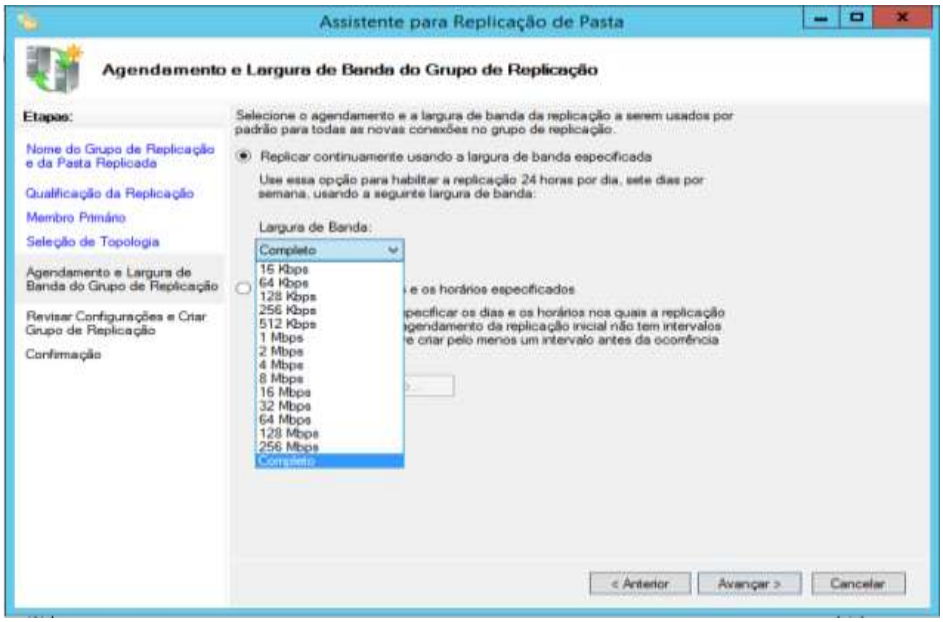
A janela acima apresenta as pastas compartilhadas que foram indicadas durante o processo de criação do namespace, caso existissem outras pastas, mesmo que em outros computadores, estariam aparecendo aí. No entanto, observe que apenas duas pastas compartilhadas, em dois computadores diferentes, fazem parte de nosso cenário de DFS.



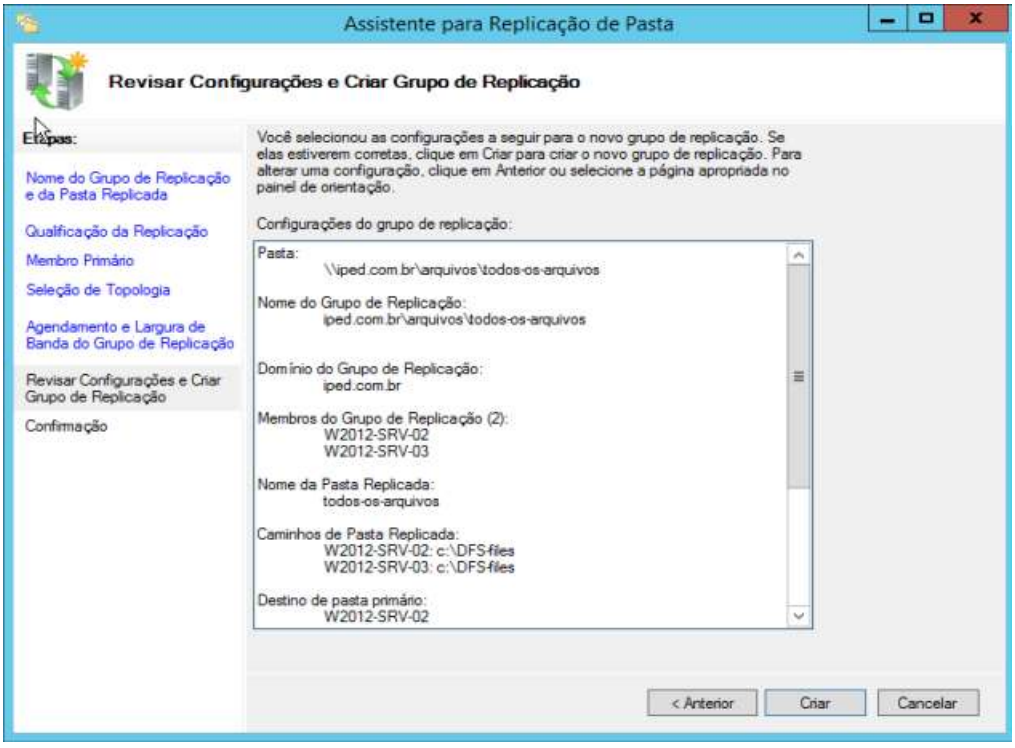
A janela acima é a etapa onde devemos escolher o servidor primário do DFS, cuja finalidade é apenas controlar as réplicas de conteúdo das pastas entre os demais servidores DFS. Nós iremos escolher W2012-SRV-02, mas poderíamos ter escolhido qualquer outro servidor da lista.



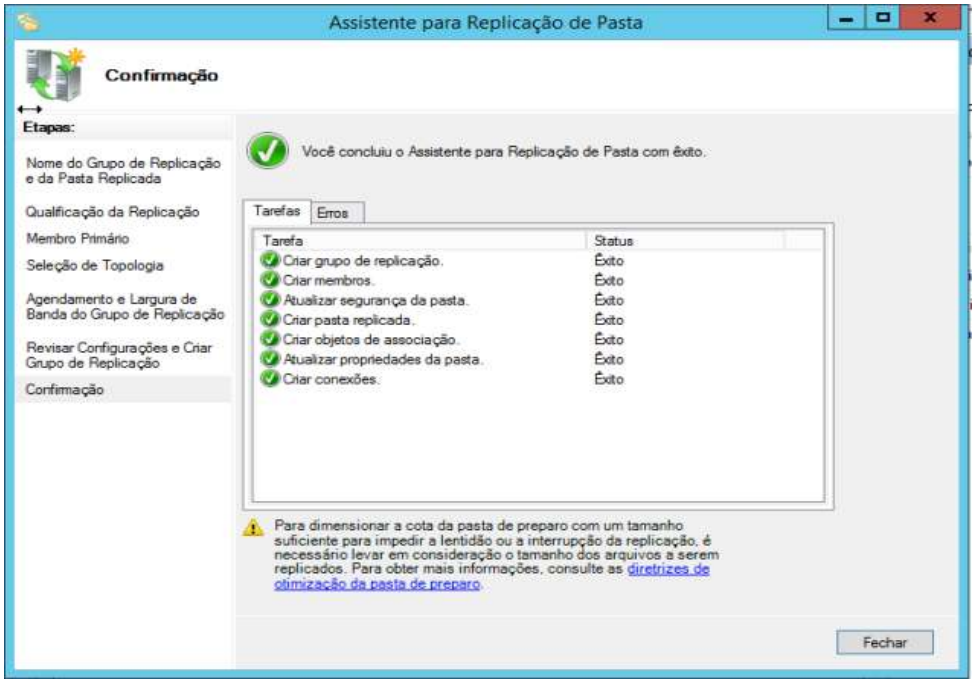
Na janela acima, defina a topologia “malha completa” e clique em avançar.



Neste passo, defina o uso de banda que será utilizado para replicação entre os servidores de acordo com a largura que você terá disponível em sua infraestrutura. Como o nosso cenário roda em uma rede local, podemos escolher a opção “completo”. Feito a escolha de uso de banda, clique em “avançar”.



Acima a tela-resumo das configurações feitas, caso haja alguma divergência entre seu projeto e o que está sendo exibido, clique em “anterior” e faça a modificação necessária, caso esteja de acordo com o planejado, clique em criar.



Acima a janela informa êxito na criação do ambiente de replicação. A partir de agora as pastas envolvidas serão replicadas entre os servidores.

Acima a opção “replicação” expandida, onde é possível confirmar as pastas que estão envolvidas na replicação.

Encerramento

Chegamos ao final de nosso curso e acreditamos ter conseguido transmitir os conhecimentos necessários para a instalação e funcionalidade do windows server 2012. Assim como, a interface de gerenciamento centralizada de servidores que é uma das inovações desse sistema.

Contudo, esperamos que esses conhecimentos transmitidos no decorrer do curso o ajudem a se tornar um profissional cada vez mais eficiente.

Boa sorte e sucesso!