GUIA PRÁTICO DE REDES WINDOWS

PARA NOVOS ADMINISTRADORES DE REDE

Professor: Márcio L. M. Nogueira
Versão 2.0

Índice

1 Objetivos 3

2 Competências 3

3 Habilidades 3

4 Bases Tecnológicas 3

5 Ementa da Disciplina 3

6 Carga Horária 3

7 Competência 1 – Sistemas Operacionais Servidores 4
7.1 Famililia de sistemas operacionais servidores 4
7.2 Requisitos de Hardware e Software 7
7.3 Arquitetura de Sistemas Operacionais Servidores 9
7.4 Tipos de Instalações 17
7.5 Sistemas de Arquivos 28
7.6 Principais Serviços Suportados 53

8 Competência 2 – Manipulação de SOS de Redes 69
8.1 Serviços Básicos de Rede 71
8.2 Ferramentas de Segurança 110
8.3 Ferramentas de Backup 126
8.4 Serviços Avançados de Rede 142

9 Competência 3 – Sistemas Operacionais Clientes 175
9.1 Família de Sistemas Operacionais Clientes 175
9.2 Requisitos de Hardware e Software 181
9.3 Principais Ferramentas 182

10 Competência 4 – Integração SOC e SOS 198
10.1 Configuração dos Serviços de Acesso a Rede 198
Quando usar grupos com escopo de domínio local 209
Quando usar grupos com escopo global 209
Quando usar grupos com escopo universal 210
10.2 Atualização do Sistema Operacional 223

Guia Prático de Redes para Novos Administradores de Rede

1 OBJETIVOS

Tornar o futuro profissional a operar os recursos de uma estação de trabalho (cliente e servidor) através de um sistema operacional proprietário multiusuário baseado na plataforma MS-Windows.

2 COMPETÊNCIAS

C1 Selecionar o sistema operacional servidor proprietário de acordo com as necessidades do usuário.

C2 Analisar os serviços e funções de sistemas operacionais servidor proprietários, utilizando seus recursos em atividades de configuração, manipulação de arquivos, segurança e outras.

C3 Conhecer a instalação, configuração e funcionamento dos sistemas operacionais de rede cliente de arquitetura proprietária.

C4 Conhecer técnicas e ferramentas de conectividade entre sistemas operacionais proprietários.

3 HABILIDADES

H1 Instalar e configurar o Sistema Operacional Servidor definindo seus padrões de funcionamento.

H2 Associar os diversos recursos de uma rede proprietária de acordo com as necessidades da organização.

H3 Orientar o usuário na escolha do sistema operacional proprietário cliente que melhor se adeqüe as suas necessidades.

H4 Promover os padrões de serviços de redes corporativas.

4 BASES TECNOLÓGICAS

B1 Arquitetura geral de computadores.

B2 Funções do sistema operacional.

B3 Instalação e configuração de serviços do sistema operacional.

B4 Gerenciamento de memória, arquivos e impressão

B5 Compartilhamento de recursos em rede.

B6 Gerenciamento de contas de usuários.

5 PROPOSTA DE EMENTA PARA DISCIPLINA

Família de um sistema operacional; considerações a serem analisadas na instalação de um sistema operacional (compatibilidade de hardware e software); arquitetura de um sistema operacional servidor; arquitetura de rede de um sistema operacional servidor, requisitos mínimos; tipos de instalações; sistema de arquivos; principais serviços suportados pelo sistema operacional; serviços de rede disponibilizados; ferramentas para administração; ferramentas de segurança; ferramentas para backup; ativando o servidor web e ftp; recursos avançados de um sistema operacional servidor (servidores dial-up, servidor VPN, diretivas de acesso remoto e etc); recursos de impressão; manutenção de usuários e grupos de usuários; gerenciamento do computador; update do sistema operacional.

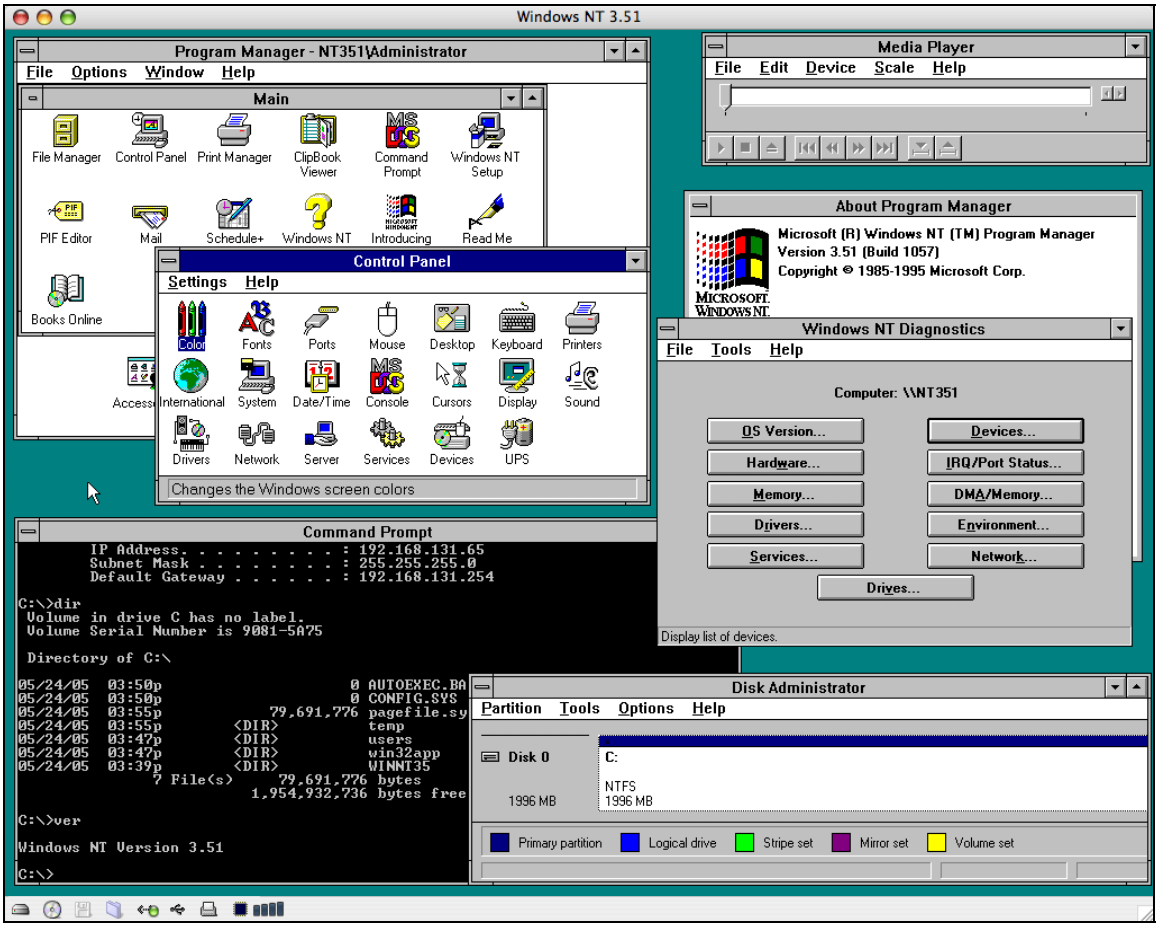
6 CARGA HORÁRIA PROPOSTA

Esta obra possui **120 horas** aula, e sendo recomendada para práticas em laboratório.

7 COMPETÊNCIA 1 – SISTEMAS OPERACIONAIS SERVIDORES

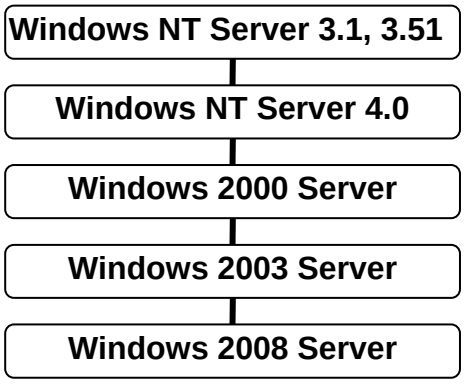
7.1 FAMILÍLIA DE SISTEMAS OPERACIONAIS SERVIDORES

A Microsoft inicia a concorrência sobre o mercado de sistemas operacional servidores em 1994, com o Windows NT Server 3.1, seguido do 3.51. Até então, este mercado era dominado massivamente pelo Unix e parte pelo Novell.

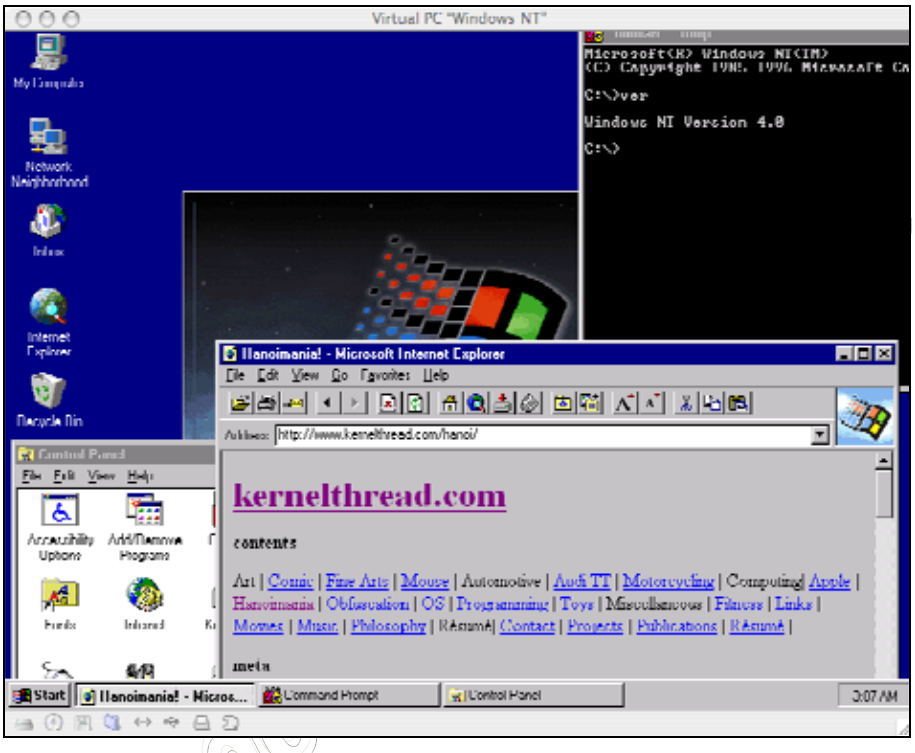


O NT Server, de New Tecnology, inicialmente não possuía os mesmos recursos de desempenho e segurança de seus rivais. Porém o NT veio para concorrer em um mercado ainda pouco explorado (e que poucos acreditavam que teria futuro): o mercado de servidores baseados em processadores padrão Intel (x386).

Porém a realidade é que o NT Server teve uma boa aceitação. Entre seus diferenciais estavam o uso do sistema de arquivo NTFS com compactação, o WinLogin para múltiplos usuários, suporte 3D ao OpenGL, uso de rotas IP persistentes para o TCP/IP, e o “tooltips” (dicas em forma de balão ao pousar o mouse sobre ícones). O sucesso foi enorme que versões melhoradas surgiram ao longo dos anos:

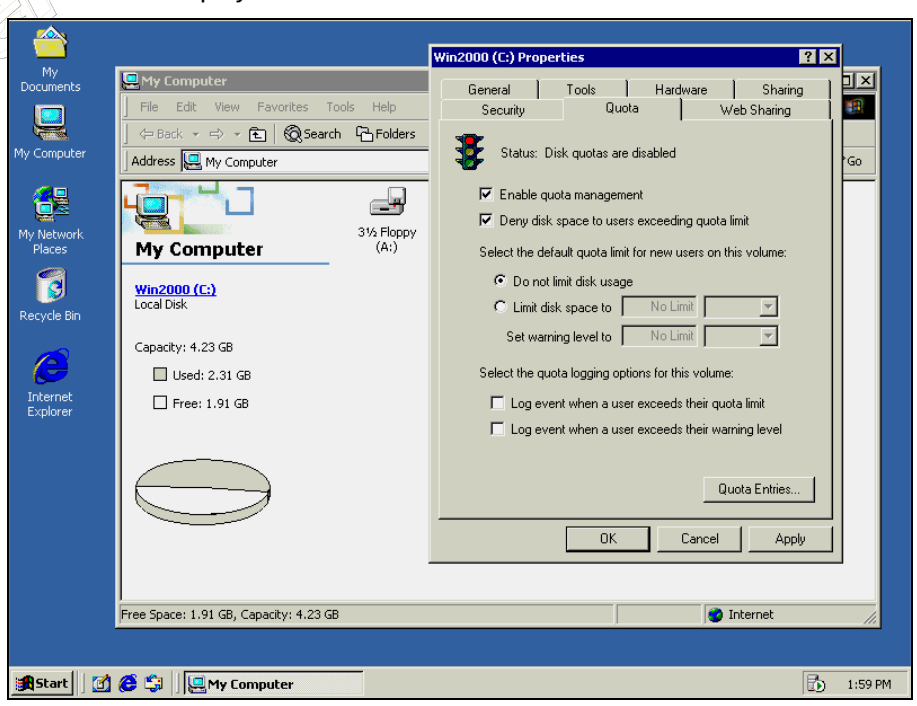


Em 1996 a Microsoft lança o Windows NT Server 4.0, uma versão consideravelmente melhorada do Windows NT 3.51, em termos de suporte a hardware, desempenho e segurança. Com interface similar ao do Windows 95, muitos acreditavam ser o NT 4.0 uma promessa antiga da Microsoft em unificar as linhas de produtos servidores e clientes, mas não foi bem isso o que aconteceu.



O NT Server 4.0 apresentou-se bem ao mercado empresarial, porém ainda possuía sérias limitações para uso residencial, principalmente em questões de jogos e periféricos.

Em 2000 a Microsoft lança o Windows Server 2000, uma verdadeira revolução nos sistemas operacionais de rede. Com a introdução do Active Directory (Serviço de Diretório) entre outros serviços inovadores. A Microsoft deixaria de ser um mero ator do mercado empresarial para ser o principal e mais distanciado player de todos.



Alguns dos motivos que conduziram a revolução do Windows Server 2000 ao sucesso absoluto foram: a existência de profissionais capacitados, farta literatura, fontes de referência na Internet, estabilidade comprovada e segurança. Pontos esses considerados hoje a receita de bolo para o sucesso de qualquer sistema operacional servidor.

Em 2003 é lançado o Windows Server 2003, versão melhorada do 2000 em relação a desempenho e segurança. Um dos pontos fortes do 2003 é sua mudança de paradigma em relação a segurança. Até seu antecessor o Windows Server 2000 a ideologia dos serviços de redes era facilitar ao máximo para o administrador de redes, com o Server 2003 a ideologia passa a ser a mesma praticada pelo principal concorrente, o Unix/Linux, que seja a de proteger ao máximo ao invés de facilitar. A partir de agora, para manusear o Windows Server 2003, os administradores precisariam de noções básicas e intermediárias tanto dos serviços quanto do uso do próprio sistema.

Iniciaremos a disciplina apresentando o papel do Microsoft Windows Server 2003, como sistema operacional de servidores em uma rede.

O Windows Server 2003 apresenta uma coleção completa de serviços para compor a infra-estrutura de rede, baseada no modelo Cliente/Servidor. A arquitetura cliente/servidor de redes é um conjunto de dispositivos, normalmente computadores, onde um número reduzido de equipamentos atua como Servidor – Disponibilizando recursos e serviços para os demais – e a maioria dos dispositivos atua como cliente, acessando os recursos e serviços disponibilizados pelos Servidores.

Aqui é importante não confundir o conceito de redes Cliente/Servidor com os modelos de desenvolvimento de softwares 2 camadas, ou Cliente/Servidor, lembrando que em programação também existe o modelo 3 camadas, ou Web. Apesar dos conceitos do modelo Cliente/Servidor serem diferentes nas áreas de redes e desenvolvimento, porém apresentam uma relação muito próxima. Para relembrar esses conceitos consulte o livro ASP.NET: Uma Nova Revolução na Criação de Sites e Aplicações Web.

Em uma rede de computadores temos, basicamente, dois tipos de equipamentos conectados (além dos ativos e passivos responsáveis pela conectividade, como: hubs, switchs, roteadores, etc):

- Estações de trabalho
- Servidores

Como o próprio nome sugere, um Servidor fornece serviço para vários clientes. Por exemplo, podemos ter um servidor de arquivos onde ficam gravados arquivos, os quais podem ser acessados através da rede, por todas as estações da rede (estações de trabalho), as quais são conhecidas como Clientes. Outro tipo bastante comum de serviço é uma impressora compartilhada no servidor, para a quais diversos clientes podem enviar impressões. Poderíamos citar uma série de serviços que podem ser oferecidos por um servidor com o Windows Server 2003 instalado.

Um exemplo típico é o acesso à Internet: quando você acessa o site da Microsoft na Internet: http://www.microsoft.com. As informações disponibilizadas no site, ficam gravadas nos servidores da Microsoft, enquanto que o seu computador que está acessando estes recursos (informações), está atuando como um cliente. Neste caso o tipo de serviço que está sendo disponibilizado são informações em um servidor Web, também conhecido como Servidor HTTP (que é o protocolo mais utilizado para o transporte de informações na Internet). O Navegador que você utiliza para acessar estas informações está atuando como Cliente.

Sob este ponto de vista, podemos afirmar que a Internet é na verdade uma gigantesca rede Cliente-Servidor, de alcance mundial, com alguns milhões de servidores e com centenas de milhões de clientes acessando os mais variados recursos e serviços disponibilizados pelos servidores.

A forma como toda a comunicação é estabelecida, entre os diversos países, computadores e softwares, são dados através dos protocolos. Protocolos são softwares comuns a todos, utilizados para gerenciar a comunicação. Exemplos de protocolos são o TCP/IP, para as redes, o SMTP, para envio de mensagens, o DNS, para resolução de nomes.

7.2 REQUISITOS DE HARDWARE E SOFTWARE

É importante saber que o Microsoft Windows Server 2003 é disponibilizado em diferentes edições, para atender determinadas condições de recursos e limites de hardwares, são elas:

- Windows Server 2003 Web Edition
- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Data Center Edition

O que diferencia uma edição de outra são as funcionalidades disponíveis em cada edição, as necessidades mínimas de Hardware e os limites máximos de Hardware suportados, tais como quantidade máxima de memória RAM, números de processadores, número máximo de servidores em Cluster e assim por diante.

O Windows Server 2003 Web Edition é uma edição especificamente projetada para servidores que prestarão serviços de hospedagem de sites, de aplicações Web e aplicações baseadas na plataforma .NET, utilizando tecnologias como ASP.NET, XML e Web Services. Recursos como Active Directory e Terminal Server não estão disponíveis nessa versão específica, além de apresentar os seguintes limites de Hardware:

- Suporta, no máximo, dois processadores;
- Suporta, no máximo, 2Gb de RAM.

Já, o Windows Server 2003 Standard Edition é indicado para ser utilizado em servidores de pequenas e médias organizações ou servidores departamentais, com um número médio de usuários entre 10 e 100. Normalmente utilizado para serviços como compartilhamento de arquivos e impressoras, gerenciamento centralizado das estações de trabalho, servidores de Intranet e servidor de conectividade com a Internet. Recurso de Cluster não está presente, e apresenta as seguintes limitações quanto ao hardware:

- Até quatro processadores;
- Máximo de 4 Gb de memória RAM;
- Não suporta a versão de 64 bits para processadores Intel Itanium;
- Não suporta a troca de memória sem desligar o servidor;
- Não suporta o serviço de Metadiretório;
- Não suporta o WSRM – Windows System Resource Manager, recursos que permite a alocação de recursos de hardware para processos específicos.

O Windows Server 2003 Enterprise Edition é uma edição mais robusta, com mais recursos do que a Standard Edition, e de preço consideravelmente mais caro também. É recomendada para redes de porte médio tendendo para grande (um pouco acima de 100 usuários), a fim de realizar serviços, como: roteamento, servidor de Banco de Dados (MS SQL, Oracle), correio eletrônico e aplicativos de colaboração (Microsoft Exchange, Lotus Notes), sites de comércio eletrônico e outros aplicativos utilizados em redes de grande porte. Apresenta as seguintes limitações quanto ao hardware:

- Máximo de oito processadores na versão de 32 bits;
- Máximo de 32 Gb de memória RAM na versão de 32 bits;
- Cluster com até oito servidores;

Windows Server 2003 Data Center Edition, a versão mais robusta do Server 2003. Apresenta o maior número de recursos e maior capacidade para atender aplicações com um grande número de usuários e com elevadas exigências de desempenho. Indicado para as chamadas aplicações de missão-crítica, ou seja, aquelas aplicações que não podem falhar em hipótese alguma, como: bolsa de valores, comércio eletrônico, banco, ERP, etc. Apresenta as seguintes limitação de hardware:

- 32 processadores na versão de 32 bits e até 64 processadores na versão de 64 bits, para servidores baseados no processador Intel Itanium;

- 64 Gb de memória RAM na versão de 32 bits e até 512 Gb de RAM na versão de 64 bits, para servidores baseados no processador Intel Itanium;
- Cluster com até oito servidores.

Um detalhe importante é que o Windows Server 2003 Data Center Edition não pode ser adquirido simplesmente comprando licenças desta edição, o que é possível com todas as demais edições. O Windows Server 2003 Data Center Edition somente está disponível através do programa conhecido como "Windows Datacenter High Availability Program". Para maiores detalhes sobre este programa, consulte o endereço: http://www.microsoft.com/windowsserver2003/datacenter/dcprogram.mspx.

O objetivo do Windows Datacenter High Availability Program é fazer com que os fabricantes de hardware, que queiram comercializar servidores com o Windows Server 2003 Data Center Edition, passem por uma série de testes. O objetivo destes testes é garantir que o equipamento esteja de acordo com as especificações da Microsoft, que seja completamente compatível com o Windows Server 2003 Data Center Edition e que atenda aos requisitos de desempenho e de gerenciabilidade definidos no programa. Somente os fabricantes que passarem nos testes do Windows Datacenter High Availability Program, terão permissão da Microsoft para comercializar servidores com o Windows Server 2003 Data Center Edition instalado.

No site da Microsoft http://www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx encontramos algumas comparações interessantes sobre as quatro edições comentadas:

Recurso	Web	Standard	Enterprise	Data Center
CPU mínima	133 MHZ	133 MHZ	133 MHZ p/x86 733 MHZ p/Intel Itanium	400 MHZ p/X86 733 MHZ p/Intel Itanium
CPU Recomendada	550 MHZ	550 MHZ	733 MHZ	733MHZ
RAM Mínima	128 MB	128 MB	128 MB	512 MB
RAM Recomendada	256 MB	256 MB	256 MB	1024 MB
Espaço em Disco p/instalar	1,5 GB	1,5 GB	2,0 GB	2,0 GB

Estes são valores definidos na documentação oficial do produto, mas que não espelham a realidade de um servidor em produção, atendendo a um grande número de usuários. Os recursos necessários de hardware são determinados por uma série de fatores, tais como o número de aplicações que irá rodar no servidor, o número de usuários simultâneos, o desempenho esperado, etc.

No site da HP: http://www27.compaq.com/SB/MSVS/UI/index.aspx é possível achar uma ferramenta que ajuda a dimensionar o hardware para servidores, mas como regra geral o ideal é manter sempre uma folga nos recursos, como:

- O processador acima de 75% em uso é sinônimo de possíveis lentidões;
- O processador com temperatura acima de 70° graus é sinônimo de travamentos;
- O HD acima de 90% em uso é sinônimo de lentidão e desfragmentação;
- O HD com temperatura acima de 60° graus é sinônimo de desgaste garantido;
- A RAM acima de 90% em uso é sinônimo de lentidões;
- A Memória Virtual ou Paginada acima de 512Mb é sinônimo de RAM esgotada;
- A placa mãe ou o interior do gabinete não pode ultrapassar os 40° graus.

Para saber a temperatura máxima que seu processador pode suportar, consulte o site do Clube do Hardware: http://www.clubedohardware.com.br/artigos/645/1

Ainda no site da Microsoft é possível encontrar as funcionalidades de cada edição divididas por categorias, como: tecnologias de cluster, serviços de diretório, serviços de arquivo e impressão.

Legenda: ●=Suportado ◒=Parcialmente Suportado ○=Não Suportado

Recurso	Servidores Web	Standard Server	Enterprise Server	Datacenter Server
Tecnologias de cluster				
Balanceamento de carga da rede	●	●	●	●
Cluster de falhas	○	○	●	●
Comunicações e serviços de rede				
Conexões de rede virtual privada (VPN)	◒	●	●	●
Serviço de protocolo de início de sessão (SIP)	○	●	●	●
Serviço de autenticação da Internet (IAS)	○	●	●	●
Ponte de rede	○	●	●	○
Compartilhamento de conexão com a Internet (ICS)	○	●	●	○
Serviços de diretório				
Active Directory™	○	●	●	●
Suporte para serviços de metadiretório (MMS)	○	○	●	●
Serviços de arquivo e impressão				
Sistema de arquivos distribuídos (DFS)	●	●	●	●
Sistema de arquivos com criptografia (EFS)	●	●	●	●
Restauração de cópia duplicada	○	●	●	●
SharePoint™ Team Services	○	●	●	●
Armazenamento removível e remoto	○	●	●	●
Serviço de fax	○	●	●	●
Serviços para Macintosh	○	○	●	●
Serviços de gerenciamento				
IntelliMirror	○	●	●	●
Conjunto de diretivas resultante (RSoP)	○	●	●	●
Windows Management Instrumentation (WMI)	○	●	●	●
Servidor de instalação remota (RIS)	○	●	●	●
Serviços de segurança				
Firewall de conexão com a Internet	○	●	●	○
Serviços de certificado	○	◒	●	●
Serviços de terminal				
Área de trabalho remota para administração	●	●	●	●

Agora que temos uma boa base sobre a evolução e as características da família Windows Server, vamos estudar a teoria sobre os sistemas operacionais de rede, começando pelas classificações dos sistemas operacionais, conhecendo um pouco da historia dos antigos sistemas centralizados, ou baseados em Mainframe, e por fim as arquiteturas dos sistemas operacionais.

7.3 ARQUITETURA DE SISTEMAS OPERACIONAIS SERVIDORES

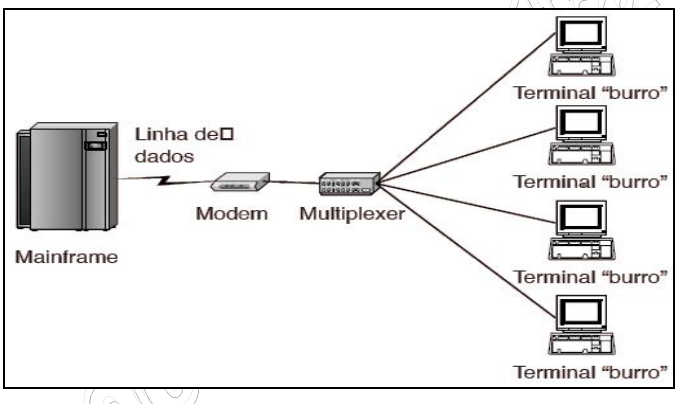
Os sistemas operacionais são classificados em:

- Sistemas Operacionais Centralizados
  - Sistema com um único computador;
  - Um usuário acessa recursos locais da própria máquina;
- Sistemas Operacionais de Rede
  - Vários sistemas distintos;
  - Recursos compartilhados entre usuários;
  - Usuários precisam saber onde estão os recursos;
- Sistemas Operacionais Distribuídos
  - Sistemas distintos, mas visão unificada;
  - Recursos estão acessíveis de forma transparente;

Os sistemas operacionais centralizados são aplicados a sistemas convencionais de recursos centralizados, arquiteturas mono ou multi-processadas, e multi-tarefas e multi-usuários. Como características principais apresentam o compartilhamento de recursos através de interrupções, todos os recursos são acessíveis internamente e a comunicação entre processos é realizada via memória compartilhada ou através de facilidades providas pelo núcleo do sistema. Apresentam como objetivos a virtualização de recursos do hardware, o gerenciamento e uso dos recursos locais e a sincronização de atividades. Como exemplo podemos citar os antigos Mainframes.

Há algumas décadas, quando a informática começou a ser utilizada para automatizar tarefas administrativas nas empresas, tínhamos um modelo baseado nos computadores de grande porte, os chamados Mainframes.

Durante a década de 70 e até a metade da década de 80, este foi o modelo dominante, sem nenhum concorrente para ameaçá-lo. Os programas e os dados ficavam armazenados nos computadores de grande porte. Para acessar estes computadores eram utilizadas os chamados terminais burros, conforme apresentado na imagem abaixo:



O Mainframe é um equipamento extremamente caro, equivale ao preço de algumas dezenas de servidores de médio porte. Normalmente o Mainframe é adquirido para hospedar tanto os sistemas quanto os dados de diversos seguimentos distintos. É possível hospedar e executar simultaneamente diferentes sistemas operacionais e aplicativos, sem que um interfira no desempenho ou performance dos demais. O Mainframe é um equipamento que precisa de instalações adequadas, nas quais exige controle de temperatura, unidade de ar e alimentação elétrica estabilizada e aterrada.

Um exemplo de uso do Mainframe é quando uma empresa X, dona do Mainframe, aloca espaço para uma terceira empresa Y. Neste cenários, o sistema operacional da empresa Y, bem como suas aplicações e dados, estão contidos no Mainframe de X. Para ter acesso a estes dados, a empresa Y contrata uma linha de dados. Na sede da empresa X, a linha de dados de Y é conectada a um Modem, o qual conecta com um equipamento chamado MUX. O papel do MUX é permitir que mais de um terminal burro possa se comunicar com o Mainframe, usando uma única linha de dados. Os terminais burros eram ligados ao equipamento MUX, diretamente através de cabos padrões para este tipo de ligação.

Com isso os terminais são, na pratica, uma extensão da console do Mainframe, o qual permite que vários terminais estejam conectados simultaneamente, inclusive acessando diferentes sistemas. Este modelo ainda é muito utilizado, embora novos elementos tenham sido introduzidos. Por exemplo, os terminais burros foram praticamente extintos. Agora o terminal é simplesmente um software emulador de terminal, que fica instalado em um computador PC ligado em rede. Mas muitos dos sistemas e dados empresariais, utilizados hoje em dia ainda estão hospedados em Mainframe. Pegue a lista dos dez maiores bancos brasileiros (públicos e privados) e, no mínimo, cinco deles, ainda tem grande parte dos dados no Mainframe.

O modelo baseado no Mainframe tem muitas vantagens, como:

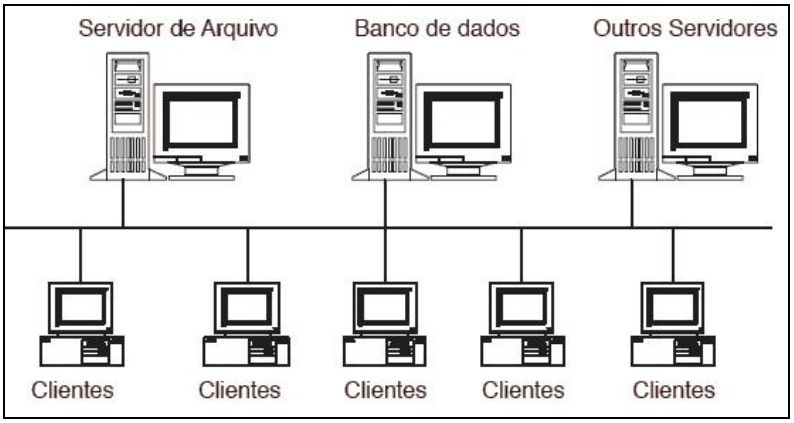
- Gerenciamento e Administração centralizada: Com os programas e os dados ficam instalados no mainframe, fica mais fácil fazer o gerenciamento deste ambiente. A partir de um único local o Administrador pode instalar novos sistemas, atualizar as versões dos sistemas já existentes, gerenciar o espaço utilizado em disco, gerenciar as operações de Backup/Restore, atualizações do sistema operacional e configurações de segurança;
- Ambiente mais seguro: Com o gerenciamento centralizado é mais fácil manter o ambiente seguro, uma vez que um número menor de pessoas tem acesso ao ambiente. A segurança física também fica mais fácil de ser mantida, pois exige um único local a ser protegido;
- Facilidade para atualizações dos sistemas: Como os sistemas são instalados em um único local, centralizada no Mainframe, fica muito simplificada a tarefa de instalar novos sistemas e fazer atualizações nos sistemas já existentes.

Dentre as principais desvantagens podemos citar:

- O custo é elevado, ou pelo menos as pessoas achavam que o custo era elevado, ate descobrirem o chamado TCO (Total Cost Ownership), do modelo Cliente/Servidor;
- As linhas de comunicação no Brasil apresentavam problemas sérios de desempenho e custavam verdadeiras fortunas, além de existir uma dependência completa, ou seja, quando a linha ficasse fora do ar (o que acontecia com acentuada freqüência ate o fim dos anos 90), ninguém tinha acesso aos sistemas;
- Na maioria dos casos, os sistemas e dados da empresa eram administrados por terceiros. O fato de os dados vitais para o funcionamento da empresa estarem sob a guarde de terceiros começou a ser questionado. As empresas não tinham nenhuma garantia concreta de como estes dados estavam sendo manipulados, e sobre quem tinha acesso aos dados e aos logs de auditoria aos dados. Neste momento começa a surgir um movimento pró descentralização dos dados, em favor de trazer os dados para servidores dentro da empresa ou sob o controle da empresa.

No final da década de 80, inicio dos anos 90, os computadores padrão PC já eram uma realidade. Com o aumento das vendas os custos começaram a baixar e mais e mais empresas começaram a comprar computadores padrão PC. O próximo estagio neste processo foi, naturalmente, a ligação destes computadores em rede. Desde as primeiras redes, baseadas em cabos coaxiais, até as modernas redes, baseadas em cabeamento estruturado e potentes Switchs de 100/1000 Mbits, o computador padrão PC continua sendo amplamente utilizado.

A idéia básica do modelo Cliente/Servidor era uma descentralização dos dados e dos aplicativos, trazendo os dados para servidores localizados na rede local, onde estes pudessem ser utilizados, e os aplicativos instalados nos computadores da rede. Este movimento de um computador de grande porte – Mainframe, em direção a servidores de menor porte – servidores de rede local, foi conhecido como Downsizing, ou retroceder.



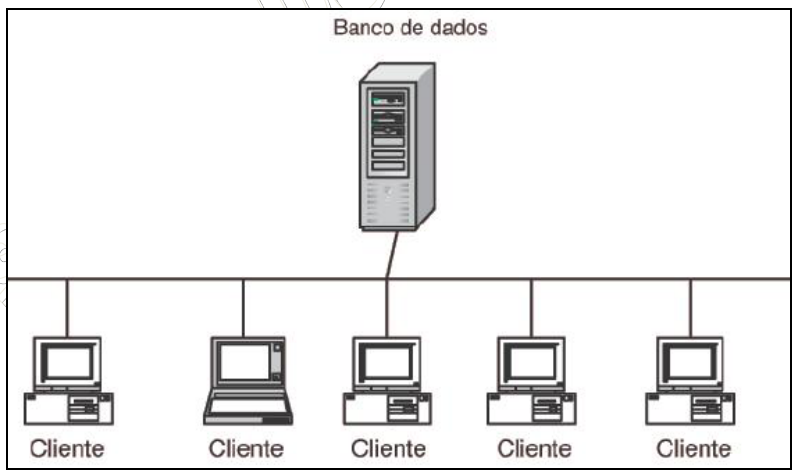
No modelo Cliente/Servidor temos um ou mais equipamentos de maior capacidade de processamento, atuando como Servidores. Estes equipamentos normalmente ficam reunidos em uma sala conhecida como “Sala dos Servidores”. São equipamentos com maior poder de processamento (normalmente com vários processadores), com grande quantidade de memória RAM e grande capacidade de armazenamento em disco. Os servidores normalmente rodam um Sistema Operacional especifico para servidor, como por exemplo o Windows Server 2003.

Nos servidores ficamos recursos a serem acessados pelas estações de trabalho da rede, como por exemplo pastas compartilhadas, impressoras compartilhadas, paginas da Intranet da empresa, aplicações empresariais, bancos de dados, etc. Como o próprio nome sugere, o servidor “Server” recursos e serviços que serão utilizados pelas estações de trabalho da rede, as quais são chamadas de estações clientes ou simplesmente clientes.

O modelo Cliente/Servidor pareceu, no inicio, ser uma solução definitiva em substituição ao modelo baseado em Mainframe. Porém os problemas, que não foram poucos, começaram a aparecer, dentre eles o elevado custo de administração e manutenção de uma rede baseada neste modelo. Para compreender esses problemas vamos explicar as diferentes versões do modelo Cliente/Servidor

Modelo em 2 camadas

No inicio da utilização do modelo Cliente/Servidor, as aplicações foram desenvolvidas utilizando-se um modelo de desenvolvimento em duas camadas. Neste modelo, os programas, normalmente desenvolvidos em um ambiente gráfico de desenvolvimento, como o Visual Basic, Delphi ou PowerBuilder, são instalados em cada estação de trabalho Cliente. Este programa acessadados em um servidor de banco de dados, conforme ilustrado abaixo:



No modelo de 2 camadas toda a “lógica do negócio” fica no Cliente. Quando o programa Cliente é instalado, são instaladas todas as regras de acesso ao Banco de dados.

Neste modelo, cada programa é instalado na estação de trabalho Cliente. Programa esse que faz acesso ao banco de dados que fica residente no Servidor de Banco de dados. A aplicação Cliente é responsável pelas seguintes funções:

- Apresentação: O código que gera a Interface visível do programa, faz parte da aplicação do cliente. Todos os formulários, menus e demais elementos visuais, estão contidos no código da aplicação cliente. Caso sejam necessárias alterações na interface do programa, faz-se necessária a geração de uma nova versão do programa, e todas as estações de trabalho que possuem a versão anterior, devem receber a nova versão, para que o usuário possa ter acesso as alterações da interface. Ou seja, uma simples alteração de interface, é suficiente para gerar a necessidade de atualizar a aplicação em dezenas de estações de trabalhos, dependendo do porte da empresa. O gerenciamento desta tarefa é algo extremamente complexo e oneroso financeiramente.

- Lógica do Negócio: As regras que definem a maneira como os dados serão acessados e processados, são conhecidas como “Lógica do Negócio”. Fazem parte da Lógica do Negócio, desde funções simples de validação de entrada de dados, como o calculo do digito verificador de um CPF ou CNPJ, ate funções mais complexas, como descontos escalonados para os maiores clientes, de acordo com o volume da compra. Alterações nas regras do negócio são bastante freqüentes, ainda mais com as repetidas mudanças na legislação de nosso país. Com isso, faz-se necessária a geração de uma nova versão do programa, cada vez que uma determinada regra de negócio muda, ou quando regras forem acrescentadas ou retiradas. Desta forma, todas as estações de trabalho que possuem a versão anterior, devem receber a nova versão, para que o usuário possa ter acesso as alterações. Ou seja, qualquer alteração nas regras do negócio (o que ocorre com freqüência), é suficiente para gerar a necessidade de atualizar a aplicação, em dezenas de computadores.

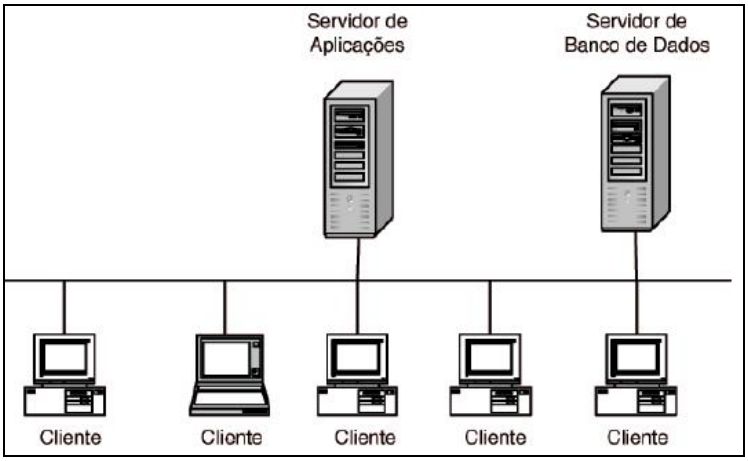
A outra camada, no modelo de 2 camadas, é o Banco de Dados, o qual fica armazenado no Servidor de Banco de Dados. Com a evolução do mercado e as alterações da legislação, mudanças nas regras do negócio tornaram-se bastantes freqüentes. Com isso o modelo de 2 camadas, demonstrou-se de difícil manutenção e gerenciamento, alem de apresentar um TCO – Total Cost of Ownership (Custo Total de Propriedade) bastante elevado.

O TCO é uma medida do custo total, anual, para manter uma estação de trabalho conectada a rede, e funcionando com todos os programas que o usuário necessita, atualizados. Este custo leva em conta uma série de fatores, tais como o custo do Hardware, o custo das licenças de software, o custo do desenvolvimento de aplicações na própria empresa, o custo das horas paradas em que o funcionário não pode utilizar os sistemas por problemas na sua estação de trabalho e assim por diante.

Na prática este custo mostrou-se impraticável, o que levou a proposta do modelo de 3 camadas.

Modelo em 3 Camadas

Como uma evolução do modelo de 2 camadas, surge o modelo de três camadas. A idéia básica do modelo de 3 camadas, é retirar as Regras do Negócio, da aplicação Cliente e centralizá-las em um determinado ponto (as aplicações saíram do Mainframe para as estações de trabalho e agora começam a ser centralizadas novamente nos servidores da rede), o qual é chamada de Servidor de Aplicações. O acesso ao banco de dados é feito através das regras contidas no Servidor de Aplicação. Ao centralizar as Regras do Negócio em um único ponto, fica muito mais fácil a atualização destas regras, as quais conforme descrito anteriormente, mudam constantemente. A figura a seguir ilustra o novo modelo:



No modelo de 3 camadas, toda a “lógica do negócio” fica no Servidor de Aplicações. Com isso, a atualização das regras de negócio fica mais fácil.

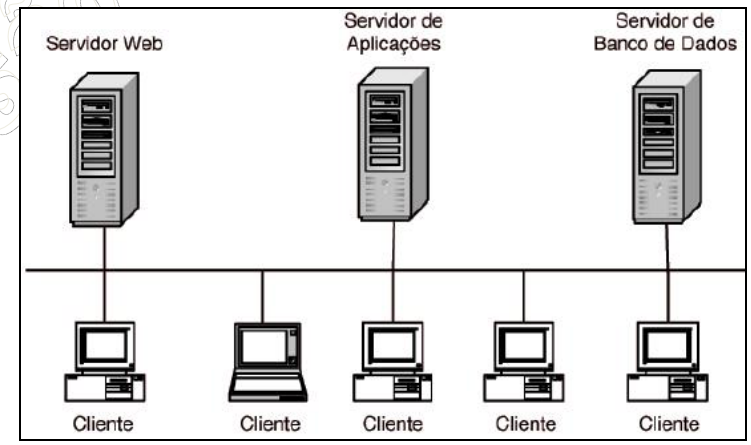
Todo o acesso do cliente, aos dados do servidor de Banco de Dados, é feito de acordo com as regras contidas no Servidor de Aplicações. O cliente não tem acesso aos dados do servidor de Banco de Dados, sem antes passar pelo servidor de aplicações, Com isso as três camadas são as seguintes:

- Apresentação: Continua a fazer parte do programa instalado no cliente. Alterações na Interface do programa, ainda irão gerar a necessidade de atualizar a aplicação em todas as estações de trabalho da rede, onde a aplicação estiver sendo utilizada. Porém cabe ressaltar, que alterações na interface, são menos freqüentes do que alterações nas regras do Negócio;
- Lógica: São as regras do negócio, as quais determinam de que maneira os dados serão utilizados e manipulados pelas aplicações. Esta camada foi deslocada para o Servidor de Aplicações. Após a atualização, todos os usuários passarão a ter acesso a nova versão, sem que seja necessário reinstalar o programa cliente em cada um dos computadores da rede;
- Dados: Nesta camada temos o servidor de banco de dados, no qual reside toda a informação necessária para o funcionamento da aplicação. Cabe reforçar que os dados somente são acessados através do Servidor de Aplicação, e não diretamente pela aplicação cliente. Esta é uma característica muito importante do modelo em 3 camadas, ou seja, a aplicação nunca faz acesso direto aos dados. Todo acesso aos dados é feito através do servidor de aplicações, onde estão as regras do negócio.

Com a introdução da camada de Lógica, resolvemos o problema de termos que atualizar a aplicação, em dezenas de estações de trabalho, toda vez que uma regra do negócio for alterada. Porém continuamos com o problema de atualização da interface da aplicação. Por isso que surgiram os modelos de n-camadas.

Modelo em 4 camadas

Com a evolução do modelo de três camadas, surge o modelo de quatro camadas. A idéia básica do novo modelo é retirar a apresentação do cliente e centralizá-la em um determinado ponto (agora está ainda mais parecido com a época do Mainframe), o qual na maioria dos casos é um servidor Web. Com isso o próprio Cliente deixa de existir como um programa que precisa ser instalado em cada computador da rede. O acesso a aplicação é feito através de um Navegador, como por exemplo o Internet Explorer. A figura abaixo ilustra o novo modelo:



No modele de 4 camadas o Cliente só precisa de um Navegador para ter acesso a aplicação.

Para acessar a aplicação o cliente acessa o endereço da aplicação (url), utilizando o seu navegador, como por exemplo: http://intranet.empresa.com.br/sistema/ponto.aspx

Todo o acesso do cliente ao Banco de Dados é feito de acordo com as regras contidas no Servidor de Aplicações. O cliente não tem acesso ao Banco de Dados, sem antes passar pelo servidor de aplicações. Com isso temos as seguintes camadas:

- Cliente: Neste caso o Cliente é o Navegador utilizado pelo usuário, que seja o Internet Explorer ou qualquer outro;

- Apresentação: Passa a ser disponibilizada pelo Servidor Web. A interface pode ser composta de paginas HTML, ASP, PHP, Flash ou qualquer outra tecnologia capaz de gerar conteúdo para o navegador. Com isso as alterações na interface da aplicação são feitas diretamente no servidor Web, sendo que estas alterações estarão, automaticamente, disponíveis para todos os Clientes. Com este modelo não existe a necessidade de reinstalar a aplicação em todos os computadores da rede. Fica muito mais fácil garantir que todos estão tendo acesso a versão mais atualizada da aplicação. A única coisa que o cliente precisa ter instalado na sua máquina é o navegador. Com isso os custos de manutenção e atualização de aplicações fica bastante reduzido, ou seja, baixa o TCO – Total Cost of Ownership;
- Lógica: São as regras do negócio, as quais determinam de que maneira os dados serão utilizados. Esta camada está no Servidor de Aplicações. Desta maneira, quando uma regra do negócio for alterada, basta atualizá-la no Servidor de Aplicações;
- Dados: Nesta camada temos o servidor de Banco de Dados, no qual reside toda a informação necessária para o funcionamento da aplicação;

Os servidores de Aplicação, Web e Banco de Dados, não precisam necessariamente ser servidores separados, isto é, uma maquina para fazer o papel de cada um dos servidores. O conceito de servidor de Aplicação, servidor Web ou servidor de Banco de Dados, é um conceito relacionado com a função que o servidor desempenha. Podemos ter, em um mesmo equipamento, todos os servidores reunidos. Claro que questões de desempenho devem ser levadas em consideração.

O modelo de 4 camadas se assemelha ao modelo Mainframe, com aplicações e dados no servidor, administração centralizada e redução no custo de propriedade (TCO), porém com todos os benefícios e custos dos atuais computadores.

Na prática, o que está em uso nas empresas é um modelo misto, onde algumas aplicações rodam no PC do usuário e outras são acessadas através da rede, mas rodam nos servidores da rede da empresa. O que se busca é o "melhor dos dois mundos", ou seja, os recursos sofisticados e aplicações potentes com interfaces ricas do modelo Cliente/Servidor, com a facilidade e baixo custo do modelo Centralizado.

Com esta visão, podemos agora introduzir o Windows Server 2003 como um projeto para ser o sistema operacional dos servidores da rede da empresa.

Sistemas Operacionais de Redes baseados no modelo Cliente/Servidor

Um Sistema Operacional de Redes (SOR) é uma coleção de computadores conectados através de uma rede. Nesta rede, cada computador possui seu próprio Sistema Operacional Local (SOL). Cada máquina possui alto grau de autonomia em relação aos demais.

O SOR é uma evolução dos Sistemas Operacionais Locais, ou centralizados, incorporando módulos para acessar recursos remotos. Esses módulos, ou funções básicas de uso geral, tornam a comunicação entre estes sistemas transparentes para uso dos recursos compartilhados, e é realizado através de protocolos de transporte, como: Sockets e RPC (Remote Procedure Call). Essa comunicação é realizada com transferências explícitas, ou seja, o usuário deve conhecer a localização exata dos recursos na rede, e estes recursos pertencem a computadores específicos. Como exemplos podemos citar: o compartilhamento de impressoras e arquivos, web, e-mail e serviços de autenticação.

O computador tem, então, o Sistema Operacional Local (SOL) interagindo com o Sistema Operacional de Redes (SOR), para que possam ser utilizados os recursos de rede tão facilmente quanto os recursos na máquina local.

Em efeito, o SOR coloca um redirecionador entre o aplicativo do cliente e o Sistema Operacional Local para redirecionar solicitações de recursos da rede para o programa de comunicação que vai buscar os recursos na própria rede.

A tabela a seguir resume as principais diferenças entre o SOL e o SOR:

	SO Centralizado ou Local	SO de Rede
Serviços	Gerenciamento de processos, memória, dispositivos, arquivos.	Acesso remoto, troca de informações.
Objetivos	Gerenciar recursos, máquina estendida, virtualização.	Compartilhar recursos, interoperabilidade.
Se parece com um único processador virtual?	Sim	Não
Todas as máquinas executam o mesmo sistema operacional?	Sim	Não
Como a comunicação ocorre	Memória compartilhada	Arquivos compartilhados, protocolos de transporte
Há uma única fila de execução?	Sim	Não
Quantas cópias do sistema operacional existem?	1	N

O Modelo de Operação do Sistema Operacional de Rede é o modelo Cliente / Servidor:

- Ambiente onde o processamento da aplicação é partilhado entre um outro cliente (solicita serviço) e um ou mais servidores (prestam serviços).

Os módulos do SOR podem ser:

- Módulo Cliente do Sistema Operacional (SORC)
- Módulo Servidor do Sistema Operacional (SORS)

Os tipos de arquiteturas para Sistemas Operacionais de Rede são:

- Peer-to-Peer
- Cliente-Servidor:
    - Servidor Dedicado
    - Servidor não Dedicado

Na arquitetura Peer-to-Peer temos várias máquinas interligadas, cada uma com serviços de Servidor e de Cliente na mesma máquina junto com o Sistema Operacional Local. São exemplos de serviços: o Kaaza e e-Mule.

Na arquitetura Cliente-Servidor com Servidor Dedicado, temos uma máquina servidora que não executa aplicativos locais. Geralmente ela só é acessada através de console, ou terminal, e administrada por empresas terceirizadas.

Na arquitetura Cliente-Servidor com Servidor não Dedicado, temos uma máquina servidora que executa aplicativos locais, além de prover os serviços de Servidor. Geralmente adotada por empresas de pequeno a médio porte, cuja relação custo x benefício pesa mais do que o desempenho propriamente dito.

Uma nova arquitetura em ascensão é a baseada em servidores virtualizados, onde um único servidor passa a hospedar diferentes e diversas máquinas virtuais. Cada máquina virtual pode executar seu próprio sistema operacional, o servidor host aloca diferentes recursos de hardwares para cada máquina virtual, respeitando o total de recursos existentes.

Agora que sabemos o que é e para que serve o Windows Server 2003, vamos analisar suas formas de instalação e conhecer todos os serviços disponíveis em sua edição.

7.4 TIPOS DE INSTALAÇÕES

Existem basicamente duas formas de instalação do Windows Server 2003:

- Instalação em um servidor novo, no qual não existe nenhum sistema operacional instalado: Neste caso, basta ligar o servidor com o CD-Rom do Windows Server 2003 no drive. O processo de instalação inicia automaticamente.
- Atualização de uma versão do Windows já existente: Por exemplo, você pode querer atualizar um servidor com o Windows 2000 Server ou NT Server para o Windows Server 2003. Neste caso, com o servidor ligado, basta inserir o CD do Windows Server 2003 no drive e seguir os passos do assistente de instalação.

Antes de iniciar a instalação é recomendado que você faça uma verificação para ver se existe alguma incompatibilidade com o Windows Server 2003. As incompatibilidades podem ser de dois tipos: de hardware ou de software.

Uma incompatibilidade de hardware significa que algum componente de hardware do computador não é compatível com o Windows Server 2003, como ocorre geralmente com placas de vídeos voltadas para jogos, e neste caso pode ocorrer de o respectivo dispositivo de hardware não funcionar após a instalação do Windows Server 2003. Uma segunda situação possível é quando o hardware funciona, porém de forma incorreta, comprometendo a estabilidade do conjunto dos demais hardwares que se relacionam. O ideal é que antes de adotar o Windows Server 2003 como plataforma operacional de rede, se certificar de que o hardware seja compatível e homologado para este sistema.

Uma incompatibilidade de software significa que algum componente de software do computador não é compatível com o Windows Server 2003, como ocorre geralmente com aplicações para MS-DOS ou de 16 bits, e neste caso não irão funcionar sobre as plataformas de 32 ou 64 bits do Windows Server 2003. Aplicações 16 bits exigem dedicação exclusiva do processador, enquanto que em plataformas 32 bits ou superiores, nenhuma aplicação detém exclusividade do processador. Semelhante a incompatibilidade de hardware, softwares não compatíveis e instalados, podem comprometer a estabilidade de todo o sistema, fazendo com que o mesmo apresente “travamentos”, atrase a inicialização de outros aplicativos, ou mesmo corrompendo outros aplicativos relacionados com ele.

O Windows Server 2003 oferece um assistente que faz a verificação de todos os componentes do computador e retorna um relatório de possíveis incompatibilidades.

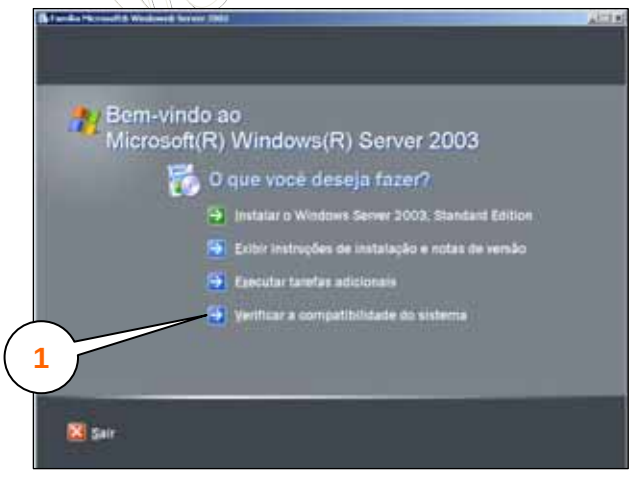


Figura 1. Assistente de Instalação do Windows

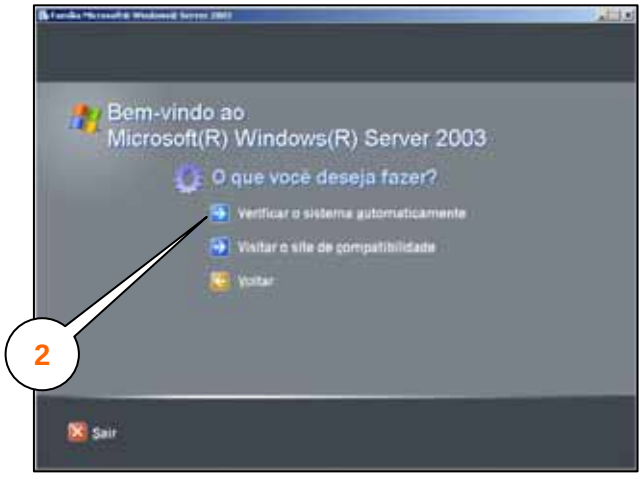


Figura 2. Assistente de Compatibilidades

É possível que o assistente localize incompatibilidades. As observações são sempre relatadas na forma de um relatório, como nas ilustrações abaixo:

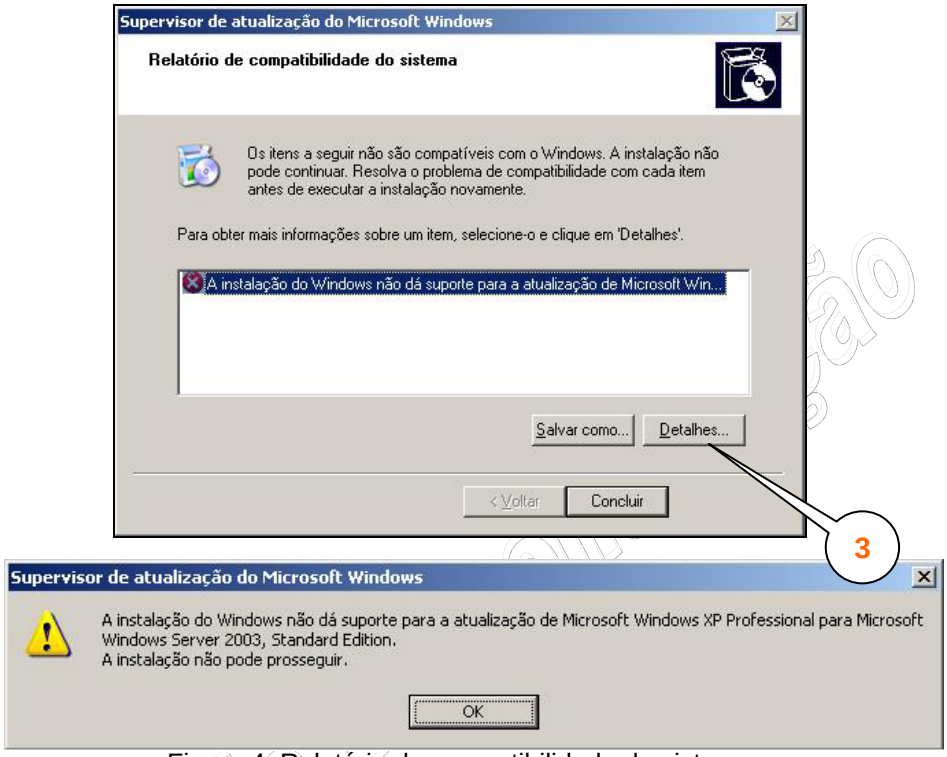


Figura 4. Relatório de compatibilidade do sistema

Outra alternativa de consultar compatibilidades com o sistema, sem precisar do CD-Rom de instalação, é através do site, http://www.windowsservercatalog.com :

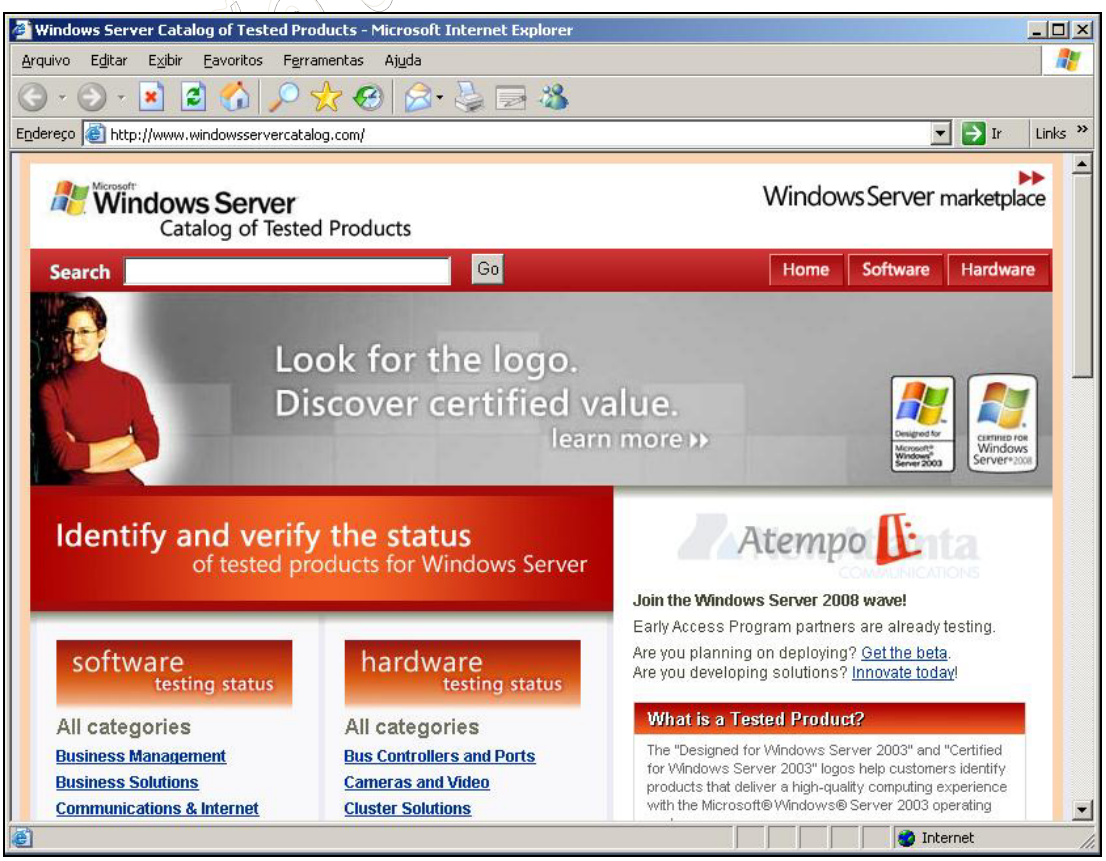


Figura 5. Site de verificação de compatibilidade do Windows Server 2003

Para servidores que já tem o Windows Server 2000 ou o NT Server 4.0 instalado, você pode optar por fazer uma atualização da versão atual para o Windows Server 2003. Ao fazer o upgrade, todos os programas e configurações serão mantidos. Porém se houver problemas de sistemas não funcionando direito, com configurações incorretas ou arquivos corrompidos, estes problemas também estarão presentes após a atualização (upgrade) para o Windows Server 2003. A vantagem deste método é que não é necessária a reinstalação de todos os programas. Mesmo que você realize um upgrade, sempre é recomendável, para não dizer obrigatório, que você faça um backup completo do servidor. Caso haja algum problema durante o processo do upgrade, sempre é possível utilizar o backup para restaurar a versão anterior do sistema operacional.

Você somente consegue fazer o upgrade para o Windows Server 2003, das versões de servidor do Windows. Por exemplo, não é possível fazer um upgrade a partir do Windows 2000 Professional ou do Windows XP Professional. Na tabela abaixo você tem um relação dos caminhos de atualização de outras versões do Windows para Windows Server 2003:

Versão Anterior	Pode atualizar para o Windows Server 2003
Windows NT 3.51 ou anterior	Não. Primeiro você deve fazer a atualização do Windows NT 3.51 ou anterior para o Windows NT Server 4.0, com Service Pack 5.0 ou superior.
Windows NT 4.0 Server	Sim, porém deve estar instalado o Service Pack 5.0 ou superior.
Windows 2000 Server	Sim
Windows 2000 Advanced Server	Sim
Windows 2000 Professional	Não
Windows XP Professional	Não

Outras decisões que precisam ser tomadas quando se está instalando o Windows Server 2003, porém que só analisaremos mais a frente, são:

- Quantas partições o servidor terá em seu disco rígido?
- Qual o sistema de arquivos a ser adotado: FAT32 ou NTFS?
- O novo servidor será um controlador de domínio ou um servidor autônomo?
- O servidor fará parte de um domínio ou de um Grupo de Trabalho (Workgroup)?
- Qual será o nome do servidor? Sempre lembrando que não pode haver dois servidores com o mesmo nome, no mesmo domínio.
- Quais as configurações do protocolo de redeTCP/IP? Geralmente servidores possuem endereços configurados manualmente, mas é possível manter a configuração de endereço dinâmico, ou DHCP. No caso de configurações manuais, você precisará ter anotado: o endereço IP, máscara de sub-rede, endereço IP do Default Gateway (ou roteador da rede), endereço IP dos servidores de nomes DNS e WINS, nome do host e domínio DNS.

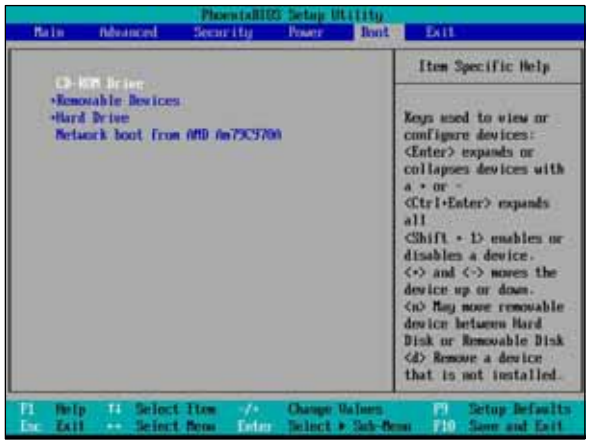
A questão do sistema de arquivos será o assunto do próximo capítulo, e em relação a controlador de domínio, servidor autônomo, serviços do servidor, veremos tudo isso na próxima competência.

Existem ainda outras formas de instalação do Windows Server 2003, tais como instalações não assistidas, usando um arquivo de respostas. Passaremos agora a ver a instalação do Windows Server 2003 a partir do zero, realizando o boot a partir de um CD-Rom:

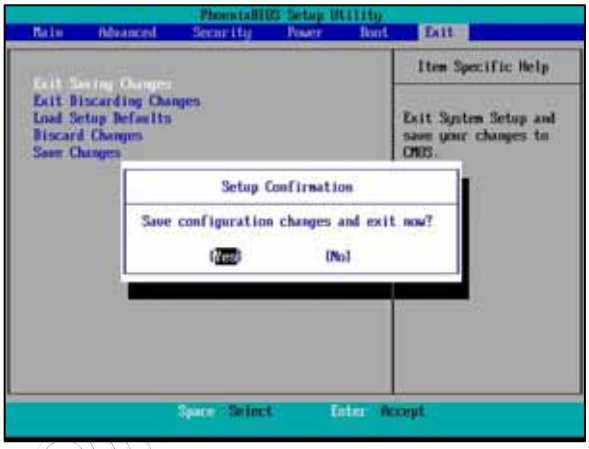
Instalando o Windows Server 2003 a partir do zero, via boot de CD-Rom

O procedimento para fazer a instalação de qualquer edição do Windows Server 2003 é praticamente o mesmo. Vamos demonstrar o passo-a-passo a seguir:

1. Ligue o computador, insira o CD-Rom do Windows Server 2003 no drive e aguarde até que o sistema seja inicializado a partir do CD-Rom. Em alguns computadores surge uma mensagem pedindo para que seja pressionada qualquer tecla para fazer a instalação, em outros computadores mais antigos é necessário acessar a tela de configuração do BIOS (geralmente as teclas F2, F10 ou F12 acessam o BIOS assim que você liga o computador):

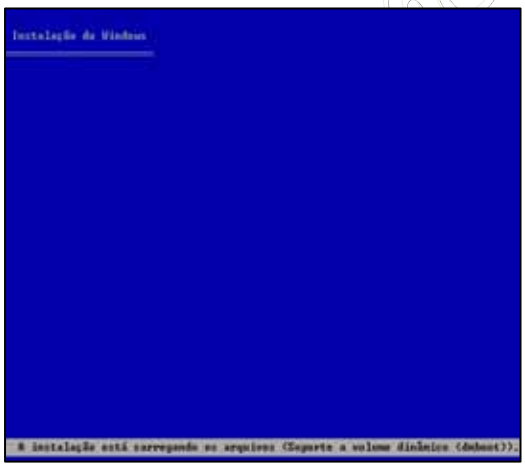


Selecione o CD-Rom como primeira opção de Boot



Salve as configurações antes de sair

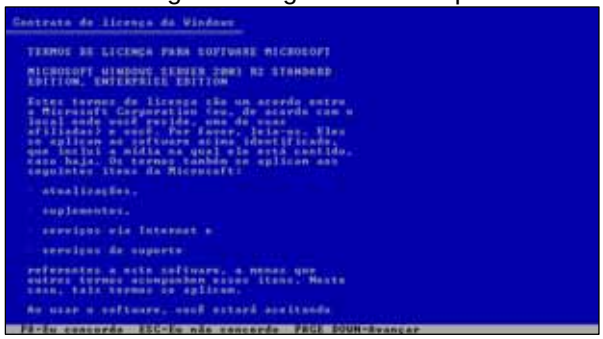
2. Em seguida o Windows Server 2003 começa a ser carregado a partir do CD-Rom, surge então uma tela azul com a mensagem “Instalação do Windows”. Esta é a fase chamada de “fase DOS” ou fase de caractere, pois nestas etapas iniciais o programa de instalação ainda não está em modo gráfico:



Tela de Preparação da Instalação

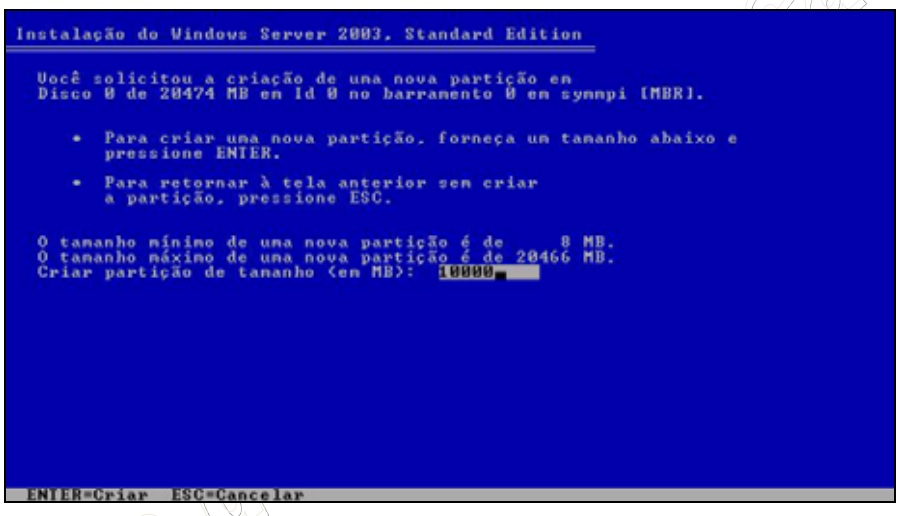
Tela Inicial de Instalação

3. Pressione o <ENTER> e inicie a instalação do Windows Server 2003. Nas próximas telas você será apresentado ao contrato de licença, o qual você pode aceitar pressionando a tecla “F8”. Em seguida chegou a hora de particionar o disco rígido:

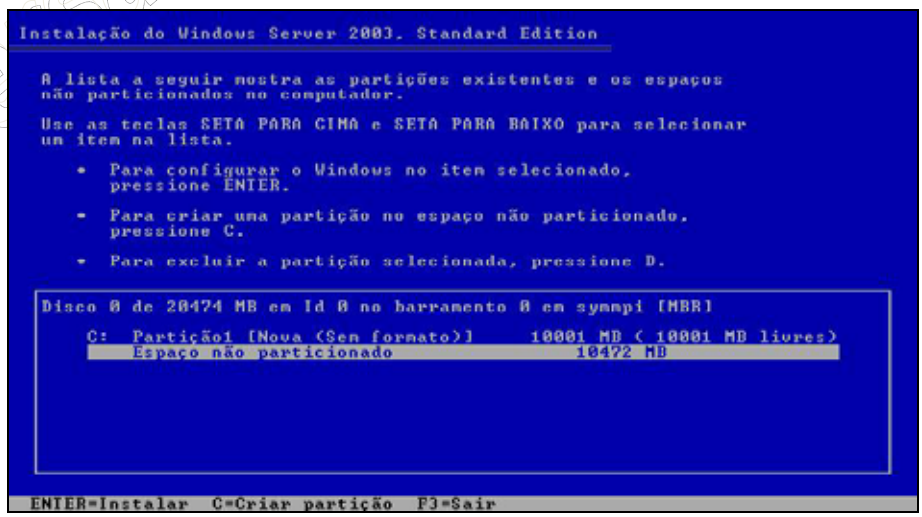


No próximo capítulo estudaremos o sistema de arquivos NTFS da Microsoft, por hora precisamos apenas definir como ficará a topologia lógica do nosso sistema de arquivos. O recomendado é você pensar sempre em “acesso” e “desfragmentação”. Acesso implica em definir uma área junto ao disco rígido que seja especializada em provê acessos contínuos e frequentes, como por exemplo, uma partição onde ficarão o próprio Windows, a pasta Arquivos de Programas e outras pastas de aplicativos a serem utilizados com freqüência. Desfragmentação implica em definir uma área onde serão alocados muitos arquivos pequenos, de constante movimentação e que exigem que o as agulhas do disco rígido trabalhem mais sobre determinada área do disco rígido. Como exemplo podemos citar as pastas de arquivos temporários, cachês ou mesmo uma partição exclusiva para guardar apenas os dados do servidor. Uma partição exclusiva para dados permite que configuremos o modo de partição compactada, de forma a conter mais dados do que sem a compactação extra.

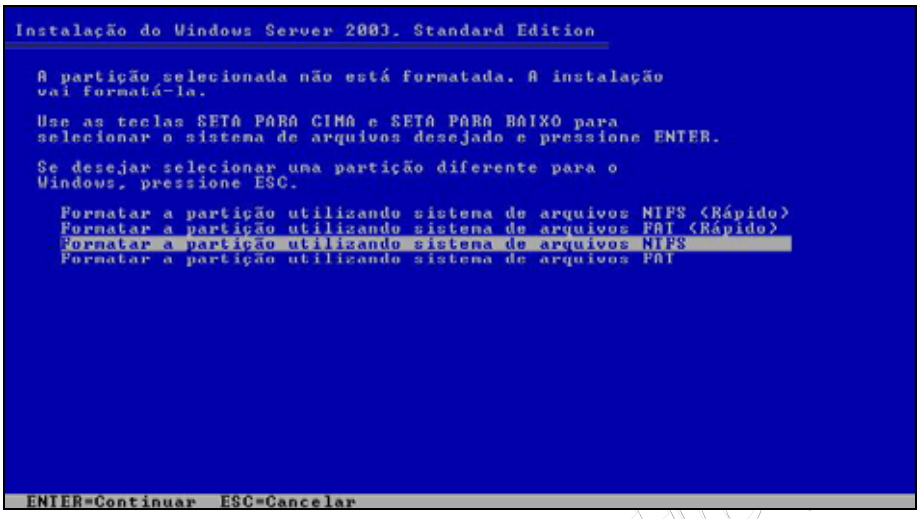
Criaremos duas partições em nosso servidor, uma para sistemas e outra apenas para dados:



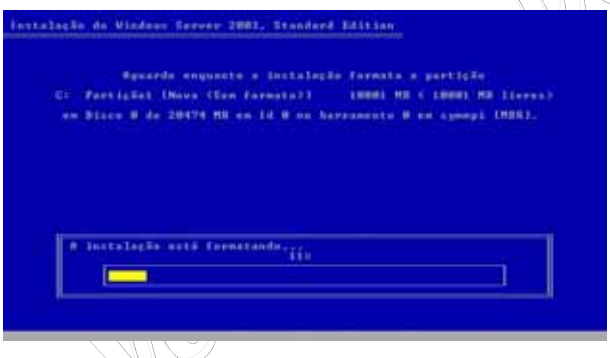
Após precionar a tecla “C” da tela anterior a seguinte tela é apresentada para definir o tamanho da partição, escolhemos participar o HD em 50% para sistema. Após definição do tamanho precionamos <ENTER> para afirmar nossa escolha;



Retornamos novamente para a tela de configuração das partições, podemos optar por deixar a criação da segunda opção para depois, quando o Windows estiver instalado, e vamos agora formatar nossa nova partição de sistemas para poder copiar os arquivos. Selecione a partição “C” e precione o <ENTER> para instalar o Windows no C:



Selecione o sistema de arquivos NTFS. O modo Rápido só é recomendado quando você está realizando um upgrade no antigo sistema, de forma que o NTFS ou FAT já existam e você queira apenas apagar os dados contidos nesta partição. O modo completo irá, além de apagar os dados, zerar todos os clusters e ligações da MBR. O sistema de arquivos NTFS possui muitas vantagens sobre o FAT, como permissões de acesso a arquivos e pastas, compactação, indexação, entre outros. O FAT geralmente é utilizado por dispositivos móveis, como pendrivers, câmeras digitais e filmadoras digitais.



Formatando o sistema de arquivos

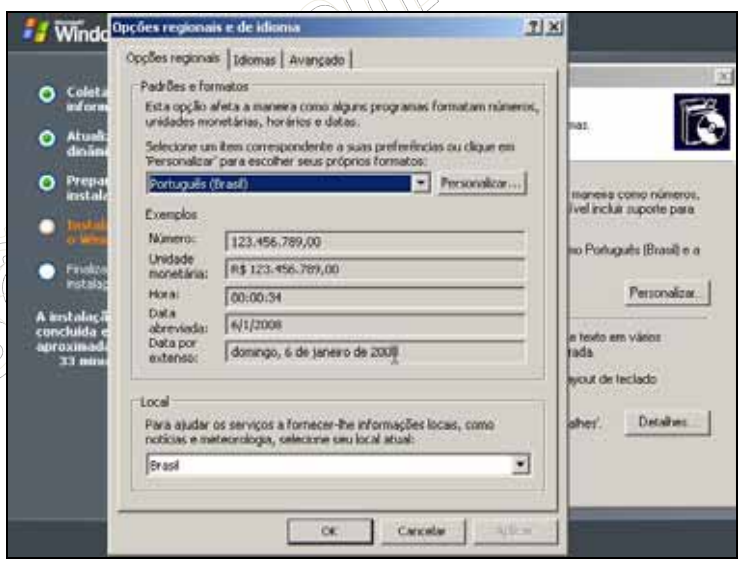
Iniciando a copia dos arquivos para C:

Após concluir a formatação o assistente de instalação do Windows irá copiar os arquivos de instalação do CD-Rom para uma pasta temporária em C: e iniciar a interface gráfica de instalação do Windows.

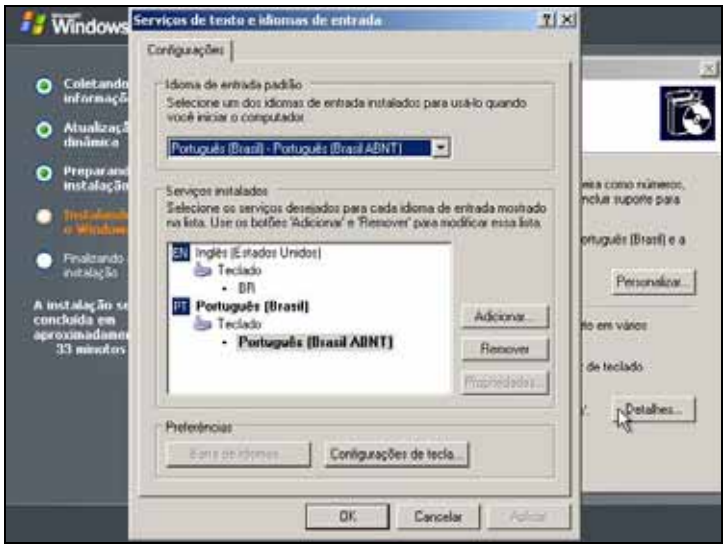
4. Uma vez iniciada a instalação em modo gráfico do Windows você será questionado a responder umas poucas perguntas até que o sistema seja plenamente instalado:

A primeira interação com a instalação ocorrerá logo após o início da instalação do Windows, onde será questionado sobre as opções regionais e de idioma:

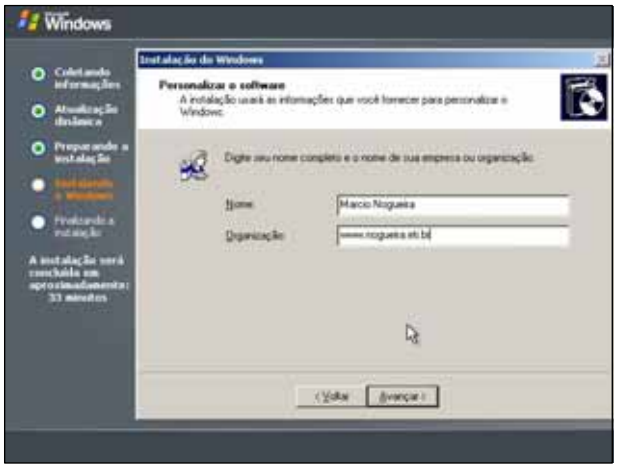
Em “Personalizar” você encontrar as opções de configuração regionais para o idioma “Português (Brasil)”:



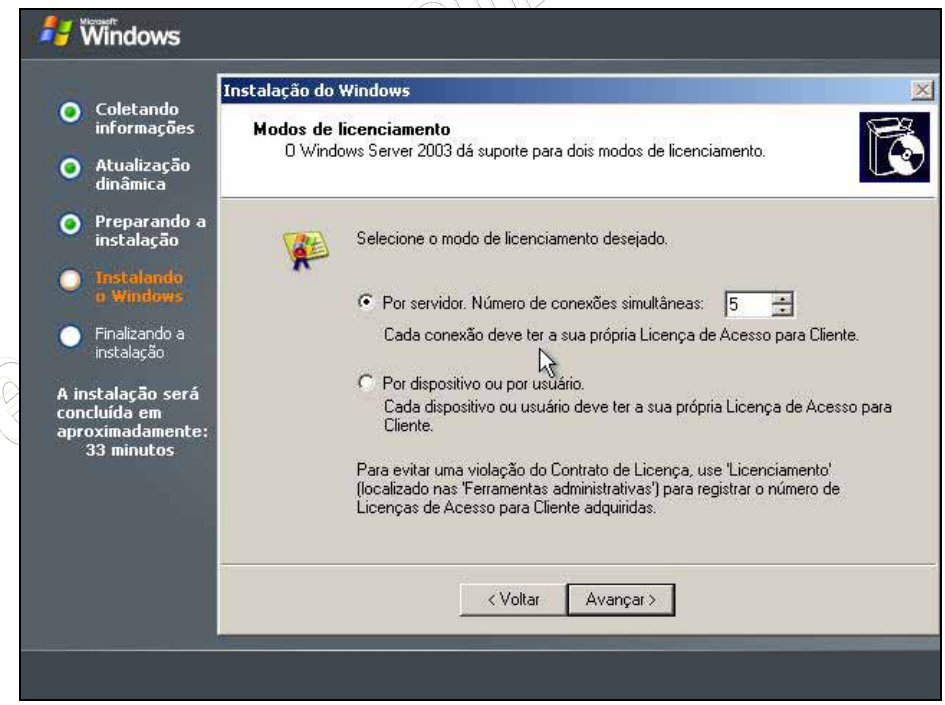
Em “Detalhes” você encontrará as configurações de teclado:



Seguindo adiante com a instalação você deverá preencher os dados de registro, ou seja, os dados de quem comprou o Windows e o número de série, fornecido juntamente com o CD-Rom ou sobre a etiqueta da Microsoft, localizada na parte traseira do servidor.



A próxima pergunta, sobre Modo de Licenciamento, é um pouco mais complexa e vai depender do tipo de licença que você adquiriu ao comprar o Windows:



As diferenças entre os dois modos de licenciamento são:

- Por servidor: esta forma de licenciamento é mais indicado para pequenas empresas, nas quais existe um único servidor com o Windows 2003 Server instalado. Com este tipo de licenciamento, o número de licenças define o número máximo de usuários conectados simultaneamente ao servidor. Se o número máximo de conexões for atingido e mais um usuário tentar acessar um recurso do servidor, este último não conseguirá fazer a conexão e receberá uma mensagem de erro. O número de licenças (e consequentemente de conexões simultâneas) é definido pelo número de CAL – Client Access Licences que você adquiriu. Ao comprar o Windows Server 2003 este já vem com um determinado número de licenças. Se você precisar de um número maior de licenças, deverá adquirir mais CALs, de acordo com o número de licenças que for necessário.

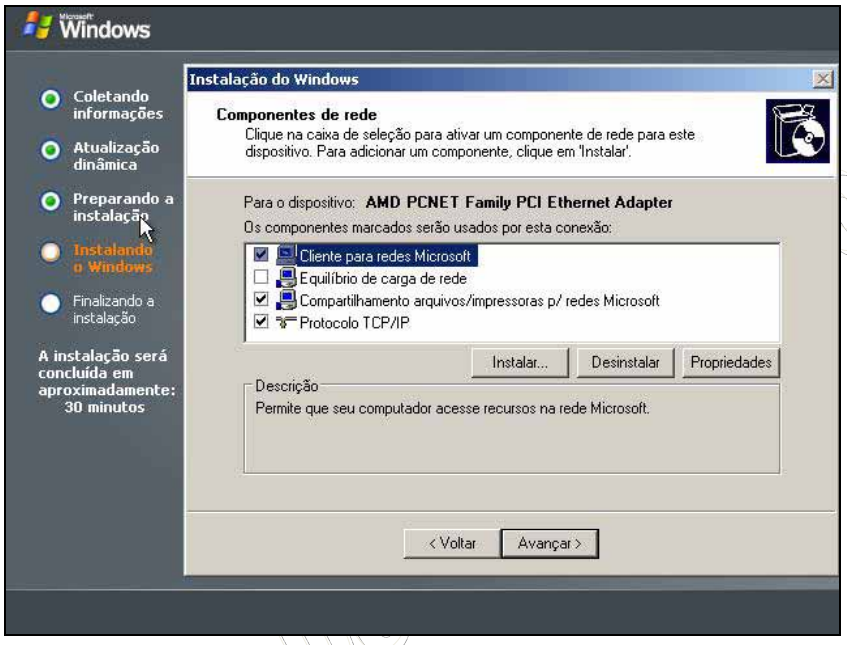
- Por dispositivo ou por usuário: Neste modo de licenciamento, uma CAL é necessária para cada estação de trabalho que faz a conexão com o servidor, independente de quantas conexões esta estação de trabalho venha a estabelecer com o servidor. Os clientes podem ser estações de trabalho baseadas no Windows ou em outro sistema operacional, como por exemplo um aplicativo em uma estação de trabalho Linux, acessando dados de um banco de dados SQL Server, em um servidor com o Windows Server 2003. Por exemplo, se a rede da sua empresa tem 1000 máquinas, você deve adquirir 1000 CALc, uma para cada estação de trabalho. O preço de uma CAL para este modo de licenciamento é maior do que o Por Servidor, mas em compensação com uma única CAL, a estação de trabalho pode acessar recursos em qualquer servidor que esteja utilizando o licenciamento Por Servidor.

A próxima fase da instalação é a definição do nome do computador e da senha do Administrador:

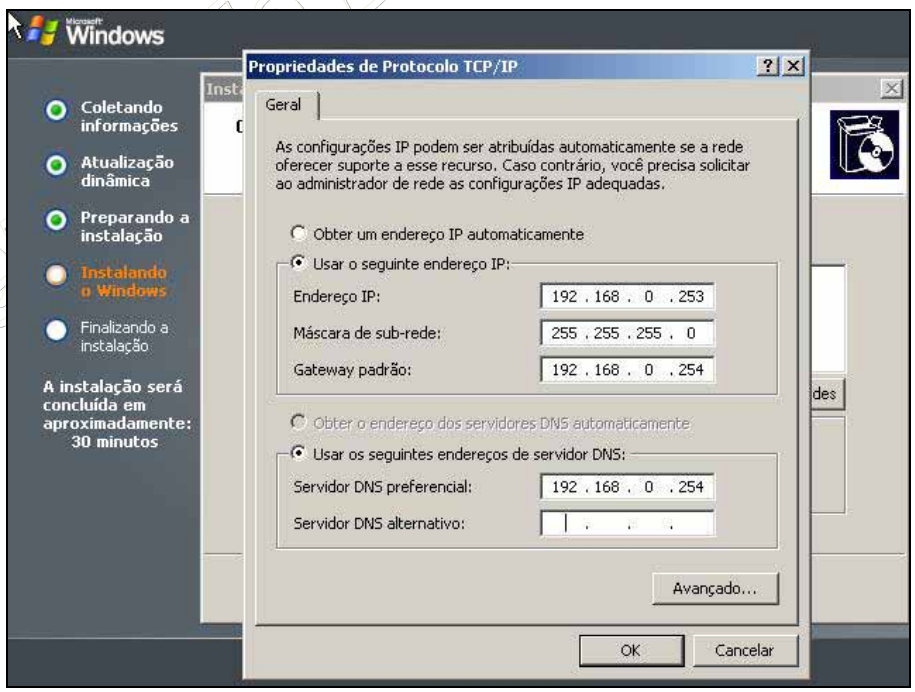
Ao definir uma senha muito fraca para a conta do Administrador uma tela de Alerta será exibida recomendando critérios para a escolha de uma senha segura. É altamente recomendado que você passe a adotar esses critérios em todas as suas senhas, visto as inúmeras tecnologias de fraudes existentes nos dias atuais.

Prosseguindo a instalação, chegaremos na etapa das configurações de rede:

Nas configurações de rede, como estamos tratando de um servidor, e como vimos nas definições de um sistema operacional servidor de rede, este precisa ser localizado para poder prestar seus serviços, então definiremos uma configuração manual de IP para que este possa ficar fixo e ser sempre localizados na rede:

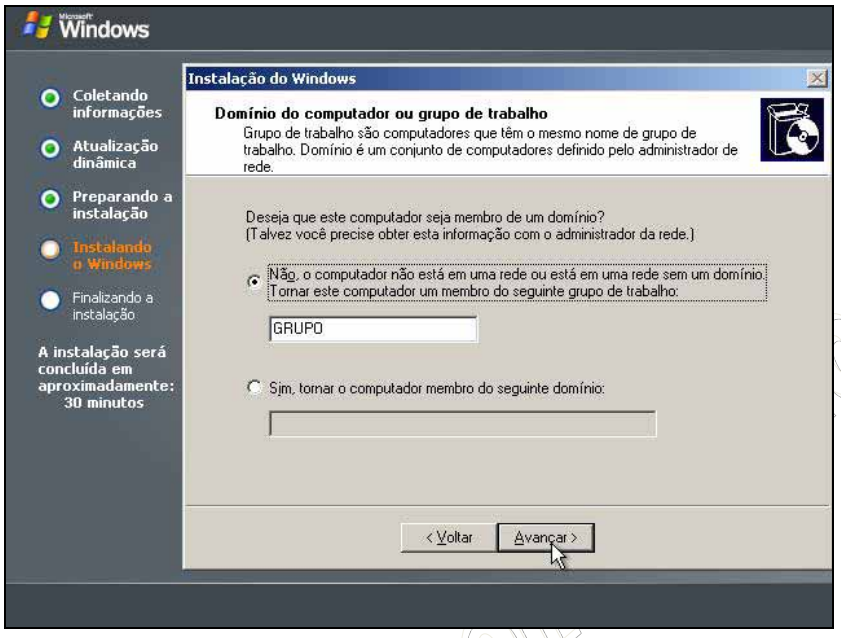


Clique em “Protocolo TCP/IP” e em seguida no botão “Propriedades”:



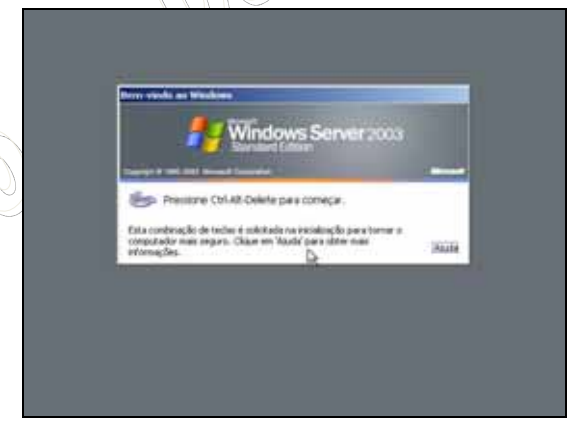
Informe os endereços conforme sua rede. Em caso de dúvidas consulte o seu administrador de rede.

A última etapa de respostas na fase de instalação é a definição do domínio ou grupo de trabalho:



Por ora estaremos trabalhando em um grupo de trabalho qualquer, visto que nosso interesse é transforma este Windows Server 2003 no domínio principal da rede.

Este último passo encerra as configurações de instalação do Windows. Quando o mesmo concluir de instalar todos os arquivos reiniciará o computador e a seguinte tela de Logon lhe será exibida:



Precione juntas e simultaneamente as teclas: <CTRL>+<ALT>+<DEL>, e em seguida informe a senha de Administrador que você configurou nos passos anteriores.

Pronto, a instalação está concluída! No primeiro acesso ao servidor lhe será apresentada uma tela para adicionar os serviços do servidor. Traremos desse assunto na próxima competência.

7.5 SISTEMAS DE ARQUIVOS

Agora que sabemos realizar a instalação do Windows Server 2003, voltemos a questão da escolha do tipo de sistema de arquivos. Esta escolha é importante pois a depender dela, você pode aproveitar ou não uma série de vantagens.

Para compreendermos o funcionamento dos sistemas de arquivos façamos antes uma revisão sobre os conceitos de armazenamento em computadores: o armazenamento básico e armazenamento dinâmico. Cada tipo de armazenamento está relacionado a uma tecnologia, como disco físico ou volume lógico.

Disco Físico

Chamamos de Disco Físico, ou simplesmente disco, a cada HD (Hard Disk) instalado no computador. O primeiro HD instalado é denominado de Disco 0, o segundo HD de Disco 1 e assim por diante. Um disco físico pode ser configurado como Disco Básico ou Disco Dinâmico. Mais adiante explicaremos as diferenças entre um disco básico e um disco dinâmico. Um disco básico pode ser dividido em uma ou mais partições, e um disco dinâmico pode ser dividido em um ou mais volumes.

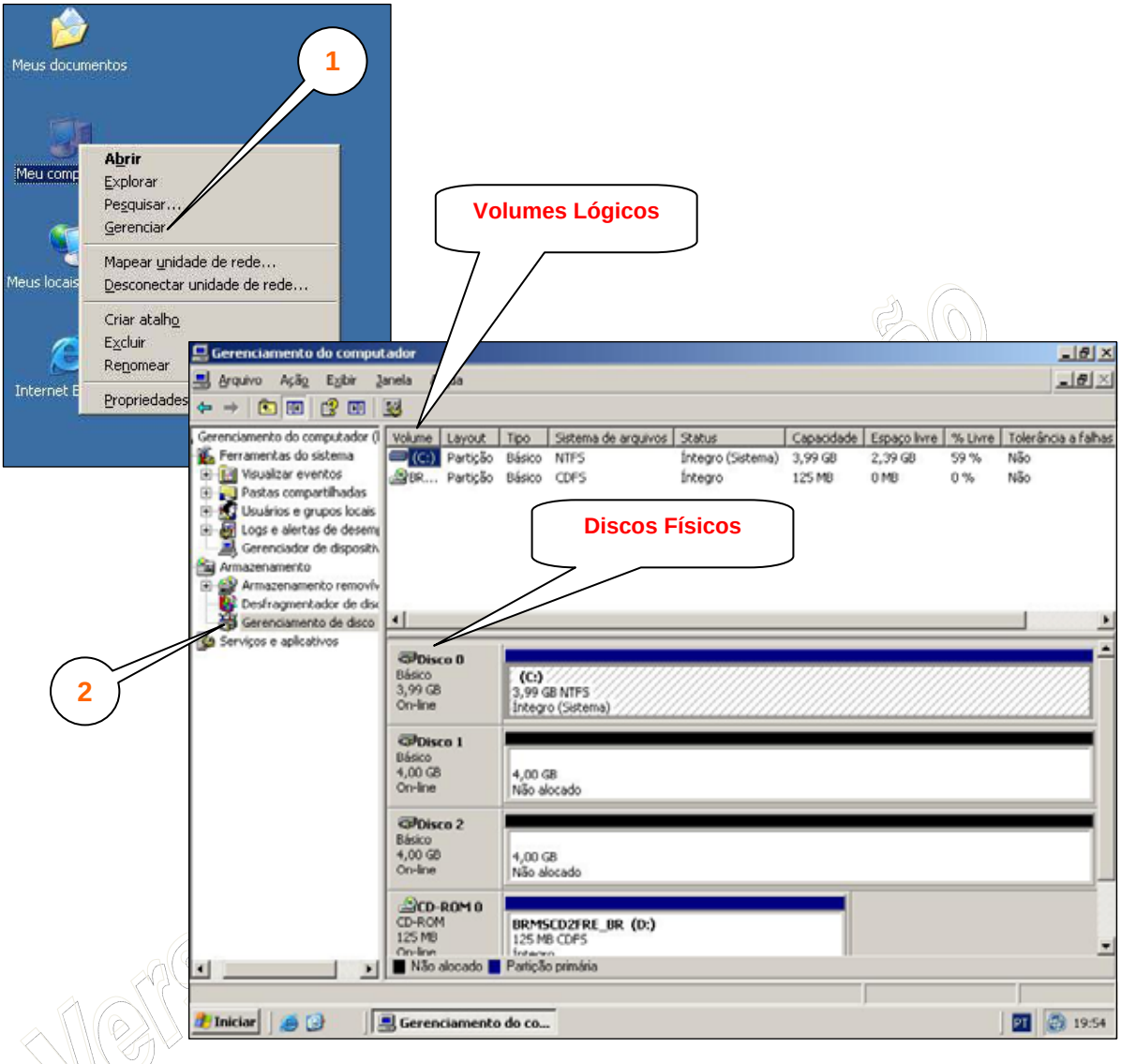
Duas observações importantes:

- Sistemas operacionais anteriores ao Windows 2000, não conseguem acessar discos dinâmicos. Por isso, se você está utilizando um sistema multi-boot, com mais de uma versão do Windows instalada, tenha cuidado ao converter um disco de dinâmico para básico, pois isso fará com que versões do Windows,anteriores ao Windows 2000, não consigam mais inicializar e ter acesso ao disco dinâmico.
- Em servidores, onde é utilizada uma placa da RAID por hardware (estudaremos RAID mais adiante), pode acontecer de um conjunto de três ou mais discos físicos, que fazem parte do RAID, seja visualizadas como um único disco pelo Windows Server 2003. Por exemplo, pode acontecer de você ter cinco discos de 50 Gb formando o RAID, e estes discos serem visualizados como um único disco de físico de 160 Gb (mais a frente estudaremos o por quê desta perda de 20% no espaço total do RAID).

Volumes Lógicos

Um volume lógico aparece para o sistema operacional, normalmente, como uma unidade a mais, tal como F:, G:, M: e assim por diante. Você pode dividir um disco físico em um ou mais volumes. Por exemplo, um disco de 80 Gb, pode ser dividido em três volumes, como: C: com 40Gb, onde será instalado o Windows Server 2003 e os aplicativos, D: com 20Gb, onde serão gravados arquivos de log do sistema operacional, o banco de dados do Active Directory e arquivos de logs de outros serviços, e finalmente um E: com 20Gb restantes, onde serão gravados arquivos dos usuários. Observe que neste exemplo temos um disco físico (Disco 0), o qual foi dividido, ou particionado, em três volumes lógicos, C:, D: e E:.

No Windows Server 2003 o procedimento para configuração dos discos físicos e volumes lógicos é: acessar o menu “Gerenciar”, clicando com o botão direito do mouse sobre o ícone do “Meu Computador” na área de trabalho. Estando com a janela “Gerenciamento do coputador” aberta clicar em “Gerenciamento de discos”, as ilustrações abaixo demonstram a execução destes procedimentos:



Armazenamento Básico e Armazenamento Dinâmico

Antes que seja possível utilizar um novo disco no Windows Server 2003, o administrador deve realizar algumas operações. Um dos aspectos que o administrador deve definir é o tipo de armazenamento que será utilizado no disco. No Windows Server 2003 é possível optar entre dois tipos de armazenamento: armazenamento básico ou o armazenamento dinâmico.

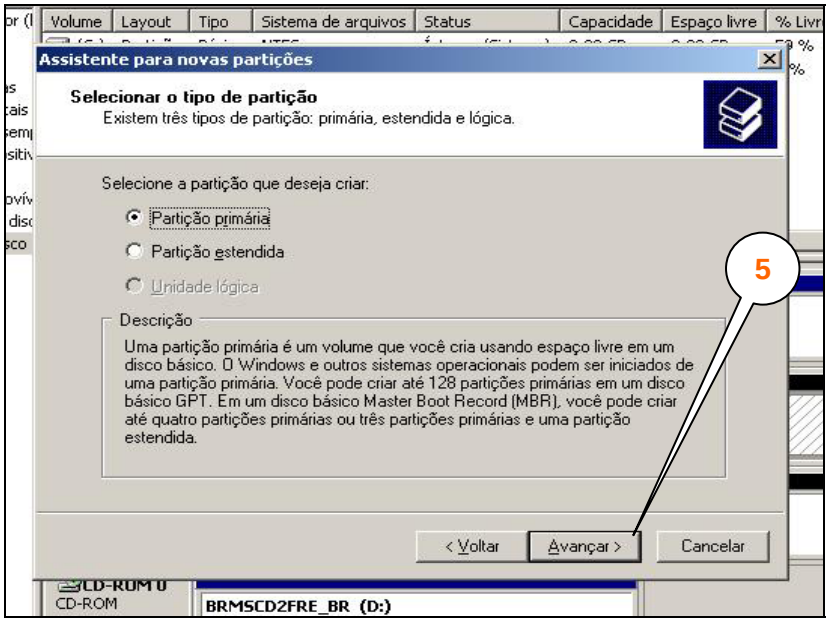
Armazenamento Básico

É o tipo de armazenamento que vem sendo utilizado desde a época do MS-DOS. É utilizado pelas versões anteriores ao Windows 2000, e é o tipo de armazenamento padrão no Windows Server 2003, isto é, todos os novos discos são criados com Armazenamento básico. Caso seja necessário o administrador pode transformá-los para armazenamento dinâmico sem perda de dados. Um disco com armazenamento básico é chamado de “disco básico”.

No armazenamento básico, o disco é dividido em partições (ou volumes básicos). Uma partição é uma parte, um pedaço do disco que se comporta como se fosse uma unidade de armazenamento separada. Por exemplo, em um disco de 4Gb, posso criar duas partições de 2Gb, que na pratica se comportam como se fossem dois discos de 2Gb independentes. Em um disco com armazenamento básico, é possível ter Partições primárias, partições estendidas e unidades lógicas.

A figura abaixo ilustra a tela do Windows no momento de configuração de um disco básico:

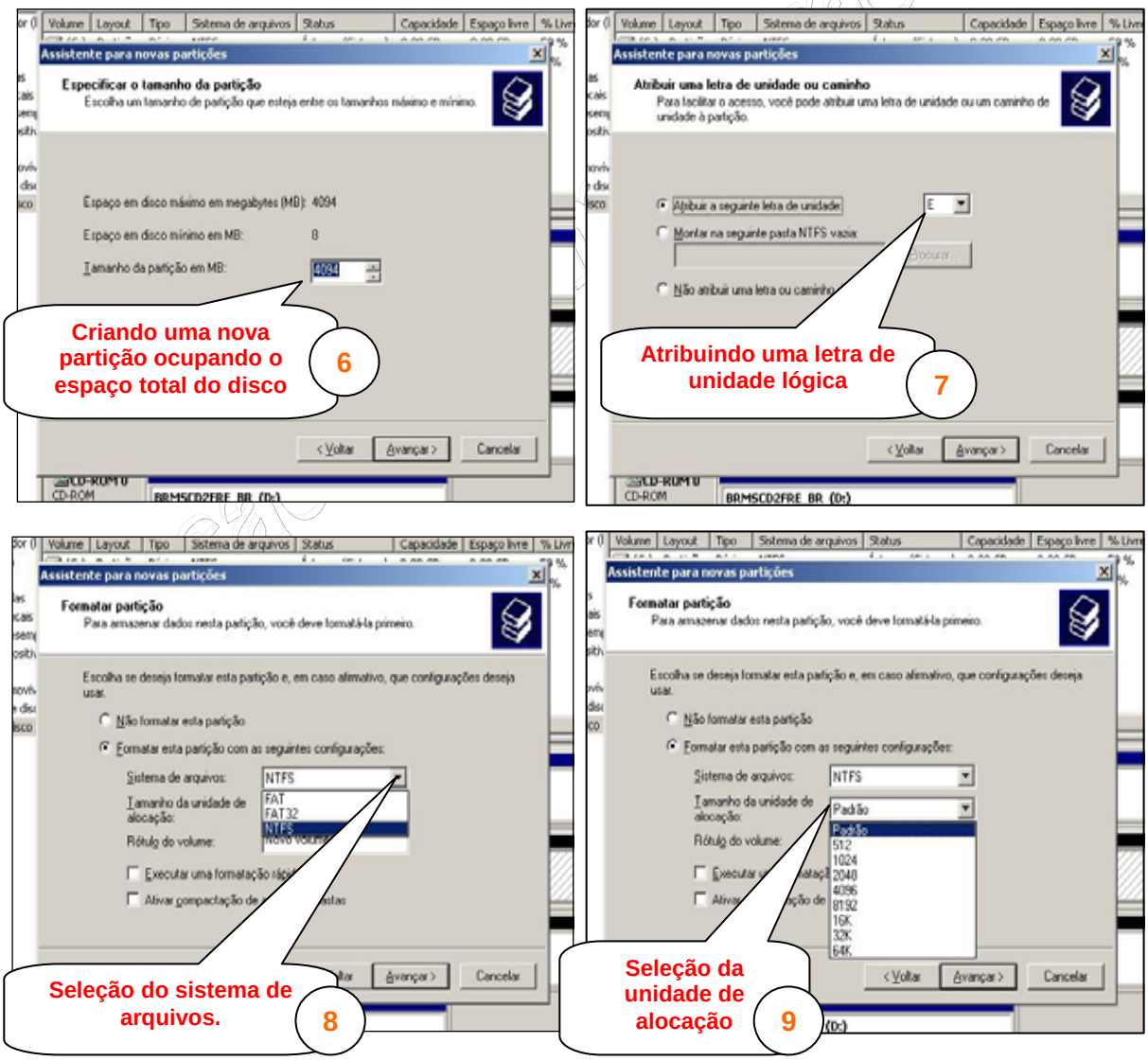
- Partição Primária: O Windows Server 2003 pode utilizar uma partição primária para inicializar o computador, sendo que somente partições primárias podem ser marcadas como ativas. Uma partição ativa é onde o computador procura pelos arquivos de inicialização para efetuar o processo de boot do Sistema Operacional. Um disco básico somente pode possuir uma única partição marcada como ativa, e conter no máximo quatro partições primárias. O assistente abaixo mostra como criar uma segunda partição primária, em um disco básico 1, onde no disco básico 0 já se encontra a partição primária ativa:



O número de partições que você pode criar em um disco básico depende do estilo de partição do disco:

- Em discos de registro de inicialização principal (MBR), todos os computadores baseados no Intel x86 (ou mais conhecidos como plataformas de 16 e 32 bits), você pode criar até quatro partições primárias por disco ou até três partições primárias e uma partição estendida. Na partição estendida você pode criar unidades lógicas ilimitadas;
- Em discos de tabela de partição GUID (GPT), para plataformas de 64 bits, você pode criar até 128 partições primárias. Como os discos GPT não limitam a quatro partições, não é necessário criar partições estendidas ou unidades lógicas.

Os próximos passos no assistente são: definição do tamanho da partição, atribuição de uma letra ao volume, seleção do sistema de arquivos da partição e seleção do tamanho da unidade de alocação:



A seleção do sistema de arquivos envolve uma das três opções possíveis: FAT (geralmente utilizada por dispositivos móveis como pendrivers e câmeras digitais até 4 Gb), FAT32 (versão melhorada da FAT e que suporta tamanhos de partições acima de 4 Gb e até 32 Gb), NTFS (padrão para sistemas operacionais Windows, a partir do Windows 2000, não possui na prática limites de tamanho). O NTFS é a opção mais recomendada na maioria das situações. Vejamos um comparativo entre estes três sistemas de arquivos:

O NTFS (NT File System ou Sistema de Arquivos do Windows NT) sempre foi um sistema de arquivos mais poderoso do que o FAT (tabela de alocação de arquivos) e FAT32 (tabela de alocação de arquivos de 32 bits). O Windows 2000, o Windows XP e a família de produtos Windows Server 2003 incluem uma nova versão do NTFS, com suporte a vários recursos, incluindo o Active Directory, que é necessário para domínios, contas de usuário e outros recursos de segurança importantes.

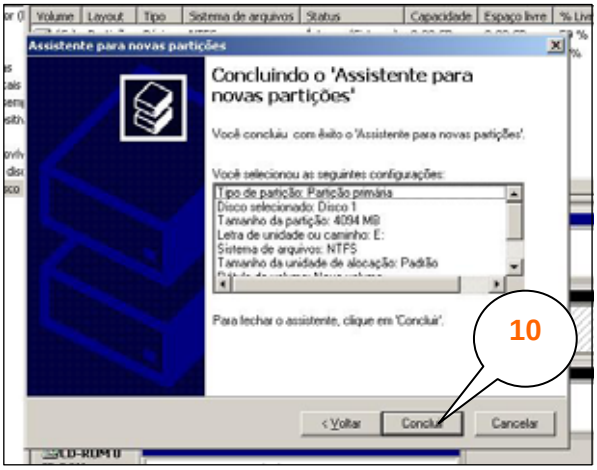
NTFS	FAT	FAT32
Um computador que execute o Windows 2000, o Windows XP ou um produto da família Windows Server 2003 pode acessar arquivos em uma partição NTFS local. Um computador que executa o Windows NT 4.0 com Service Pack 5 ou posterior pode ter acesso a alguns arquivos. Outros sistemas operacionais não permitem acesso local.	O acesso a arquivos em uma partição local está disponível através de MS-DOS, todas as versões do Windows e OS/2.	O acesso a arquivos em uma partição local está disponível somente através do Windows 95 OSR2, Windows 98, Windows Millennium Edition, Windows 2000, Windows XP e produtos da família Windows Server 2003.

Uma observação importe a cerca dos sistemas de arquivos e uso das redes. Em rede, podem haver computadores com FAT, FAT32, NTFS ou qualquer outro tipo de sistema de arquivos. O protocolo da rede, geralmente o TCP/IP, é o responsável por converter do sistema de arquivos nativo para uma linguagem universal. Dessa forma, qualquer computador que tenha o TCP/IP instalado pode conversar em rede independente do seu tipo de sistema de arquivos.

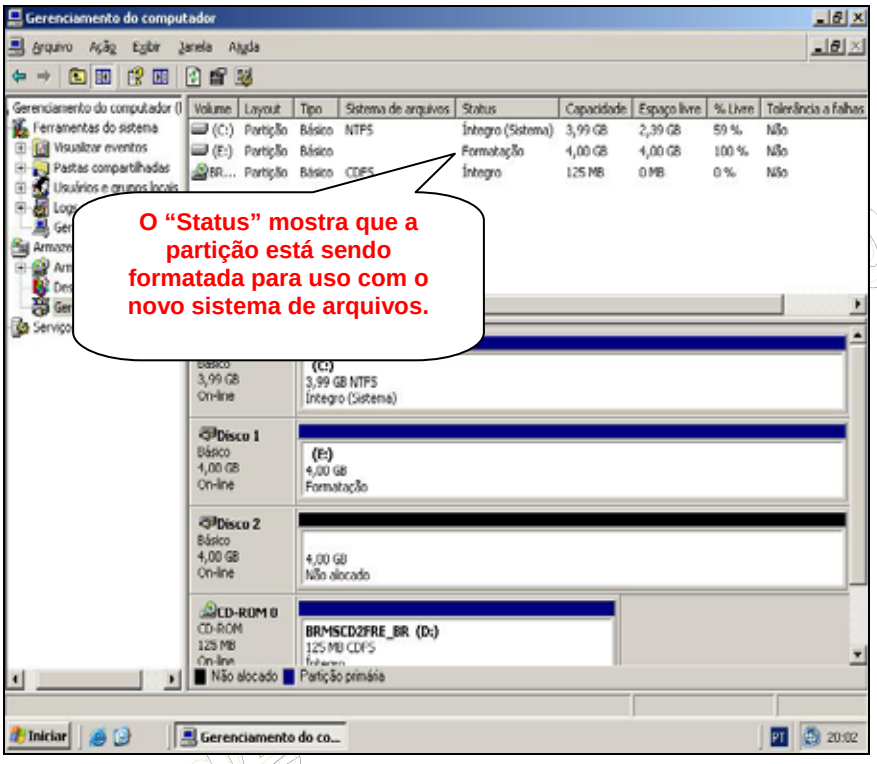
Por fim a escolha do tamanho da unidade de alocação implica no espaço ocupado em disco. A escolha de tamanhos pequenos, como 512 bits significa que cada arquivo no computador será alocado em disco através de blocos de 512 bits, ou seja, um arquivo de 1K ocupará dois blocos de 512 bits, enquanto que arquivos de 2 bits ocuparão os mesmos 512 bits de espaço em disco. A vantagem deste esquema é que nos dias atuais dificilmente você terá arquivos menores que 512 bits, por sua vez, este esquema apresenta a desvantagem de fragmentar muito o disco, e tornar seu desempenho lento, visto que a agulha terá que percorrer diversos blocos minúsculos atrás de informações.

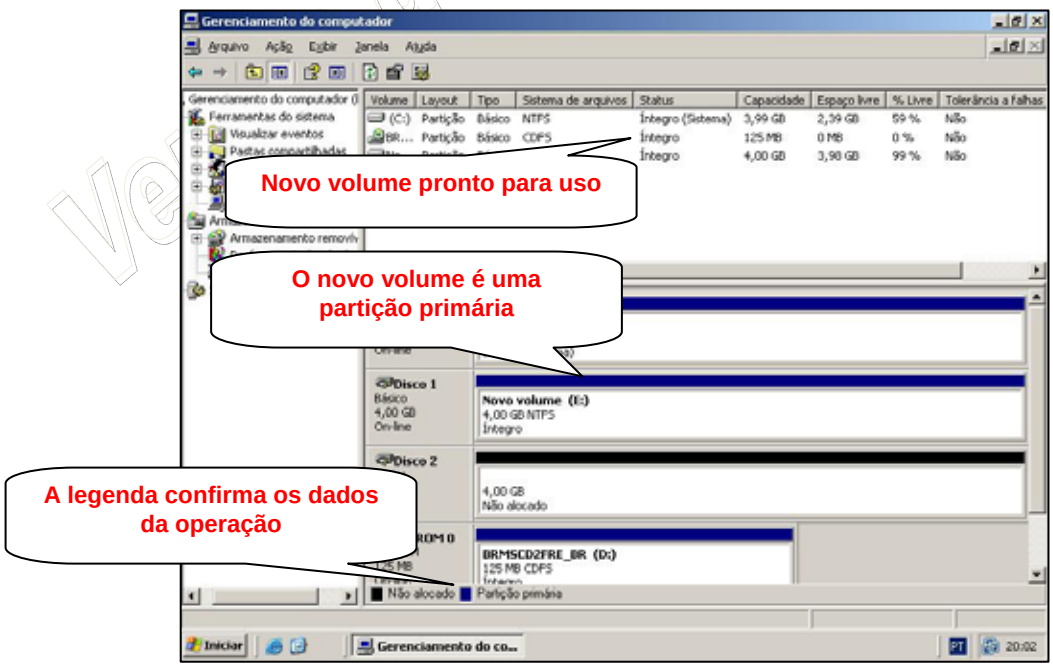
Já, para a escolha de blocos grandes, como 64000 bits, se seu computador possuir muitos arquivos pequenos (menores de 64k), você estará desperdiçando espaço em disco, por outro lado, como os blocos são maiores, o desempenho também aumenta proporcionalmente. O padrão do Windows Server 2003 é o tamanho de 1024 bits, ou 1k, faça a seguinte experiência para descobrir o tamanho de alocação do seu sistema operacional: através de um editor de texto simples, como o notepad, crie um arquivo com apenas um único caracter, um “.” por exemplo. Salve este arquivo em disco e via o Windows Explorer verifique o tamanho do arquivo. O tamanho exibido corresponde ao tamanho da sua unidade de alocação.

A seguir apresentamos o resumo do assistente de criação da partição primária em um segundo disco físico:

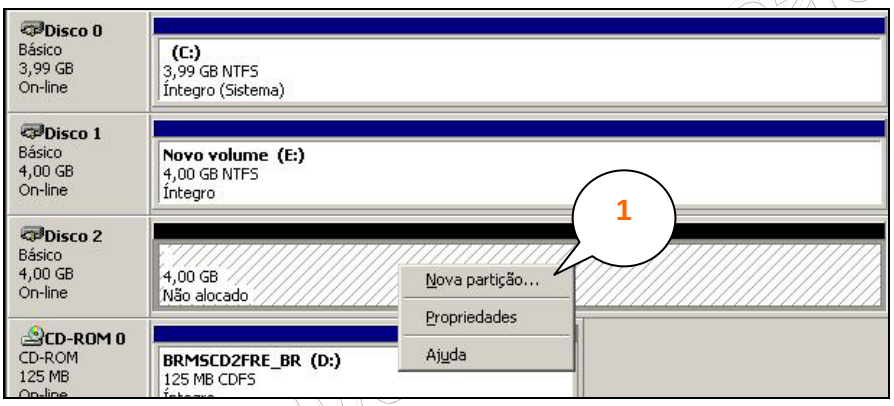


Uma vez concluído o assistente o Windows irá formatar a nova partição. Concluída esta etapa final o “status” do volume passará para “Íntegro” informando que a nova unidade encontra-se pronta para uso:

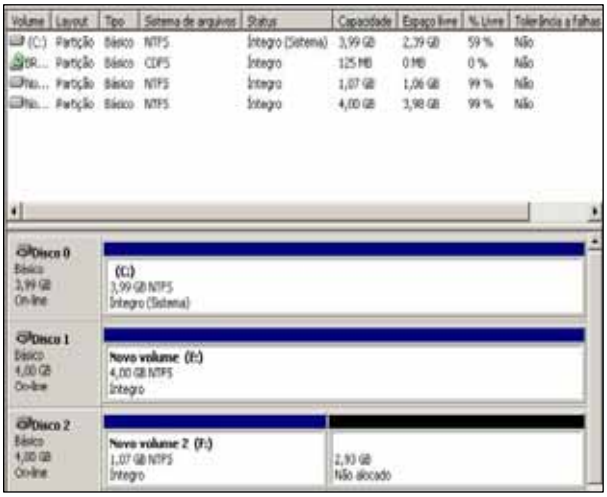




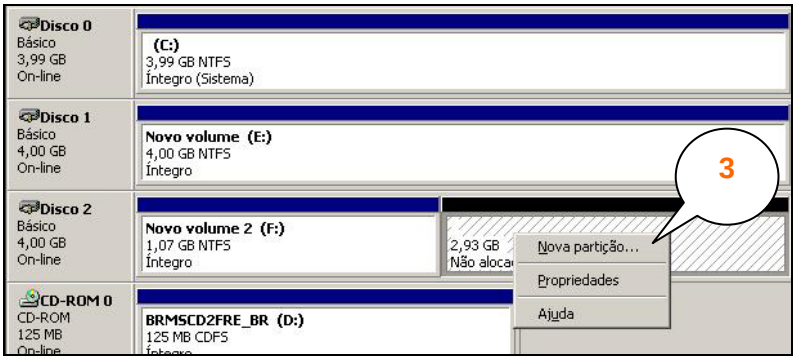
- Partição Estendida: Apenas uma partição estendida pode ser criada em um disco básico. Partições estendidas são criadas a partir do espaço livre no disco básico. Espaço livre é o espaço que não está sendo ocupado por nenhuma partição. Por isso é aconselhável, quando da criação de uma partição estendida, que todo o espaço livre seja ocupado. A partição estendida é dividida em segmentos, sendo que cada segmento representará uma unidade lógica. Deve ser atribuída uma letra para cada unidade lógica e esta deve ser formatada com um sistema de arquivos – FAT, FAT32, NTFS ou NTFS 5. Com o uso de uma partição estendida e unidades lógicas, é possível superar o limite de quatro unidades por disco, que é imposto quando se utiliza apenas partições primárias. O esquema a seguir demonstra como criar em um único disco físico sete unidades lógicas, através da criação de uma partição primária, seguida por uma partição estendida, e dentro da partição estendida a criação de seis unidades lógicas estendidas:

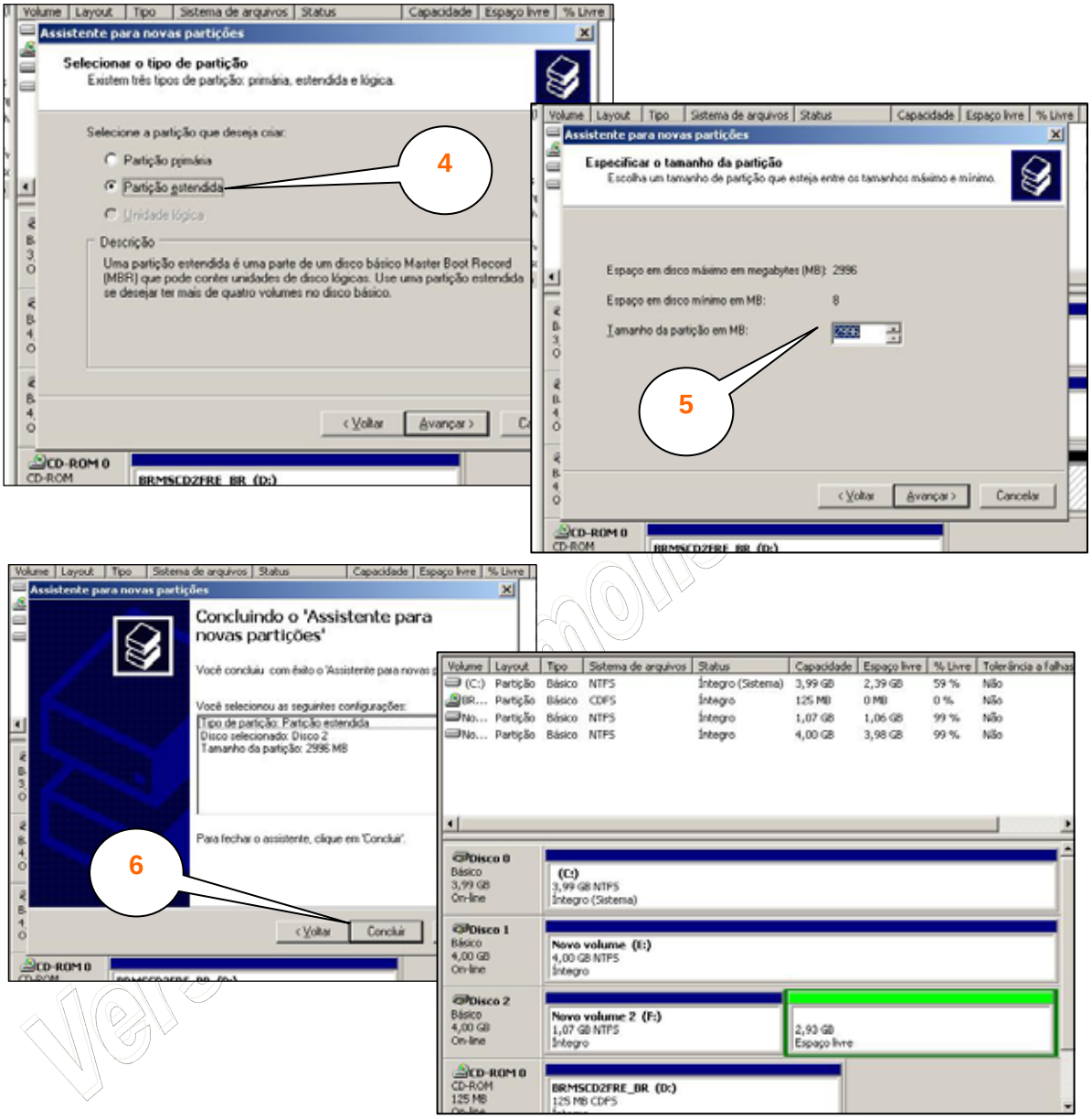


No terceiro disco físico, ou Disco Básico 2, iremos criar uma nova partição primária, mas desta vez não utilizando todo o espaço do disco:

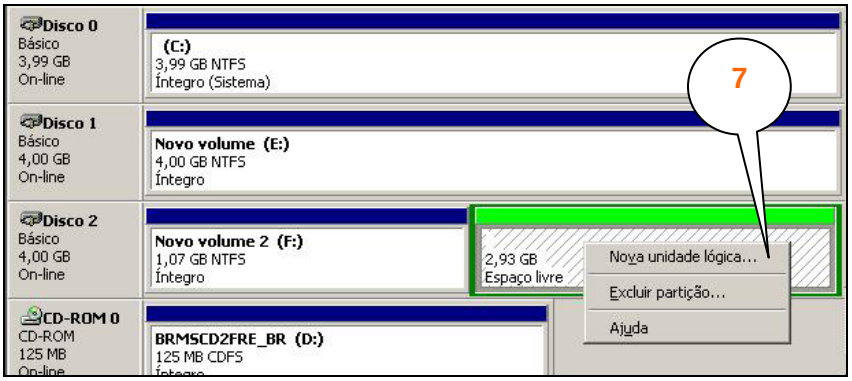


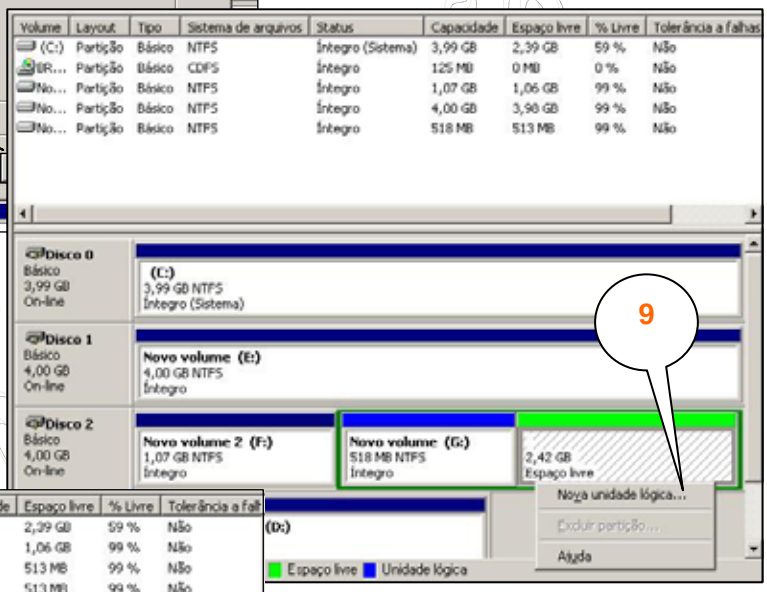
No espaço restante, não alocado, iremos agora criar a partição estendida, ocupando todo o restante do disco:



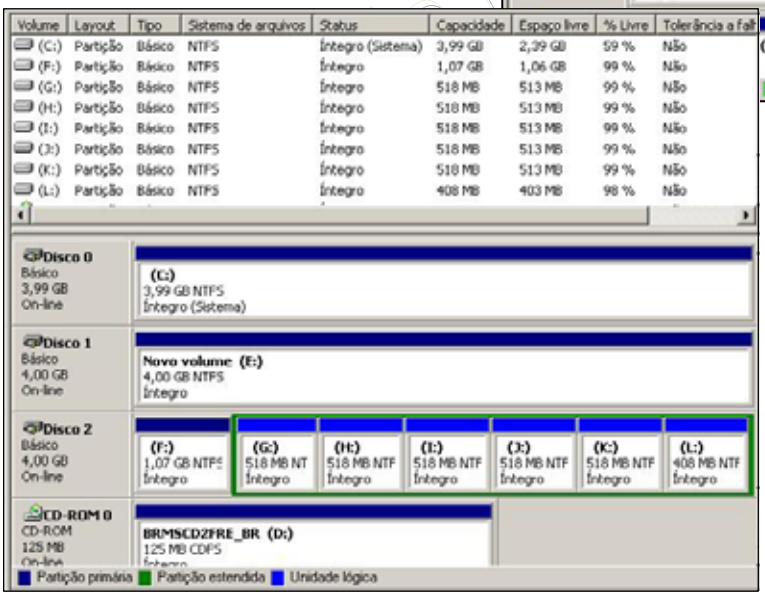


E finalmente criaremos as seis unidades lógicas restantes:

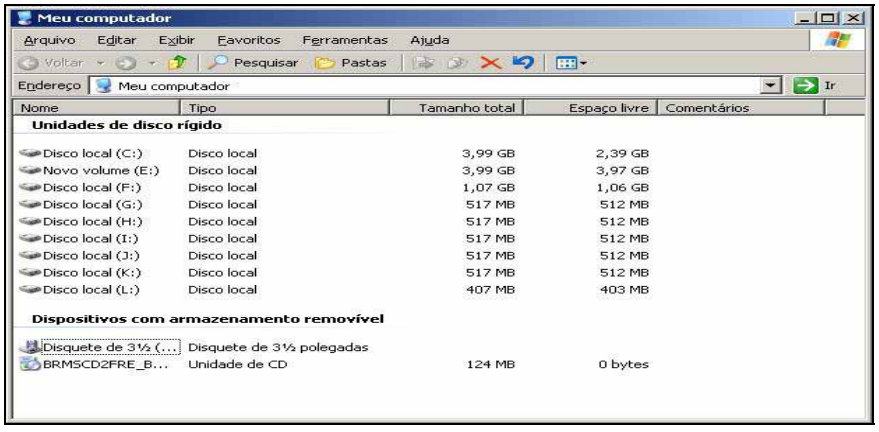




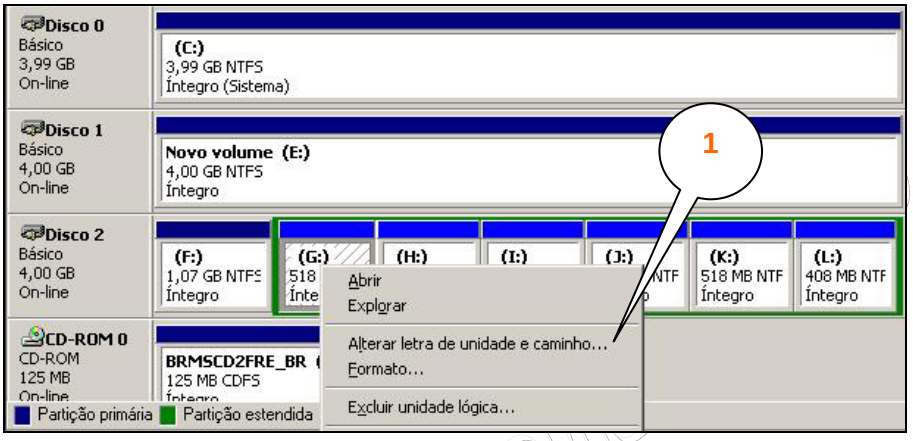
Iremos repetir o processo de criação das unidades lógicas por seis vezes iguais, como mostra a figura ao lado. Ao final das seis interações nosso sistema ficará conforme a imagem abaixo:



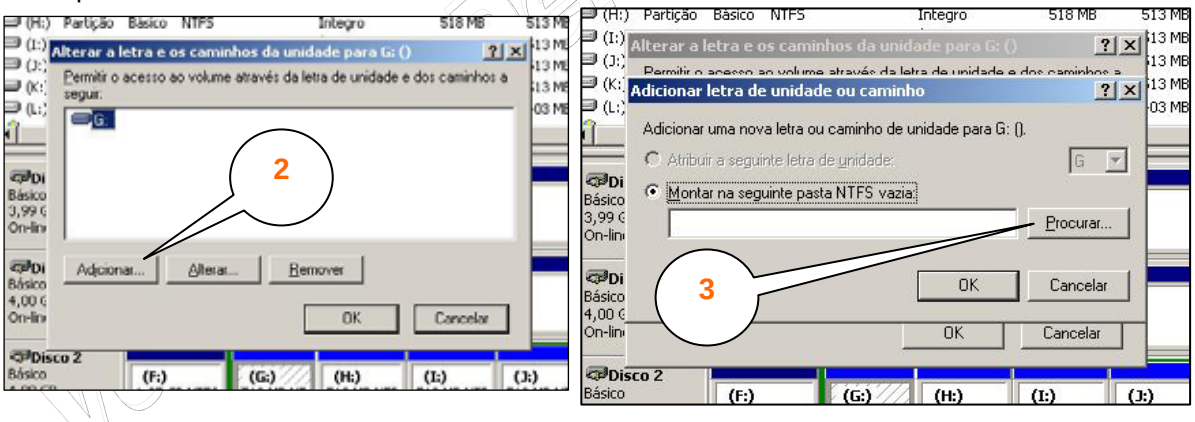
Por fim teremos no disco básico 2: uma partição primária C:, não ativa por não conter o sistema operacional e uma partição estendida contendo seis unidades lógicas. Para visualizar na prática estes esquemas abra o “Meu Computador” e visualize todas as unidades criadas até o momento:

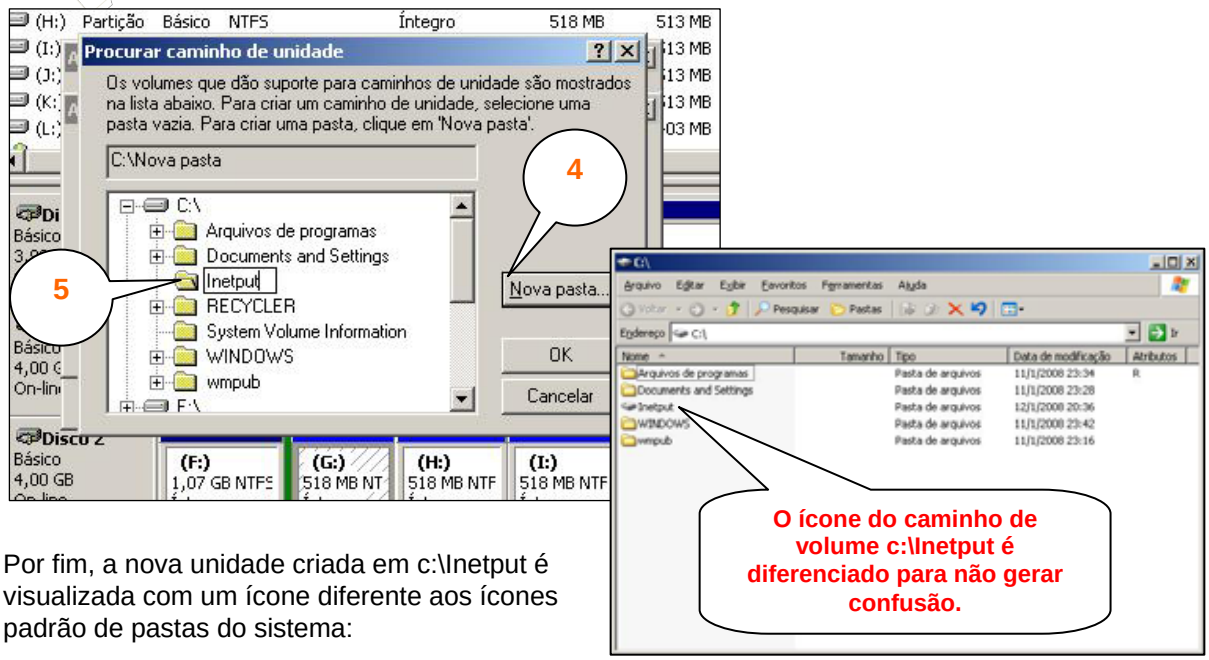


No Windows, uma alternativa prática ao uso de letras para acesso as unidades é a criação de caminhos, ou PATH, dentro do próprio sistema operacional. Por exemplo, vamos supor que estejamos criando um servidor WEB neste nosso Windows Server 2003. Para disponibilizar um disco físico exclusivo para os dados deste servidor, sem precisar alterar as configurações padrões do servidor Web, estabelecesse um caminho de unidade para a pasta física dos dados. Vejamos:



Vamos alterar as configurações da partição já existente G: de forma que a criar um caminho de acesso alternativo, do tipo c:\Inetpub. Ou seja, para acessar o disco básico 2, em sua unidade lógica G:, a partir do volume C:, basta acessar a pasta c:\Inetput. Todos os dados dentro de c:\Inetput estarão na verdade dentro de G:





Por fim, a nova unidade criada em c:\Inetput é visualizada com um ícone diferente aos ícones padrão de pastas do sistema:

Para o Windows Server 2003 existem duas partições que são muito importantes. A Partição do Sistema – System Partition, é a partição ativa, a qual contém os arquivos necessários para o processo de boot do Windows Server 2003 (normalmente é a primeira partição ativa do primeiro disco). A partiçãode boot – Boot Partition, é uma partição primária, ou um drive lógico, onde estão instalados os arquivos do Windows Server 2003, normalmente em uma pasta chamada WinNT ou Windows. Muitas vezes estes conceitos causam uma certa confusão, porque podemos dizer que a "Partição do Sistema contém os arquivos de boot e a Partição de boot contém os arquivos do Sistema Operacional". Normalmente a Partição de Sistema e a Partição de Boot estão na mesma partição, tipicamente no drive C:.

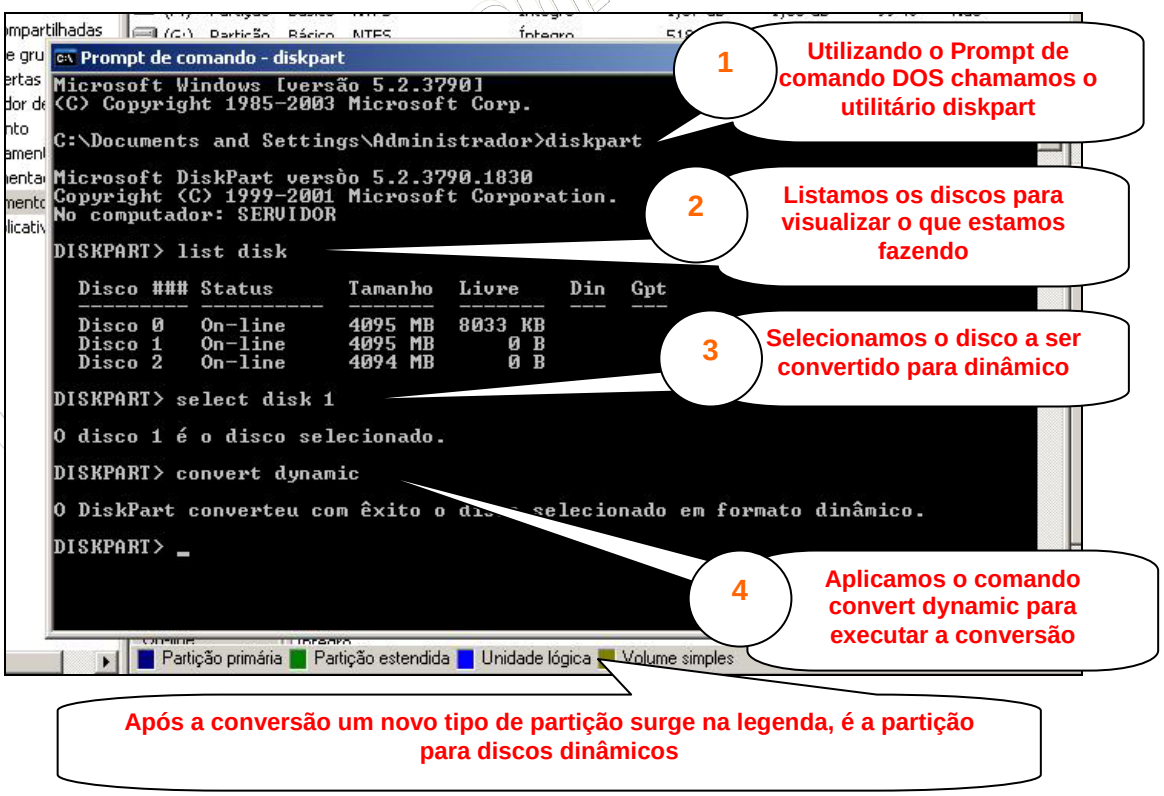
O Windows Server 2003 dá suporte ao gerenciamento de discos realizado através de controladoras externas. Controladoras externas são placas do tipo PCI ao qual os HD´s são conectados, ao invés dos tradicionais IDE ou SATA, atualmente algumas placas mães já vêem de fábrica com controladoras externas onboard, onde suas configurações podem ser acessadas através da própria BIOS do computador ou com um disco de boot específico. Através dessas controladoras externas é possível criar novas formas de partição para discos básicos. Dependendo da maneira com que as partições são criadas ou combinadas, podem existir diversos tipos de partições em um disco de armazenamento básico, conforme descrito a seguir:

- Partição de Sistema: Contém os arquivos necessários para o boot do Windows Server 2003, padrão dos discos básicos, mesmo sem a presença de controladoras externas;
- Partição de Boot: Contém os arquivos do Windows Server 2003, tipicamente em uma pasta WinNT ou Windows, também padrão para qualquer estilo de disco básico;
- Volume Set: Para criar um Volume Set é necessário o uso de uma controladora externa. Utiliza-se o espaço de duas ou mais partições, no mesmo disco ou em discos diferentes e de mesmo tamanho ou de tamanhos diferentes, de tal forma que estas partições, sejam visualizadas pelo Windows Server 2003 como uma única unidade. Por exemplo, podemos combinar uma partição de 1 Gb do disco básico 1 com outra de 4 Gb do disco básico 2, para formar uma unidade de 5Gb. Podemos aumentar o tamanho sem que haja perda de dados. É possível usar até 32 partições para criar um Volume Set. O Windows Server 2003 preenche todo o espaço da primeira partição, depois o da segunda e assim por diante. Se uma das partições apresentar problemas, todo o Volume Set será perdido. Um Volume Set só não pode conter a Partição de Sistema, nem a Partição de Boot.
- Stripe Set - RAID-0: Para criar um Stripe Set combinam-se espaços iguais de dois ou mais discos. Não podem ser utilizadas duas partições do mesmo disco. Podendo ser utilizado até 32 partições. Os dados são gravados em todas as partições de uma maneira uniforme, isto é, o espaço de cada partição vai sendo preenchido a medida que os dados são gravados. Não apresenta tolerância a falhas, pois se uma das partições apresentar problemas, todo o Stripe Set será perdido. Uma das vantagens do Stripe Set é que o desempenho melhora devido as gravações simultâneas em mais de um disco. Não pode conter a Partição de Sistema, nem a Partição de Boot.
- Mirror Set – RAID 1: Permite a duplicação de uma partição em um disco básico. Com isso a medida que os dados vão sendo gravados, o Windows Server 2003, automaticamente vai duplicando os dados na partição espelhada. Pode conter a Partição de Sistema e também a Partição de Boot. O maior inconveniente é que existe um comprometimento de 50% do espaço em disco. Por exemplo, para fazer o espelhamento de uma partição de 2 Gb, serão necessários 4 Gb de espaço em disco (2Gb da partição original mais 2 Gb da partição espelhada). Apresenta tolerância a falhas, pois se uma das partições espelhadas falhar, a outra continua funcionando. O administrador pode substituir o disco defeituoso e restabelecer o espelhamento.

- Stripe Set com Paridade – RAID 5: Um Stripe Set com Paridade é um Stripe Set com tolerância a falhas. Junto com os dados, o Windows Server 2003 grava informações de paridade (obtidas a partir de cálculos matemáticos) nos vários discos que formam o Stripe Set com Paridade. Com isso, no evento de falha de um dos discos, toda a informação do disco com problemas, pode ser reconstituída a partir das informações de paridade dos outros discos. O disco defeituoso pode ser substituído e a informação nele contida pode ser recriada a partir da informação de paridade nos demais discos do RAID-5. Para que possa ser criada uma partição do tipo RAID-5, um mínimo de três discos é necessário. Porém se dois discos falharem, ao mesmo tempo, não será possível recuperar a informação. Também existem implementações de RAID-5 em hardware, que são mais rápidas, porém tem um custo maior.

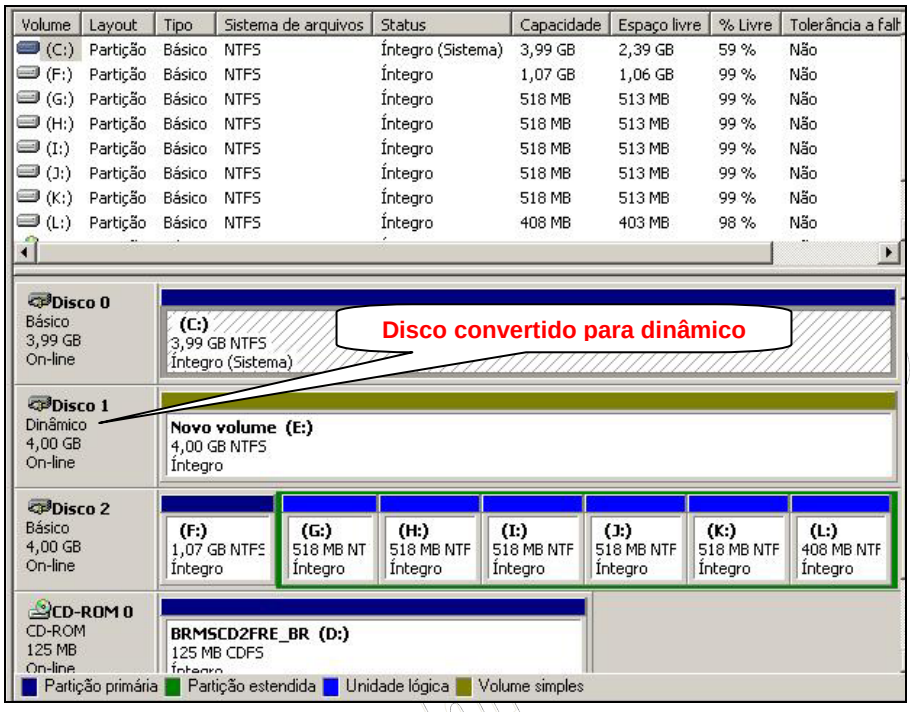
Armazenamento Dinâmico

No armazenamento dinâmico, é criada uma única partição com todo o espaço do disco. Um disco configurado com armazenamento dinâmico é chamado de Disco Dinâmico. Um disco dinâmico pode ser dividido em volumes. Um volume pode conter uma ou mais partes de um ou mais discos. Também é possível converter um disco básico para dinâmico, diretamente, sem perda de dados, veja o exemplo abaixo onde utilizamos o utilitário de linha de comando "diskpart" para converter os discos dos nossos exemplos anteriores para o formato de disco dinâmico:

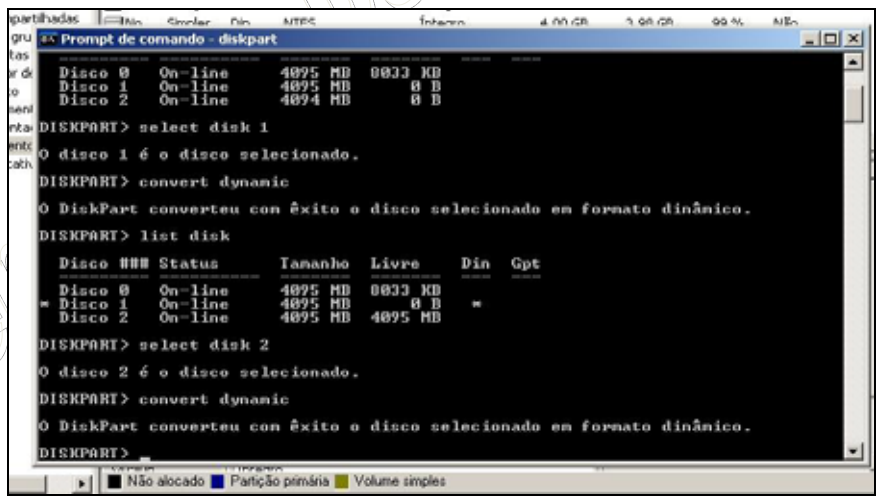


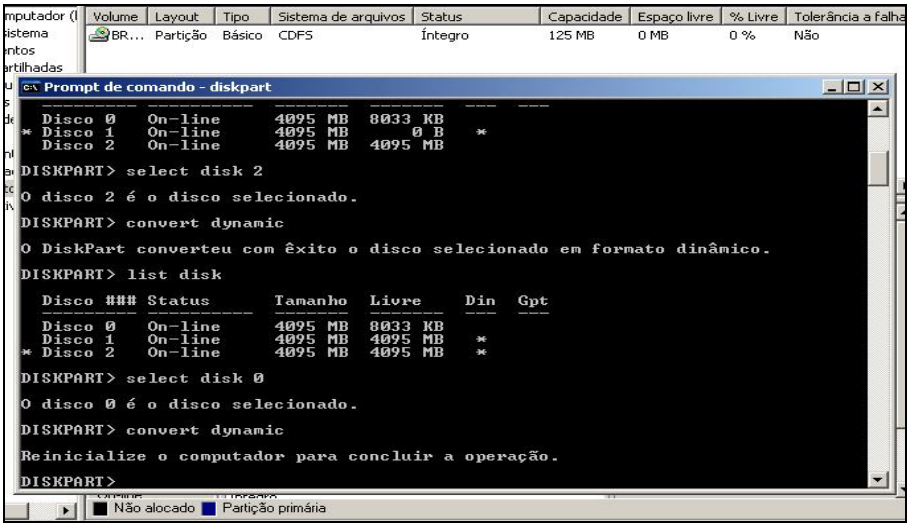
O volume criado foi do tipo simples, mas existem diferentes tipos de volumes. O tipo de volume a ser utilizado, é determinado por fatores como espaço disponível, performance e tolerância a falhas. A tolerância a falhas diz respeito a possibilidade do Windows Server 2003 manter as informações, mesmo no evento do comprometimento de um disco ou volume.

Na imagem a seguir apresentar o Gerenciador de discos após a conversão do disco básico 1 para disco dinâmico 1, ressaltando que a conversão não compromete os dados existentes, ou seja, a migração é realizada sem a necessidade de formatar a unidade:



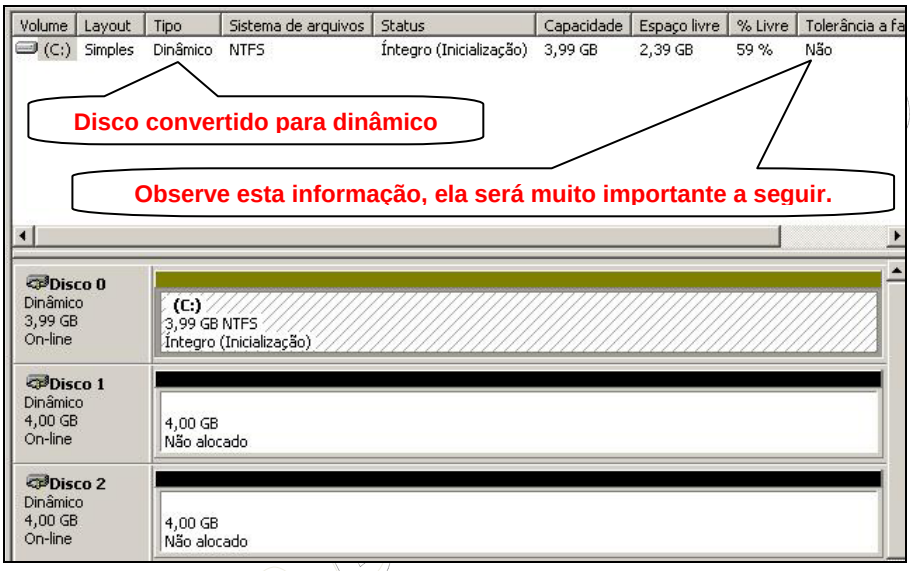
Podemos aproveitar também para converter os demais discos básicos para dinâmico, o mesmo procedimento utilizado no disco básico 1 será utilizado nos discos básicos 2 e 0, acompanhe:



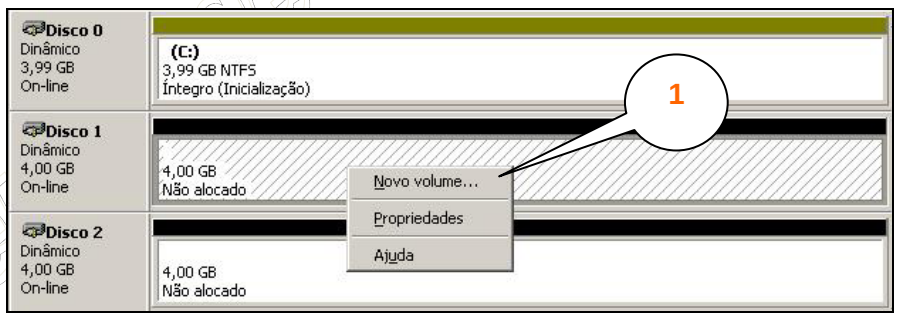


Se você observou bem, reparou que após a conversão do disco básico 2 em disco dinâmico 2 tudo ocorreu igualmente a conversão do disco básico 1 em disco dinâmico 1, porém a conversão do disco básico 0 em disco dinâmico 0 fez com que a tabela de partições desaparecesse do Gerenciador de discos, além de solicitar que o computador fosse reinicializado. Isso ocorre no disco básico 0 por ele ser a partição ativa, ou partição de sistema.

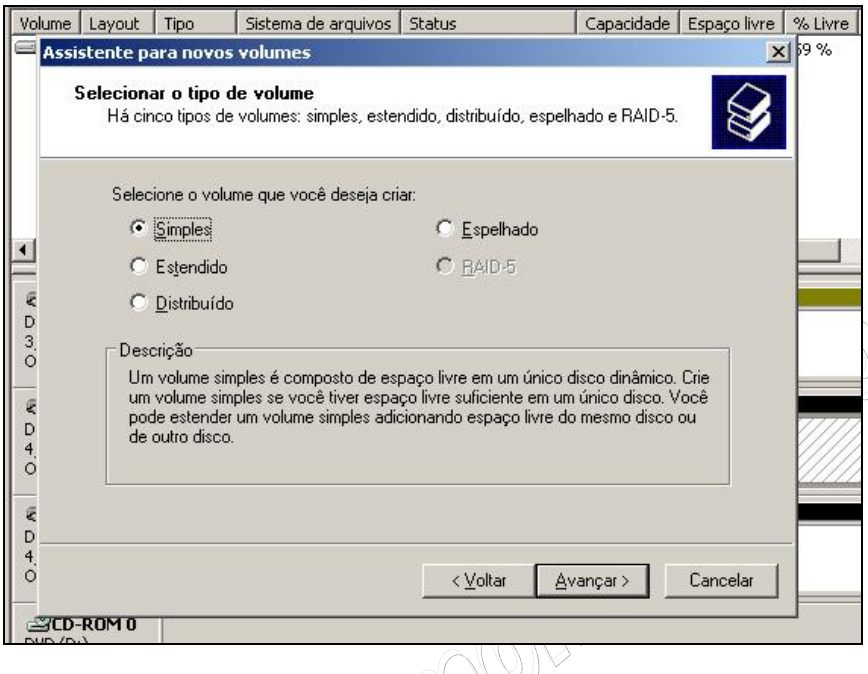
Após reinicializar o computador e excluir os volumes dos discos 1 e 2, nosso Gerenciador de discos fica da seguinte forma:



Em discos dinâmicos, com espaço não alocado, podem ser criados os seguintes tipos de volumes:

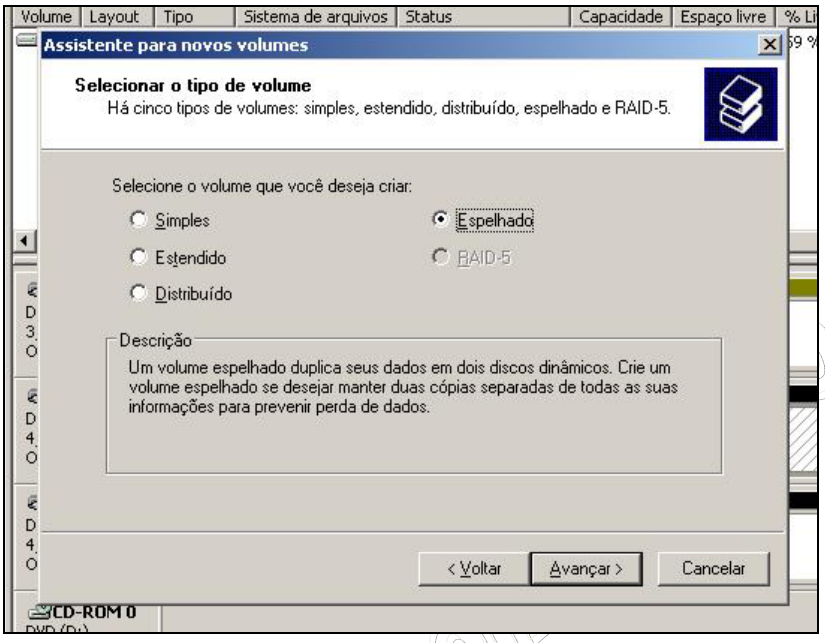


- Volume Simples: É criado usando todo ou parte do espaço de um único disco. Também pode ser criada usando duais ou mais partes de um mesmo disco dinâmico. Não fornece mecanismo de tolerância a falhas, isto é, se houver algum problema com o disco onde está o volume, toda a informação será perdida. O Windows Server 2003 pode ser instalado em um volume simples. Se o volume simples não for utilizado como volume do sistema (onde estão os arquivos de boot do Windows Server 2003) ou como volume de boot (onde estão os arquivos do Sistema Operacional), ele pode ser estendido (adicionadas novas porções) usando partes do mesmo disco ou de outros discos. Não é possível estender um volume simples se ele for o volume de boot ou o volume de sistema. Ao estender um volume simples, usando porções de dois ou mais discos, ele torna-se um Spanned Volume (Volume Estendido).

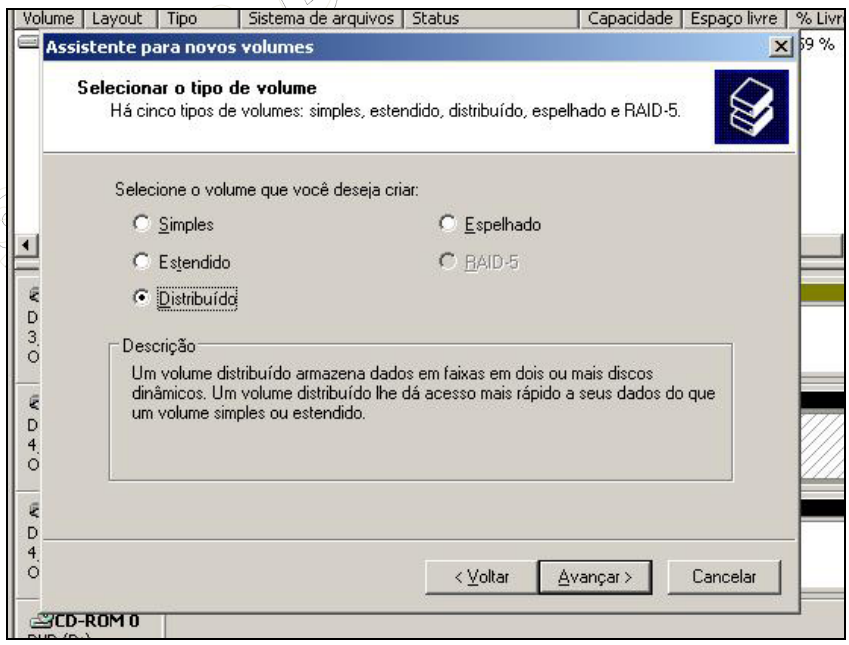


- Volume Estendido: Pode incluir o espaço de até 32 discos. O Windows Server 2003 começa a preencher o espaço do primeiro disco, após este estar esgotado, passa para o espaço disponível no segundo disco e assim por diante. Não fornece nenhum mecanismo de tolerância a falhas. Se um dos discos que formam o volume apresentar problemas, todo o volume estará comprometido. Também não oferece melhoria no desempenho, uma vez que a informação somente é gravada ou lida em um disco ao mesmo tempo.

- Volume Espelhado (Mirrored Volume): É formado por duas cópias idênticas do mesmo volume, sendo que as cópias são mantidas em discos separados. Volumes espelhados oferecem proteção contra falha, uma vez que se um dos discos falhar, a informação do outro disco pode ser utilizada. O espelhamento pode ser desfeito, o disco defeituoso substituído e o espelhamento pode ser refeito. O único inconveniente é que devido a duplicidade das informações, o espaço de armazenamento necessário é exatamente o dobro. Por exemplo, para espelhar um volume de 10Gb você precisará de um espaço adicional de 10Gb em outro disco rígido. Ou seja, para 10 Gb de informações você utiliza 20 Gb, sendo os 10 Gb adicionais para o espelhamento.

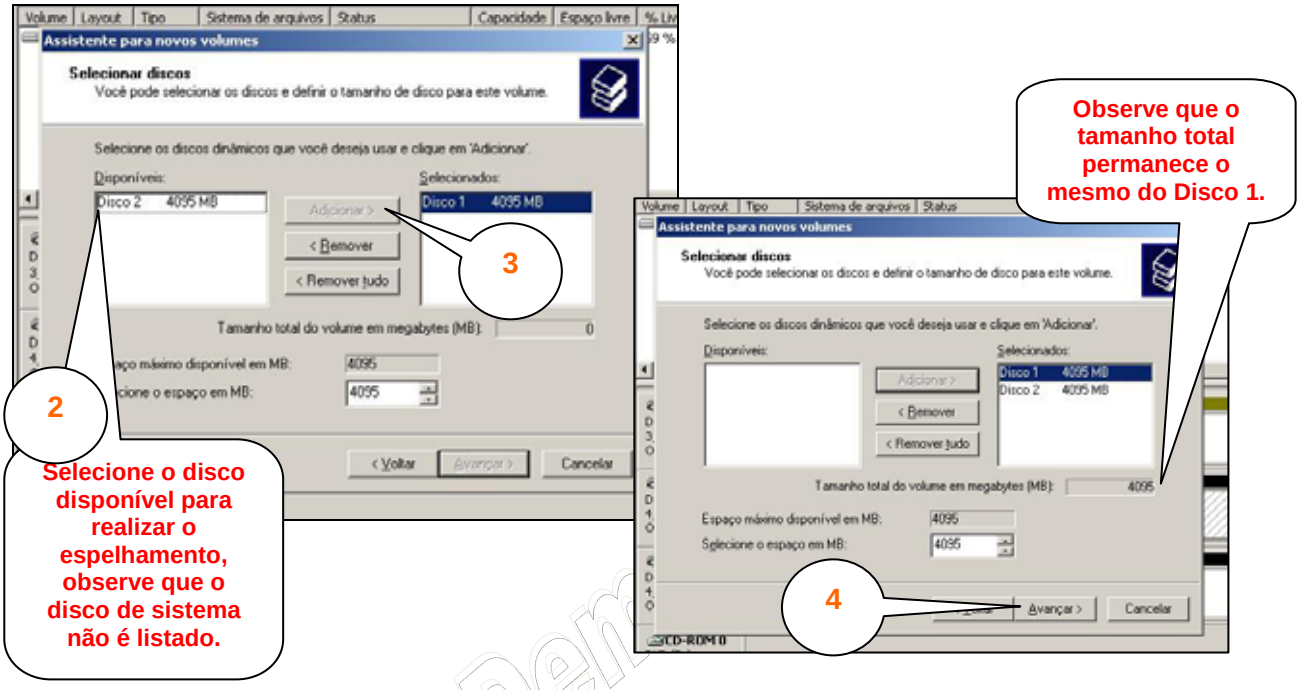


- Volume Distribuído: Podem ser combinadas áreas de espaço livre de até 32 discos. Não apresentam nenhum mecanismo de tolerância a falhas, pois se um dos discos do Striped Volume falhar, toda a informação estará comprometida. Uma das vantagens é que o desempenho melhora, uma vez que as informações são gravadas nos diversos discos ao mesmo tempo.

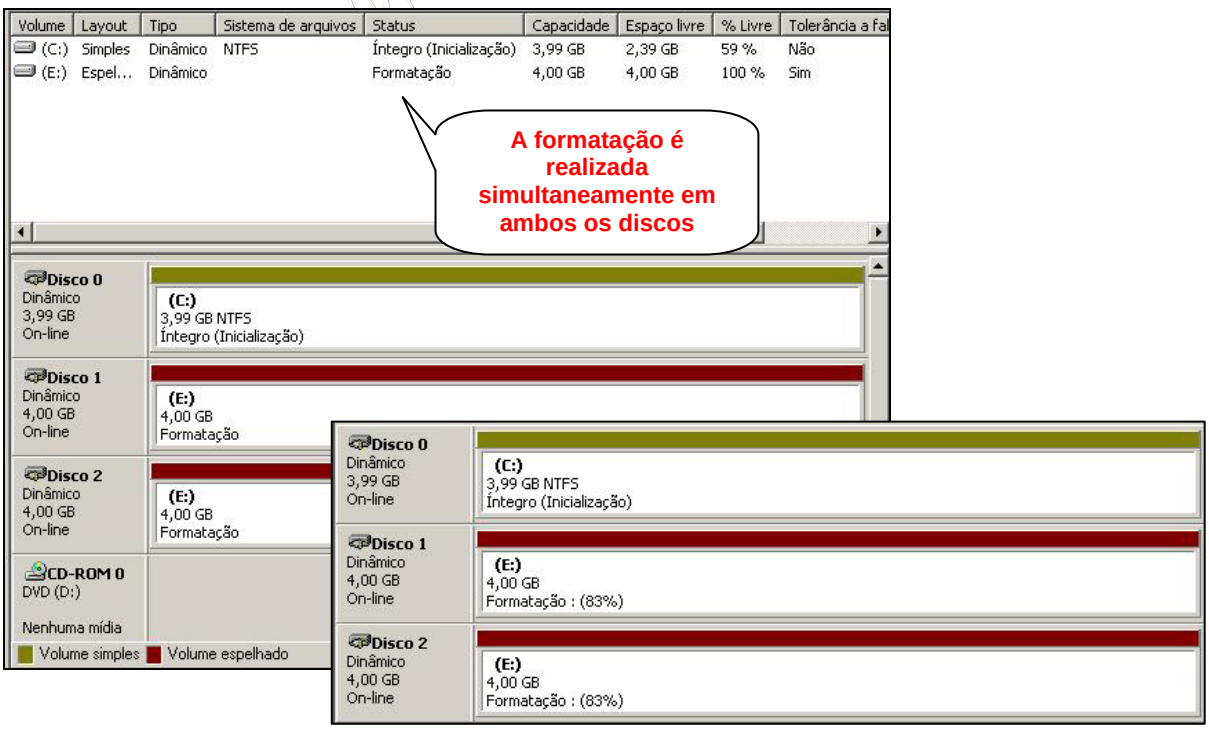


- Volume do Tipo RAID-5: Um Volume do Tipo RAID-5 é um volume distribuído, porém com tolerância a falhas. Junto com os dados, o Windows Server 2003 grava informações de paridade (obtidas a partir de cálculos matemáticos) nos vários discos que formam o volume do tipo RAID-5. Com isso, no evento de falha de um dos discos, toda a informação do disco com problemas, pode ser reconstruída a partir das informações de paridade, contida nos demais discos do volume RAID-5. Para que você possa criar um volume do tipo RAID-5, é necessário espaço disponível em, pelo menos, três discos físicos diferentes. O mecanismo de tolerância a falhas restringe-se a falha de um dos discos do volume, se dois discos falharem ao mesmo tempo, não será possível recuperar os dados.

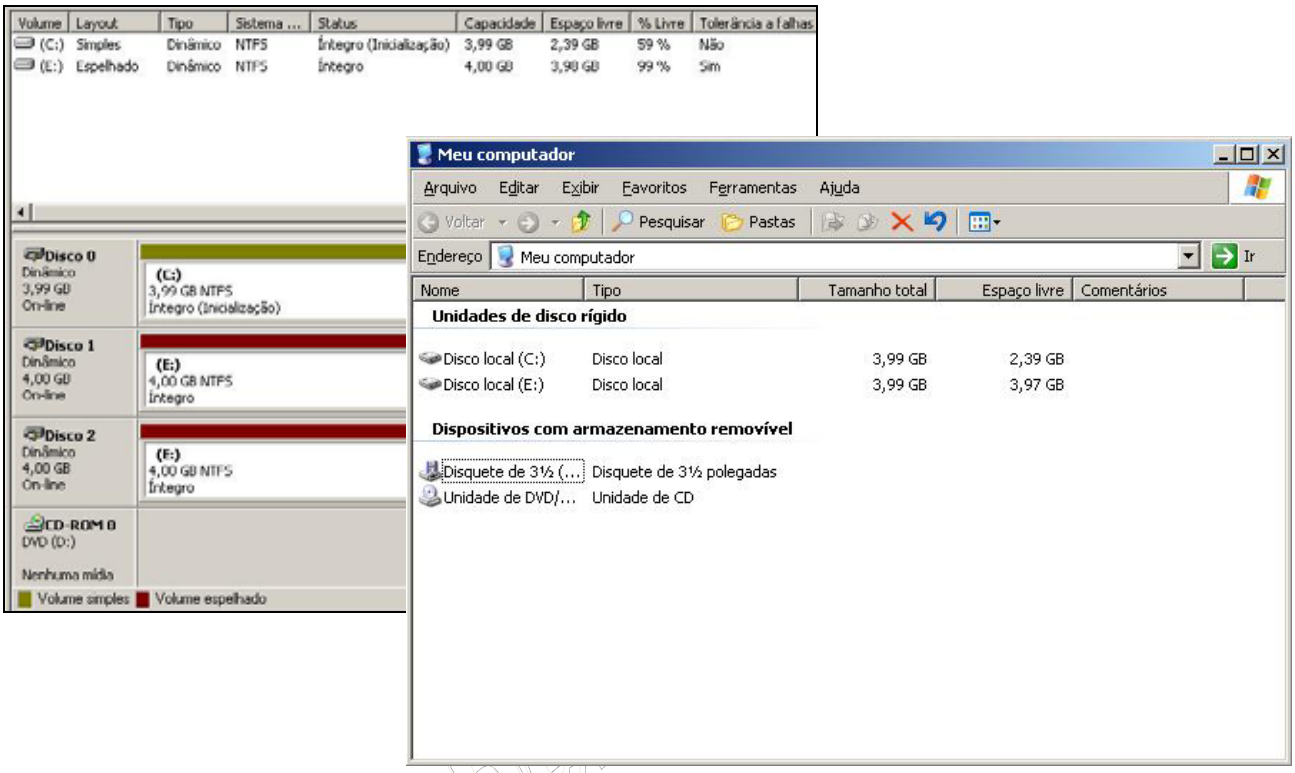
Vejamos como manusear cada um destes tipos de volumes dinâmicos. Começaremos pela criação de um volume espelhado, visto que o volume simples não possui novas informações:



Após a conclusão do assiste o Windows irá preencher todo o espaço em disco de ambos os discos selecionados e por fim uma sincronização, para garantir a geometria dos discos seja compatível com a matemática da partição:

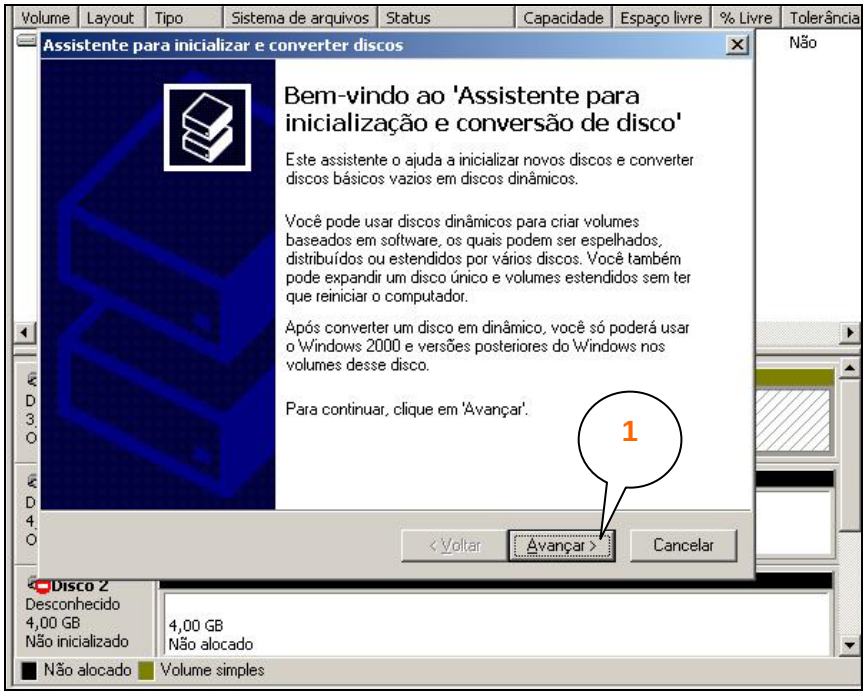


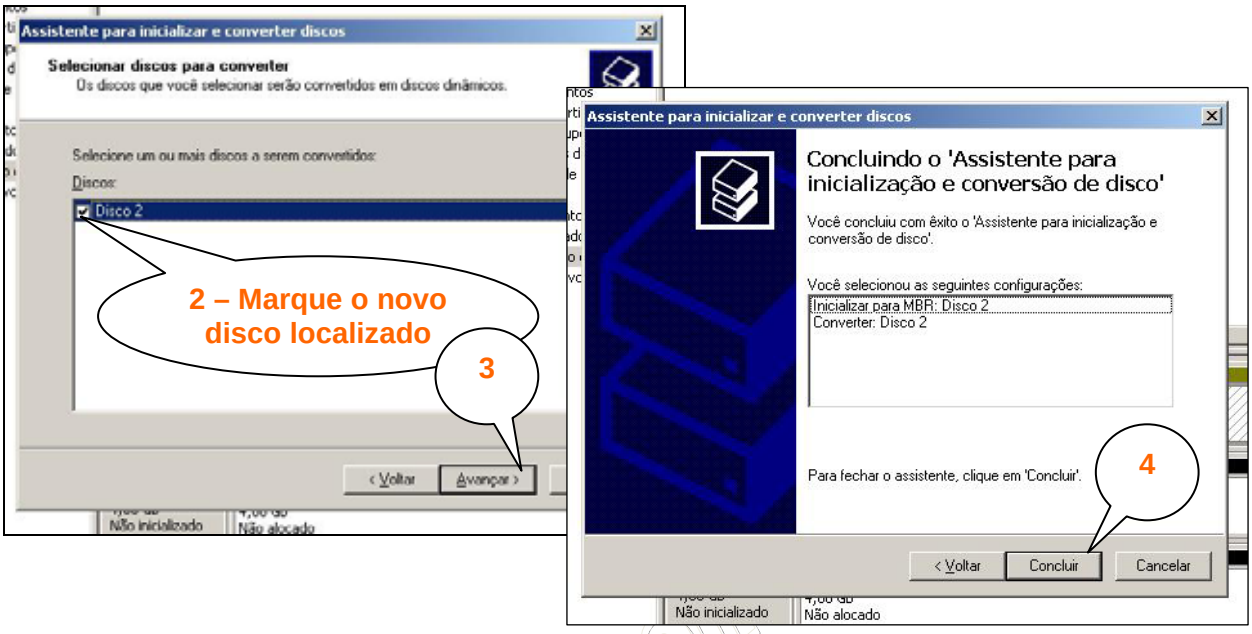
Após a formatação tanto o Gerenciador de discos quanto em “Meu Computador” apresentará a nova unidade E:, como sendo o espelhamento dos discos dinâmicos 1 e 2:



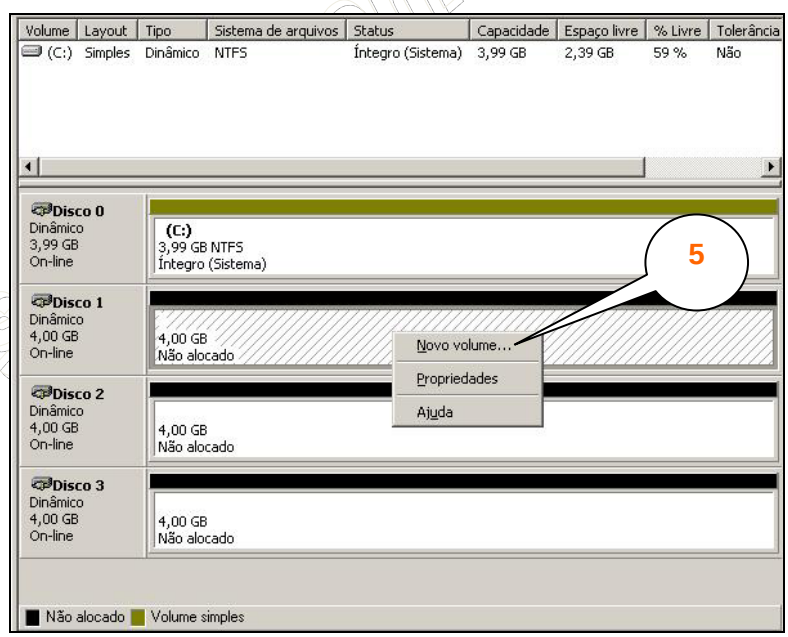
Demonstraremos agora a criação de sistemas RAID-5, um dos mais procurados por administradores de redes e sistemas por apresentar espelhamento com desempenho:

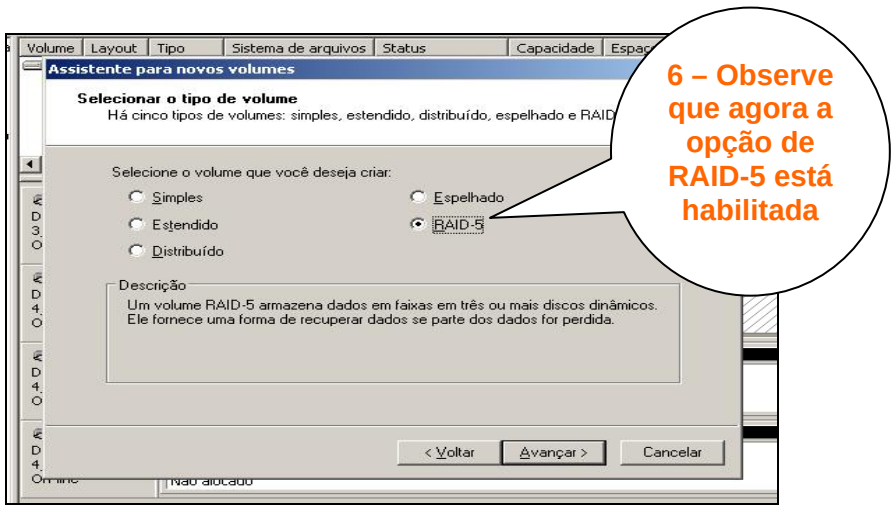
Para criar um sistema RAID-5 é necessário um mínimo de 03 discos físicos disponíveis, ou seja, que não tenham partições alocadas. Isso significa que criar um sistema RAID-5, via software do Windows Server 2003, implica que você não poderá incluir a partição de sistema (ou Inicialização). Para nosso exemplo acima não poderemos incluir uma partição RAID-5, a menos que adicionemos um novo disco físico, dessa forma foi adicionado um novo disco e reinicializado o computador, veja a tela de inicialização e conversão para disco dinâmico que o Windows apresenta assim que logamos no servidor:



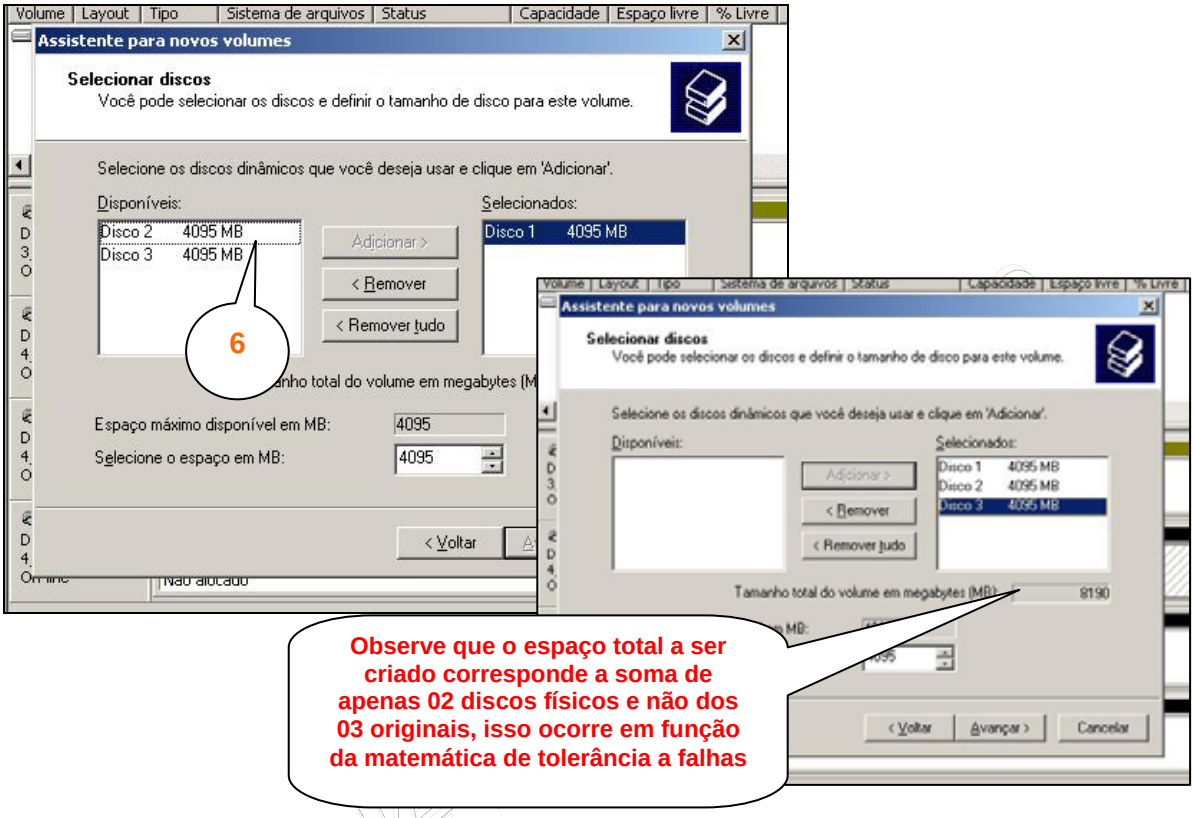


Agora que temos 04 discos físicos no computador, sendo um apenas para sistema, podemos realizar a conversão dos demais discos dinâmicos para o volume RAID-5:

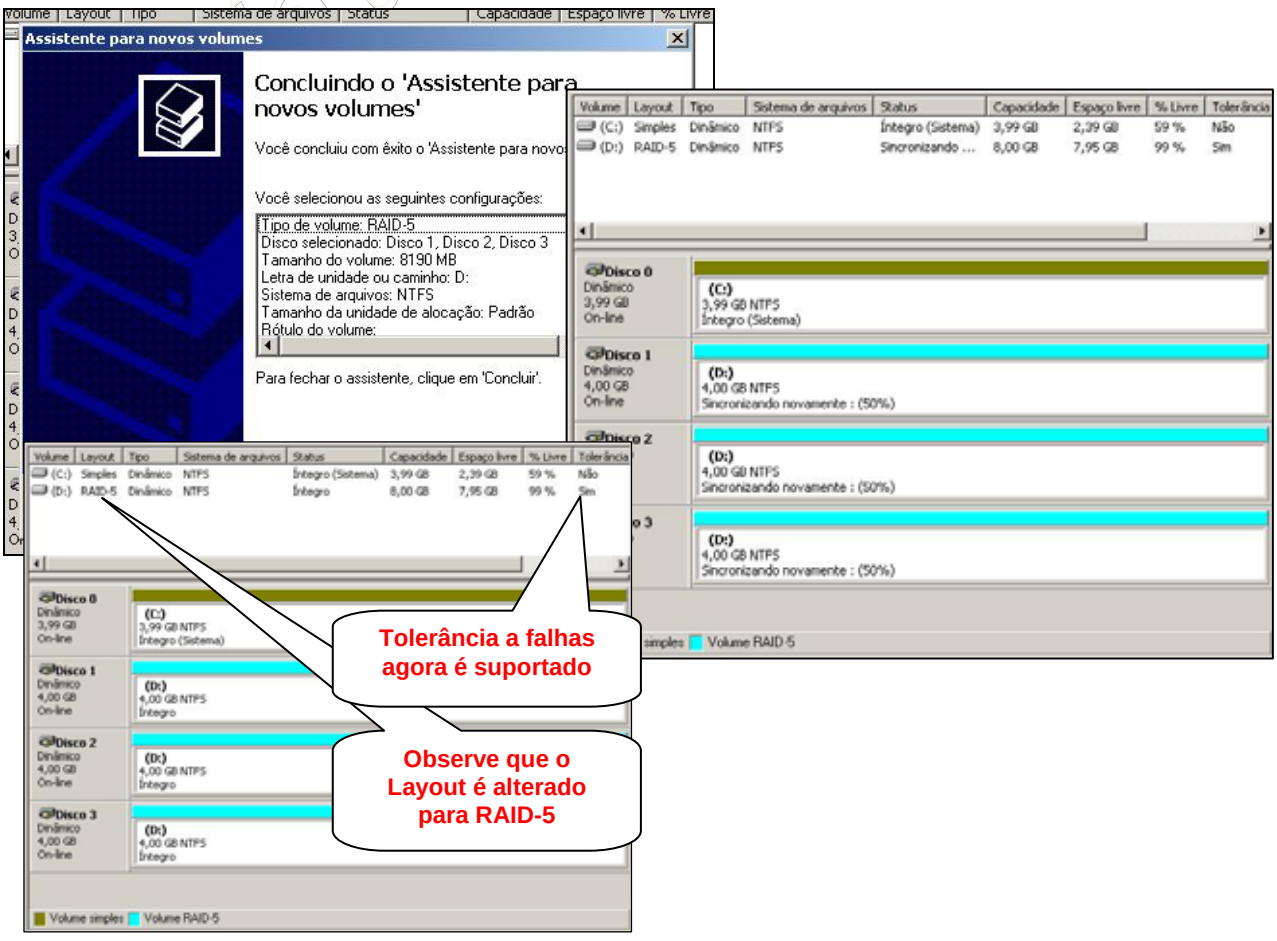




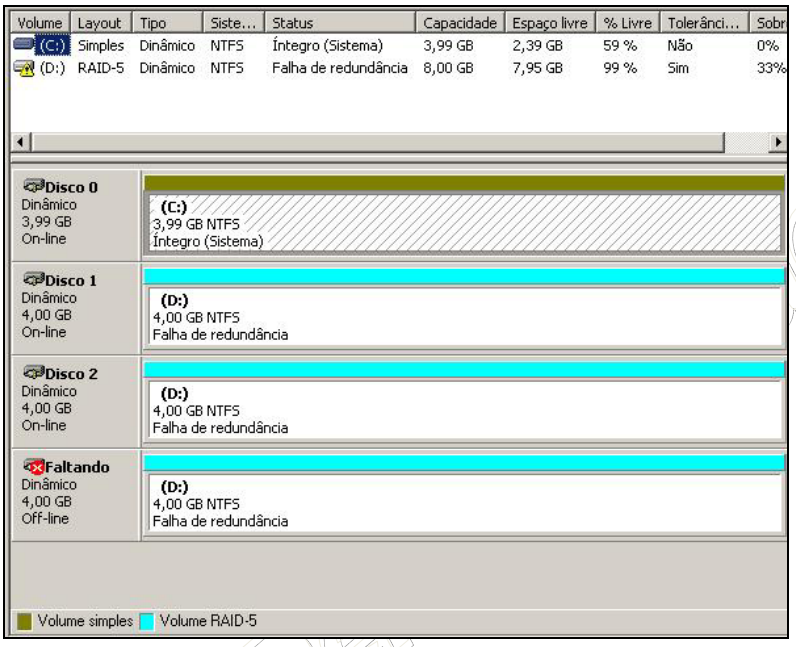
Selecione os discos que farão parte do RAID-5:



Uma vez concluído o assistente, e semelhante ao processo de espelhamento, o Windows irá preencher em sua totalidade as partições selecionadas para o RAID-5, formatar e sincronizar:



Uma curiosidade muito grande dos administradores de rede e sistemas é sobre “e quando um dos discos falha?”. A figura abaixo ilustra exatamente este cenário, onde foi realizada a remoção de um dos HDs do RAID-5 e reinicializado o servidor:



Observe que mesmo sem um dos HDs foi possível reinicializar o servidor. Na verdade é possível copiar todos os dados da unidade D: sem perca de informações, e inclusive escrever novos dados se necessário. Recomenda-se, porém, que ao perder um dos discos do RAID-5 que se faça a reposição o mais breve possível, pois como o sistema depende de um terceiro HD para ter espaço para os cálculos de paridade (matemática da tolerância a falhas), é possível que em algum momento ele exiba a informação de que está sem espaço livre disponível.

Ao incluir um novo HD ao servidor será apresentada uma opção de reconstruir o RAID-5 com o novo hardware. Esse processo de reconstrução é transparente e não envolve a perca de dados.

O último detalhe a ser lembrado é que o armazenamento dinâmico somente é suportado pelo Windows 2000, 2003 e XP, não sendo reconhecido por outros sistemas operacionais.

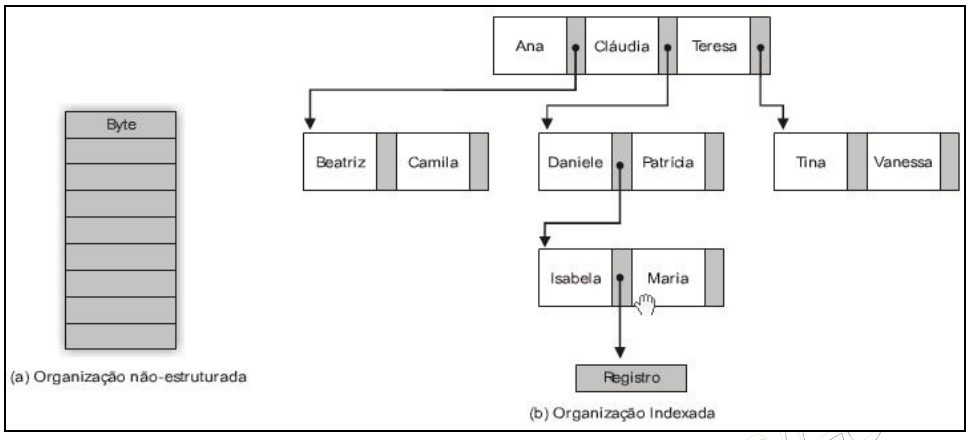
Vamos agora estudar um pouco mais sobre como o sistema de arquivos, em especial o NTFS, se comporta junto ao computador. Esse estudo é importante para compreendermos o que significa um sistema desfragmentado.

Sistema de Arquivos

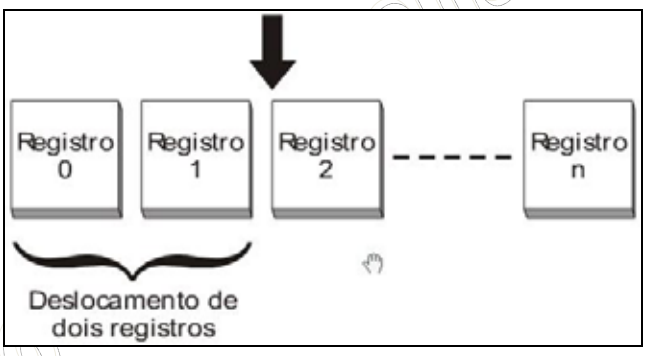
Um sistema de arquivos é a forma como o sistema operacional reconhece os dados que estão armazenados no disco ou volume. Consiste numa seqüência de espaços físicos que contem dados. Esta seqüência pode apresentar uma organização estruturada, não-estruturada ou indexada.

Em uma organização estruturada encontramos todos os dados formando uma seqüência contínua ao longo de todo o disco, existindo um cabeçalho de inicio, fim e informações sobre determinado bloco contínuo. Dificilmente encontraremos uma organização estruturada em discos rígidos, apenas em unidades de Fitas Magnéticas e Discos Magnéticos (cd-rom e dvd-rom).

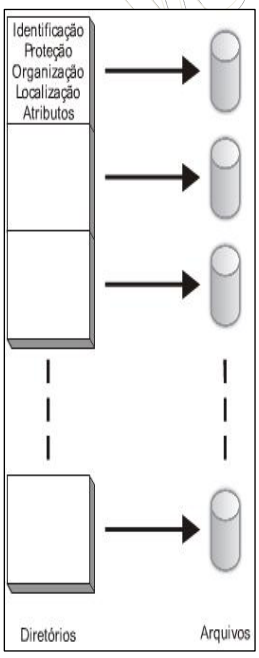
Os discos atuais operam geralmente sobre a organização não-estrutura ou indexada. Na não-estruturada apresenta uma série de blocos distintos, separados fisicamente, porém unidos como um conjunto seqüencial, ou seja, os dados, agrupados em blocos de tamanhos fixos, formam um conjunto seqüencial de blocos fixos, onde reside a informação. Já na organização indexada, temos diversos blocos também de tamanhos fixos, porém distribuídos aleatoriamente pelo disco rígido. Suas ligações são realizadas através de seus cabeçalhos, onde cada bloco informa onde no disco rígido está a sua próxima continuação. A figura abaixo ilustra estas diferenças:

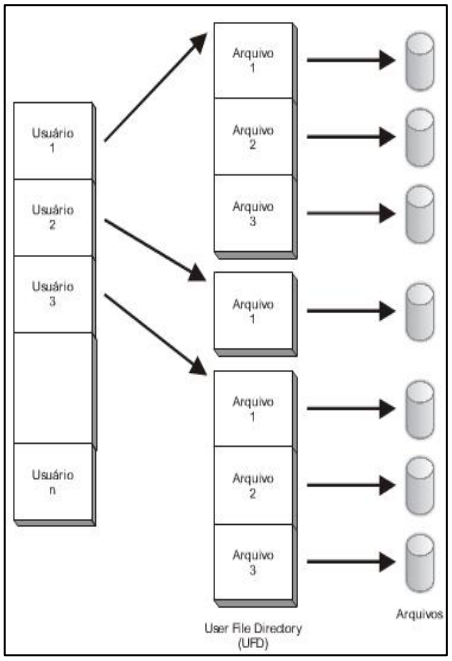


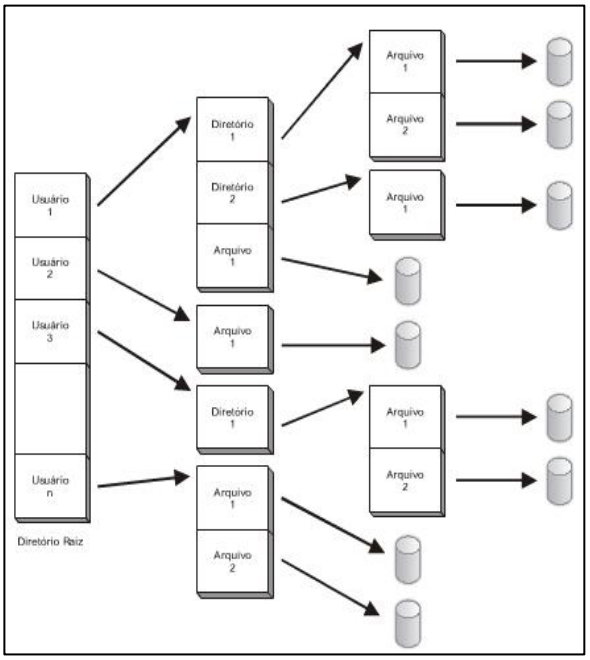
Uma vez definida a organização dos dados para o sistema operacional, podemos dizer que o método de acesso ao dado será direto se o sistema estiver organizado de forma indexada. A organização não-estruturada não permite um acesso direto aos dados, pois é necessário acessar toda a pilha de dados. Já a organização indexada permite que alcancemos nossos dados de forma direta, ou como registros (dados + informações de acesso ao próximo dado):



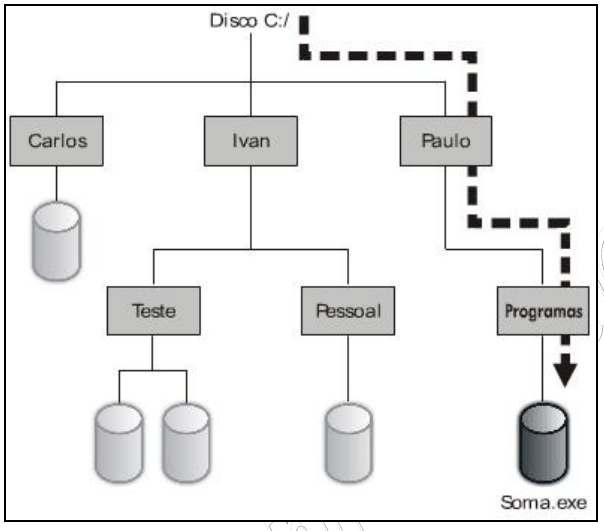
Sobre uma estrutura indexada, com método de acesso direto podemos construir uma hierarquia de acesso aos dados, o que chamamos de diretórios. A estrutura de diretórios pode ser: de nível único, dois níveis ou em árvore:



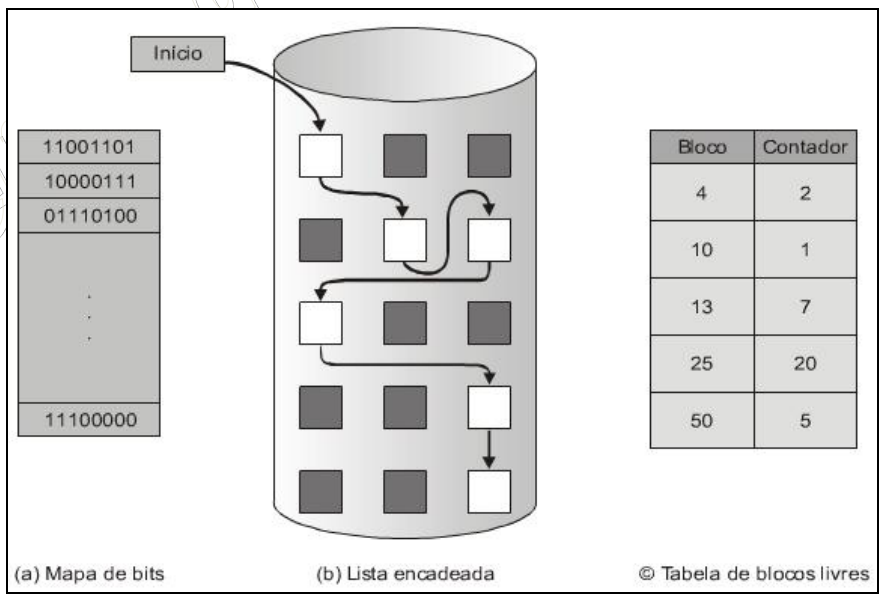




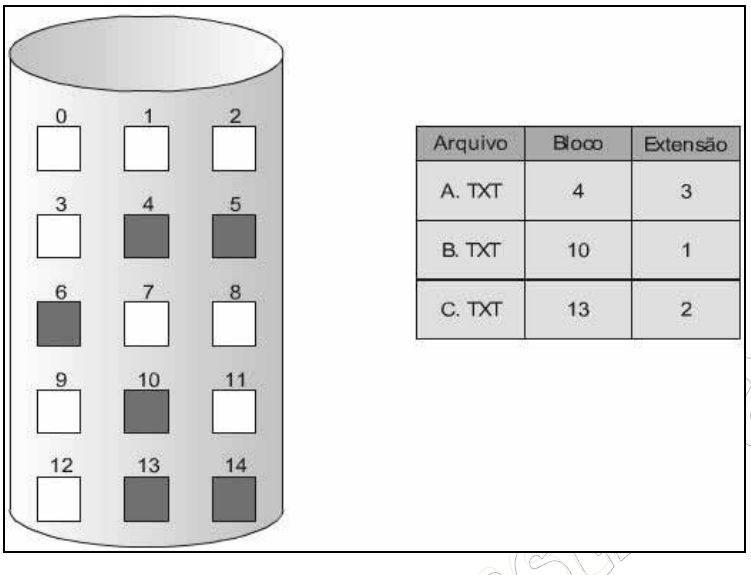
Ao processo de localizar um arquivo, sobre a hierarquia dos dados, denominados de PATH, ou caminho até o dado. Por exemplo, se definirmos que nossa raiz da hierarquia é o identificador C:, e que este por sua vez possui ligações até um diretório definido com “Paulo”, possuindo “Paulo” um acesso direto a um outro diretório “Programas”, onde finalmente encontra-se o dado “soma.exe”, podemos dizer que o PATH para acesso ao dado “soma.exe” é igual a “c:\paulo\programas”.



A alocação de espaço em disco pode ser realizada de três formas distintas: mapa de bits, lista encadeada ou tabela de blocos livres. O sistema operacional, através do sistema de arquivos, é quem escolhe qual o método a ser utilizado em cada situação. A parti do momento que o disco vai sendo alocado dizemos que o sistema de arquivos está sendo preenchido, ou seja, os espaços físicos alocados são registrados em uma tabela de informações para consulta do sistema operacional, esta tabela mais os dados é o que chamamos de sistema de arquivos.

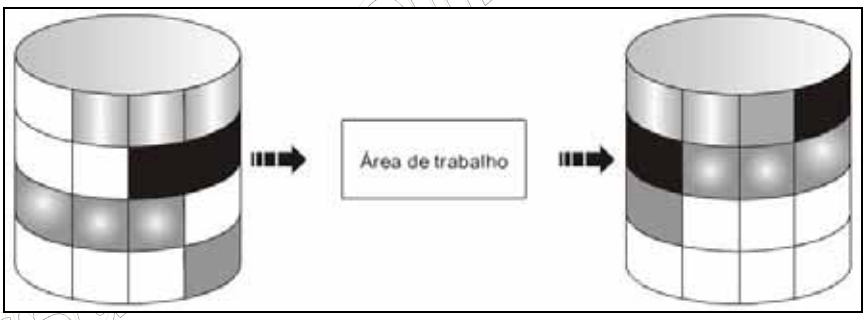


O sistema de arquivos é preenchido de forma contínua, ou seja, os arquivos são alocados em posições contíguas disponíveis:

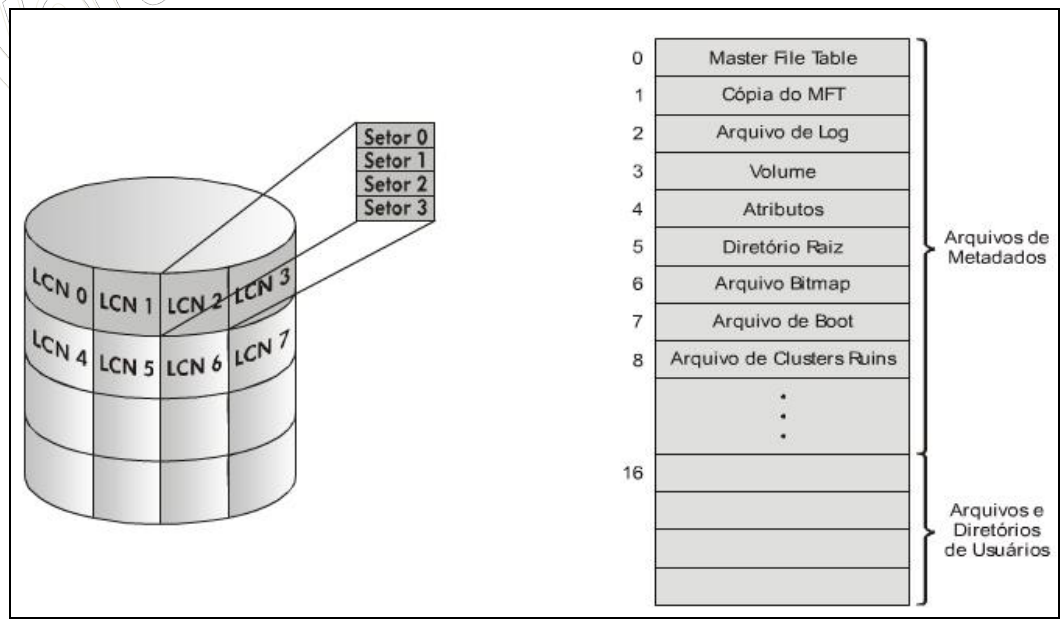


Arquivo	Bloco	Extensão
A. TXT	4	3
B. TXT	10	1
C. TXT	13	2

Quando muitos arquivos são alocados em partes distintas do sistema de arquivos é hora de realizar uma desfragmentação, de forma a re-agrupar as partes dos arquivos e tornar o acesso aos mesmos mais ágeis:

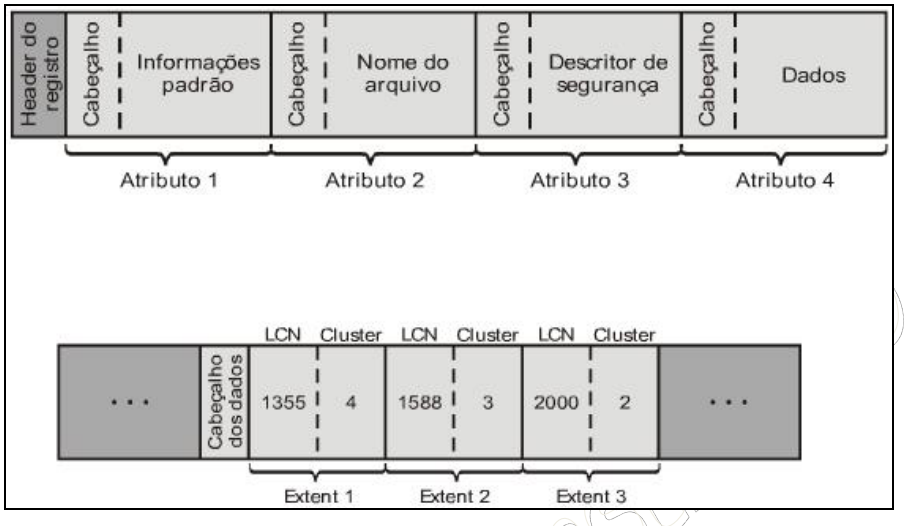


No NTFS (Sistema de Arquivos do Windows NT) os dados são organizados da seguinte forma:



Na posição zero do sistema de arquivos está localizada a tabela principal, ou a Tabela Mestre dos Arquivos, também conhecida como MBR (Master Boot Record), é nela que estão as informações para cada registro no disco rígido. Em seguida temos uma cópia de segurança da MBR. Na posição 3 do sistema de arquivos NTFS encontramos as informações sobre os volumes do disco básico, seguido de atributos, do diretório raiz e arquivo de boot.

Cada registro do sistema de arquivos apresenta a seguinte estrutura:



As vantagens de utilização do NTFS sobre outros sistemas de arquivos, como FAT e FAT32, são:

- Melhor escalabilidade para grandes unidades. O tamanho máximo de partição ou volume para o NTFS é muito maior que para o FAT (tabela de alocação de arquivos), e à medida que o tamanho do volume ou partição aumenta, o desempenho do NTFS não diminui como ocorre com o FAT.
- Active Directory (e domínios, que fazem parte do Active Directory). Com o Active Directory, você pode exibir e controlar facilmente os recursos de rede. Com domínios, você pode ajustar as opções de segurança, ao mesmo tempo mantendo simples a administração. Os controladores de domínio e o Active Directory requerem o NTFS.
- Recursos de compactação, inclusive a capacidade de compactar ou descompactar uma unidade, uma pasta ou um arquivo específico. (Contudo, um arquivo não pode ser compactado e criptografado ao mesmo tempo.)
- Criptografia de arquivos, que melhora muito a segurança. (Contudo, um arquivo não pode ser compactado e criptografado ao mesmo tempo.)
- Permissões que podem ser definidas em arquivos específicos em vez de apenas em pastas.
- Armazenamento remoto, que fornece uma extensão no espaço em disco tornando a mídia removível (como fitas) mais acessível.
- Log de recuperação de atividades de disco, que permite ao NTFS restaurar informações rapidamente no caso de falha de energia ou outros problemas do sistema.
- Arquivos esparsos. Esses são arquivos muito grandes criados por aplicativos de modo que seja necessário somente um espaço limitado em disco. Isto é, o NTFS aloca espaço em disco apenas para as partes gravadas de um arquivo.
- Cotas de disco, que você pode usar para monitorar e controlar a quantidade de espaço em disco utilizada por usuários individualmente.

Agora que realizamos um estudo teórico bastante aprofundado sobre os sistemas operacionais vamos terminar esta primeira parte do curso analisando as possibilidades que um sistema operacional de rede pode trazer para o dia-a-dia.

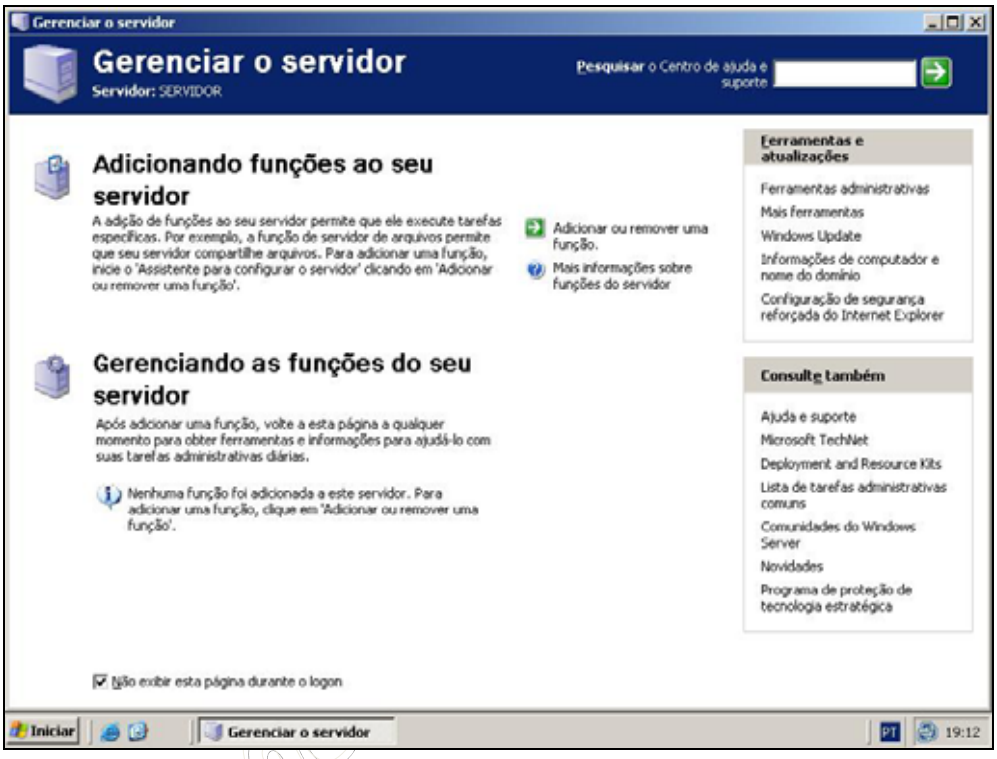
7.6 PRINCIPAIS SERVIÇOS SUPORTADOS

O Windows Server 2003 pode desempenhar diversos papéis na rede através de serviços comuns, são eles:

- Servidor de Internet/Intranet, prestando serviços de hospedagem de sites (http), cópia de arquivos (ftp), envio de mensagens (smtp), servidor de aplicativos Web (asp.net), hospedando páginas ASP ou ASP.NET, etc;
- Controlador de domínio – DC (Domain Controler): um servidor onde está instalado o Active Directory, que é o banco de dados onde ficam gravadas as contas e senhas de usuários, contas dos computadores da rede, nome dos grupos de usuários e listas de membros de cada grupo;
- Serviços de rede: oferecendo serviços de resolução de nomes, tais como DNS e WINS, serviço de configuração automática do protocolo TCP/IP (DHCP), roteamento e acesso remoto (RRAS);
- Servidor de banco de dados: um servidor com o Windows Server 2003 instalado e com o SQL Server 2005 instalado;
- Servidor de correio eletrônico e de ferramentas de colaboração: um servidor como Windows Server 2003 instalado e com o Exchange 2005 instalado.O Exchange é uma plataforma para desenvolvimento de aplicações de Workflow, bem como um servidor de correio eletrônico. Com o Exchange você pode, facilmente, desenvolver aplicações do tipo Workflow, como por exemplo, um aplicativo de despesas de viagem. O funcionário que vai viajar preenche um formulário solicitando recursos para a viagem. O formulário é enviad, automaticamente, para o e-mail do chefe. O chefe analisa a solicitação e aprova ou não. Uma vez aprovada a solicitação, o pedido de liberação de recursos é automaticamente enviada para o e-mail do responsável pela liberação e uma cópia é enviada para o funcionário. Uma vez liberados os recursos, o sistema avisa, via e-mail, o funcionário. Este tipo de aplicação, onde um documento eletrônico passa por diversas etapas e é enviado para diferentes pessoas, é um exemplo típico de aplicação do tipo Workflow;
- Servidor de aplicação;
- Servidor de firewall;

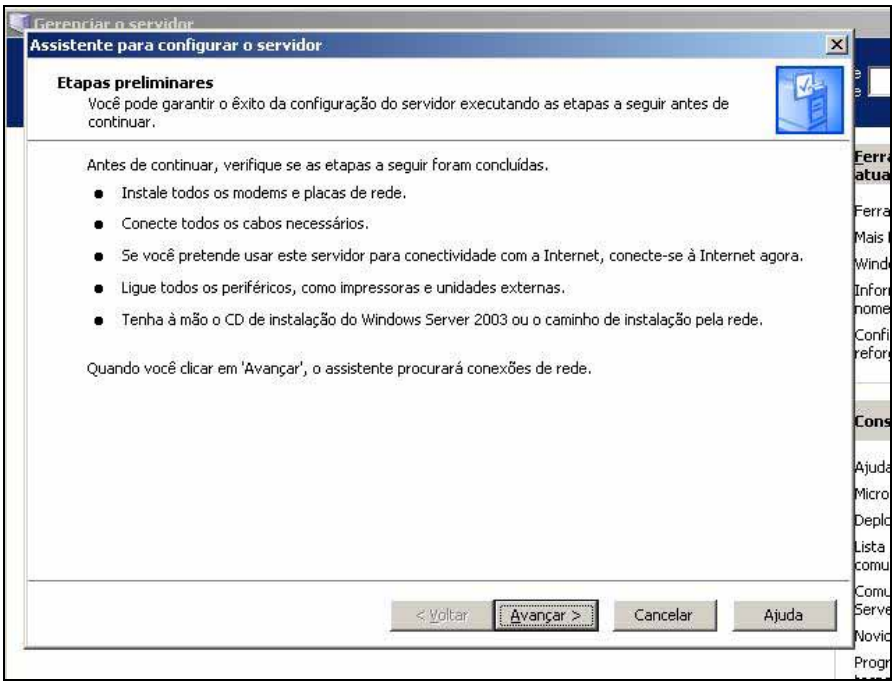
Para falar de cada um desses serviços chamaremos o próprio assistente de configuração do servidor para nos orientar. Este assistente é inicializado logo após o primeiro logon em um servidor Windows Server novo, ou através do menu: Iniciar -> Ferramentas Administrativas -> Gerenciar o Servidor:

A próxima tela é o próprio assistente de configuração e gerenciamento do servidor, ele provê recursos para instalar novos serviços ou administrar serviços instalados. Nesse primeiro momento mostraremos apenas a primeira tela, sem nenhum serviço instalado, na próxima competência passaremos para os detalhes de configuração de cada serviço:

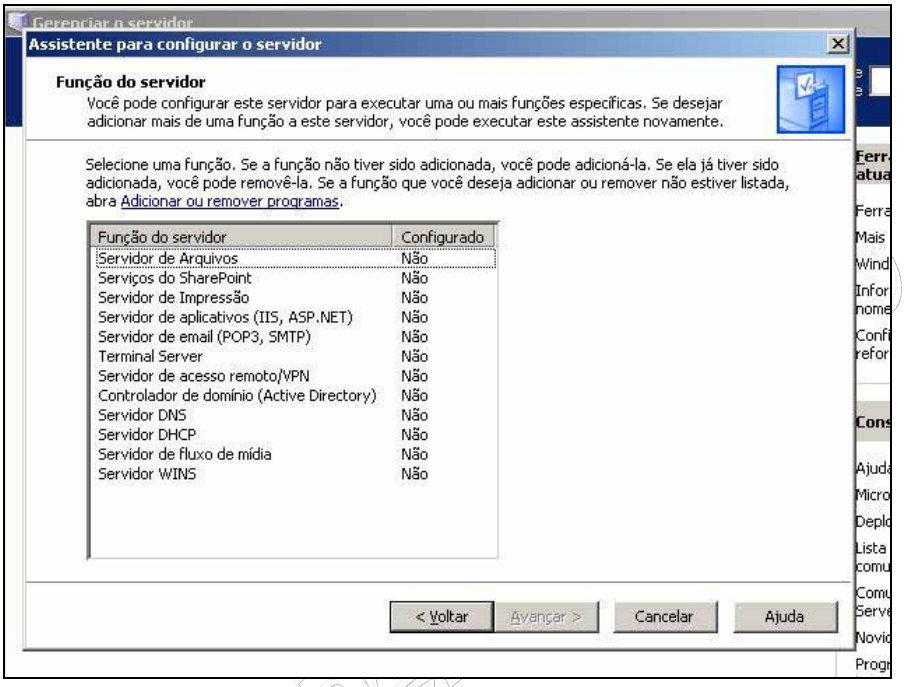


É importante destacarmos os objetivos de um serviço de rede. Um serviço de rede é um software em execução em um servidor de redes, cujo objetivo é prover determinado tipo de funcionalidades para clientes remotos na rede. Ou seja, o serviço é um software, que fica constantemente em execução no servidor, e que é acessado pelos clientes na rede. Esses softwares, ou serviços, são de diversas formas e com diversas utilidades.

Uma das vantagens em utilizar o assistente é que o mesmo se preocupa com uma série de pré-requisitos, que ao longo dos anos foram observados como os erros, ou esquecimentos, mais comuns dos administradores de rede:

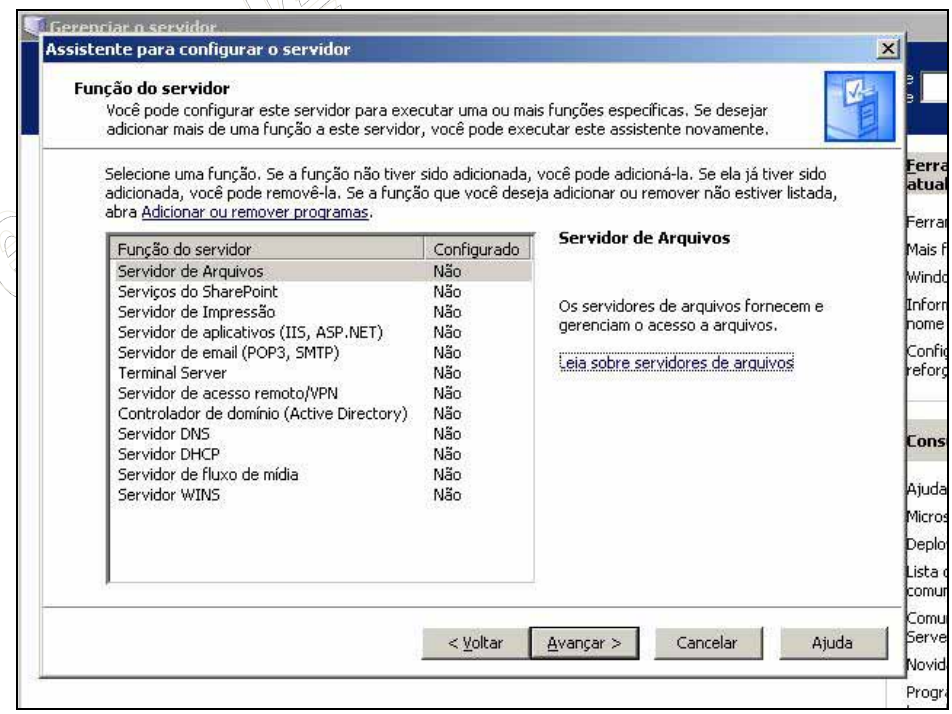


Após realizar as etapas preliminares o assiste apresentará uma série de serviços mais comuns a serem instalados:



Falaremos sobre cada um desses serviços, ou função do servidor, abaixo:

O Servidor de Arquivos



O servidor de arquivos fornece um ponto centralizado na rede para armazenamento e compartilhamento de arquivos entre os usuários. Quando desejarem usar um arquivo importante que deva ser acessado por muitos usuários, como um planejamento de projeto, os usuários podem acessá-lo remotamente no servidor de arquivos, em vez de precisarem repassar o arquivo entre cada computador. Se os usuários da sua rede precisarem acessar os mesmos arquivos e aplicativos ou se um gerenciamento centralizado de backup e de arquivos for importante para sua organização, configure o computador como um servidor de arquivos.

A função do servidor de arquivos usa muitos recursos que já estão instalados como parte do sistema operacional Windows Server 2003, como NTFS, Desfragmentador de Disco e Espaço para Nomes DFS (Domain File System). Por padrão, a função de servidor de arquivos instala os seguintes recursos:

- Gerenciamento de Servidor de Arquivos : Oferece uma ferramenta centralizada para o gerenciamento do servidor de arquivos. Com o Gerenciamento de Servidor de Arquivos, você pode criar e gerenciar compartilhamentos, definir limites de cota, criar relatórios de utilização de armazenamento, replicar dados a partir de um servidor de arquivos e para ele, gerenciar redes de área de armazenamento (Redes SAN – Storage Area Network) e compartilhar arquivos com sistemas UNIX e Macintosh.
- Relatório de Armazenamento: Permitem que você analise como o espaço em disco é usado em um servidor. Por exemplo, você pode gerar relatórios por demanda ou agendados que identificam arquivos duplicados. Depois é possível excluir essas duplicações para recuperar espaço em disco.
- Cotas e Triagem de Arquivos: As cotas permitem que você limite o tamanho de um volume ou de uma subárvore da pasta. Você pode configurar o Windows para notificá-lo quando limites de cota forem alcançados. A triagem de arquivos permite a você impedir que determinados tipos de arquivos sejam salvos em uma pasta ou volume. A triagem de arquivos ajuda a garantir que usuários não salvem arquivos ou dados que não sejam críticos e que possam violar leis de propriedade intelectual no servidor.
- Gerenciamento DFS: Permite que você gerencie a replicação de dados de servidores em locais de ramificação para servidores em centros de dados (hub). O backup dos dados pode então ser feito centralmente, o que elimina a necessidade do backup dos dados ser feito nas ramificações/filiais. Com o Gerenciamento DFS, você também pode agrupar as pastas compartilhadas localizadas em servidores diferentes e apresentá-las aos usuários como uma árvore virtual de pastas, conhecida como espaço para nome (DFS). Um espaço para nome oferece vários benefícios, incluindo maior disponibilidade de dados, balanceamento de carga e migração de dados simplificada.

Além disso, você tem a opção de atualizar um servidor de arquivos existente com ferramentas adicionais como:

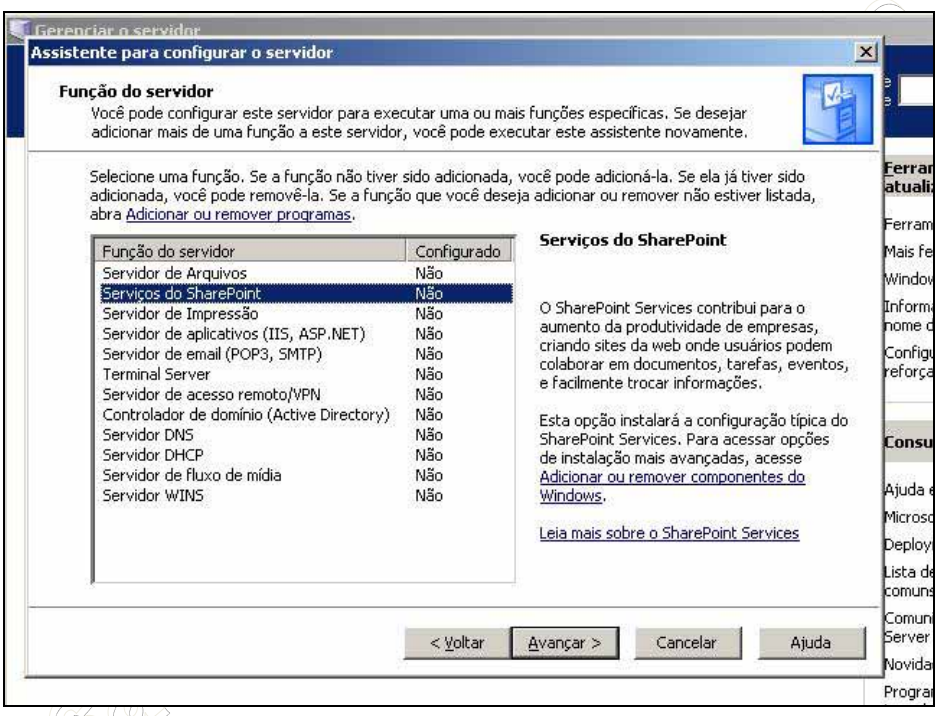
- Replicação DFS: É um mecanismo de replicação entre servidores DFS baseado em estado, que oferece suporte ao agendamento de replicação e à aceleração da largura de banda. A Replicação DFS usa um algoritmo de compactação conhecido como RDC (Compactação Diferencial Remota), que pode ser usado para atualizar os arquivos de forma eficiente, em uma rede de largura de banda limitada, pela replicação apenas dos blocos de arquivos alterados quando há atualizações de arquivos.
- Gerenciador de Armazenamento para Redes SAN: Permite a você configurar o armazenamento em um ou mais subsistemas de armazenamento iSCSI e de Fibre Channel em uma rede de área de armazenamento (Rede SAN).
- Serviços Microsoft para NFS (MS-NFS): O MS-NFS permite o compartilhamento de arquivos em um ambiente misto de computadores, sistemas operacionais e redes.
- Serviços para Macintosh: Os Serviços para Macintosh permitem que os computadores cliente Macintosh e os baseados em Windows compartilhem arquivos e impressoras e se conectem remotamente a uma rede Microsoft.

Antes de configurar o computador como um servidor de arquivos, verifique se:

- O computador é associado a um domínio do Active Directory como servidor membro. Você pode aperfeiçoar a segurança e a autenticação do usuário fazendo com que o computador ingresse em um domínio do Active Directory.
- Todos os volumes de disco existentes usam o sistema de arquivos NTFS. Volumes FAT32 não são protegidos e não oferecem suporte à compactação de arquivos e pastas, a cotas de disco, à criptografia de arquivos ou a permissões de arquivo individuais.

- O Firewall do Windows está habilitado. Para obter mais informações, consulte a Documentação do Agente de Configuração de Segurança (http://www.microsoft.com/). Se o Firewall do Windows estiver habilitado, você deverá selecionar Compartilhamento de Arquivo e Impressora na guia Exceções nesse Firewall, para que a função de servidor de arquivos atue corretamente.
- O Assistente de Configuração de Segurança está instalado e habilitado.

Os Serviços do SharePoint



Os sites baseados no Microsoft Windows SharePoint Services 2.0 oferecem um local em que a sua equipe pode se comunicar, compartilhar documentos e trabalhar em conjunto em um projeto. Você pode criar um site separado para cada projeto em que a equipe esteja trabalhando.

Os usuários do site podem contribuir usando apenas um navegador da Web. Entretanto, se os usuários possuem programas clientes compatíveis com o Windows SharePoint Services instalados em seus computadores, tal como o Microsoft Office 2003, eles poderão trabalhar totalmente integrados com o site, salvando arquivos em bibliotecas, editando documentos no programa cliente, movendo ou vinculando essas informações ao site.

Este tópico explica o procedimento básico para configurar um servidor Windows SharePoint Services. Depois de configurar um servidor Windows SharePoint Services básico, você pode executar outras tarefas de configuração, dependendo de como você deseja usar o servidor Windows SharePoint Services.

Antes de configurar o seu computador como um servidor Windows SharePoint Services, verifique se:

- As Extensões de Servidor do FrontPage 2002 não estão sendo executadas na porta 80.
- O Firewall do Windows está habilitado.
- O Assistente de Configuração de Segurança está instalado e habilitado.

O Servidor de Impressão

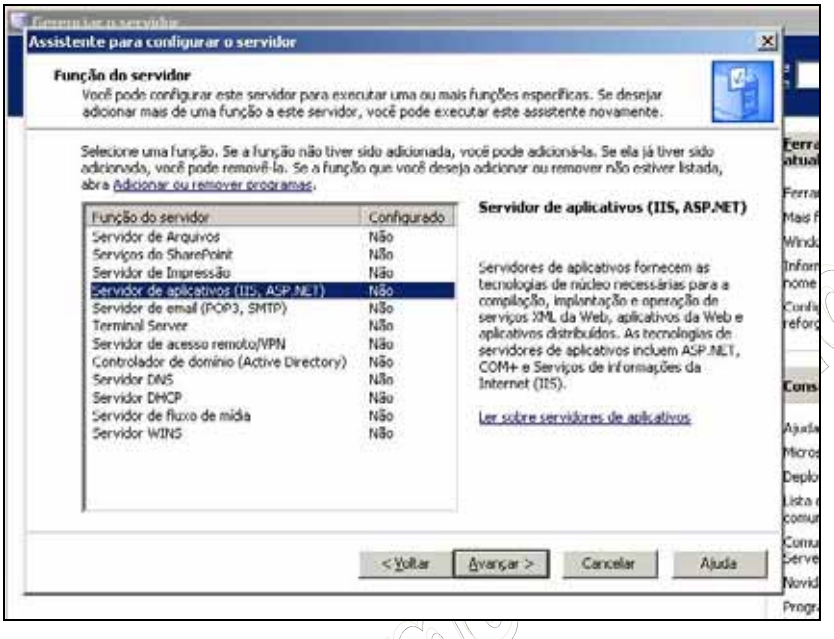
Os serviços de impressão fornecem e gerenciam o acesso às impressoras de rede e aos drivers de impressora.

Observação: Este recurso não está incluído em computadores que executam o sistema operacional Microsoft Windows Server 2003, Web Edition.

Antes de configurar o servidor como um servidor de impressão, verifique se:

- O sistema operacional está configurado corretamente. Nos sistemas operacionais Windows Server 2003, os serviços de impressão dependem da configuração adequada do sistema operacional e seus serviços. Se houver uma nova instalação de um sistema operacional Windows Server 2003, você poderá usar as configurações padrão do serviço. Nenhuma outra ação é necessária.
- O computador é associado a um domínio do Active Directory como servidor membro. O servidor de impressão deve ser associado a um domínio se você quiser restringir o acesso a alguma impressora, para que apenas determinados usuários do domínio possam utilizá-la, ou se desejar que o servidor de impressão publique as impressoras compartilhadas no Active Directory, para que os usuários do domínio possam facilmente encontrar essas impressoras. Se você não precisa realizar essas tarefas, não é necessário associar o servidor de impressão a um domínio.
- Todos os volumes de disco existentes usam o sistema de arquivos NTFS. Os volumes FAT32 não são tão seguros. Para obter mais informações sobre a criptografia de dados armazenados em volumes NTFS, inclusive trabalhos de impressão no spool, consulte Armazenando dados de forma segura.
- O Firewall do Windows está habilitado.
- O Assistente de Configuração de Segurança está instalado e habilitado.

O Servidor de Aplicativos (ISS, ASP.NET)



O servidor de aplicativos é uma tecnologia fundamental que fornece infra-estrutura e serviços importantes aos aplicativos hospedados em um sistema. Os servidores de aplicativos típicos incluem o seguinte:

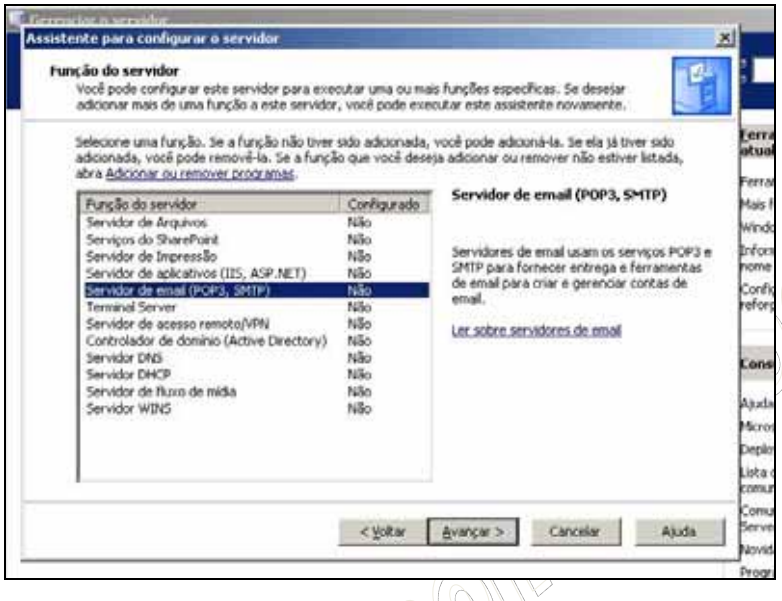
- Pool de recursos (por exemplo, pool de conexões com bancos de dados e pool de objetos)
- Gerenciamento distribuído de transações
- Comunicação assíncrona entre programas, geralmente por meio de enfileiramento de mensagens
- Um modelo de ativação de objetos Just-in-Time
- Interfaces automáticas dos serviços XML da Web para acessar objetos de negócios
- Serviços de detecção de failover e da integridade do aplicativo
- Segurança integrada

Os sistemas operacionais Windows Server 2003 incluem toda essa funcionalidade, além dos serviços para o desenvolvimento, implantação e gerenciamento em tempo de execução de serviços XML da Web, aplicativos para Web e aplicativos distribuídos.

Antes de configurar o computador como um servidor de aplicativos, verifique se:

- Todos os volumes de disco existentes usam o sistema de arquivos NTFS. Volumes FAT32 não são protegidos e não oferecem suporte à compactação de arquivos e pastas, a cotas de disco, à criptografia de arquivos ou a permissões de arquivo individuais. Para descobrir o tipo de sistema de arquivos, em Meu computador clique com o botão direito no volume de disco e clique em Propriedades.
- O computador possui conectividade de rede e um endereço IP estático ou dinâmico.

O Servidor de e-mail (SMTP, POP3)



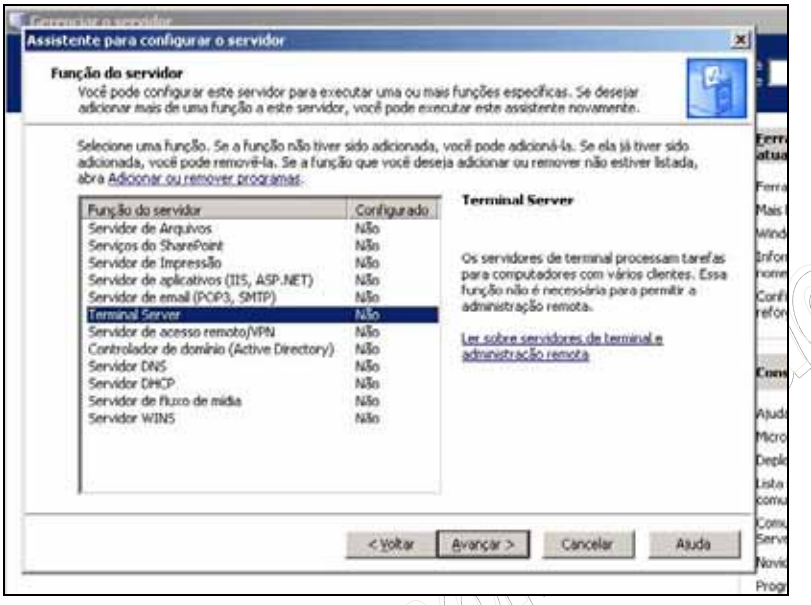
Configure o computador como um servidor de email para instalar os Serviços de Email, que oferecem a transferência e a recuperação de email. Os Serviços de email incluem os serviços POP3 e SMTP, que oferecem, respectivamente, a recuperação e a transferência de emails. Os administradores podem usar o serviço POP3 para armazenar e gerenciar contas de email no servidor de email. Depois de configurar o computador como um servidor de email, os usuários poderão se conectar a esse servidor e recuperar emails em seus computadores locais usando um cliente de email que ofereça suporte ao protocolo POP3, como o Microsoft Outlook.

É importante destacar que para usar o protocolo LDAP, um protocolo padrão para webmails, é necessário a aquisição do serviço Microsoft Exchange. O Microsoft Exchange é um produto a parte com funções muito melhoradas a do SMTP e POP3. O Microsoft Exchange, além de substituir estes primos mais básicos provê uma série de novos serviços, como listas de e-mails, filtros anti-spam, relatórios de desempenho, entre outros.

Antes de configurar o computador como um servidor de email, verifique se:

- O servidor no qual você pretende instalar os serviços de email está conectado à Internet.
- Existe uma partição NTFS disponível. Com a partição NTFS, você pode aproveitar a segurança mais eficaz oferecida pelas cotas de disco. Para obter mais informações sobre cotas de disco, consulte Configurando cotas de disco para o serviço POP3.
- Você registrou o nome de domínio de email. Contate o seu provedor para obter auxílio ao registrar um nome de domínio de email.
- Existe um registro do Mail eXchanger (MX) para o nome de domínio de email, que corresponde ao nome do servidor. Contate o seu provedor para criar um registro MX.
- Você configurou seu servidor para endereçamento estático. Contate o seu provedor para obter as informações necessárias para configurar o servidor para endereçamento estático. Para obter mais informações sobre como configurar seu servidor de email com um endereço IP estático, consulte a Ajuda (F1) do Windows Server 2003.
- O Firewall do Windows está habilitado.
- O Assistente de Configuração de Segurança está instalado e habilitado.

O Terminal Server



Utilizando um servidor de terminal, os usuários de locais remotos podem executar programas, salvar arquivos e usar recursos de rede como se estes estivessem instalados em seus próprios computadores. Instalando programas em um servidor de terminal, você pode garantir que todos os usuários utilizem a mesma versão de um programa. Se você planeja usar esse computador para permitir que vários usuários acessem um programa ao mesmo tempo e partindo de um único ponto de instalação, configure o computador como servidor de terminal.

Entretanto, se seu plano é usar o computador para administração remota com sistemas operacionais Windows Server 2003, não é necessário instalar o Terminal Server. Em vez disso, você pode usar a Área de trabalho remota para administração (antes chamada de serviços de terminal no modo Administração remota), que é instalada por padrão em computadores que executam os sistemas operacionais Windows Server 2003. Após a ativação de conexões remotas, a Área de trabalho remota para administração permite que você gerencie remotamente servidores de qualquer cliente em uma conexão LAN, WAN ou dial-up. Até duas sessões remotas, além da sessão do console, podem ser acessadas ao mesmo tempo, sem necessidade de licenciamento do Terminal Server. Para obter mais informações sobre a Área de trabalho remota para administração, consulte Administração remota usando os serviços de terminal.

Antes de configurar o computador como um servidor de terminal, verifique se:

- O computador é um servidor em uma rede ou domínio, mas não é um controlador de domínio. A instalação do Terminal Server em um controlador de domínio afeta o desempenho devido à memória adicional, ao tráfego de rede e ao tempo de processador necessários para executar as tarefas de um controlador de domínio em um domínio.

- O Firewall do Windows está habilitado. Habilite a exceção da Área de Trabalho Remota no Firewall do Windows . Se o Terminal Server e o Licenciamento do Terminal Server estiverem sendo executados em computadores separados, adicione a porta TCP 135 na lista de exceções do Firewall do Windows.

- O Assistente de Configuração de Segurança está instalado e habilitado.

- O computador satisfaz os requisitos de processador e memória para oferecer suporte a várias sessões simultâneas onde houver muitos usuários conectados. Um servidor de terminal exige, no mínimo, 128 MB de memória RAM, além de memória RAM adicional para cada usuário, a fim de oferecer suporte à execução dos programas de cada usuário no servidor. Recomenda-se acrescentar outros 10 MB de RAM para cada usuário leve - aquele que geralmente executa um programa por vez - e até 21 MB de RAM para cada usuário avançado, que executa normalmente três ou mais programas simultaneamente. Ademais, se você planeja instalar aplicativos de 16 bits

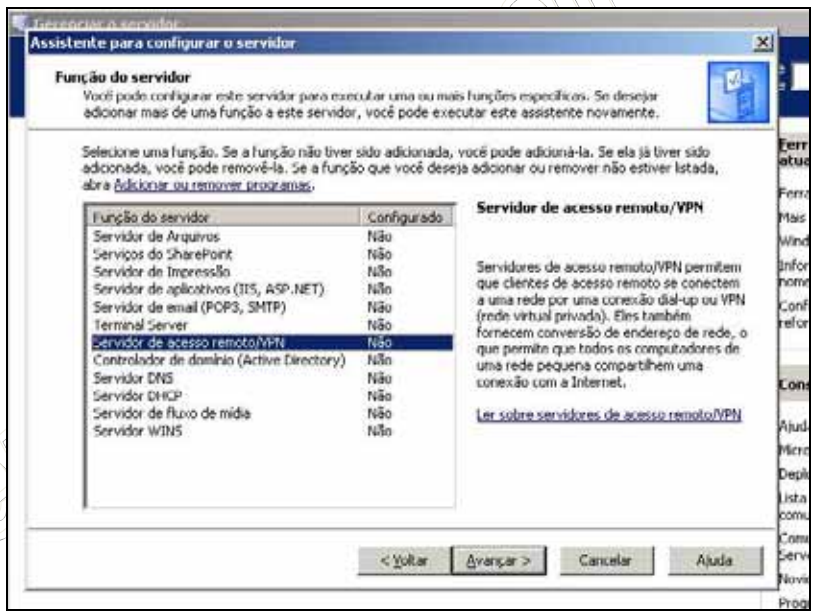
no servidor de terminal, lembre-se de que eles consomem outros recursos quando executados em ambientes de 32 bits, como os sistemas operacionais Windows Server 2003.

- Não há programas instalados no computador. Você deve adicionar a função Terminal Server antes de instalar os programas aos quais deseja conceder acesso para os usuários. Se já houver programas instalados no computador, você deverá reinstalá-los para assegurar que funcionem corretamente no ambiente do Terminal Server.

- Nenhum usuário pode fazer logon remotamente no computador. Permita que os usuários acessem o servidor de terminal somente depois que você instalar os programas, testar a instalação e executar os ajustes necessários para que eles funcionem em um ambiente com várias sessões. Para obter informações sobre como desabilitar temporariamente conexões de serviços de terminal, consulte Desabilitar conexões dos serviços de terminal.

- Todos os volumes de disco existentes usam o sistema de arquivos NTFS. Os volumes FAT32 não fornecem o nível exigido de segurança para os usuários de um ambiente com várias sessões, nem a capacidade de definir permissões de arquivos.

Serviço de Acesso Remoto/VPN



Você pode configurar um servidor que permita aos usuários remotos acessar recursos de sua rede privada através de conexões dial-up ou de redes virtuais privadas (VPN). Esse tipo de servidor é chamado de servidor de acesso remoto/VPN. Os servidores de acesso remoto/VPN também pode oferecer a conversão de endereços de rede (NAT). Com a NAT, os computadores da rede privada podem compartilhar uma única conexão com a Internet. Com a VPN e a NAT, seus clientes VPN podem determinar os endereços IP dos computadores de sua rede privada, o que não é possível para outros computadores da Internet.

Antes de configurar o servidor como um servidor de acesso remoto/VPN, verifique se:

- O servidor está corretamente configurado para fornecer segurança às necessidades de sua rede. Como o servidor de acesso remoto/VPN será conectado à rede privada, à Internet e aos clientes remotos, certifique-se de ele seja seguro. A segurança da rede privada depende da segurança do servidor de acesso remoto/VPN. Para obter mais informações, consulte Informações sobre segurança para acesso remoto.
- O Firewall do Windows está habilitado.
- O Assistente de Configuração de Segurança está instalado e habilitado.

- Este computador possui duas interfaces de rede: uma conectada à Internet e outra conectada à rede privada. A primeira deve ser uma conexão dedicada, com largura de banda suficiente que permita aos usuários VPN se conectar à rede privada e aos usuários desta se conectar à Internet. A conexão com os computadores da rede privada deve ser feita por meio de um dispositivo de hardware, como o adaptador de rede.
- Todos os protocolos de rede necessários às interfaces de rede foram instalados.

Controlador de Domínio (Active Directory)

Os controladores de domínio armazenam dados e gerenciam interações entre os usuários e o domínio, inclusive processos de logon do usuário, autenticação e pesquisas de diretório. Se você planeja usar este servidor para fornecer o serviço de diretórios Active Directory a usuários e computadores, configure o servidor como um controlador de domínio.

Para configurar um servidor como controlador de domínio, instale o Active Directory no servidor. Existem quatro opções disponíveis no Assistente para instalação do Active Directory. Você pode criar um controlador de domínio adicional em um domínio existente, um controlador de domínio para um novo domínio filho, um outro para uma nova árvore de domínio ou ainda para uma nova floresta.

- Crie controladores de domínio adicionais se quiser melhorar a disponibilidade e confiabilidade dos serviços de rede. Adicionando outros controladores de domínio, você pode oferecer tolerância a falhas, equilibrar a carga dos controladores de domínio existentes, fornecer suporte de infra-estrutura adicional aos sites e melhorar o desempenho facilitando a conexão dos clientes ao controlador de domínio quando eles fizerem logon na rede.

- Crie um controlador de domínio para uma nova floresta quando você quiser atualizar um domínio Windows NT para que ele se torne o primeiro domínio de uma nova floresta, segmentar sua rede para obter autonomia administrativa, fornecer um limite de segurança para proteger dados sensíveis, isolar o escopo da replicação de diretórios ou usar um espaço para nome DNS não contíguo que seja diferente de uma floresta existente de sua rede.

- Crie um controlador de domínio para um novo domínio filho quando desejar criar um domínio que compartilhe um espaço para nome contíguo com um ou mais domínios existentes. Isso significa que o nome do novo domínio contém o nome completo do domínio pai. Por exemplo, child.microsoft.com é um domínio filho de microsoft.com.

- Crie um controlador de domínio para uma nova árvore de domínio quando quiser criar um domínio que possua um espaço para nome DNS sem relação com os outros domínios da floresta. Isso significa que o nome do domínio raiz da árvore (e todos os seus filhos) não precisam conter o nome completo do domínio pai. Uma floresta pode conter uma ou mais árvores de domínio. Por exemplo, msn.com é uma nova árvore de domínio da floresta microsoft.com.

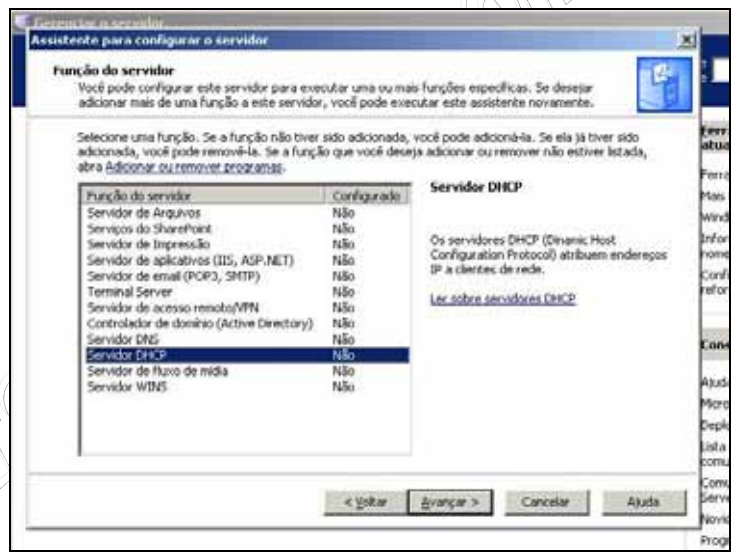
O Servidor DNS (Domain Name System)

Os servidores de serviço de nomes de domínio (DNS) abrigam registros de um banco de dados DNS distribuído e usam os registros que abrigam para resolver consultas de nomes DNS enviadas por computadores clientes DNS, como consultas sobre nomes de sites da Web ou de computadores da rede ou da Internet. Se você planeja usar o computador para responder às consultas DNS de computadores da rede, adicione a função servidor DNS.

Geralmente, o servidor DNS não é essencial em uma pequena organização, já que é usado o método de resolução de nome serviço de cadastramento na Internet do Windows (WINS) para localizar recursos da rede. Os recursos da Internet são localizados com os servidores DNS executados por um provedor de serviços de Internet. No entanto, à medida que mais redes são integradas à Internet, o DNS torna-se mais comum em redes de pequeno porte.

O uso do DNS na rede não requer necessariamente que você administre uma infra-estrutura DNS. Se você possui uma rede pequena na qual as informações são mantidas de forma dependente, você pode optar por ter o espaço para nome DNS administrado por uma organização diferente, especializada nesse assunto, como a administração pública ou um provedor de serviços de Internet. Nesse caso, a outra organização hospedará e administrará as informações DNS para você ou integrará seus computadores com um servidor DNS existente hospedado na rede da organização.

O Servidor DHCP (Dinamic Host Configuration Protocol)



Os servidores DHCP gerenciam centralmente endereços IP e informações afins, fornecendo-as aos clientes. Isso permite que você defina configurações de rede cliente em um servidor, em vez de configurá-las em cada computador clientes. Se você quiser que este computador distribua endereços IP aos clientes, configure-o como um servidor DHCP.

Terminologia do DHCP:

- Escopo: Um escopo é o intervalo consecutivo completo dos endereços IP possíveis para uma rede. Em geral, os escopos definem uma única sub-rede física na rede à qual serão oferecidos serviços DHCP. Os escopos também fornecem o método principal para que o servidor gerencie a distribuição e atribuição de endereços IP e quaisquer parâmetros de configuração relacionados para clientes na rede.

- Superescopo: Um superescopo é um agrupamento administrativo de escopos que pode ser usado para oferecer suporte a várias sub-redes IP lógicas na mesma sub-rede física. Os superescopos contêm somente uma lista de escopos membros ou escopos filho que podem ser ativados em conjunto. Os superescopos não são usados para configurar outros detalhes sobre o uso do escopo. Para configurar a maioria das propriedades usadas em um superescopo, você precisa configurar propriedades de escopo membro individualmente.

- Intervalo de exclusão: Um intervalo de exclusão é uma seqüência limitada de endereços IP dentro de um escopo, excluído das ofertas de serviço DHCP. Os intervalos de exclusão asseguram que quaisquer endereços nesses intervalos não serão oferecidos pelo servidor a clientes DHCP na rede.

- Pool de endereços: Após definir um escopo DHCP e aplicar intervalos de exclusão, os endereços restantes formarão o pool de endereços no escopo. Os endereços em pool são qualificados para atribuição dinâmica pelo servidor a clientes DHCP na rede.

- Concessão: Uma concessão é um período de tempo especificado por um servidor DHCP durante o qual um computador cliente pode usar um endereço IP atribuído. Uma concessão está ativa quando ela é feita a um cliente. Geralmente, o cliente precisa renovar sua atribuição de concessão de endereço no servidor antes que ela expire. Uma concessão torna-se inativa quando ela expira ou é excluída no servidor. A duração de uma concessão determina quando ela expirará e com que freqüência o cliente precisa renová-la no servidor.

- Reserva: Você usa uma reserva para criar uma atribuição de concessão de endereço permanente pelo servidor DHCP. As reservas asseguram que um dispositivo de hardware especificado na sub-rede sempre poderá usar o mesmo endereço IP.

- Tipos de opção: Os tipos de opção são outros parâmetros de configuração de cliente que um servidor DHCP pode atribuir ao oferecer concessões a clientes DHCP. Por exemplo, algumas opções usadas com freqüência incluem endereços IP para gateways padrão (roteadores), servidores WINS e servidores DNS. Geralmente, esses tipos de opção são ativados e configurados para cada escopo. O console DHCP também permite a você configurar tipos de opção padrão que são usados por todos os escopos adicionados e configurados no servidor. A maioria das opções é predefinida através da RFC 2132, mas você pode usar o console do DHCP para definir e adicionar tipos de opção personalizados, se necessário.

- Classe de opções: Uma classe de opções é uma forma de o servidor gerenciar os tipos de opção fornecidos aos clientes. Quando uma classe de opções é adicionada ao servidor, os clientes dessa classe podem receber tipos de opção específicos de classe para suas configurações. No Microsoft® Windows® 2000 e Windows XP, os computadores clientes também podem especificar uma identificação de classe durante a comunicação com o servidor. Para clientes DHCP anteriores que não oferecem suporte ao processo de identificação de classe, o servidor pode ser configurado com classes padrão quando estiver inserindo clientes em uma classe. As classes de opções podem ser de dois tipos: classes de fornecedor e classes de usuário.

Ao adicionar a função do servidor DHCP, você cria um escopo que define o intervalo de endereços IP que o servidor DHCP aloca aos clientes de uma sub-rede. Você deve criar um escopo para cada sub-rede que possua clientes que você deseja gerenciar com DHCP.

Antes de configurar o computador como um servidor DHCP, verifique se:

- Você está familiarizado com os conceitos de DHCP, como escopos, concessões e opções.

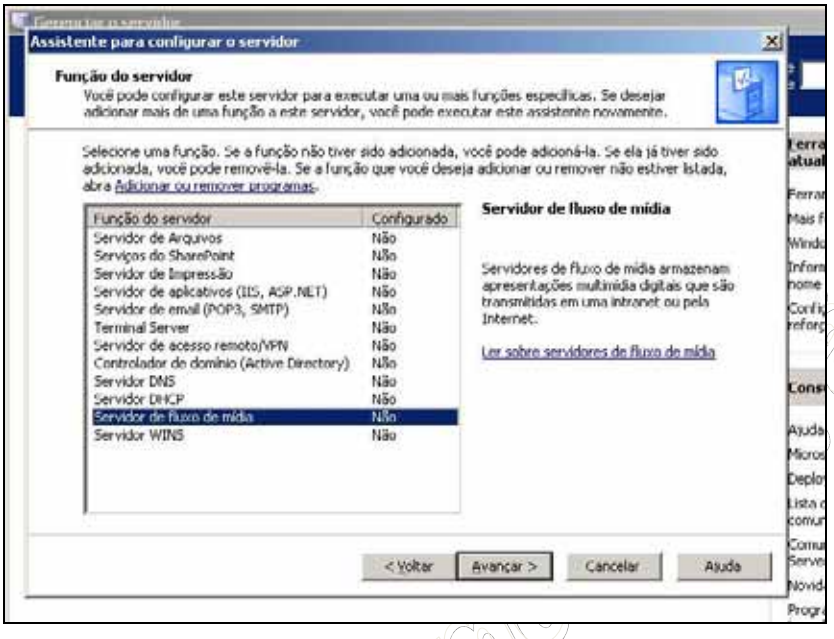
- Este computador tem um endereço IP estático.

- Todos os volumes de disco existentes usam o sistema de arquivos NTFS. Volumes FAT32 não são protegidos e não oferecem suporte à compactação de arquivos e pastas, a cotas de disco, à criptografia de arquivos ou a permissões de arquivo individuais.

- O Firewall do Windows está habilitado.

- O Assistente de Configuração de Segurança está instalado e habilitado.

Servidor de Fluxo de Mídia



Você pode usar o Windows Media Services para disponibilizar o fluxo do conteúdo de áudio e vídeo pela Internet ou por uma intranet (Streamming). Os clientes podem ser computadores ou dispositivos que reproduzem conteúdo usando um player, como o Windows Media Player, ou computadores que executam o Windows Media Services (chamados de servidores Windows Media) que armazenam em proxy ou em cache ou redistribuem o conteúdo. Os clientes também podem ser aplicativos personalizados desenvolvidos com SDK (kit de desenvolvimento de software) Windows Media Software.

Nos últimos 08 anos, o desenvolvimento de aplicações utilizando fluxo de mídia tem crescido aceleradamente. São exemplos: O Big Brother Brasil via Internet, o Globo Media Center, a exibição de trailers de filmes pelos principais portais de conteúdo, os novos canais de televisão exclusivos pela Internet, o YouTube, e nos próximos meses a certeza de canais pessoais através dos sistemas de televisão digital.

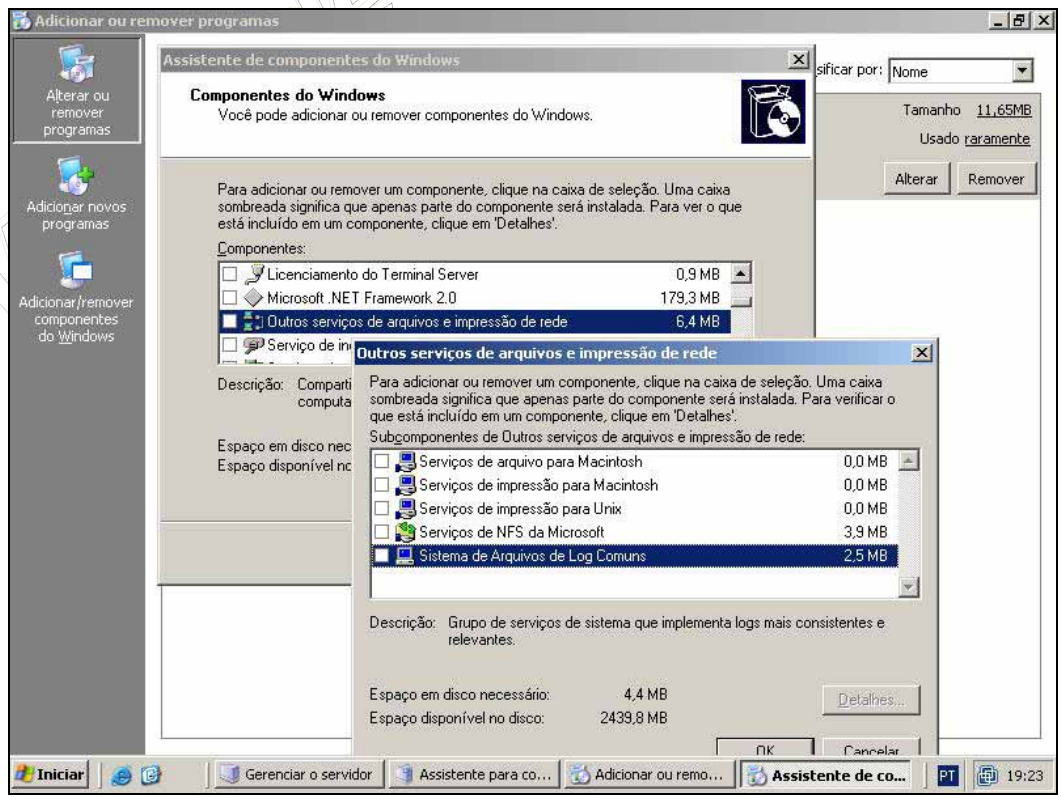
O Serviço WINS

Os servidores do serviço de cadastramento na Internet do Windows (WINS) mapeiam dinamicamente endereços IP para nomes de computadores (nomes NetBIOS). Isso permite que os usuários acessem recursos usando o nome do computador, em vez do endereço IP. Se você quiser que o computador rastreie os nomes e endereços IP de outros computadores da rede, configure-o como um servidor WINS.

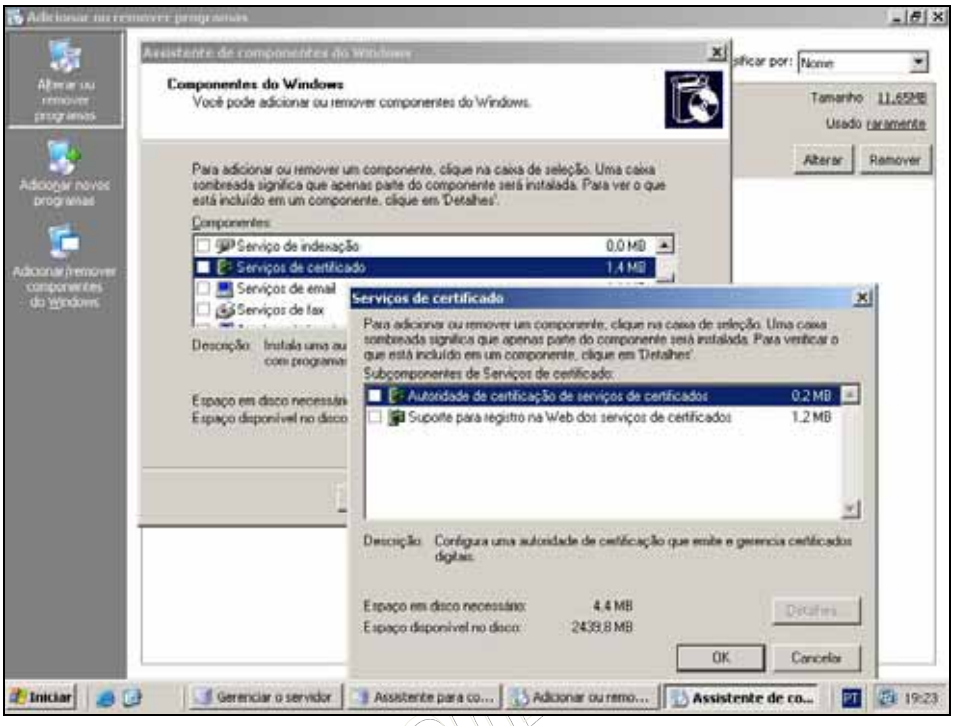
Antes de configurar o computador como um servidor WINS, verifique se:

- Você está familiarizado com os conceitos WINS, como nomes de NetBIOS, servidores WINS, clientes WINS e parceiros de duplicação. Para obter mais informações, consulte Noções básicas sobre WINS.
- O sistema operacional está configurado corretamente. Nos sistemas operacionais Windows Server 2003, o WINS depende da configuração adequada do sistema operacional e seus serviços. Se houver uma nova instalação de um produto no Windows Server 2003, você poderá usar as configurações padrão do serviço. Nenhuma outra ação é necessária.
- Você sabe quantos servidores WINS precisa instalar e onde localizar cada servidor na rede. Quando você adicione a função de servidor WINS, configura esse servidor para manter um banco de dados de nomes de computadores e endereços IP. Em uma rede maior, talvez você precise adicionar a função de servidor WINS a outros servidores para assegurar que os computadores clientes sempre tenham acesso a pelo menos um servidor WINS.
- Este computador tem um endereço IP estático.
- Todos os volumes de disco existentes usam o sistema de arquivos NTFS. Volumes FAT32 não são protegidos e não oferecem suporte à compactação de arquivos e pastas, a cotas de disco, à criptografia de arquivos ou a permissões de arquivo individuais.
- O Firewall do Windows está habilitado.
- O Assistente de Configuração de Segurança está instalado e habilitado.

Além desses serviços assistidos por um assistente, o Windows Server 2003 ainda proporciona alguns outros serviços, como:



O sistema de Log Comuns, permite a centralização do sistema de logs de outros servidores, equipamentos de redes e estações de trabalho, em conjunto com recursos de filtros e relatórios, o que proporciona informações mais consistentes e relevantes.



Serviço de certificado, permite o gerenciamento de uma infra-estrutura de chaves públicas (ICP). É possível criar uma autoridade certificadora (CA) local ou associada a uma rede pública, como a ICP-Brasil, e dessa forma emitir certificados legítimos juntamente com smartcards e diversas outras tecnologias de criptografia.

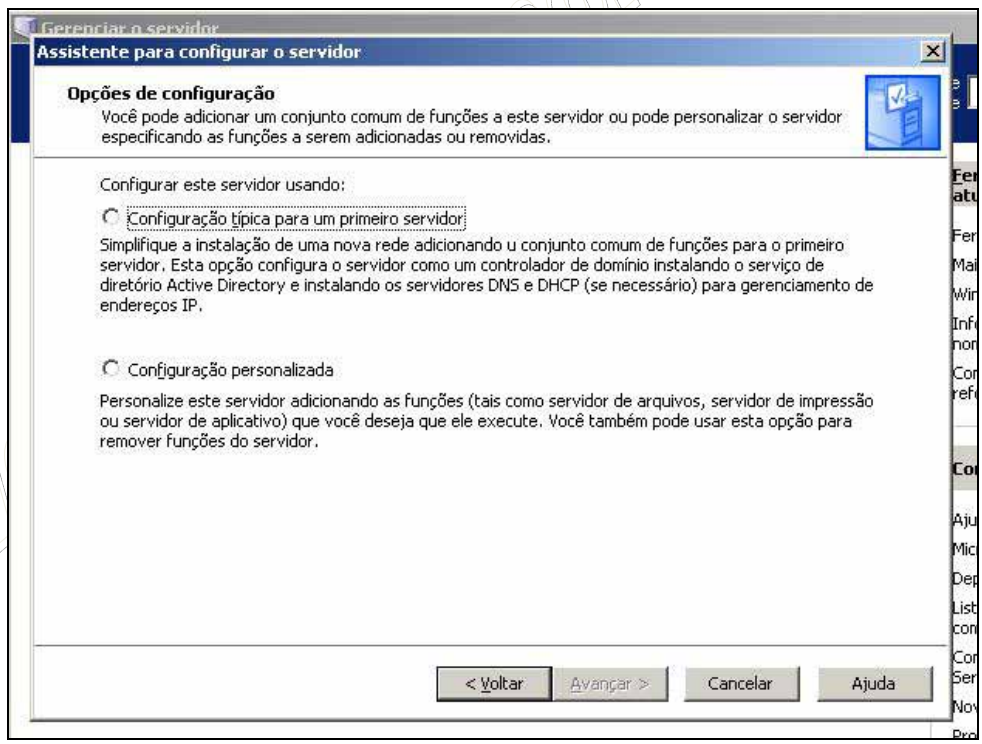
Serviços de rede extras, para compatibilidade com outros sistemas operacionais ou serviços de redes antigos.

Agora que temos noções dos serviços de rede que o Windows Server 2003 pode oferecer estudaremos na próxima competência como instalar e configurar cada um deles.

8 COMPETÊNCIA 2 – MANIPULAÇÃO DE SOS DE REDES

Agora que sabemos o potencial de uso do Windows Server 2003 como um sistema operacional de redes, chegou o momento de aprendermos a manipular seus serviços. Começaremos pelos serviços básicos de rede, aqueles que atendem a maioria das pequenas e médias empresas. Em seguida estudaremos as ferramentas utilizadas para administração do servidor e dos seus respectivos serviços. Veremos ferramentas de segurança e backup, para logo em seguida aprofundarmos nos serviços avançados de rede. A cada passo veremos os conceitos vistos sobre servidor de rede realizando práticas sobre a manutenção básica de um sistema operacional de redes baseado em Microsoft Windows Server 2003.

Mas para começar, o que seriam serviços básicos de redes? Entendemos como serviços básicos aqueles serviços mais utilizados pela maioria dos clientes. E como saber quais são estes serviços? Desde o surgimento da Internet, por volta de 1985, as listas de discussões sobre como instalar serviços de redes têm crescido bastante. É sobre estas perguntas mais freqüentes que identificamos os serviços mais demandados pelas empresas, e que na verdade oferecem suporte a uma gama de outros serviços. No Windows Server 2003, encontramos uma própria recomendação da Microsoft sobre a instalação dos serviços básicos, e que se apresenta para o administrador de redes como um assistente de instalação de novos serviços, observe a tela abaixo:

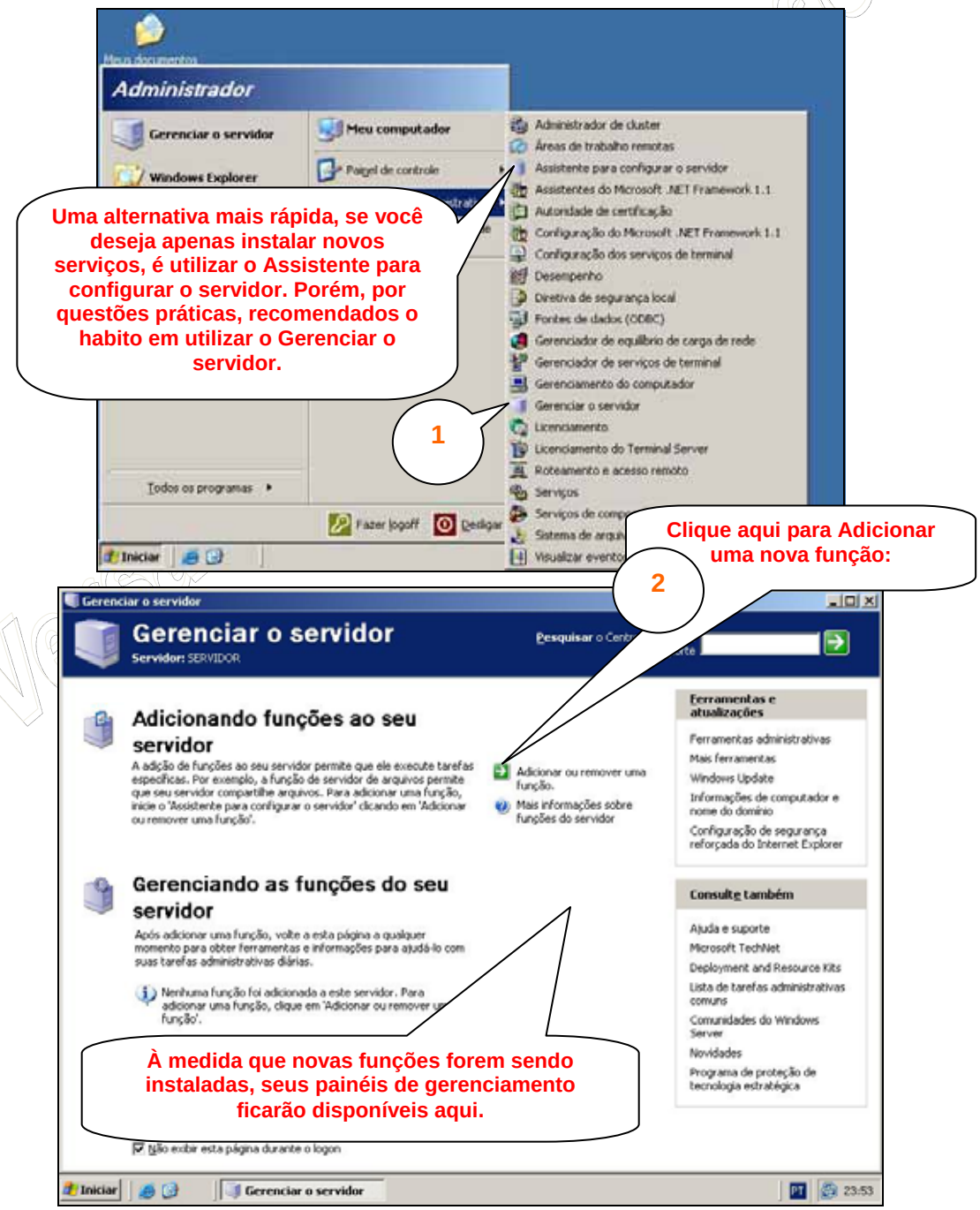


Assim que instalamos um novo servidor e efetuamos o logon pela primeira vez o assistente para configuração do servidor é executado. Este assistente traz a opção de realizarmos uma "Configuração típica para um primeiro servidor", que consiste na instalação dos serviços: Controlador de Domínio, DNS e DHCP.

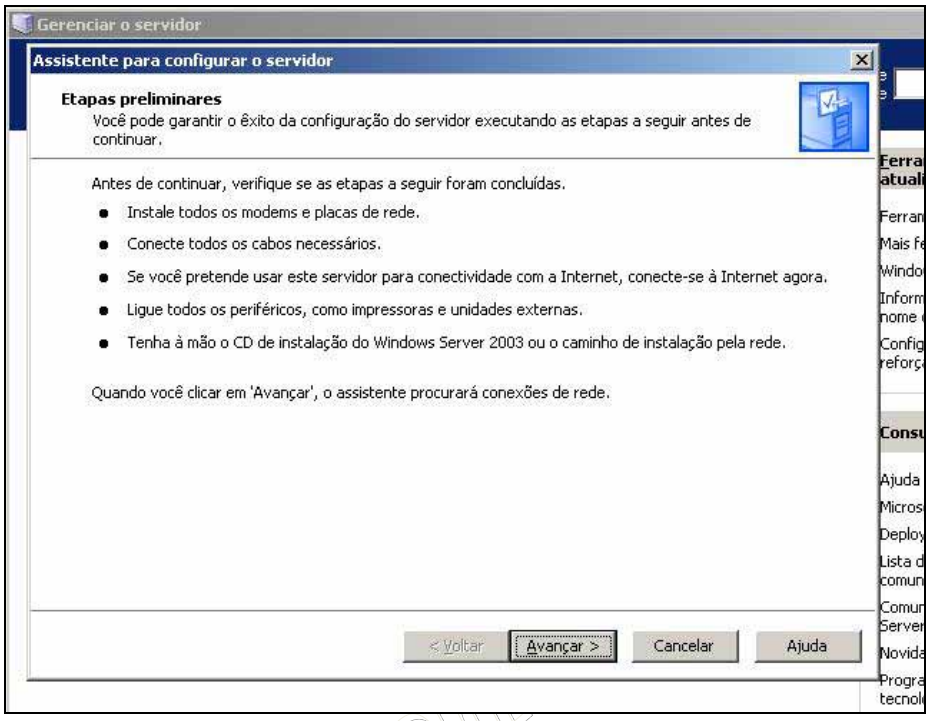
O Controlador de Domínio, como vimos na primeira competência, é o servidor responsável pelo banco de usuários e senhas da rede, além de outros recursos. O DNS é o servidor responsável por traduzir os nomes em endereços IP. O DHCP é o serviço que configura automaticamente os dados de rede nas estações de trabalho que estiverem ligadas ao mesmo HUB ou Switch.

Vamos então partir para a “Configuração personalizada”, onde além de instalador os serviços típicos recomendados, iremos também instalar os serviços de: Servidor de Arquivos, Servidor de Impressão e WINS. Os quais entendemos como essenciais para qualquer empresa. O Servidor de Arquivos é o servidor de rede responsável por compartilhar em um local central todos os arquivos e dados dos usuários da rede. O Servidor de Impressão é o responsável por centralizar todas as impressoras, mesmo que estas estejam instaladas em máquinas distintas da rede, e os drivers para instalação dessas impressoras. Por último, o WINS, que é semelhante ao DNS mas para um escopo menor, apenas em redes locais. O DNS, em conjunto com o WINS, proporcionam o melhor desempenho possível na tradução de nomes e domínios para IP.

Para começar a instalação dos serviços vamos chamar o Gerenciador do Computador, anote bem este paço pois ele será executado diversas vezes a partir de agora:

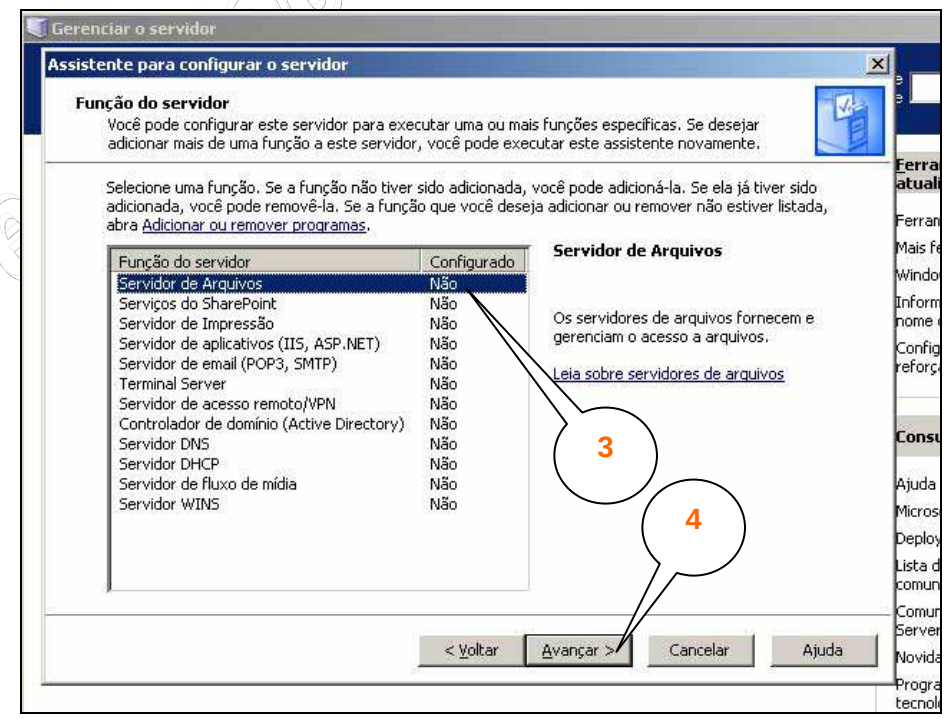


Uma das vantagens na utilização do assistente do próprio Windows é que ele já vem previamente preocupado em não deixar o administrador se esquecer de etapas preliminares, como:



Tenha certeza de que todas estas etapas foram atendidas antes de iniciar a instalação, caso contrário você corre o risco de ter uma instalação corrompida, onde em casos extremos, será necessário reinstalar todo o servidor.

E finalmente a tela de instalação dos serviços, ou funções do servidor:

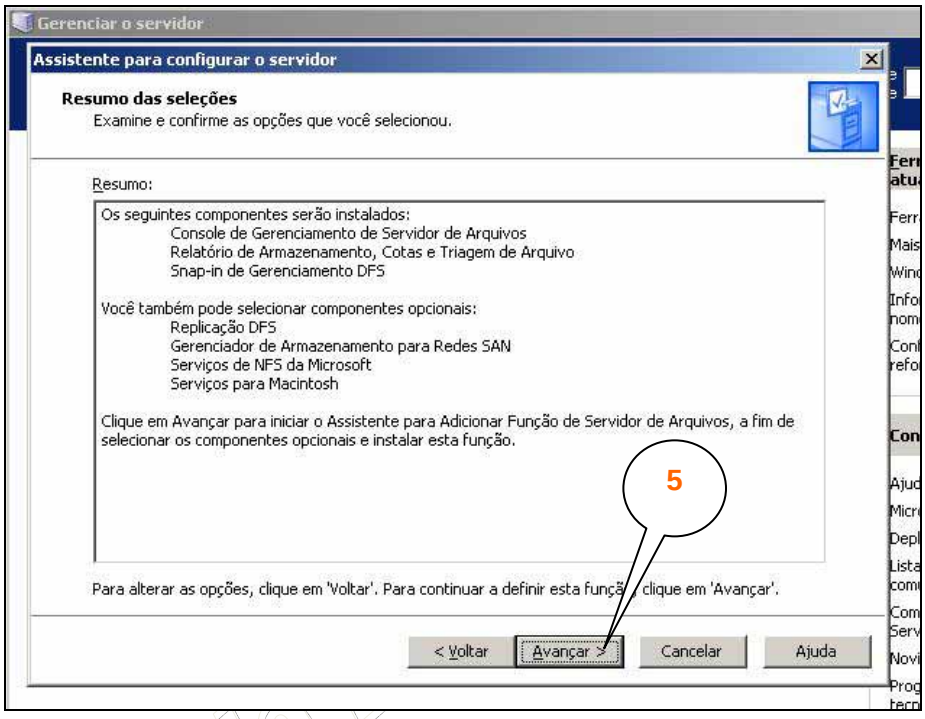


8.1 SERVIÇOS BÁSICOS DE REDE

Para a maioria das empresas, em especial as empresas de pequeno e médio porte, os seguintes serviços de redes serão desejados: servidor de arquivos, servidor de impressão, controlador de domínio (Active Directory), servidor DNS, servidor DHCP e servidor Wins. Veremos nesse capítulo como configurar cada um desses serviços.

Servidor de Arquivos

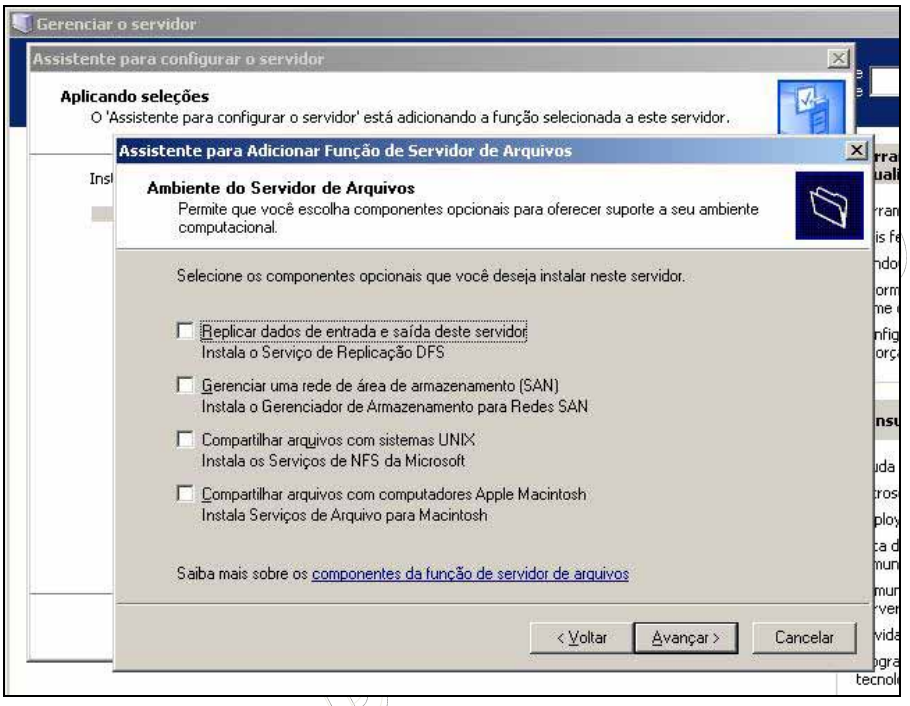
Uma vez iniciado o “Assistente para configurar o servidor” e avançando sobre a instalação do servidor de arquivos, somos apresentados a seguinte tela:



Aqui observamos que ao selecionar o Servidor de Arquivos para ser instalado, ele já vem com os seguintes pacotes prontos para execução: “Console de Gerenciamento de Servidor de Arquivos”, “Relatório de Armazenamento, Cotas e Triagem de Arquivo” e “Snap-in de Gerenciamento DFS”.

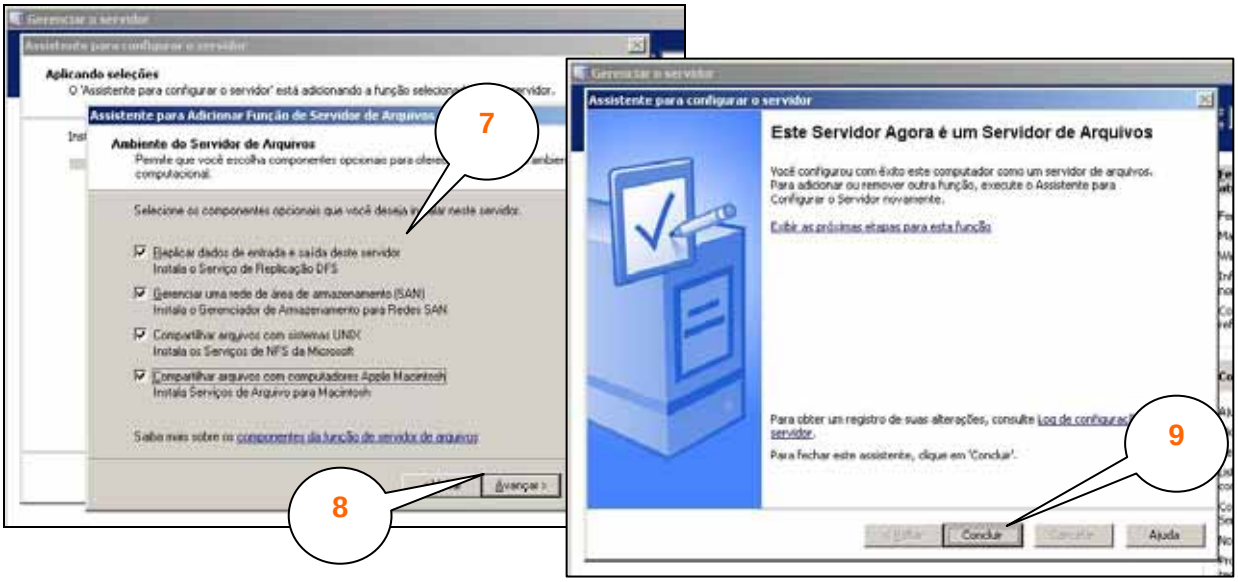
O Console de Gerenciamento é a interface que iremos utilizar para configurar o Servidor de Arquivos, o Relatório de Armazenamento são modelos pré-configurados que nos ajudam a criar monitores agendados sobre o uso dos arquivos em nosso servidor, como espaço utilizado, arquivos maiores de 200Mb, entre outros. Cotas é o sistema que monitora o uso do espaço em disco pelos usuários, proibindo ou alertando ao administrador sobre o excesso de uso por parte dos usuários. Triagem de arquivos é o sistema que proíbe que os usuários salvem determinados tipos de arquivos no servidor. O Snap-in de Gerenciamento DFS (Distributed File System) é a interface que nos permite juntar diversos compartilhamentos espalhados em rede em um único servidor e gerenciar diversos servidores de arquivos espalhados em uma rede.

Ao inicializar e avançar o assiste nos serão questionado sobre outras funções para o servidor de arquivo, como: “Replicação DFS”, “Gerenciador de Armazenamento para Redes SAN”, “Serviços NFS da Microsoft”, “Serviços para Macintosh”.

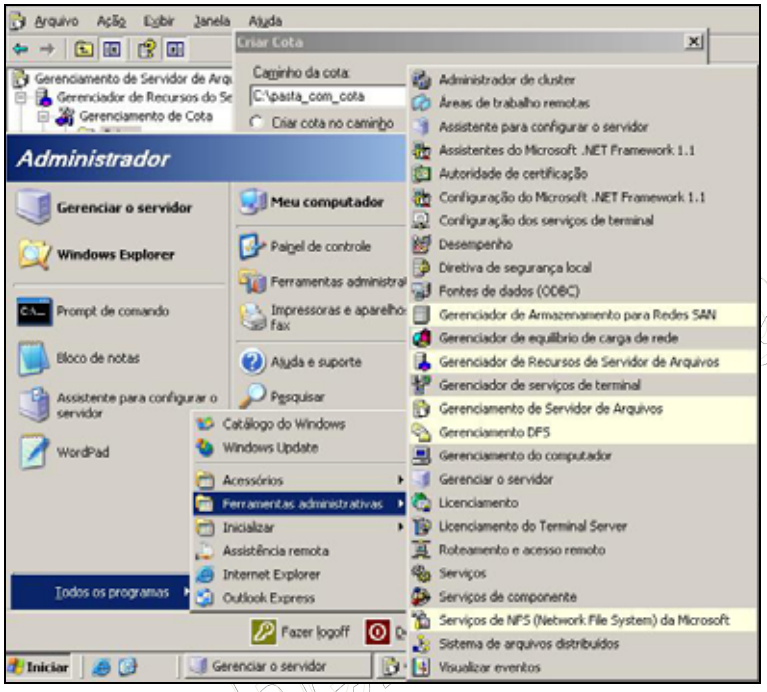


A Replicação DFS é o serviço que permite replicar dados entre servidores de rede. Isto possibilita realizar uma redundância dos dados, a fim de garantir a segurança e o backup centralizado. O Gerenciamento de Redes SAN (Storage Area Network) é o serviço que permite administrar e interagir com dispositivos de armazenamento remotos. Estes dispositivos são equipamentos, especialmente equipados com diversos discos físicos, de forma a armazenar maiores volumes de dados do que os limitados slots das placas mães de computadores. Como exemplo, enquanto que um servidor modesto pode acumular até 04 discos físicos de 500 Gb cada, um equipamento SAN pode acumular entre 16 à 32 discos de mesmo tamanho.

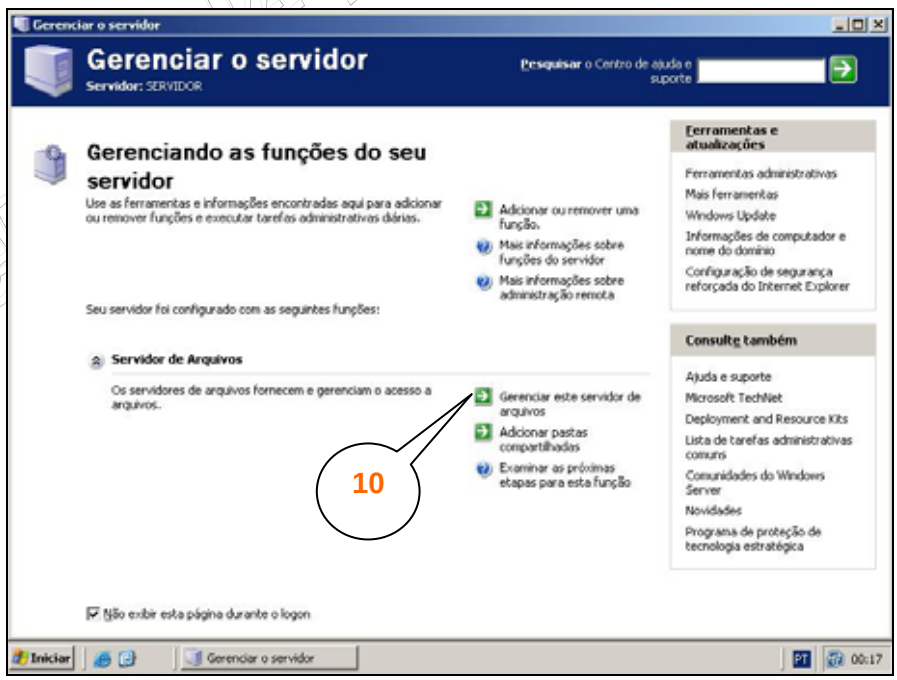
O Windows Server 2003 prove suporte a comunicação com outros sistemas operacionais, como o caso do Unix e do Macintosh. Para isso oferece o serviço NFS e o protocolo Apple. Esses protocolos são importantes quando temos uma rede heterogenia, formada por estes três sistemas operacionais citas. Porém, se não for o caso da sua rede, mantenha estes protocolos desativados, pois eles exigem maiores consumo de hardware. Por questões de aprendizado iremos selecionar todos os serviços opcionais e finalizar o assistente:

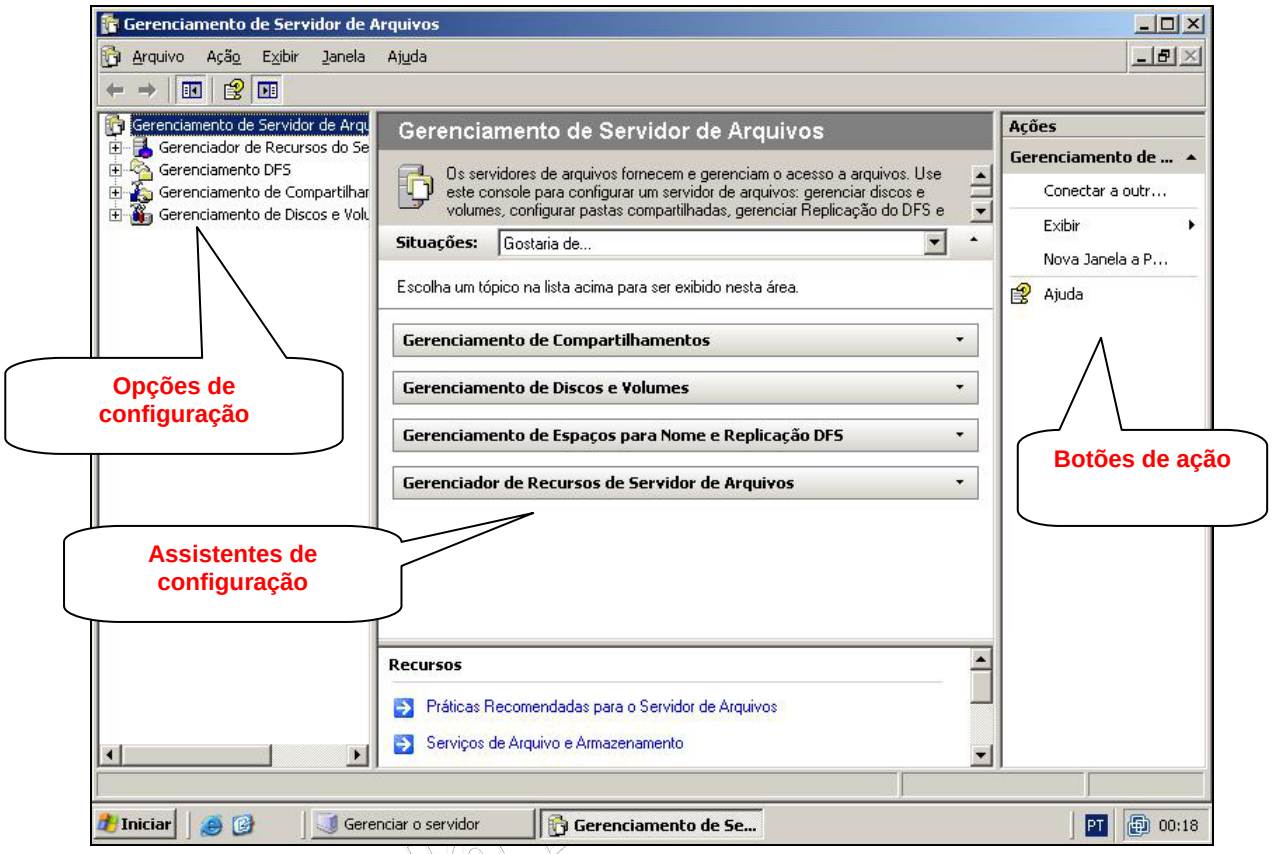


Uma vez instalado o Servidor de Arquivos, uma série de novos ícones ficam a nossa disposição no item de Ferramentas Administrativas, outra alternativa para configurar o servidor:



Voltamos agora para a interface do “Gerenciar o servidor” e vamos conhecer as possibilidades de uso e configuração deste novo servidor:

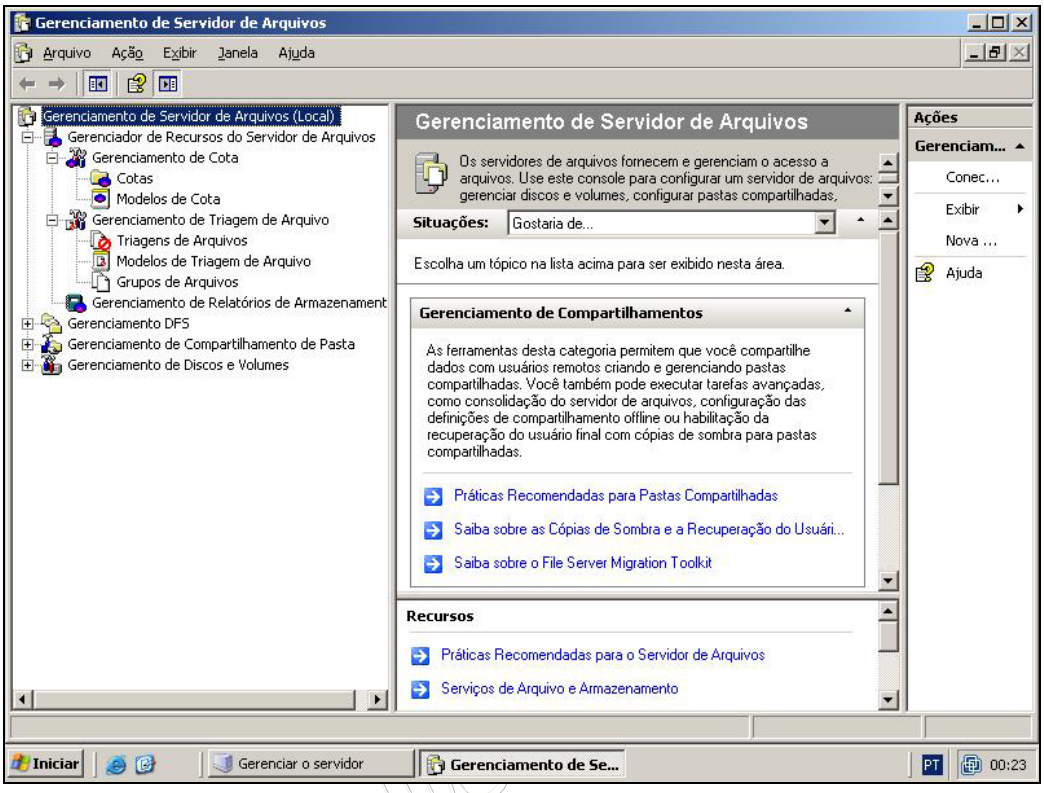




Aqui vemos o Gerenciador de Servidor de Arquivos, o primeiro item instalado, e padrão, do servidor de Arquivos. É nesta interface que estão agrupadas todas as ferramentas individuais para manipulação nos arquivos do servidor.

Nesta primeira janela, encontramos ao centro, diversos assistentes que nos orientam nas configurações do servidor de arquivos. É muito importante ressaltar, para aqueles que já vem de um Windows 2000 Server, que a partir da versão Windows Server 2003, a Microsoft não disponibiliza o servidor pronto para executar após sair da caixa. Ou seja, é necessário instalar e configurar cada recurso desejado. Por um lado isso é bom pois aumenta a segurança do sistema, por outro é ruim pois não permite fácil dedução para seu uso. Mas para compensar o excesso de segurança, a Microsoft disponibilizou estes assistentes, que encontram-se facilmente em todo o ambiente.

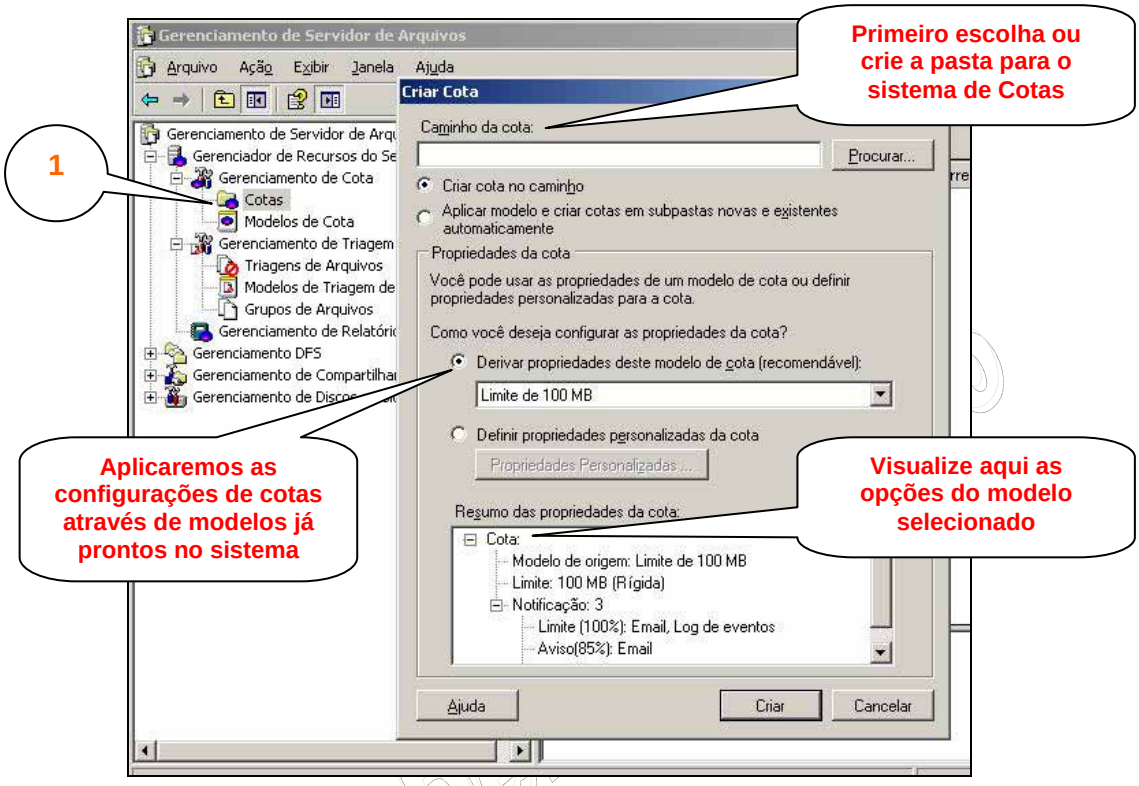
Veja o exemplo de uso de um desses assistentes:



Vamos para a primeira observação. Caso, após a instalação, você se depare com a seguinte mensagem de erro:

Esse erro ocorre em função de após você ter instalado o servidor de arquivos não ter reinicializado o servidor. Reinicialize que o erro não mais aparecerá.

Agora vamos para a primeira opção de configuração do servidor de arquivo, o sistema de cotas. Siga os passos na imagem abaixo para localizar as configurações para cotas. Em seguida, clique com o botão direito do mouse sobre “Cotas” e clique em “Criar Cota”. Iremos agora adicionar uma nova monitoração de Cotas para pastas do sistema, ou seja, passaremos a ter restrições de uso do espaço em disco, por parte dos usuários, e relatórios automáticos para acompanhamento:

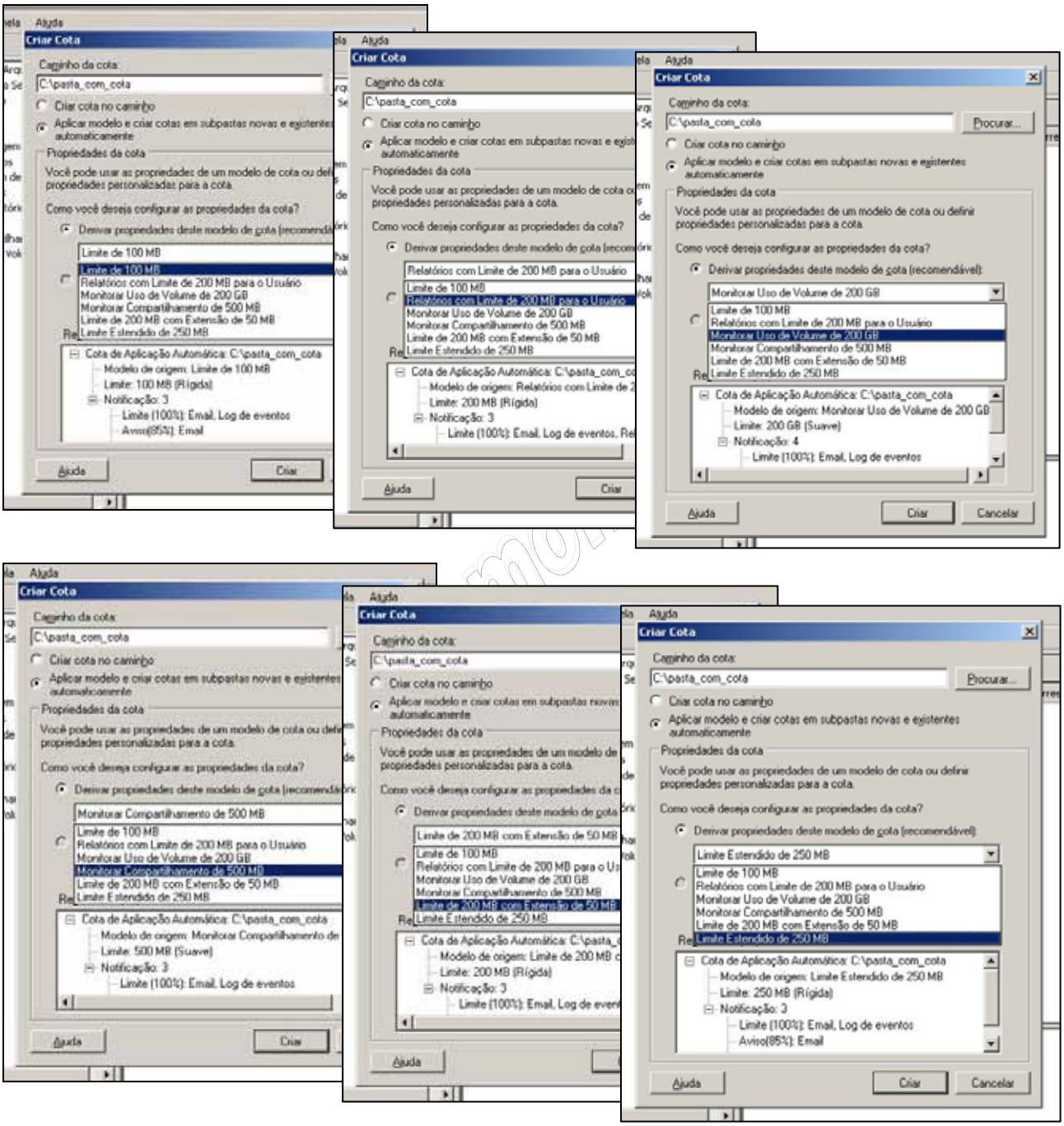


Você pode escolher aplicar um modelo de cotas para uma determinada pasta, por exemplo: c:\dados, ou escolher uma ramificação de pastas e aplicar modelos diferentes, por exemplo: c:\dados\modelo1 e c:\dados\modelo2, onde c:\modelo não está sujeito ao sistema de cotas e as subpastas modelo1 e modelo2 cada uma está regida por um modelo diferente de cotas.

Antes de configurar o sistema de cotas tenha a plena certeza do que deseja fazer, pois remover o sistema não é tão simples quanto instalar.

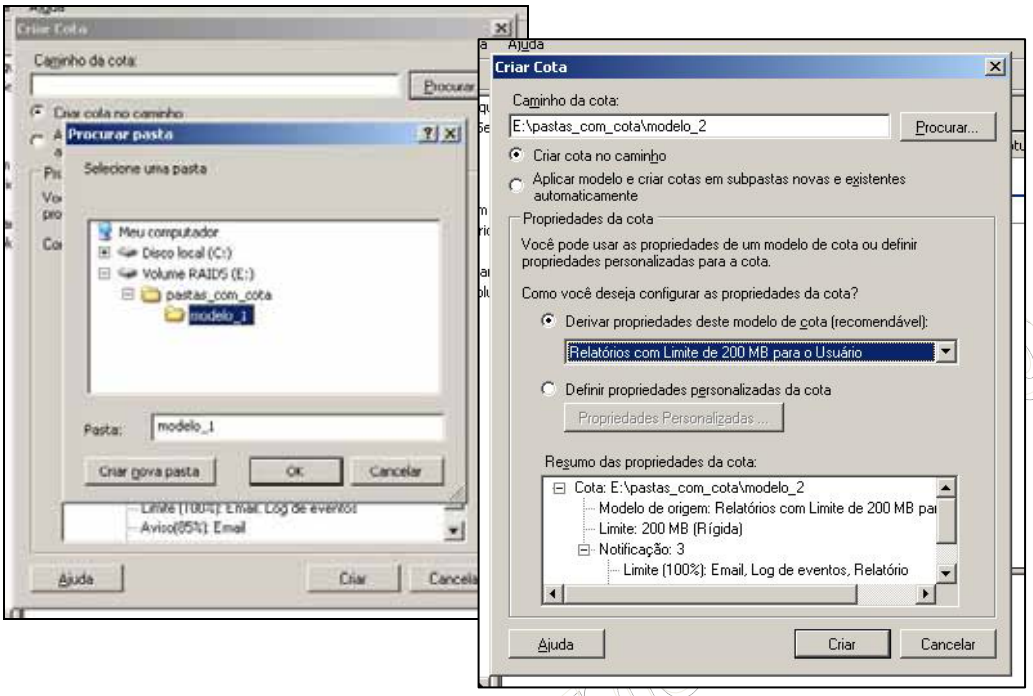
Vamos dar um exemplo prático, vamos supor que em nossa rede temos 3 departamentos: compras, vendas e financeiro. Em cada departamento existe uma coordenação. Criaremos a seguinte estrutura de Cotas para os usuários de nossa rede: c:\dados, c:\dados\operacional (aplicando modelo 1 de Cotas) e c:\dados\coordenacao (aplicando modelo 2 de Cotas). Em c:\dados\operacional, todos os funcionários operacionais da empresa poderão armazenar seus dados pessoais, limitados a 1 Gb cada. Já em c:\dados\coordenacao, apenas os coordenadores poderão armazenar seus dados aqui, e a restrição de 1 Gb já é flexível, ou seja, é possível passar de 1Gb e tanto o administrador do sistema quando o usuário receberão um aviso de que foi extrapolado o limite de uso, porém não impede que o usuário continue a utilizar e gravar novos dados.

Vejamos agora cada um dos seis modelos pré-disponíveis através do Windows Server 2003, recomendados que para uma melhor visualização e compreensão, todas as telas aqui apresentadas tentem ser acessadas por você em seu próprio Windows Server 2003:

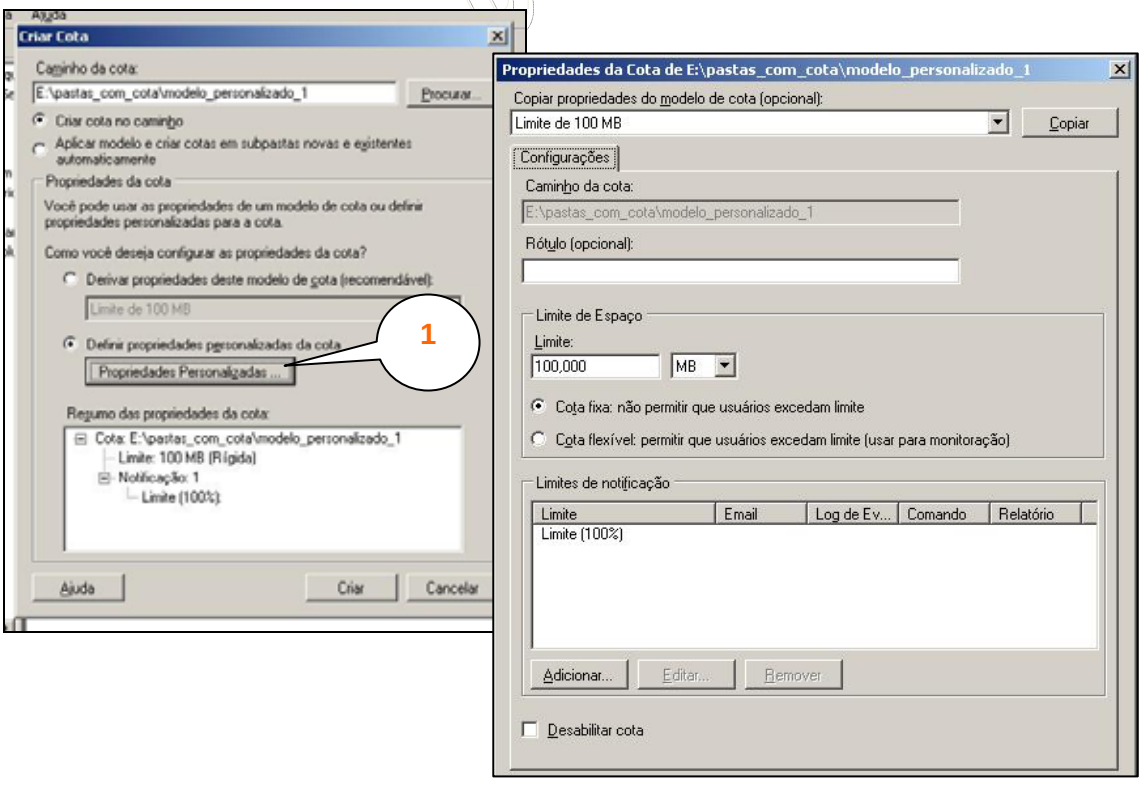


Agora que sabemos utilizar os modelos de Cotas e o próprio sistema de Cotas, vamos aprender como personalizar as Cotas para nossas atividades do dia-a-dia:

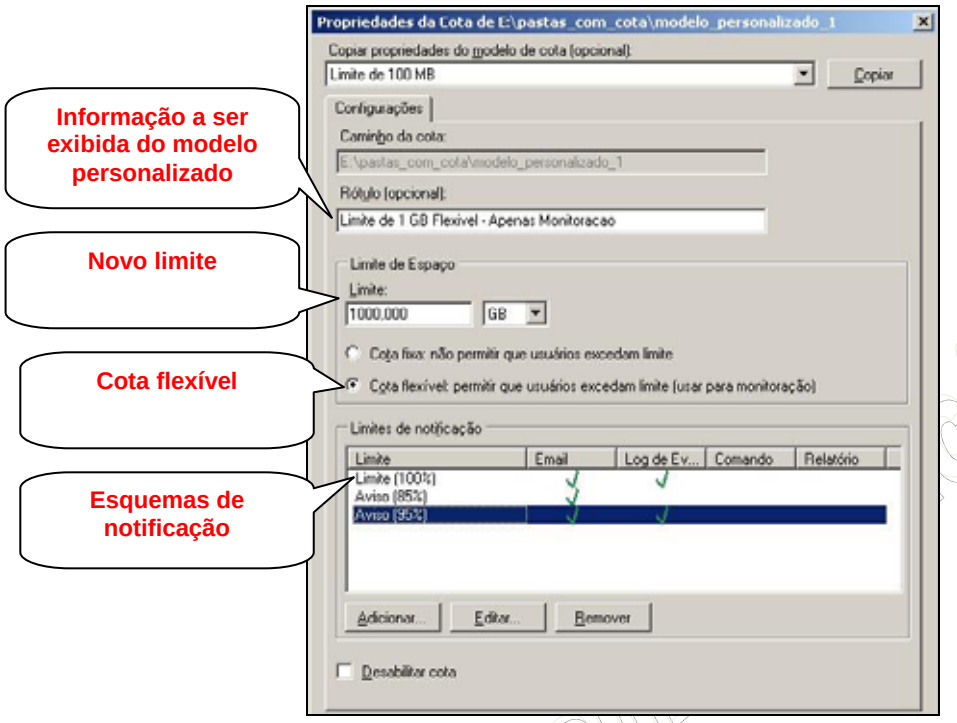
A primeira ação é criar um pasta no disco dinâmico RAID-5 (e:\pastas_com_cotas) de onde criaremos as demais subpastas (modelo1, modelo2 e modelo_personalizado1), cada qual com seu respectivo modelo de Cotas:



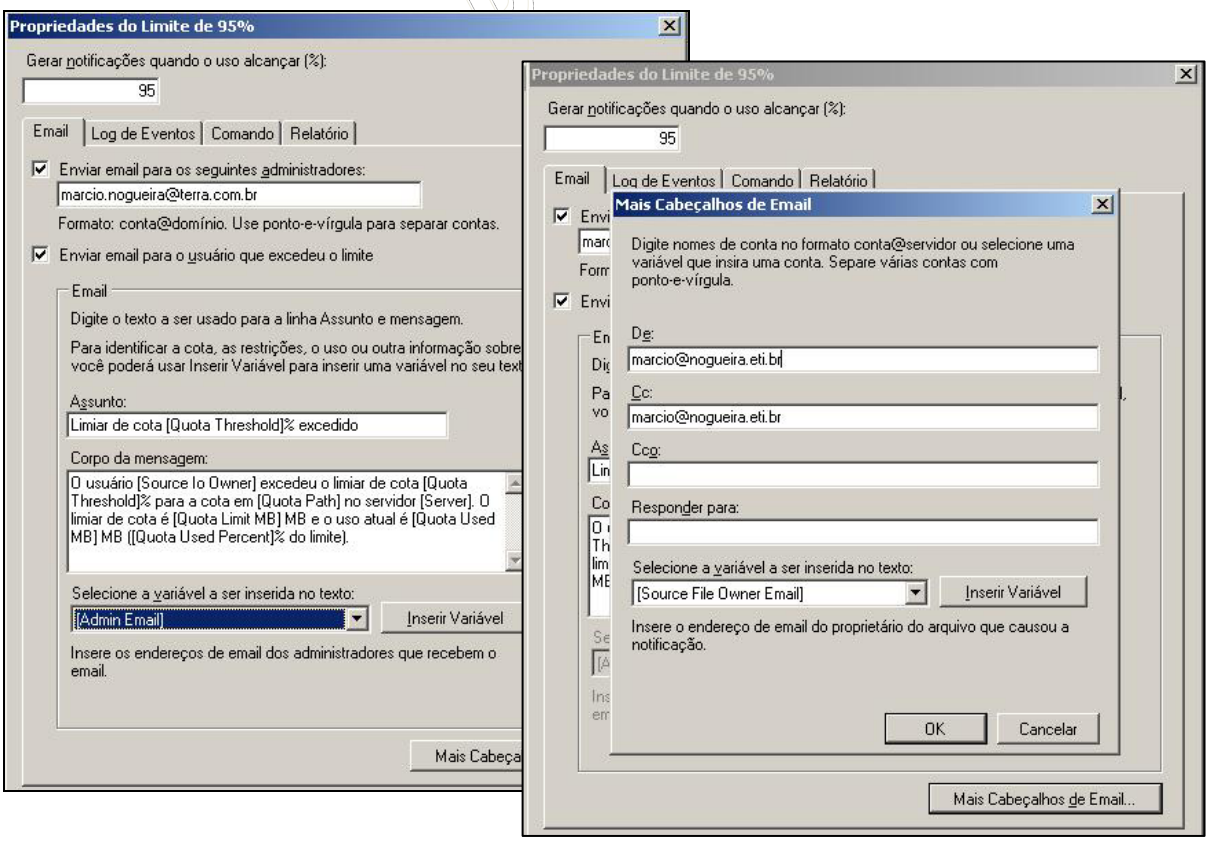
Agora vamos criar na subpasta e:\pastas_com_cotas\modelo_personalizado_1 um sistema de Cotas personalizado:



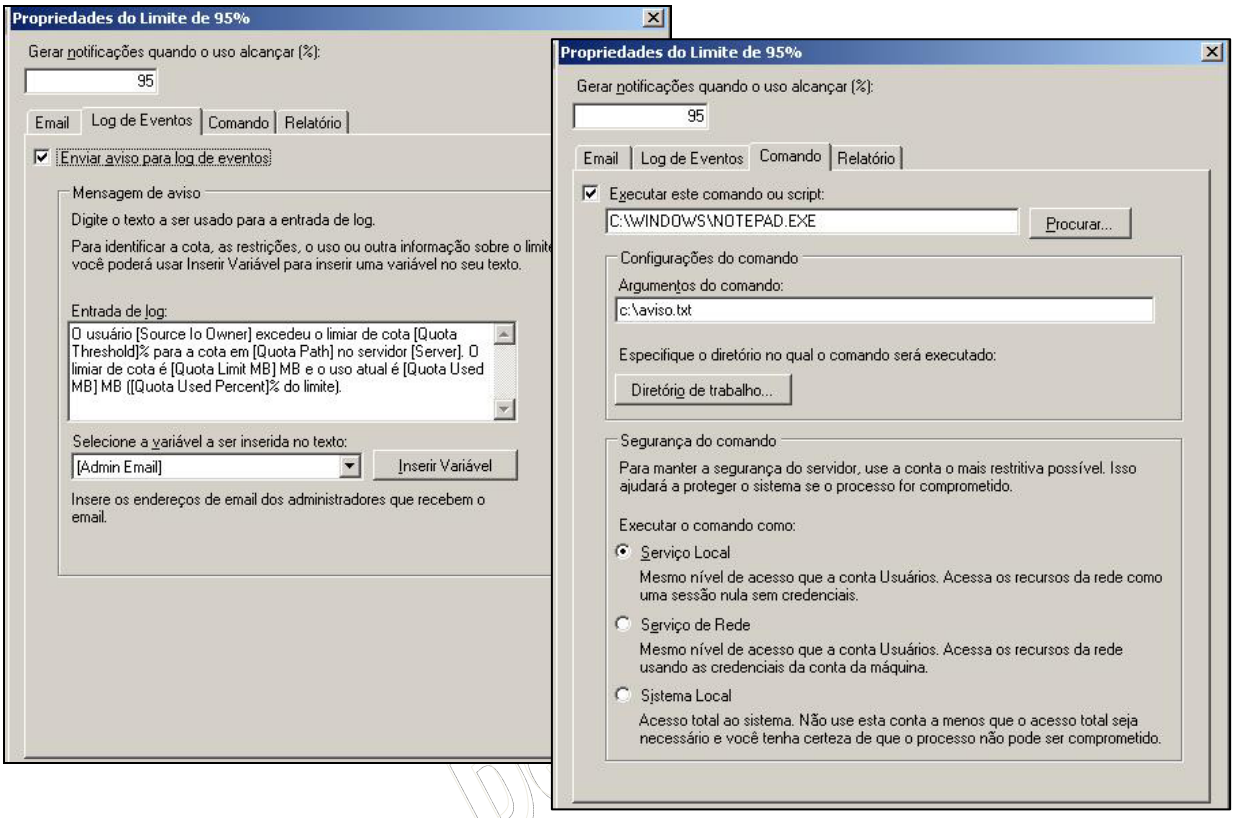
Após realizar uma cópia do modelo em questão, iremos personalizar nossa pasta para um Limite de 1 Gb, flexível, ou seja, não irá impedir que usuários possam extrapolar seus limites, apenas irá notificar sobre o uso excedente. As notificações serão realizadas da seguinte forma: Quando o percentual de uso de 85%, do espaço permitido, for alcançada uma notificação via e-mail, para o usuário e o administrador, será enviado. Quando o percentual alcançar a taxa de 95% e 100%, além de enviar um e-mail será registrado no Log de Eventos do Windows Server 2003. Veja as configurações na próxima imagem:



As alternativas para os limites de notificação são demonstradas abaixo, começando pelas opções de configuração do envio por e-mail:

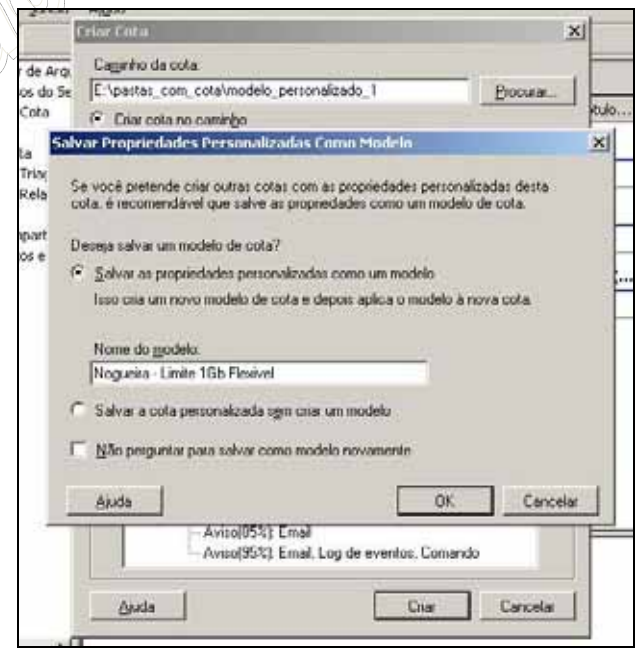


Em seguida são configuradas as notificações para o Log de Eventos do Windows e comandos externos que podem ser executados no momento em que o agente monitorador for executado:

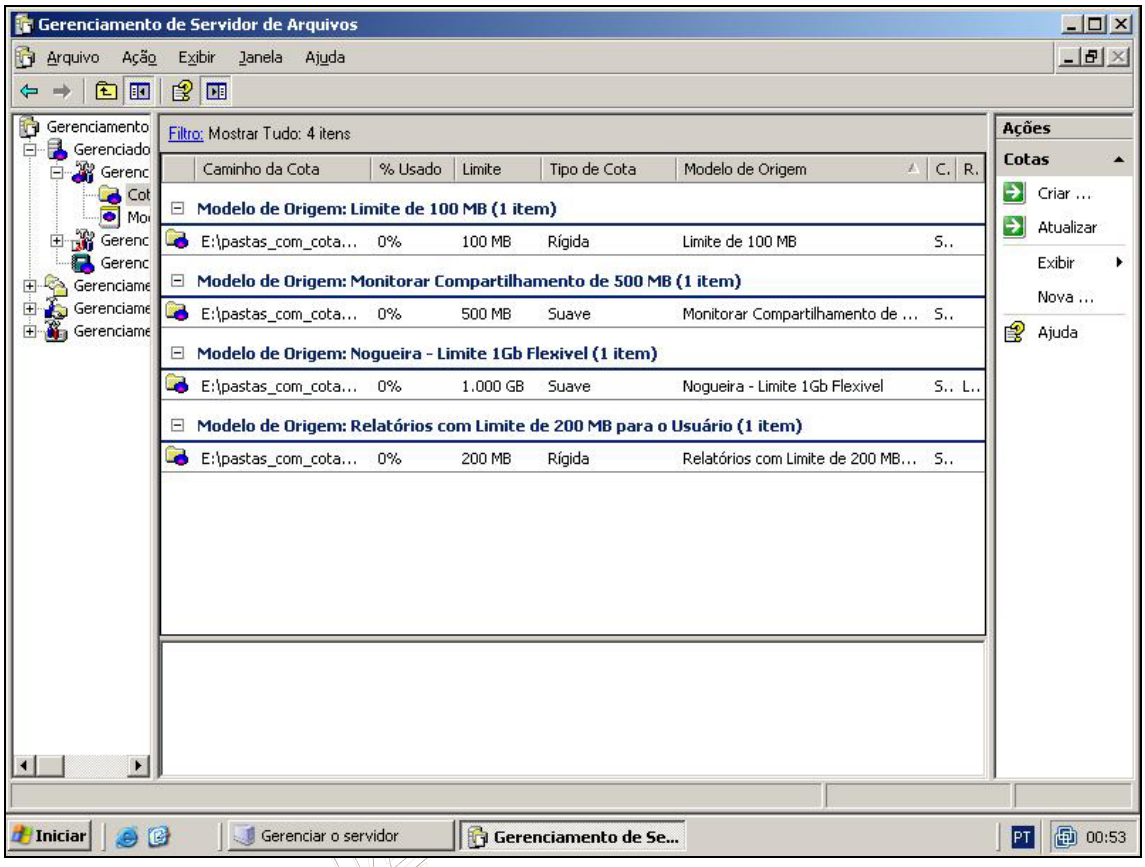


No exemplo acima, quando o agente monitorador for executado ao uso do espaço em disco por 95%, um arquivo texto c:\aviso.txt será executado na tela do usuário, porém este exemplo só é válido caso o usuário esteja logando no próprio servidor.

Por fim podemos salvar esse nosso modelo personalizado para uso futuro:

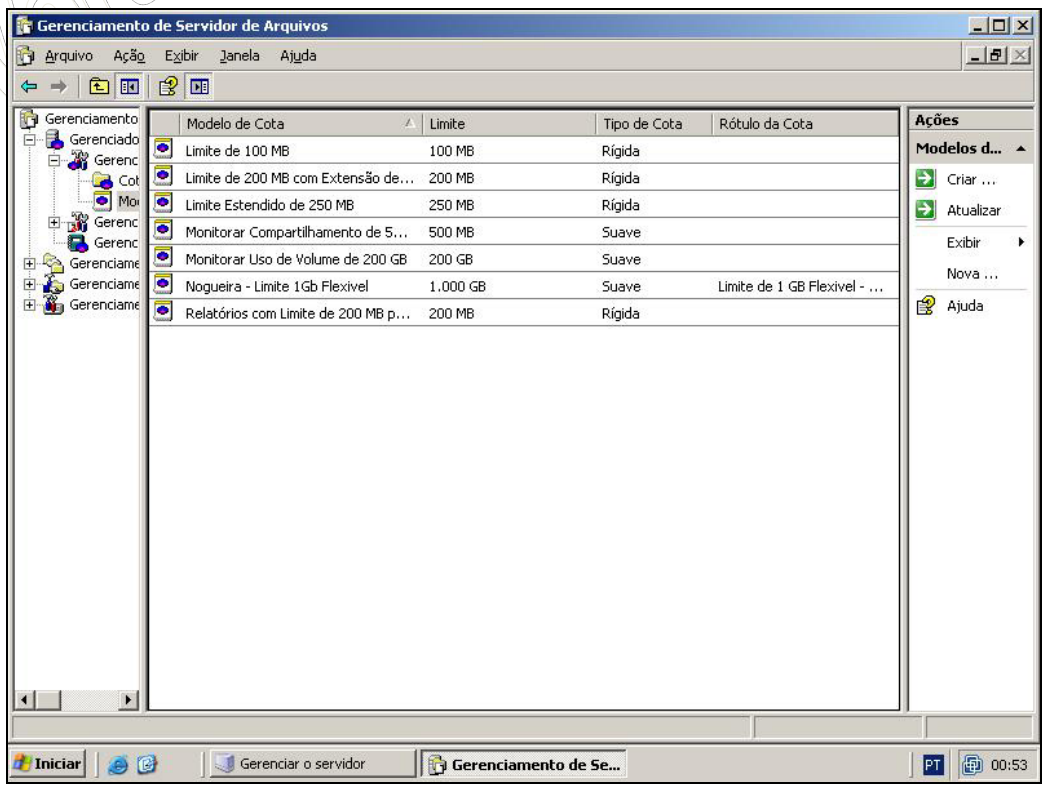


Observe o resumo dos modelos de cotas aplicados as subpastas: modelo1, modelo2, modelo3 e modelo_personalizado_1:



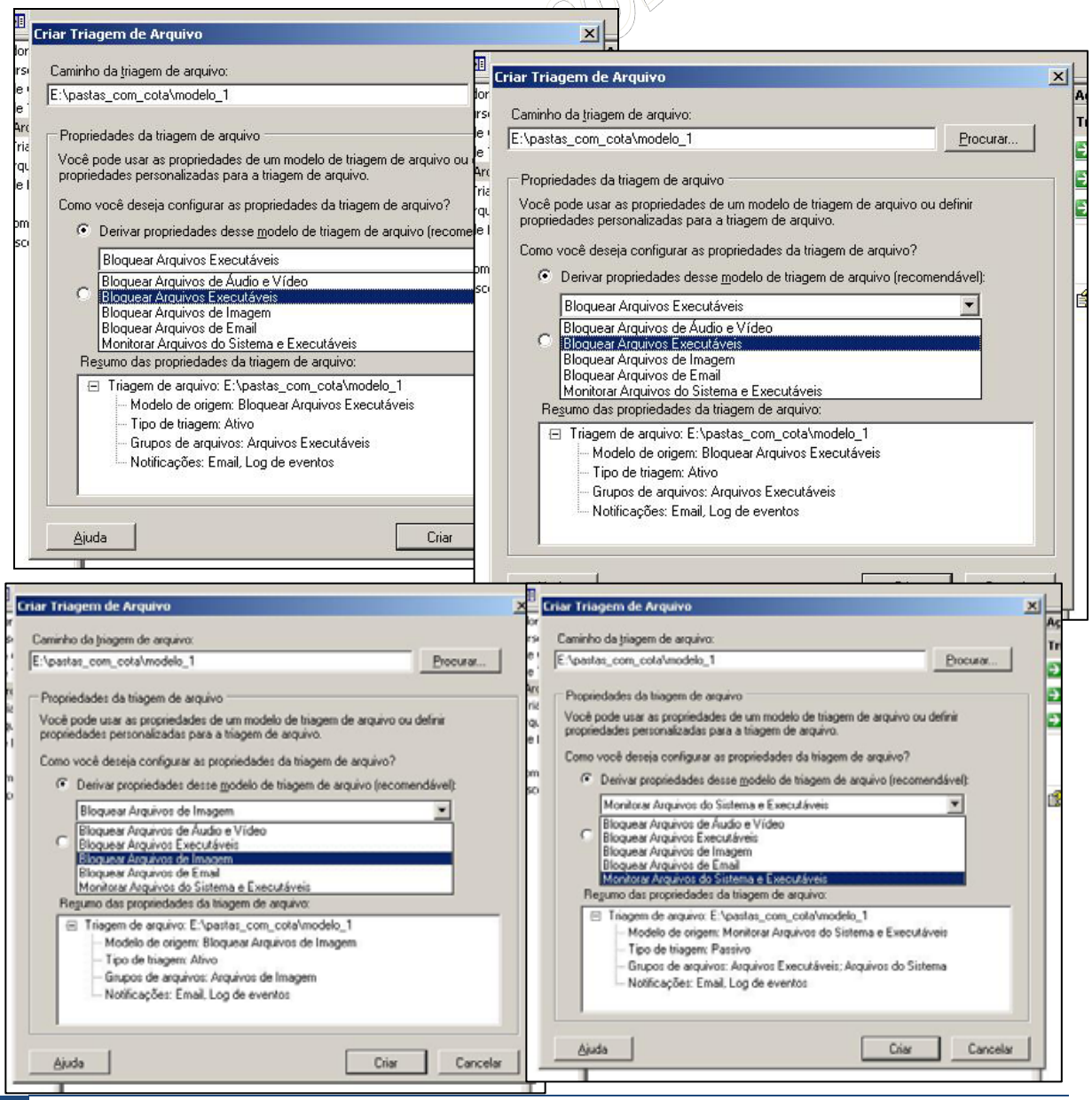
Como exercício, é verdade que o modelo aplicado na segunda pasta, visualizada no gerenciamento do servidor de arquivos, permite que os usuários extrapolem o limite de 2 Gb em suas pastas? Resposta: sim, é verdade. O limite é de 500 MB, porém suave, ou seja, permite que o usuário extrapole esse valor sem restringir que o mesmo grave novas informações.

Vejamos agora a aba de "Modelos de Cotas", onde encontraremos um resumo de todos os modelos disponíveis no sistema, inclusive aqueles criados por nós:

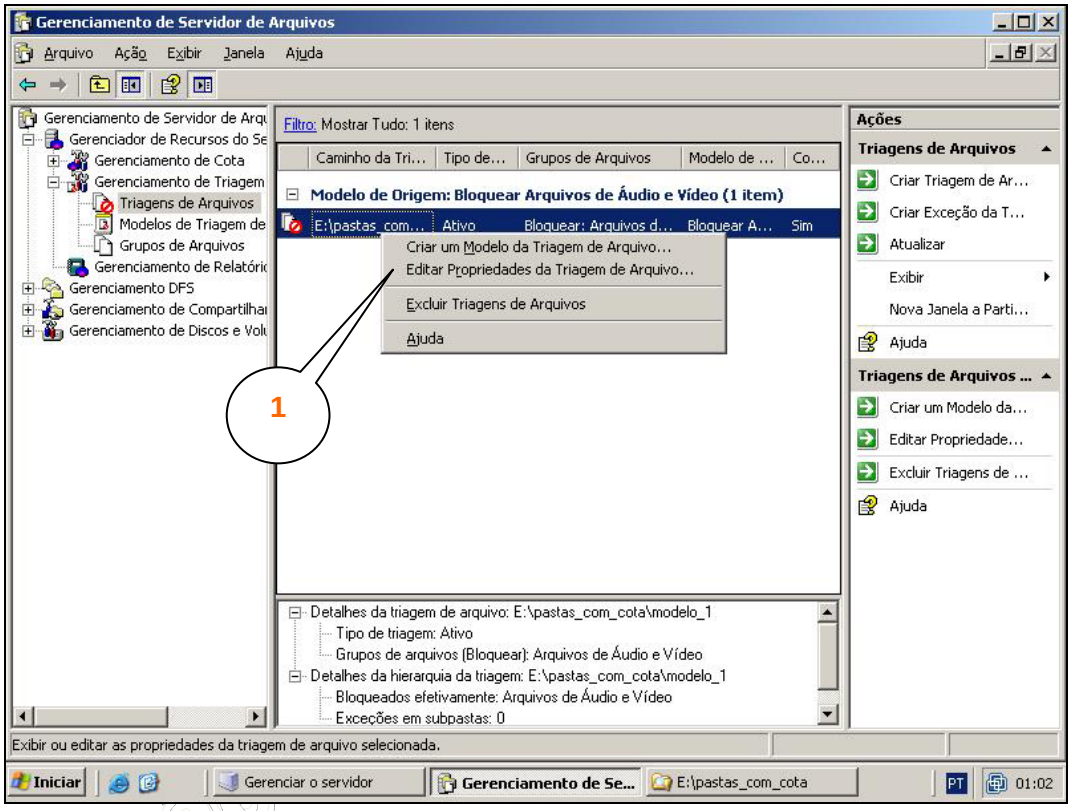


Vamos agora ver as opções do serviço de Triagem de Arquivos, o próximo item após o Gerenciamento de Cotas:

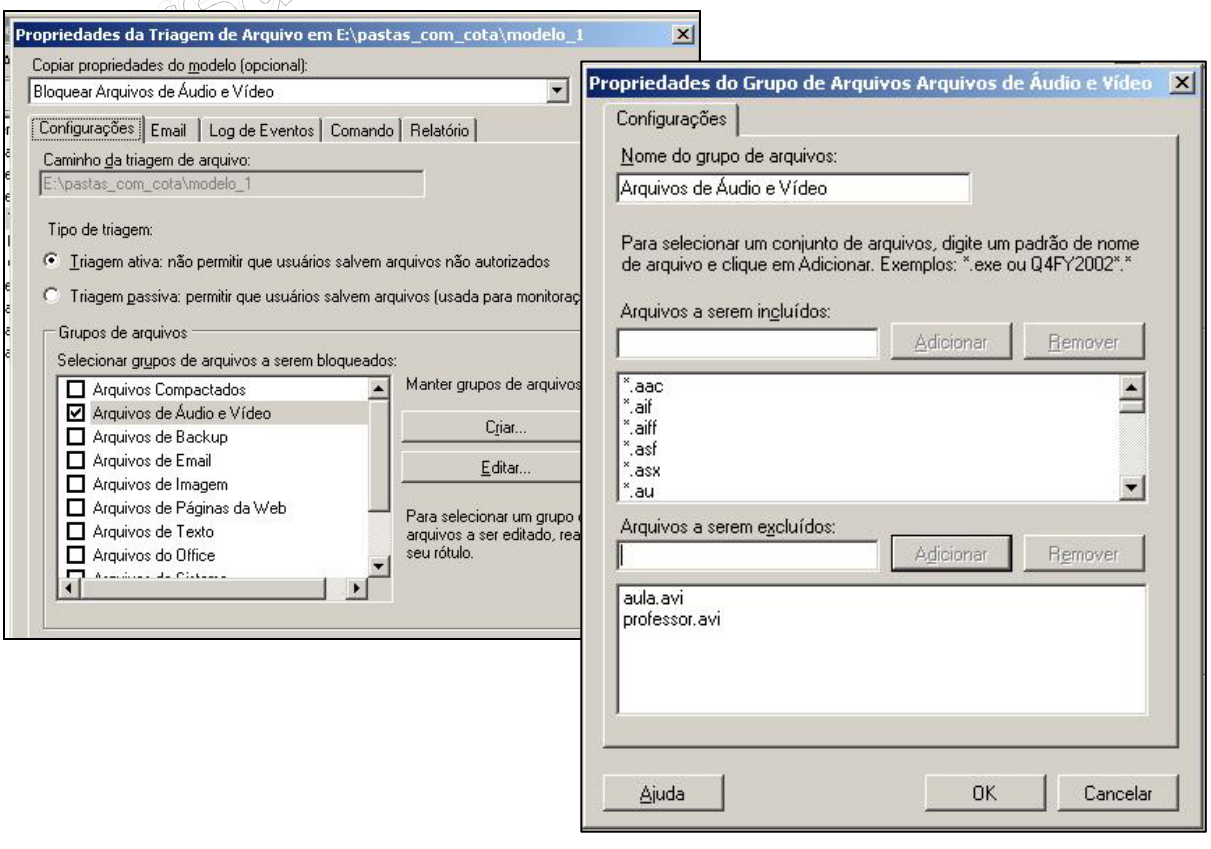
A triagem de arquivos impede que os usuários da rede, salvem nas pastas compartilhadas pelo servidor, arquivos proibidos, como: jogos, músicas piratas e vírus. Sua configuração é semelhante ao Gerenciamento de Cotas, ou seja, definimos as pastas a serem restritas e aplicamos modelos pré-disponíveis pelo Windows, vejamos estes modelos disponíveis:



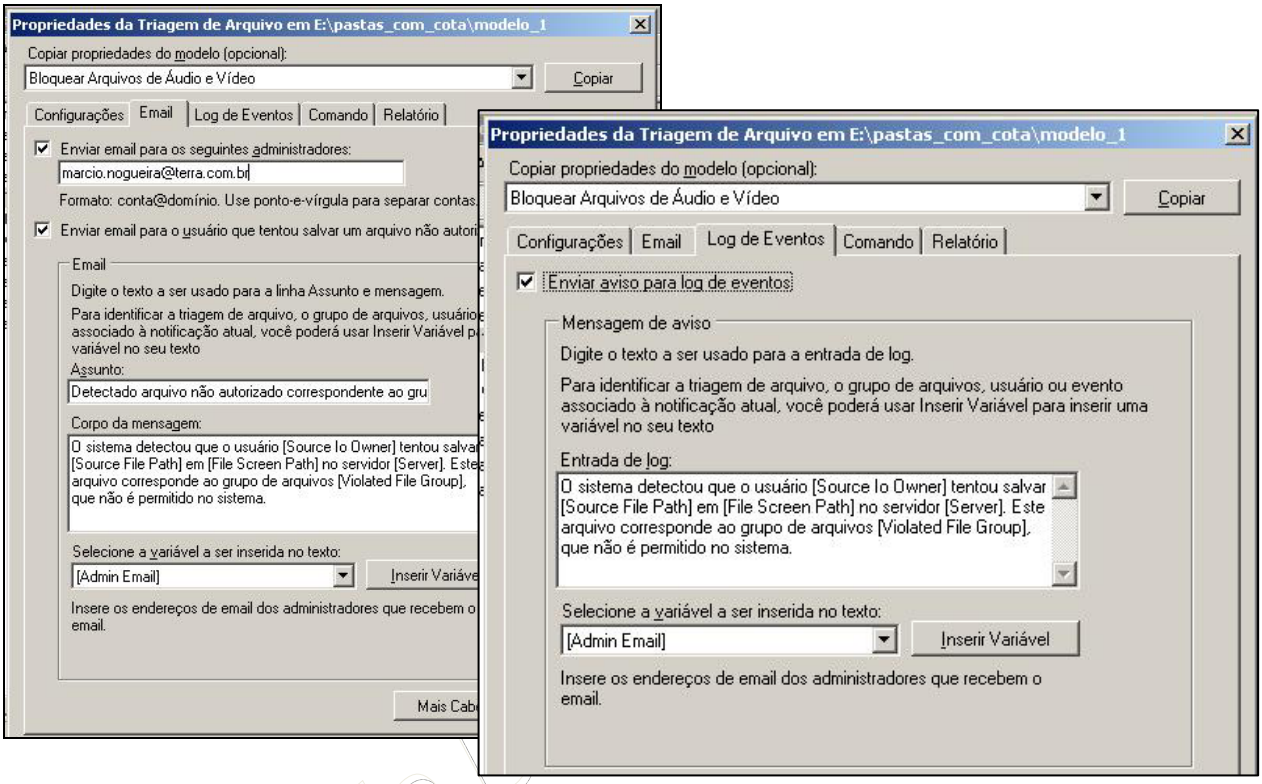
Como no sistema de Cotas, também podemos editar os modelos padrões. Vamos exemplificar essa ação através da seguinte necessidade: vamos restringir todo e qualquer tipo de arquivo de Áudio e Vídeo de serem salvos nas pastas compartilhadas, com exceção dos arquivos especiais: aula.avi e professor.avi, que são os arquivos efetivamente utilizados no negócio da nossa empresa. Dessa forma, vamos modificar o modelo padrão de Triagem de forma a atender nossa realidade:



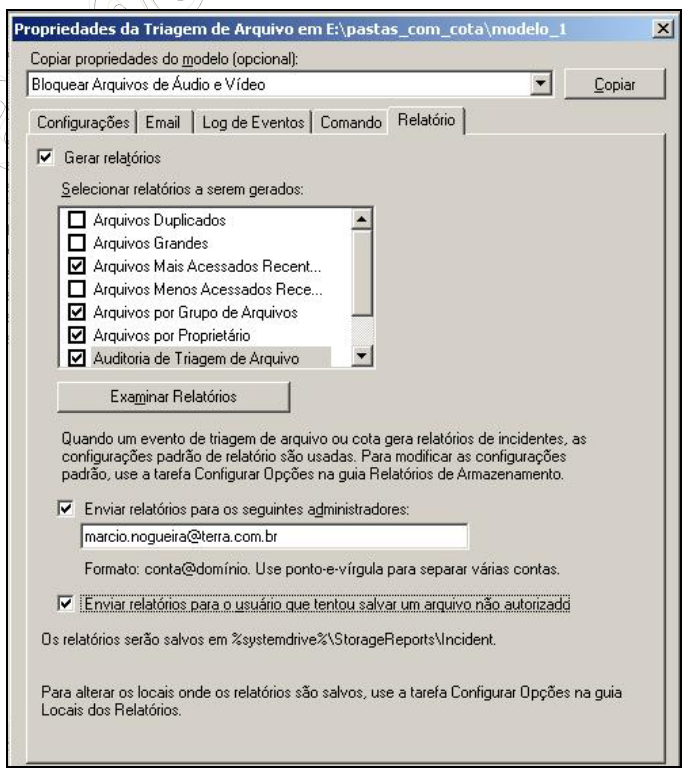
Seguem as telas de configuração:



Após configurada a Triagem podemos definir os padrões para notificação:



E podemos também gerar os relatórios para esse sistema de triagem:

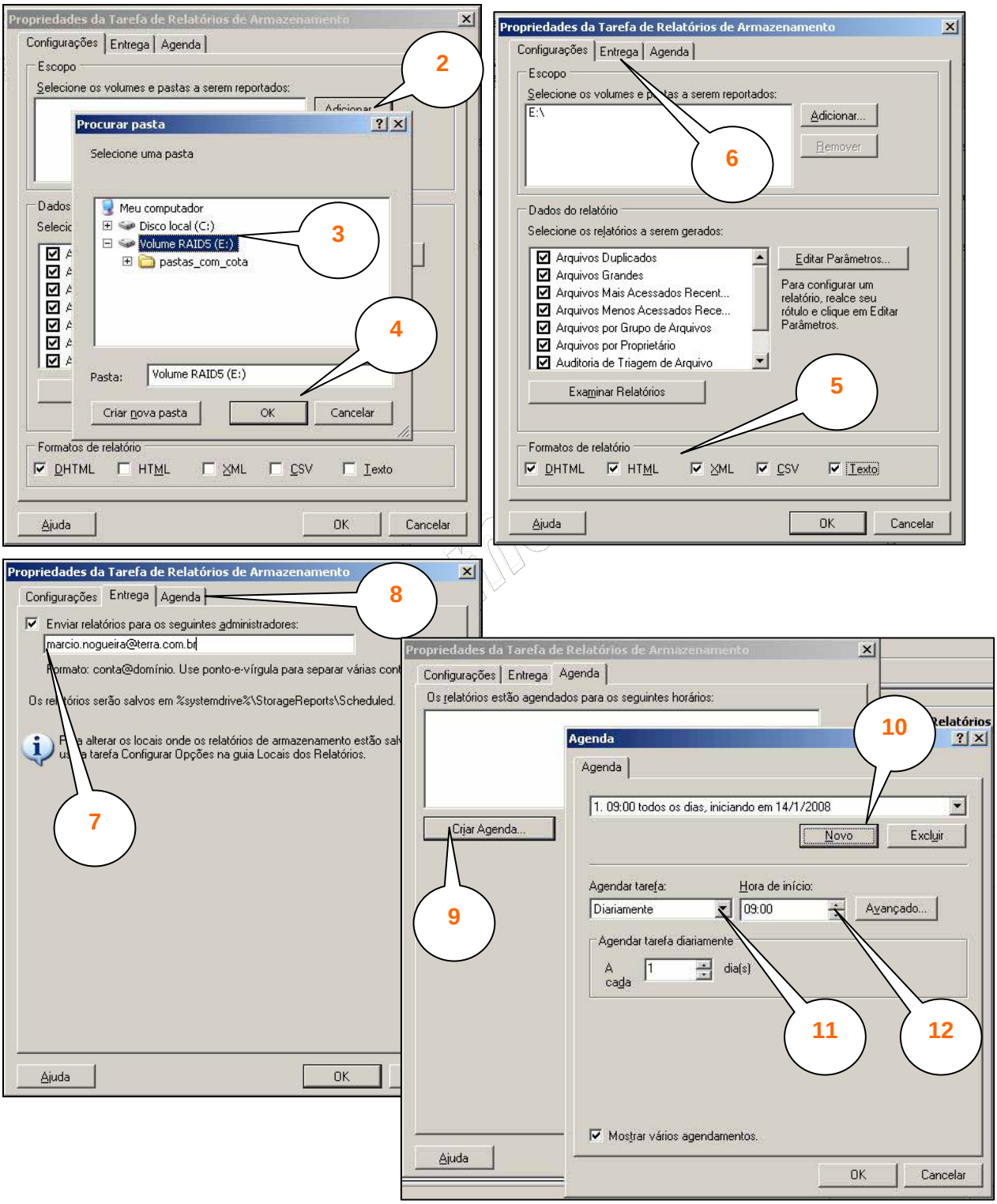


Vejamos agora a aba de “Modelo de Triagem de Arquivos”, que resume os modelos pré-disponíveis no Windows Server 2003:

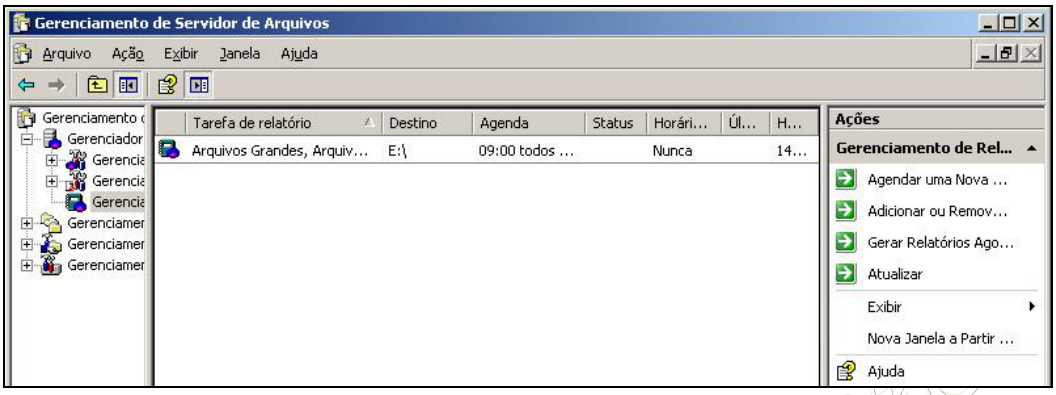
Em grupos de arquivos encontramos as extensões pré-disponíveis pelo Windows e aquelas que acabamos de criar ou modificar:

O último item do gerenciador de Servidor de Arquivos é o Gerenciamento de Relatórios de Armazenamentos. Nele podemos configurar uma séria de relatórios a serem gerados automaticamente pelo sistema e enviado para os administradores via e-mail ou Log de Eventos do Windows:

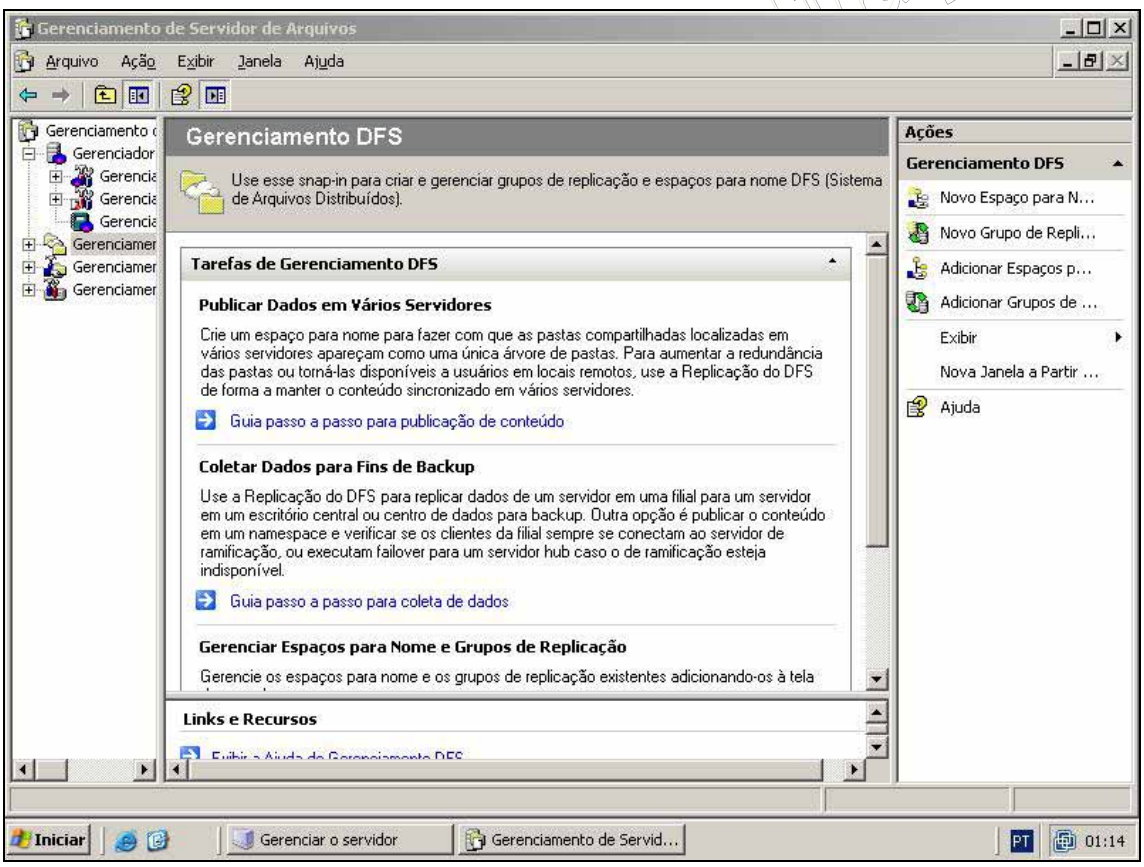
Vejamos como criar um relatório de armazenamento:



Por fim, é possível visualizar os relatórios agendados através da console de gerenciamento:



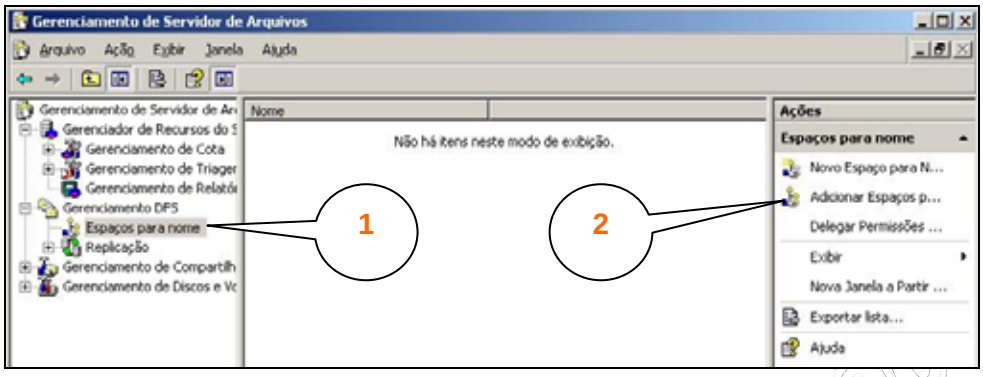
Passaremos agora para um dos mais importantes recursos do Servidor de Arquivos, o Gerenciamento de Sistemas de Arquivos Distribuídos (DFS). Veja abaixo uma descrição deste serviço:



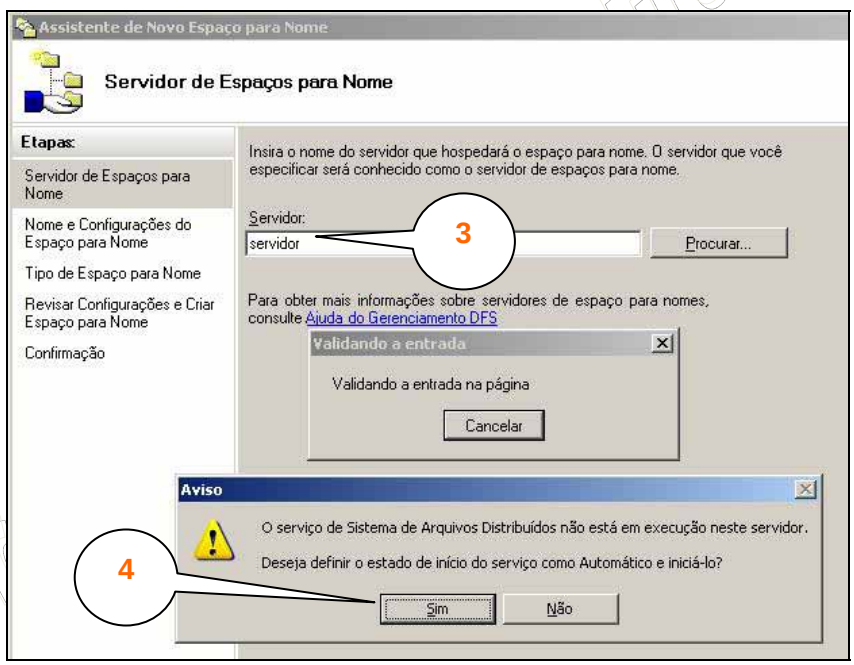
Como é possível observar, o próprio assistente de configuração do servidor nos ajuda tanto a compreender os conceitos quanto a configurar o servidor. Isso é muito importantes para nós que precisamos ser autodidatas em nossos estudos.

Demonstraremos agora como criar um espaço para nomes. Nosso objetivo é termos um compartilhamento público em nossa rede, \\servidor\area_publica, onde todos possam ler e gravar informações. Essa área de acesso público funciona como um disco removível, ideal para armazenar dados temporários quando não estamos operando em nossa própria estação de trabalho.

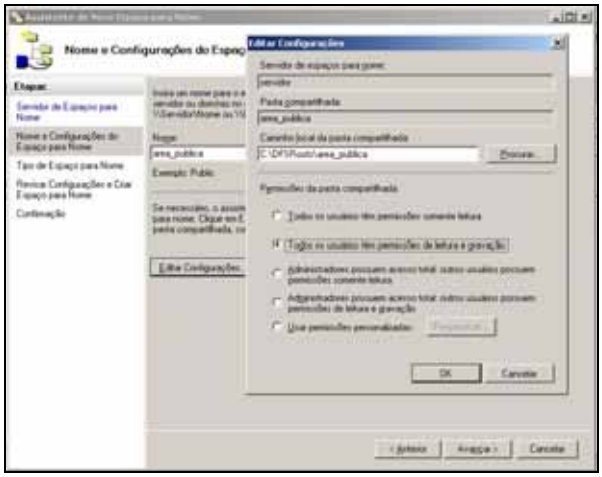
Para começar, vamos até o Gerenciador de Servidor de Arquivos, depois em Gerenciamento DFS e finalmente: Espaços para nome:



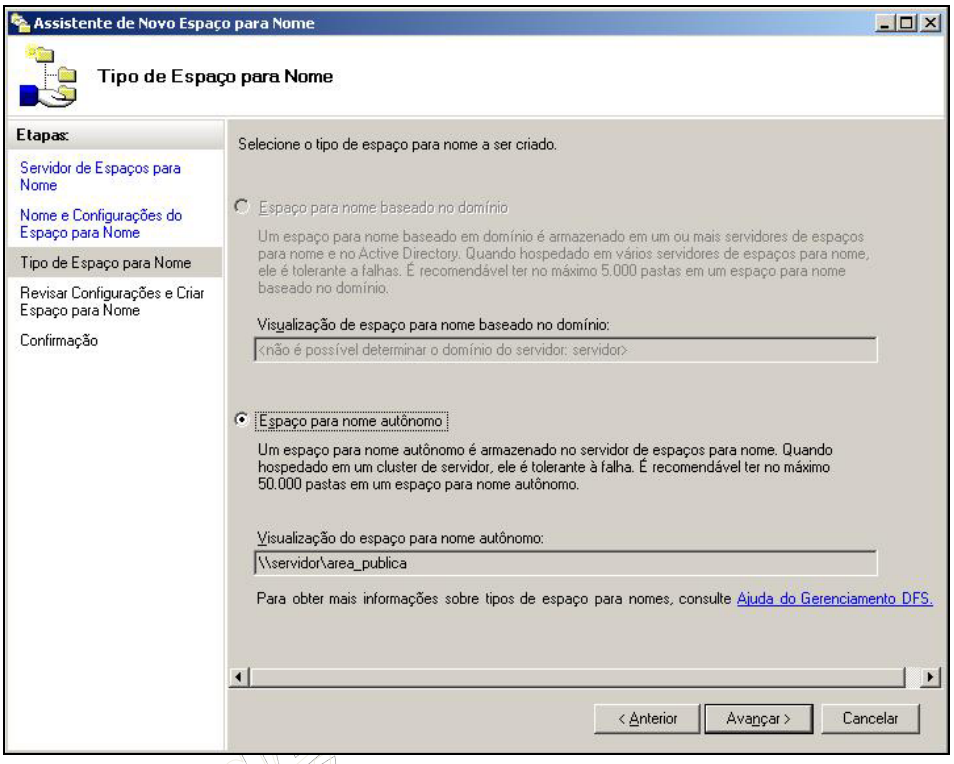
Uma nova janela solicita o nome do servidor que hospedará o espaço para nome, em nosso caso é próprio servidor. Quando executado pela primeira vez este assistente, ele retornará um aviso, questionando se pode inicializar de forma automática o serviço de arquivos distribuídos, responda sim e prossiga com a configuração:



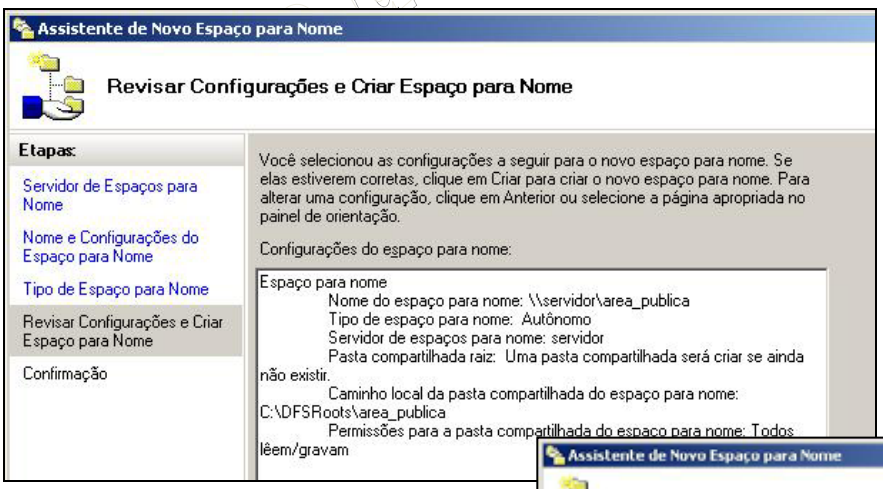
Agora selecione a pasta ao qual será compartilhada pelo espaço de nomes. Atenção para o seguinte detalhe: nesse momento estamos definindo que a pasta está hospedada em nosso próprio servidor, porém está pasta poderia estar hospedada em qualquer outro servidor da rede. Uma segunda possibilidade é que dois ou mais servidores possuam este mesmo compartilhamento, e uma vez definido que o servidor de espaço de nomes é o nosso servidor, então haverá um balanceamento de cargas e tolerância a falhas para o compartilhamento \\servidor\area_publica:

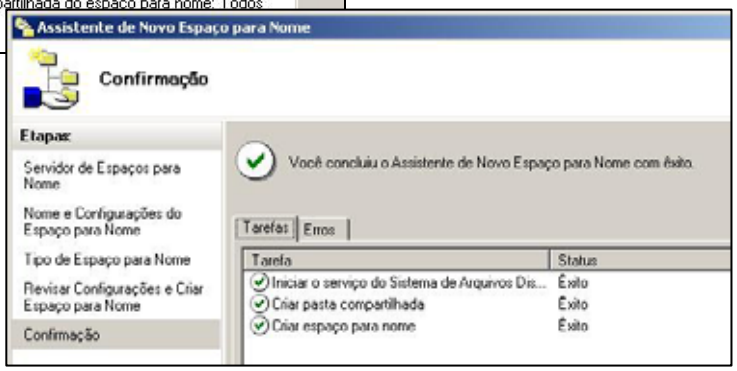


E por fim, a última configuração. Agora teremos que escolher se nosso servidor trabalhará de forma autônoma ou integrada ao Active Directory. A vantagem em operar em conjunto com o Active Directory está em relação as relações de confianças:



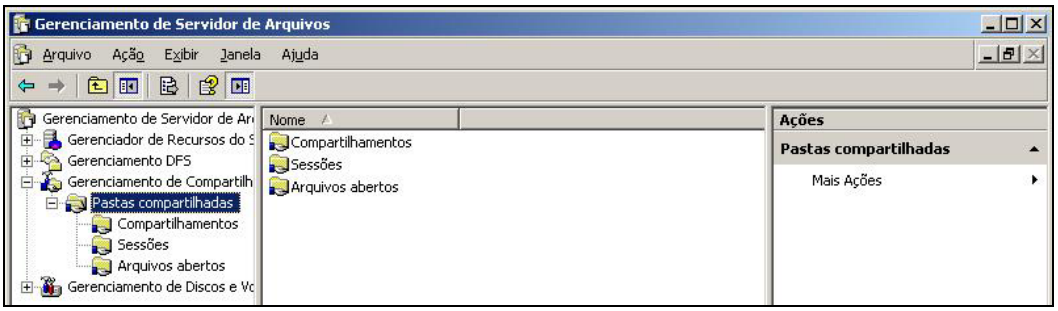
Veja o resumo do nosso espaço de nomes:



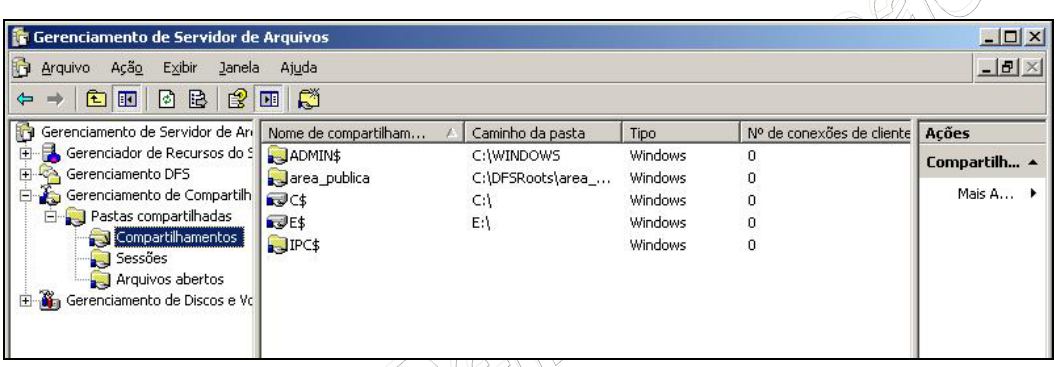


A próxima função do Gerenciamento DFS é a criação de servidores para replicação de dados, ou seja, manter os dados em dois ou mais servidores simultaneamente, sincronizados, de forma a ter tolerância a falhas e redundância. Não demonstraremos a criação desse item, deixamos isso como atividade para ser feita em casa.

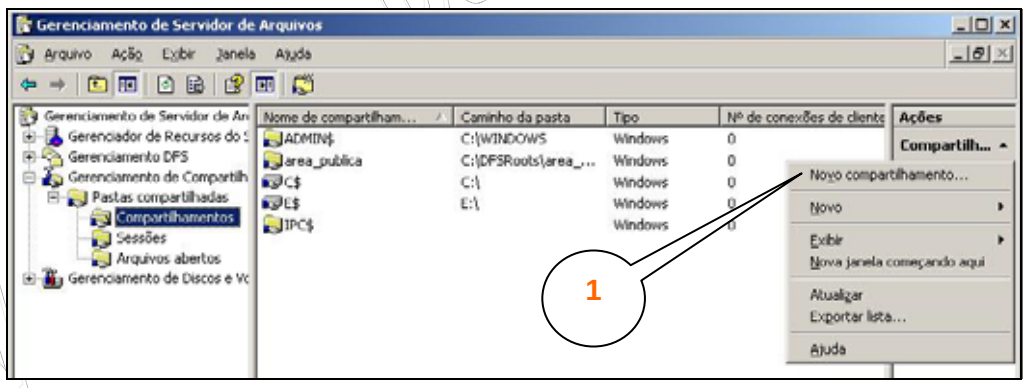
O Gerenciamento de Servidor de Arquivos ainda dispõe de uma ferramenta para a administração das pastas compartilhadas. Essa é talvez a ferramenta mais clássica da família Windows NT, vejamos:

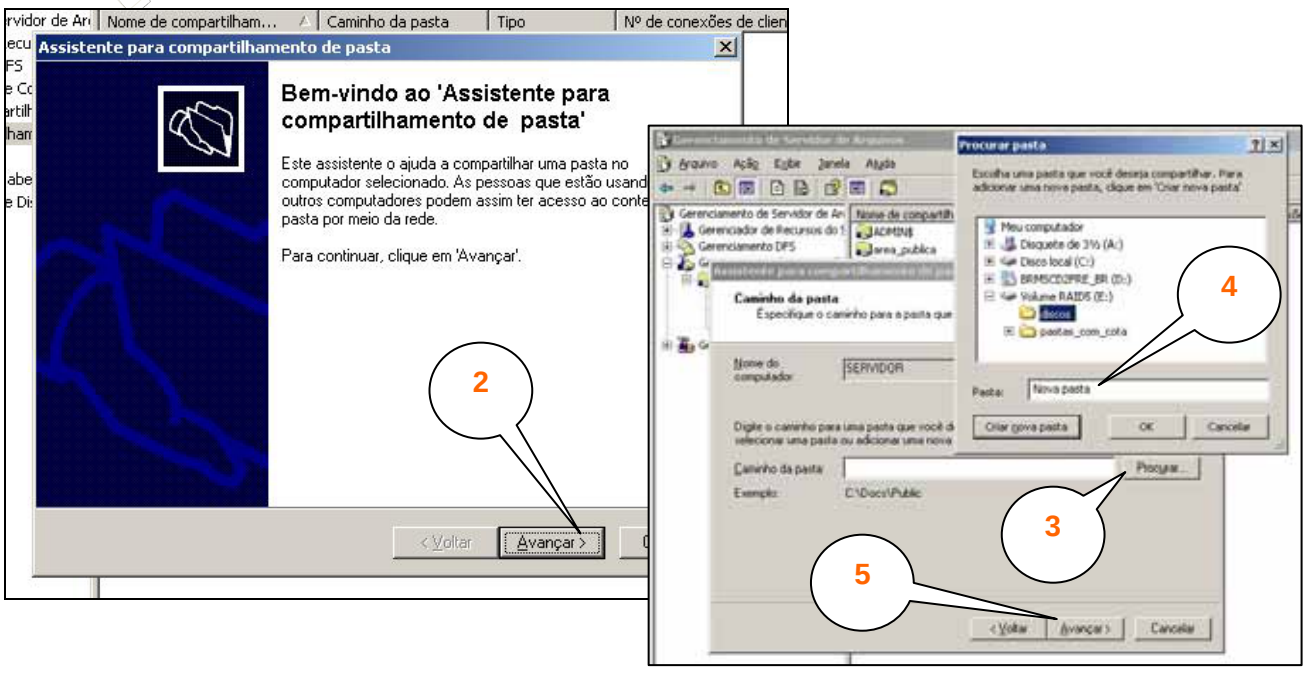


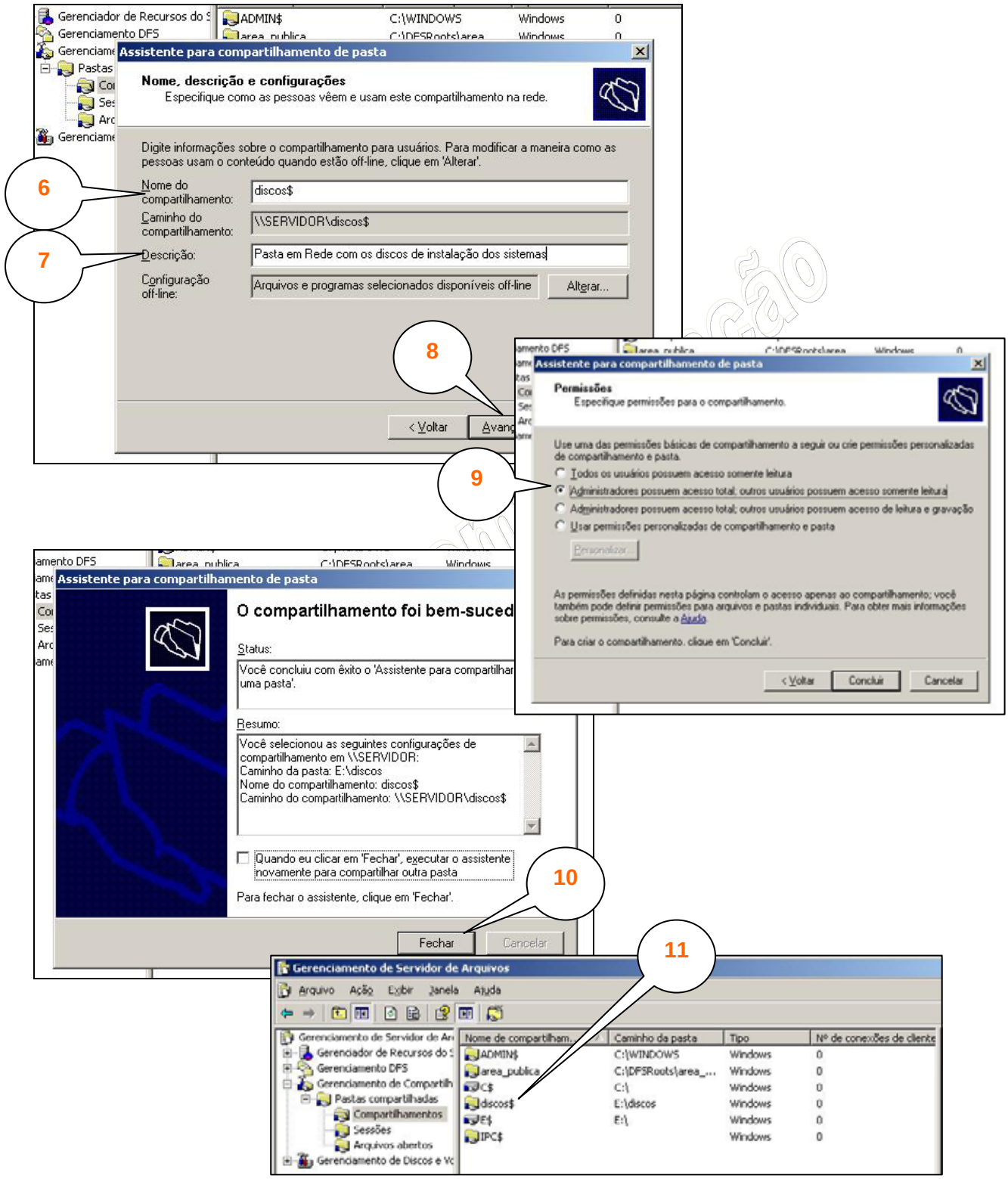
É através desta interface que podemos visualizar, adicionar ou remover compartilhamento do servidor local:



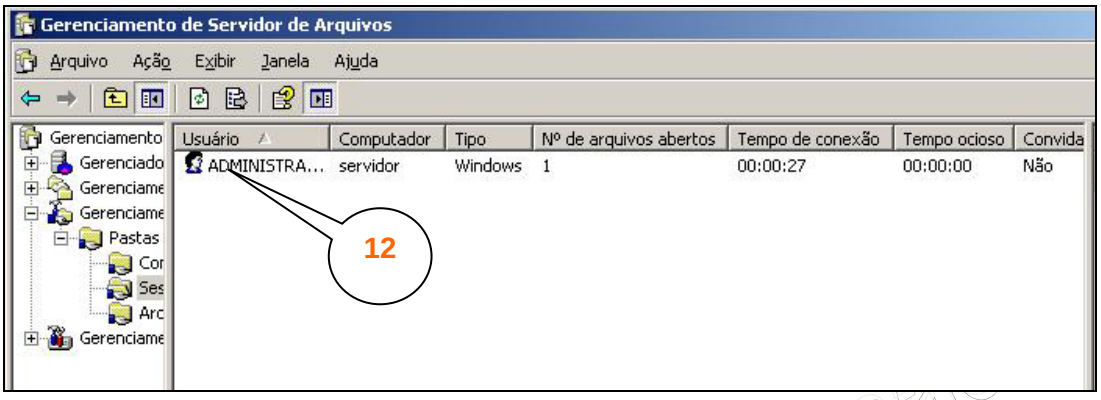
Para adicionar siga os passos a seguir:



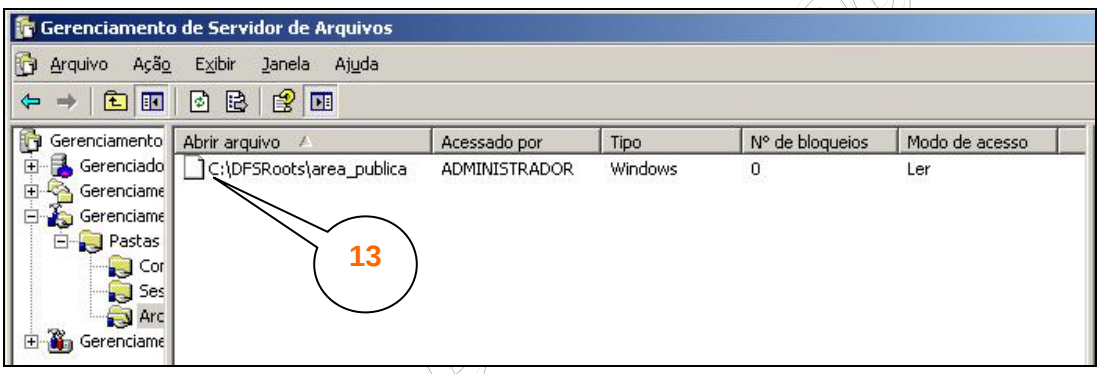




Além de administrar os compartilhamentos você ainda pode visualizar quem está atualmente conectado as pastas compartilhadas, e saber quais arquivos cada usuário está acessando. Na imagem a seguir vemos o usuário Administrador, acessando através do computador de nome "servidor", que é um sistema operacional do tipo "Windows", atualmente com apenas "1" arquivo aberto, conectado a 27 segundos e sem tempo de ociosidade. A última coluna "Convidado", indica se um usuário autenticado no Controlador de Domínio ou um acesso anônimo, ou denominado "convidado", para o Windows Server 2003.

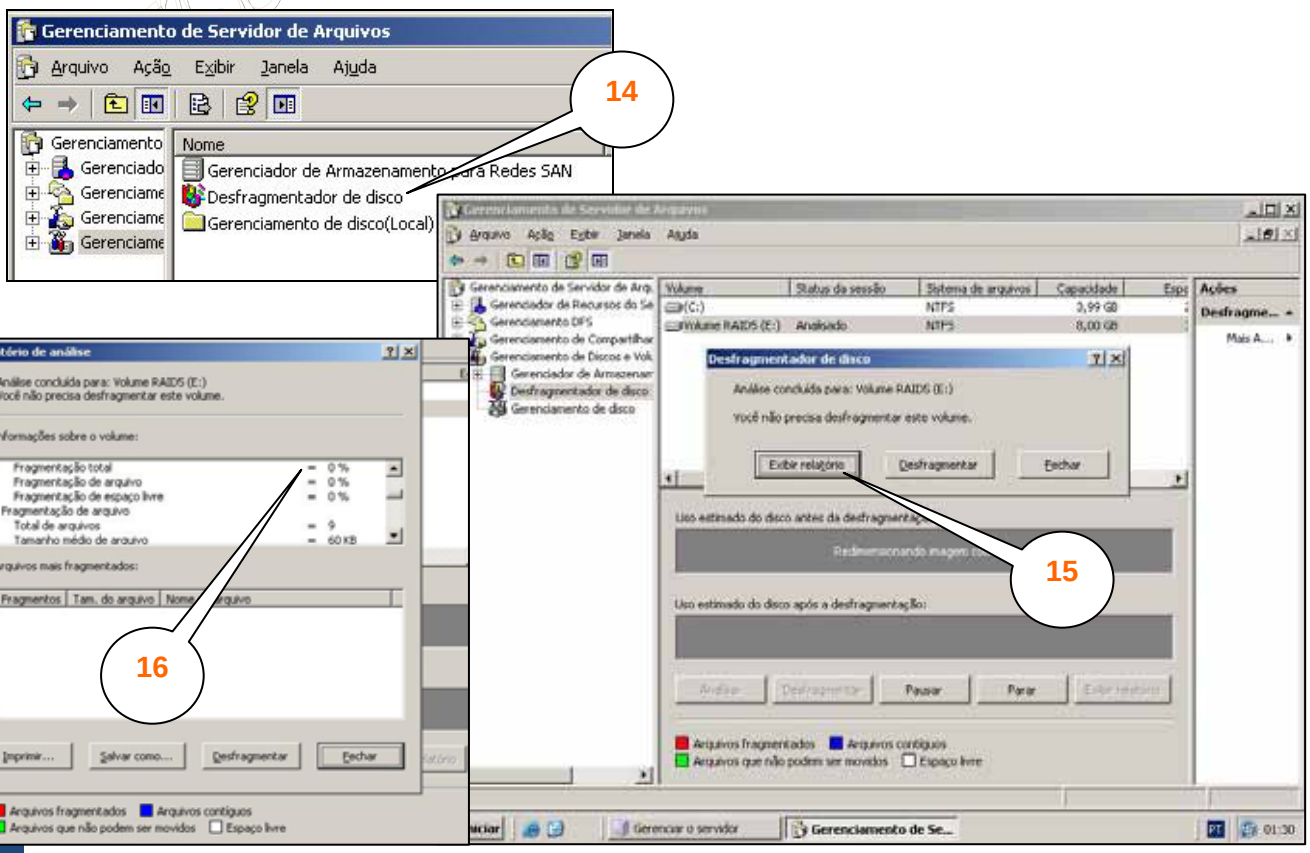


Para saber o arquivo que está sendo aberto pelo Administrador, a aba “Arquivos Abertos” responde:



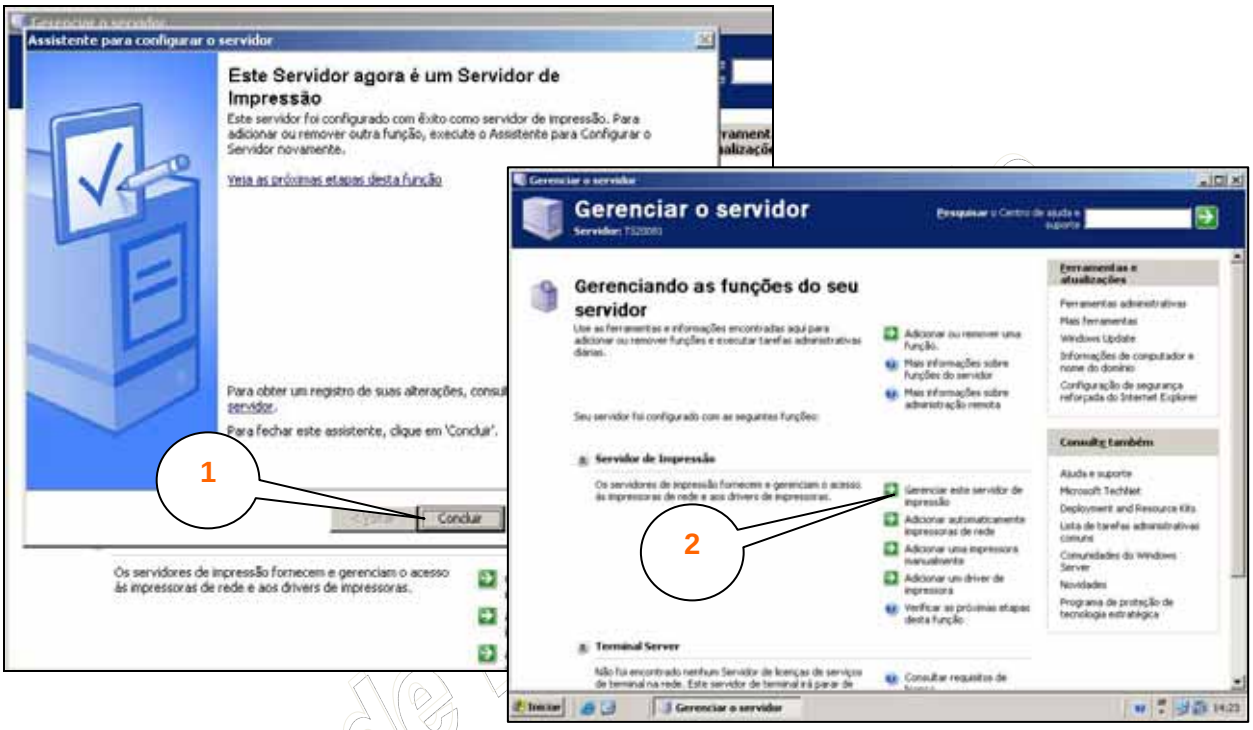
Neste observa-se que o Administrador esta acessando a pasta “área_publica”, porém não está lendo ou escrevendo nenhum arquivo para o mesmo.

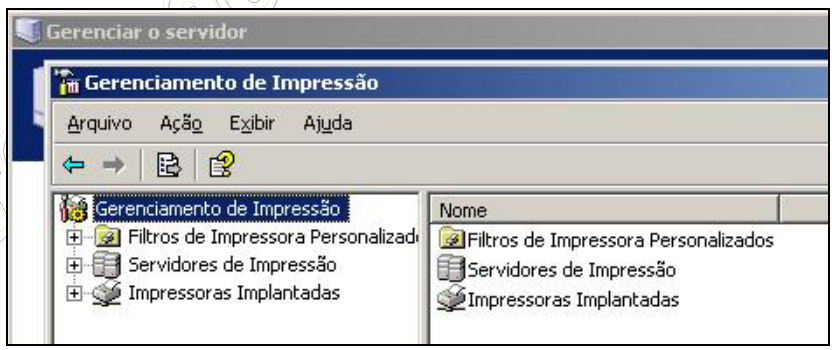
A última ferramenta do Gerenciamento do Servidor de Arquivos é o utilitário: Gerenciamento de Discos e Volumes. Essa ferramenta nos auxilia na operação das redes SAN, manutenção dos nossos discos físicos através do desfragmentador, e o próprio gerenciamento local dos discos físicos, como aprendemos na primeira competência:



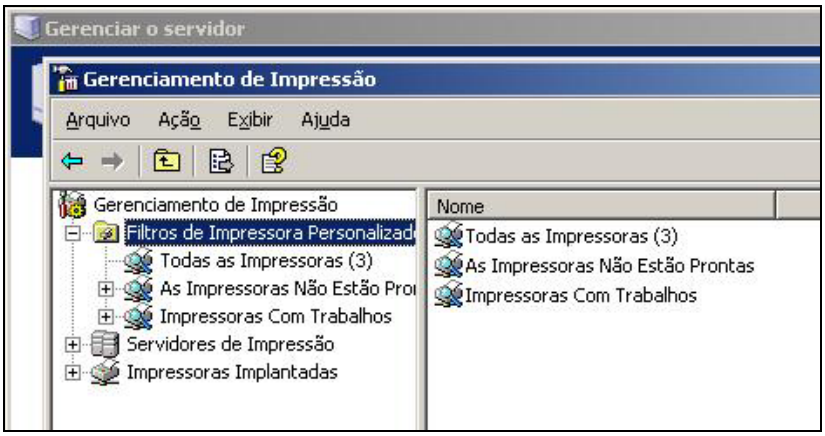
Servidor de Impressão

A próxima função que iremos aprender é o Servidor de Impressão. Com ele podemos disponibilizar através de um único ponto central todas as impressoras de rede e seus respectivos drivers para todas as estações da rede. Vamos a instalação:

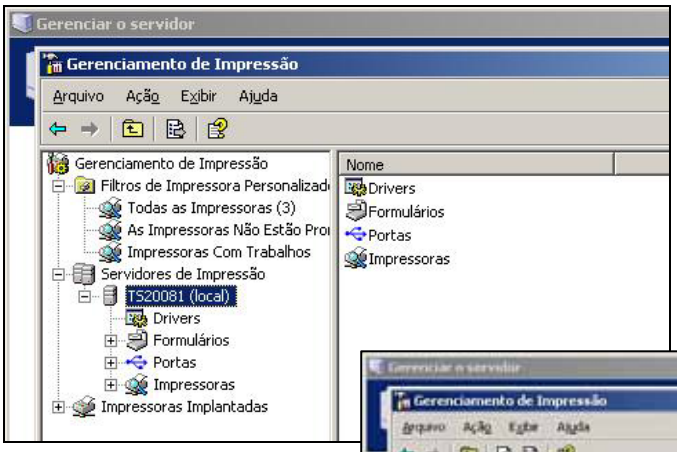


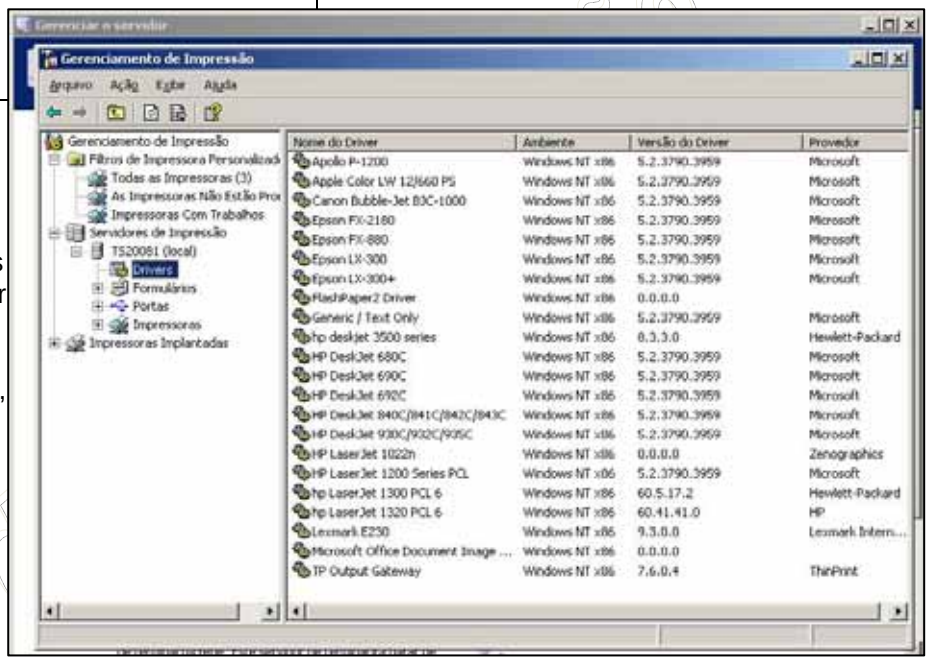


A primeira opção do Gerenciamento de Impressão são os filtros de Impressoras Personalizadas. Estes filtros nos ajudam a ter uma macro visão sobre a rede em relação aos estados das impressoras:



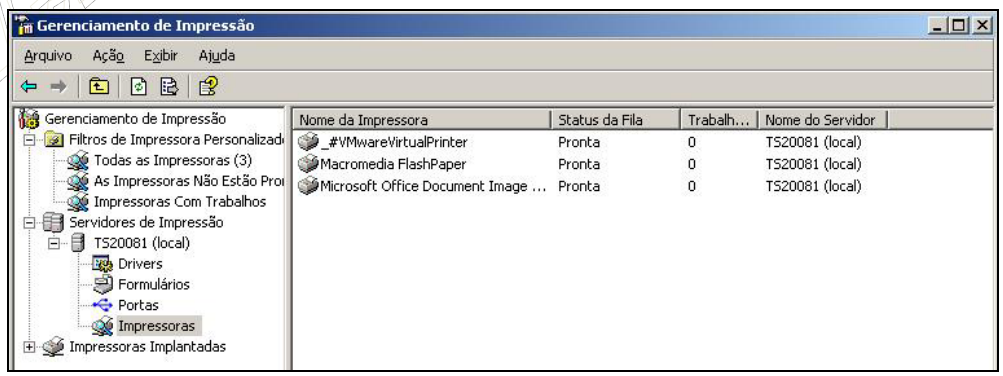
Em servidores de Impressão podemos visualizar os componentes instalados e ofertados para o serviço em redes:



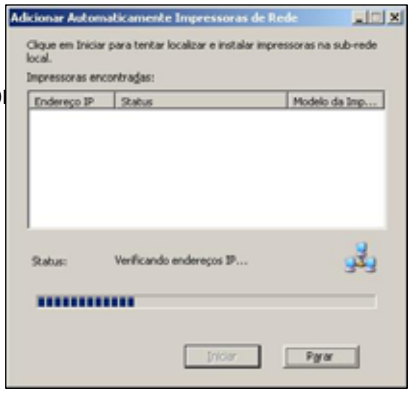


A aba de “Drivers” é sem dúvidas um dos recursos mais interessantes do servidor de impressão. Esta listagem nos informa quais os drivers que o Windows Server 2003 poderá fornecer de forma automática para as estações de trabalho, ou seja, todo vez que uma estação de trabalho precisar utilizar uma das impressoras do servidor de Impressão, e estando o seu respectivo driver listado nessa relação, então a estação de trabalho poderá de forma automática baixar esses drivers.

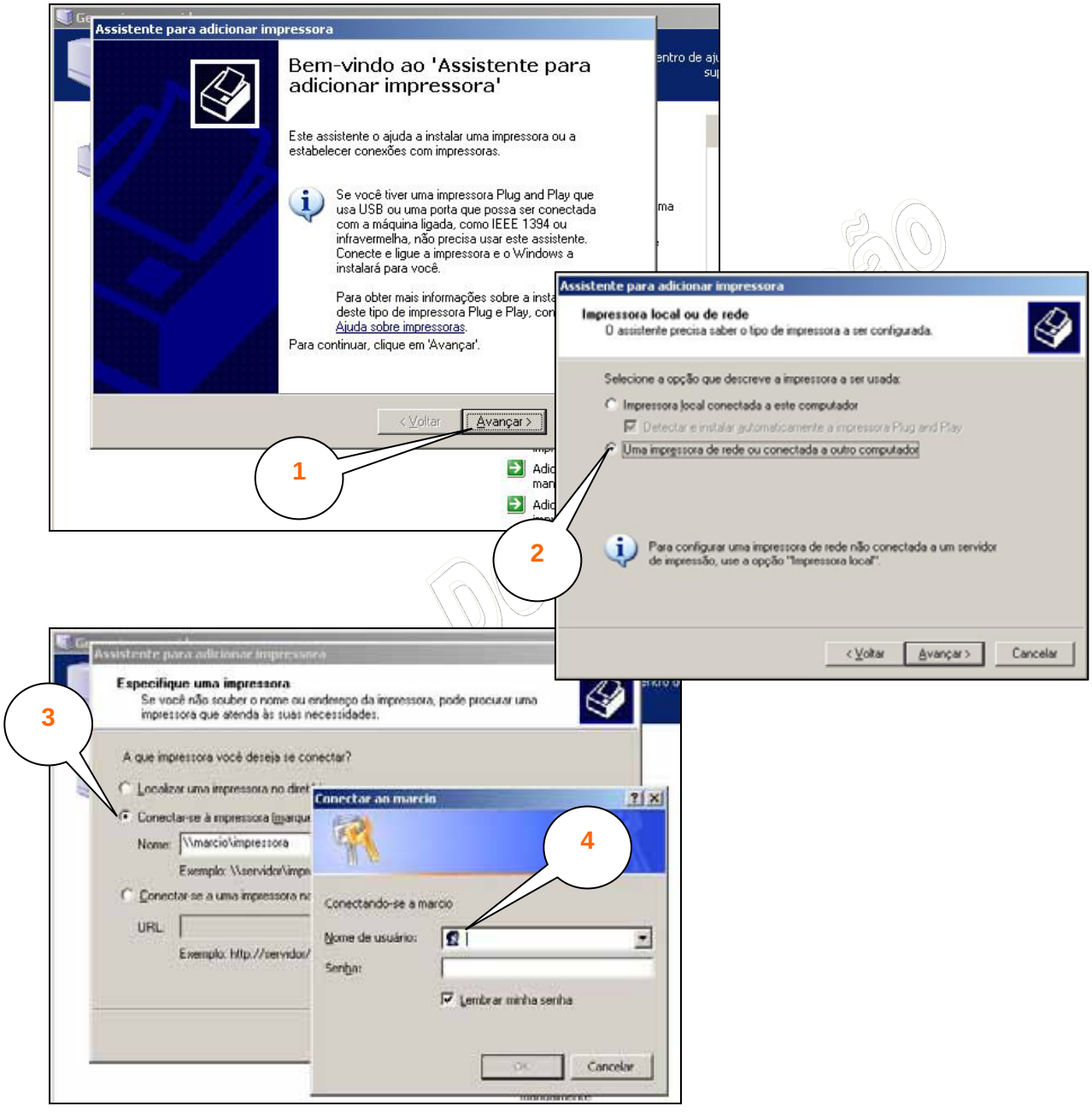
Uma outra aba de bastante utilidade é “Impressoras” onde listamos a relação de todas as impressoras ofertadas através deste servidor de impressão:



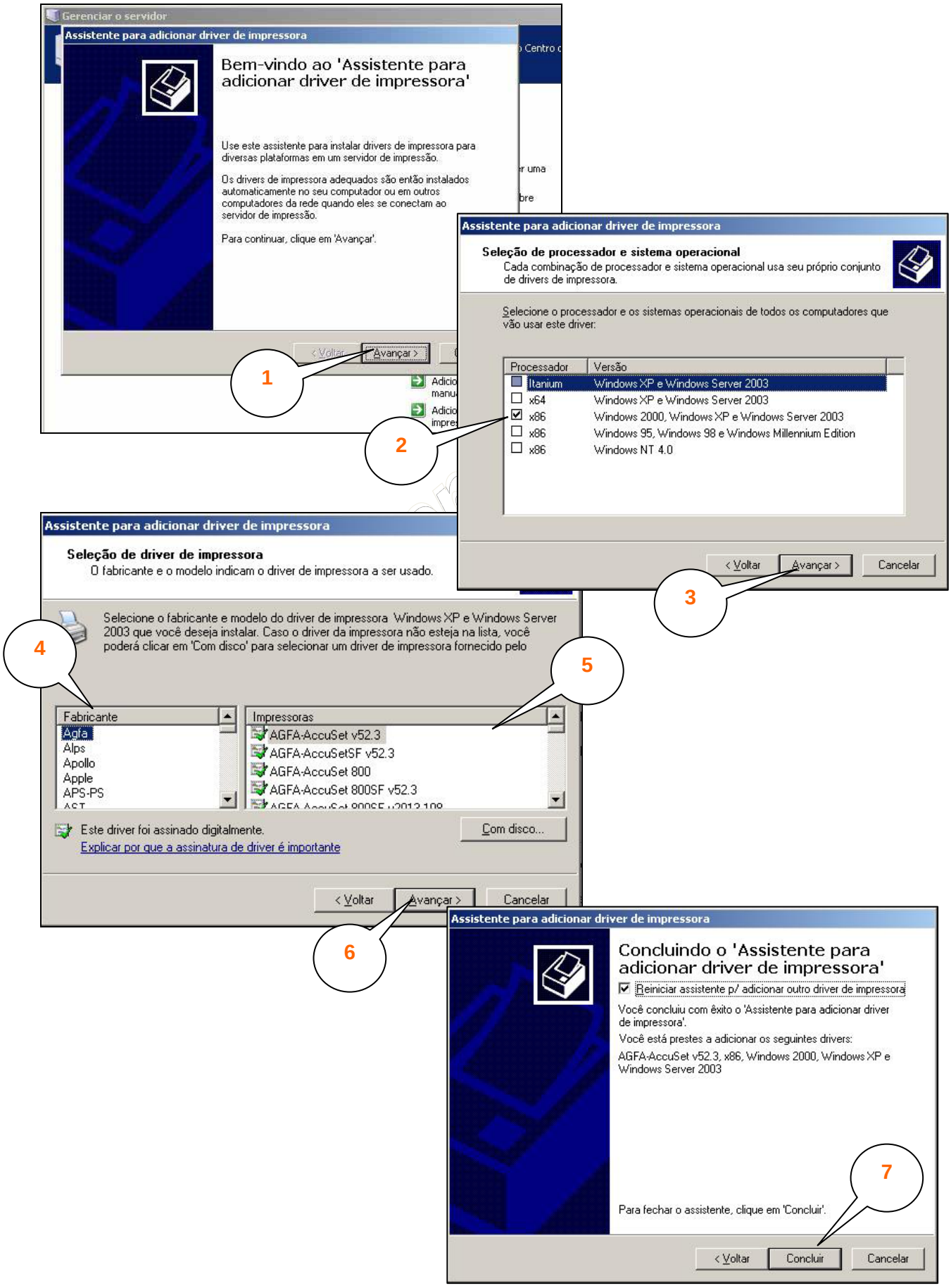
Nessa aba podemos localizar impressoras já em rede, instaladas em estações de trabalho ou operando diretamente em rede, de forma automática e com isso passar a ofertá-las através do servidor de impressão. A vantagem da centralização é que ocorrendo qualquer mudança na estação de trabalho não se faz necessário reconfigurar as demais máquinas da rede.



Podemos também realizar a instalação manual de impressoras. Demonstraremos a instalação de uma impressora de rede:

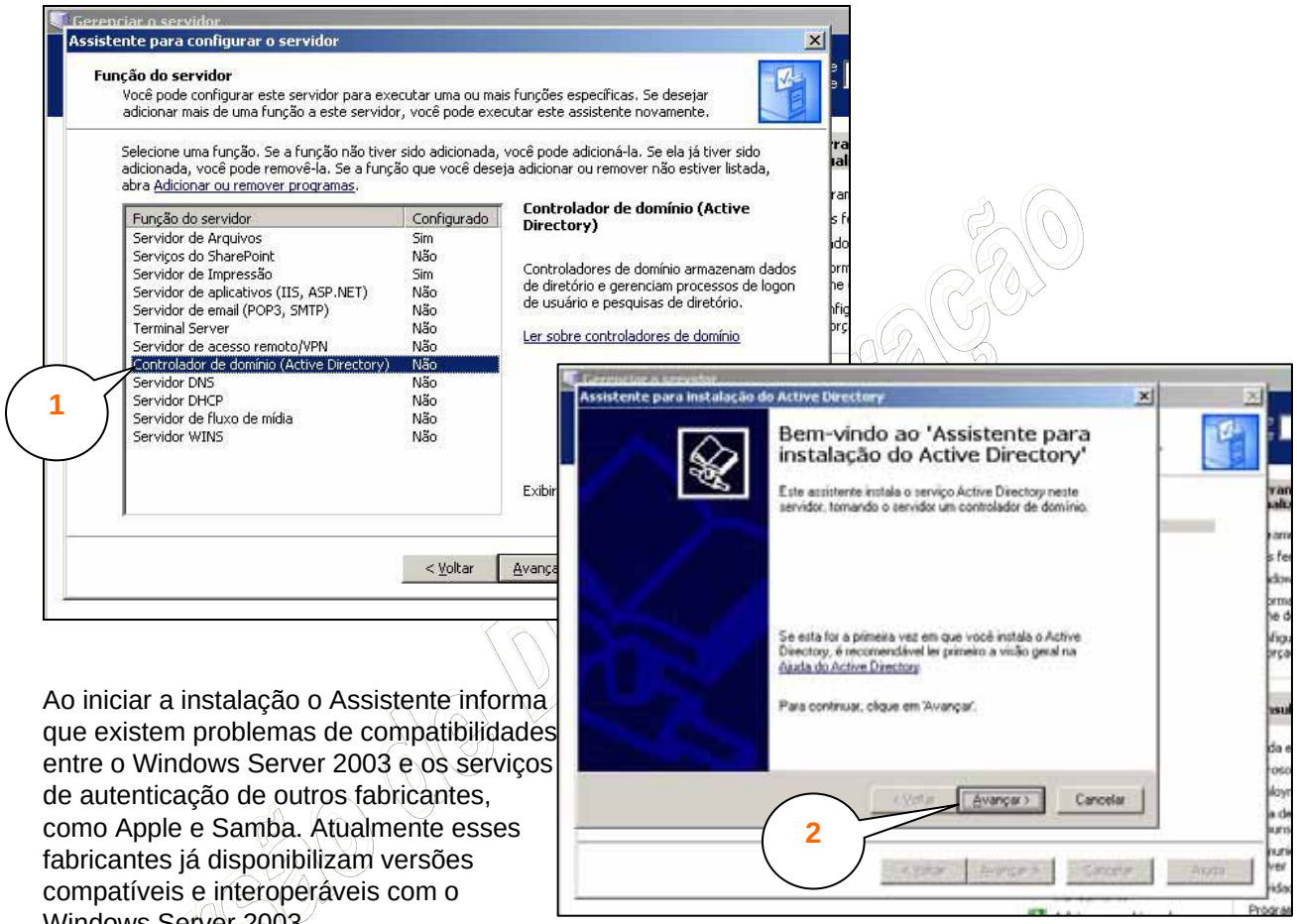


Em redes com vários tipos de impressoras instaladas, será bastante conveniente disponibilizar através do servidor de Impressão, os drivers para todas as impressoras. Isso facilita o suporte, manutenção e instalação das impressoras nas estações de trabalho. Vejamos a seguir como disponibilizar drivers de impressoras em um servidor de impressão:



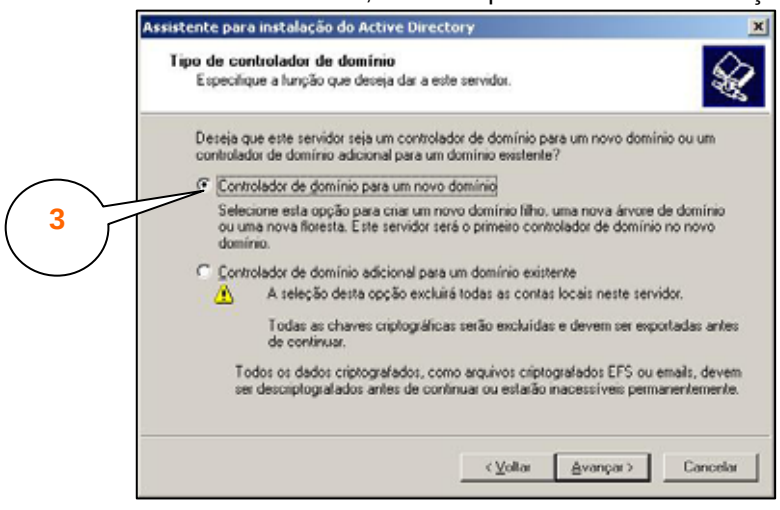
Controlador de Domínio (Active Directory)

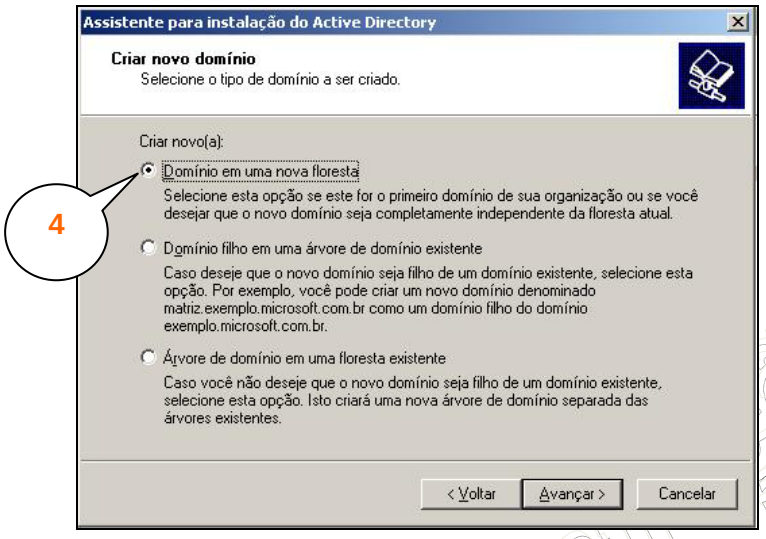
Demonstraremos agora como realizar a instalação e configuração do controlador de domínio, o serviço cuja função principal é a administração do banco de usuários e senhas para acesso a rede.



Ao iniciar a instalação o Assistente informa que existem problemas de compatibilidades entre o Windows Server 2003 e os serviços de autenticação de outros fabricantes, como Apple e Samba. Atualmente esses fabricantes já disponibilizam versões compatíveis e interoperáveis com o Windows Server 2003.

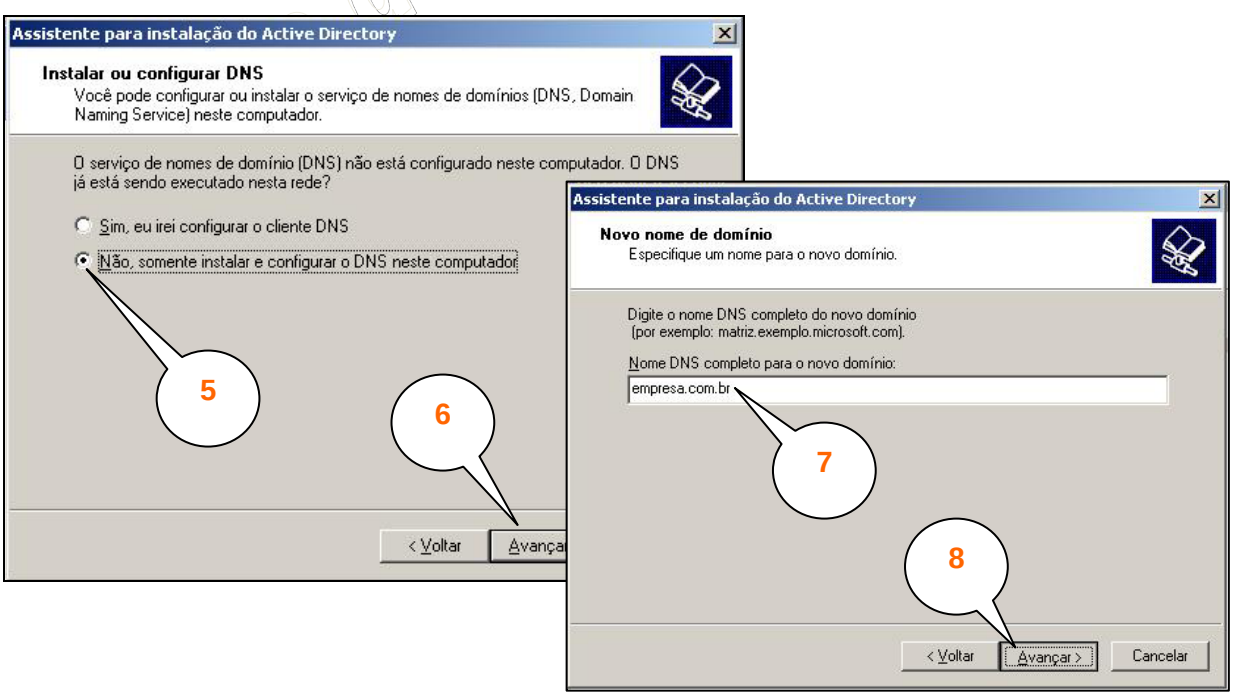
Realizaremos uma instalação básica do Active Directory de forma a atender nossa pequena rede. Esta instalação consiste na criação de um AD para o chamado novo domínio. Domínios, como na Internet (nogueira.eti.br) são espaços de nomes que definem um ambiente geográfico. Por exemplo, você pode definir que o domínio pai da sua empresa seja: empresa.com.br, o mesmo do seu site na Internet. Já suas filiais podem operar através dos domínios: filial1.empresa.com.br e filial2.empresa.com.br. Da mesma forma, você também pode disponibilizar domínios específicos para setores críticos, como: producao.empresa.com.br. Neste subdomínio as contas de usuários são distintas do domínio pai, porém, usuários do domínio pai poderão acessar o domínio filho com seus mesmos nomes de usuários e senhas, isso é o que chamamos de relação de confiança entre domínios.



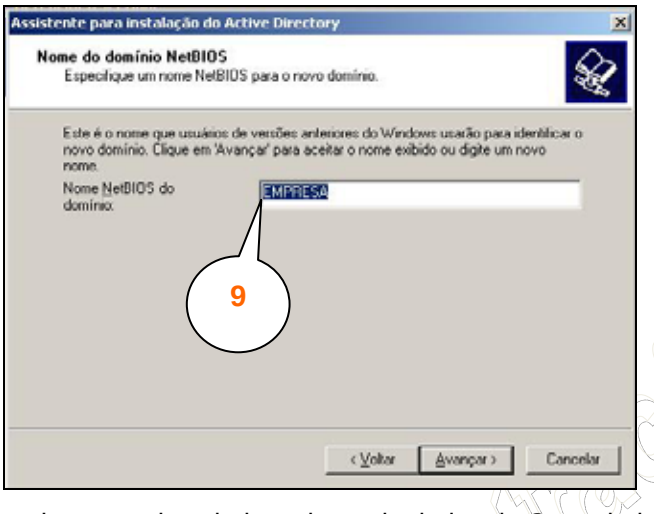


O próximo passo do assistente é verificar se o serviço de DNS está instalado e disponível. Como na Internet o servidor DNS será o responsável por administrar os IPs do nosso domínio, ou seja, se definirmos nosso domínio como “empresa.com.br”, isso significa que todos os computadores que possuírem uma conta no AD (estações com a função de logar no domínio), terão um nome associado na forma “estacao01.empresa.com.br”. A resolução deste nome para o respectivo IP da estação de trabalho será gerenciado pelo DNS.

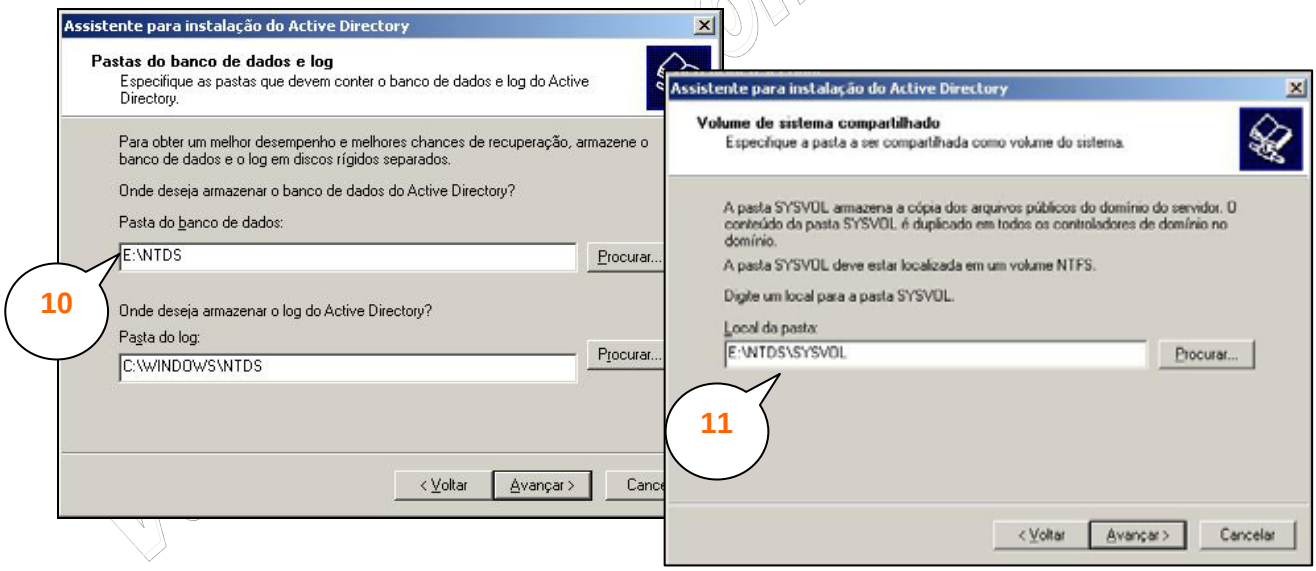
Como estamos instalando um novo servidor, é normal que não tenhamos o serviço de DNS ainda instalado. Isso na verdade é quase estratégico, pois o assistente de configuração do Controlador de Domínio pode se encarregar de instalar e configurar o DNS para nós, o que de certa forma é muito interessante pois evita que tenhamos que decorar uma série de passos para a devida configuração e segurança do mesmo:



Após definir o domínio completo para o servidor o assistente recomendará um novo nome, baseado nas suas informações, para o nome NETBIOS do computador na rede. O Nome NetBIOS é um protocolo de compartilhamento de informações de máquinas em rede. Para redes que não estão conectadas diretamente a Internet, ou que operem no nível de redes locais, este é o protocolo padrão. Observe que a tendência é que todas as redes estejam conectadas diretamente (através de IP válido público) a Internet. Porém, ainda é grande o uso de endereços privados, dessa forma, a utilização de protocolo NetBios para redes locais ainda será amplamente útil:

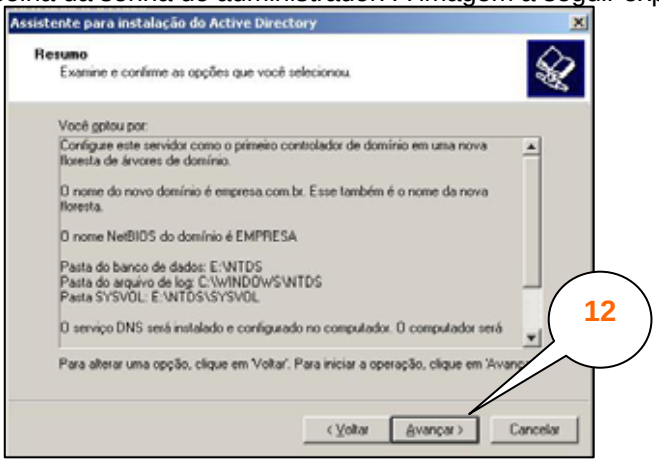


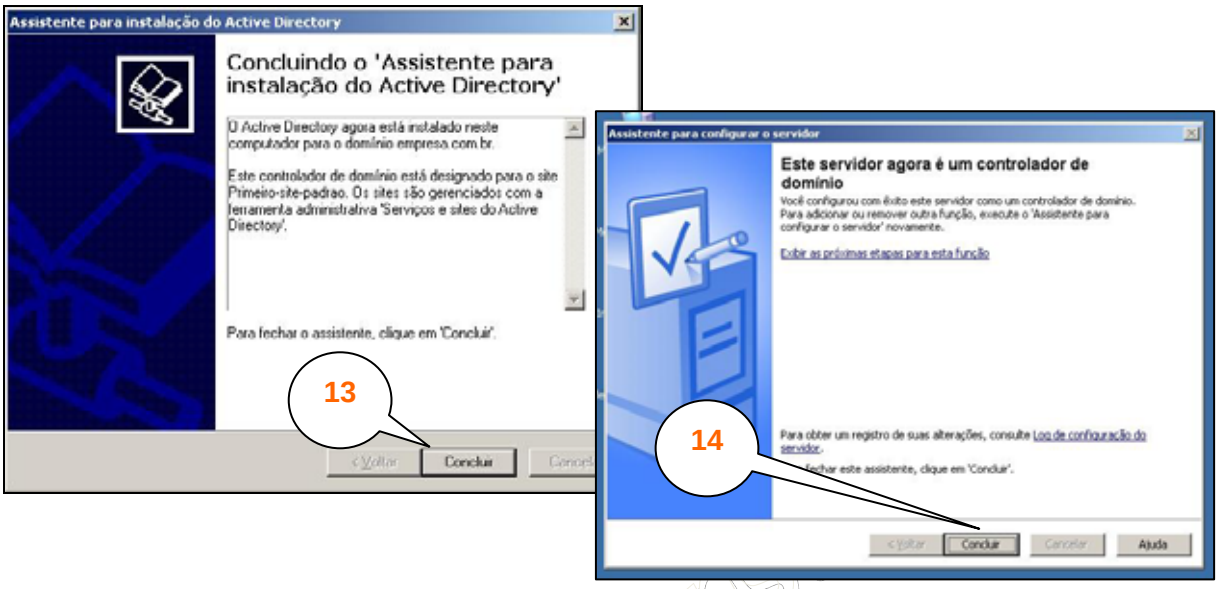
Iremos agora definir o local a serem instalados a base de dados do Controlador de Arquivos e os arquivos de Logs. Por questões de segurança recomendamos que os arquivos do banco de dados sejam armazenados em volumes RAID-5 e os logs no volume do sistema. Isso aumenta tanto a segurança quanto o desempenho do servidor:



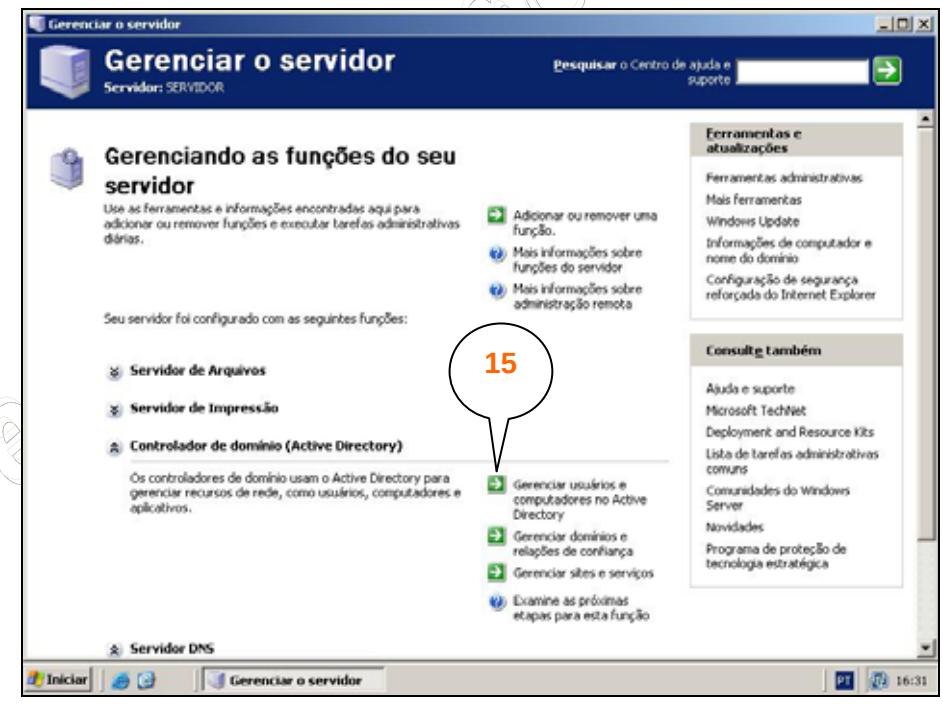
A próxima pasta a ser criada é a SYSVOL, é nela que ficarão publicados os scripts e regras de segurança. Também recomendamos que esta pasta esteja em um volume RAID-5.

Os passos seguintes, e que omitiremos por questões de simplicidade, consiste na escolha das permissões. Você pode optar entre ter compatibilidade com servidores Windows 2000, e perder recursos, ou ter todos os recursos, porém não sendo compatível com servidores Windows 2000. Em seguida é a hora da escolha da senha do administrador. A imagem a seguir expressa o resumo das configurações feitas:



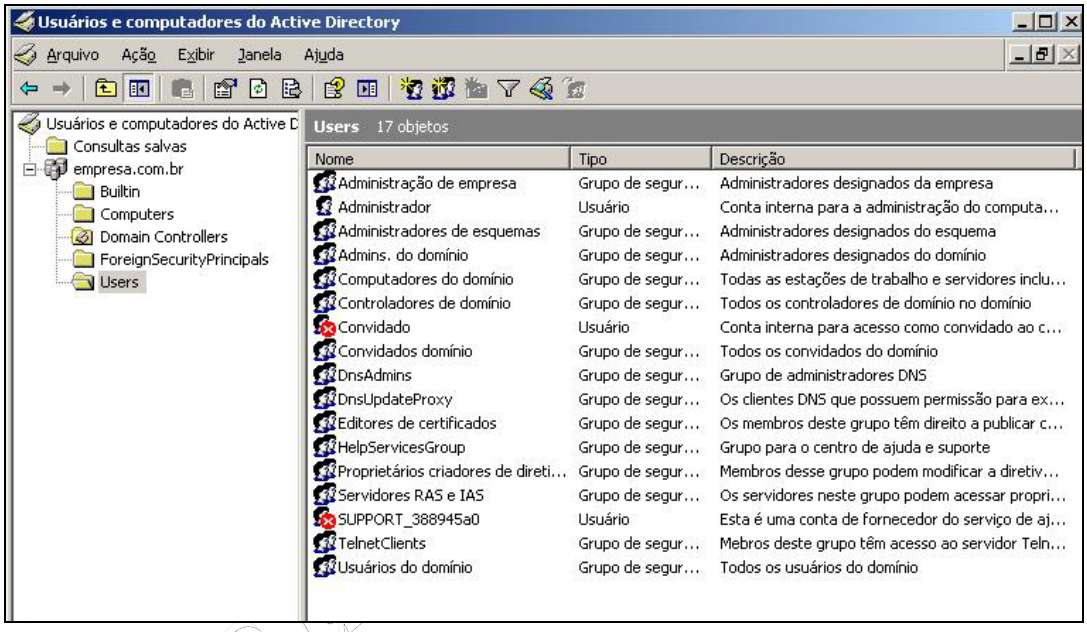


Agora que possuímos o Controlador de Arquivos em nossa rede é hora de manusearmos a criação de contas de usuários:



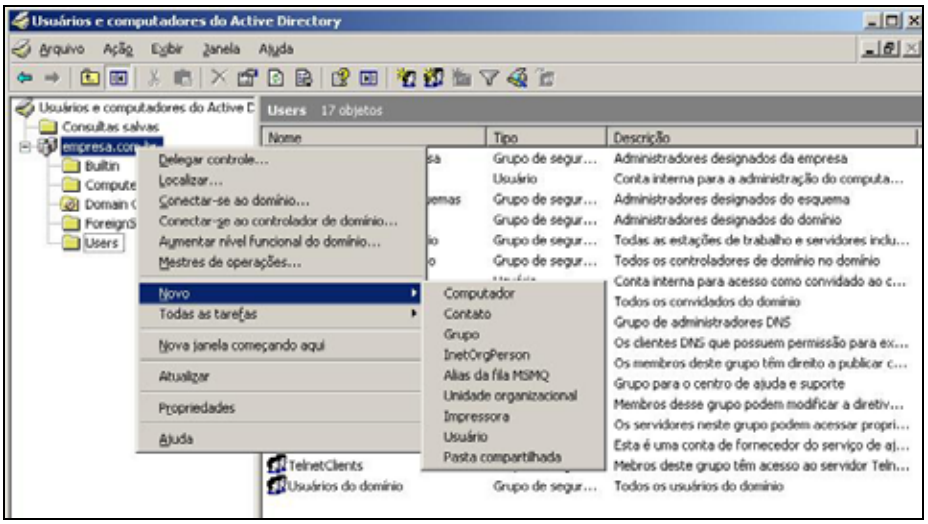
Em “Usuários e computadores do Active Directory” encontramos uma série de opções para consulta e configuração. As principais opções são:

Na aba “Builtin” encontramos as contas criadas por padrão junto ao controlador de domínio, elas são úteis para utilizarmos como modelos ou se necessário for voltar ao modo original. A aba “Computers” apresenta a relação de computadores cadastrados em nosso banco de contas. Esses são os computadores que podem apresentar a tela de “Fazer Logon no Domínio”. Na aba “Domain Controllers” encontramos a relação de controladores de domínios disponíveis em nossa rede, em nosso caso só haverá um, porém é possível criar outros controladores de domínio de forma a balancear ou espelhar os dados. Em “ForeignSecurityPrincipal” encontramos informações de segurança sobre o domínio. E finalmente em “Users” encontramos os dados das contas para acesso aos serviços ofertados em conjunto com o controlador de domínio:



A relação de usuários pode conter contas e também grupos. Os grupos servem para agrupar determinadas contas de forma a otimizar a manutenção nas mesmas. Por exemplo, podemos criar um grupo denominado Comercial, e nele inserir as quinze contas dos membros do departamento comercial. Ao compartilharmos uma pasta em rede, e definirmos suas permissões de acesso apenas para o departamento comercial, só precisaremos informar o grupo Comercial que o Windows reconhece que as restrições serão configuradas sobre as contas do grupo Comercial.

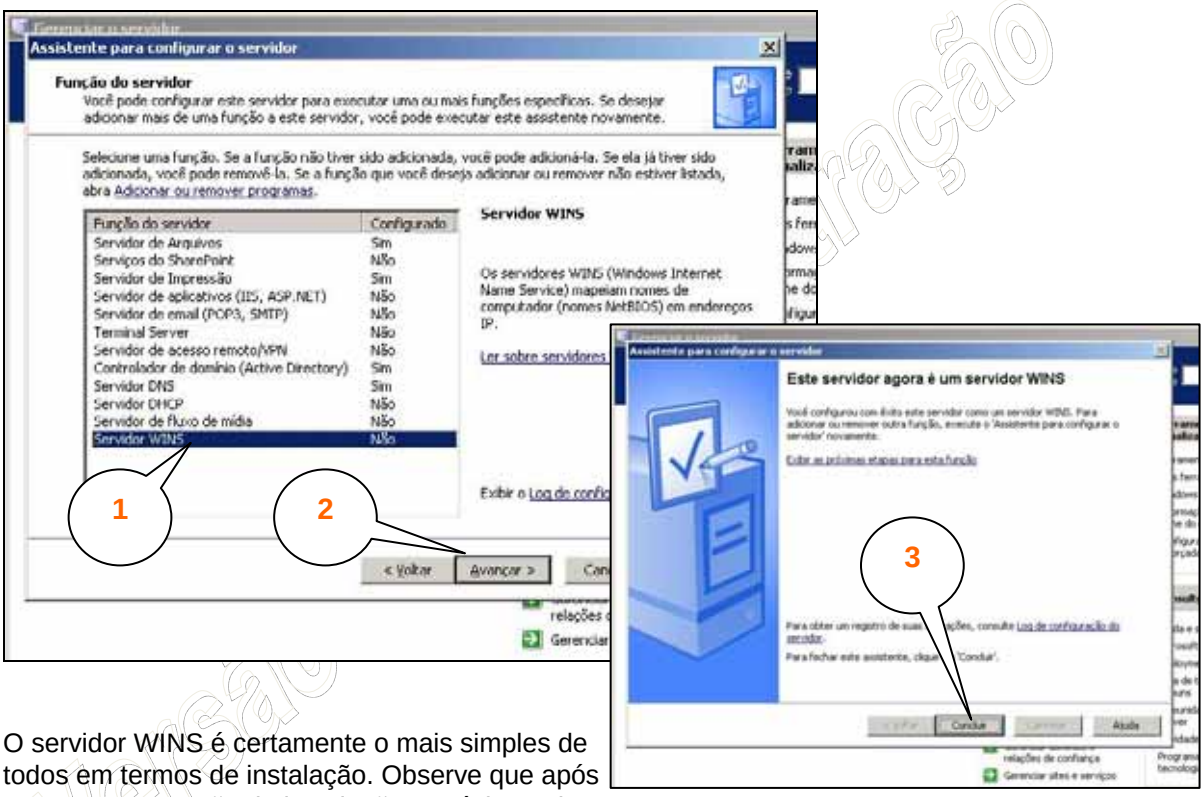
Também é nesta aba que podemos realizar a adição ou remoção de contas de usuários, grupos e computadores, além de outras opções:



Como atividade, tente criar um grupo denominado Informática e criar algumas contas no servidor. Em seguida insira essas contas no grupo Informática e compartilhe uma pasta apenas para esse grupo.

Servidor WINS

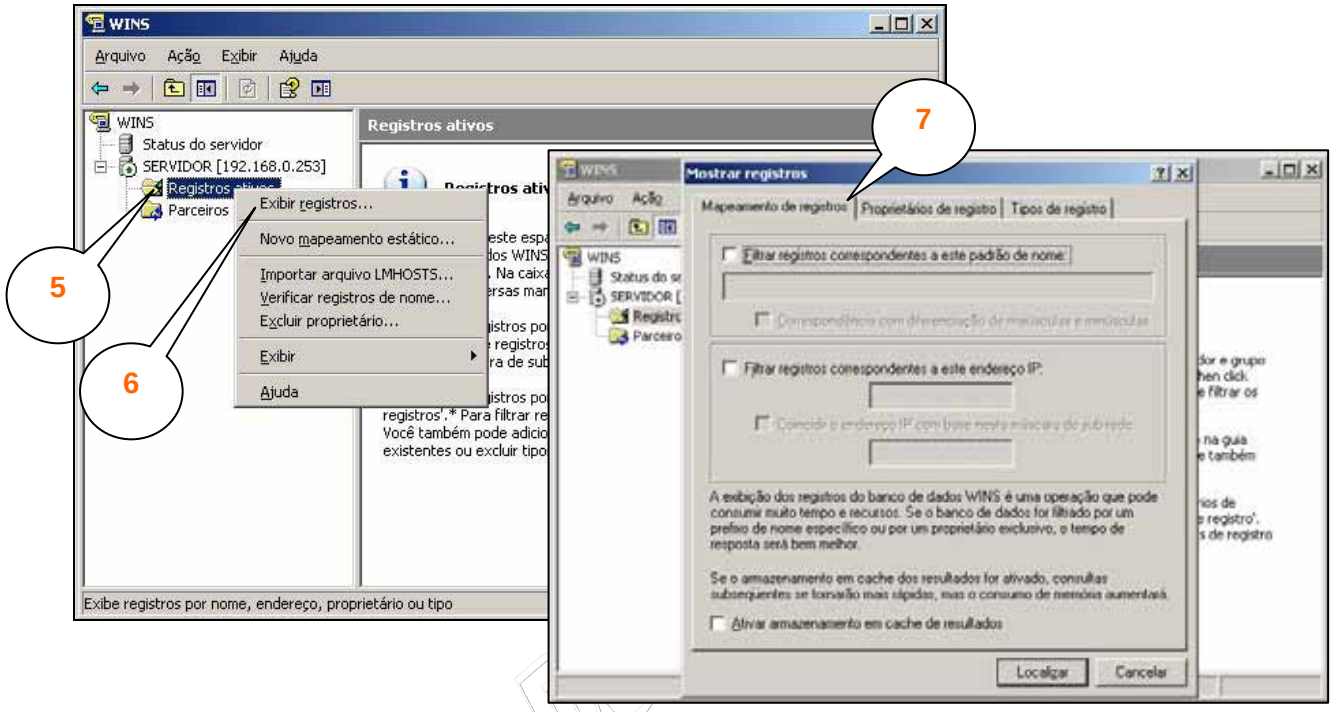
Vimos acima que o Controlador de Domínio instala e configura o servidor de DNS para operação junto ao domínio. Em seguida ela atribui um nome NetBIOS para o servidor. O Serviço que trata da resolução de nomes NetBIOS para IP é chamado WINS, e em conjunto com o DNS ele provê alto desempenho em termos de resolução de nomes em redes locais. É verdade que uma rede local pode operar apenas com DNS ou apenas com o WINS, porém há uma perda de desempenho quando consultas forem realizadas para a Internet (ausência do DNS) ou na intranet (ausência do WINS). Dessa forma, uma boa prática, é sempre instalar o WINS no mesmo servidor de DNS do Controlador de Domínios:



O servidor WINS é certamente o mais simples de todos em termos de instalação. Observe que após marcarmos a opção de instalação a próxima tela respectiva é a de mensagem de conclusão.

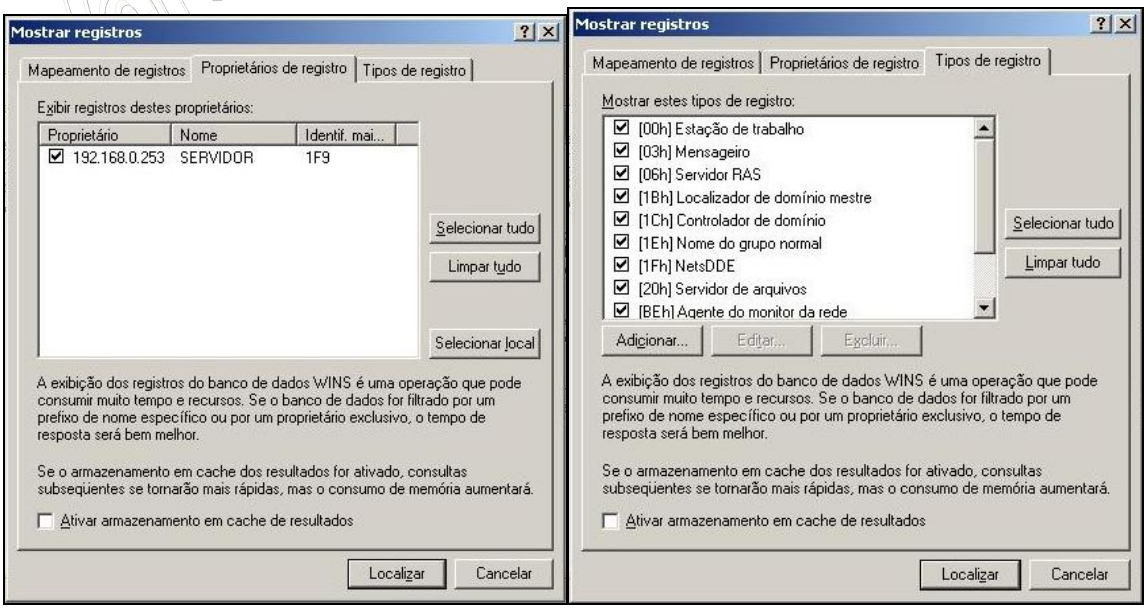
De fato, o WINS funciona como uma banco de dados de nomes com seus respectivos IP´s, e constantemente atualiza de forma dinâmica estas informações. É muito comum após a instalação de um servidor WINS do administrador ignorar sua existência em função de não haver necessidades de manipulações no banco WINS. Isso é fato positivo, pois temos um serviço que aprimora o desempenho da rede sem que precisemos nos preocupar com sua administração ou manutenção, mas vejamos algumas dicas de uso:

A interface de administração também é simples, mas existe um procedimento a ser seguido para conseguir visualizar seus dados, siga esse caminho:



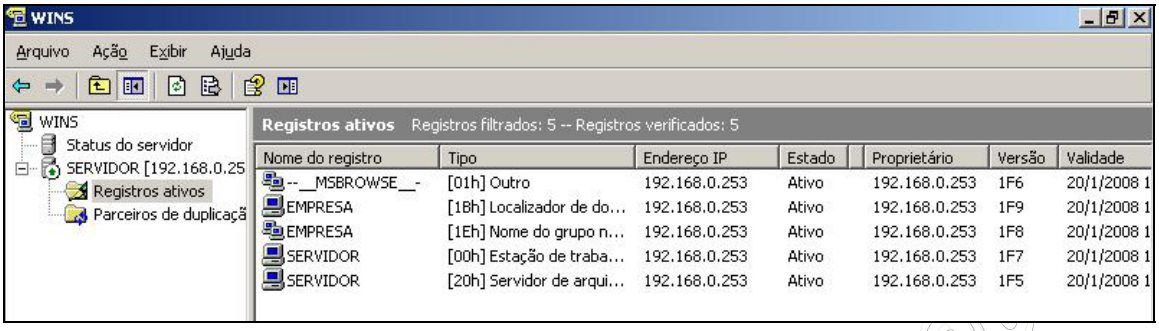
Na janela de “Mostrar registros” você pode criar filtros para facilitar a pesquisa de dados na rede. Para redes pequenas, de até 200 computadores, é possível exibir todos os computadores e ainda manter uma boa visão sobre o que se passa na rede. Acima disso é recomendável a manipulação dos filtros, para que pequenos detalhes não passem desapercebidos.

Em “Proprietários de registro” encontramos a lista de servidores WINS da rede. Uma característica do servidor WINS, que inspirou a prática do próprio DNS, é a possibilidade de realização de consultas abertas em seu banco de dados. Ou seja, qualquer pessoa ou servidor pode consultar o banco de dados WINS para saber qual o IP associado a um determinado nome:



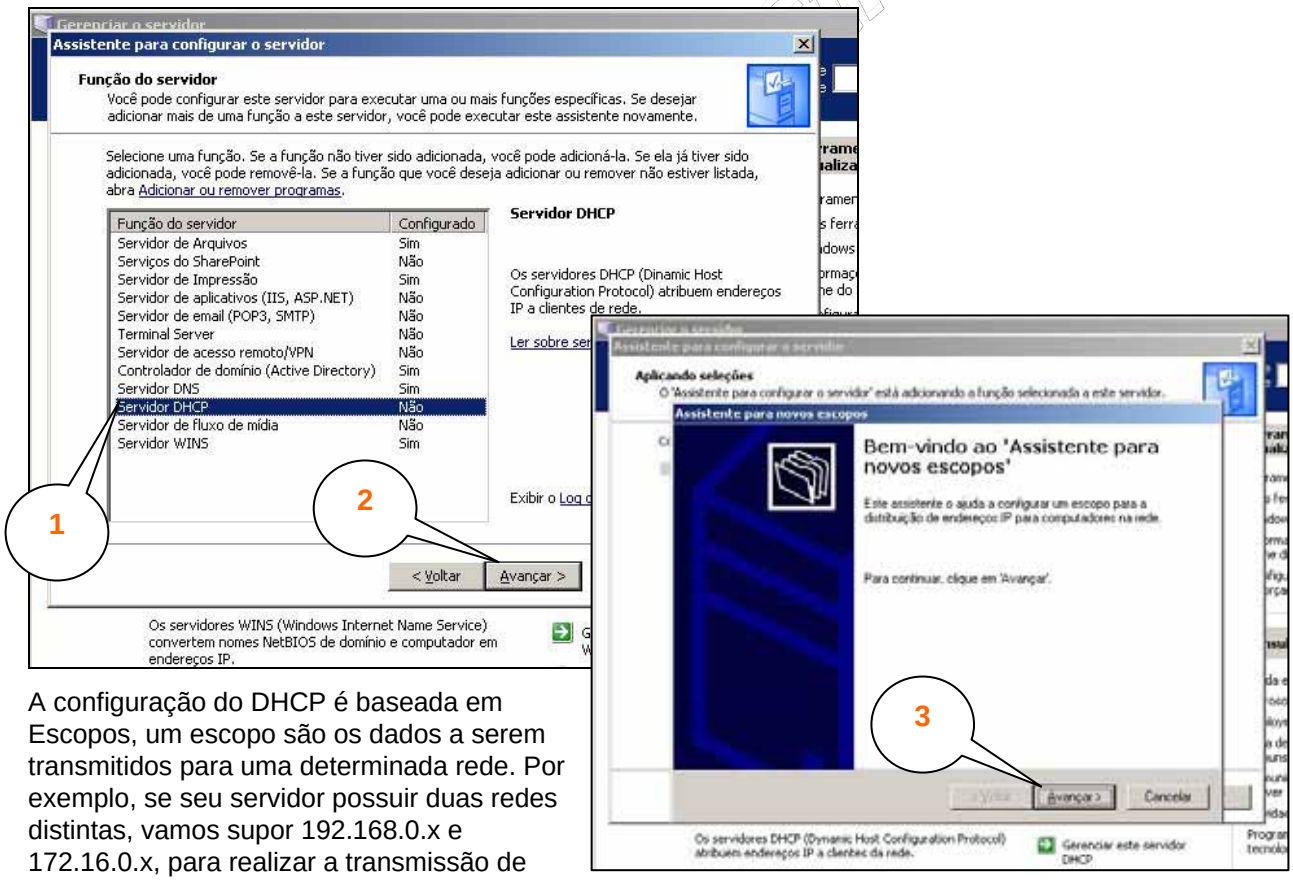
A última aba “Tipos de registro” permite que realizemos uma busca no banco de dados através de tipos específicos de registro, como: apenas estações de trabalho, apenas servidores de acesso remoto (RAS), apenas controladores de domínio, e assim sucessivamente. Através desse recursos é possível realizar pequenos inventários em rede, como: saber a quantidade total de estações de trabalho operantes nos últimos 30 dias.

E finalmente a consulta realizada ao banco de dados:



Servidor DHCP

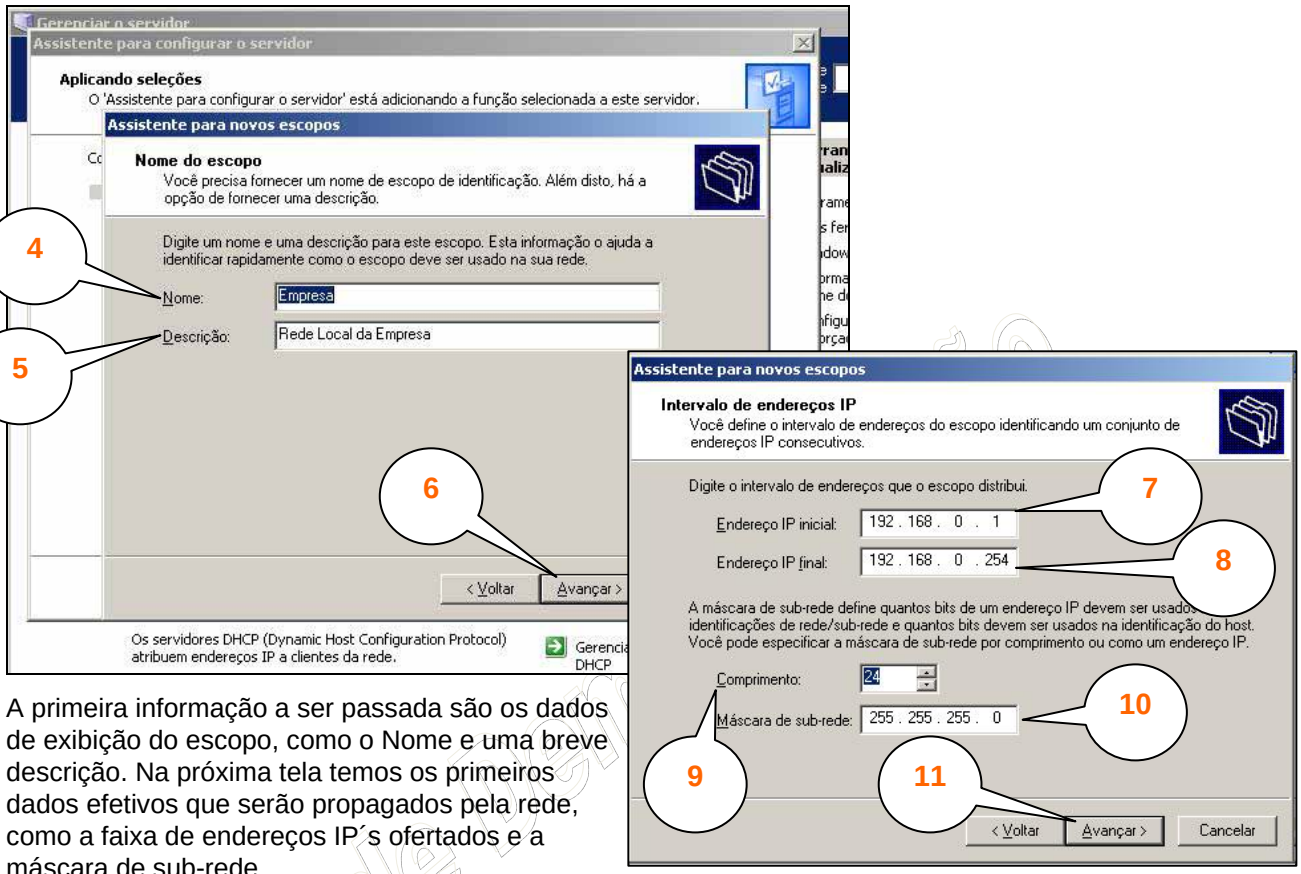
O último serviço básico de rede a ser visto é o DHCP, de Dinamic Host Configuration Protocol, ou protocolo de configuração dinâmica de hosts. Sua função é provê informações automáticas sobre os dados da rede para estações de trabalho, vamos as suas configurações:



A configuração do DHCP é baseada em Escopos, um escopo são os dados a serem transmitidos para uma determinada rede. Por exemplo, se seu servidor possuir duas redes distintas, vamos supor 192.168.0.x e 172.16.0.x, para realizar a transmissão de endereços ips para essas duas redes você precisará definir dois escopos, sendo um para cada rede.

Agora vai uma dica. É possível definir mais de um endereço IP por interface de rede, porém o servidor DHCP apresenta dificuldades para manusear os endereços a partir do segundo. A forma correta de utilizar escopos de DHCP é utilizando uma placa física de rede para cada ligação de rede.

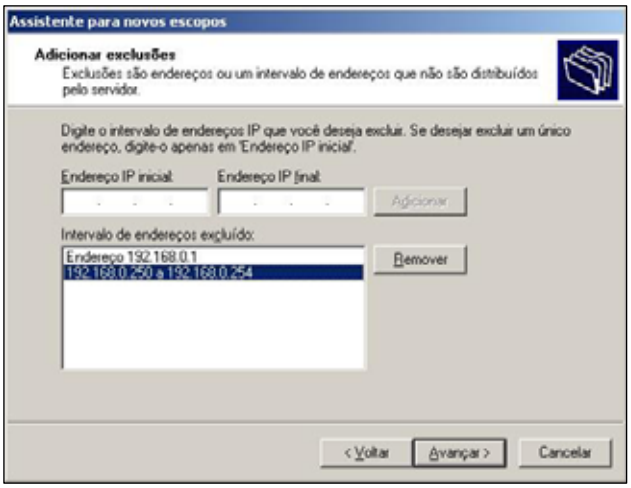
Vejamos agora a criação do escopo para nossa rede local:



A primeira informação a ser passada são os dados de exibição do escopo, como o Nome e uma breve descrição. Na próxima tela temos os primeiros dados efetivos que serão propagados pela rede, como a faixa de endereços IP´s ofertados e a máscara de sub-rede.

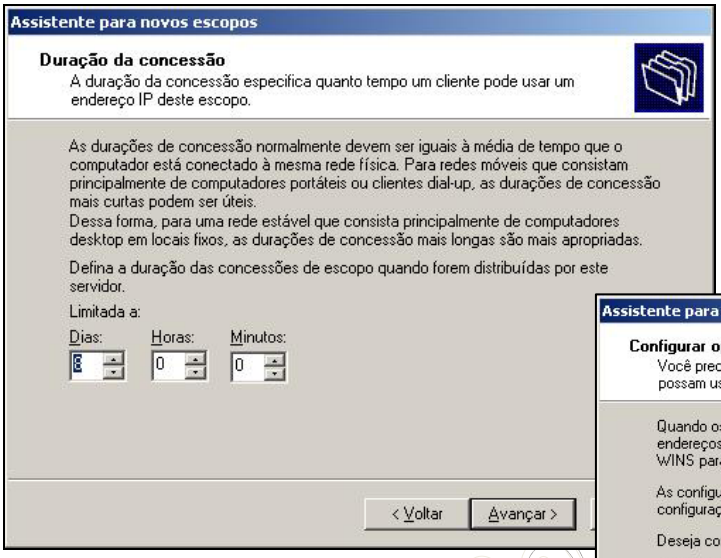
Agora vejamos o seguinte detalhe, estamos definindo no escopo DHCP, para serem ofertados todos os IP´s do bloco 192.168.0.0/255.255.255.0, porém alguns desses endereços IP´s já encontram-se em uso e não podem ser ofertados para as estações de trabalho, como o endereço IP 192.168.0.1, que é o nosso gateway da rede, o IP 192.168.0.253, que é o nosso próprio IP, entre outros possíveis. Então precisaremos excluir esses endereços do Intervalo de endereços IP. Para isso o assistente possui a próxima tela:

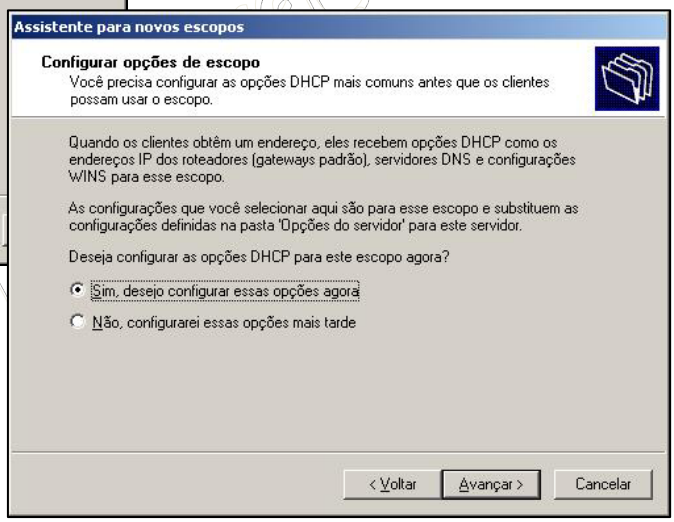
Podemos observar na imagem ao lado que os endereços IPs 192.168.0.1 e o conjunto de 192.168.0.250 à 192.168.0.254 foram excluídos da oferta DHCP. Essas exclusões se dão em virtude dos servidores já existentes e de uma margem para operar novos servidores.



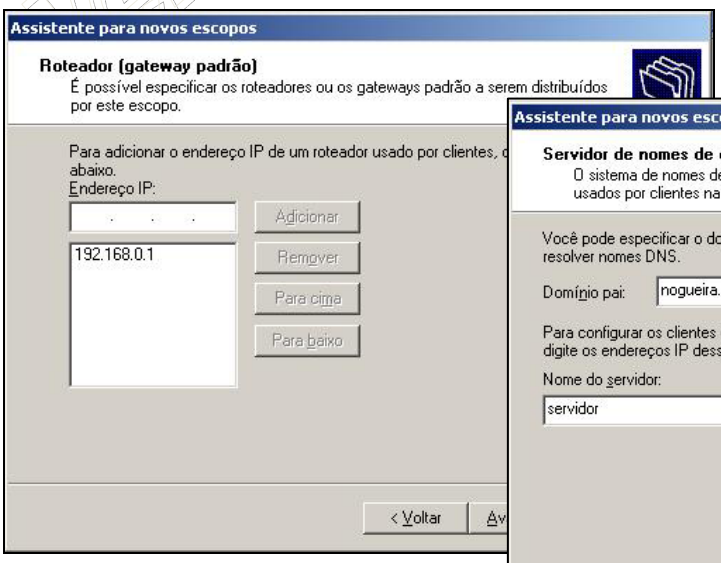
A próxima tela configura a duração da concessão das configurações de rede para cada estação, ou seja, se uma determinada estação ultrapassar o tempo de concessão, sua reserva junto ao banco de dados será excluída e seu endereço IP ofertado para outras estações. Uma prática observada sobre essa duração da concessão é que é possível uma determinada estação de trabalho da rede ficar meses com o mesmo endereço IP, como isso ocorre? Se definirmos um tempo de 12 horas para a duração da concessão, havendo uma estação de trabalho na rede que não passe mais do que 12 horas desligada, então essa estação não perderá sua concessão de endereço IP.

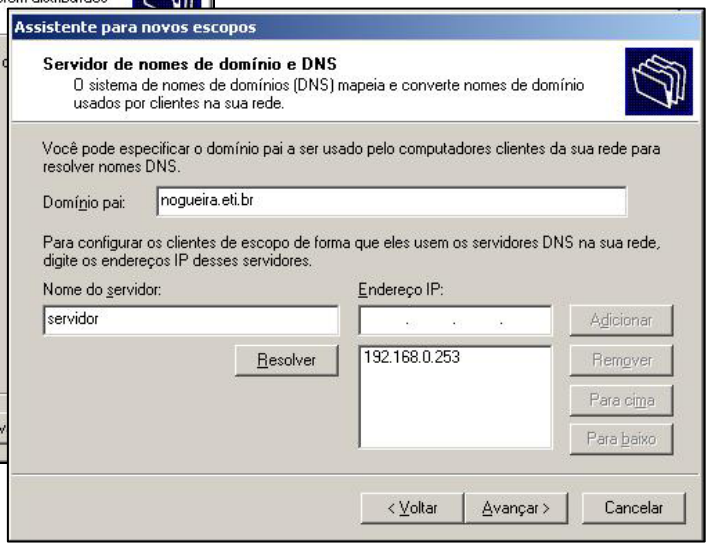
É importante fazer o bom dimensionamento desse tempo, pois ele pode implicar em performance de rede. Caso sua rede possua muitas estações de trabalho, sofra poucas mudanças e o maior recesso sejam os fins de semana, então um tempo razoável para sua rede é de 3 dias. Já, sendo a rede com muitos visitantes (notebooks) ou de acesso público (lan-house e cyber-café), então é interessante definir um tempo bem menor, como 1 hora.

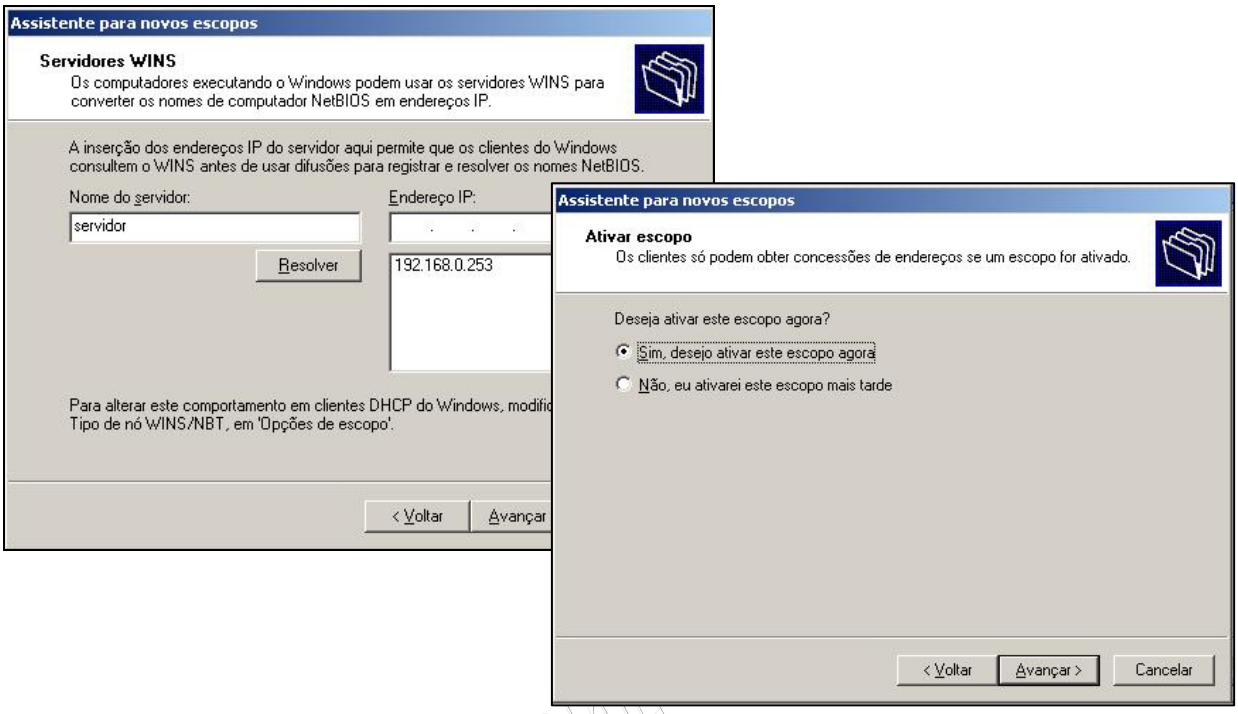




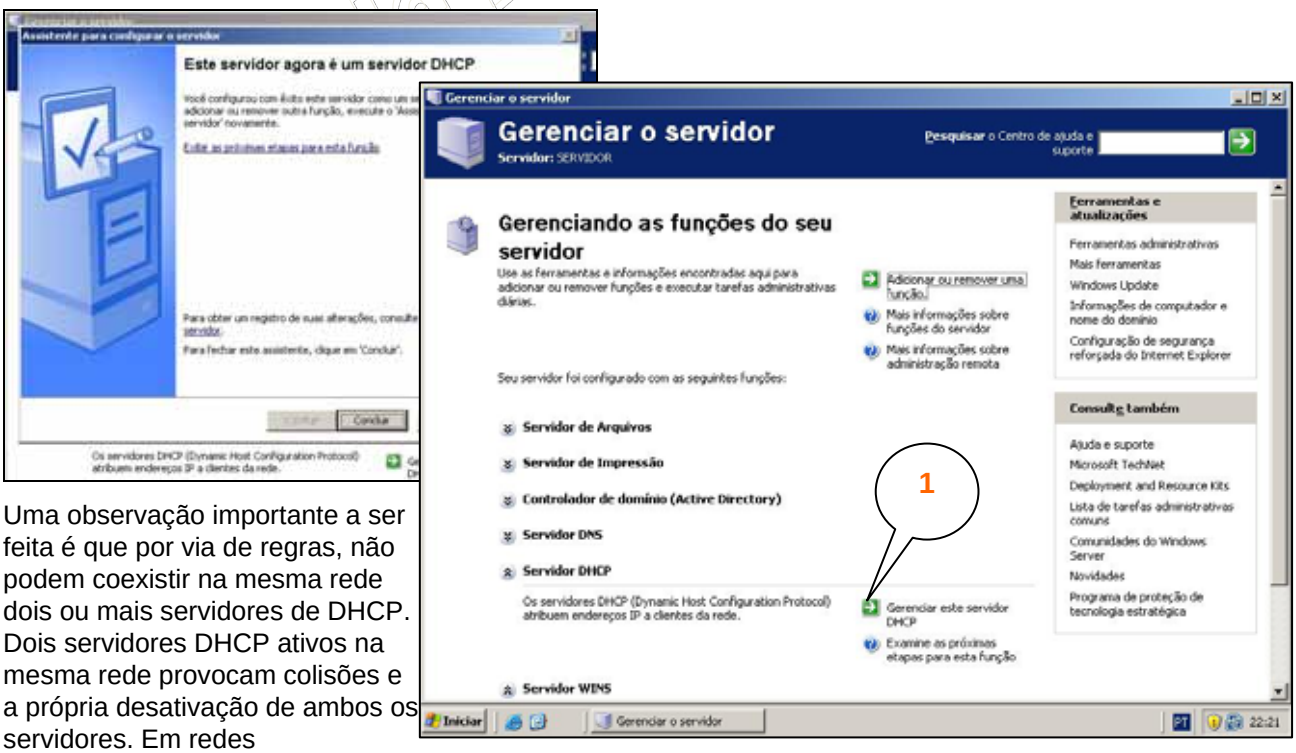
A próxima janela inicia as configurações das opções de escopo, como: endereço do gateway, servidores de DNS e WINS. Uma pequena observação que fazer aqui é que estas configurações podem ser realizadas no nível de Escopo ou no nível de Servidor. Opções realizadas no nível de escopo estão restritas a rede onde o escopo é aplicado. Opções realizadas no nível de servidores atuam sobre todos os escopos configurados:





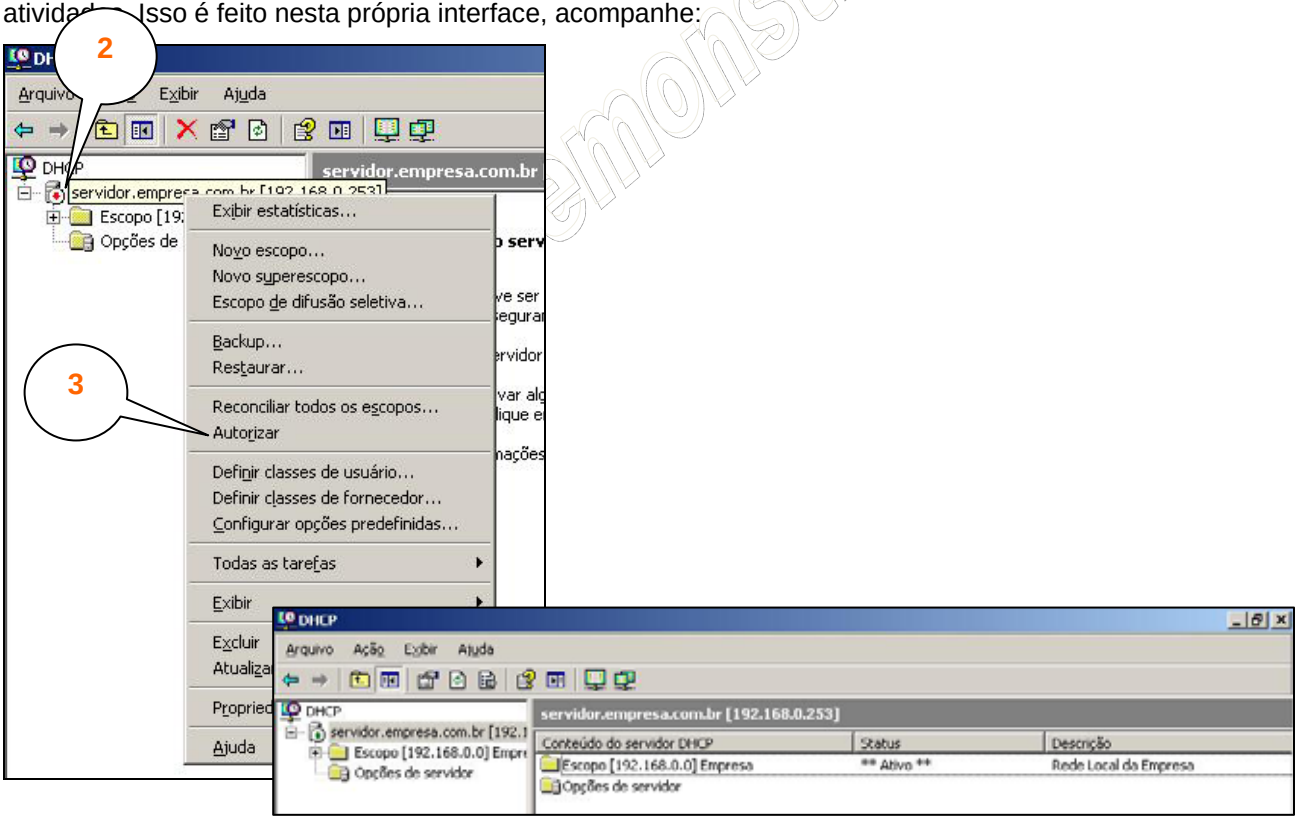


Ao concluir o assistente para a criação de um novo escopo será questionado se este escopo deverá ser ativado. Um escopo pode ser configurado porém, permanecer desativado, para questões de configuração. Ao ativar um escopo em rede suas configurações estarão sendo automaticamente propagadas pela rede.

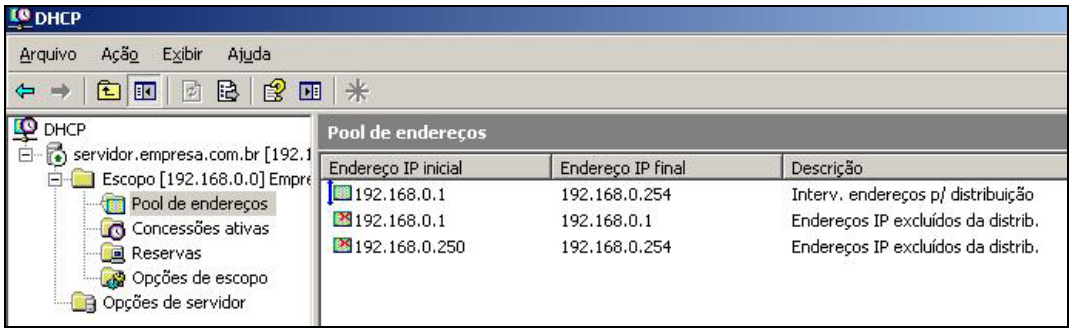


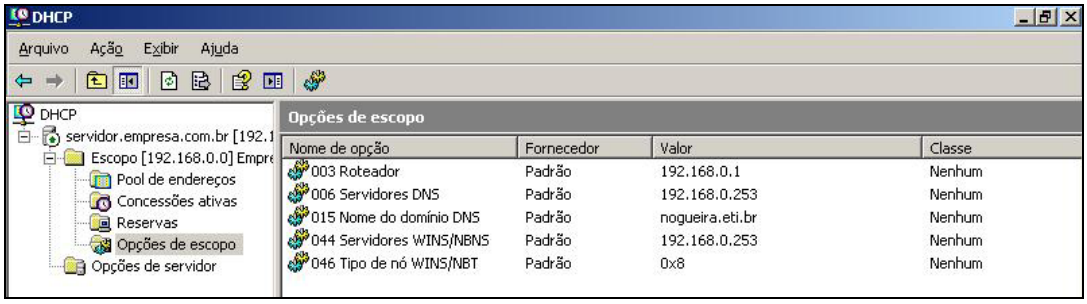
Uma observação importante a ser feita é que por via de regras, não podem coexistir na mesma rede dois ou mais servidores de DHCP. Dois servidores DHCP ativos na mesma rede provocam colisões e a própria desativação de ambos os servidores. Em redes administradas por um controlador de domínio, você só consegue ativar um servidor DHCP após autorizar esse novo servidor junto ao controlador de domínio, essa exigência visa justamente essa segurança em não permitir duas instâncias de servidores DHCP sobre a mesma rede:

Como podemos observar das imagens a cima, apesar das confirmações de êxito na instalação e configuração do servidor DHCP, porém ao acessarmos sua interface de administração o mesmo encontra-se desativado, justamente em função da proteção do controlador de domínio. Para efetivamente ativarmos o servidor DHCP precisaremos autorizar no controlador de domínio suas atividades. Isso é feito nesta própria interface, acompanhe:

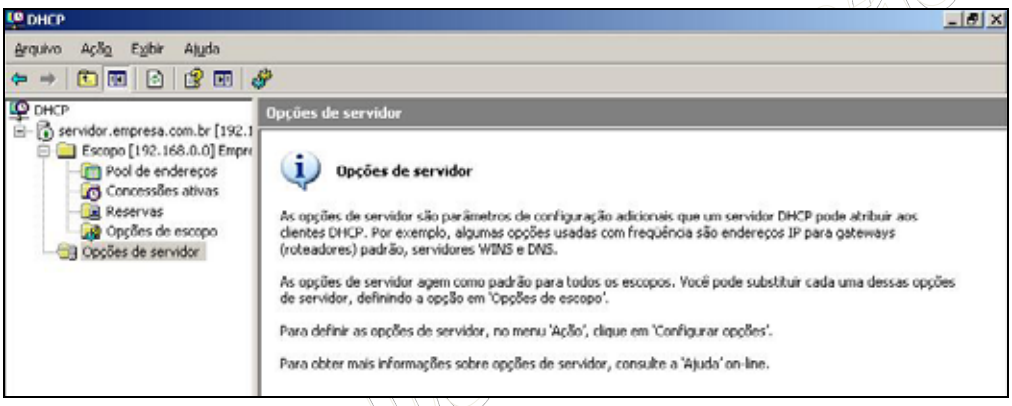


Uma vez com o servidor ativo podemos visualizar as configurações feitas através da aba “escopo”:





A última opção são as configurações realizadas no nível de servidor, a menos que você saiba exatamente o que pretende, não recomendamos as configurações dos itens nessa aba:



Com isso concluímos a primeira etapa da operação dos serviços básicos. Veremos a seguir como utilizar ferramentas para garantir a segurança e o backup das informações.

8.2 FERRAMENTAS DE SEGURANÇA

Nosso objetivo agora é apresentar as principais ferramentas utilizadas para a manutenção da segurança em redes baseada na infra-estrutura de sistemas operacionais de rede. Em se tratando do Windows Server 2003 as principais referências desta área estão nos links abaixo:

Introdução a Segurança do Windows 2003:
http://www.microsoft.com/brasil/security/guidance/prodtech/win2003/secmod117.mspx

Ameaças e Contramedidas:
http://www.microsoft.com/brasil/security/guidance/topics/ThreatsCountermeasures.mspx

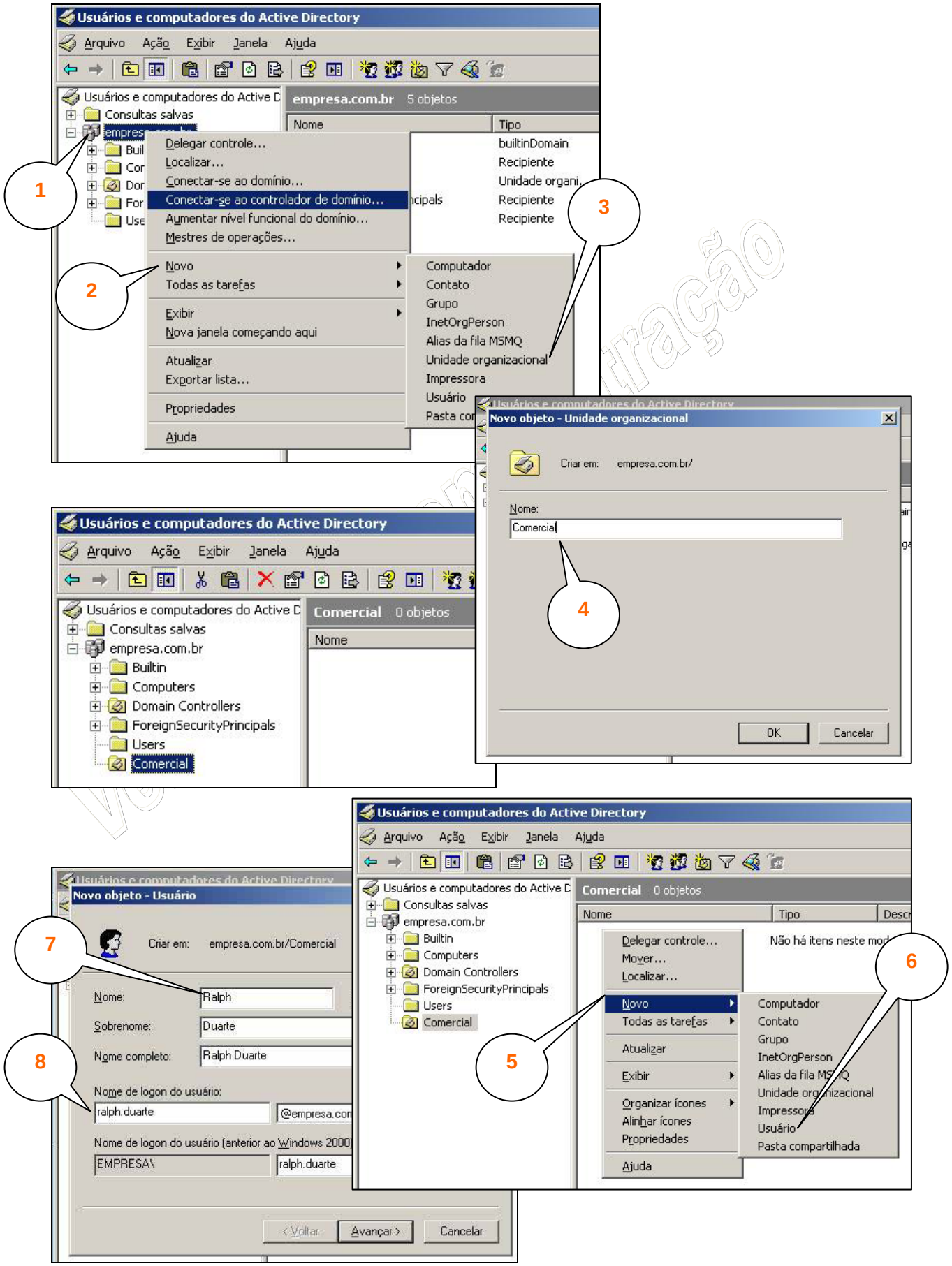
Ambas são referências oficiais da Microsoft e que devem ser estudadas cuidadosamente por aqueles que pretendem implementar servidores em ambientes hostis de produção.

As ferramentas abordadas nesta apostila serão:

- Proteção ao nível de domínio com o design de unidades organizacionais;
- Proteção ao nível de domínio com a implementação de políticas de grupos;
- Auditoria e gerenciamento de logs de segurança;

Unidades Organizacionais

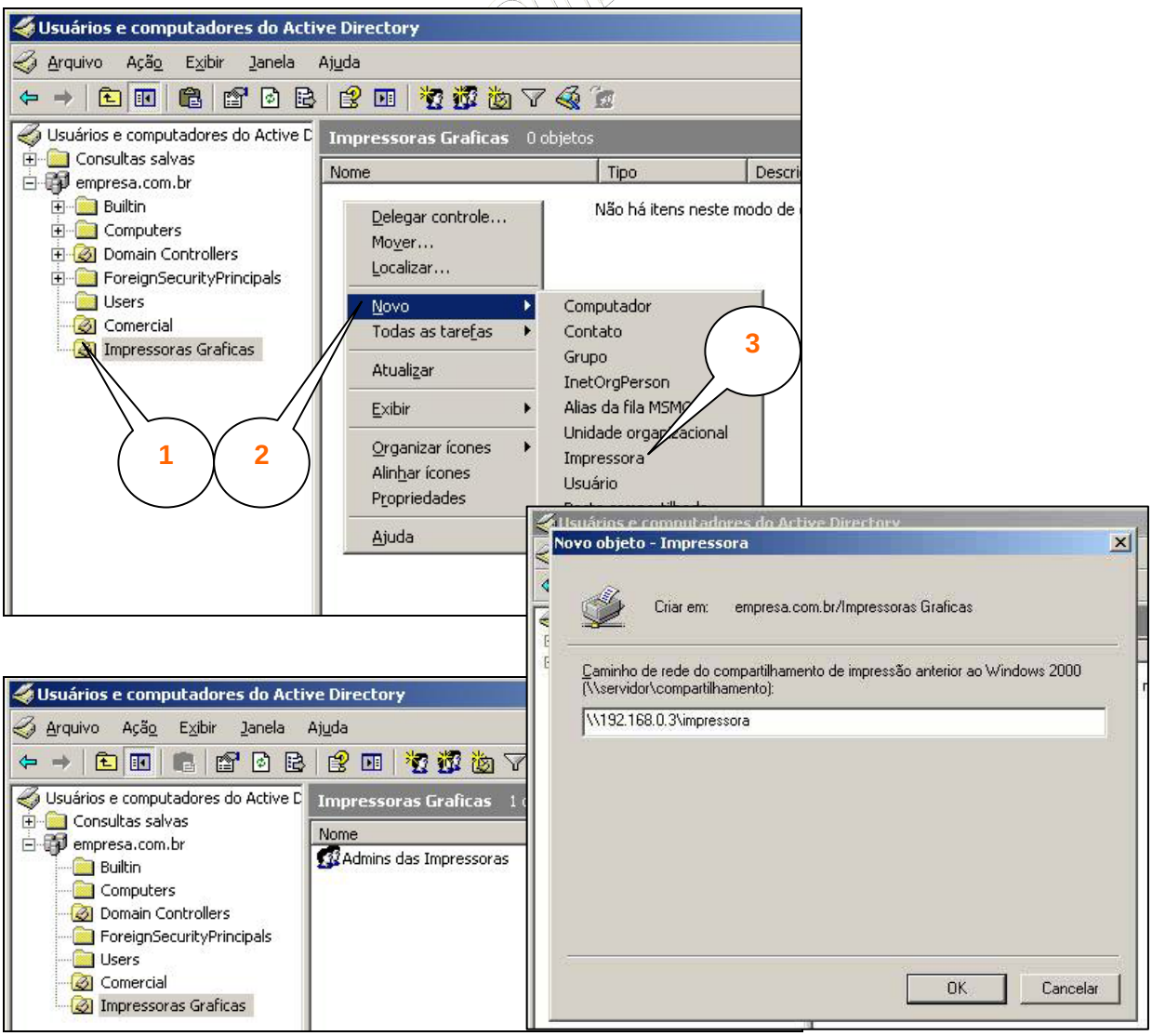
As Unidades Organizacionais (UO), são semelhantes a pastas, exibidas na interface de administração do Controlador de Domínio “Usuários e computadores do Active Directory”. A criação de contas no domínio pode ser realizada diretamente no domínio, onde serão exibidas na pasta “Users” ou em pastas distintas “Unidades Organizacionais”. Veja abaixo como criar uma UO e adicionar um usuário a esta pasta:



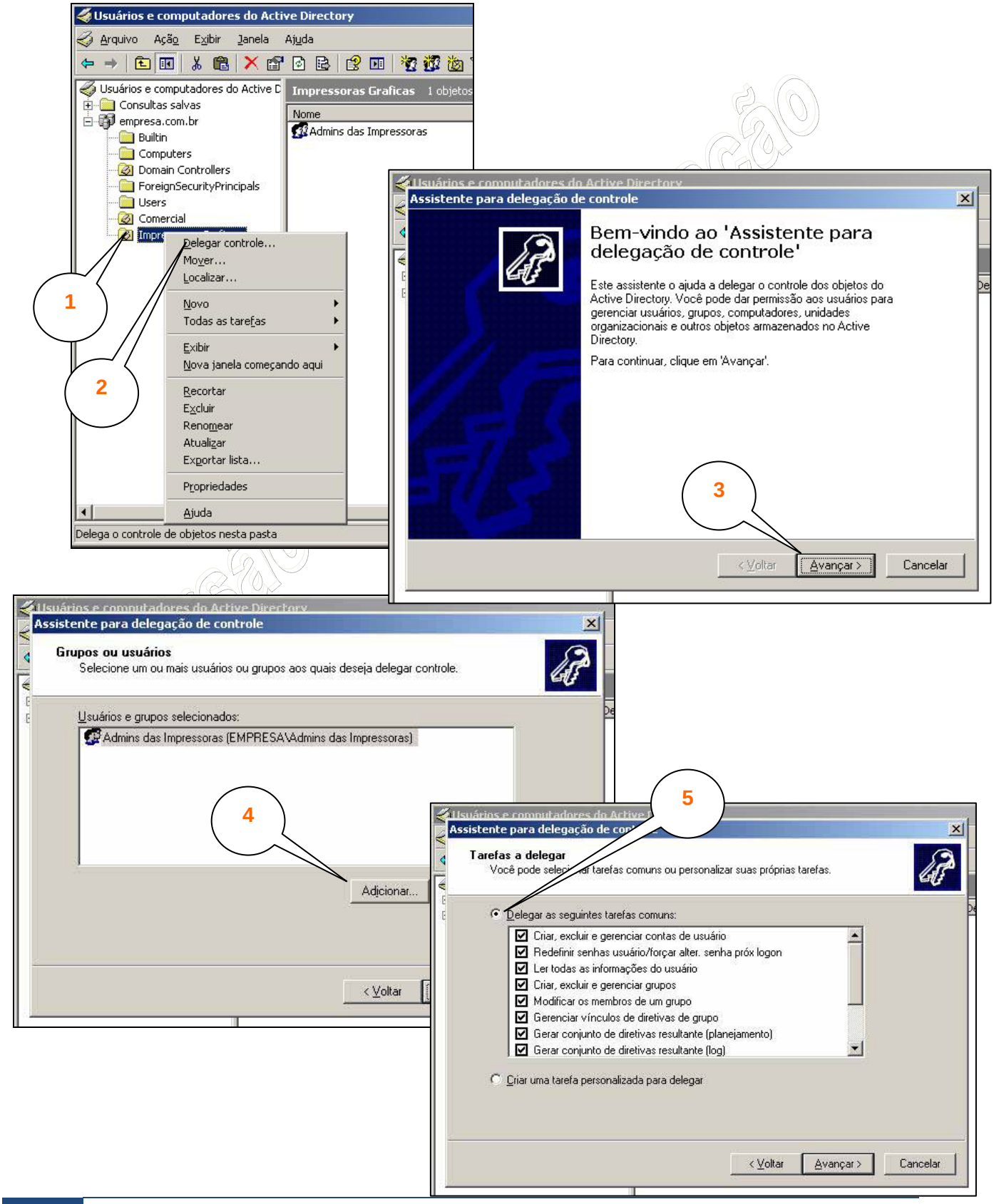
Com as UO podemos realizar as seguintes tarefas:

- Criar conjuntos de usuários com políticas de contas diferentes de forma a poder dar-lhes solicitações mais ou menos rígidas;
- Dar o controle de um conjunto de contas de usuários e/ou máquinas para um conjunto de usuários permitindo que você, por exemplo, defina um conjunto de pessoas que poderão redefinir senhas em um determinado departamento sem ter que torná-los administrador com mais poderes que o desejável e, além disso, restringindo o grupo de pessoas cujas senhas ele poderão alterar;
- Controlar e bloquear as máquinas dos usuários por meio do uso de Objetos de Diretiva de Grupo (GPO) ferramenta de controles semelhantes às políticas de controle do NT4; apesar de seu nome, entretanto as políticas de Diretivas de Grupo n(GPO) Não são aplicadas a grupos de usuários apenas a: **Unidades Organizacionais, Domínios ou Sites.**

Um exemplo de uso das UO é para criar contas de SubAdministradores, por exemplo: Suponha que o Departamento GRAFICOS tenha um conjunto de impressoras de alto Custo compartilhadas na rede. Eles Não gostariam que pessoas comuns controlassem tais impressoras, eles querem que seus técnicos locais sirvam de Administradores de impressão. Nesse caso, você pode criar uma UO denominada IMPRESSORAS GRÁFICAS e colocar as impressoras especiais nessa UO. Então você pode dar controle dessa UO e no processo das impressoras na UO para uma determinada conta de usuário ou talvez para um grupo que você queira. Vejamos abaixo como executar esse exemplo:



Nas imagens acima foram criados: Uma Unidade Organizacional denominada “Impressoras Graficas”, depois foram inseridas as impressoras especiais dentro desta UO, em seguida criamos um grupo de usuários denominado “Admins das Impressoras” e dentro deste grupo inserimos as contas dos próprios técnicos do departamento gráfico, estes serão os técnicos que poderão administrar sem restrições a UO Impressoras Gráficas. Vejamos como autorizar esse grupo para ter controle irrestrito:



A seguir o relatório de conclusão do assistente:

Existem grandes diferenças entre um Grupo de usuários para as UO. De maneira simples podemos dizer que você coloca coisa que deseja controlar em UO e depois você concede esse controle para um GRUPO. Caso você queira por exemplo, criar um subGrupo de uma empresa como um departamento e depois designar um grupo de pessoas que poderiam agir como administradores para esse departamento, então o departamento poderia ser uma UO e os administradores escolhidos poderiam formar um GRUPO. Você delegaria então autoridade sobre a UO para o Grupo. Mas existem alguns detalhes a serem observados:

- Uma conta de usuário só pode estar em uma UO, mas ele pode ser membro de quantos grupos você quiser. Uma conta der usuário ou de máquina existe em apenas um Domínio de forma geral, mas a conta também pode viver em uma UO dentro do Domínio, assim como você ou eu podemos viver dentro de uma mesma cidade em um estado, mas cada um de nós vive apenas em uma cidade. Em contraste, por exemplo não importa em que cidade você viva, você poderá ser um membro de tantas associações - grupos - quantas quiser;
- Você pode usar os grupos para designar permissões - você pode por exemplo, negar acesso a um arquivo a qualquer membro de um determinado grupo. O Windows 2003 não o deixará fazer atribuições de permissões com UO; você não poderá negar acesso a uma impressora ou arquivo compartilhado para toda uma OU;
- Em contraste você poderá usar UO para designar uma coleção de usuários que precisam trocar sua senhas com mais ou menos frequência do que os demais, mas não poderá fazer isso com um grupo. Você pode aplicar uma política de Grupo (GPO) (por exemplo distribuir um aplicativo) para uma determinada UO, mas não para um grupo;

Políticas de Grupo

Até agora aprendemos sobre UO e suas funções, mas agora veremos como tirar o máximo de proveito dessa ferramenta usando as Diretivas de Grupo.

Para aqueles que já tiveram a oportunidade de operar um NT 4.0 as diretivas de grupos se assemelham as políticas de sistema. Com as políticas de sistema do NT 4.0 você podia controlar uma grande variedade de itens, como: definir um menu iniciar/programas específico para um determinado usuário, determinar a aparência para a área de trabalho, proibir de mudar a página inicial do navegador. Todas essas restrições eram reunidas em um único arquivo denominado NTCONFIG.POL, que você então posicionaria em cada um dos compartilhamentos NETLOGON do controlador de domínio. A pasta NETLOGON, como vimos na instalação e configuração do Controlador de Domínio, é o local onde residem os scripts de rede, ou seja, toda vez que um usuário realizar o logon na estação da redes um determinado conjunto de instruções, executados através desses scripts, é processado. Você não podia ter mais de um arquivo de políticas do NT 4.0 e existia o utilitário poledit.exe que manipulava essas regras diretamente na estação.

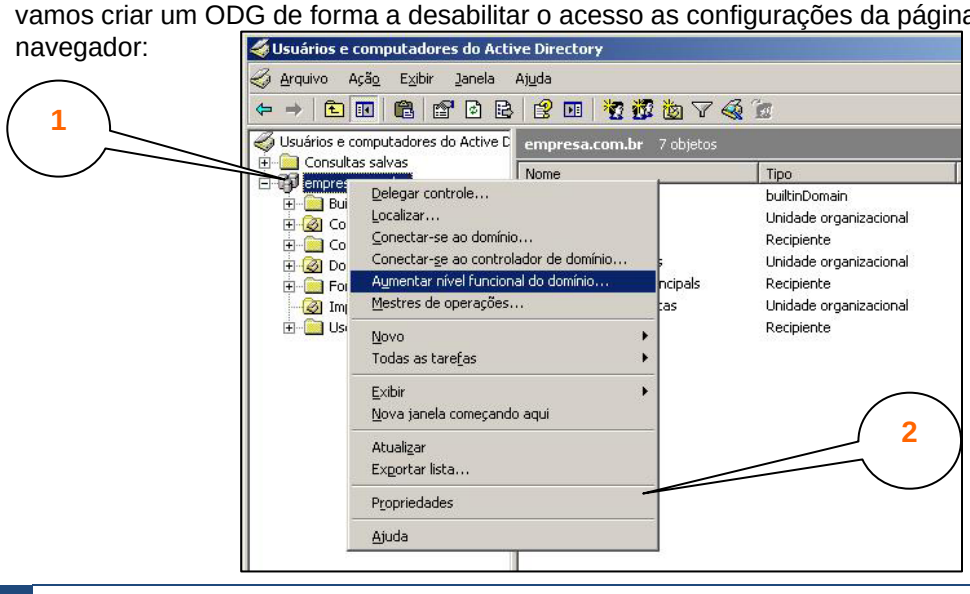
Com o Windows Server 2003 não há um arquivo tangível e separado para as políticas. Em vez disso, o Windows 2003 armazena as informações de políticas no Active Directory. Você coloca essas informações no AD na forma de OBJETOS DE DIRETIVAS DE GRUPO, ou ODGs. Você pode colocar tantas políticas específicas em um determinado ODG quantos quiser. Suponha, por exemplo, que você gostaria de executar três ações com as políticas para todos os usuários:

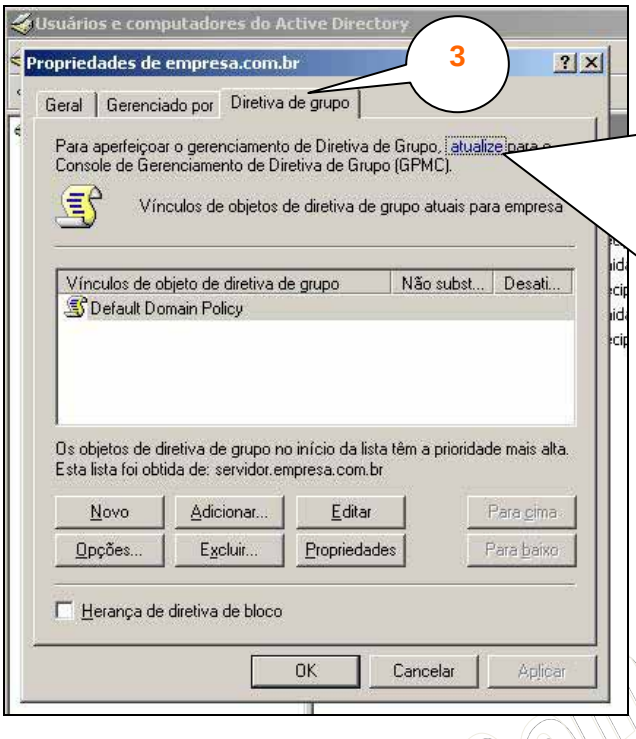
1. Que todos fossem capazes de alterar o horário do sistema em suas estações de trabalho. (por padrão usuários comuns não podem fazer isso no Win2000);
2. Que a pasta MEUS DOCUMENTOS de todos fossem armazenadas na rede em vez de serem armazenadas nos seus discos rígidos, para que o backup seja feito de forma centralizada;
3. Que a inicialização do Word 2000 para todos os usuários se desse apartir de um servidor central;

Você pode criar um único ODG e incluir todas essas três políticas no seu interior e depois aplicar essa ODG para todos. Ou poderia ter três ODGs separados, colocar uma das políticas em cada um deles e depois aplicar cada uma das três políticas para todos, ou qualquer coisa intermediária entre esses dois métodos. Todas essas soluções produziriam o mesmo efeito.

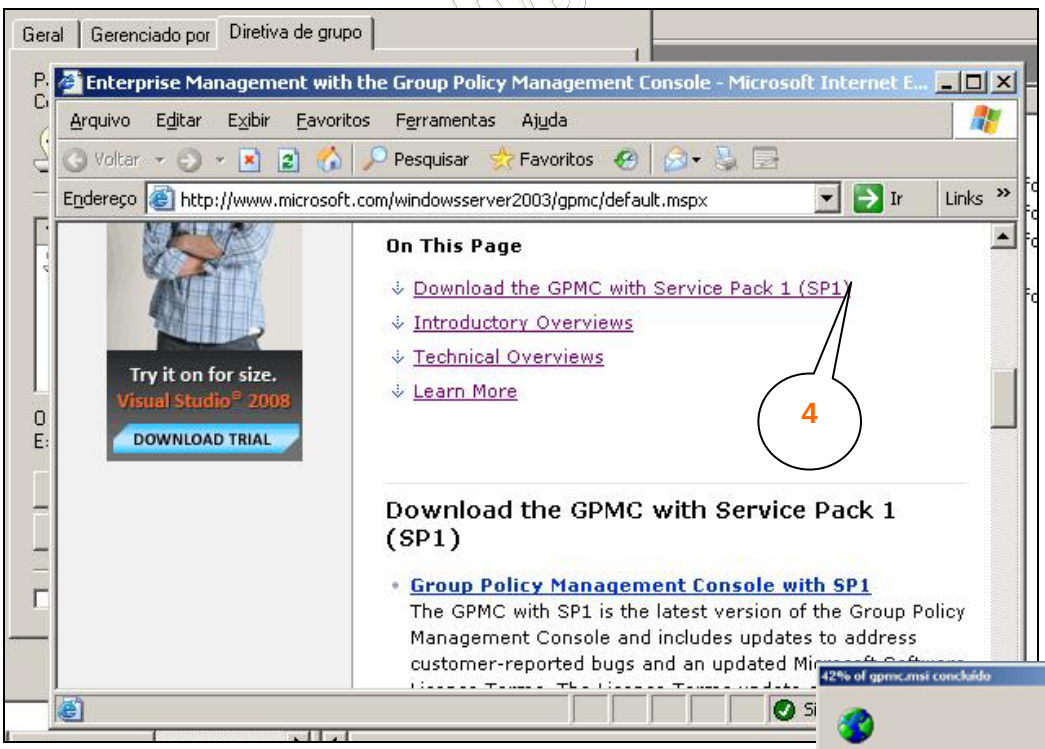
Talvez você então perguntaria: por quê você poderia criar ODGs múltiplos ou ODGs separados ? Quanto menos o ODGsm mais rápidas serão as conexões. Toda vez que um usuário se conectar, o active directory precisa varrer todos os seus ODGs para verificar quais deles se aplicam a esse usuário. Por outro lado você poderia criar ODGs diferentes se quisesse aplicar políticas diferentes para pessoas diferentes. - se quisesse por exemplo que o pessoal de uma UO fosse capaz de alterar os horários de suas estações de trabalho mas quisesse uma pasta MEUS DOCUMENTOS diferente para a UO na rede, então criaria uma ODG que permitisse aos usuários alterar os horários de suas estações de trabalho e aplicaria esse ODG para a primeira UO, e depois criaria um ODG diferente movendo a pasta MEUS DOCUMENTOS para a rede e o aplicaria para a segunda UO.

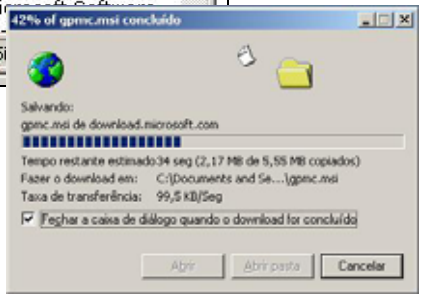
Para exemplificar essa teoria vamos aproveitar o primeiro exemplo, o das impressoras gráficas, e vamos criar um ODG de forma a desabilitar o acesso as configurações da página inicial do navegador:





Por padrão, a Microsoft não disponibiliza a Console de Gerenciamento de Diretivas de Grupo (GPMC), porém permite o seu download, gratuito, através de seu site na Internet. Através deste link você pode baixar e instalar o GPMC. Uma vez instalado esta aba de "Diretiva de grupo" será substituída por uma nova interface, bem mais sofisticada e com novos recursos. Realize esta atualização antes de continuar.

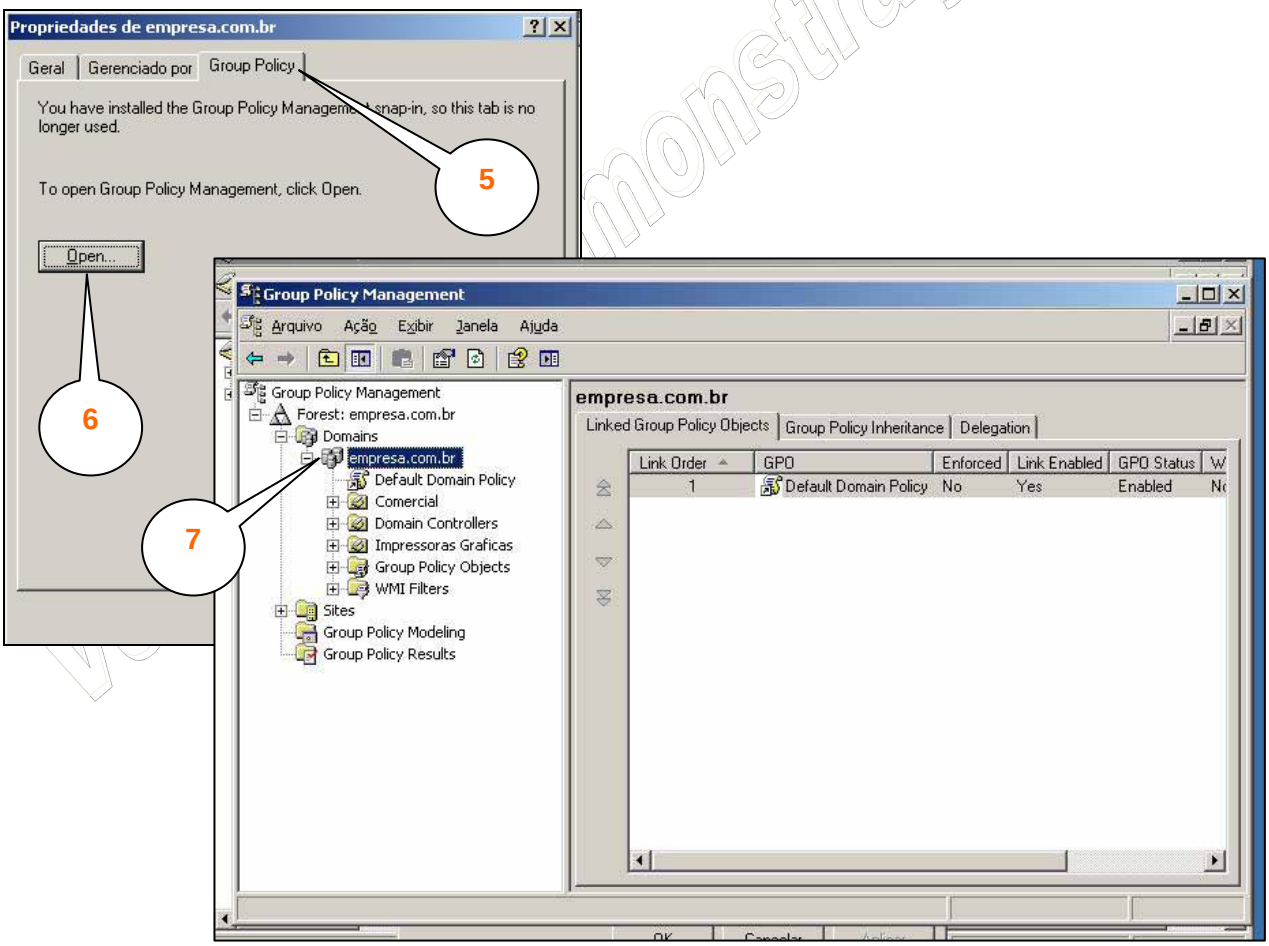




Após realizar o download e iniciar a instalação caso apareça o seguinte aviso abaixo, pode continuar a instalação sem problemas. O aviso se refere a uma atualização do componente MS-XML, porém esta atualização só está disponível para as distribuições em inglês.

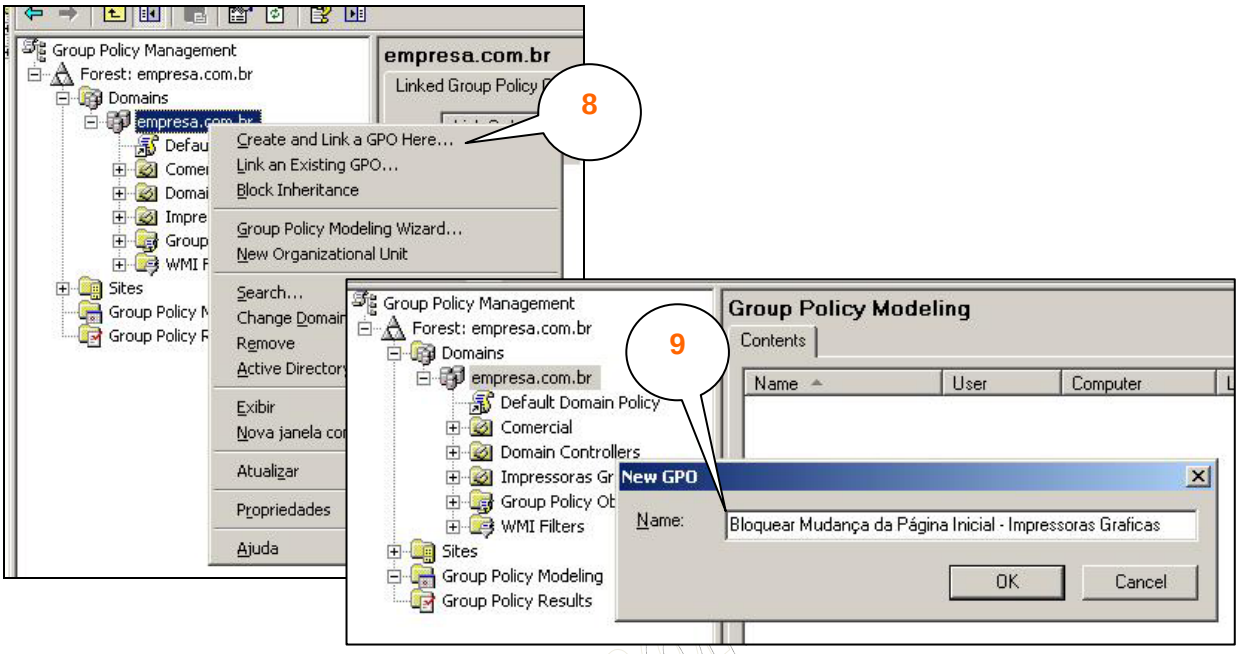
Após a instalação do GPMC é necessário reinicializar o Windows, mesmo que não seja solicitado.

Voltando para nossa interface de administração em “Usuários e computadores do Active Directory”, observamos que a aba “Diretiva de grupo” é substituída pela “Group Policy”, e que o acesso as edições das diretivas muda para um botão.

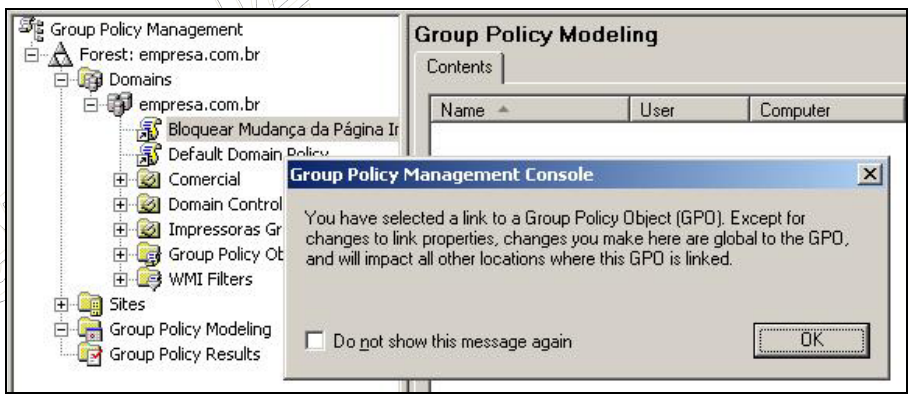


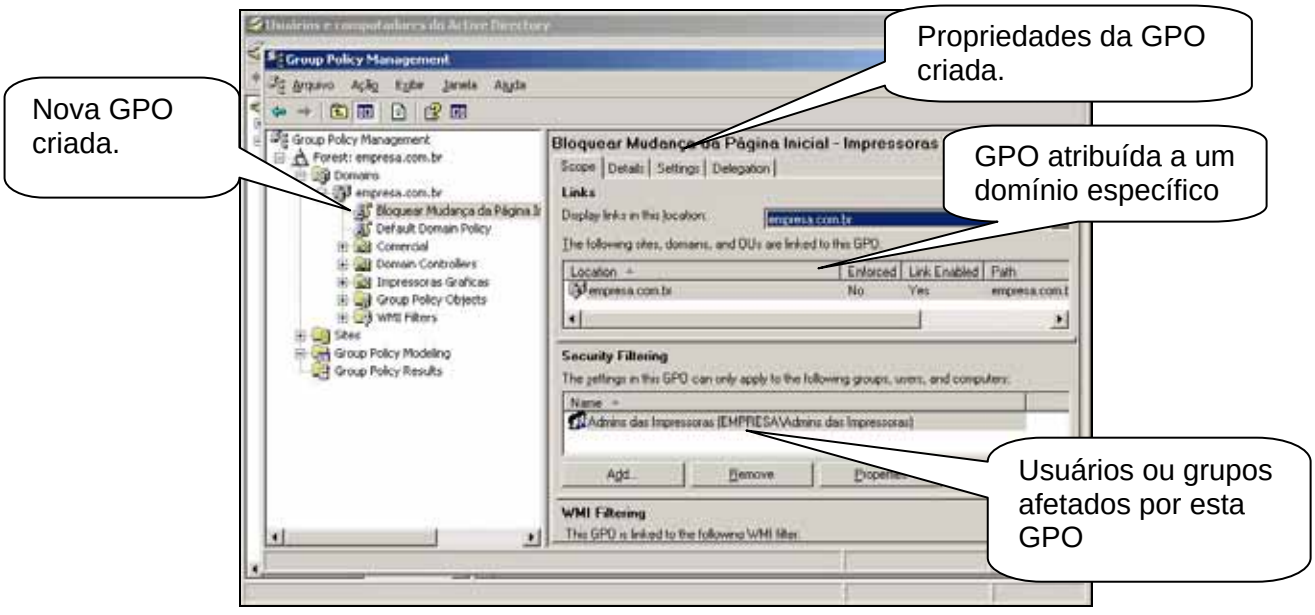
Na interface do “Group Policy Management”, ao acessarmos o nosso domínio “empresa.com.br” iremos nos deparar com algumas novas informações. O “Default Domain Policy” é uma diretiva pré-estabelecida, porém sem nenhuma funcionalidade. Seu objetivo é muito mais de orientar do que executar. É possível apenas editar essa diretiva e a utilizar para aplicação de restrições.

O correto é ignorarmos essa regra default (posteriormente também é bom apagá-la, pois quanto mais regras existirem mais lentos serão os logons de rede) e criarmos as nossas próprias. Vejamos agora o exemplo:

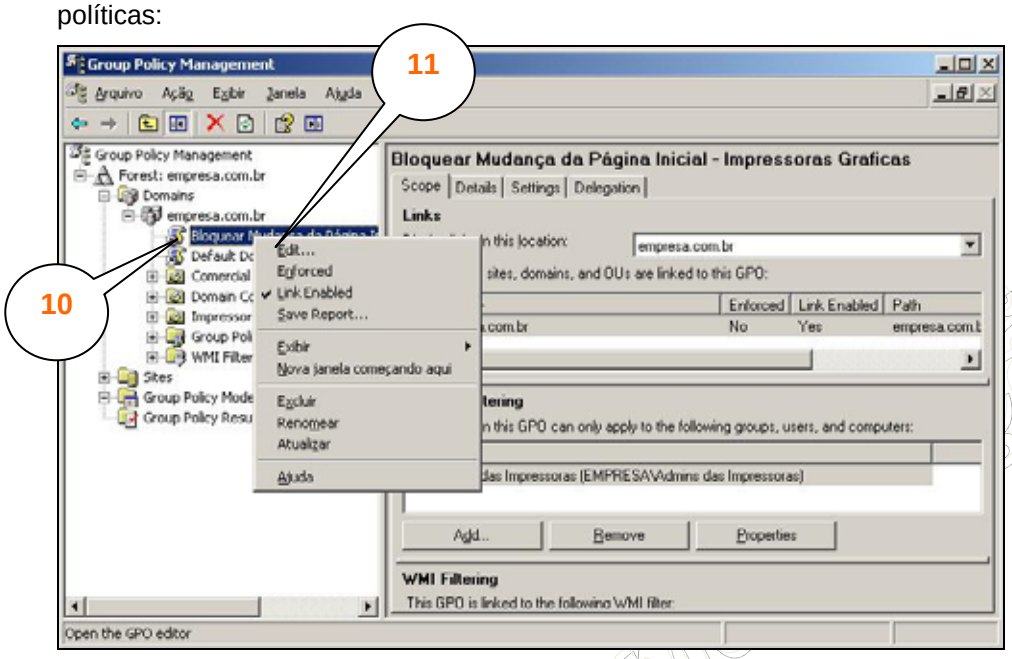


Ao tentar criar ou modificar um ODG, ou em inglês GPO, é alertado que está GPO faz parte de um escopo global, e que qualquer alteração nesta GPO específica afetará e sobrescreverá demais GPOs existentes. Esse aviso alerta para o caso de haverem controladores de domínios filhos ou unidades organizacionais. Aceite o aviso e se quiser marque a opção de não mostrar esse aviso novamente.

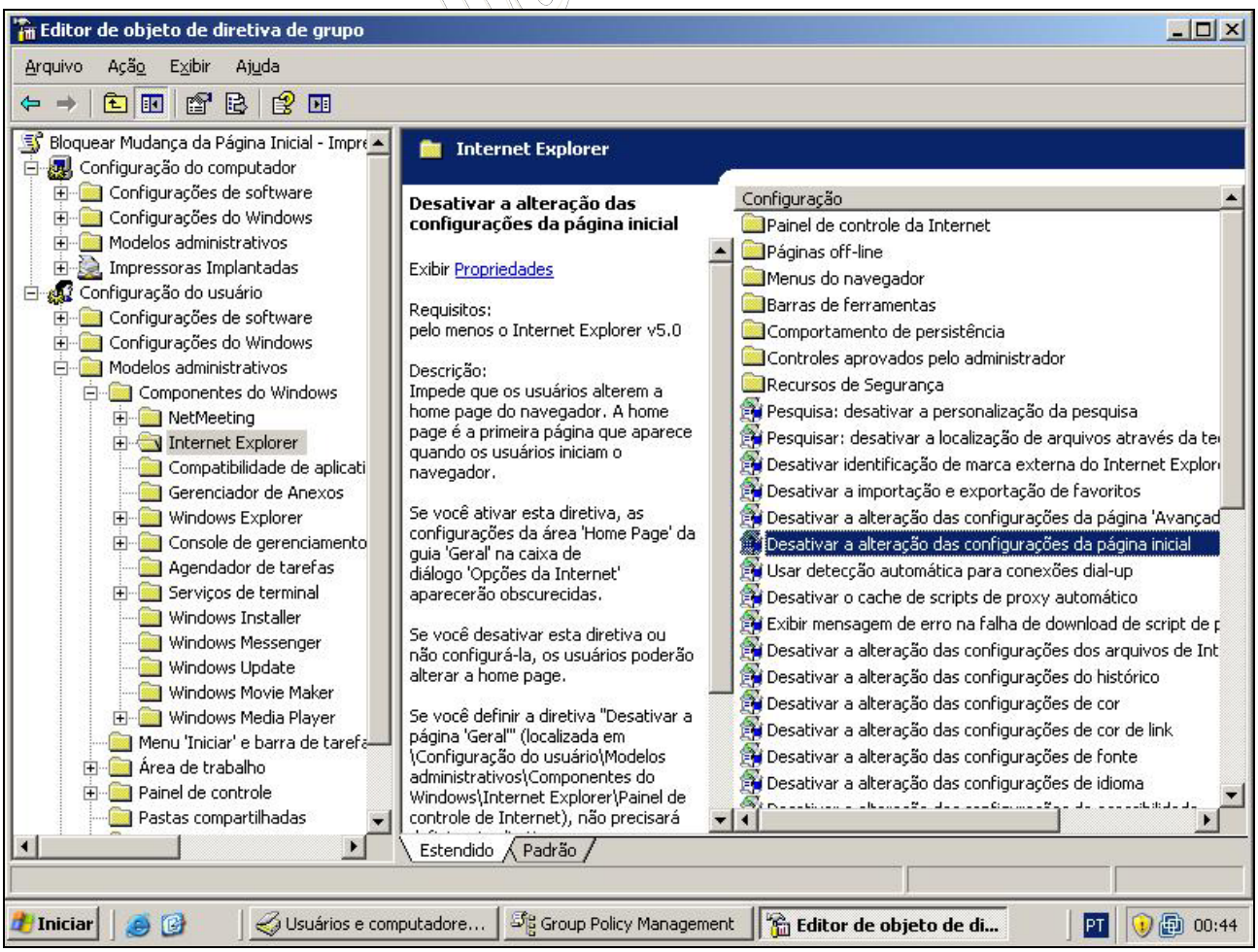




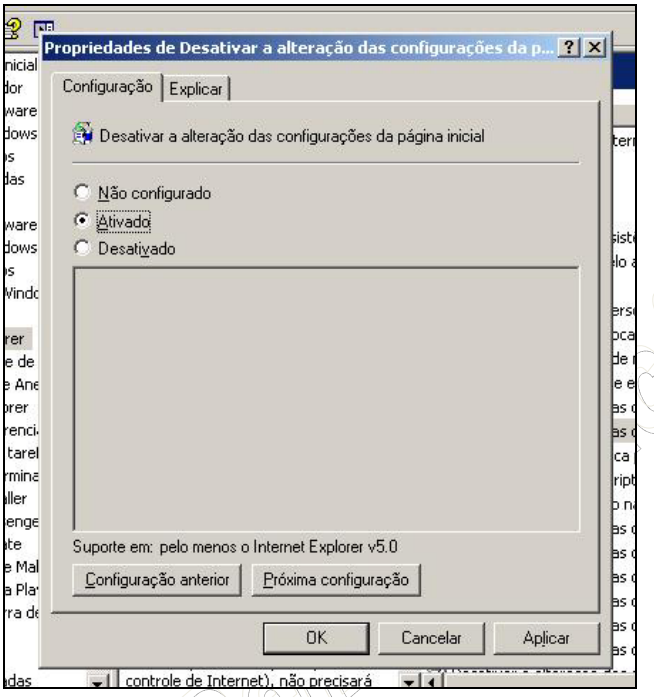
Uma vez criada a GPO agora passaremos para a parte mais interessante, a de edição das regras e políticas:



Observe que existem várias itens possíveis de configuração. A grande maioria sendo auto-explicativa e com apenas opções de habilitar ou desabilitar, vejamos abaixo:

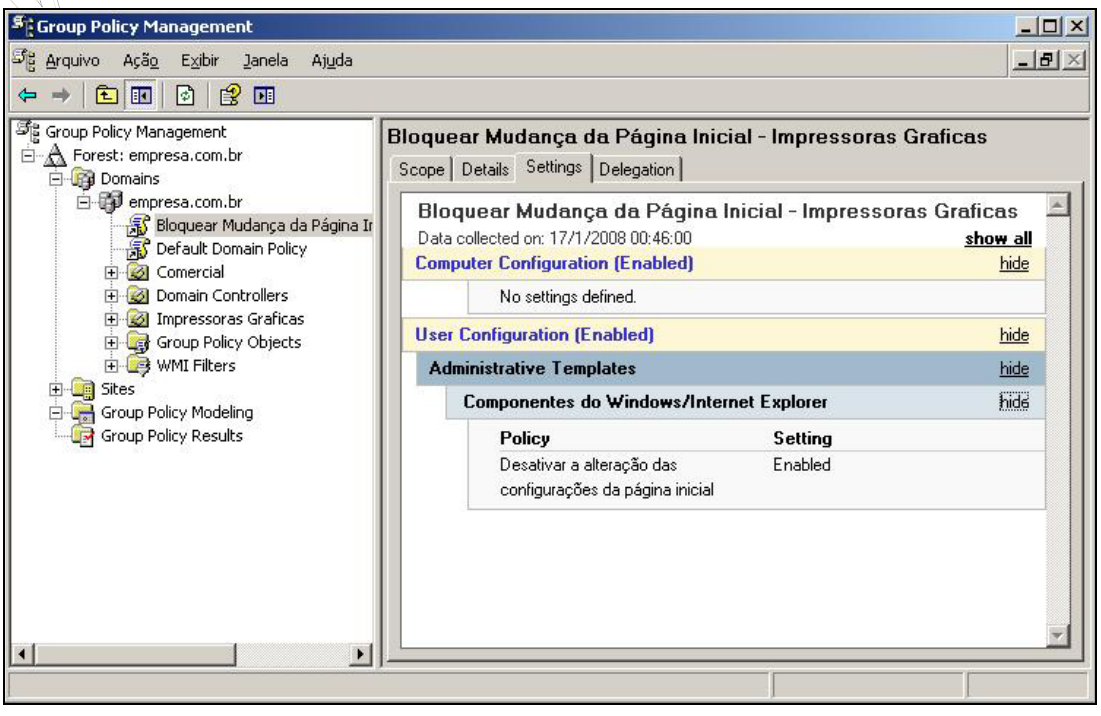


Ao selecionarmos um item para modificação a seguinte janela de propriedades é apresentada:



Aqui encontramos três opções: Não configurado (para voltar ao padrão original sem precisar ter que restaurar todas as regras), Ativado (força que a propriedade seja ativa), ou Desativado (força que a propriedade seja desativada). A depender da forma como você cria sua política é possível que algum item que seja expressamente Desativado, volte a ser Ativo em uma política mais a frente. As diretivas funcionam como uma grande lista de regras, que são executadas em ordem, de cima para baixo, ao ter uma regra inicial sobrescrita por uma regra de fim de listagem nenhum aviso é emitido e com isso a GPO não funcionar a contento. Para evitar esses tipos de erros recomenda-se a criação de GPOs distintas, porém isso acarreta em perda de desempenho para os clientes da rede. O ideal é que você crie as GPOs individualmente e ao longo do tempo, baseado em testes de laboratório e observações, tente mesclar as GPOs, de forma a ficar com o mínimo possível.

Através da interface de administração do GPM é possível listar as configurações feitas em cada GPO. Isso é extremamente útil para não termos que editar a GPO e tentar achar as alterações:



Auditoria e Gerenciamento de Logs de Segurança

Antes de apresentarmos o Visualizador de Eventos, falaremos sobre alguns conceitos, como: eventos, log de eventos, tipos de logs e tipos de eventos.

- **Eventos**: são ações efetuadas pelos usuários, baseadas em diretivas de auditoria, ou ações efetuadas pelo próprio Windows 2003. Através dos eventos, ficamos sabendo sobre erros, tentativas de ruptura da segurança, entre outras informações ocorridas no sistema;
- **Log de Eventos**: com os logs, podemos monitorar informações sobre segurança e identificar problemas de software, hardware e sistema. Existem 3 tipos de logs:
    - **Log de sistema**: armazena os eventos registrados por componentes do Windows 2003, como o não carregamento de um driver, entre outros;
    - **Log de aplicativo**: armazena os eventos registrados por aplicativos ou programas;
    - **Log de segurança**: registra os eventos de segurança, como tentativas de logon válidas e inválidas, entre outros;

O log de segurança só pode ser visualizado por usuários com direitos administrativos. Com relação aos eventos de sistema e aplicativos, podemos ter 3 tipos:

- **Informação**: exibe informações sobre operações bem sucedidas de um aplicativo;
- **Aviso**: pode indicar um problema futuro. Fique atento a esses eventos;
- **Erro**: indica problemas significativos nas operações do sistema;

Já os eventos de log de segurança podem ser:

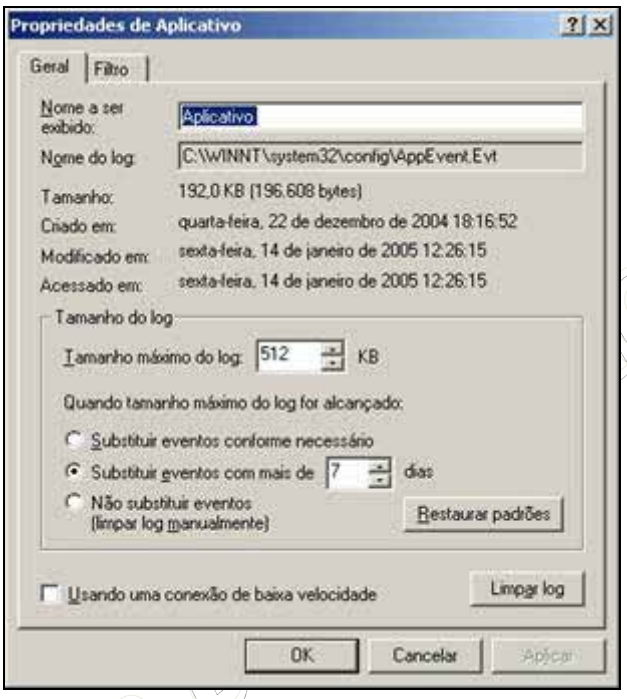
- Auditoria com êxito: registra auditorias executadas com sucesso, como tentativas de logon efetuadas com sucesso;
- Auditoria sem êxito: registra auditorias executadas sem sucesso, como tentativa de logon efetuada sem sucesso;

Finalmente, para visualizarmos todos esses eventos, o Windows 2000 nos fornece o console Visualizador de Eventos. Acessamos esse console através das Ferramentas Administrativas, localizadas no Painel de Controle:

Algumas considerações sobre sobe o Visualizador de Eventos:

- Podemos visualizar os logs de computadores remotos;
- Em cada log de evento, podemos visualizar as seguintes propriedades de um evento: tipo, data, hora, origem, categoria, evento, usuário e computador;

- Podemos também procurar por eventos específicos;
- Podemos limitar o tamanho dos logs de evento. O tamanho do log varia de 64 KB a 4 GB. O valor padrão é 512 KB:



- Quando um log de eventos está cheio, podemos definir quais serão as ações do Windows 2000. As opções são as seguintes:
  - **Substituir eventos conforme necessário** : com essa opção ativada, você pode perder informações se o log ficar cheio antes de você arquivá-lo;
  - **Substituir eventos com mais de x dias** : parecida com a opção anterior, porém podemos especificar a quantidade de dias que um evento deverá permanecer no log;
  - **Não substituir eventos** : essa opção exige que você limpe o log manualmente. Quando o log estiver cheio, o Windows deixará de registrar os eventos e emitirá uma mensagem informando que o log está cheio;
- Podemos arquivar o conteúdo de um log de evento em 3 formatos, os quais são:
  - **.evt** : podemos visualizar os logs no Visualizador de Eventos posteriormente;
  - **.txt** : podemos visualizar os logs em processadores de texto;
  - **.csv** : formato de arquivo de texto delimitado por virgulas. Pode ser visualizado e planilhas eletrônicas e banco de dados;
- Podemos também limpar o log de eventos.

Agora que sabemos visualizar os logs vamos partir para a configuração das auditorias. Podemos controlar as atividades dos usuários e do sistema em um computador Windows 2003, utilizando a auditoria. Com isso, podemos detectar tentativas de invasão em nossa rede.

Recordando, quando ocorrer algum evento relacionado com a auditoria habilitada, o Windows 2003 grava esse evento no log de segurança. Para visualizarmos esses eventos utilizamos o Visualizador de Eventos. As informações gravadas no log de segurança são as seguintes:

- Ação executada;
- Usuário que executou a ação;
- Êxito ou falha na ação, e quando ocorreu a ação;

- Computador no qual a ação foi executada;

Configuramos as auditorias através das diretivas de segurança, e podem ser habilitadas em um computador local ou em uma GPO.

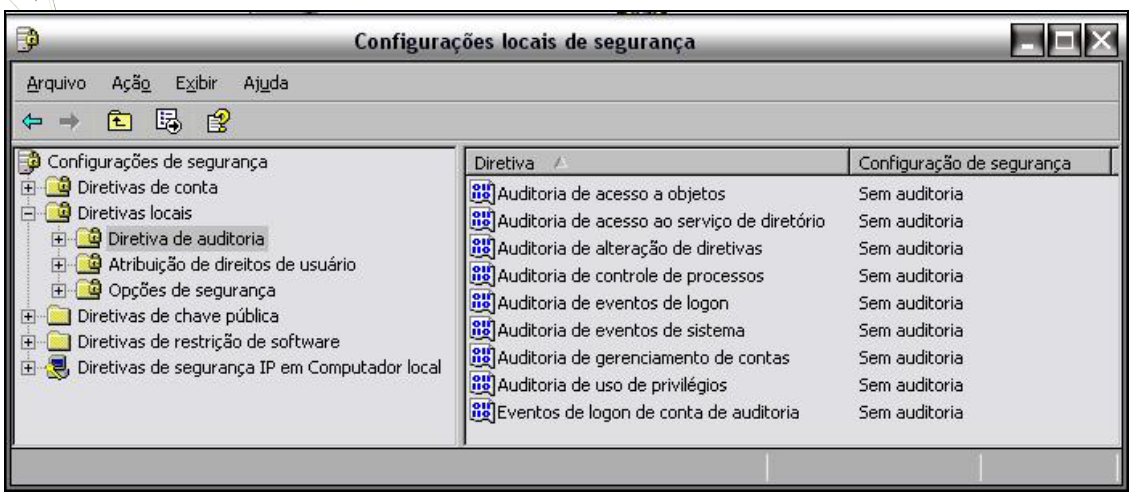
Os tipos de auditorias que podem ser realizadas pelo Windows 2003 são:

- **Auditoria de Acesso a Objetos**: ocorre quando um usuário acessa um arquivo, pasta ou impressora. Os objetos devem estar configurados para a auditoria;
- **Auditoria de Acesso ao Serviço de Diretórios**: ocorre quando um usuário obtém acesso a um recurso do AD;
- **Auditoria de Alteração de Diretivas**: ocorre quando as opções de segurança do usuário, direitos do usuário e diretivas de auditoria são alterados;
- **Auditoria de Controle de Processos**: ocorre quando algum aplicativo executa uma ação;
- **Auditoria de Eventos de Logon**: ocorre quando um usuário efetua logon e logoff em um computador local;
- **Auditoria de Eventos de Sistema**: ocorre quando o computador é desligado e reiniciado;
- **Auditoria de Gerenciamento de Contas**: ocorre quando o administrador cria, altera ou exclui uma conta ou grupo de usuário;
- **Auditoria de Uso de Privilégios**: ocorre quando um usuário utiliza um direito, por exemplo, alterar hora do sistema e apropriar-se de um arquivo;
- **Eventos de logon de conta de auditoria**: ocorre quando um usuário efetua logon em um domínio;

Ao configurar as auditorias, tenha em mente que quanto mais auditorias forem habilitadas, menor será o desempenho do computador. Portanto, habilite somente as auditorias que lhe fornecerá informações necessárias.

Ao habilitarmos uma auditoria, deveremos informar quais eventos serão auditados. Esses eventos podem ser: Sucesso ou Falha.

Para configurarmos a auditoria em um computador local, utilizamos o console Diretivas de Segurança Local. Somente membros do grupo Administradores podem habilitar a auditoria.



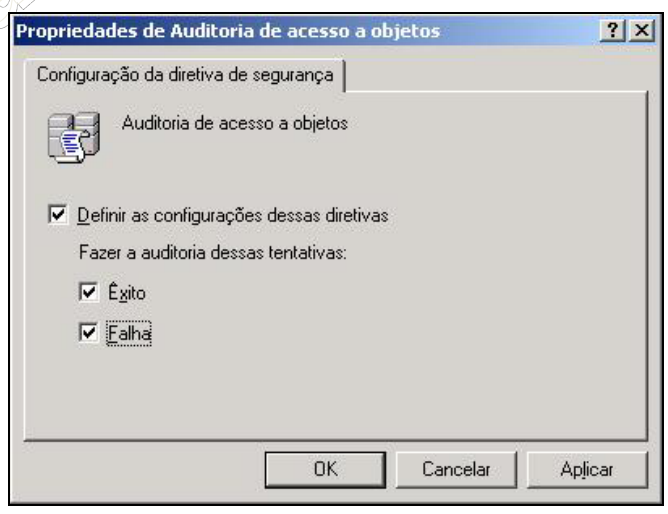
Quando formos configurar a auditoria “Acesso a Objetos”, devemos executar duas tarefas:

1. Habilitar a auditoria “Acesso a Objetos”;
2. Selecionar os objetos e os tipos de acesso que serão auditados;

Demonstraremos abaixo como habilitar as auditorias via GPO:

1. Efetue logon com uma conta de usuário com direitos administrativos;
2. Abra o console “Usuários e Computadores do AD”;
3. Clique com o botão direito sobre o domínio e escolha a opção Propriedades;
4. Clique na aba “Diretiva de Grupo”;
5. Dê 2 cliques sobre a GPO desejada ou selecione a GPO e clique em Editar;
6. Acesse a opção “Configuração do Computador”, “Configurações do Windows”, “Configurações de Segurança”, “Diretivas Locais”, “Diretiva de Auditoria”. Observe que aqui podemos configurar todas as diretivas de auditoria;

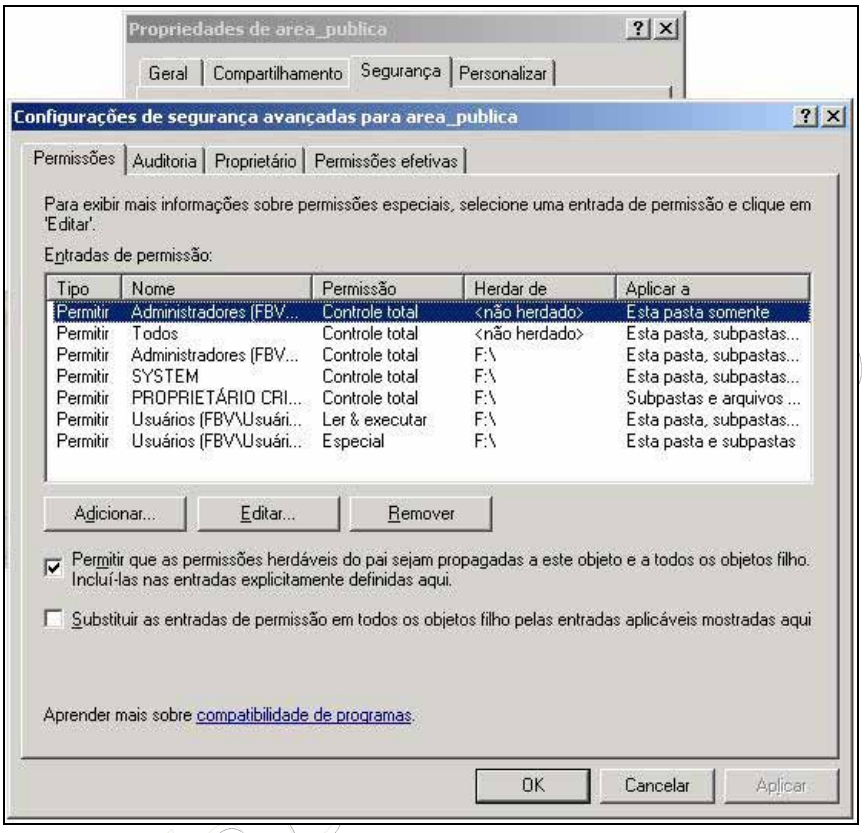
7. Clique 2 vezes sobre a auditoria que deseja habilitar e selecione as opções Sucesso ou Falha ou ambas as opções;



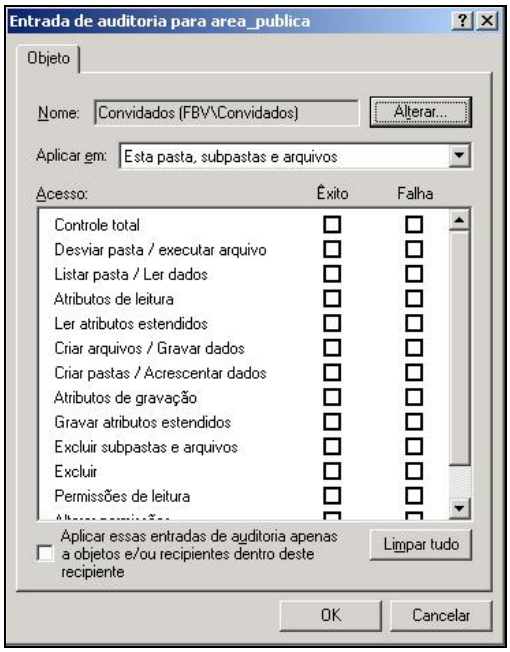
8. Clique em OK.

Agora vamos habilitar a auditoria para uma pasta do sistema, a isso chamamos de configurar a auditoria para acesso a objetos via GPO:

1. Habilite a auditoria “Acesso a Objetos”, seguindo os passos do exemplo anterior;
2. Agora abra o Windows Explorer e selecione uma pasta ou arquivo do qual deseja realizar a auditoria;
3. Clique com o botão direito sobre a pasta ou arquivo e escolha a opção Propriedades;
4. Clique na aba Segurança e clique em Avançado;

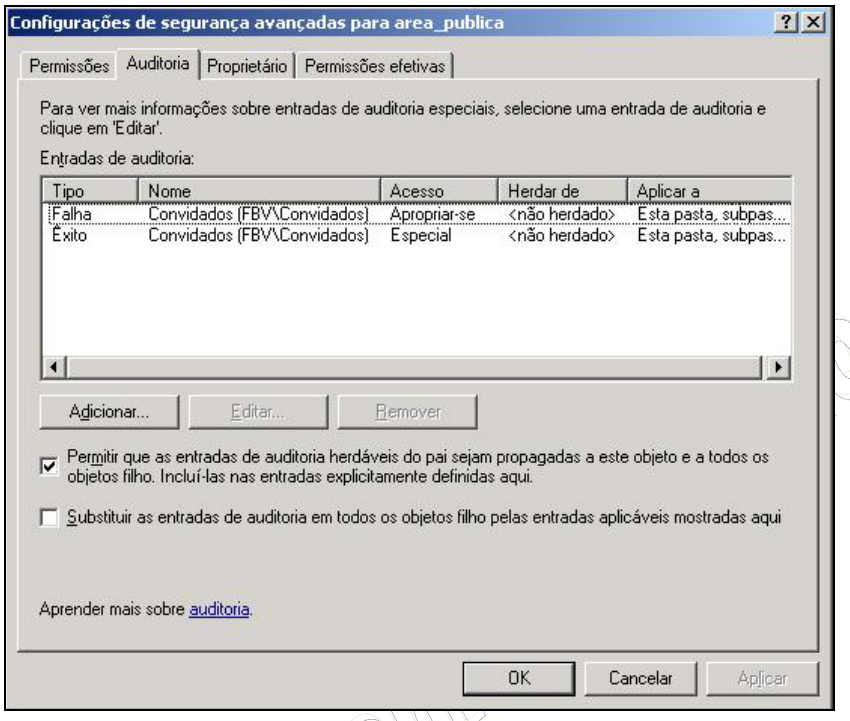


5. Clique na aba Auditoria e clique em Adicionar;
6. Selecione o grupo ou usuário que será auditado e clique em OK;
7. Será exibida uma janela para que você configure os eventos a serem auditados. Selecione os eventos desejados e clique em OK;



8. Para auditar mais usuários ou grupos, repita os procedimentos acima;
9. Clique em Aplicar e OK 2 vezes.

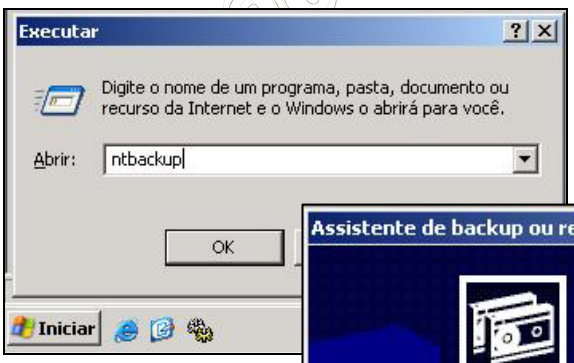
No final será exibido as entradas de auditorias definidas:

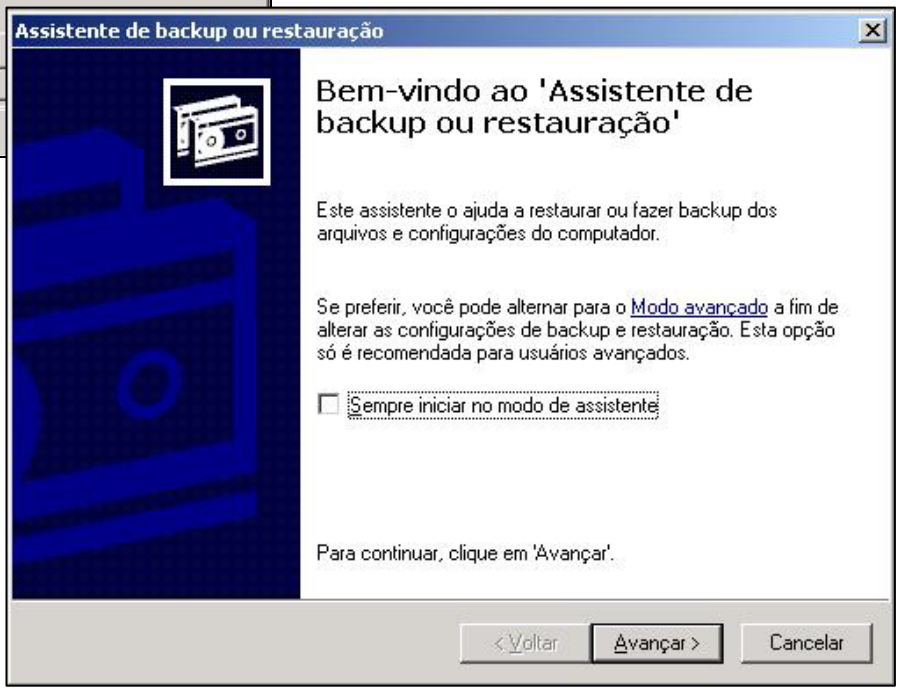


Agora que sabemos como auditar os logs, vamos aprender como realizar o backup dos dados e sistema.

8.3 FERRAMENTAS DE BACKUP

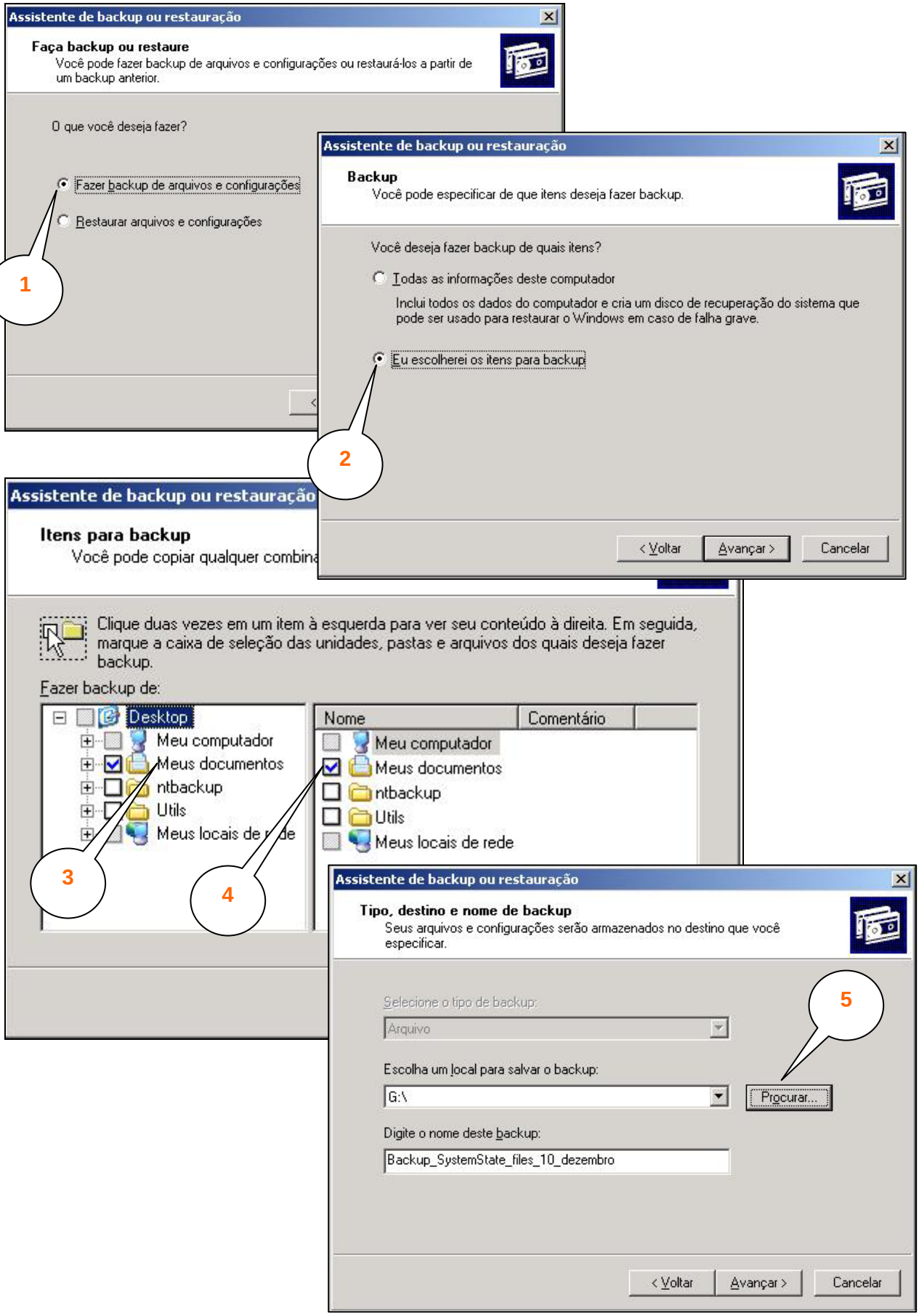
O serviço de rede mais importante de todos certamente é o backup. Sem ele não temos como garantir nenhuma manutenção ou continuidade do negócio. Veremos agora as diversas formas de realizar o backup tanto dos dados quanto do próprio sistema. A primeira atividade que devemos realizar é chamar o utilitário ntbackup:



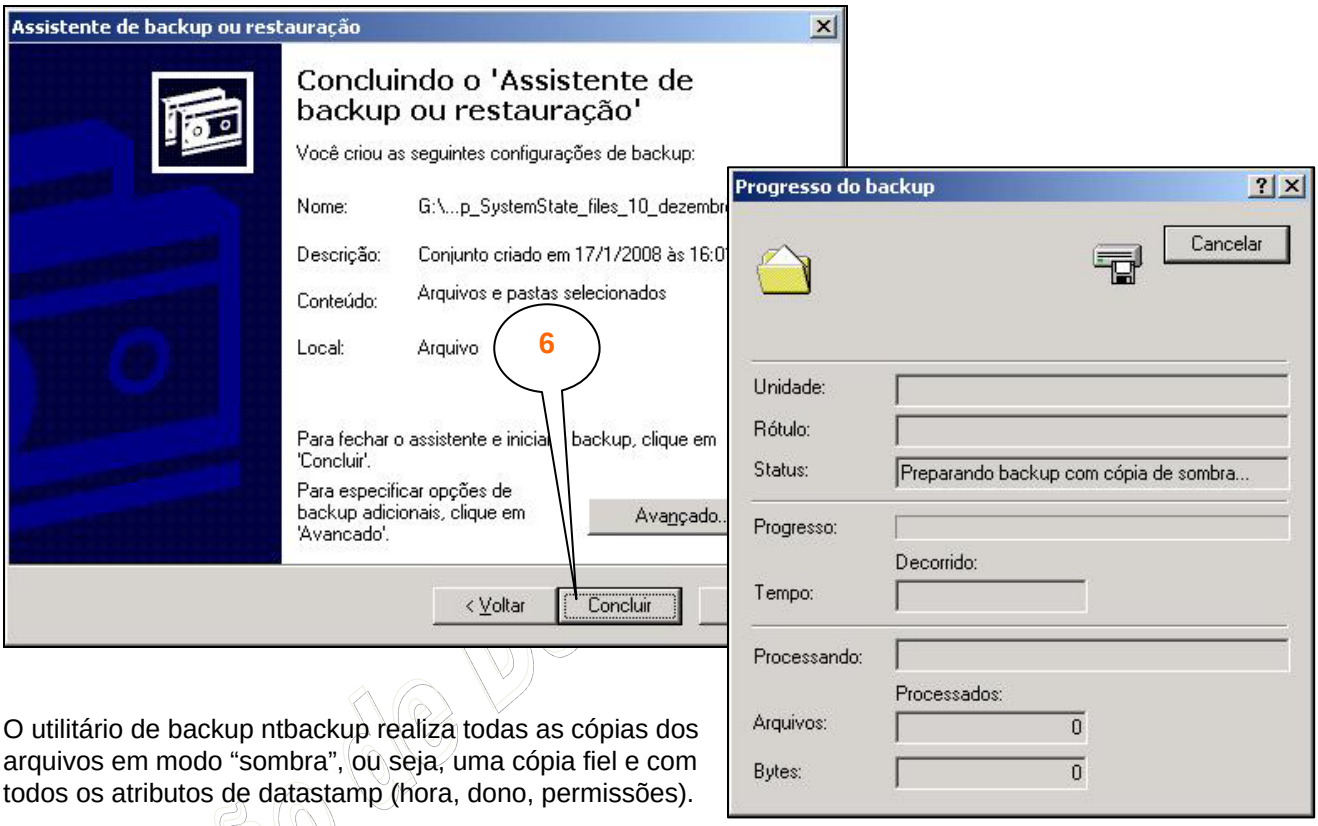


Quando executamos esse aplicativo pela primeira vez, ele apresenta um assistente de backup ou restauração de backups. Opcionalmente ao assistente existe uma interface avançada, ao qual falaremos mais adiante.

Vejamos como realizar o backup de arquivos do servidor de uma forma bem amigável:

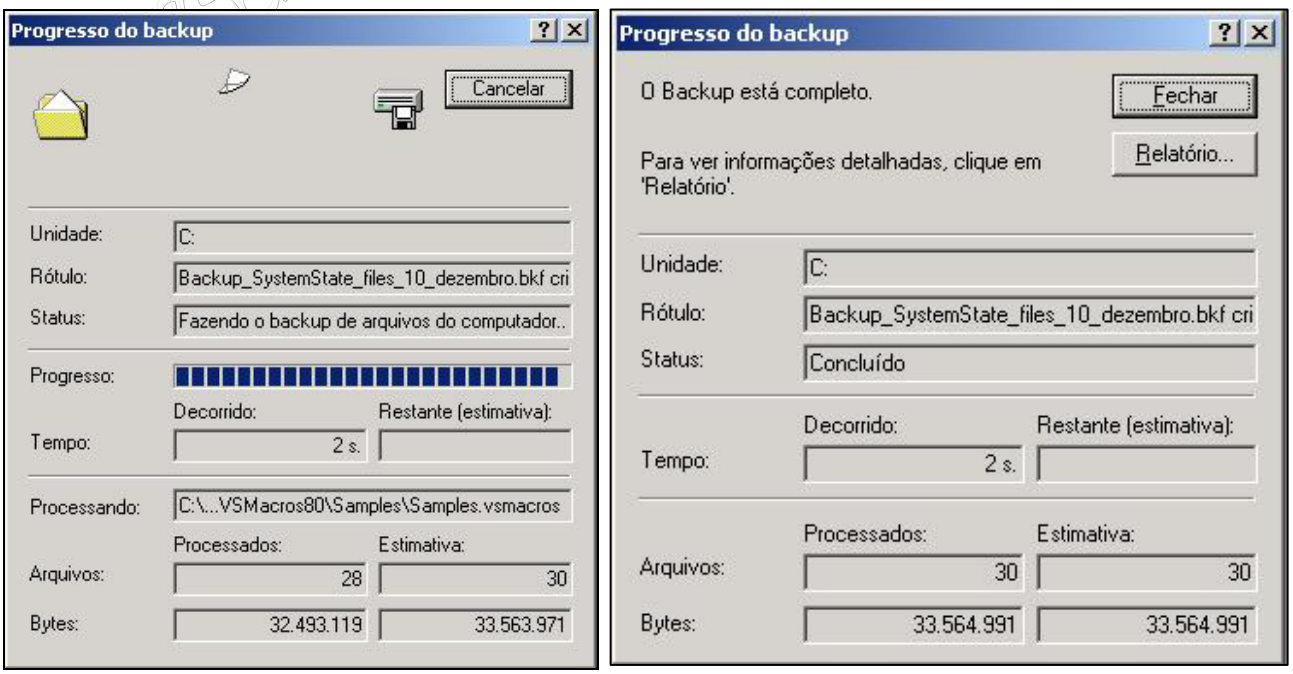


Uma vez concluídas as configurações para a realização do backup o assistente apresenta um breve resumo, caso seja necessário, ainda é possível alterar os dados dessa configuração, ou acrescentar novos itens, clicando no botão “Avançado”. Quando você terminar e concluir os passos de configuração o assistente executará as operações de backup:



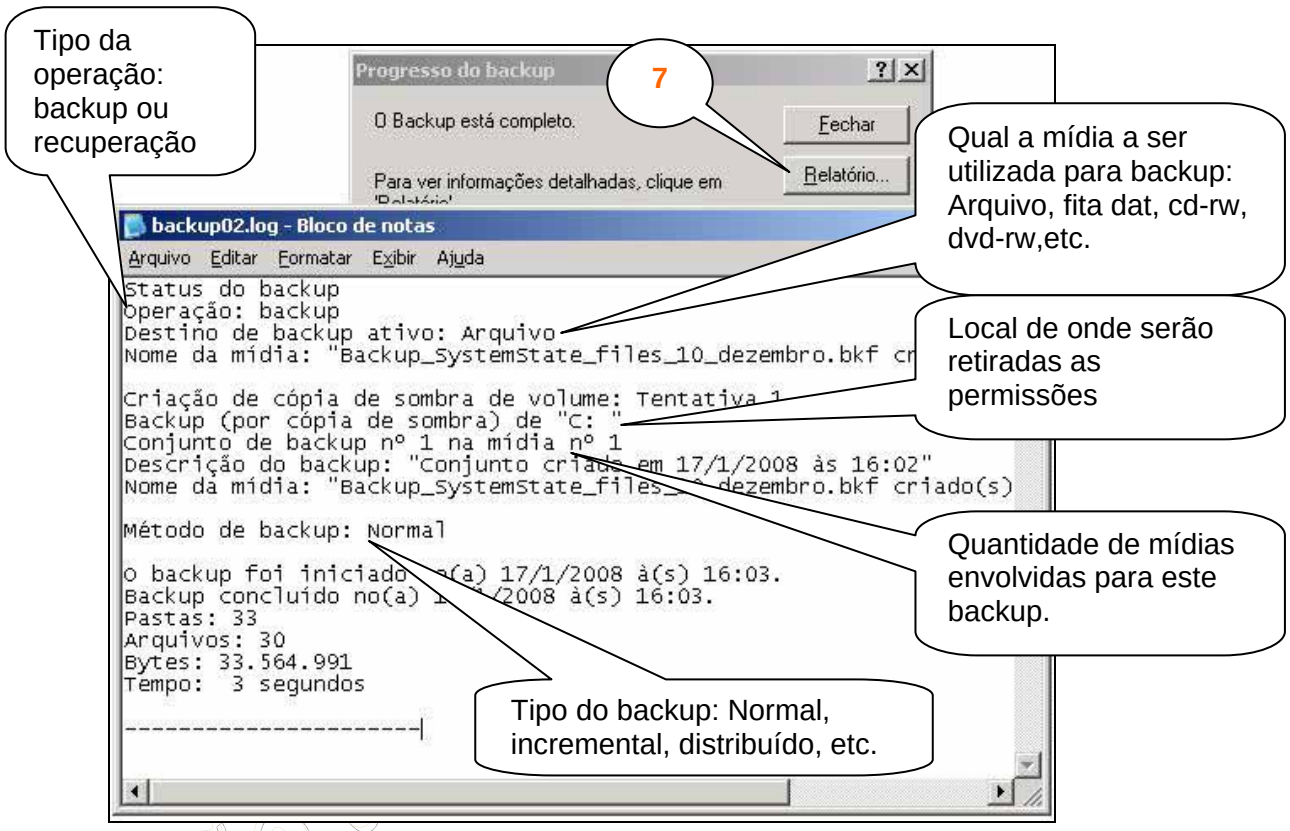
O utilitário de backup ntbackup realiza todas as cópias dos arquivos em modo “sombra”, ou seja, uma cópia fiel e com todos os atributos de datastamp (hora, dono, permissões).

O ntbackup exibirá uma tela com o progresso do backup, aqui você pode acompanhar todo o andamento: tempo decorrido, tempo restante, quantidade de arquivos copiados, entre outros:

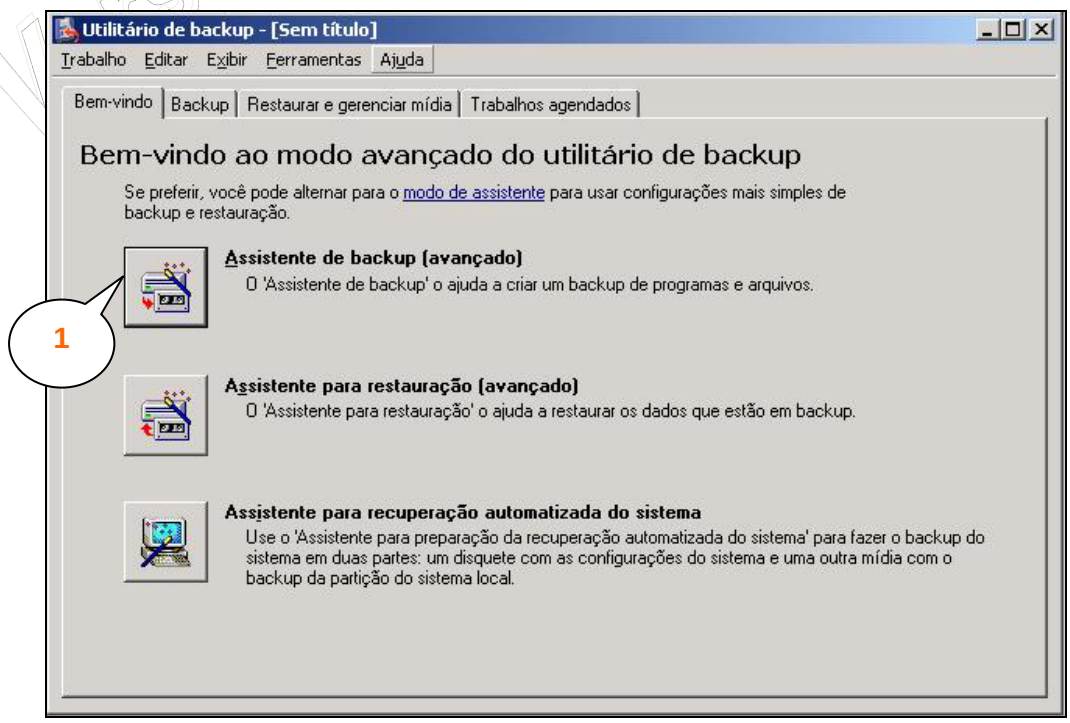


Este exemplo foi meramente ilustrativo, e utilizados apenas dois arquivos de texto para backup, em sistemas operando em tempo real é possível que o backup se prolongue por horas.

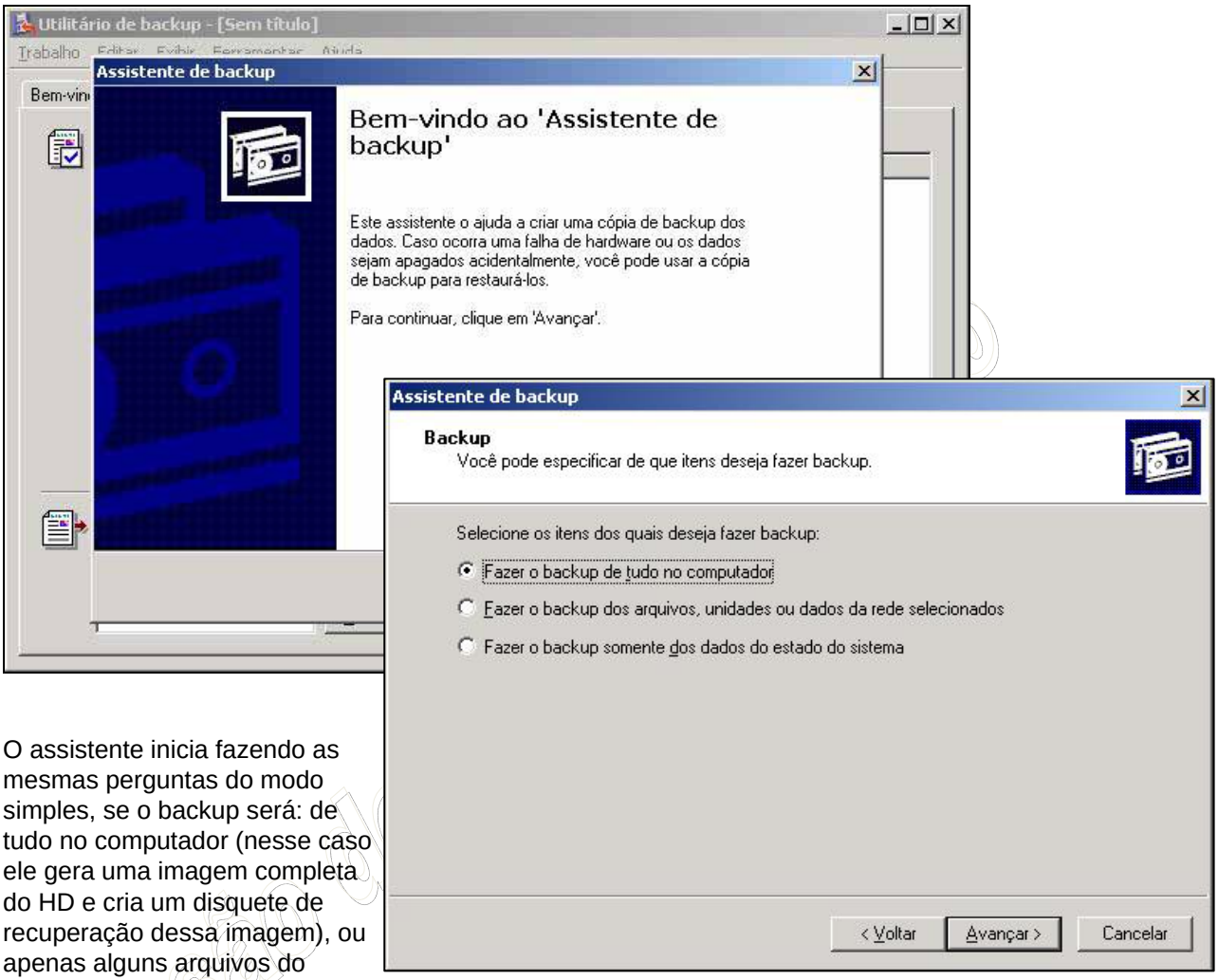
Ao concluir o backup será ofertado para exibir o relatório, uma boa prática é sempre imprimir este relatório e deixar junto com a mídia onde está residindo o backup. Isso ajuda na identificação do backup realizado. Vamos tentar entender o que está escrito nele:



Como vimos, a utilização do assiste simplifica muito a operação de backup, porém é bem mais provável que em seu servidor você precise de mais opções para o backup. Vamos demonstrar agora o uso da interface avança e aprender a operá-la:



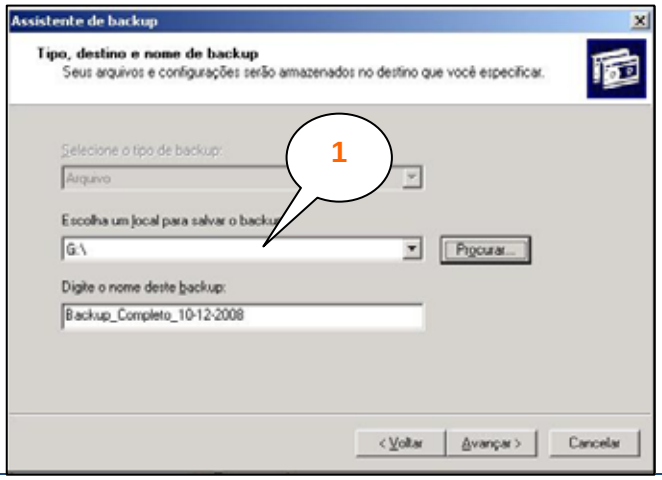
A interface avançada inicia um novo assistente, similar ao do modo simples, porém com mais opções de escolha:



O assistente inicia fazendo as mesmas perguntas do modo simples, se o backup será: de tudo no computador (nesse caso ele gera uma imagem completa do HD e cria um disquete de recuperação dessa imagem), ou apenas alguns arquivos do computador, e agora apresenta uma nova opção que é o de fazer o backup somente dos dados do estado do sistema.

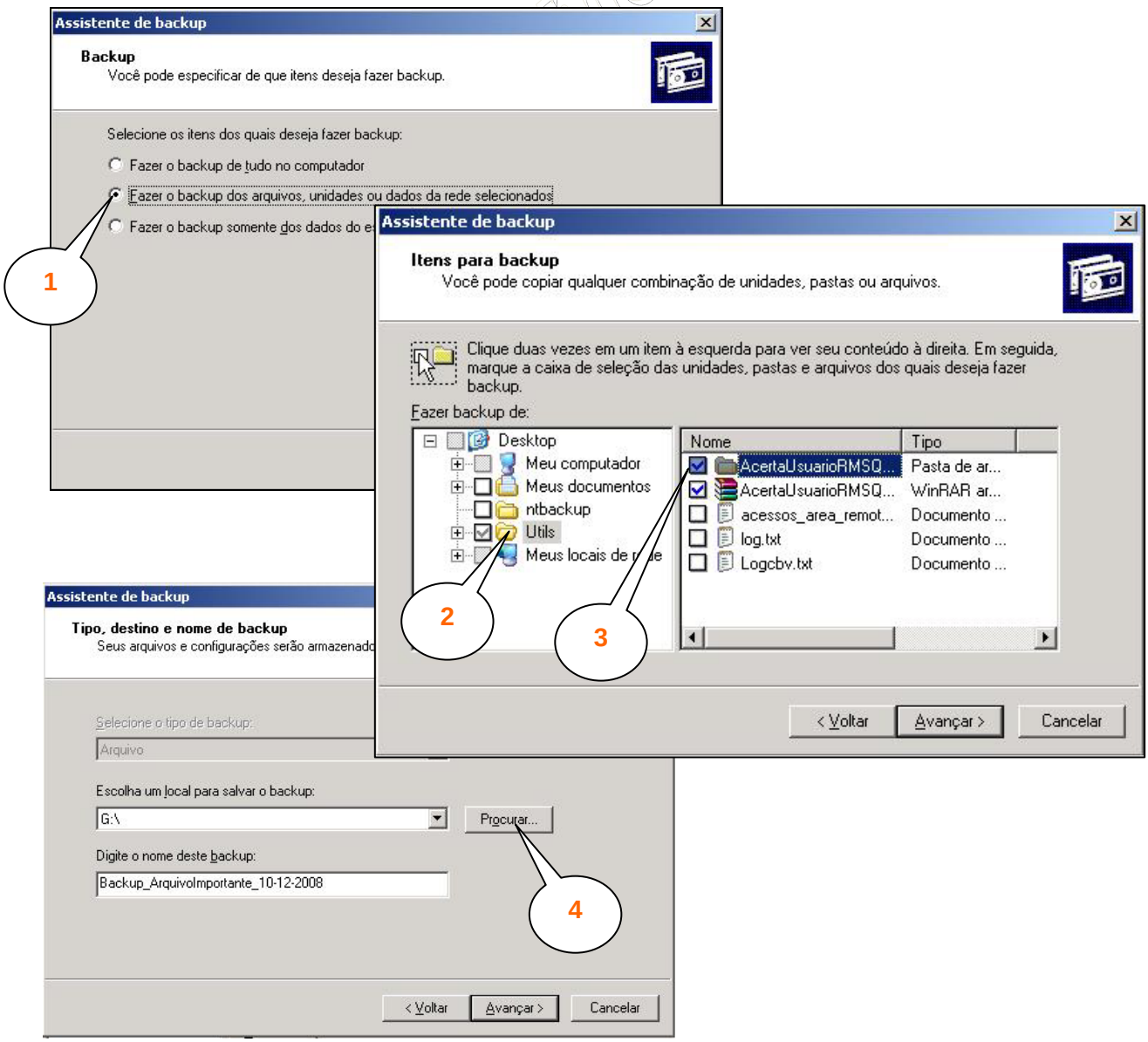
O Estado do Sistema são dados como: tabela de alocação dos arquivos (NTFS/MBR), permissões dos arquivos, principais arquivos de inicialização do Windows, principais drivers de dispositivos em uso, entre outros. Realizar uma cópia desses arquivos implica em dizer que, havendo uma necessidade de restaurar o último estado válido, onde tudo estava funcionando, então esses dados irão sobrescrever os arquivos defeituosos.

Na opção de Fazer o backup de tudo no computador, como já vimos, será feita uma imagem do volume para uma mídia, e gerado um diskete de recuperação do estado do sistema:



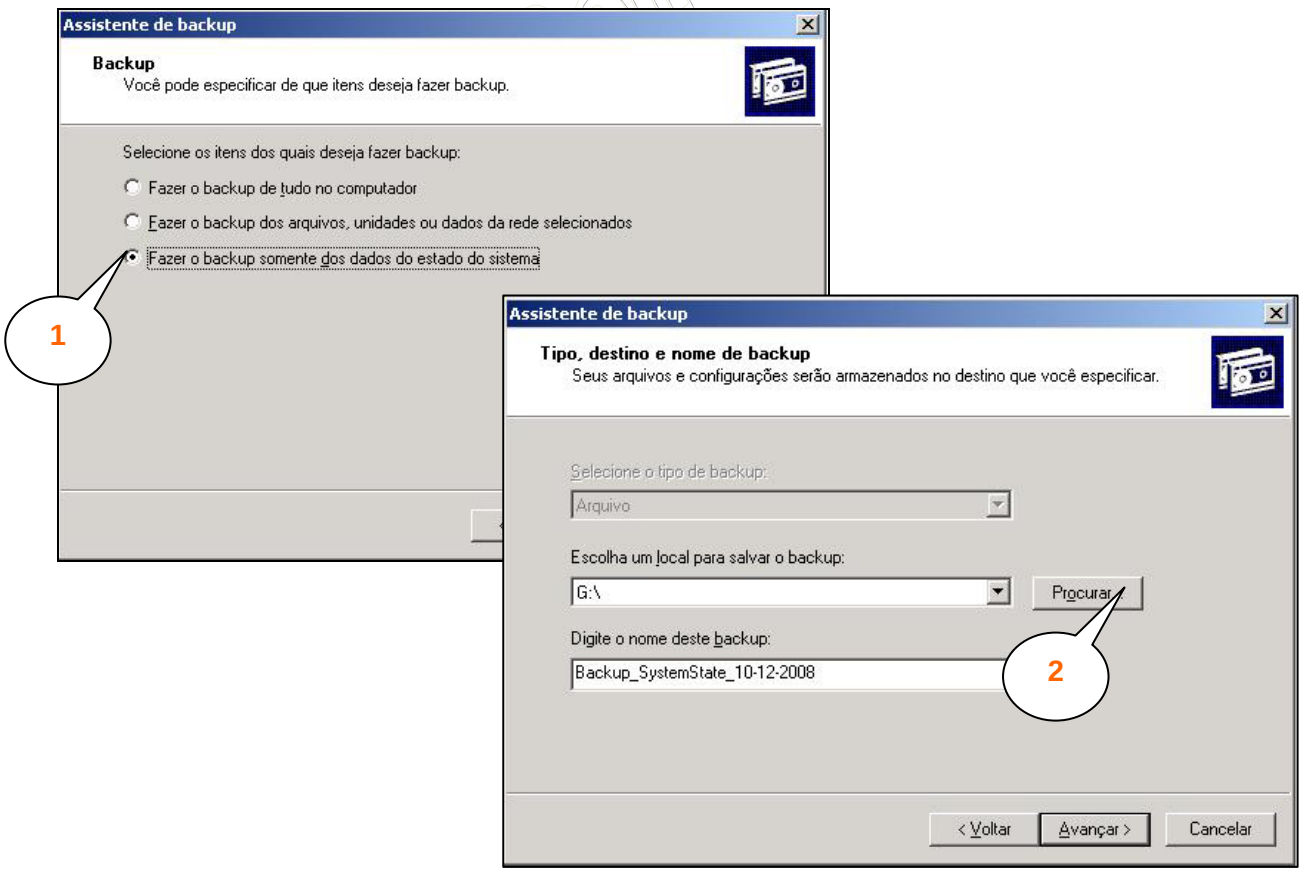
Sumário do assistente de backup para o modo completo:

Agora vejamos o backup dos arquivos, unidades ou dados da rede:

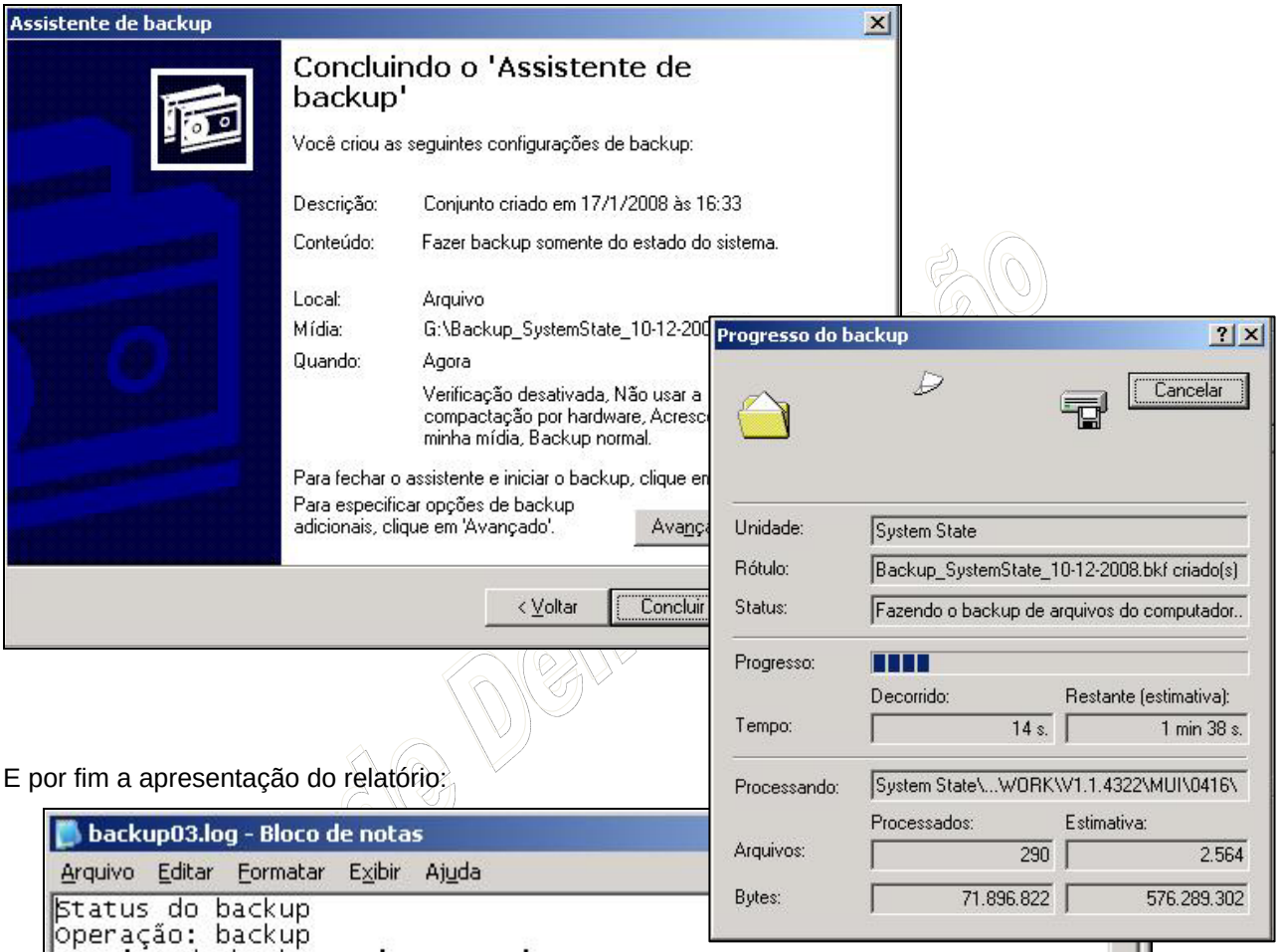


Sumário do assistente de backup de arquivos e pastas:

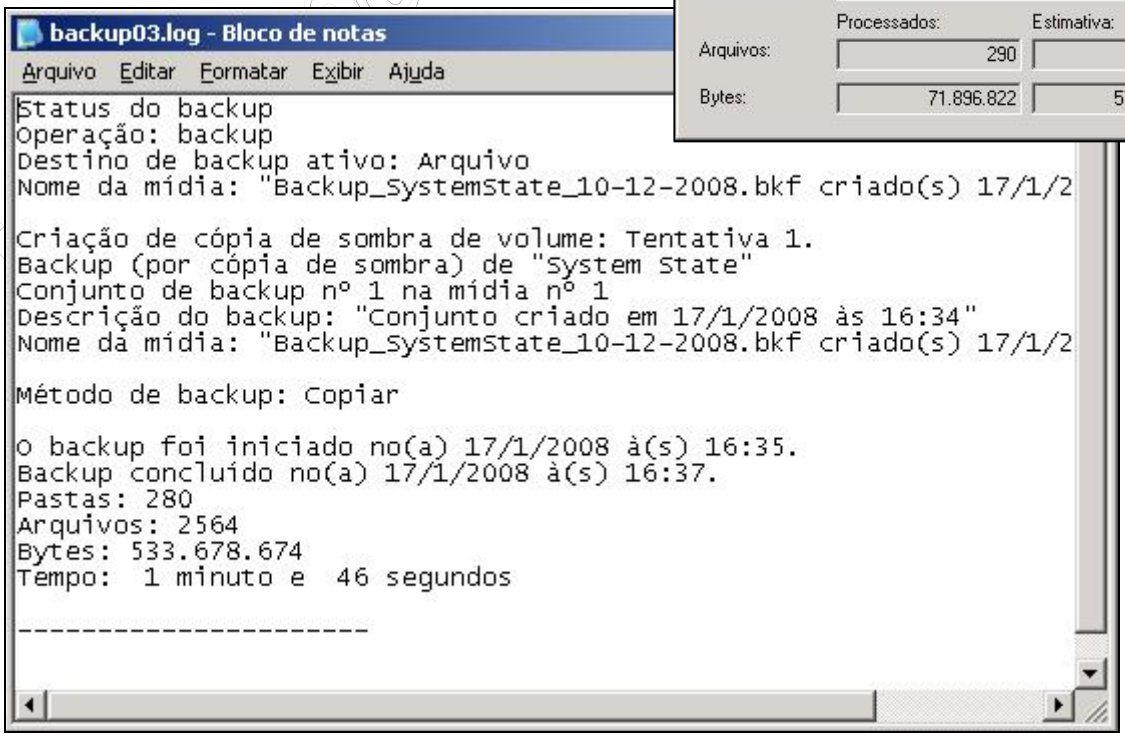
E finalmente o backup somente dos dados do estado do sistema:



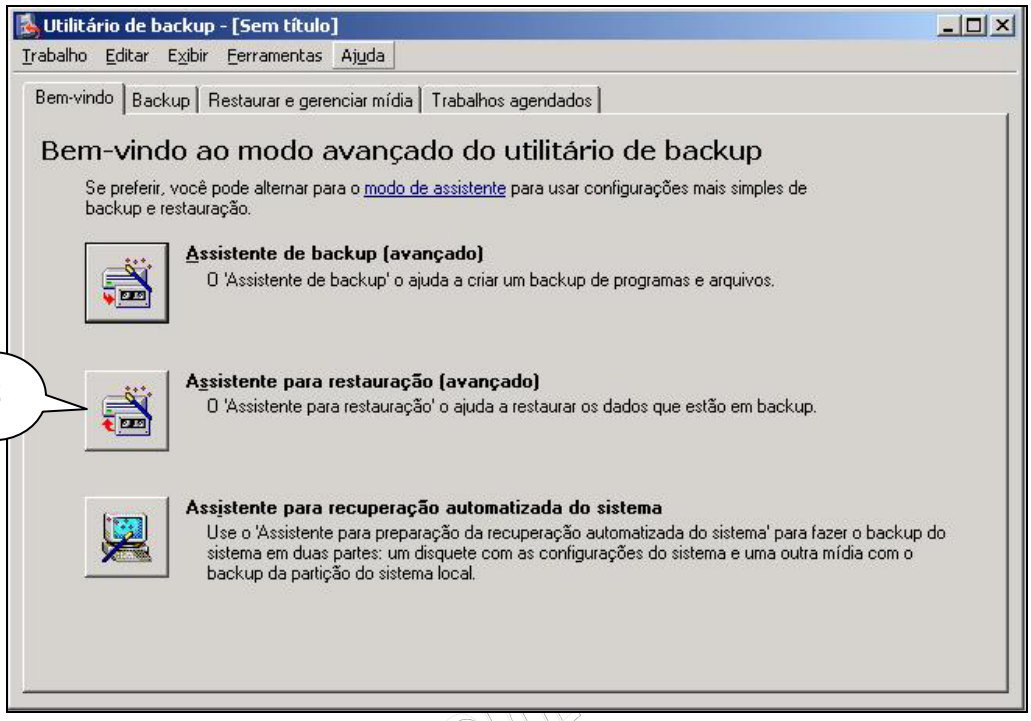
Sumário do backup do estado do sistema. Após a conclusão do ntbackup irá realizar o processo de backup:

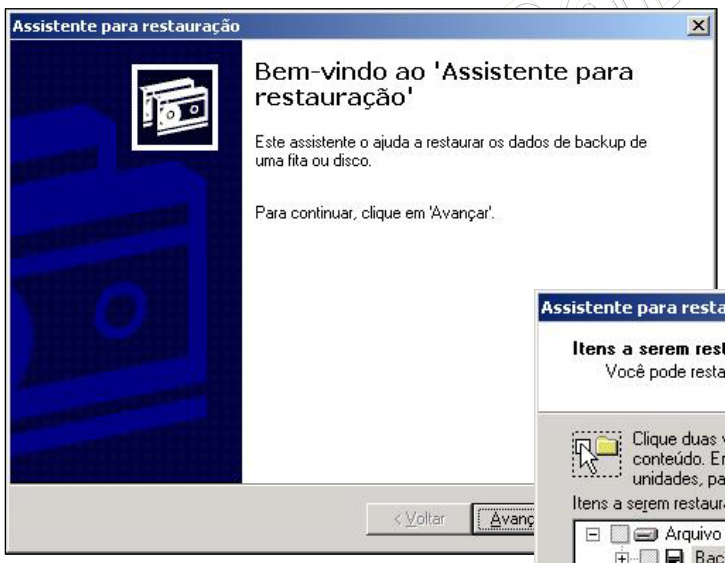


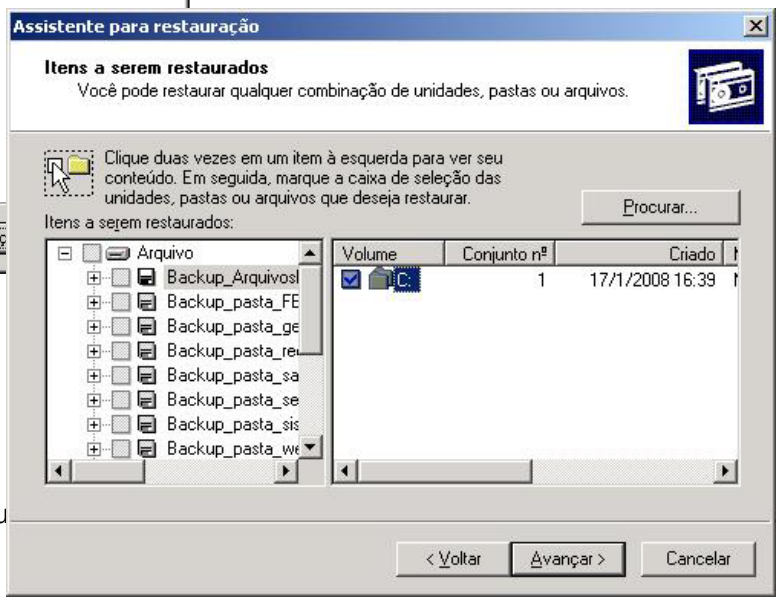
E por fim a apresentação do relatório:



Vejamos agora se processa a restauração de um backup. Muitos administradores acabam cometendo o erro da acomodação, ou seja, se habitam a realizar os backups fielmente, porém não realizam a validação desse backup. Validar significar tentar restaurar, para saber se todos os arquivos estão de fato sendo armazenados, se as permissões estão corretas, etc.

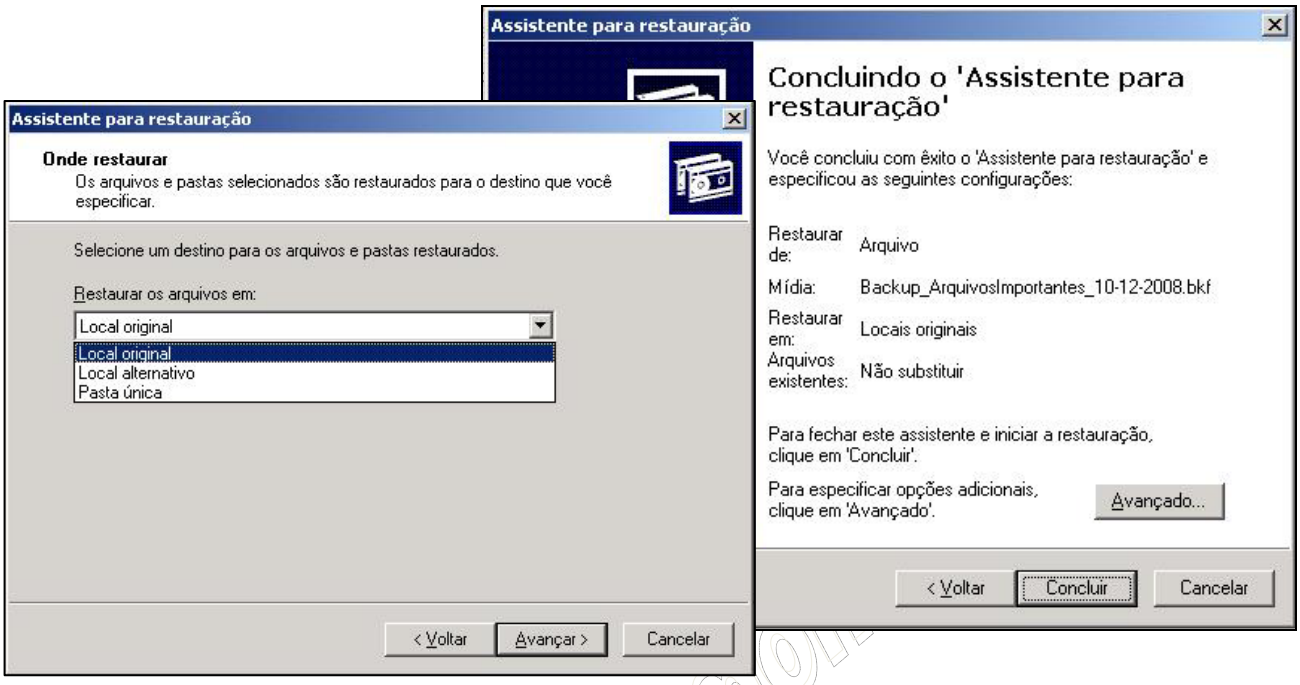






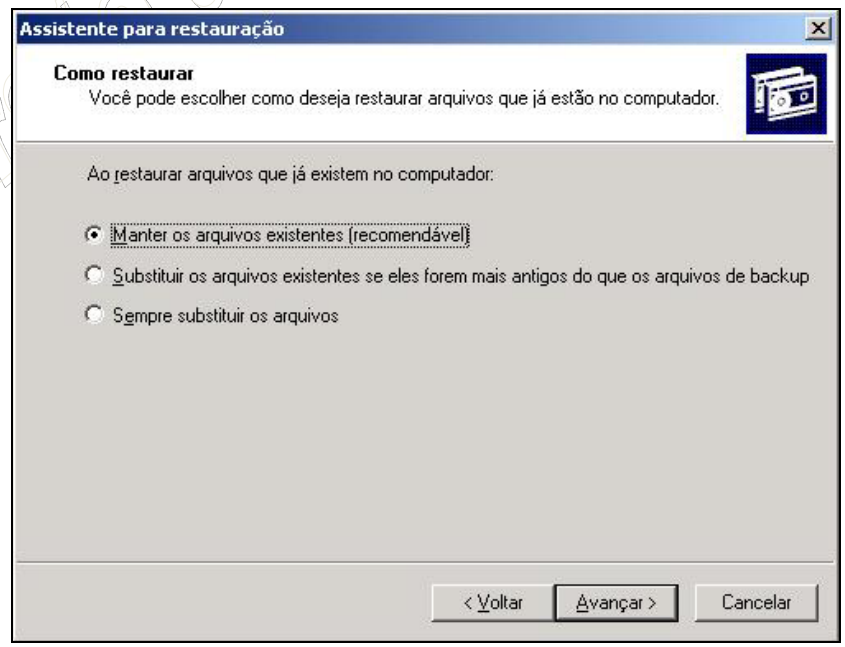
O assistente de restauração irá apresentar todos os backups realizados no servidor, incluindo os realizados em mídias removíveis, tipo um histórico. Sobre essa relação de backups feitos é possível escolher qual deles restaurar, ou selecionar um arquivo de backup realizado em outro computador.

Existem várias opções para efetuar a restauração de arquivos, pastas ou de todo o computador, através da tela de sumário é possível acessar as configurações avançadas da restauração de backups:

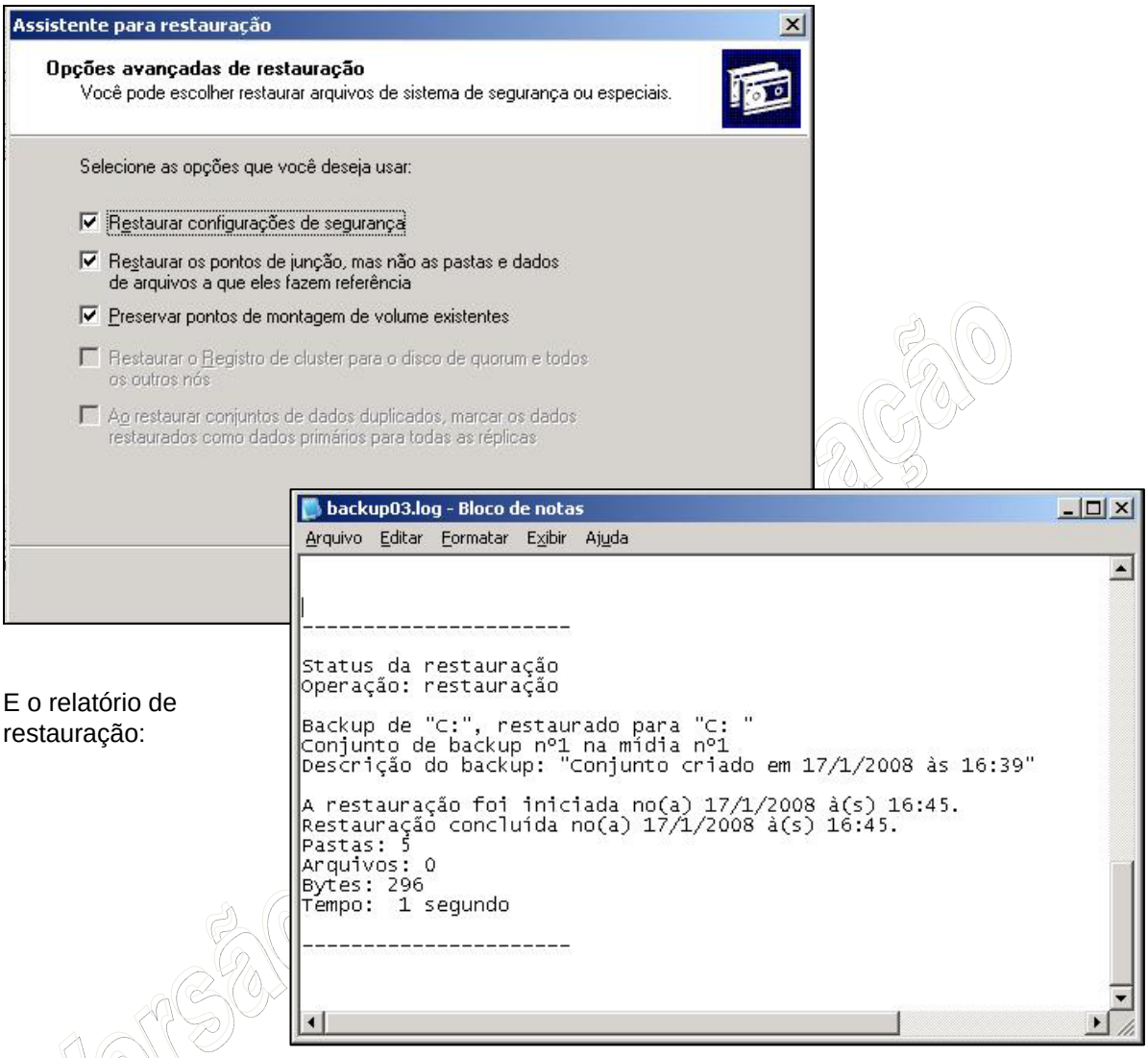


É possível escolher o local para onde serão restaurados os arquivos da mídia de backup, como: local original (segue o mesmo path, ou caminho, de quando foi realizado o backup e mantém toda sua estrutura de diretórios), local alternativo (é possível selecionar uma nova unidade ou pasta para onde toda a estrutura de arquivos e diretórios serão recriados), e pasta única (todos os arquivos da mídia são extraídos para uma única pasta, não havendo ou perdendo a estrutura de diretórios).

É possível também escolher entre substituir ou não arquivos existentes pelos que estão sendo restaurados:

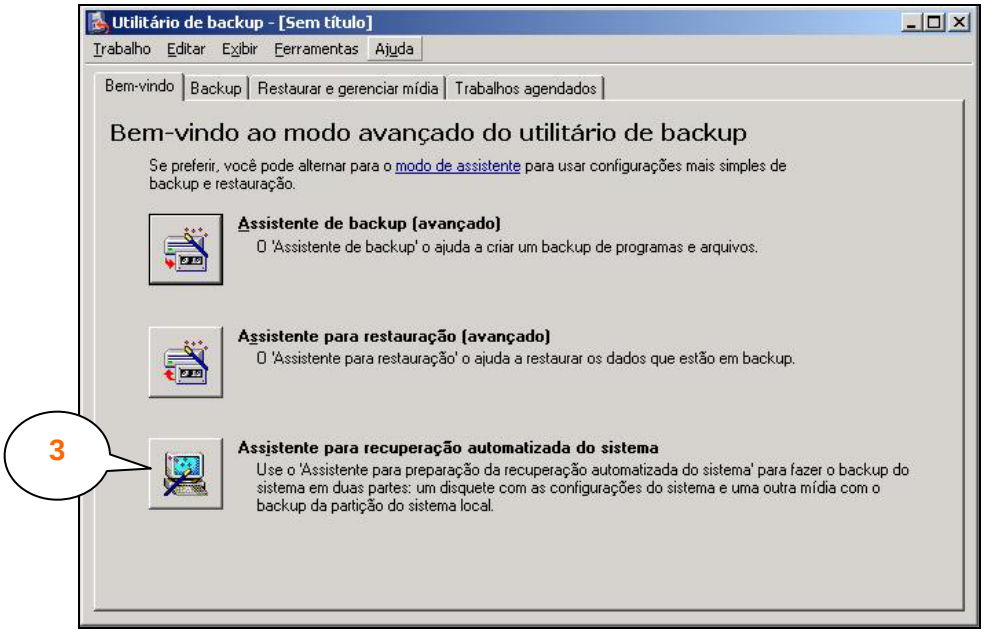


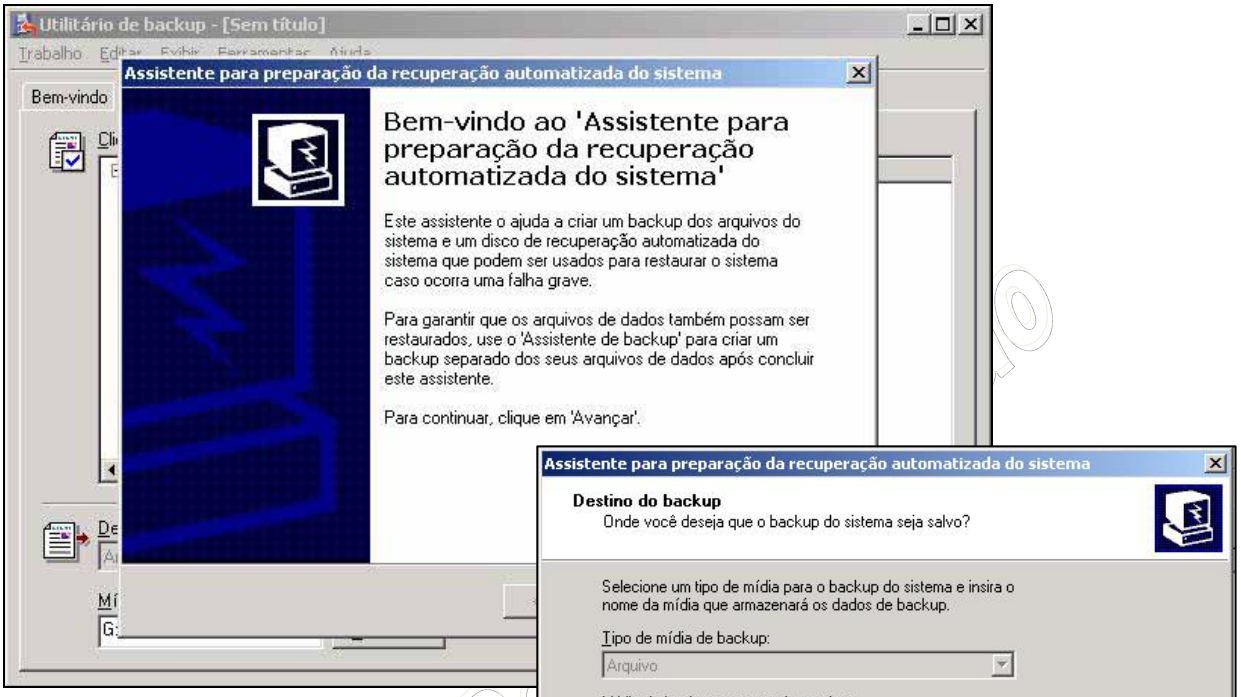
Entre as opções avançadas de restauração estão os arquivos de sistema de segurança:



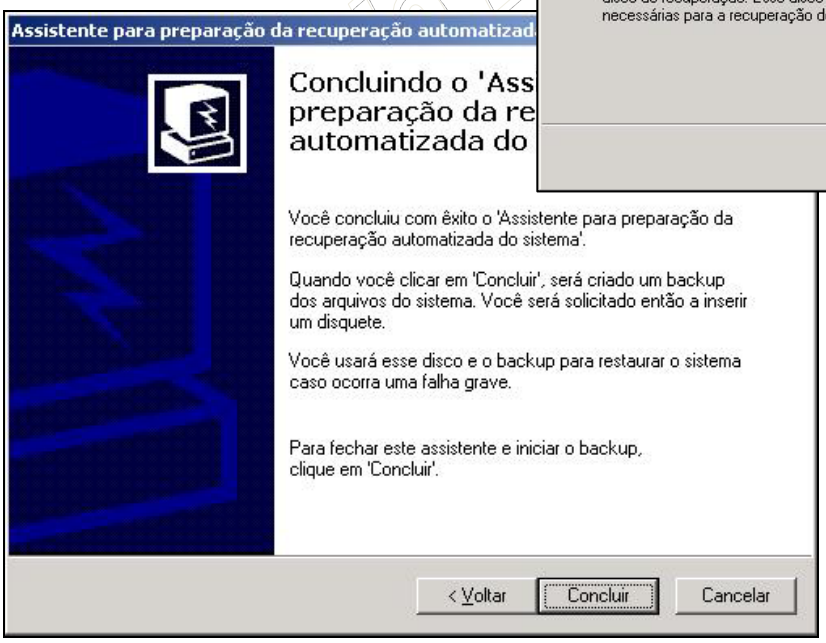
E o relatório de restauração:

E a última opção do assistente em modo avançado: recuperação automatizada do sistema. Aqui todos os dados, inclusive o estado do sistema, é salvo e gera-se um disquete com as configurações do sistema:



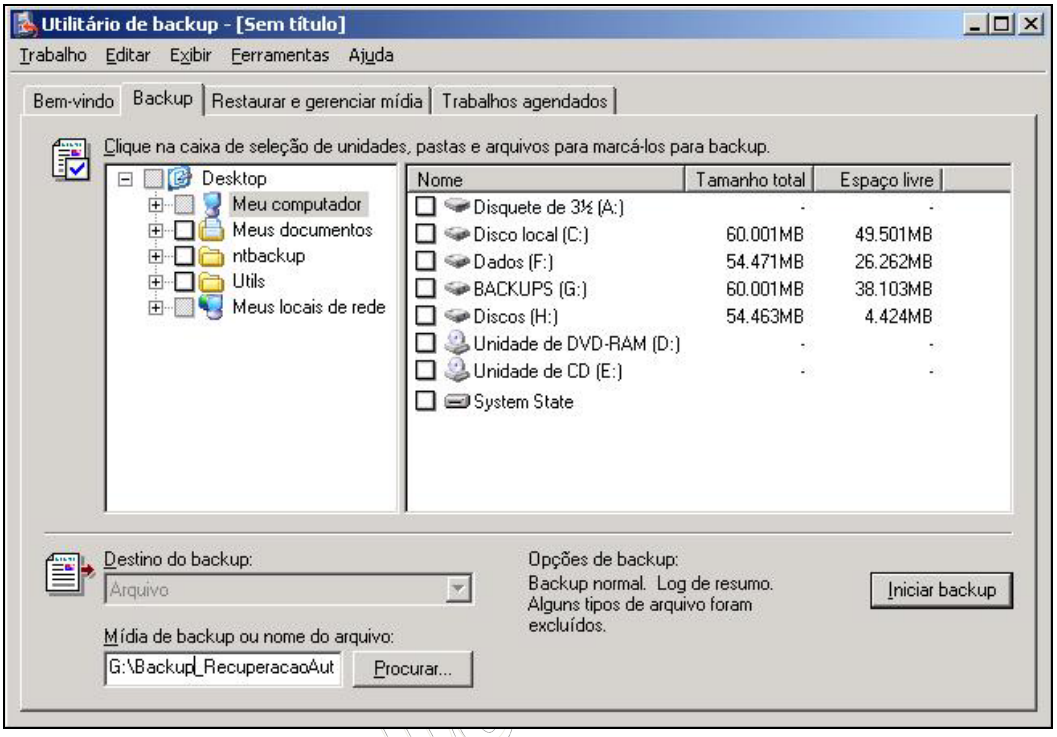


Outro assistente muito simples:

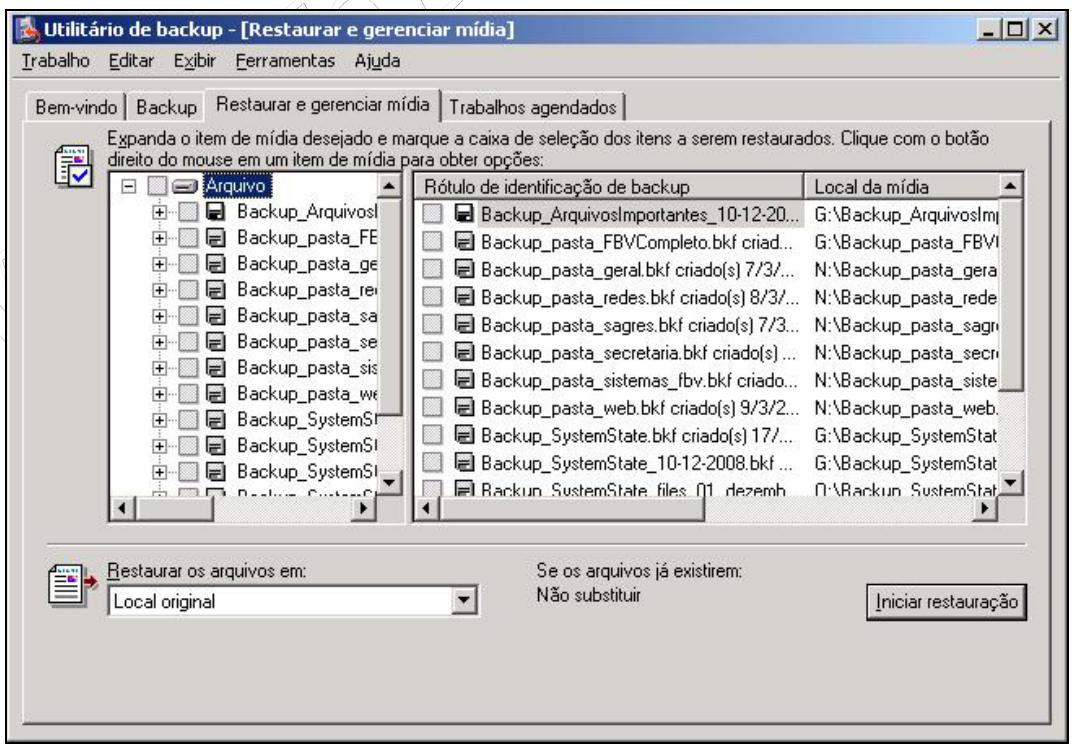


Outra alternativa para a realização de backups e restaurações é sem a ajuda dos assistentes. Neste caso você deverá acessar diretamente os menus de configuração do ntbackup e realizar suas próprias operações, vejamos as telas da interface:

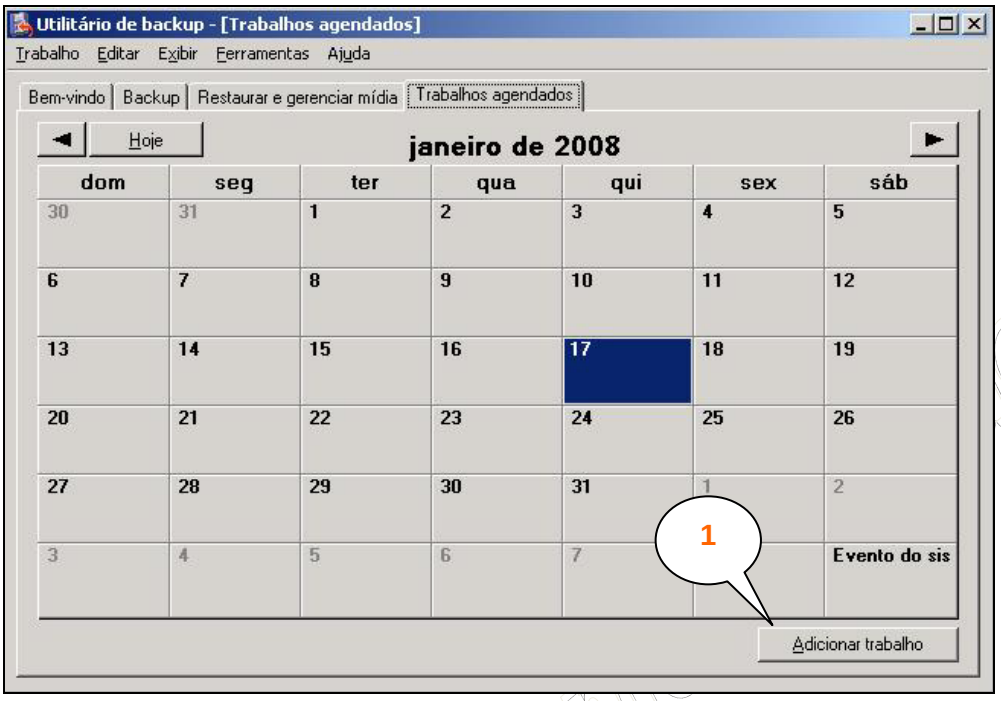
Interface para realização de backups:



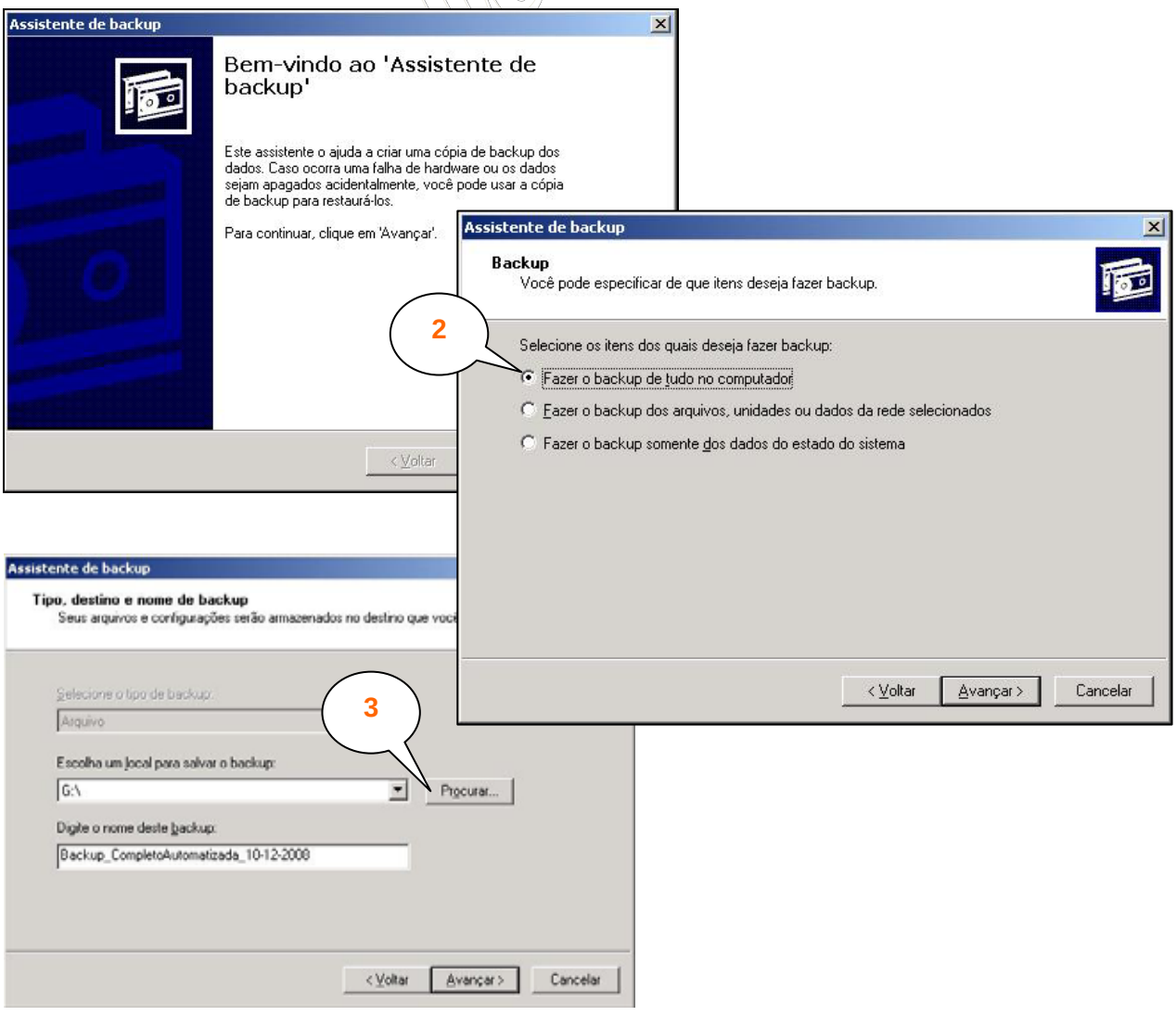
Interface para restauração de backups:



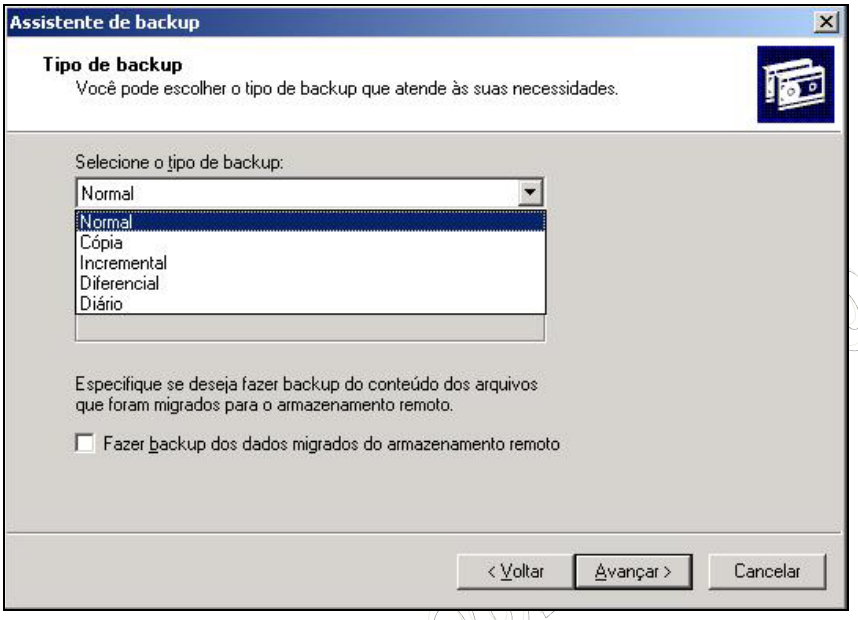
E a última parte consiste no agendamento ou automatização dos backups. É possível, através da interface de Trabalhos Agendados, programar uma rotina de backup completa, veja as opções:



O assistente é novamente chamado, com as mesmas opções anteriores, porém desta vez serão questionados os dados sobre o agendamento:

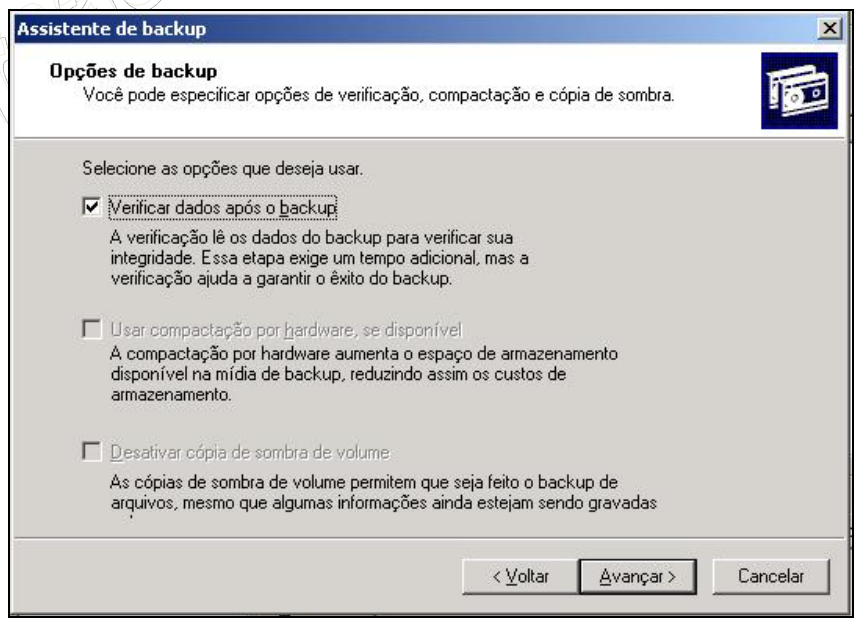


As perguntas sobre o tipo de backup são mais direcionadas, para não haver erros, veja:

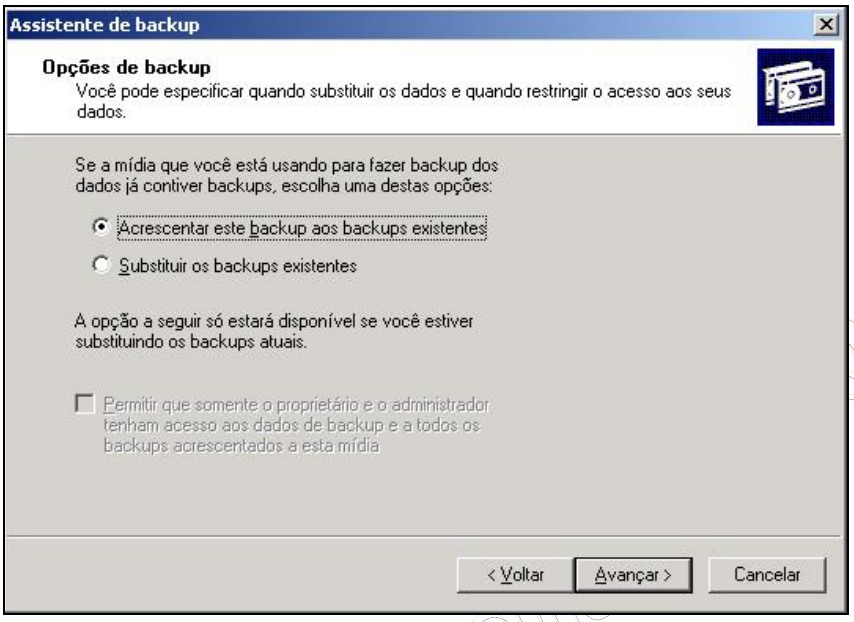


Os tipos são: Normal (realiza o backup dos arquivos e pastas como se fosse a primeira vez, não faz o sombreamento das permissões), Cópia (backup semelhante ao normal, porém a cópia realizada é de sombra), Incremental (verifica os arquivos que já estão dentro de um pacote de backup existente e adiciona somente novos arquivos que foram modificados desde a data do último backup), Diferencial (verifica os arquivos que já estão dentro de um pacote de backup existente e sobrescreve aqueles que foram modificados deste a última data do backup), Diário (realiza um novo backup por dia).

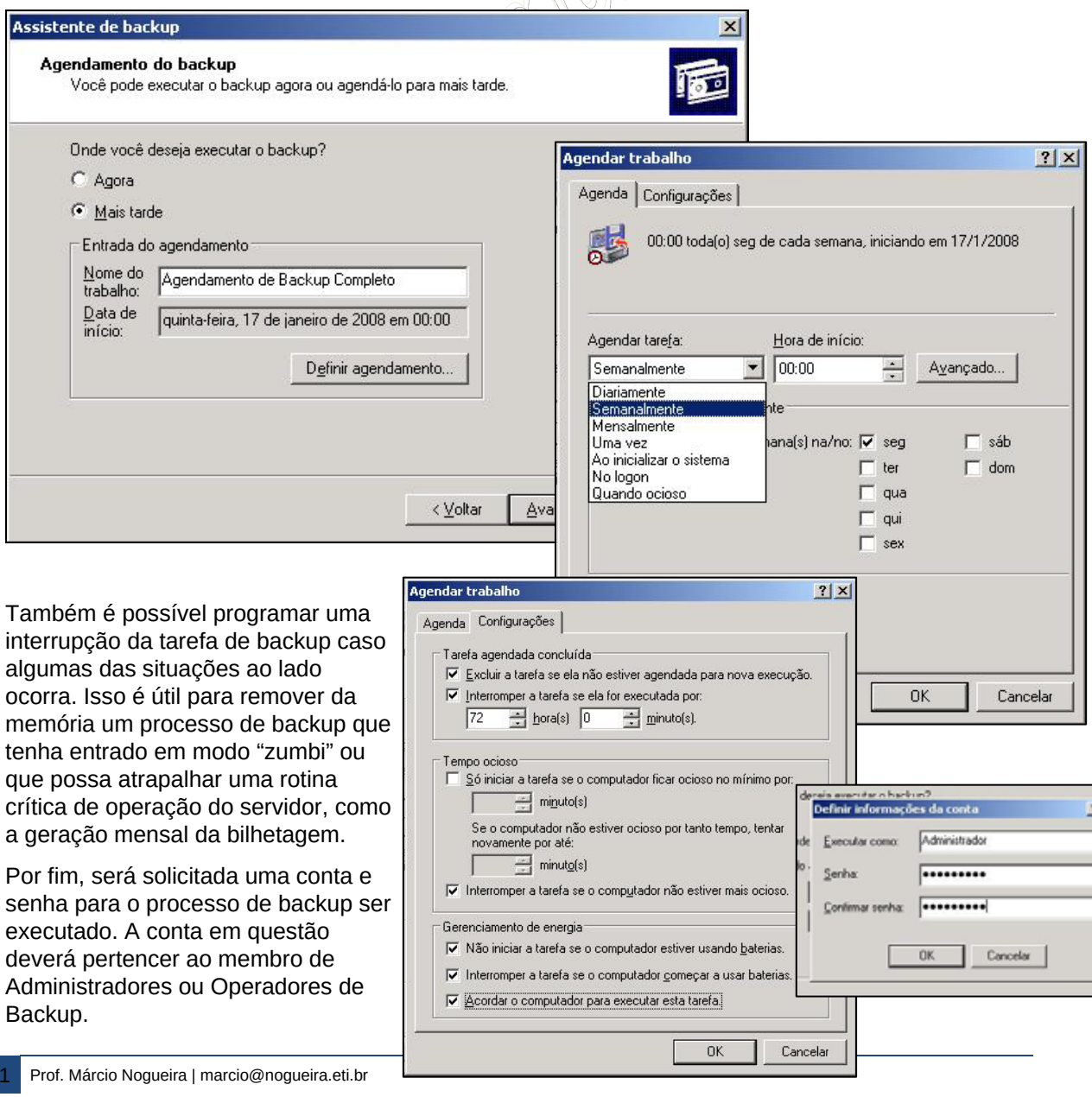
Um dos recursos avançados do ntbackup é zelar pela integridade do arquivo ".bkp" gerado:



Ao criar uma nova tarefa de backup agendado você poderá sobrescrever outros arquivos de backups que já tenham sido criados com o mesmo nome, e limitar o acesso a estes arquivos a apenas o Administrador e proprietário do backup:



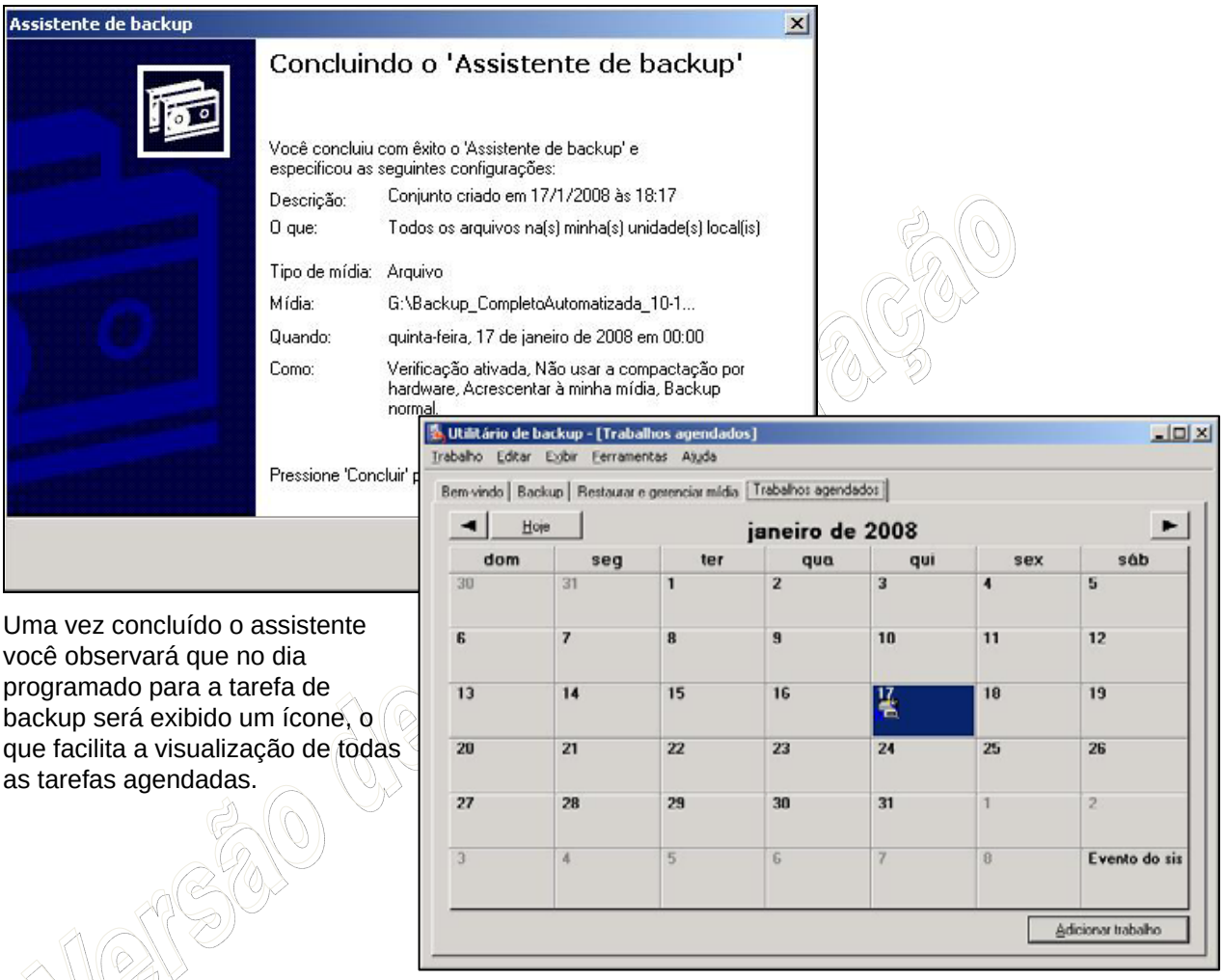
E finalmente as configurações de agendamento:



Também é possível programar uma interrupção da tarefa de backup caso algumas das situações ao lado ocorra. Isso é útil para remover da memória um processo de backup que tenha entrado em modo “zumbi” ou que possa atrapalhar uma rotina crítica de operação do servidor, como a geração mensal da bilhetagem.

Por fim, será solicitada uma conta e senha para o processo de backup ser executado. A conta em questão deverá pertencer ao membro de Administradores ou Operadores de Backup.

É muito comum, após o agendamento da tarefa de backup, observar que a mesma não foi realizada na data prevista. Na grande maioria das vezes esse erro é proporcionado em função da digitação errada da conta ou senha.



Uma vez concluído o assistente você observará que no dia programado para a tarefa de backup será exibido um ícone, o que facilita a visualização de todas as tarefas agendadas.

Nossa próxima lição será o estudo dos serviços avançados de redes.

8.4 SERVIÇOS AVANÇADOS DE REDE

Os serviços avançados são aqueles que alimentam negócios, que são indispensáveis e críticos para uma organização. Algumas organizações só existem em função deles. São eles:

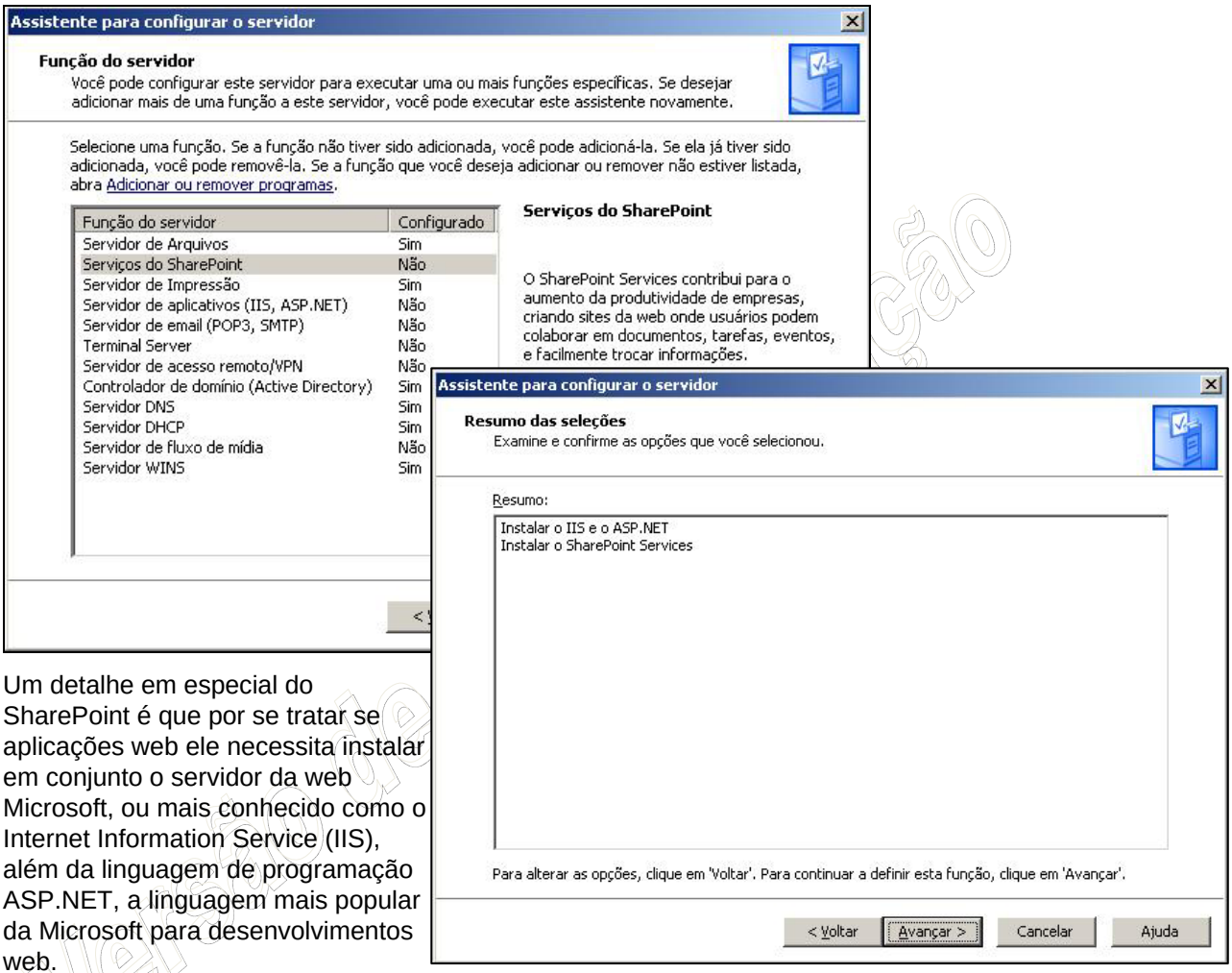
- Serviços do SharePoint
- Servidor de Aplicativos (IIS,ASP.NET)
- Servidor de E-mail (POP3, SMTP)
- Terminal Server
- Servidor de Acesso Remoto/VPN
- Servidor de fluxo de mídia

Veremos agora as principais configurações de cada, de forma a criar um negócio para a empresa:

Sérvios de SharePoint

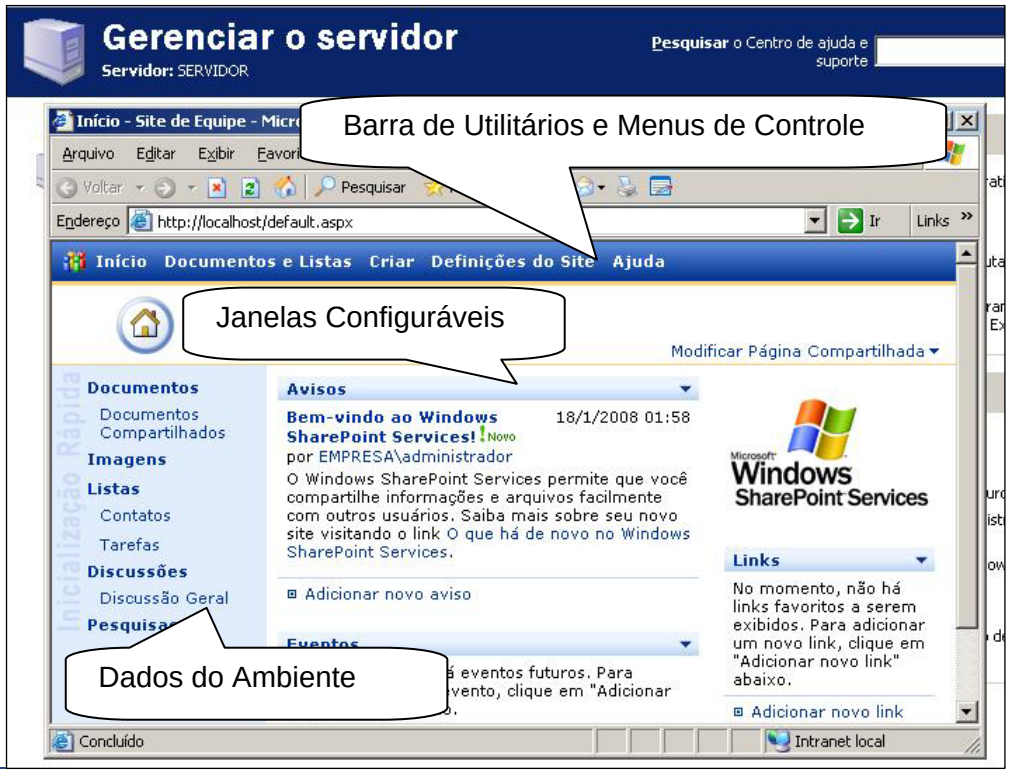
O SharePoint contribui para o aumento da produtividade de empresas, criando sites da web (intranet/extranet) onde usuários podem colaborar em documentos, tarefas, eventos e facilmente trocar informações.

O SharePoint são aplicações voltadas para a Web onde usuários de uma mesma rede, ou extranet, podem realizar a edição simultânea de documentos, mantendo o devido histórico de versões e controle, por exemplo. Vejamos sua instalação:

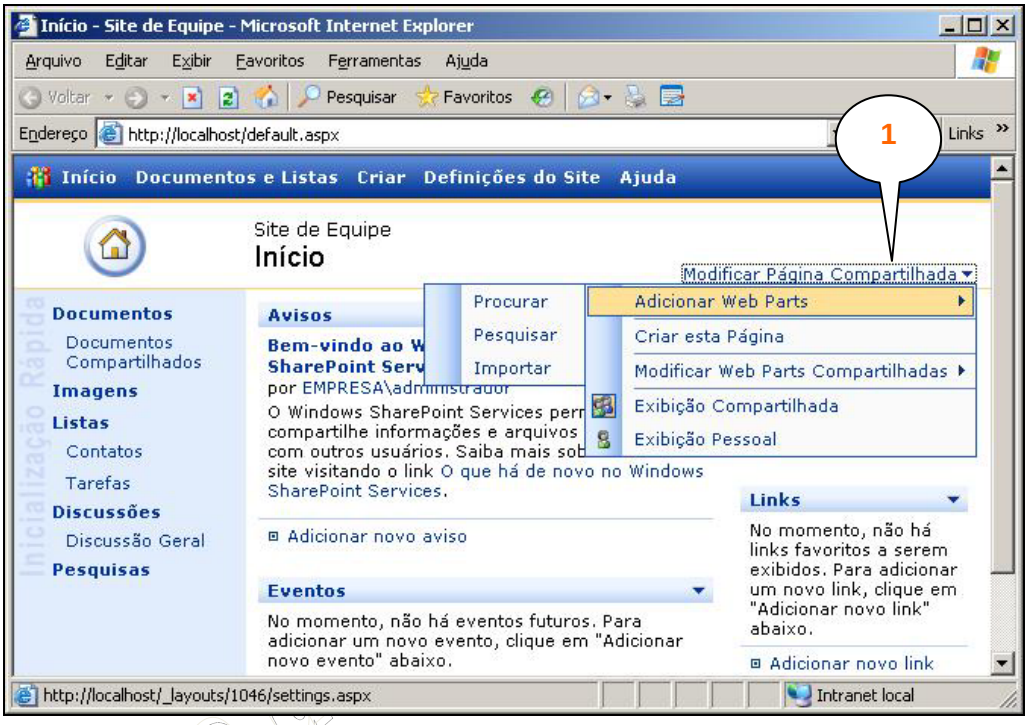


Um detalhe em especial do SharePoint é que por se tratar se aplicações web ele necessita instalar em conjunto o servidor da web Microsoft, ou mais conhecido como o Internet Information Service (IIS), além da linguagem de programação ASP.NET, a linguagem mais popular da Microsoft para desenvolvimentos web.

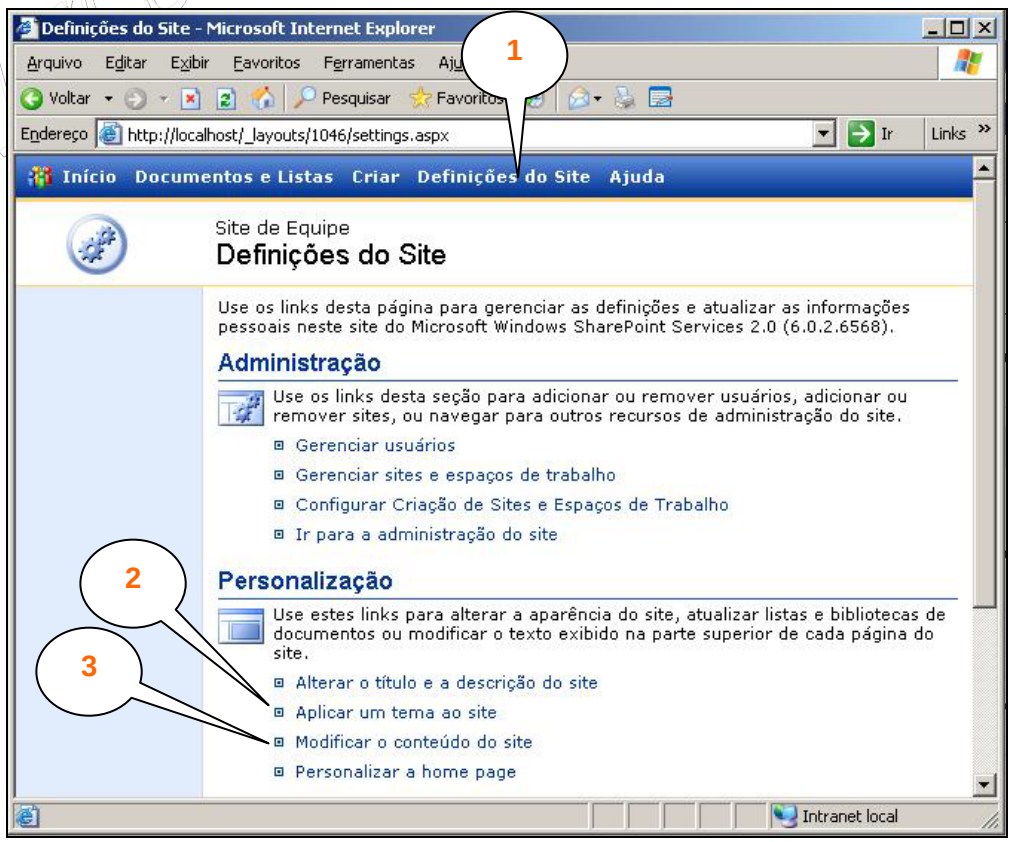
Após instalar o SharePoint você poderá gerenciá-lo através da interface de “Gerenciar o servidor”, semelhante aos demais serviços visto até agora. Porém, a interface de administração do SharePoint, como o próprio conceito do sistema, será uma interface web:

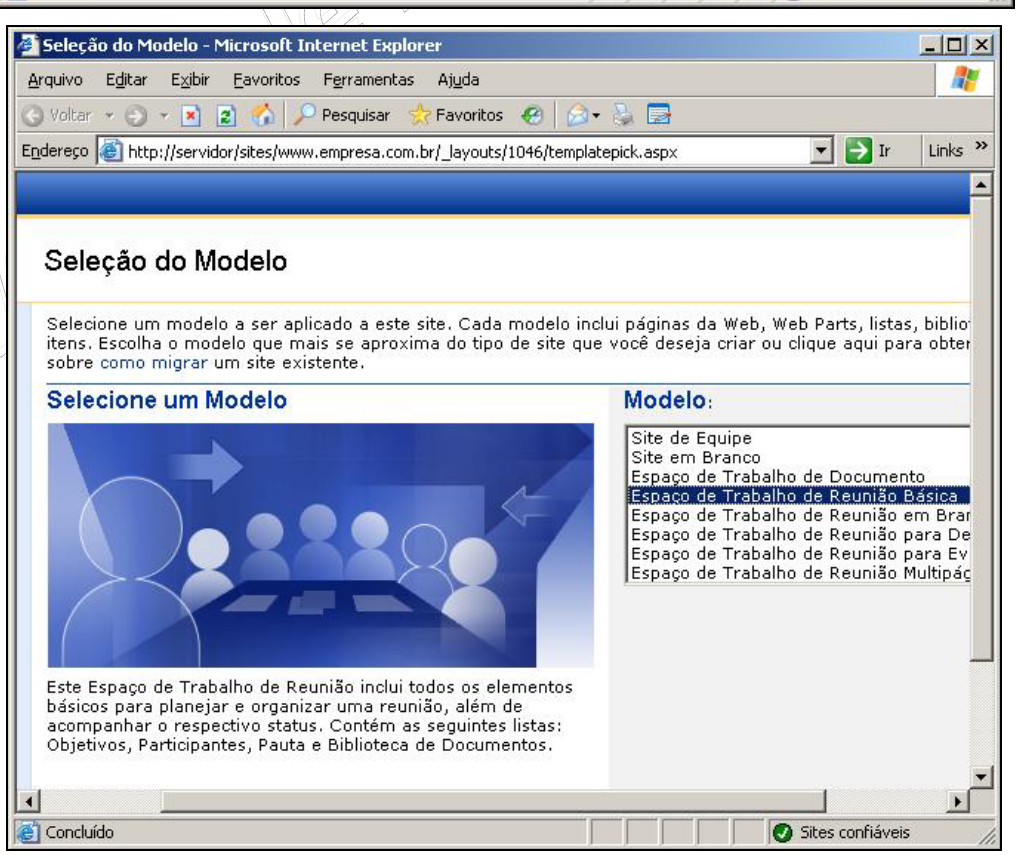


A primeira atividade que podemos desenvolver na interface de administração é a modificação das Páginas Compartilhadas. As Páginas Compartilhadas são Janelas Configuráveis, que podem estar presentes ou não na tela inicial do sistema, como: Avisos, Eventos, Links, etc. Alguns recursos que podemos acrescentar a Página Compartilhada Padrão, são: Contatos, Usuários Online e Tarefas Agendadas. Para acrescentar ou remover itens de Páginas Compartilhada execute o seguinte procedimento:

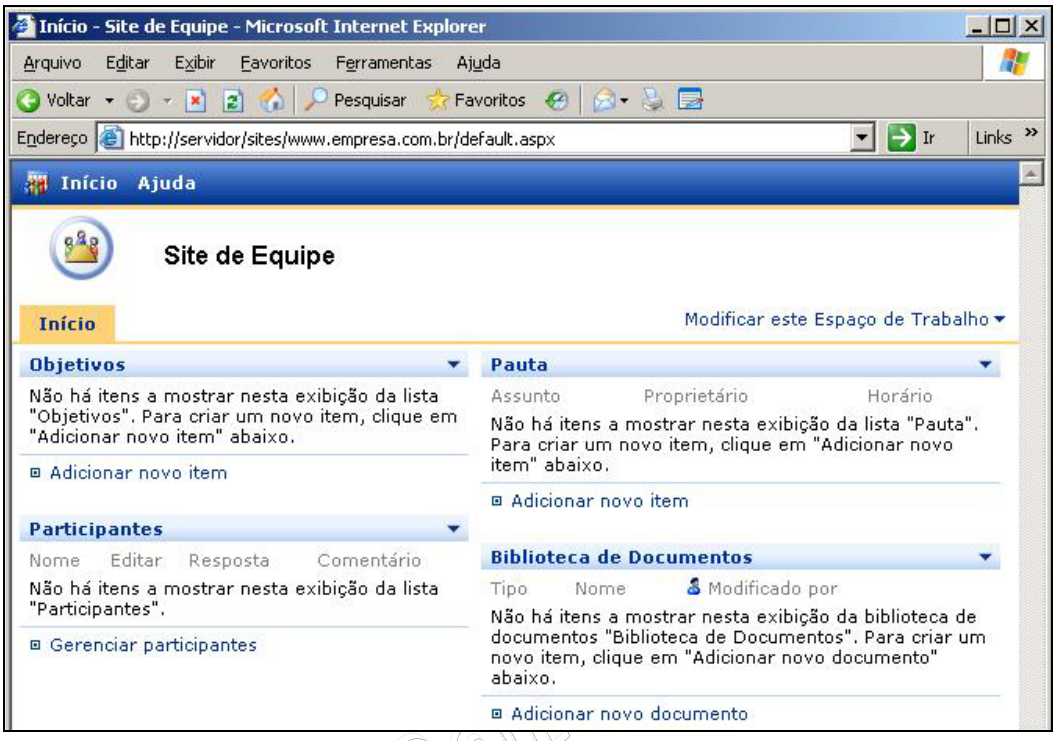


Em seguida poderemos modificar a aparência do site através da escolha de temas, e a forma como o conteúdo é apresentado, observe abaixo como modificar o visual e o conteúdo do site após a modificação:

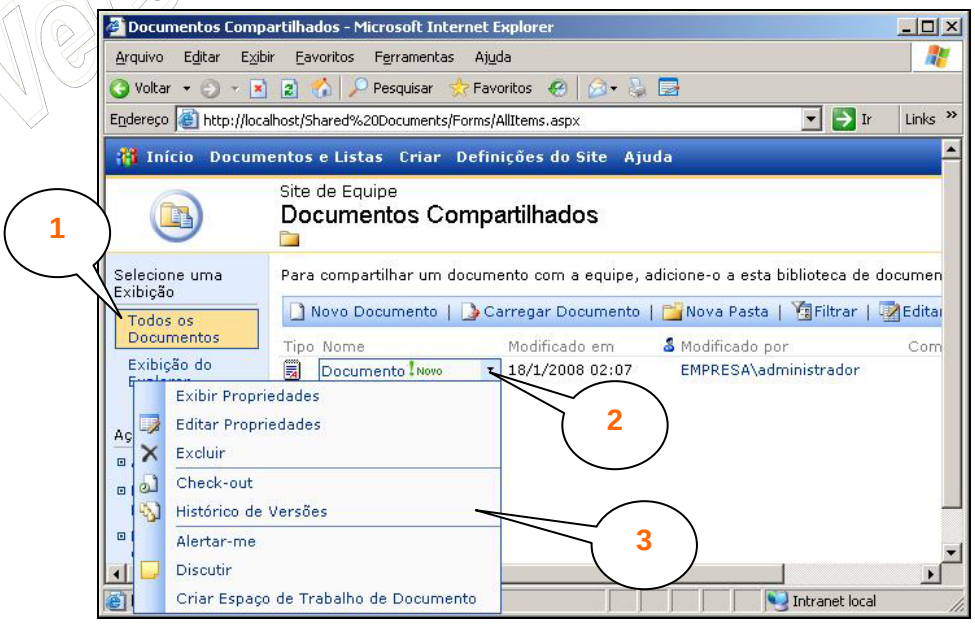




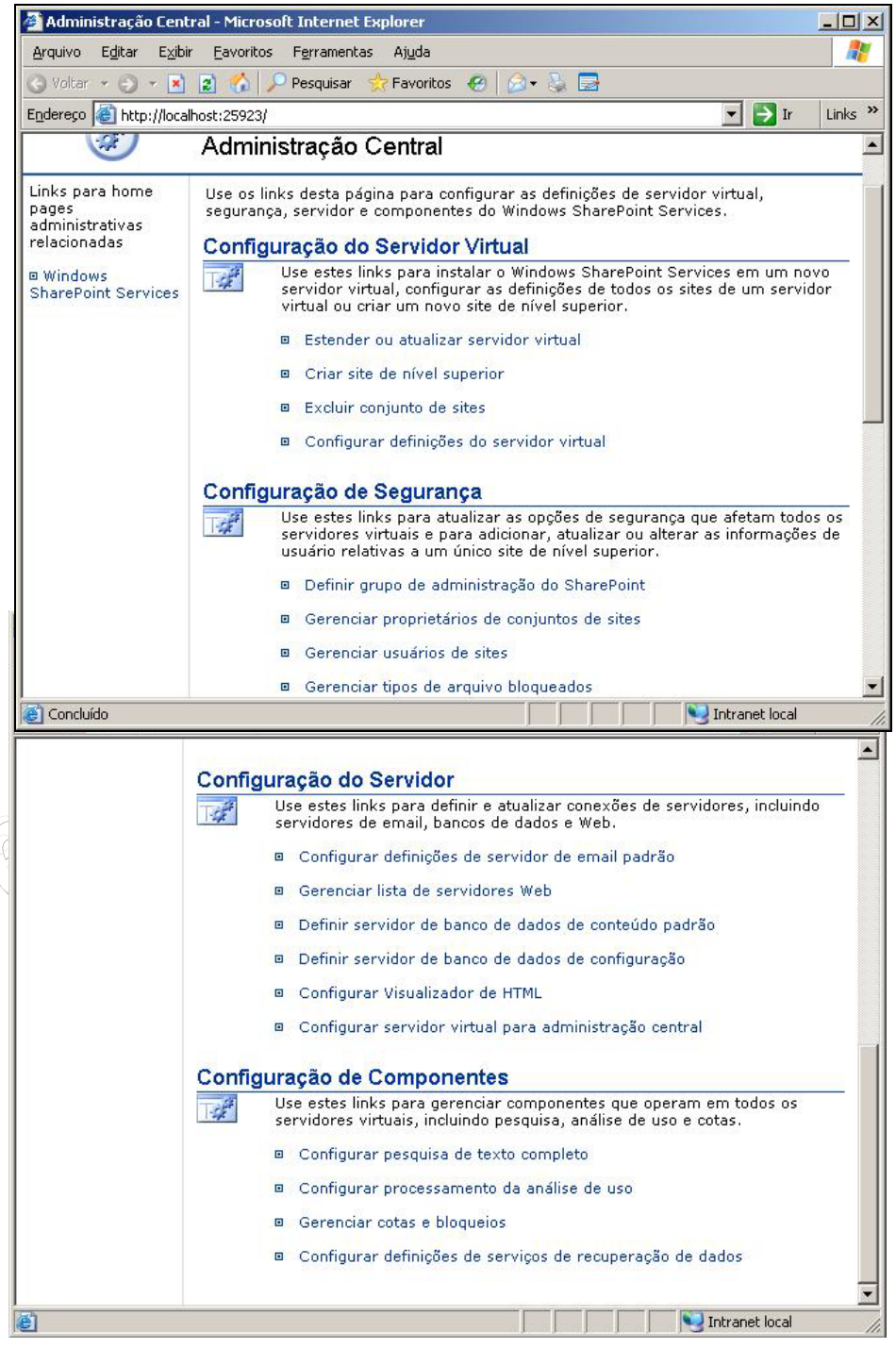
A escolha de um modelo implica em um conjunto pré-determinado de Páginas Compartilhadas, que podem ser modificados após a aplicação do modelo. Observe abaixo o resultado da aplicação do modelo na página inicial do SharePoint:



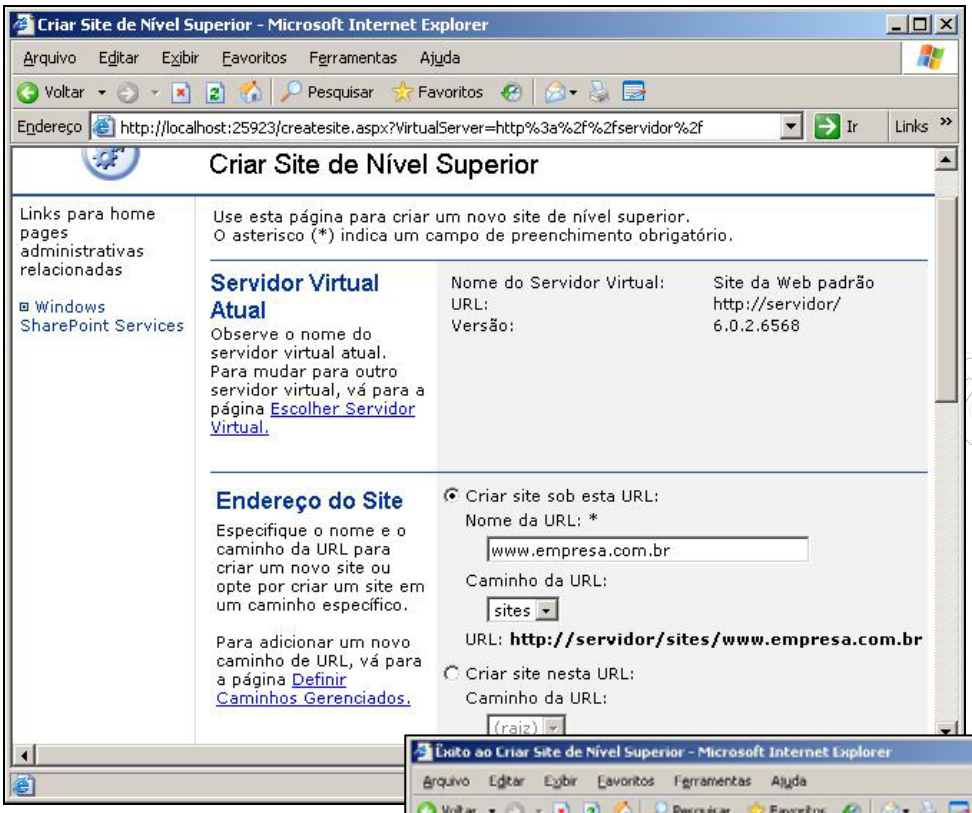
Um dos recursos mais importantes do SharePoint é a publicação de documentos compartilhados, onde os usuários do ambiente SharePoint podem editar e modificar dados desses documentos, porém, para cada versão nova modificada é gerado um histórico de modificações e controle no próprio ambiente. Como exemplo, vamos supor que a grupo do SharePoint denominado Comercial possui um documento a ser compartilhado por todos os vendedores, como: Documento.rtf. Este documento armazenará os dados de contato dos principais tele-taxis da cidade. É possível que novas empresas surjam ou desapareçam do mercado, e assim sendo, qualquer membro da equipe possui autonomia para editar e modificar o Documento.rtf. Porém, para cada nova versão de documento criada é gerado um histórico de atualizações, onde fica registrado: quem, quando e para quê realizou a modificação:



O SharePoint é destinado inicialmente para atender as redes locais, ou intranets, porém é possível estender suas funcionalidades para extranets ou a própria Internet. Através da “Administração Geral”, é possível criar um conjunto de servidores que suportem as aplicações da intranet, gerenciar permissões de usuários e grupos, e tornar o serviço em nível superior, por exemplo, através do endereço www.empresa.com.br/sharepoint qualquer pessoa na Internet poderia ter acesso aos serviços da Intranet.



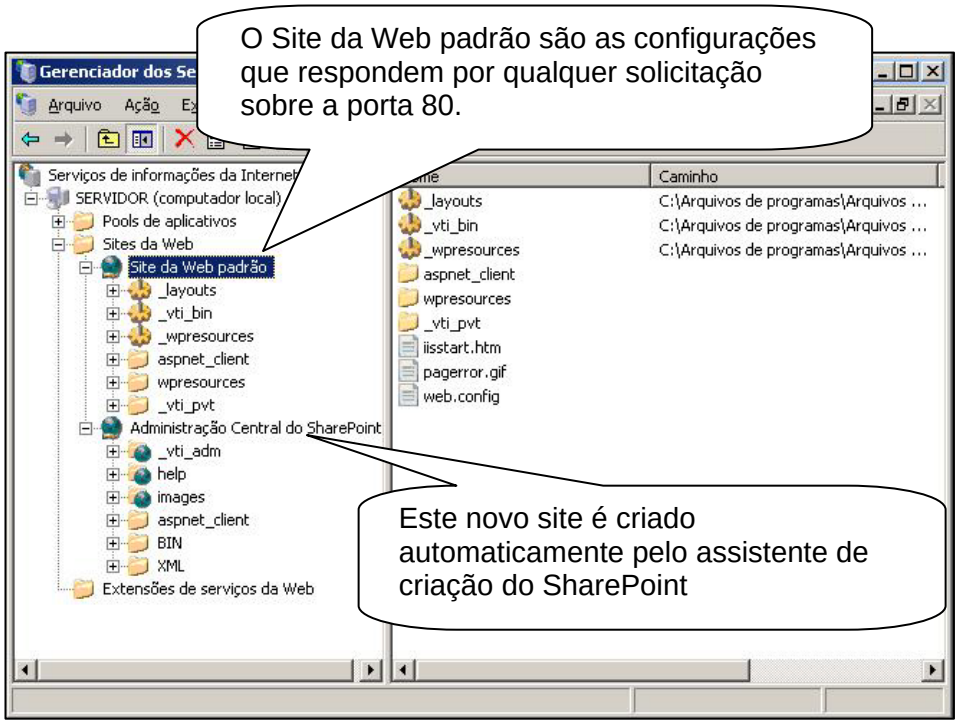
Vejamos no exemplo a seguir como realizar um upgrade dos serviços do SharePoint para responder através de um site na Internet, www.empresa.com.br:



Para que o SharePoint possa ser efetivamente publicado na Internet, precisaremos antes configurar devidamente os servidores de Web e DNS.

Ao instalarmos o SharePoint observamos que o servidor Web também foi instalado em conjunto.

Através do caminho: Painel de Controle -> Ferramentas Administrativas -> Gerenciador dos Serviços de informação da Internet (IIS), podemos administrar o servidor Web. Observe ao lado esta janela de administração:



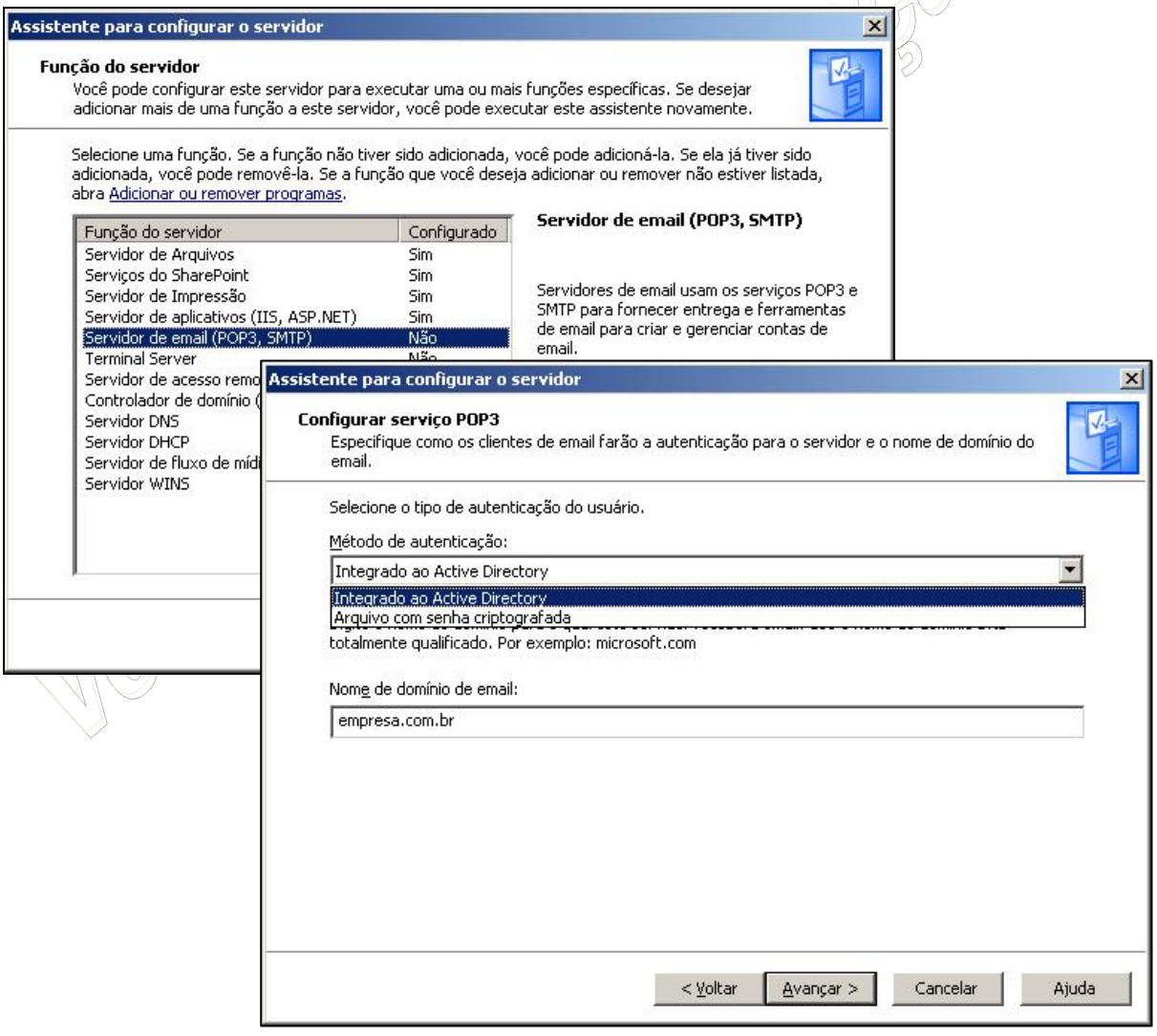
O Site da Web padrão são as configurações que respondem por qualquer solicitação sobre a porta 80.

Este novo site é criado automaticamente pelo assistente de criação do SharePoint

O Servidor Web, por padrão, está preparado através do Site da Web Padrão, para responder a qualquer solicitação via porta 80. Porém, é recomendável desativar este serviço da Web Padrão logo após a instalação do IIS, em função de muitos problemas de segurança já reportados. Em substituição ao Site da Web Padrão você pode criar um novo site, especificando com exatidão o cabeçalho do site, que em nosso caso é o www.empresa.com.br, e dessa forma evitando os riscos de segurança envolvidos nesse tipo de servidor.

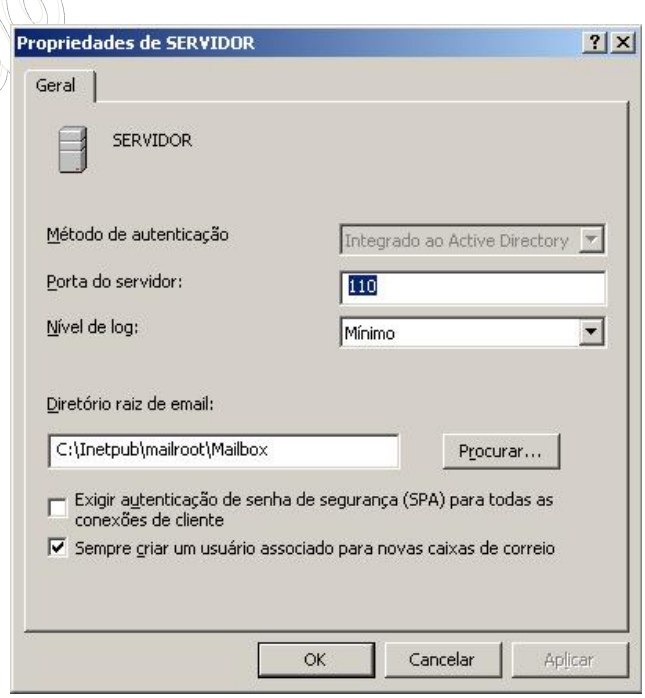
Nosso servidor de intranet está quase completo agora, resta apenas uma nova função para torná-lo 100% operacional, o servidor de envio de mensagens.

O Servidor de e-mail é composto por duas aplicações bem distintas, o serviço de recebimento, ou mais conhecido como protocolo POP3, e o serviço de envio, ou mais conhecido como protocolo SMTP. Ambos são os mais populares, porém existem diversos outros. Vejamos como adicionar estes serviços ao nosso servidor de forma a podermos realizar o envio de e-mails através do site:

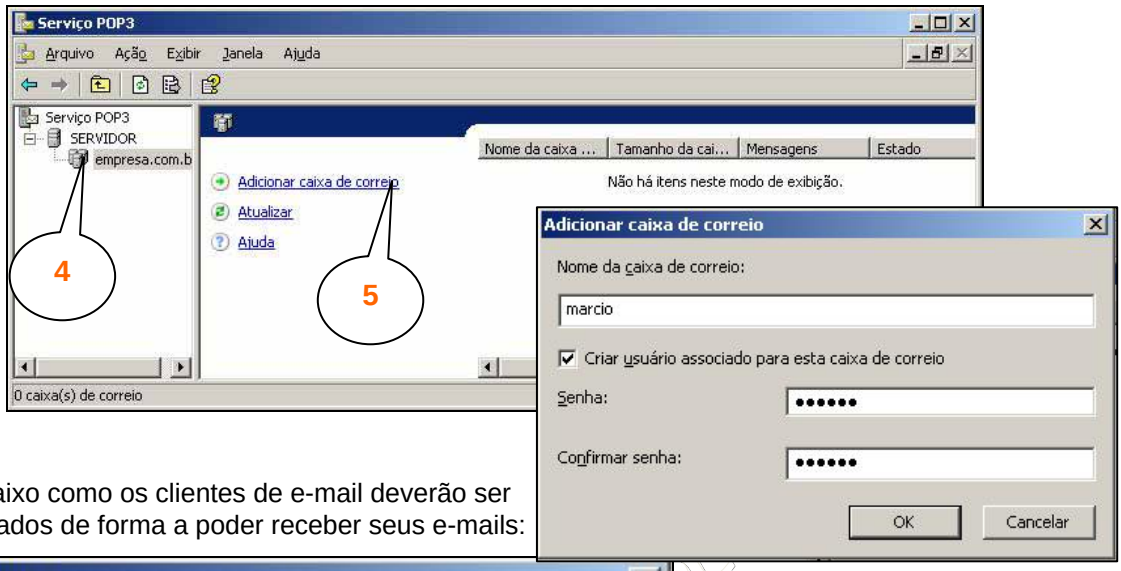


Quando Integrado ao Active Directory, cada usuário do servidor receberá uma conta de e-mail, a qual poderá utilizar tanto para enviar quanto para receber mensagens por e-mail. Toda a tecnologia de autenticação será baseada no Active Directory. Outra alternativa é quando não temos o AD instalado em nossa rede, e dessa forma poderemos criar as contas de e-mails e senhas através de um arquivo com senha criptografada. Esses usuários serão cadastrados no próprio servidor de e-mail, através da ferramenta de administração das contas pop3. A ferramenta de administração do Serviço POP pode ser acessada através da mesma interface do “Gerenciar o servidor”:

Nas propriedades do servidor podemos configurar a porta do protocolo POP3, que pertence a família de protocolos do TCP/IP. O padrão adotado universalmente para a porta POP3 é a 110. É possível escolher outra porta qualquer, como a 111, porém nos softwares clientes de e-mails, você precisará configurar manualmente esta nova porta de acesso. É também nessa tela que podemos especificar que cada usuário novo criado tanto no servidor quanto no Controlador de Domínio terão uma conta de e-mail associada. Observe também a pasta onde serão armazenados os e-mails, em servidores com muitas caixas postais o ideal é alterar esse caminho para um volume RAID-5, Espelhado ou SAN.



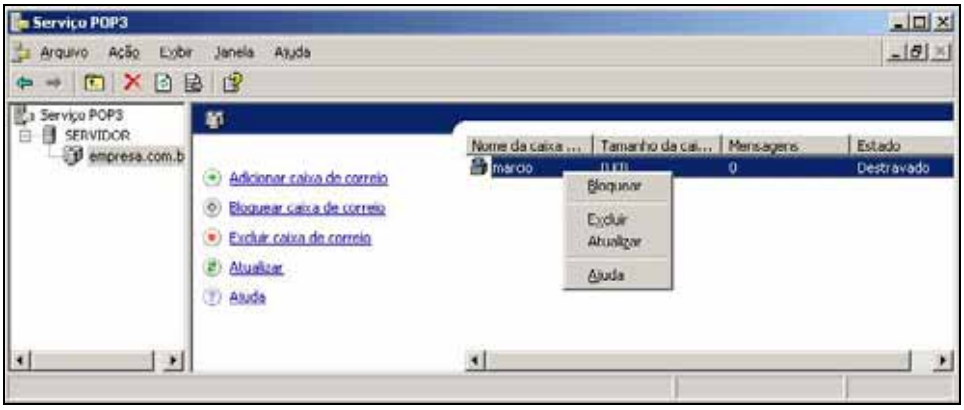
A adição de novas contas de e-mails é realizada através da interface abaixo:



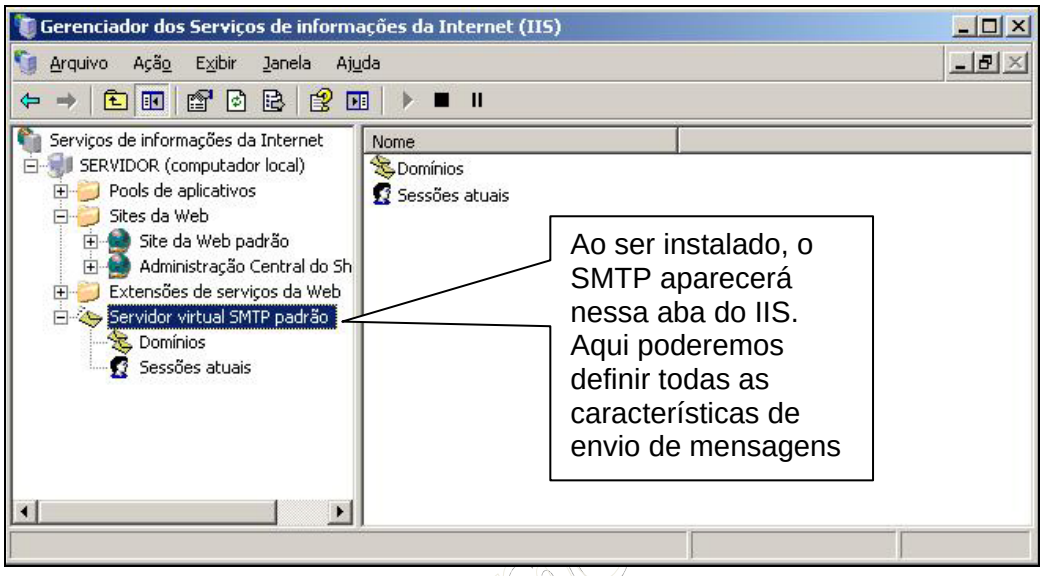
Veja abaixo como os clientes de e-mail deverão ser configurados de forma a poder receber seus e-mails:

Mais a frente veremos como realizar estas configurações no próprio cliente.

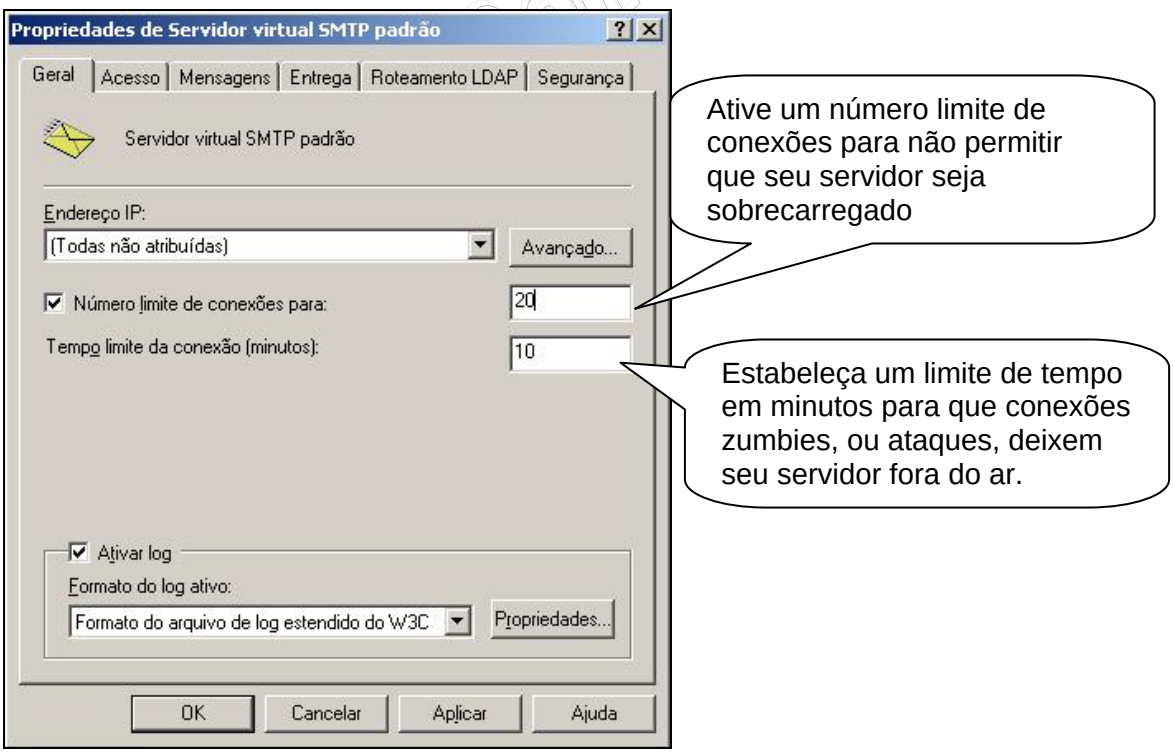
Uma vez criadas as contas o servidor nos fornece opções de bloquear a conta (permanentemente ou temporariamente) ou excluir. Informações como: tamanho atual da caixa no disco do servidor, quantidade de mensagens aguardando por serem baixadas e o estado da caixa postal também estão disponíveis na mesma interface:



Falaremos agora do serviço de envio de mensagens, o SMTP. Diferentemente do seu primo, o POP3, o SMTP não possui uma interface própria para administração, ao invés disso utiliza o Gerenciador dos Serviços de Informação da Internet (IIS):

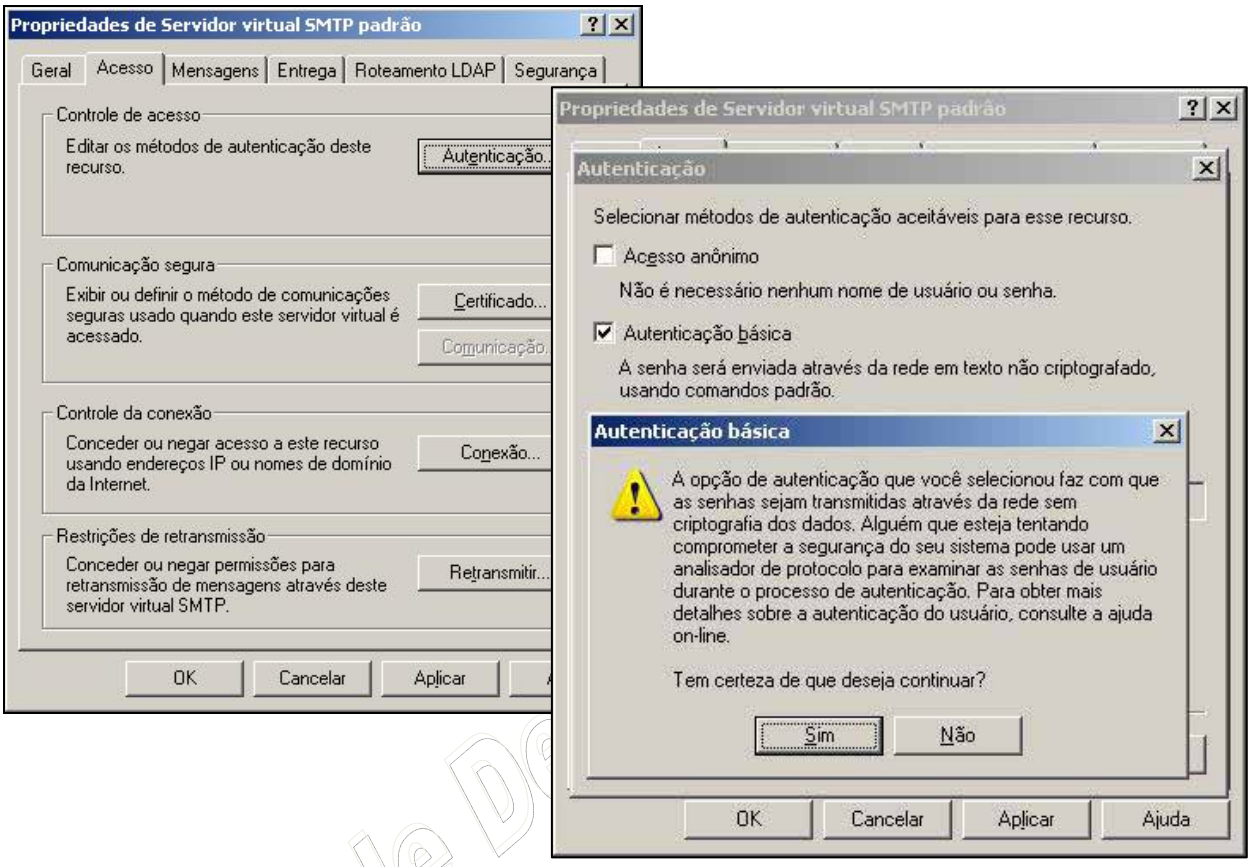


O serviço de envio SMTP possui diversas configurações possíveis, vejamos algumas delas:

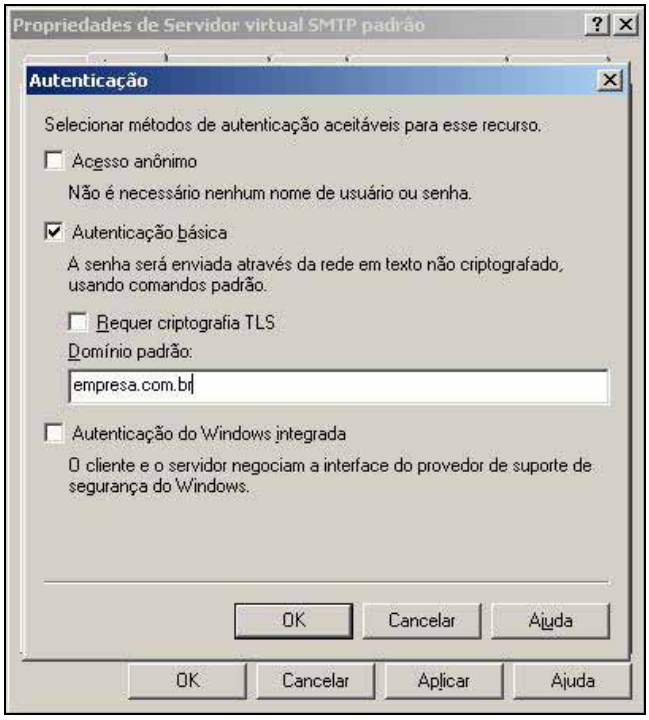


Na próxima aba, temos as configurações de “Acesso” ao servidor, que define os controles de autenticação, permissão de acesso ao servidor e retransmissão. A retransmissão, ou em inglês “*relay*” é o controle sobre quem pode enviar mensagens através deste servidor. Um dos maiores problemas de servidores SMTP é quando esta retransmissão está aberta, ou seja, qualquer pessoa pode enviar mensagens através do servidor. Muitos hackers e spammers caçam continuamente servidores SMTP abertos, ou seja, com retransmissão aberta, para poderem enviar seus spam de forma anônima na Internet. No Brasil, já existem entidades e leis que coíbem o uso de SMTP com retransmissão aberta, sendo inclusive citado no código penal.

Para evitar a retransmissão aberta a forma mais simples e comum é autenticação no SMTP, vejamos essas configurações agora:

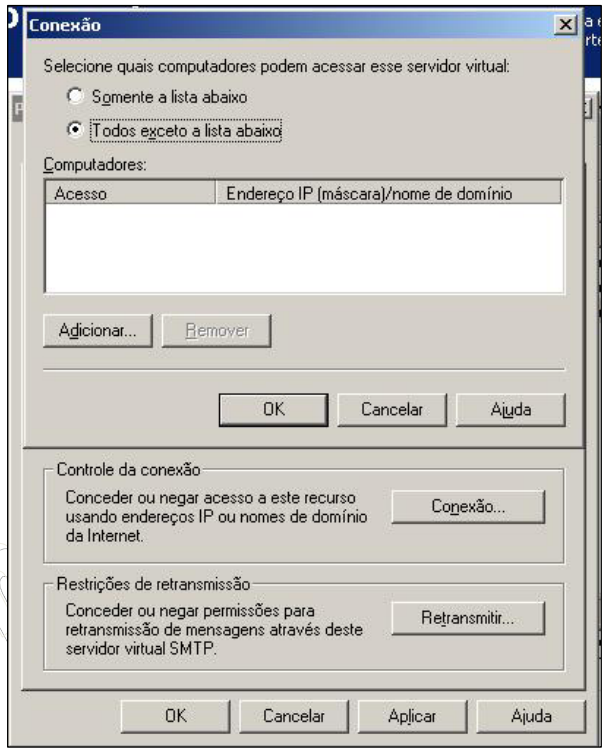


Observamos acima a configuração do método de acesso ao servidor via autenticação básica. Esse método é o mais comum e mais aceitado pelos softwares clientes de e-mails da atualidade, porém, ele possui como fragilidade o envio de senhas em texto claro, ou seja, é possível que hackers, utilizando-se de softwares de captura de senha, possam facilmente capturar essas senhas. Porém, ainda é preferível esse nível de segurança ao acesso anônimo, onde nenhum tipo de senha é transmitido. Ao configurarmos a autenticação básica precisaremos, também, configurar o domínio padrão:

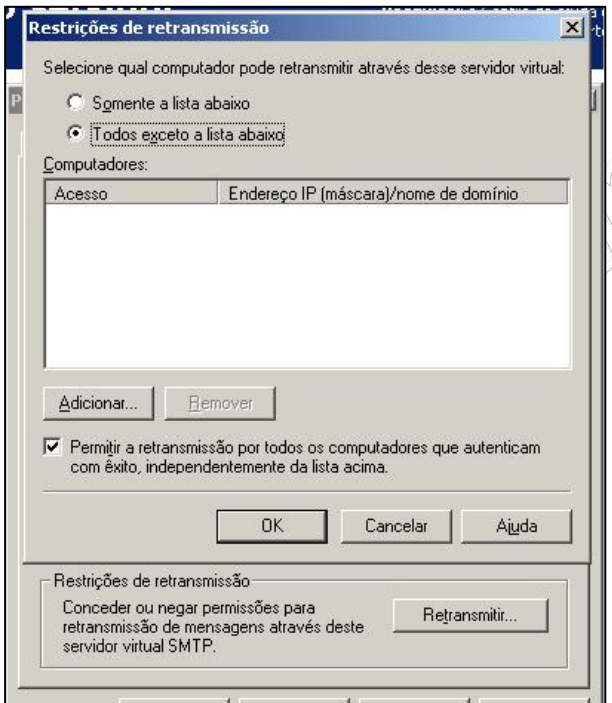


Em seguida vamos definir que nosso servidor pode ser acessado por todos os computadores em rede, e criaremos um espaço chamado “lista negra”, ou seja, todos os computadores, excetos os que estejam na “lista negra” poderão autenticar em nosso servidor para enviar mensagens:

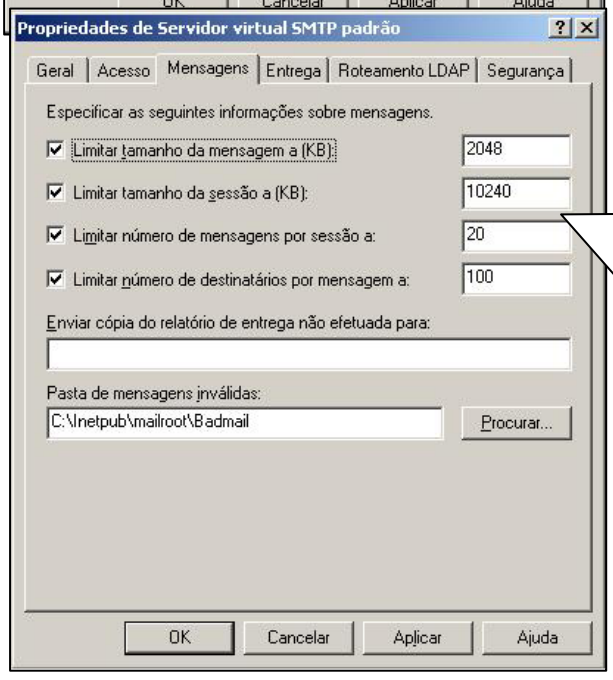
Servidores de e-mails mais especializados, como o Microsoft Exchange, utiliza “listas negras” automatizadas, ou seja, é possível assinar serviços na Internet onde são baixados automaticamente a listagem dos endereços de computadores que tentam utilizar os serviços de SMTP com fins inapropriados, como hackers ou spammers.



E realizaremos uma configuração similar para a retransmissão, onde todos, devidamente autenticados, poderão retransmitir seus e-mails para a Internet:



Seguindo com as opções de propriedade temos a aba “Mensagens”, nela poderemos configurar os limites de cada mensagem a serem enviadas através do servidor. Um ponto interessante a saber é que, o tamanho de cada mensagem, corresponde exatamente a quantidade de memória RAM que o servidor precisará alocar para processar essa única mensagem. Dessa forma, se um usuário enviar uma única mensagem de 100MB para uma lista de 10 usuários, o servidor precisará de 1GB RAM apenas para atender esta mensagem:



Uma sessão corresponde a um acesso realizado por um usuário. Ao limitar a sessão estamos limitando o envio em massa de mensagens em 10MB. E a quantidade máxima de destinatários em um único acesso a 20, ou seja, uma vez autenticado no sistema, o usuário só poderá enviar e-mails para 20 destinatários, podendo ser estes listas de e-mails ou e-mails individuais.

A principal função do servidor SMTP é gerenciar toda a comunicação de entrega das mensagens dos usuários. Antigamente, de 1979 a 1994, os serviços de envio de mensagem eram gerenciados pelos próprios usuários, onde esses precisavam encontrar o endereço IP da máquina que iria receber a mensagem, depois abrir uma sessão no serviço de entrega de mensagens do usuário, redigir a mensagem neste mesmo software para então ter a certeza de que conseguiu enviar uma mensagem. Quando o destinatário não estava on-line não era possível enviar a mensagem. Esse é um dos principais motivos da necessidade de criação dos servidores de envio de mensagens. Esses servidores tornam transparente o processo de envio para os usuários. O usuário redige sua mensagem e a entrega ao servidor, esse por sua vez negociará com o servidor SMTP do destinatário para então poder depositar a mensagem na caixa postal do destinatário. Quando o destinatário estiver novamente on-line, poderá recuperar todas as mensagens que foram enviadas a ele através de seu servidor POP3.

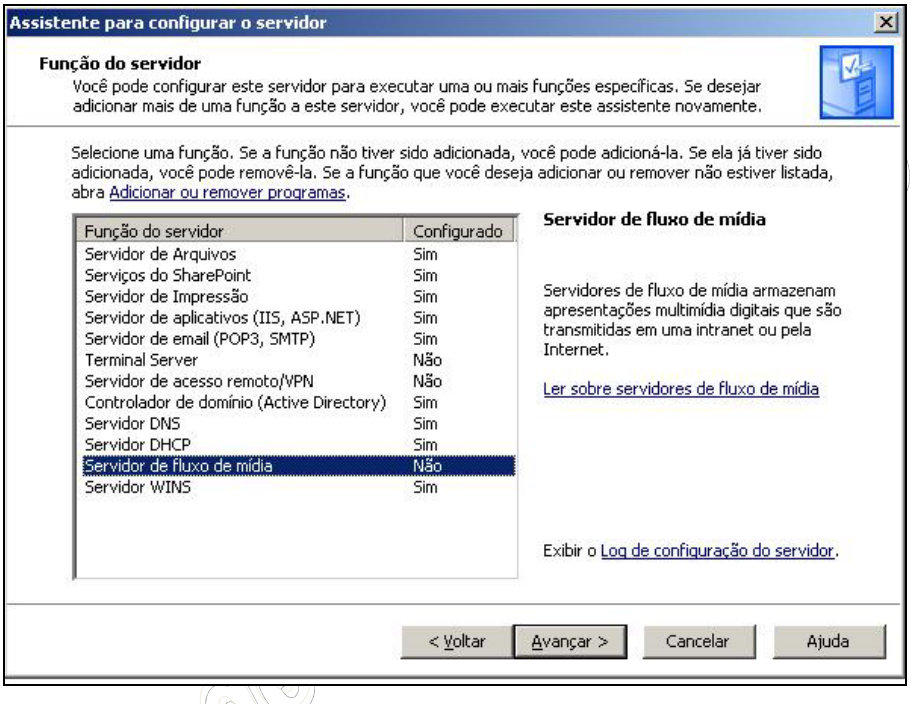
Mas mesmo essa nova infra-estrutura ainda pode sofrer atrasos na entrega das mensagens, como no caso do link de internet do provedor do remetente estar fora do ar, ou mesmo o link de internet do provedor do destinatário, e dessa forma a mensagem precisará aguardar, durante um certo intervalo de tempo, em uma fila, serão realizadas várias tentativas de entrega, e a depender do que esteja acontecendo na infra-estrutura dos provedores, essa mensagem pode levar alguns dias até ser finalmente entregue, vejamos as opções de configuração para estas filas de mensagens retidas:

Observamos ainda na imagem a existência de três botões: Segurança de saída, conexões de saída e avançada. A segurança de saída é uma configuração a mais de segurança do próprio servidor para que o mesmo exija uma autenticação antes de enviar mensagens, as conexões de saídas limitam a quantidade máxima de pessoas conectadas ao servidor, e em avançada configuramos o nome do domínio que será apresentado a todos os destinatários. Por padrão podemos manter essas configurações no estado original. As demais opções da propriedade de servidor virtual SMTP também podem ser mantidas originais, não implicando em segurança ou performance.

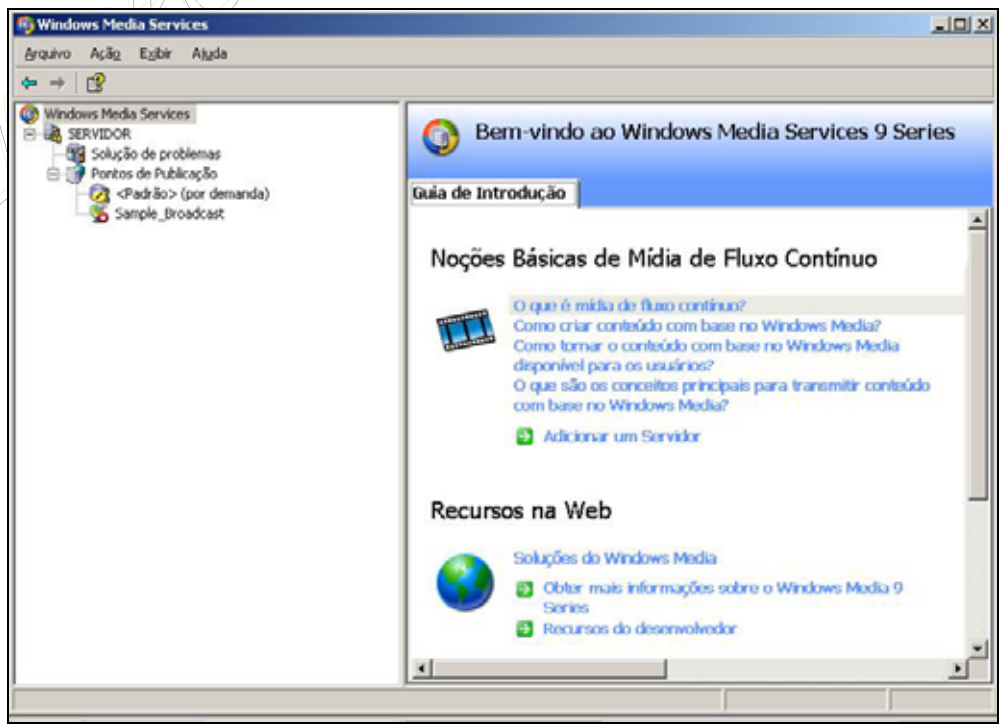
Veremos agora um novo serviço avançado, o servidor de fluxo de mídia. Um dos serviços mais elegantes e que demandam enormes recursos de infra-estrutura, como: servidores potentes, alto espaço em armazenamento, links de Internet com suficiente largura de banda e dedicados, entre outros.

Servidor de Fluxo de Mídia

Servidores de fluxo de mídia são utilizados na transmissão de eventos ao vivo pela Internet ou como repositório de conteúdo multimídia, como trailers de filmes, noticiários e filmagens em geral. Apesar de fácil configuração, porem os ajustes necessários em largura de banda, codecs, taxas de transmissão, entre outros, tornam o serviço de difícil administração.

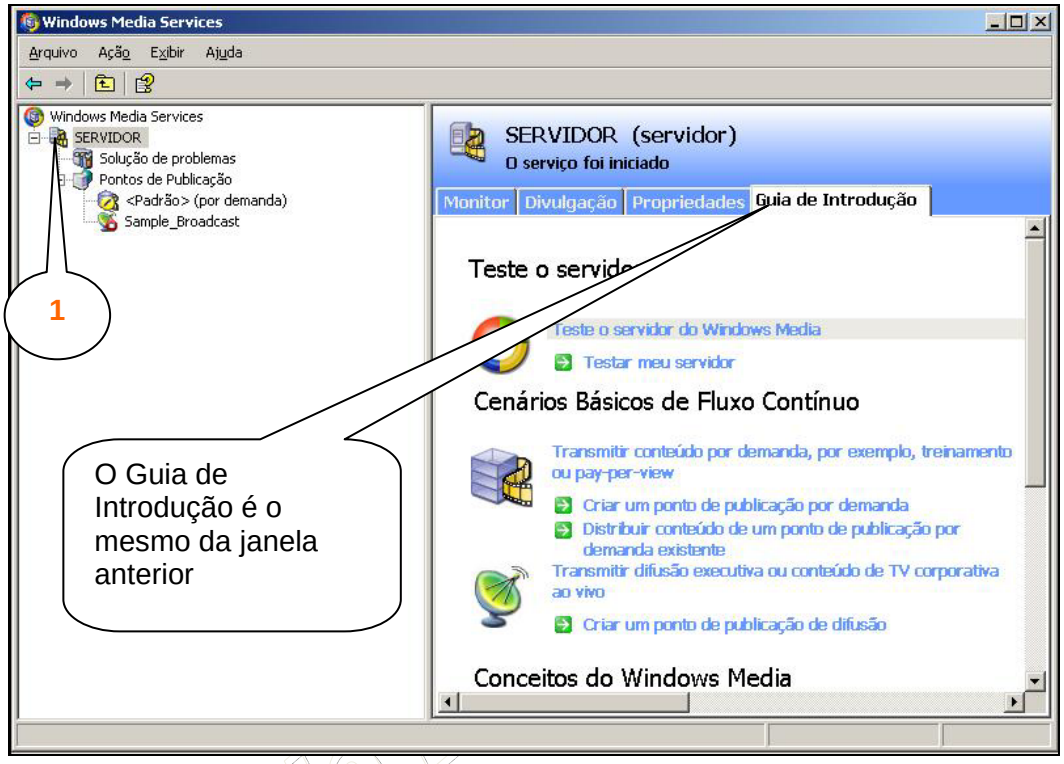


Uma vez instalado o servidor de fluxo de mídia, acessaremos sua ferramenta de administração através da já habitual interface do “Gerenciar o servidor”, pulemos direto para a interface de administração dos serviços de fluxo de mídia:

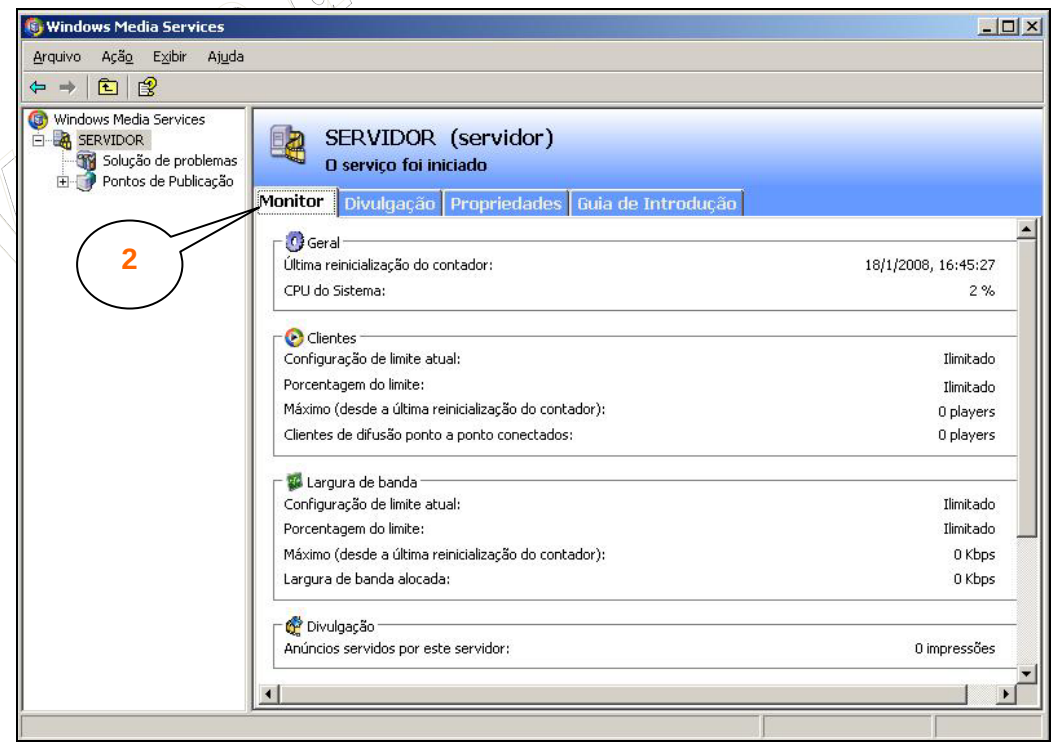


Como é possível observar, a ferramenta Microsoft para fluxo de mídia é o Windows Media Services. Apesar da difícil compreensão da usabilidade deste tipo de sistema, porém a Microsoft já disponibiliza na própria interface de administração, diversos assistentes, tanto de informações gerais, conceitos quanto da própria configuração.

A acessar o item SERVIDOR, na lateral esquerda, é possível visualizar as demais opções do servidor:

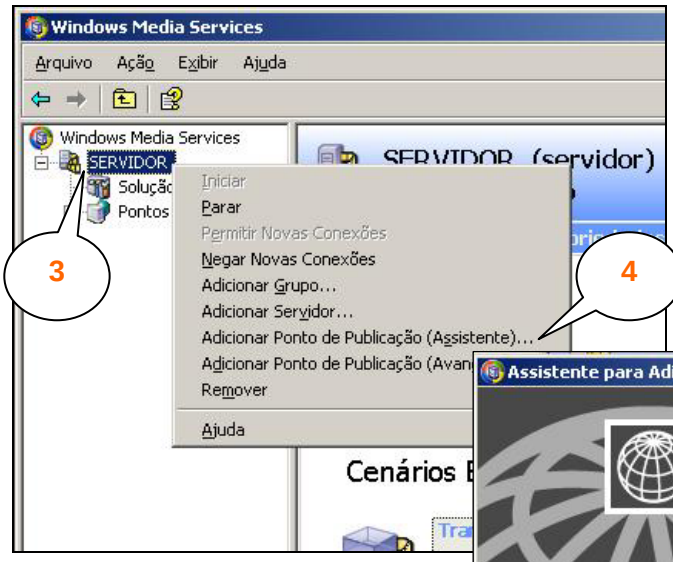


A preocupação com o hardware do servidor é tão grande para este tipo de serviço que uma tela exclusiva de monitoração dos recursos do servidor é provida:

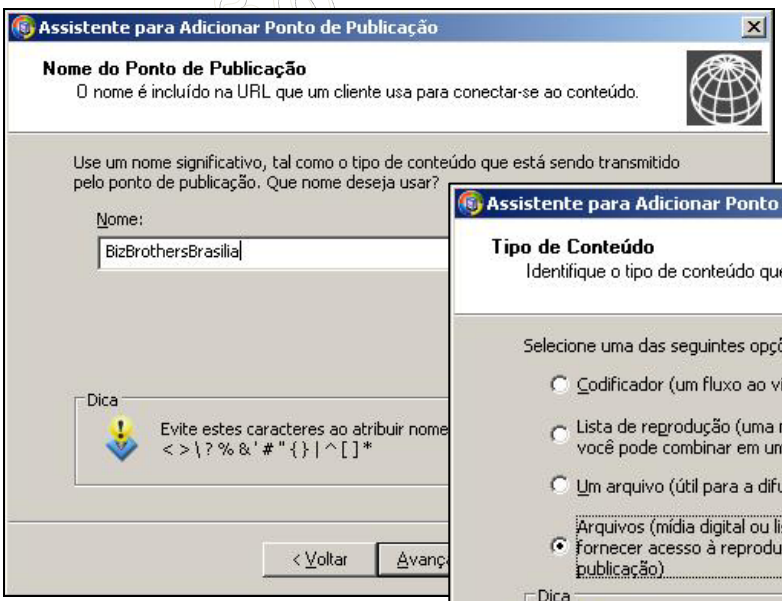


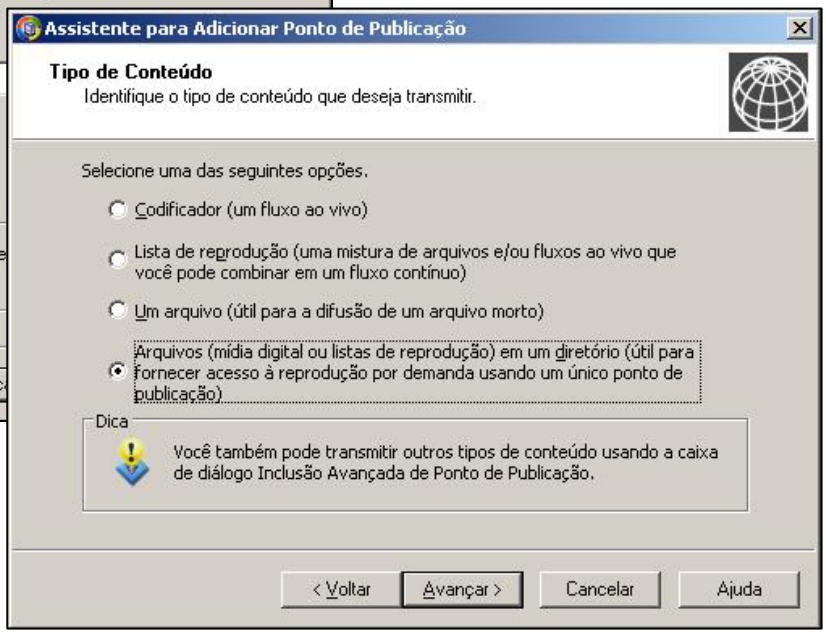
Podemos concluir que o sucesso de implantação de um servidor de fluxo de mídia está mais voltado a infra-estrutura existente do que em itens de configuração, como vimos em todos os serviços até aqui. Isso torna o serviço de fluxo de mídia um servidor especial, e que deve ser instalado e configurado a parte de qualquer outro serviço.

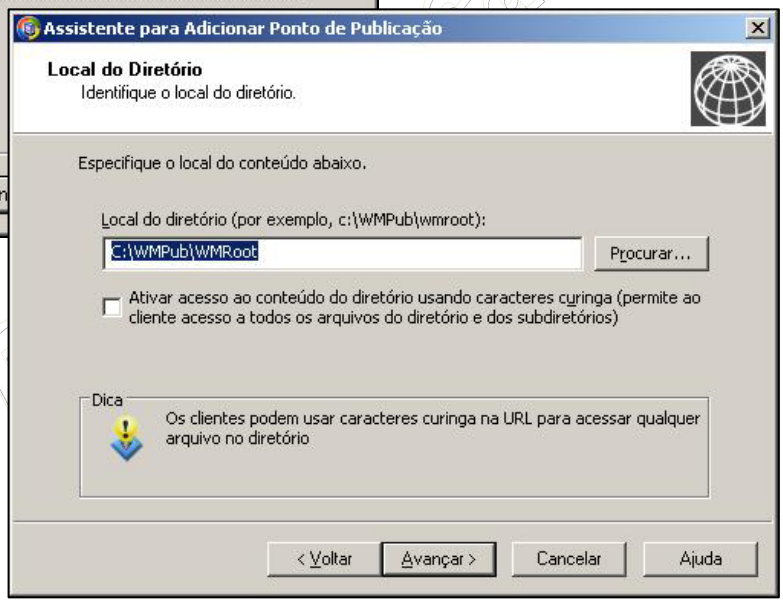
Para criar um espaço para a publicação de material multimídia devemos ser os passos a seguir:



Demonstraremos a seguir como criar um ponto de publicação. Tomaremos como exemplo o objetivo de criar um diretório na Internet, de forma a poder publicar os vídeos gravados através de um programa de televisão. Cada usuário poderá acessar o site da nossa empresa e visualizar online os vídeos disponíveis:

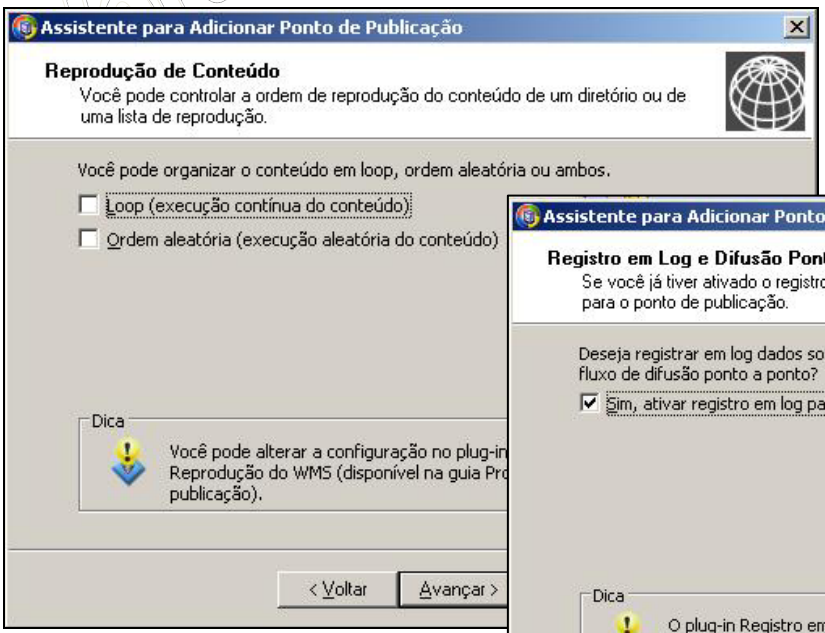




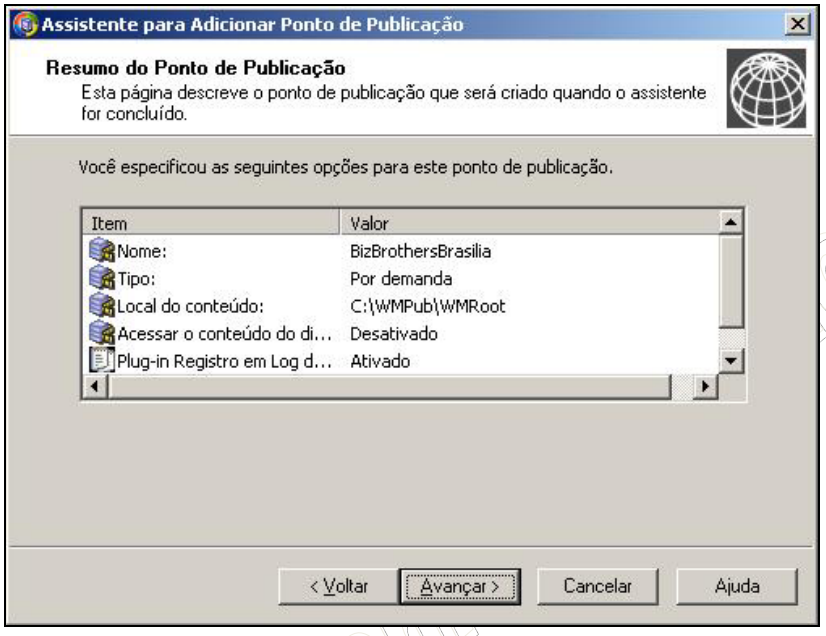


Até aqui o que fizemos foi definir o nome do evento a ser publicado na Internet, o BizBrotherBrasilia, e em seguida definir que os arquivos que estiverem no diretório c:\WMPub\WMRoot poderão ser acessados pelos visitantes.

A próxima configuração é sobre a forma de reprodução de conteúdo e dos registros em Log:



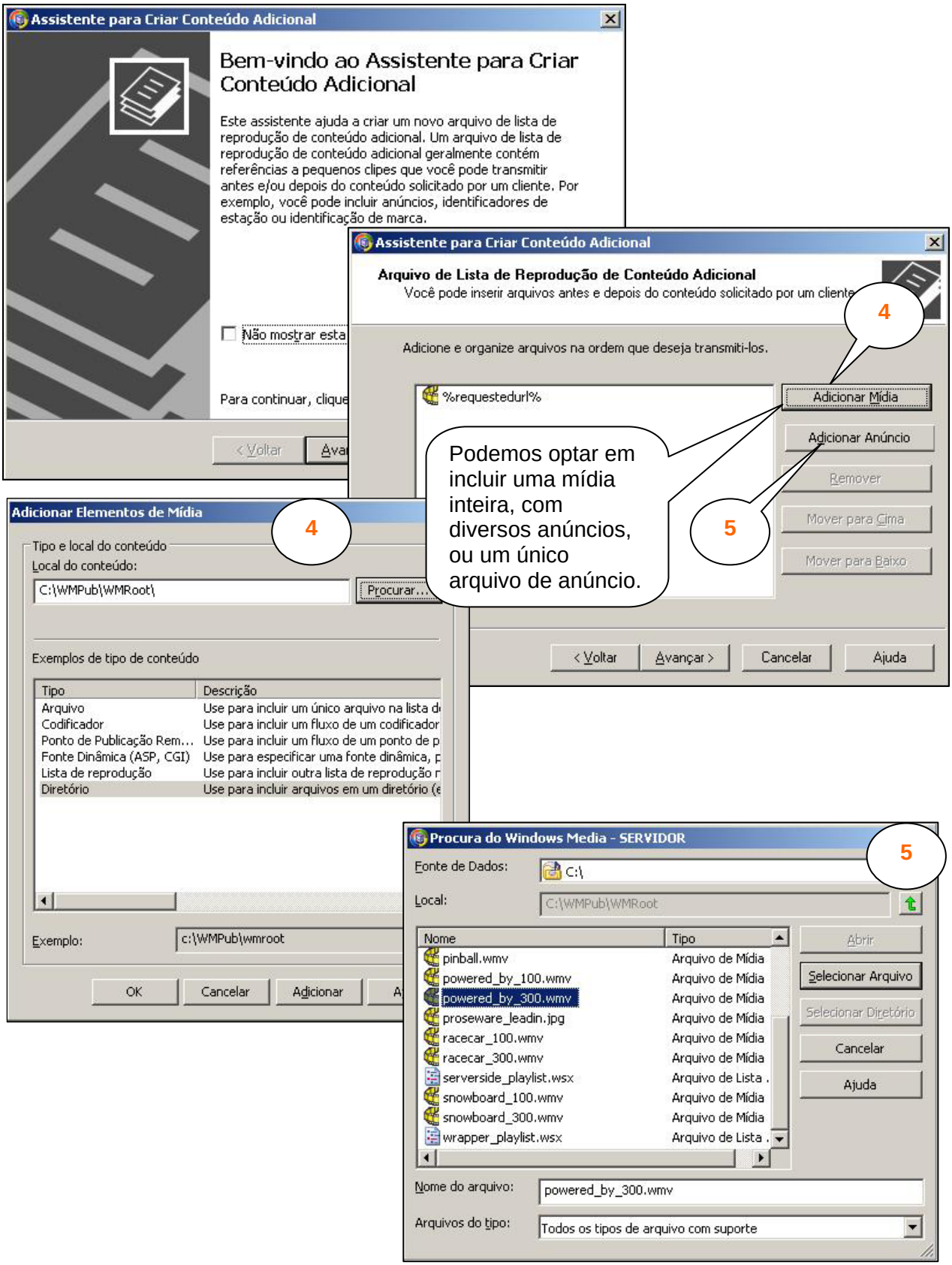
Uma vez concluído o assistente será exibido o relatório de criação, para você confirmar ou descartar os itens selecionados para configuração:



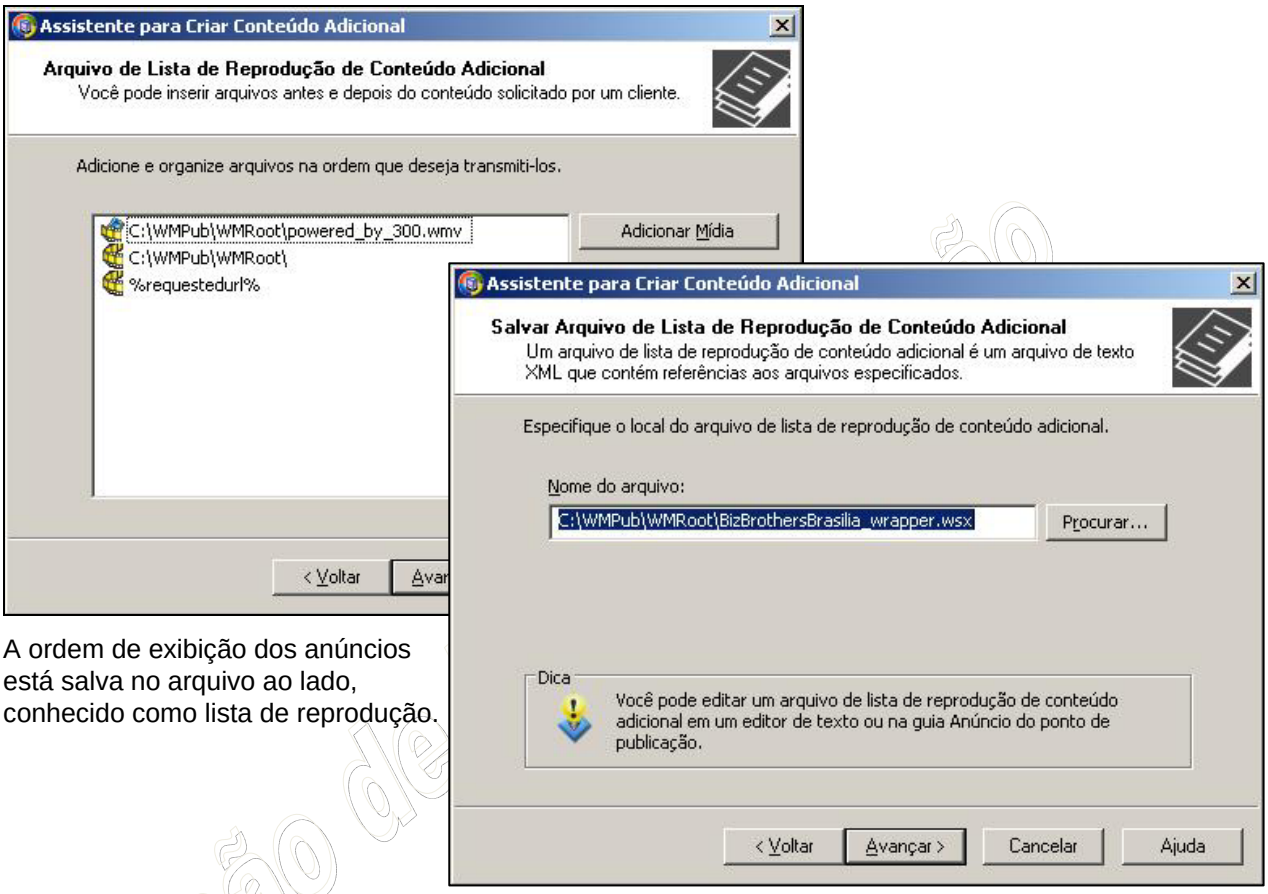
Ao avançar será iniciado um novo assistente para a adição de uma lista de reprodução dos arquivos que estão no diretório e a criação de uma página .html para acesso via servidor Web:

Uma lista de conteúdo adicional são clipes ou vinhetas a serem exibidos antes do vídeo principal, funciona como um esquema de propagandas, o arquivo de anúncio é utilizado como um endereço para acesso através dos principais players de mercado, como Windows Media, Quick Time, etc.

Para cada um desses itens serão iniciados novos assistentes, veremos agora o primeiro assistente, para criação de conteúdo adicional:

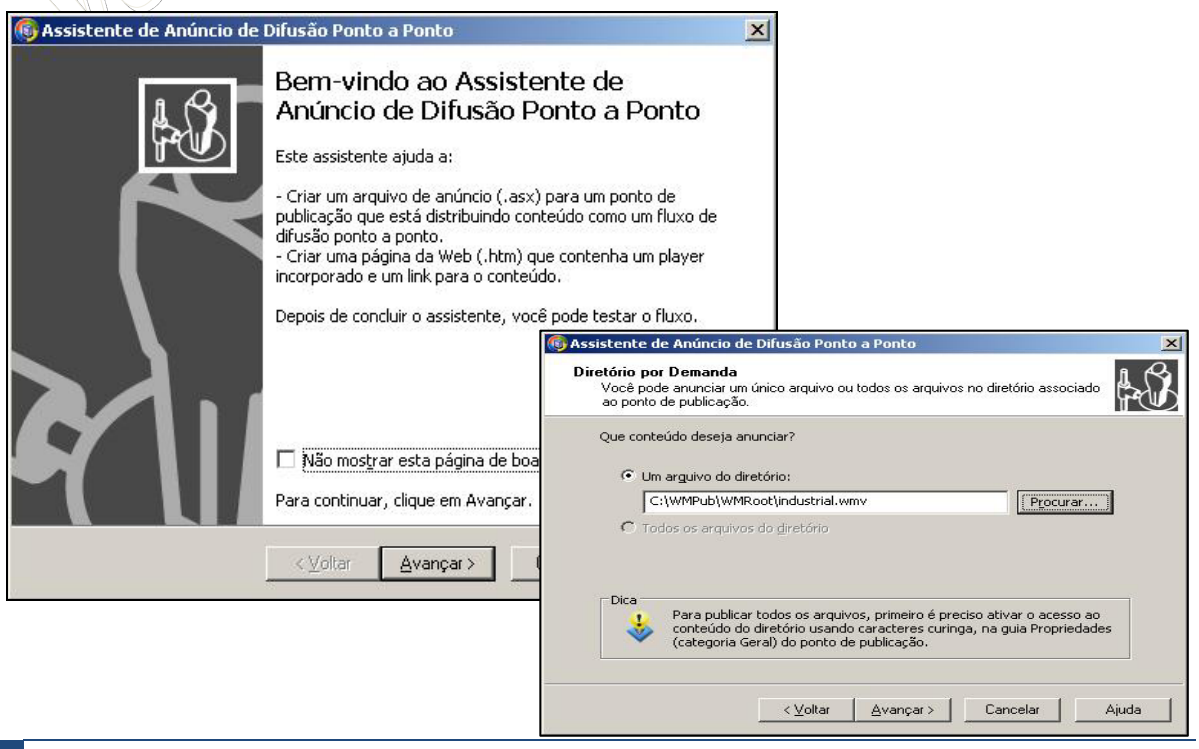


Com isso tempos um ponto de publicação denominado BizBrotherBrasil, cujos vídeos disponibilizados em c:\WMPub\WMRoot serão visualizados, juntamente com todos os anúncios no mesmo diretório e em especial o anúncio powered_by_300,wmv:

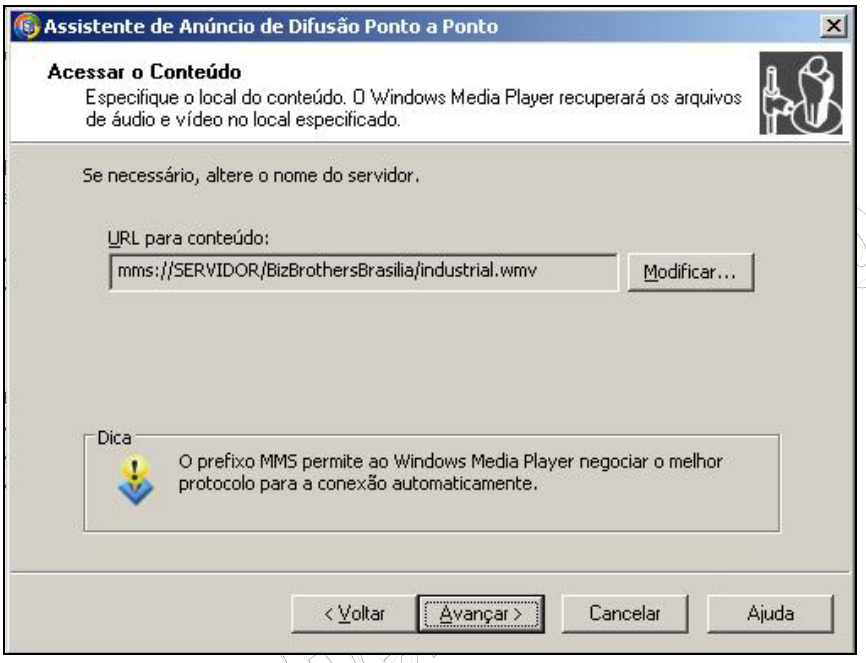


A ordem de exibição dos anúncios está salva no arquivo ao lado, conhecido como lista de reprodução.

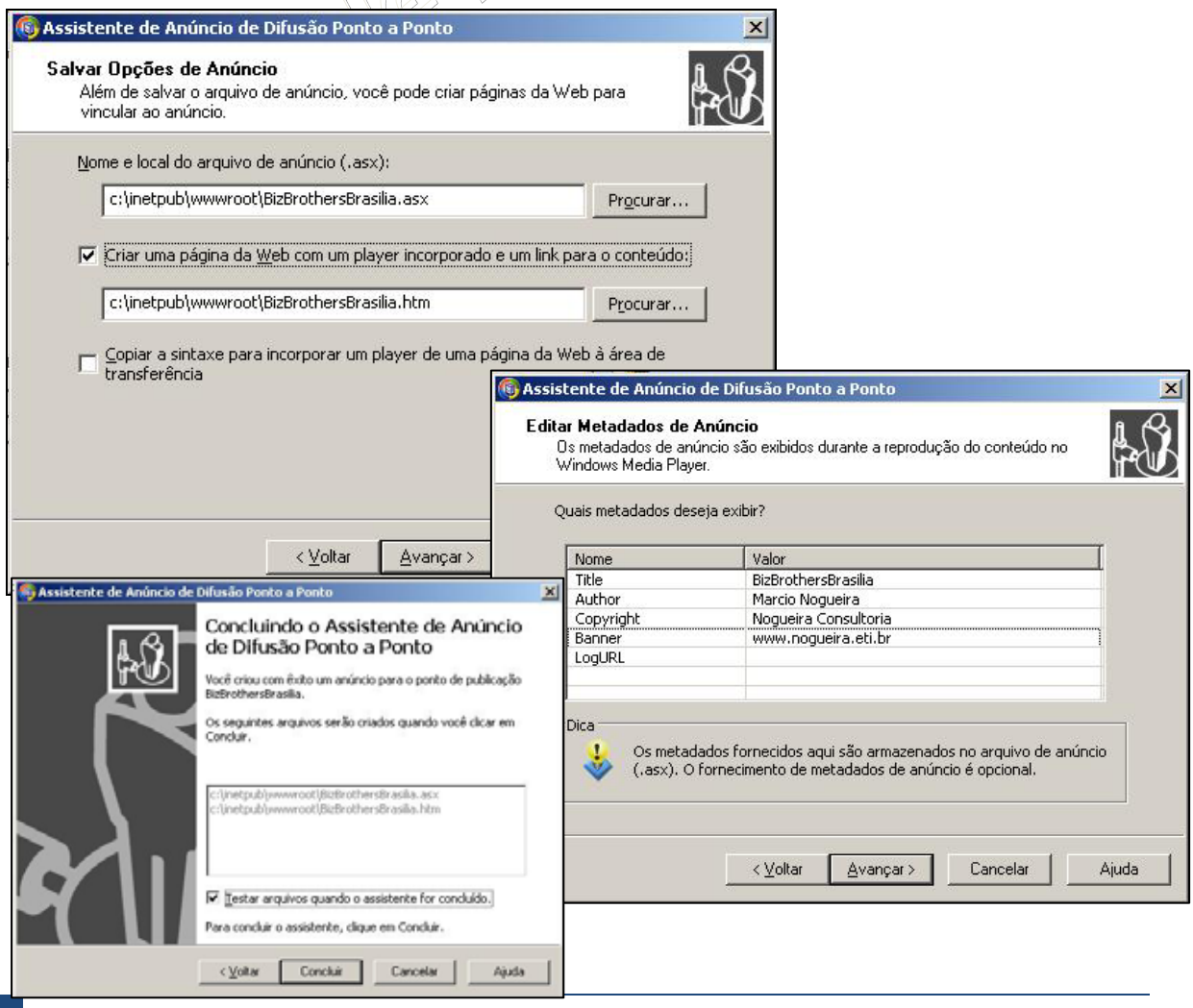
Concluído o assistente de conteúdo adicional dará início agora o assistente de anúncio, que trata-se da criação do arquivo ".asx" utilizado pelos player de mídia, como Windows Media, QuickTime, WinAMP para acessar os pontos de publicação criados:



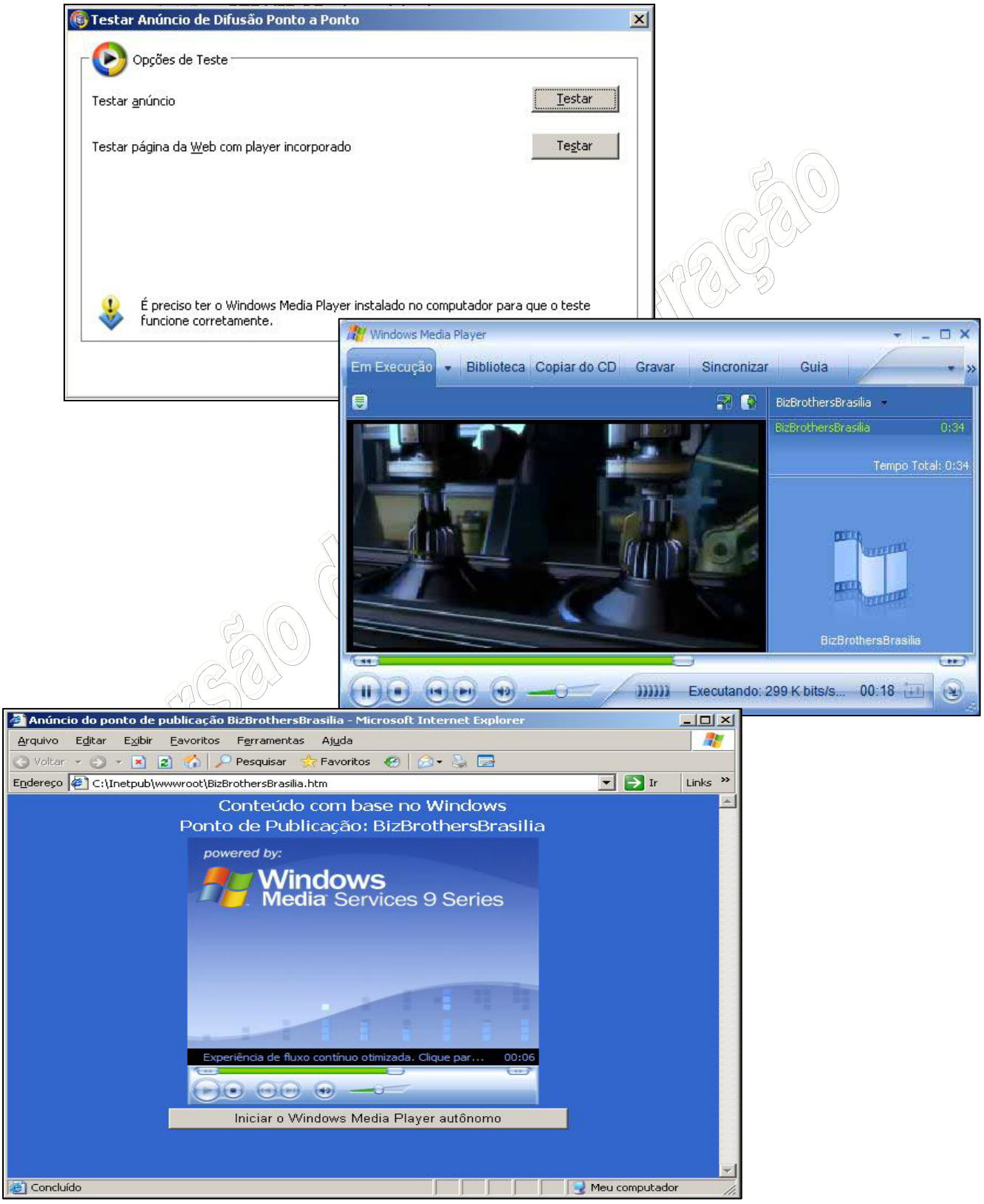
Selecione o local onde será salvo o arquivo, geralmente na mesma pasta onde já estão os vídeos para publicação. Após a criação deste arquivo o assistente informará o endereço, a ser utilizado junto aos players para exibição dos vídeos publicados:



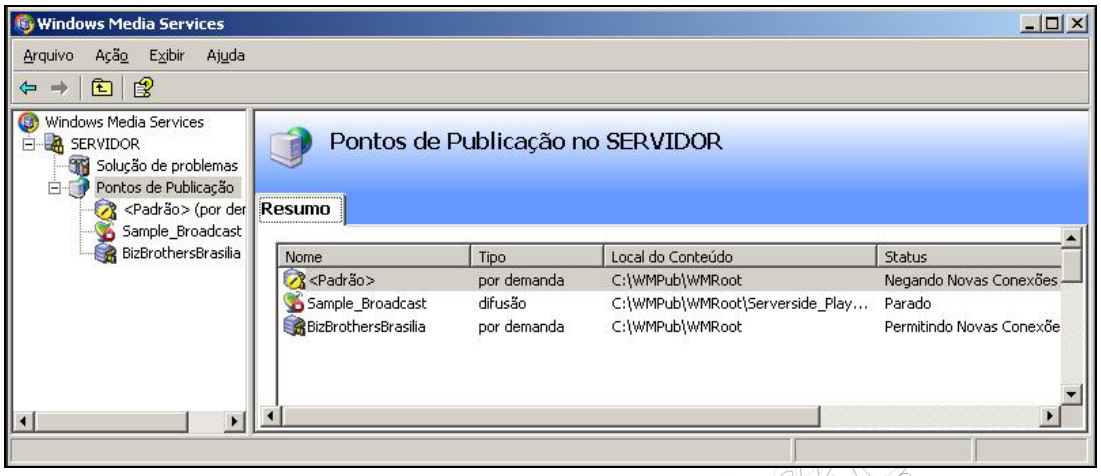
O assistente agora irá criar a página .html a ser visualizada pelos usuários ao acessarem nosso site:



Após a criação do ponto de publicação, com conteúdo adicional e página html, é hora de testar se tudo ocorreu como o esperado. A própria interface de administração do Windows Media Center provê suporte ao teste dos anúncios criados:



Uma vez concluídos todos os assistentes, a interface de administração apresentará todos os pontos de publicação criados por você:

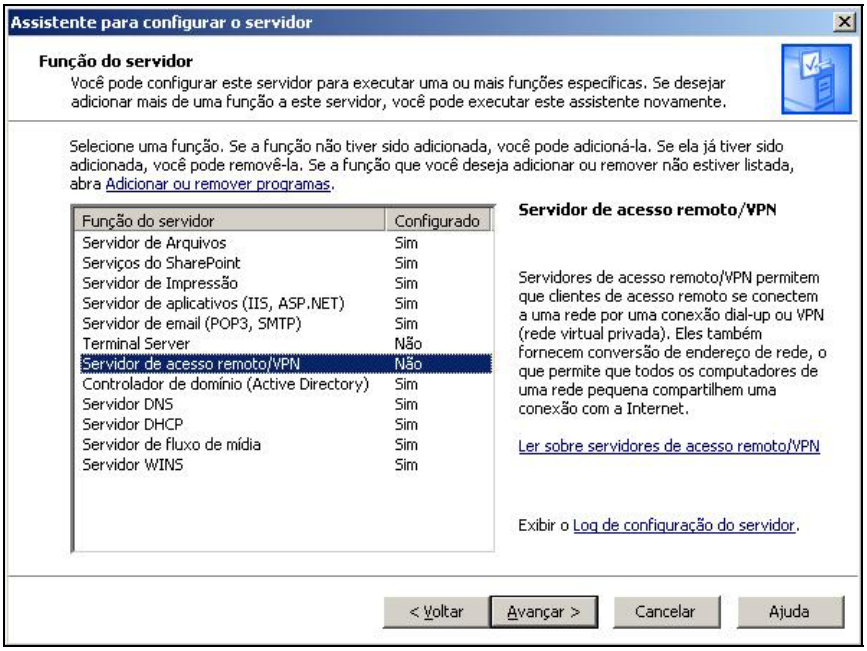


Servidor de acesso remoto/VPN

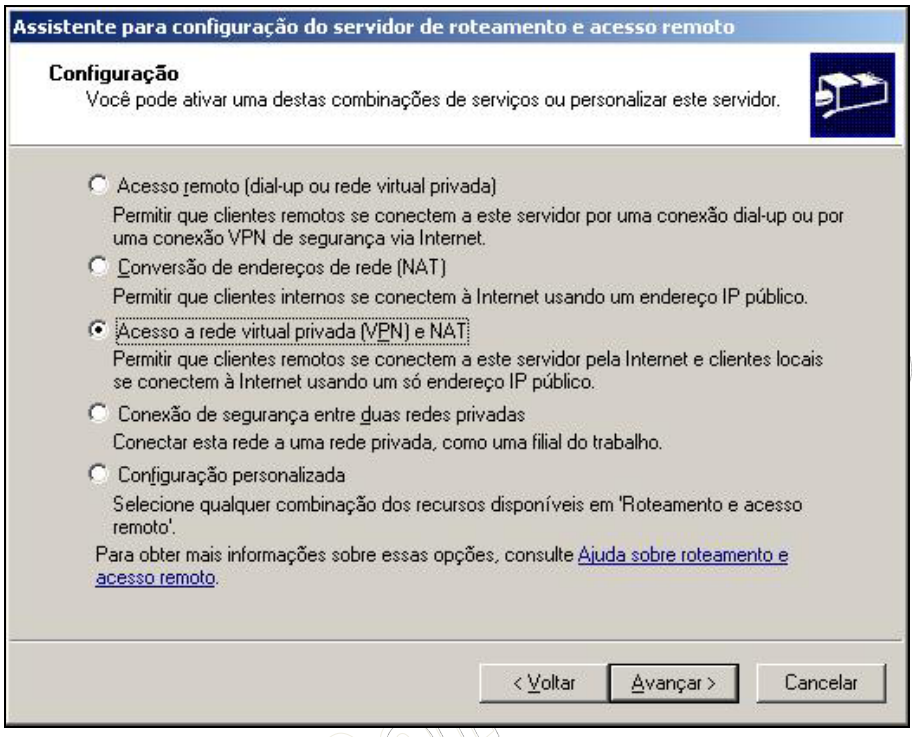
Falaremos agora de outro serviço também especializado, e que não deverá conviver com outros serviços em produção. É o servidor de acesso remoto ou VPN, Virtual Private Network. Com este serviço é possível realizar o compartilhamento de um link de Internet com todas as estações de trabalho e demais servidores da rede, ou seja, é transformar um servidor com Windows Server 2003 em um roteador de acesso a Internet. Para isso, este servidor precisará de um novo pré-requisito: a existência de pelo menos duas placas de rede distintas.

Além de provê o compartilhamento da Internet para a rede local este serviço também proporciona a criação ponto-a-ponto, com segurança, para a troca de informações entre dois hosts na Internet, como em um esquema de matriz e filial. A este tipo de arquitetura denominamos de VPN, que é a criação de um canal virtual tunelado (através de criptografia) sobre a infra-estrutura pública da Internet. A VPN pode ser de duas formas: Servidor-host, onde o servidor apenas aguarda a conexão de usuários externos, como notebooks; Servidor-Servidor, onde dois servidores (matriz-filial) estabelecem uma comunicação segura entre eles, de forma que as estações de cada uma das redes possam se comunicar com a rede remota, e onde todo o tráfego é criptografado através da Internet.

Vejamos então como instalar e configurar esse serviço:

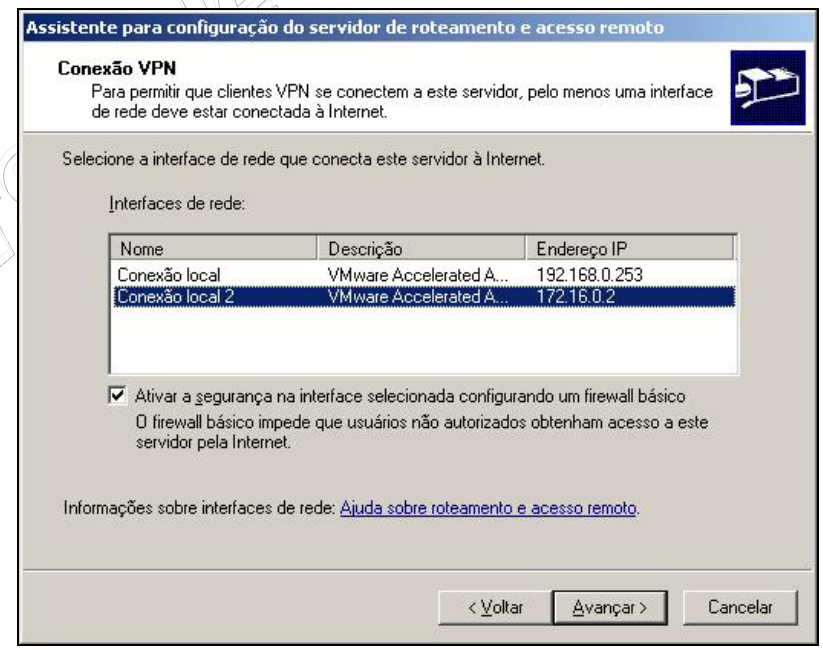


A primeira escolha a ser definida junto com o assiste é sobre o tipo de serviços a serem ofertados:



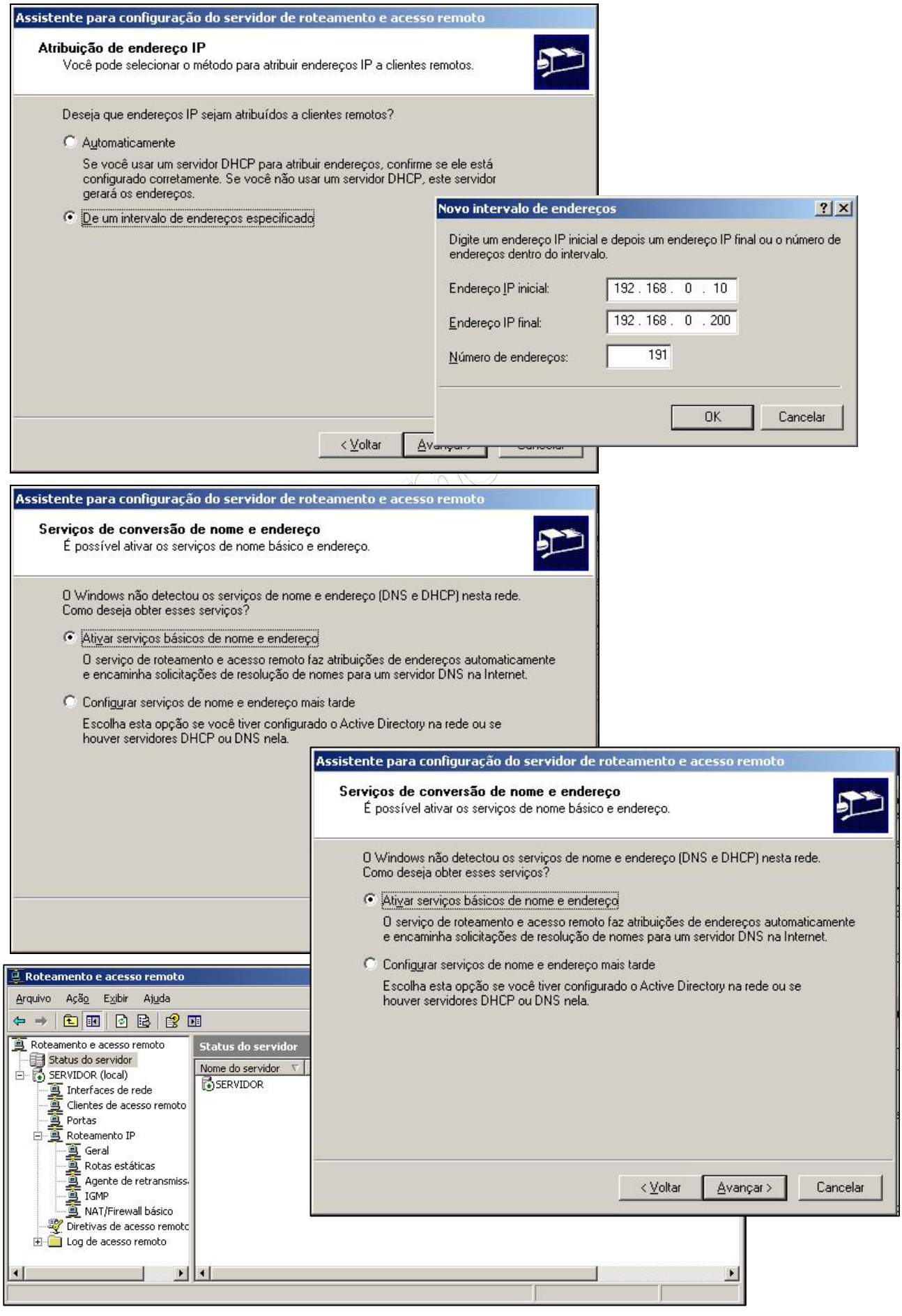
Exemplificaremos o servidor de acesso remoto através do uso do sistema VPN e NAT.

Selecione na próxima tela as interfaces de rede que estão ligadas ao roteador da Internet e a que está ligada a rede local. Não troque esses passos, caso contrário seu servidor não funcionará:



Por questões de segurança é altamente recomendável que você permita que o assistente ative o firewall básico do Windows. Este firewall atua sobre os pacotes que entram e saem do servidor e evite problemas como ataques de DoS (Denied of Service), exploração de bugs e vulnerabilidades.

Em seguida serão questionados os dados sobre a atribuição de endereços IP, DNS e formas de autenticação:



Uma vez concluído o assiste o servidor já estará realizando o compartilhamento da Internet, para isso, nas estações de trabalho da rede, configure os endereços do GateWay e DNS para este novo servidor de acesso remoto que acabamos de configurar. Uma alternativa prática, é alterar essas informações apenas no servidor de DHCP da rede e renovar os dados nas estações de trabalho.

Veremos agora o último serviço avançado do Windows Server 2003, o Terminal Server.

Terminal Server

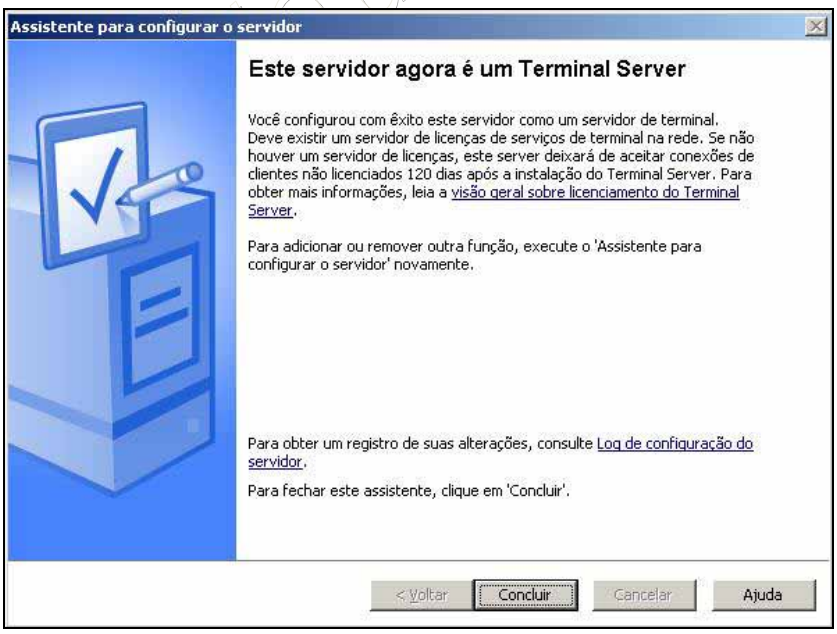
O Terminal Server se assemelha aos padrões originais das redes corporativas, onde eram utilizados mainframes e terminais de acesso. O Terminal Server provê um serviço centralizado para aplicações e dados, de forma que terminais (mas desta vez não são terminais burros, pois também podem realizar diversas outras atividades) realizem todas as suas atividades em um único servidor. Isso diminui consideravelmente o TCO (*Total Cost of Ownership*), como vimos na primeira competência, além de facilitar a manutenção dos sistemas e alguns aspectos de segurança.

Vejamos agora como instalar e configurar este último serviço:

Após utilizar o assistente de configuração do servidor será emitido um aviso importante:

Ao precionar o botão de OK o servidor será automaticamente reinicializado, dessa forma tenha cuidado para não perder dados ou trabalhos importantes.

Após ser reinicializado, o assistente apresentará uma tela de confirmação:

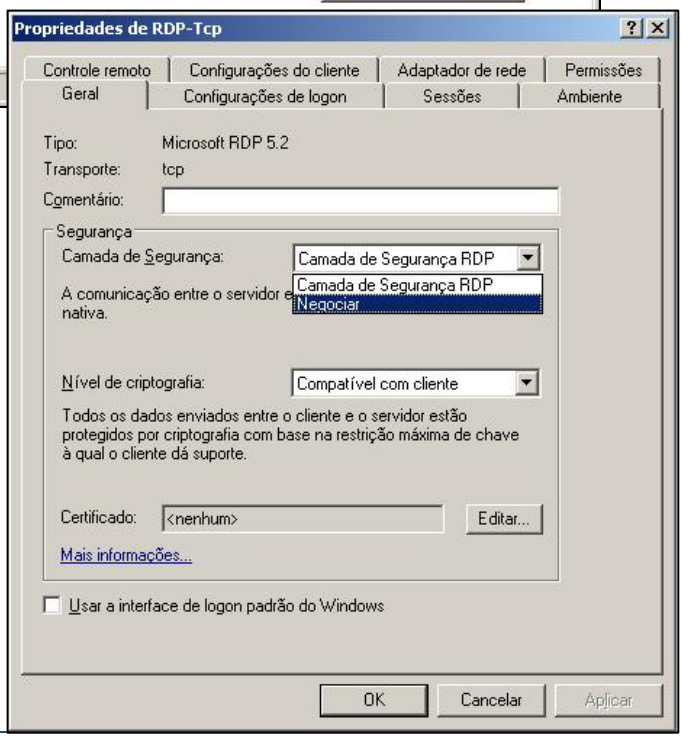


Junto ao “Gerenciar o servidor” você encontrará duas opções de administração: configuração dos serviços de terminal e gerenciamento das conexões de terminal. Vejamos inicialmente as configurações possíveis junto ao serviço de terminal:

Aqui podemos observer as configurações mais comuns, é importar salientar que as licenças de uso do Terminal Server são diferentes das licenças fornecidas com o Windows Server 2003. Ou seja, para cada conexão junto ao Terminal Server é necessário que o cliente tenha adquirido uma licença de acesso ao Terminal Server, que são comercializadas nas mesmas lojas onde se adquirem o Windows Server 2003.

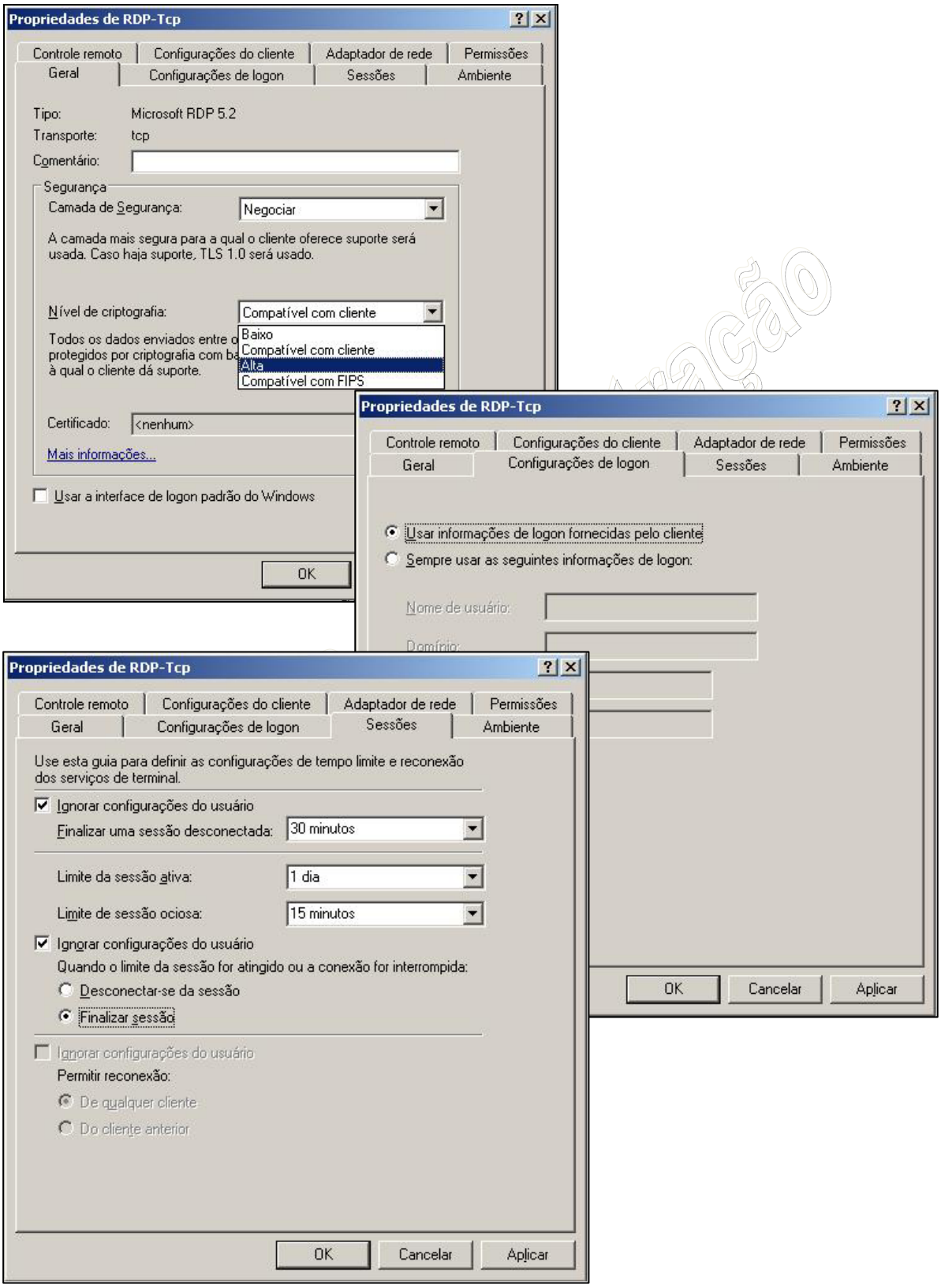
Por padrão, o Windows Server 2003, permite que você instale o opere por 120 dias o Terminal Server sem precisar instalar licenças de uso. Porém, após este período, o Terminal Server não aceitará mais conexões.

A parte mais importante do Terminal Server está nas propriedades do serviço RDP, que é o protocolo responsável pela existência desse serviço, e é de propriedade da Microsoft:



Vejamos agora os itens de configuração:

Por padrão o RDP é inicializado com uma camada de segurança da própria RDP, porém oferecendo uma baixa qualidade de criptografia. O ideal é a alterarmos esta configuração para “Negociar”, onde poderemos prover tanto a segurança básica do RDP quanto altos níveis de criptografia, conforme a disponibilidade no cliente.

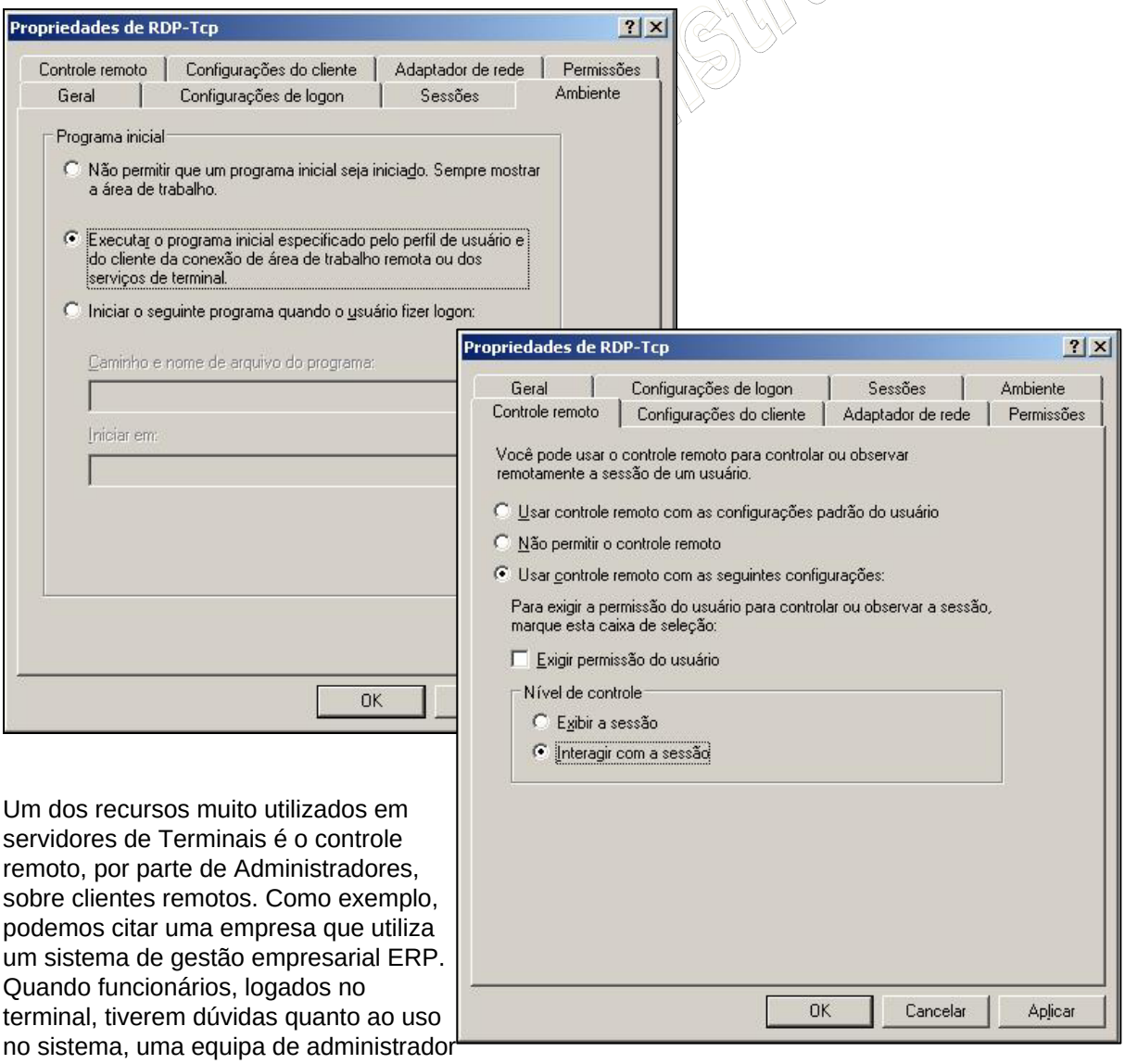


É possível controlar o tempo em que cada usuário permanece conectado ao sistema, de forma a evitar que funcionários deixem a sessão logada, mas sem uso, ocupando o espaço que poderia ser de outro funcionário ou congestionando o servidor com conexões zumbies. Uma boa prática é ignorar as configurações fornecidas pelos próprios funcionários e estabelecer limites, como uma forma de política.

É importante saber o seguinte: quando um usuário logado no Terminal Server, solicita para sair ou clica diretamente no “Fechar” da janela, ele não necessariamente está saindo do sistema. O Terminal Server possui um recurso que armazena na memória a sessão do funcionário durante algum tempo (configurado por você), chamado de Desconectar-se da Sessão. Caso o funcionário retorne dentro desse espaço de tempo, ele recuperará sua sessão da mesma forma como estava no momento de sua saída. Esse recurso é muito importante quando funcionários estão acessando através de conexões discadas, onde geralmente suas conexões são perdidas ou derrubadas várias vezes numa mesma sessão. Entretanto, funcionários também podem solicitar para “Finalizar a Sessão”, onde a mesma não ficará residente na memória do servidor após sua saída.

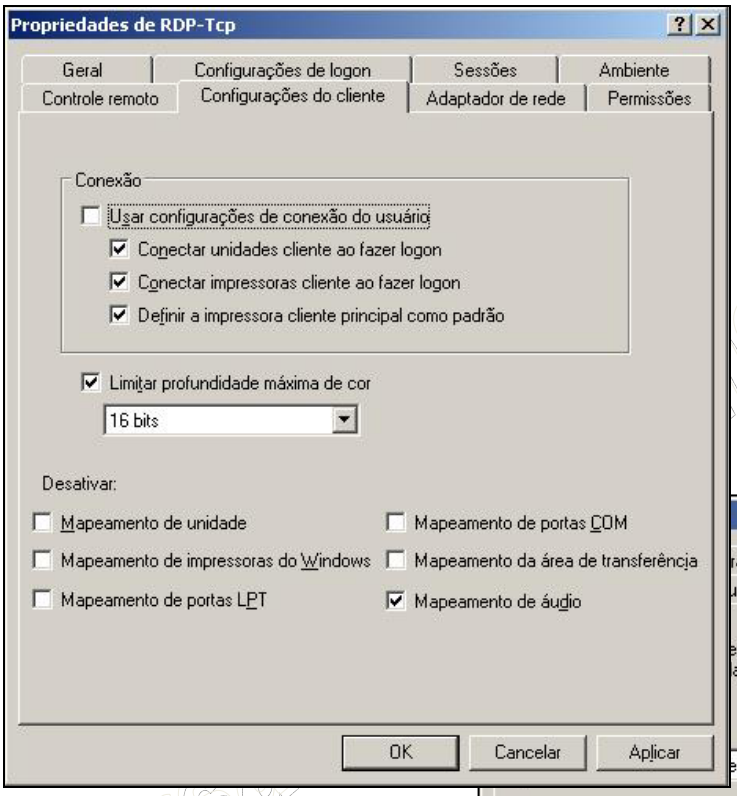
É possível determinar o tempo máximo em que uma sessão ficará ativa, ou online, em nosso caso estamos definindo em 1 dia esse limite e não permitindo que uma sessão permaneça conectada por mais de 15 minutos se ociosa.

É possível também executar scripts após o usuário acessar o Terminal, isso é útil quando se faz necessário instalar uma nova impressora local, do próprio Terminal Server, ou atualizar dados como antivírus, documentos e etc:



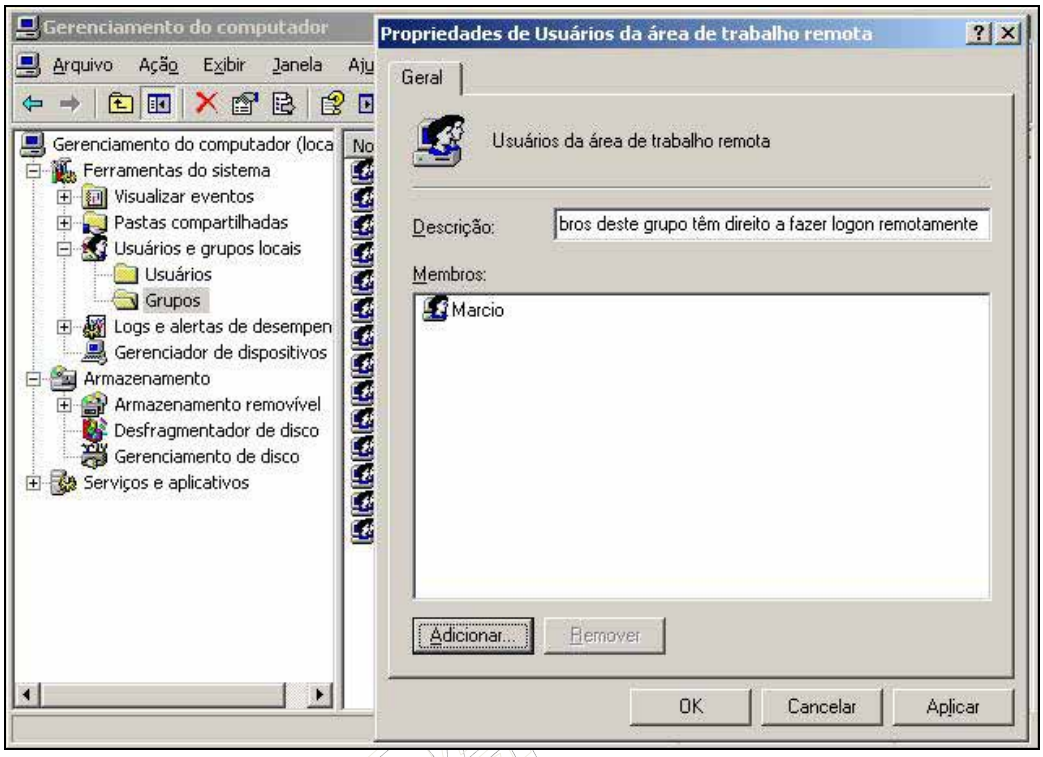
Um dos recursos muito utilizados em servidores de Terminais é o controle remoto, por parte de Administradores, sobre clientes remotos. Como exemplo, podemos citar uma empresa que utiliza um sistema de gestão empresarial ERP. Quando funcionários, logados no terminal, tiverem dúvidas quanto ao uso no sistema, uma equipa de administrador do sistema podem interagir com o funcionário na própria sessão remota e sanar as dúvidas.

Um outro recurso muito útil do Terminal Server é a possibilidade de uso dos recursos locais dentro do terminal remoto. Vamos supor que você esteja em Recife, e que a matriz, onde está localizado o Terminal Server, está em São Paulo. Em recife você possui uma impressora a laser conectada e configurada a sua estação de trabalho. Ao efetuar o logon no Terminal Server de São Paulo, dentre as impressoras existentes no ambiente de São Paulo, estará um link para a sua impressora local em Recife. Dessa forma, mesmo estando o servidor em outra localidade, você ainda poderá utilizar seus próprios recursos locais, como impressora, scanners, zip drivers, etc:

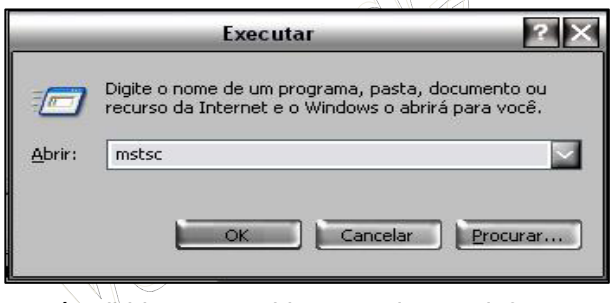


Por último, é possível estabelecer o número máximo de conexões, ou clientes, a conectarem com o nosso servidor. Isso é extremamente útil, visto que cada sessão equivale a um consumo fixo de memória RAM e processador (que vão variar conforme o tipo de aplicação que os usuários irão acessar remotamente – consulte o site da Mirosoft para maiores informações).

Após concluir as configurações do RDP você agora precisará liberar o acesso aos usuários que poderão efetuar logon no serviço de terminal. Para isso, siga o seguinte caminho: Iniciar -> Painel de Controle -> Ferramentas Administrativas -> Gerenciamento do Computador -> Usuários e grupos locais -> Grupos. Edite o grupo “Usuários da área de trabalho remota” e inclua os usuários que poderão acessar o terminal server:

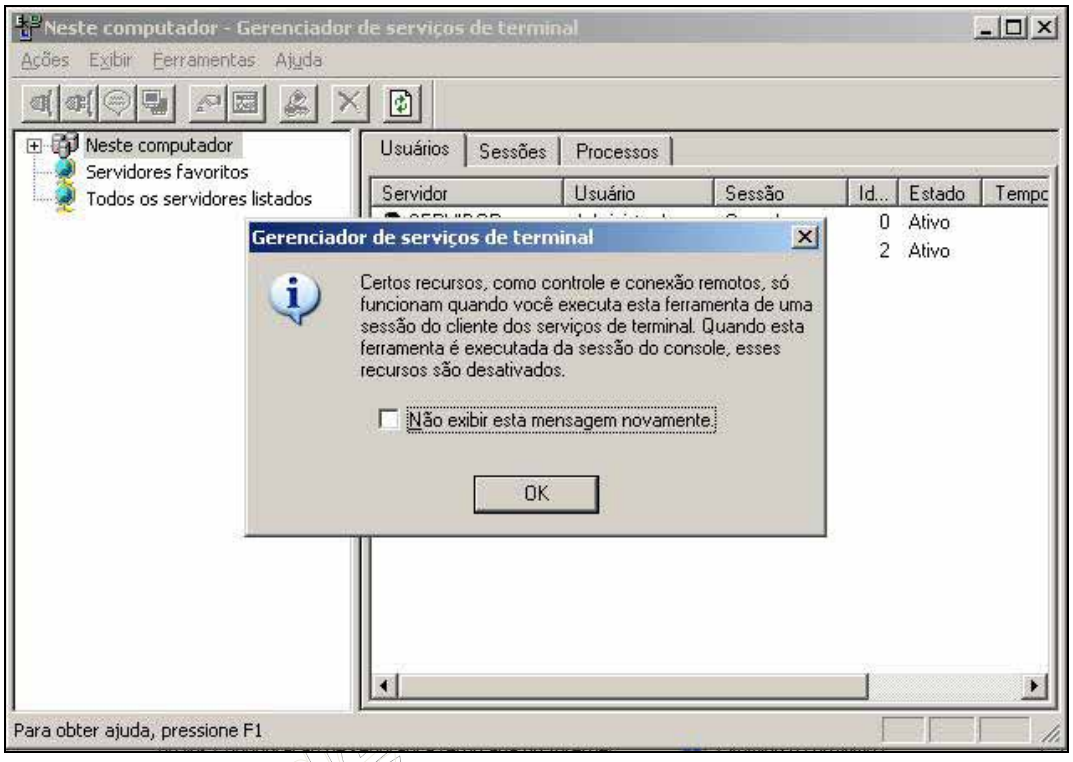


Agora que sabemos como configurar o Terminal Server, vejamos como conectar e como gerenciar as conexões conectadas. Em uma estação de trabalho qualquer digite o comando “mstsc” (de microsoft terminal server client):



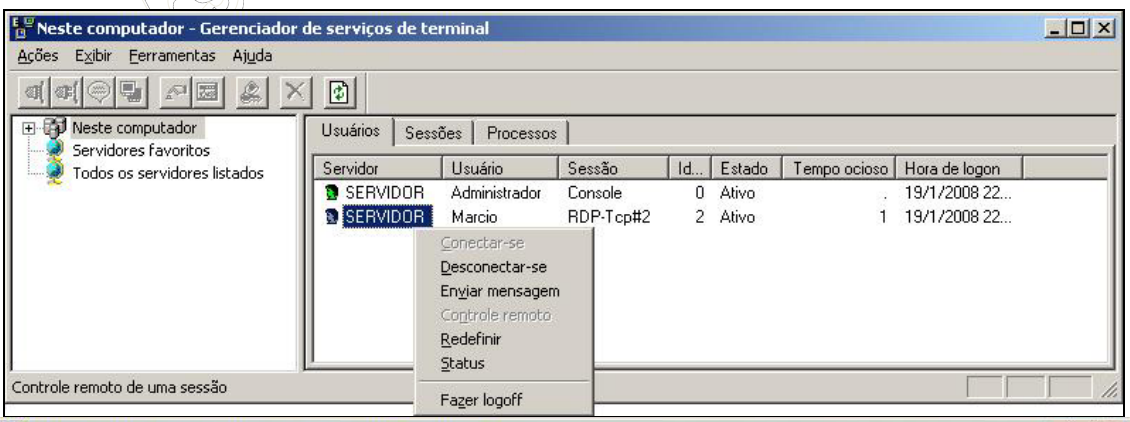
Será exibido em seguida uma tela para informar o endereço do servidor de terminal. E uma vez conectado, será apresentada a tela de logon do servidor Windows Server 2003 – Terminal Server:

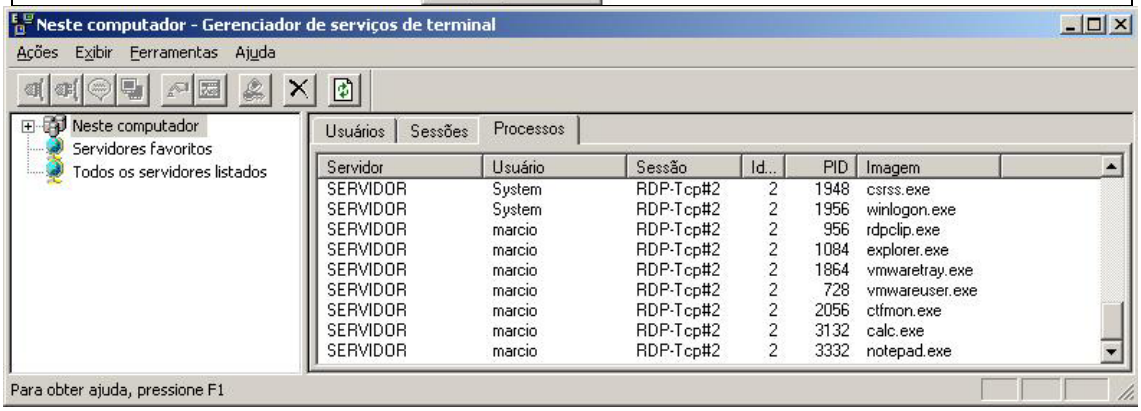
Como última atividade desta competência, vamos aprender a gerenciar as conexões conectadas via terminal server e saber como interagir com sessões remotas. Para isso acesse o “Gerenciar o computador” e na aba do Terminal Server clique em “Gerenciador de serviços de terminal”:



Observe que o aviso diz respeito a como realizar o controle e interação das sessões remotas. É preciso que você acesse o Terminal Server como Administrador, via utilitário mstsc, para ter esse controle. Diretamente via console você não poderá interagir com as sessões remotas.

Aqui você poderá visualizar os usuários conectados, tempo total de suas conexões, se estão ociosos e quais processos estão executando no servidor:





9 COMPETÊNCIA 3 – SISTEMAS OPERACIONAIS CLIENTES

9.1 FAMÍLIA DE SISTEMAS OPERACIONAIS CLIENTES

Agora que sabemos como operacionalizar os serviços de uma rede, vamos estudar como utilizar esses serviços em nosso dia-a-dia. Para começar, iremos estudar a evolução dos sistemas operacionais clientes ao longo dos anos, e aprofundaremos nossos estudos com a adoção do Windows XP Professional, por ser este ainda o mais utilizado nos dias de hoje.

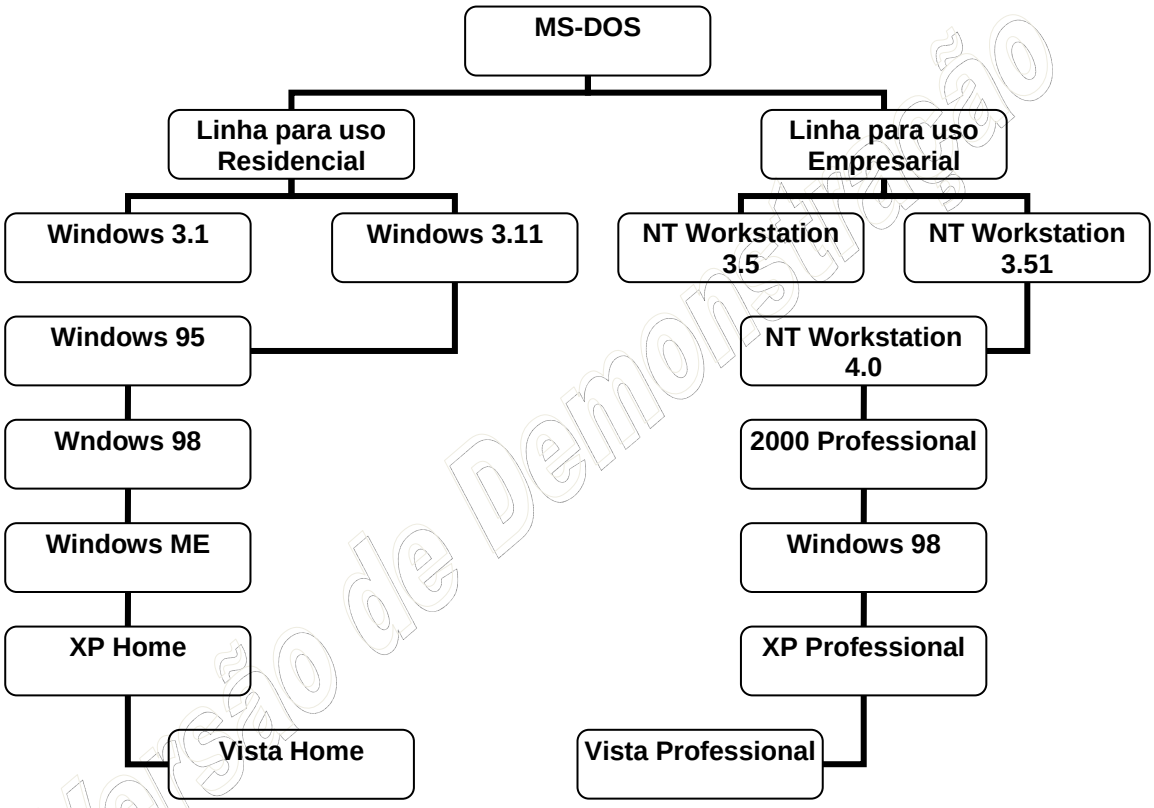


Figura. Família Windows para Estações de Trabalho no Brasil

A Microsoft inicia suas operações internacionais com o sistema operacional MS-DOS, de Microsoft Data Operation System, por volta de 1986. Sua criação está diretamente relacionada com a explosão de consumo e produção dos IBM/PC. Os primeiros computadores pessoais vendidos massivamente. O MS-DOS era composto apenas por uma interface de console, muito parecida com a interface não-gráfica dos Linux hoje em dia.

Relativamente simples de operar, possuía como núcleo principal de interação com o usuário o programa command.com, localizado na raiz do disco rígido. O command.com era uma coleção de outras ferramentas, como: dir, move, attrib, del, copy, mem, type, etc. Associado com outras ferramentas, como: deltree, format, fdisk, etc.

```
C:\>mem

Memory Type        Total   =   Used   +   Free
----------------  --------   --------   --------
Conventional         640K       76K       564K
Upper                 19K        0K        19K
Reserved               0K        0K         0K
Extended (XMS)*    31 661K    2 573K    29 088K
----------------  --------   --------   --------
Total memory       32 320K    2 649K    29 671K

Total under 1 MB      659K       76K       583K

Total Expanded (EMS)               32 000 (32 768 000 bytes
Free Expanded (EMS)*               29 328 (30 031 872 bytes

* EMM386 is using XMS memory to simulate EMS memory as needed.
  Free EMS memory may change as free XMS memory changes.

Largest executable program size       560K (573 520 bytes)
Largest free upper memory block        16K  (16 368 bytes)
MS-DOS is resident in the high memory area.
```

Como sucessor do MS-DOS, porém ainda dependente do MS-DOS, surge o Windows. As versões iniciais do Windows, 1.0 e 2.0, foram pouco utilizadas no Brasil. A primeira versão a tornar-se popular de fato foi o Windows 3.1, por volta de 1992. O sistema apresentava uma interface gráfica com ícones para interação com o usuário.

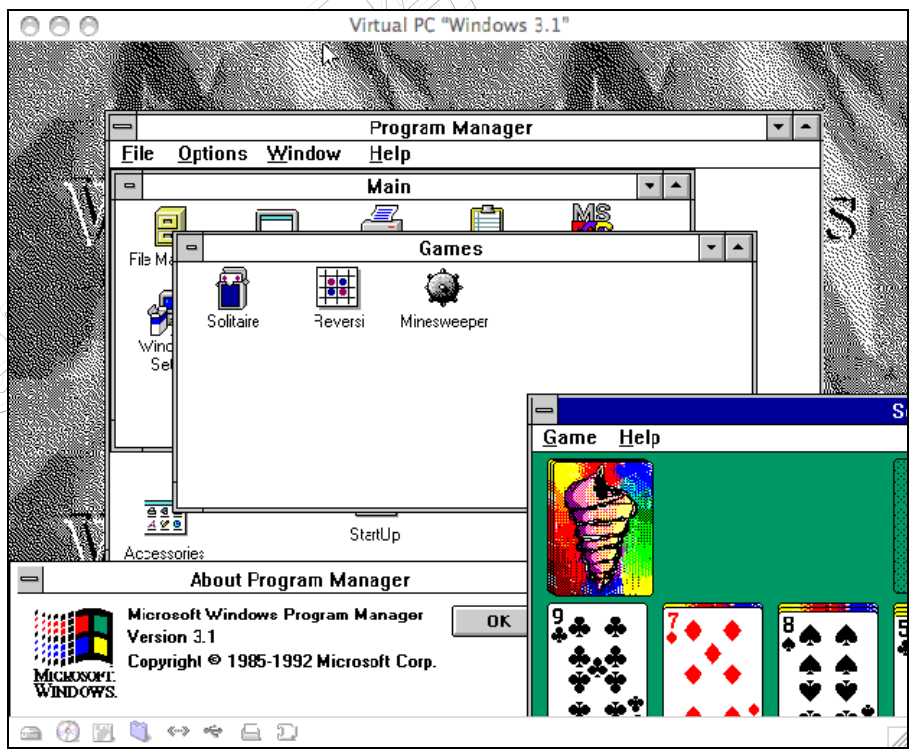
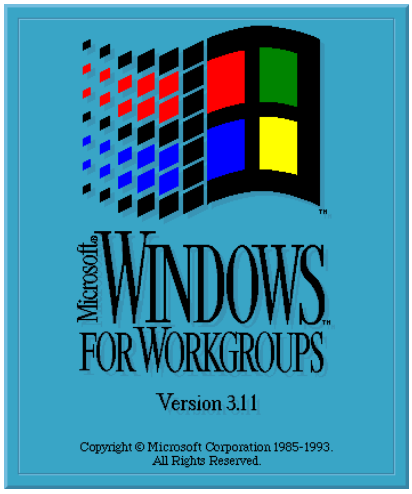


Figura. Windows 3.1

Para aqueles que tiverem a curiosidade de testar versões antigas do MS-DOS ou do Windows, é possível baixar gratuitamente no site da microsoft, http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx, o software de máquinas virtuais, o MS Virtual PC. O site http://www.kernelthread.com/mac/vpc/win.html, apresenta uma relação de sistemas possíveis de serem instalados no MS Virtual PC. Através do Virtual PC é possível instalar e executar outro sistema operacional sem precisar modificar nada em seu atual computador.

Uma observação importante sobre o Windows 3.1 é que ele não é classificado tecnicamente como um sistema operacional e sim como uma aplicação. Como aplicação ele depende do sistema operacional MS-DOS para poder ser executado. Muitos especialistas classificam o Windows 3.1 como mais do que uma aplicação, como um ambiente operacional, em função de que ele serve de suporte para a execução de várias outras aplicações que não podem ser executadas em MS-DOS nativo.

Por volta de 1993, com a evolução das redes de computadores e consequentemente a necessidade de compartilhamento de periféricos e arquivos, foi lançado o Windows 3.11, também conhecido como Windows for Workgroups.



As diferenças básicas em relação ao Windows 3.1 é que o Windows 3.11 fornecia um suporte melhorado para trabalho em rede e um pouco mais de estabilidade em relação ao Windows 3.1. Esta foi a última versão do Windows baseada na tecnologia de 16 bits.

Em 25 de Agosto de 1995 uma nova revolução mudaria os computadores para sempre. Lançado o Windows 95. Um sistema operacional baseado na tecnologia de 32 bits, com uma interface completamente nova em relação às versões anteriores do Windows. O botão Iniciar, a barra de tarefas, o explorer, entre outros elementos que hoje são muito bem conhecidos, foram novidades trazidas pelo Windows 95. Nesta mesma época a Microsoft já disponibilizava versões do NT Workstation e do NT Server, indicados para uso empresarial das estações de trabalho em rede.

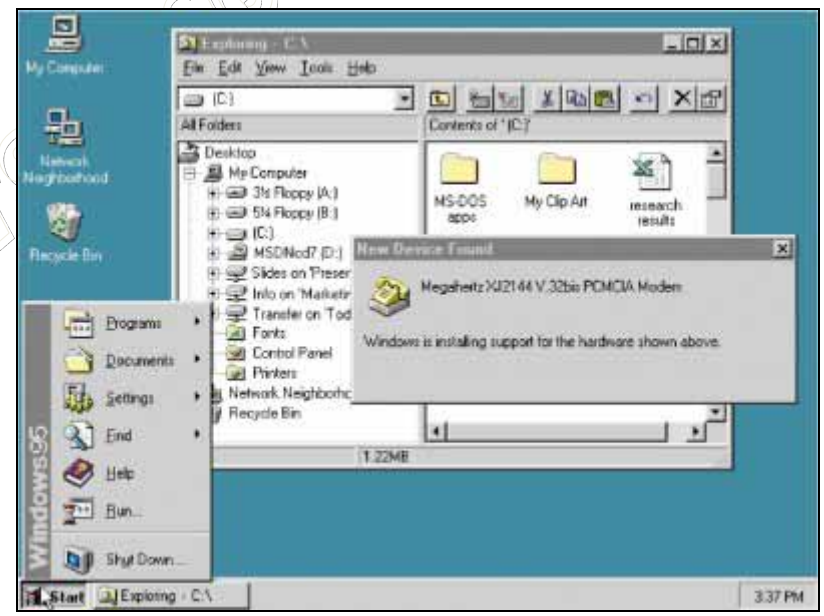
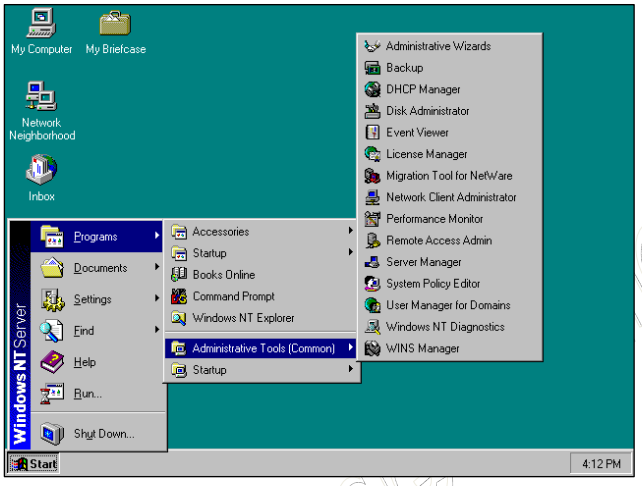
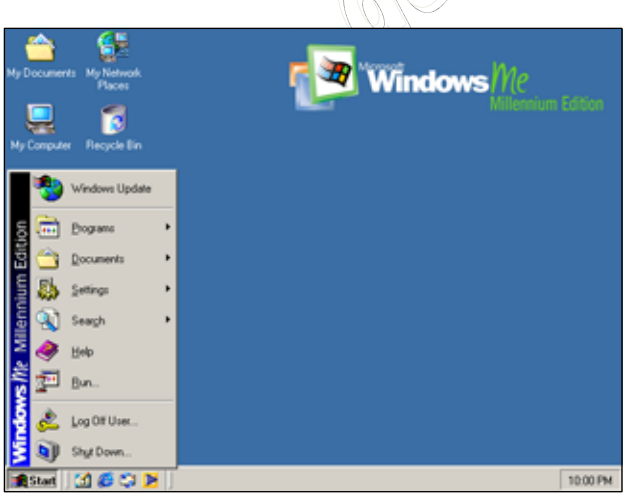


Figura. Windows 95

A estratégia da Microsoft em trabalhar com duas linhas de produção, Windows 3.1 ou 95 e NT, geraram confusões e problemas entre os usuários. Por um lado, a Microsoft defendia que a linha empresarial precisava ser mais estável, ou seja, menos susceptível a erros de softwares ou drivers. Para isso compilou o seu kernel com poucas opções de periféricos, aumentou a segurança contra a execução de aplicativos e aumentou o suporte às tecnologias de rede existentes. Por outro lado, isso tornou o NT um sistema de difícil operação, pouco atrativo e de fato voltado para aplicações exclusivamente empresariais. Usuários domésticos que se aventuraram a usar NT acabaram percebendo a necessidade de hardware mais potente, jogos não eram executados, muitos aplicativos legados do Windows 95 não eram mais suportados no NT. Em fim, o NT começou a receber muitas críticas, ora positivas pela estabilidade e segurança, ora negativas pela ausência de suporte a softwares e periféricos, e necessidade de hardware mais potente para ser executado.



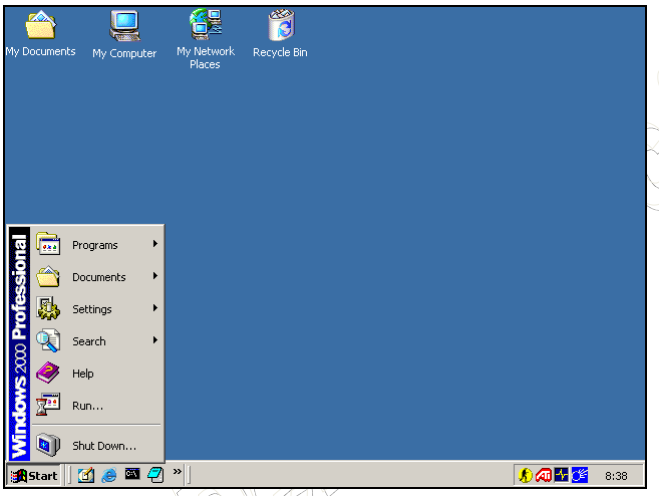
Neste momento a Microsoft já falava em unificar as duas linhas do Windows. Uma nova versão do NT foi lançada: NT Workstation 4.0 e NT Server 4.0. Esta era a versão do NT baseada na tecnologia de 32 bits e com cara de Windows 95. Melhorias substanciais foram feitas em relação a versão anterior do NT. Muitos acreditaram ser esta a versão unificada prometida, tanto que muitas empresas e usuários domésticos começaram a adotar o NT Workstation 4.0 como sistema operacional para as estações da rede e seus computadores pessoais.



Contudo, a robustez do NT persistia, e usuários residenciais começaram a perceber as vantagens que o Windows 95 ainda trazia em relação ao novo NT 4.0, em relação a jogos e periféricos. O golpe final de decisão entre o Windows 95 ou o NT 4.0 aconteceu com o lançamento do Windows 98 e em seguida do Windows ME. O Windows 98 trouxe melhorias significativas em relação ao Windows 95, como estabilidade, segurança e suporte a novos hardwares, contudo sem muitas novas aplicações.

O Windows ME, Millenium Edition, por sua vez, trouxe inovações nos assistentes de instalação, recursos visuais, suporte a novas tecnologias como PnP e USB. Era visualmente mais agradável, porém requisitava um hardware mais robusto. Tornou-se a primeira opção de consumo pelo fato de que o Windows 98, com seus diversos patches de atualizações, já não estava mais sendo suportado em funções de problemas de segurança na Internet e vírus.

Paralelamente ao Windows ME, e mantendo a divisão das linhas de produtos, a Microsoft lança o Windows 2000, nas edições Professional e Server. Embora muitos duvidassem da aceitação do Windows 2000, o fato é que a aceitação deste foi um grande sucesso e muitas empresas adotaram a nova versão. O objetivo inicial da Microsoft era que o Windows 2000 realizasse o sonho da unificação entre as duas linhas do Windows. Algumas integrações já estavam acontecendo, como por exemplo, um modelo de Drivers para dispositivos de Hardware comum às duas linhas, drivers estes baseados na tecnologia WDM – Windows Driver Model, utilizada tanto no Windows 98 quanto no Windows 2000.



Em 2001 foi lançado o Windows XP. Segundo a Microsoft XP de Experience. O Windows XP, lançado em duas versões: Home e Professional, representa o passo mais importante da Microsoft rumo a unificação das duas linhas do Windows. O XP apresenta uma interface completamente nova, combinando a facilidade do Windows 95/98/Me, com a estabilidade, confiança e segurança do Windows 2000.

Com o desenvolvimento de novas tecnologias para hardwares de servidores, a entrada de novos players no mercado da computação corporativa, e a grande demanda de consumo de todo tipo de empresa sobre a linha corporativa, a Microsoft opta em manter a divisão de sua linha de produtos. Lança em 2003 o Windows Server 2003.

Em 2007 são lançadas as novas versões do Windows para usuários: Vista. E com promessas de lançamento de um novo Windows Server 2008 em 2008. Com estes anúncios a Microsoft oficializa o não interesse em separar as linhas de produtos Windows.

O Windows Vista já é ofertado no mercado Brasileiro através de seis edições:

- Vista Starter Edition: versão voltada para usuários não experientes e sem recursos aprimorados como as janelas rotativas em 3D (Aero), é a versão voltada para o público mais carente financeiramente;
- Vista Home Basic: similar ao XP Home Edition, voltada para usuários residenciais, com pacotes extras de aplicativos anti-malwares e recursos avançados de multimídia, porém não provê suporte nem serviços para operações em rede (em especial com Active Directory);
- Vista Home Premium: versão aprimorada da Home Basic, provendo maior suporte para recursos multídias, suporte para HDTV (Televisão Digital de Alta Definição) e o software Windows Media Center, utilizado para controlar o computador através de televisões;
- Vista Business: similar ao XP Professional, versão voltada para empresas de pequeno e médio porte. Conta com serviços e ferramentas de terceiros ou da própria Mirosoft para operações em rede;
- Vista Enterprise: ofertado para as empresas de grande porte, oferece nativamente suporte ao Virtual PC, software de máquinas virtuais; interface com suporte a múltiplos idiomas e a possibilidade de fazer backups ou encriptar grandes volumes de dados;
- Vista Ultimate: a edição mais completa. Tem todas as funcionalidades das versões anteriores e novos serviços online ligados a música, filmes e entreterimento doméstico, incluindo ferramentas para aumentar a performance dos jogos eletrônicos.

Um detalhe especial é que todas as versões do Windows Vista vêm no mesmo DVD de instalação, sendo que a versão a ser instalada depende do CD Key digitado. Será possível atualizar de uma versão a outra, apenas precisando comprar um novo CD Key, que inutilizará o outro. A única exceção ocorre com o Windows Vista Starter Edition, nesta versão, você poderá apenas instalar a nova versão sobre a Starter Edition porém, inutilizando as configurações e programas instalados anteriormente. Existe uma versão em CD do Vista Starter que não possui as outras versões.

9.2 REQUISITOS DE HARDWARE E SOFTWARE

O conhecimento sobre as exigências de hardware e software para a execução de um sistema operacional cliente de rede é de extrema importância, pois uma escolha errada irá impactar diretamente na operação da empresa.

Vamos analisar três exemplos para compreendermos a necessidade da escolha certa do sistema operacional cliente de rede:

- Um banco, com 500 estações de trabalho, optou em homologar para toda a rede o sistema operacional Windows 98. O Motivo foi claro e unânime para todo o corpo de TI: as estações de trabalhos eram máquinas antigas, IBMs de 1994, com 32 MB de RAM, 10 GB de HD e processadores Intel Pentium 100 MHz. O sistema interno do banco era uma aplicação proprietária rodando em plataforma de 16 bits, ou seja, necessitava de uso exclusivo do processador. Se fosse escolhido o Windows XP as máquinas ficariam mais lentas e os novos recursos de 32 bits do XP não seriam aproveitados, pois a aplicação principal é de 16 bits;
- Um segundo banco, com 600 estações de trabalho, optou em realizar o upgrade dos Windows 98 para Windows XP. O Motivo foi claro e unânime para todo o corpo de TI: as estações de trabalhos não eram máquinas muito poderosas, IBMs de 2000, com 64 MB de RAM, 20 GB de HD e processadores Intel Pentium III 800 MHz. O sistema interno do banco também era uma aplicação proprietária rodando em plataforma de 16 bits, porém já haviam planos para uma migração completa deste sistema para um novo sistema de gestão empresarial em rede (ERP). Se fosse mantido o Windows 98, o novo sistema não poderia funcionar com todos os recursos de segurança, como garantia de autenticação em rede, e se fosse escolhido o Vista, as estações de trabalho não suportariam a exigência mínima de hardware;
- Um terceiro banco, com 700 estações de trabalho, optou em realizar o upgrade dos Windows 98 para Windows Vista. O Motivo foi claro e unânime para todo o corpo de TI: as estações de trabalhos seriam substituídas por versões modernas, de 64 bits, para rodar com o recém implantado sistema ERP, em redes. O Windows XP não garantia o uso de aplicações 64 em sua recém lançada versão de 64 bits, dessa forma o banco ficaria desprovido das garantias do fornecedor do sistema operacional cliente de rede;

Como se vê, ainda hoje existe motivos para se ter que analisar qual a versão do sistema operacional de redes clientes a ser homologado para a rede em produção. Mudanças em infra-estrutura ou em sistemas corporativas levam a necessidade de reavaliação dos hardwares das estações de trabalho.

Vejamos agora os principais recursos de hardwares exigidos pelos principais sistemas operacionais de rede cliente:

Versão do Windows	Memória Mínima	Memória Recomendada	Espaço Livre em HD	Processador Mínimo
Windows 98	16 MB	32 MB	170 MB	100 MHz, 32 bits
Windows ME	32 MB	64 MB	320 MB	300 MHz, 32 bits
Windows 2000	64 MB	128 MB	760 MB	300 MHz, 32 bits
Windows XP Pro	64 MB	128 MB	1500 MB	400 MHz, 32 bits
Windows Vista Business	512 MB	1000 MB	6000 MB	1.5 GHz, 32/64 bits
Windows Vista Enterprise	1000 MB	2000 MB	15000 MB	2.0 GHz, 32/64 bits
Windows Vista Ultimate	2000 MB	40000 MB	15000 MG	2.0 GHz, 64 bits

9.3 PRINCIPAIS FERRAMENTAS

Analisaremos agora as principais ferramentas utilizadas para acesso as redes, focaremos o uso sobre o Microsoft Windows XP Professional, em função deste ainda ser o sistema em maior uso na atualidade e provavelmente, em função do atual mercado de hardwares, a versão a ser predominante nos próximos 3 anos nos ambientes corporativos em rede.

Antes de começarmos, é importante ressaltar que estações de trabalho em redes não estão limitadas ao uso por apenas um único funcionário. É muito comum que durante o dia, mais de um funcionário utilize a mesma estação de trabalho, como no caso de empresas que possuem dois turnos para uma mesma função em departamento. Um funcionário utiliza a máquina pela manhã e, a tarde, um segundo funcionário a utiliza. Isso torna os recursos de acesso a rede mais complexos, pois precisam proteger tanto os dados do usuário 1 quanto do usuário 2, ao mesmo tempo em que libera ou restringe o acesso as recursos compartilhados em rede por usuário, e não por estação de trabalho.

As ferramentas que analisaremos são as ferramentas que não existem nas versões para usuário doméstico do Windows, e que existem tanto no XP quanto no Vista, e que são utilizadas para operações em estações de trabalho em rede:

- Controle de permissão de pastas e arquivos em partições NTFS;
- Remote Desktop;
- Diretivas de Segurança Local;
- Internet Information Services (IIS);
- Utilitário de Fax;

Controle de permissão de pastas e arquivos em partições NTFS

A partir do Windows NT/2000 um novo recurso está disponível: compartilhar recursos (pastas, arquivos) localmente ou na rede com maior segurança. É o controle de acesso, que permite selecionar quais usuários terão permissão para acessar o objeto compartilhado. O controle de acesso é feito através de permissões: NTFS e de compartilhamento.

As permissões NTFS são válidas tanto localmente (no próprio PC) quanto para a rede : quando um usuário fizer logon, seja no mesmo PC ou em outro qualquer, ele só poderá acessar o recurso compartilhado se tiver permissões adequadas.

As permissões de compartilhamento só têm efeito ao acessar recursos compartilhados na rede, mas não no próprio PC.

As permissões NTFS permitem atribuir permissões a pastas e arquivos, conferindo um alto grau de segurança e controle de acesso a nível de usuário. Têm efeito localmente e através da rede. As permissões definem o tipo de acesso concedido a um usuário ou a um grupo para um objeto: arquivos e pastas, chaves do registro, serviços, impressoras.

É um mecanismo de segurança que determina quais usuários ou grupos estão autorizados a executar quais operações em um objeto.

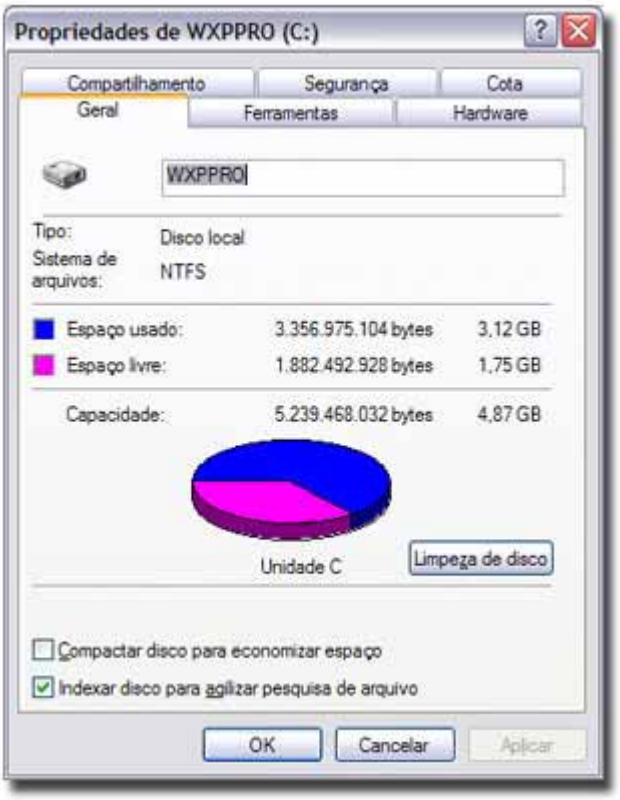
Você pode permitir ou negar acesso aos recursos compartilhados. Você também pode permitir somente permissões adequadas a um usuário: controle total, modificar, ler e executar, listar conteúdo de pastas, ler e gravar.

Como exemplo podemos citar:

1. É possível atribuir permissões a uma impressora compartilhada na rede ou localmente: somente usuários autorizados poderão imprimir, gerenciar e outras pessoas poderão ter suas permissões negadas e não poderão imprimir documentos;
2. É possível atribuir permissões a pastas e arquivos no mesmo PC: seus documentos só poderão ser visualizados a usuários com a permissão de leitura, delegados por você, e ninguém poderá alterá-los, exceto você.

Como pré-requisito para operação dos controles de permissões é necessário: que a unidade que contém as pastas e os arquivos devem estar formatadas em NTFS (WinNT e WinXP) ou NTFS 5 (Win2000 Server) e rodando um sistema operacional Win2000 ou superior.

Para confirmar o tipo de sistema de arquivos formatado em uma unidade de disco: No Windows Explorer, selecione a unidade e clique com o botão direito / Propriedades. Na guia Geral veja Sistema de arquivos.



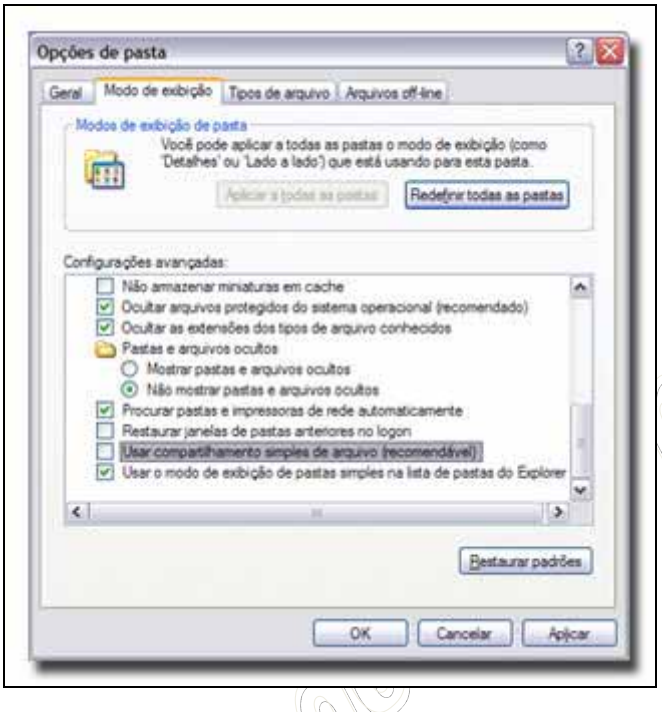
A partição formatada em NTFS tem outras vantagens em relação a FAT32 : segurança (definição de cotas de disco, auditoria de objetos, criptografia, journaling e controle de acesso), espaço livre (compactação de dados), suporte a arquivos com mais de 4 Gb e desempenho.

A única desvantagem é a compatibilidade : o sistema de arquivos NTFS só é reconhecida pelo WinNT, Win2000 e WinXP, enquanto o sistema de arquivos FAT32 é compatível com todos os Windows, exceto WinNT, e versões mais antigas do MS-DOS. Veja mais nessa matéria FAT32 X NTFS.

Podemos falar agora de nível de acesso, como sendo o controle de acesso de usuários e grupos a determinados objetos. Exemplo:

- Um usuário pode ter acesso ao conteúdo de um arquivo, outro fazer alterações, e um outro grupo nem poderá acessar o arquivo do mesmo PC.

Para Alterar permissões de pastas: No Windows Explorer clique com o botão direito no nome da pasta e clique em Compartilhamento e segurança... e na guia Segurança. Se você for membro de um grupo de trabalho e deseja visualizar a guia Segurança, abra o Painel de Controle e clique em Opções de pasta. Na guia Modo de exibição > Configurações Avançadas, desmarque Usar compartilhamento simples de arquivo (recomendável).



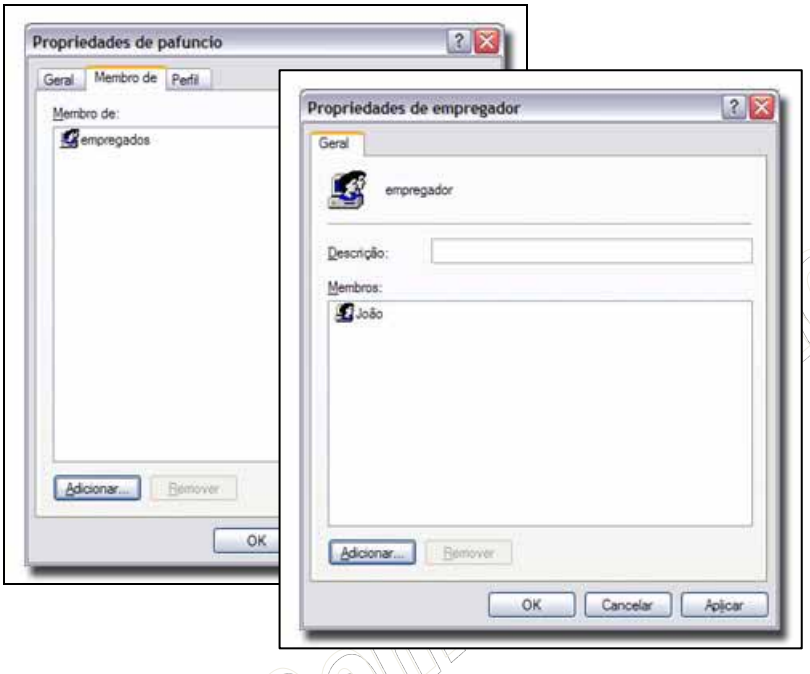
Algumas observações sobre as propriedades de objetos:

- Proprietários: Todos os objetos têm um proprietário, que por padrão é o criador do objeto. O proprietário poderá sempre alterar as permissões, independentemente das permissões definidas ao objeto;
- Herança: As permissões são automaticamente herdadas do objeto pai. Exemplo : uma subpasta herda as mesmas permissões da pasta que está contida; os arquivos criados dentro de uma pasta herdam as permissões da pasta. Esse recurso permite gerenciar e atribuir permissões com agilidade e facilidade;
- Operações: Ao copiar ou mover um objeto de uma partição para outra, as permissões serão perdidas e as novas serão herdadas do objeto pai. Se a operação for na mesma partição, as permissões serão mantidas. Ao copiar um objeto compartilhado (com permissões) de uma partição NTFS para outra FAT ou FAT32, as permissões serão perdidas;
- Tipo de objetos: As permissões são diferentes dependendo do tipo de objeto (pastas, arquivos ...). As permissões de ler, modificar permissões, alterar proprietário e excluir são comuns a todos os objetos;

Para realizar o compartilhamento de pastas execute os passos a seguir:

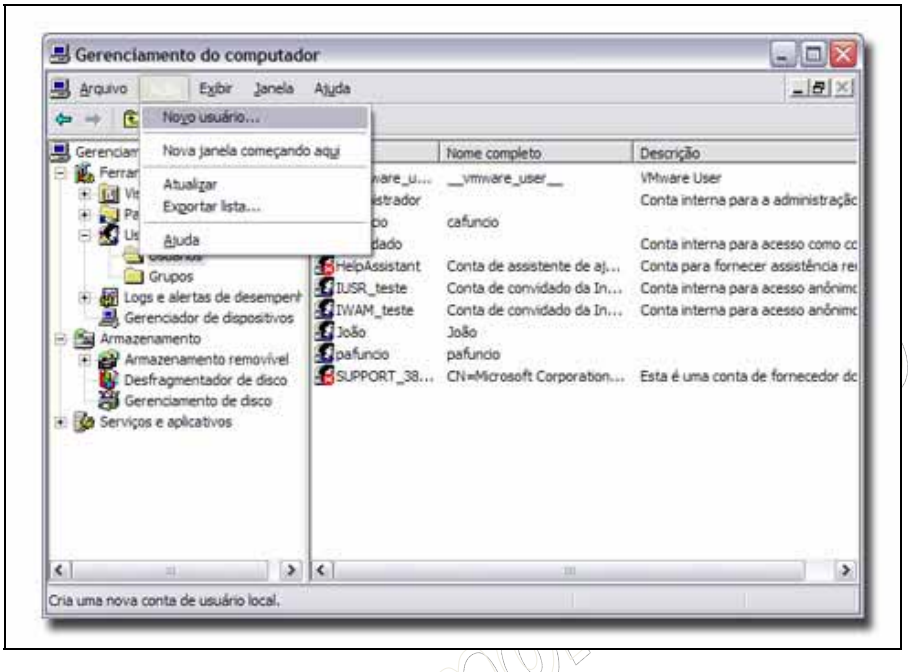
1. Faça logon como Administrador (ou usuário que tenha permissões de administrador) onde se encontra a pasta a ser compartilhada e serão definidas as permissões NTFS;

2. Criando grupos e usuários

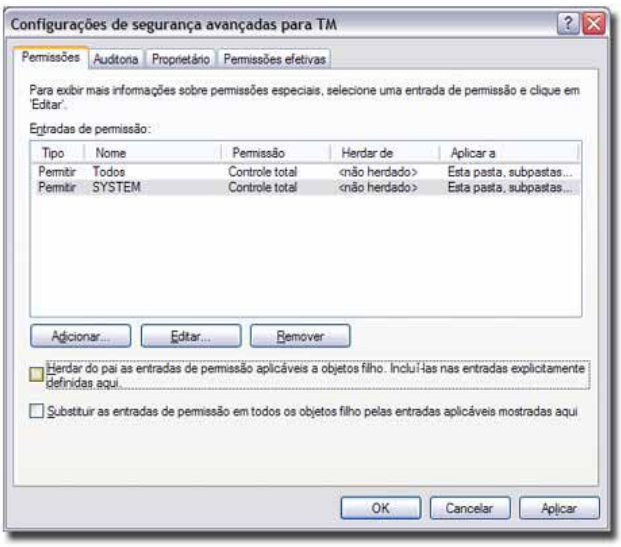


Crie dois grupos : empregados e empregador, e adicione os usuários cafuncio e pafuncio aos empregados, e João ao empregador. Para criar um novo grupo, abra Painel de Controle > Ferramentas Administrativas > Gerenciamento do computador. Clique na árvore de console e, em seguida em Usuários e grupos locais. Clique em Grupos e, em seguida, clique em Ação > Novo grupo

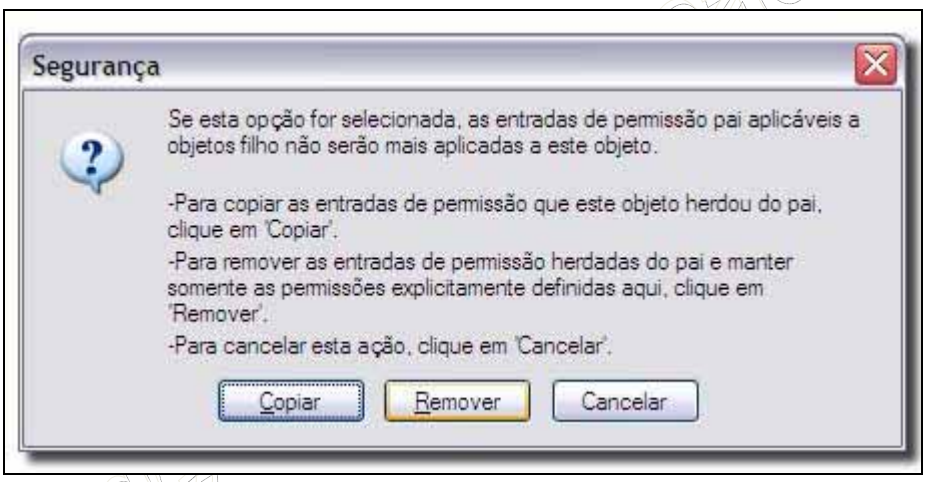
Para criar um novo usuário, siga os passos acima (com uma exceção : na árvore de console, clique em Usuários, e não em Grupos). Adicione cada usuário ao seu respectivo grupo ...



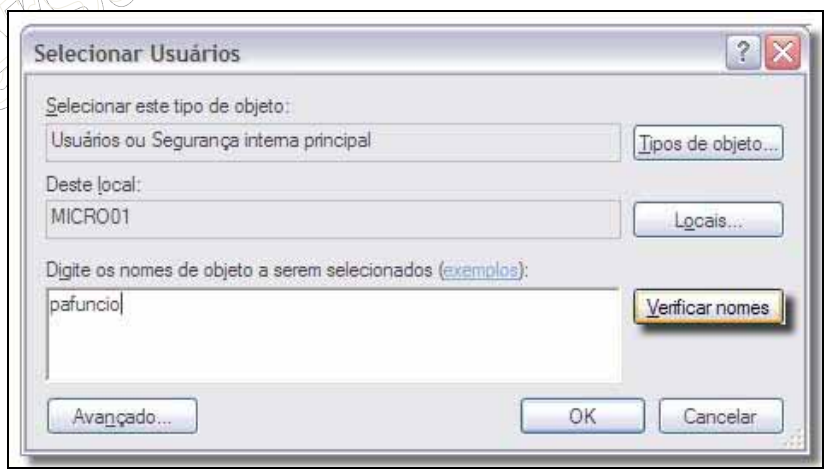
3. Criando permissões: Abra o Windows Explorer e localize a pasta para o qual você deseja definir permissões. Clique com o botão direito do mouse no arquivo ou pasta e abra a folha de Propriedades. Clique na guia Segurança. As permissões NTFS são atribuídas na guia Segurança, e as permissões de compartilhamento na guia Compartilhamento. Se você for membro de um grupo de trabalho e deseja visualizar a guia Segurança, abra o Painel de Controle e clique em Opções de pasta. Na guia Modo de exibição > Configurações Avançadas, desmarque Usar compartilhamento simples de arquivo (recomendável).Observe que todas as caixas de seleção estão sombreadas, e não é permitido modificá-las.
4. O comportamento padrão do Win2000/XP é herdar as permissões do objeto pai (veja Propriedades de objetos > Herança). Há três maneiras de efetuar alterações nas permissões de um objeto:
    - Selecionar a permissões oposta (Negar);
    - Alterar as permissões do objeto pai (as permissões serão herdadas para o objeto filho);
    - Desativar a herança de permissões:



Para desativar as heranças de permissões: Clique em Avançado e na guia Permissões. A coluna Tipo indica o tipo da permissão (Permitir ou Negar); a coluna Nome lista os usuários e os grupos com a respectiva permissão (coluna Permissão). A coluna Herdar de lista a pasta do objeto pai de onde as permissões foram herdadas. A coluna Aplicar a lista as pastas e subpastas às quais uma permissão será aplicada. Desmarque a caixa de seleção Herdar do pai as entradas de permissão aplicáveis a objetos filho. Incluí-las nas entradas explicitamente definidas aqui. Se desejar copiar as permissões herdadas e incluí-las como permissões explícitas (sem herança e que podem ser modificadas pelo administrador), clique em Copiar. O objeto deixará de herdar as permissões do objeto pai. Se deseja removê-las, clique em Remover (somente as permissões explícitas serão mantidas):

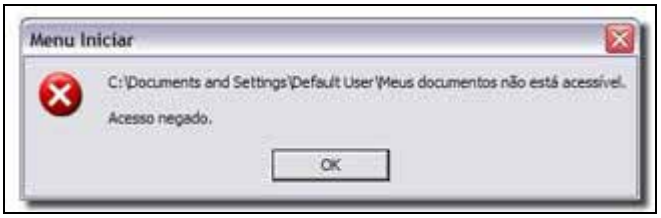


5. Atribua permissões: Clique em OK e retorne. Delete o grupo Usuários (que por padrão é atribuído a qualquer novo usuário criado). Adicione o grupo empregados (atribuir permissões a um grupo é mais rápido e eficiente) ao invés de atribuir aos usuários cafuncio e pafuncio. Atribua as permissões Ler & Executar, Listar Conteúdo da pasta e Leitura:



Adicione o usuário João e atribua permissão de Controle Total : observe que todas as caixas de seleção abaixo são selecionadas:

6. Teste local (no próprio PC): Faça logoff de Administrador (ou de um usuário que tenha permissões de administrador) e faça logon como pafuncio ou cafuncio, que têm as mesmas permissões. Abra o Windows Explorer e localize a pasta para a qual você definiu permissões. Tente acessar a pasta : você conseguirá listar o conteúdo da pasta e subpastas e ler os arquivos (as permissões foram aplicadas a esta pasta, subpastas e arquivos). Tente gravar algum arquivo : Acesso negado ! Os usuários cafuncio e pafuncio pertencem ao grupo empregados, que não tem permissões suficientes para gravar:



Faça logon como João e repita os passos acima. O usuário João tem permissão Controle Total, que permite que grave arquivos na pasta objeto. Esses procedimentos acima podem ser usados em arquivos, pastas e impressoras. As permissões definidas acima são válidas sobre pastas compartilhadas na rede também.

7. Crie agora o compartilhamento da uma pasta ou unidade na rede: Abra o Windows Explorer e localize a pasta que você deseja compartilhar. Clique com o botão direito e em Compartilhamento e segurança... Marque a caixa de seleção **Compartilhar esta pasta na rede** se ela estiver disponível (se ela não estiver disponível, este computador não está em uma rede. Clique no link **Assistente para configuração de rede** e siga as instruções para ativar o compartilhamento de arquivos). Você pode definir o número máximo de usuários acessando o compartilhamento ao mesmo tempo: clique em **Permitir este número de usuários.** As pastas compartilhadas são representadas por uma mão segurando-as:

8. Uma última dica está sobre a criação de compartilhamentos ocultos: Um compartilhamento oculto é quando a pasta está compartilhada, porém você não consegue visualizar através do Explorer. Para criar um compartilhamento oculto: No nome do compartilhamento, digite **$** no último caractere (exemplo : **TM$**, onde **TM** é o nome da pasta). Os recursos compartilhados não podem ser acessados pelo Windows Explorer.

   Para acessar um compartilhamento oculto: No menu Iniciar, clique em Executar e digite o comando **UNC** (Convenção universal de nomenclatura). A sintaxe é a seguinte:
   \\NOME_DO_COMPUTADOR\NOME_DO_COMPARTILHAMENTO\PASTA\NOME_DO_ARQUIVO$, colocando o símbolo “$” ao final do nome doarquivo.

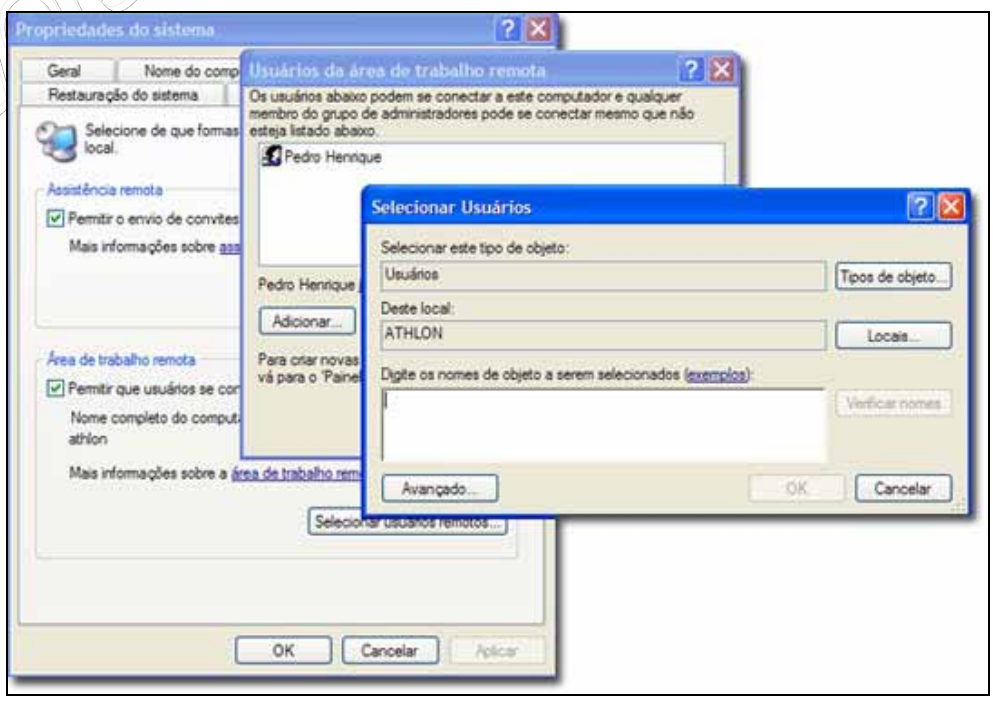
9. Para visualizar todas os compartilhamentos criado em um computador, quem está conectado ao seu computador e quais arquivos estão sendo acessados, execute o seguinte passo: Iniciar -> Painel de Controle -> Ferramentas Administrativas -> Gerenciamento do computador -> Pastas Compartilhadas.

Remote Desktop

O Remote Desktop é um serviço similar ao Terminal Server, porém com recursos limitados. É possível, uma vez habilitado e configurado, acessar uma estação de trabalho remota e ter total controle sobre a mesma. Porém, quando utilizado o Remote Desktop, apenas um único logon é permitido na estação, ou seja, se houver alguém logado na estação, usuários remotos não poderão ter acesso a estação.

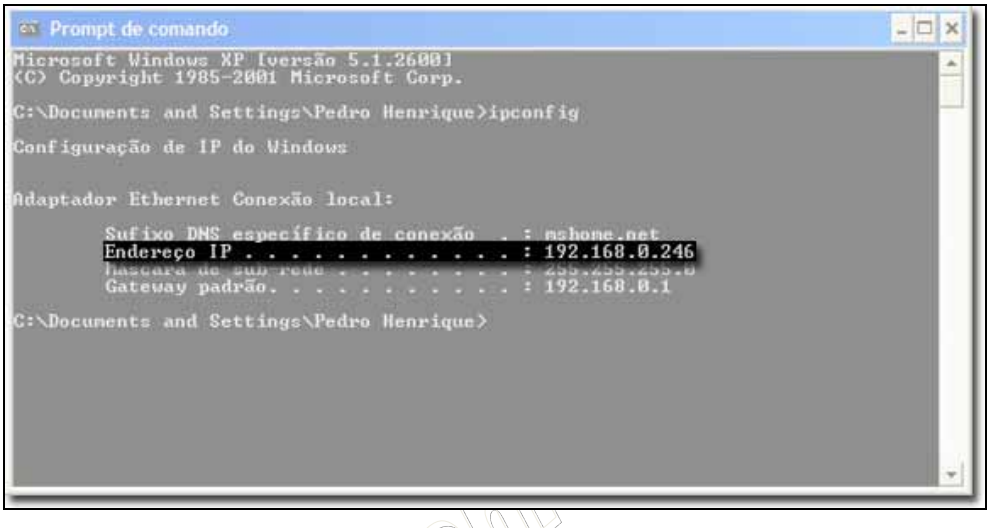
Apesar desta limitação, ainda é considerada uma ferramenta de extrema utilidade. Vamos supor que você tenha saído de sua sala para ir no departamento de RH, mas ao chegar lembra que esqueceu de enviar o e-mail. Você pode acessar remotamento sua estação, que irá efetuar o logoff do seu atual usuário ocioso e então poder enviar o e-mail.

Para habilitarmos o Acesso a Área de Trabalho Remota, realize o seguinte passo: Vá em Iniciar > Painel de controle > Sistema > guia Remoto > marque Permitir que usuários se conectem remotamente à este computador > Selecionar usuários remotos > Adicionar > escreva o nome de algum usuário cadastrado no XP > OK > OK > OK. Pronto.

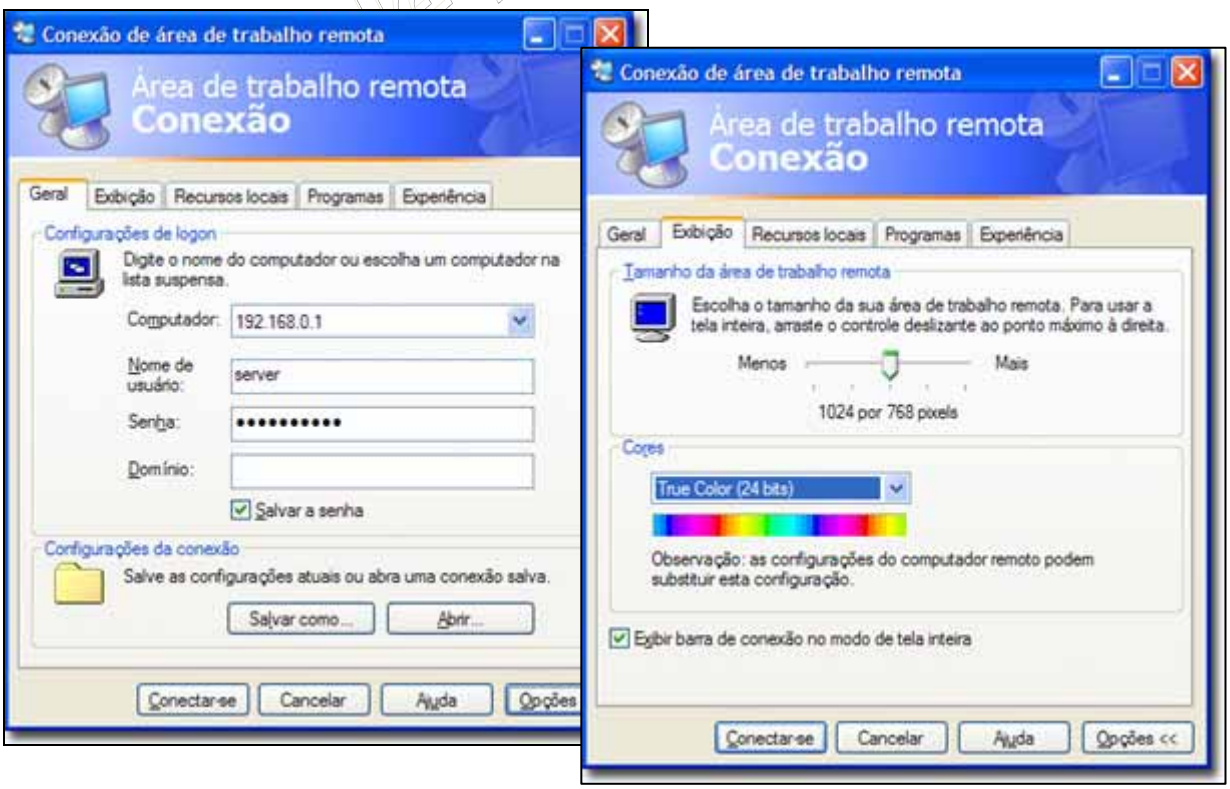


Certifique-se de que a máquina que será acessada não tenha nenhum firewall bloqueando o serviço mstsc.exe (responsável pela Conexão de área de trabalho remota) e de que a máquina esteja conectada diretamente na Internet (sem proxys, servidores, etc).

Ver o IP do computador: Iniciar / Executar / cmd / ipconfig / guarde o número denominado Endereço de IP:

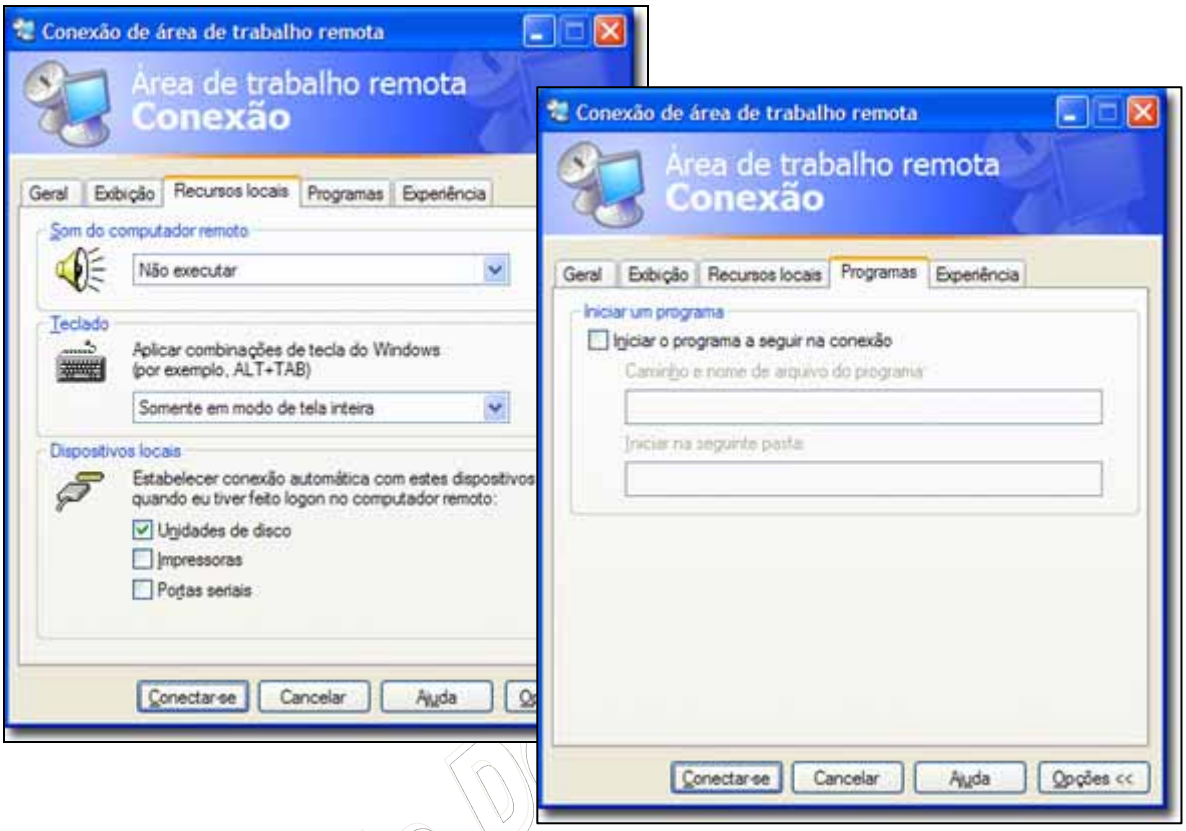


Agora que temos o Remote Desktop habilitado vamos demonstrar a conexão ao mesmo: para isso você pode utilizar o utilitário "mstsc", o mesmo visto no Terminal Server. Outra alternativa para chegar a este utilitário é: Iniciar > Todos os programas > Acessórios > Comunicações > Conexão de área de trabalho remota. Vejamos algumas das opções desta ferramenta:



Quanto maior a tela e quantidade de cores maior será a necessidade de banda de internet.

Você pode escolher quais recursos locais ficarão visíveis no ambiente virtual e opcionalmente executar um script automático quando efetuar logon:



Por último, você poderá aumentar a velocidade ou desempenho da área remota através da aba "Experiência":

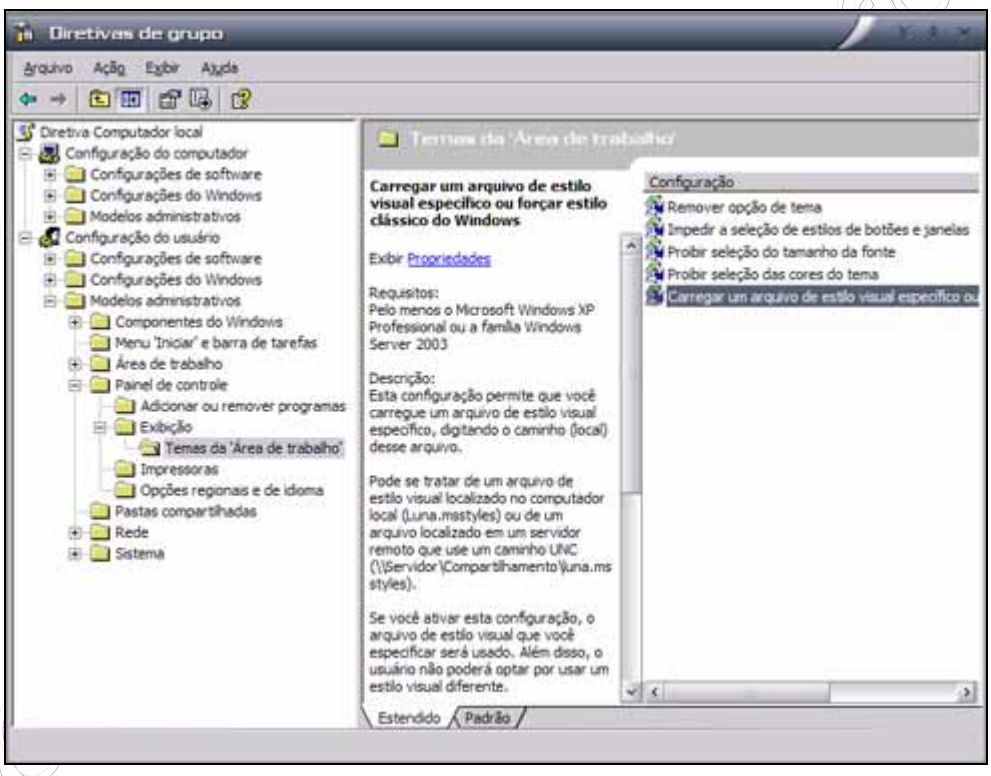
Pronto, você agora já pode realizar a conexão a estação remota. Uma observação é que todas essas configurações feitas não podem ser rejeitadas pela estação remota, como ocorre no Windows Server 2003. Essa é mais uma limitação do Remote Desktop.

Diretivas de Segurança Local

É possível aumentar o nível de segurança e restrições do uso da estação de trabalho através das Diretivas de Grupos ou Diretivas de Segurança Local, no caso de estações de trabalho. É na verdade uma versão mais reduzida e simplificada do que o Group Policie do Active Directory, mas com os mesmo tipos de objetos para edição.

Para acessar as diretivas de segurança local: Iniciar -> Painel de Controle -> Ferramentas Administrativas -> Diretivas de Segurança Local. Ou como alternativa: Iniciar -> Executar -> gpedit.msc

Aqui você poderá realizar as mesmas restrições vista no GPM, mas para os usuários locais da estação de trabalho:

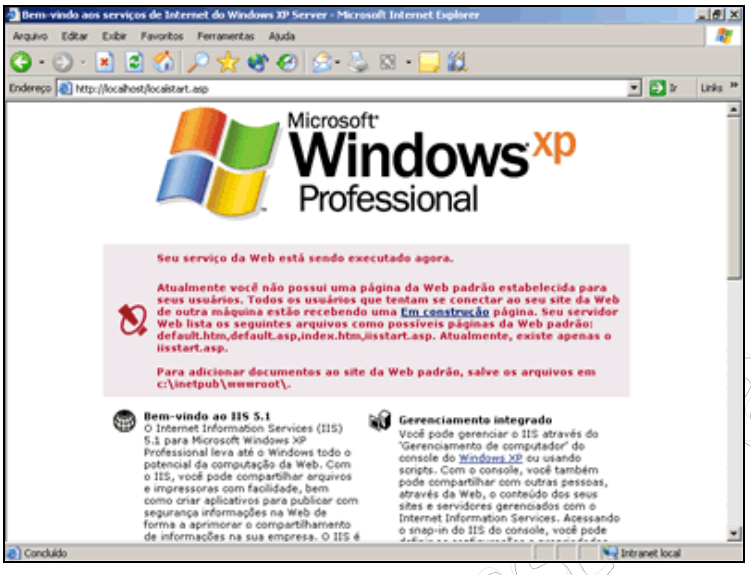


Após realizar suas configurações é necessário reiniciar o computador.

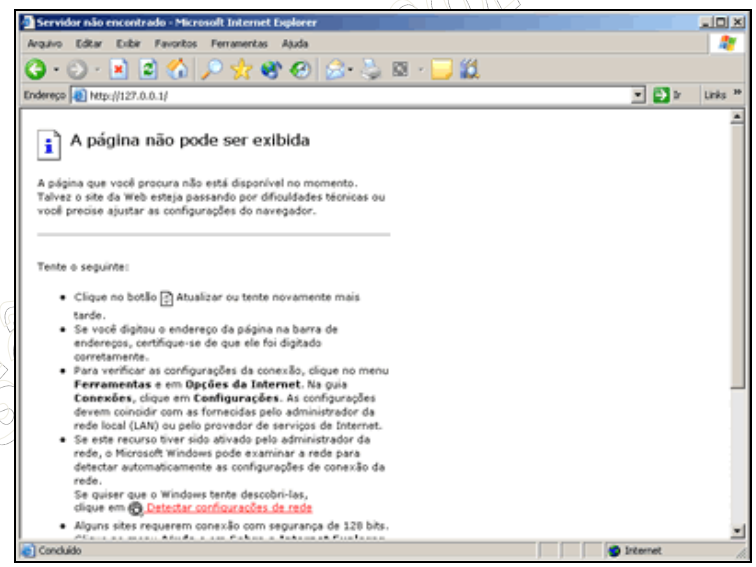
Internet Information Services (IIS)

Antes de configurar o IIS (Internet Information Server) em seu Windows XP, é preciso saber se ele já se encontra instalado em seu computador. Para tanto, abra o Internet Explorer e digite o seguinte endereço:http://localhost ou http://127.0.0.1.

Se a página seguinte for exibida, é sinal que o IIS já se encontra instalado em seu computador e apenas deverá ser configurado. Neste caso, pule a etapa 1:

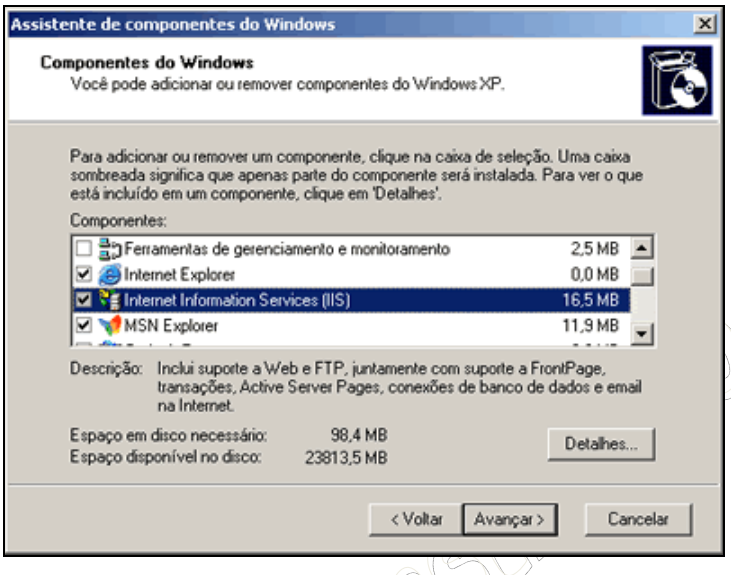


No entanto, se a página seguinte for exibida, você deverá instalar o IIS em seu computador seguindo as orientações descritas na etapa 1:



Etapa 1: Como instalar o IIS no Windows XP Professional:

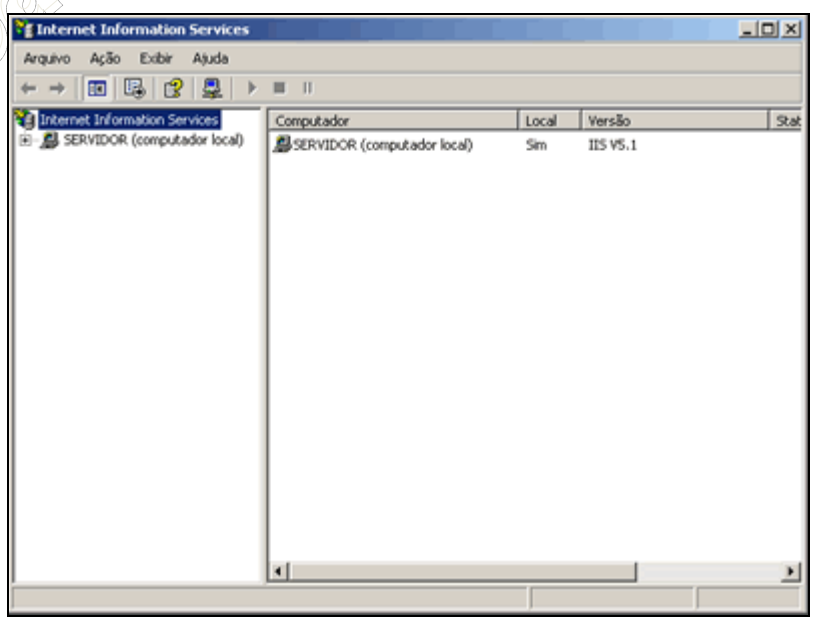
1. Clique sobre o botão Iniciar que se encontra na barra de tarefas do Windows, e em seguida sobre a opção Painel de Controle;
2. Ao ser exibida a janela do "Painel de Controle", clique sobre o ícone Adicionar ou Remover Programas;
3. Ao ser exibida a tela "Adicionar ou Remover Programas", selecione a opção Adicionar/Remover componentes do Windows que se encontra em seu painel esquerdo;
4. Procure a opção Internet Information Services (IIS) e marque sua caixa de seleção:



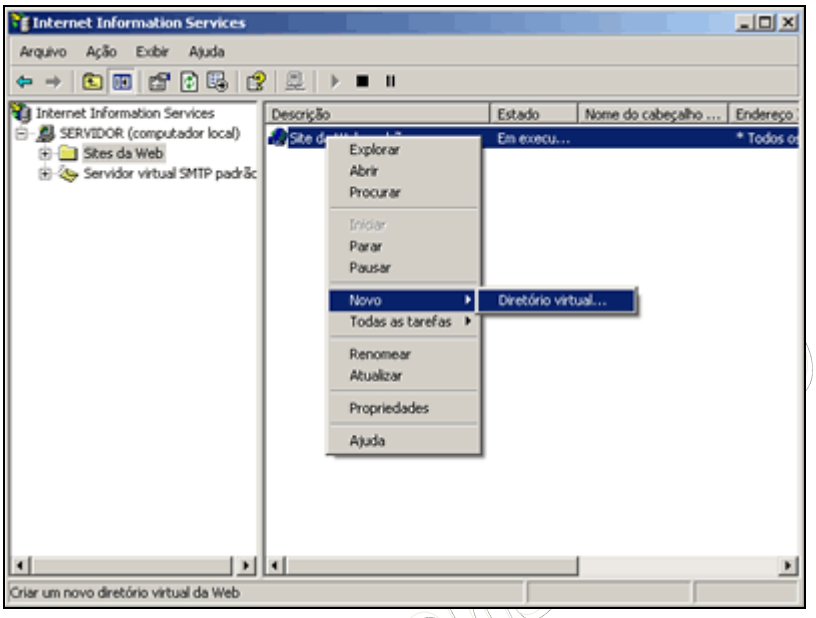
5. Clique sobre o botão Avançar e siga as instruções do instalador;
6. Uma vez terminada a instalação do IIS, você poderá prosseguir para a próxima etapa.

Etapa 2: Como configurar o IIS no Windows XP Professional:

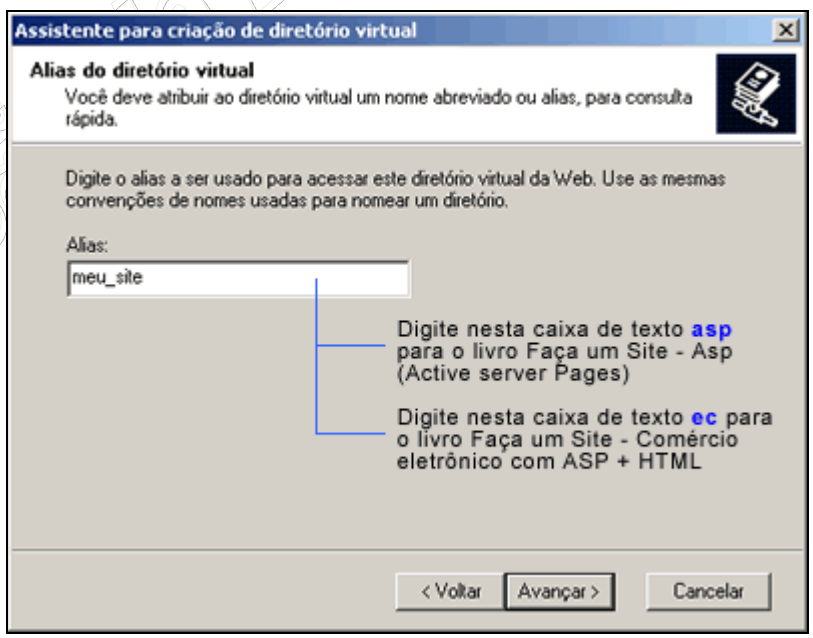
1. Clique sobre o botão Iniciar que se encontra na barra de tarefas do Windows, e em seguida sobre a opção Painel de Controle;
2. Ao ser exibida a janela do "Painel de Controle", clique sobre o ícone Ferramentas administrativas;
3. Ao ser exibida a tela "Ferramentas Administrativas", clique sobre o ícone Internet Information Services;
4. A janela do Internet Information Services será exibida na tela:



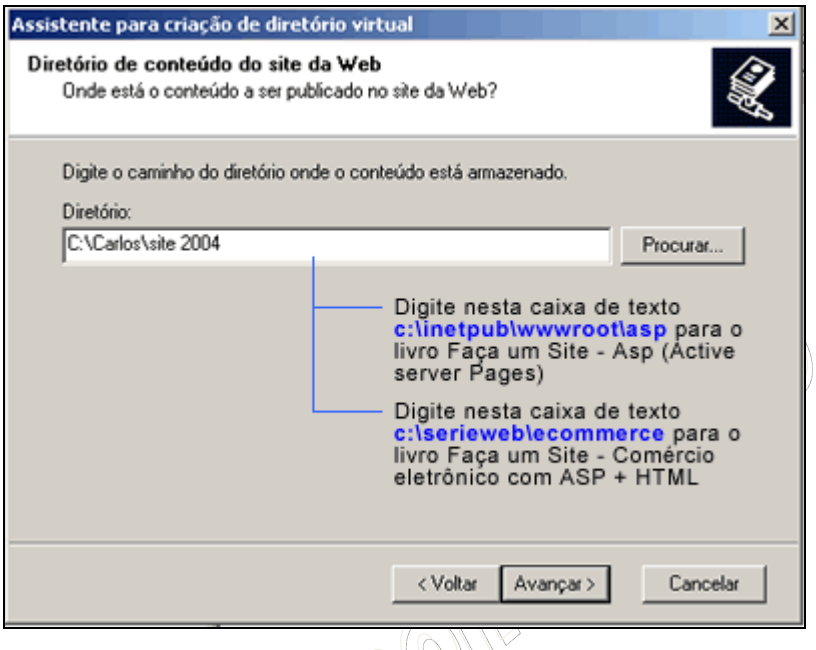
5. Em seu painel esquerdo, expanda a árvore (SERVIDOR) Computador local;
6. Ao ser expandida a árvore, selecione a pasta **Sites da Web;**
7. Clique com o botão direito do mouse sobre a opção **Site da Web padrão** que se encontra no painel direito da janela:



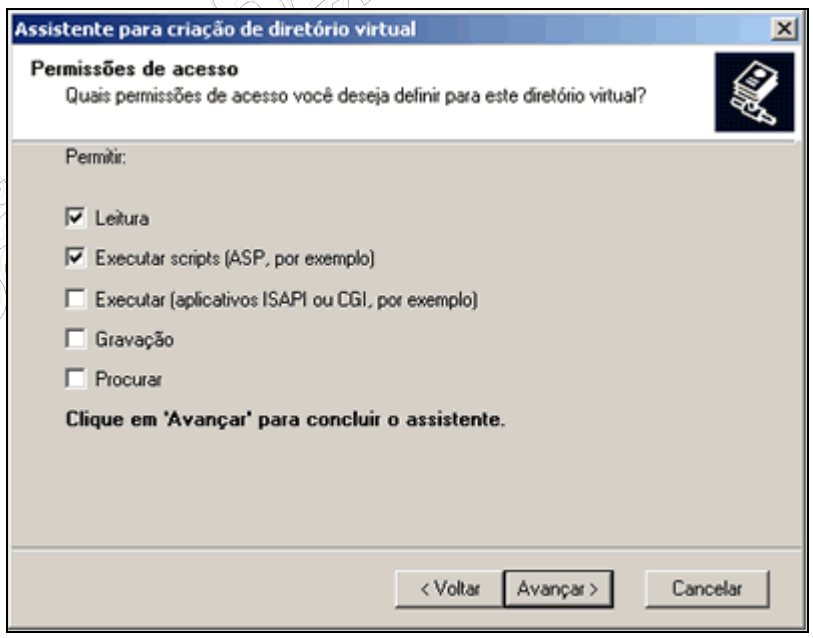
8. Ao ser exibido seu menu suspenso, escolha a opção **Novo - Diretório virtual;**
9. O assistente para a criação do diretório virtual será exibido na tela de seu computador;
10. Clique sobre seu botão Avançar;
11. Na próxima tela do assistente, você será solicitado para digitar um apelido (Alias) para o seu site, onde em nosso exemplo digitamos **meu_site:**



12. Clique sobre o botão **Avançar;**
13. Na próxima janela você deverá informar em qual diretório está localizado o projeto de seu site. Digite na caixa de texto Diretório o seguinte caminho: **c:\inetpub\wwwroot** ou o que você achar melhor:



14. Clique sobre o botão **Avançar;**
15. A janela de permissões de acesso será exibida na tela. Mantenha as configurações atuais e clique sobre o botão **Avançar:**



16. Finalmente clique sobre o botão **Concluir** para concluir a configuração do IIS.

A partir deste momento o IIS já esta configurado para ser utilizado.

Utilitário de Fax

Um utilitário para o envio e recebimento de fax em computadores é extremamente útil, principalmente quando você está em viajem com seu notebook e precisar receber os fax.

Em redes corporativas o uso do serviço de fax pode melhorar a qualidade da comunicação, pois o computador pode, alem de receber e realizar chamadas, gerenciar todos os contatos estabelecidos, como uma central digital.

Existem diversas razões para habilitar esse serviço, mas algumas considerações precisam ser avaliadas. Quando instalado, o serviço de Fax permanece na memória consumindo recursos de RAM, em média 2 MB. É necessário possui um dispositivo de fax/modem antes de realizar a instalação. Vejamos como realizar a instalação desse recurso para uso em ambientes corporativos em substituição aos equipamentos tradicionais de fax.

Por padrão, o componente Fax não é instalado durante a Instalação do Windows. Para instalar o componente Fax, execute estas etapas (texto retirado de: http://support.microsoft.com/kb/306550/pt-br):

1. Clique em **Iniciar**, em **Painel de controle** e clique duas vezes em **Adicionar ou remover programas** em **Selecione uma categoria;**
2. Clique em **Adicionar/remover componentes do Windows** para iniciar o Assistente para componentes do Windows;
3. Na lista **Componentes**, marque a caixa de seleção **Fax Services** e clique em **Avançar**. A Instalação instala os serviços de Fax. Se for solicitado, insira o CD do Microsoft Windows XP e clique em **OK**;
4. Clique em **Concluir** e clique em **Fechar**.

Para configurar o recurso de fax no Windows XP, execute estas etapas:

1. Clique em **Iniciar**, aponte para **Todos os programas**, para **Acessórios**, para **Comunicações**, para **Fax** e em seguida clique em **Console de fax;**
2. O Assistente para configuração de fax inicia. Clique em **Avançar**, digite as informações que deseja que apareça na folha de rosto do fax e clique em **Avançar;**
3. Clique no modem que deseja usar na lista **Selecione o dispositivo de fax;**
4. Se quiser desativar o recurso para enviar faxes desse computador, desmarque a caixa de seleção **Ativar envio (Observação** Por padrão, a caixa de seleção **Ativar envio** está marcada**)**;
5. Marque a caixa e seleção **Ativar recebimento** se quiser que o computador receba faxes (**Observação** Quando essa caixa de seleção estiver marcada, você poderá clicar em **Resposta manual** se não quiser que o computador receba faxes automaticamente. Por padrão, a resposta automática está ativada);
6. Clique em **Avançar;**
7. Digite o TSID (identificação do assinante transmissor) que deseja usar na caixa **TSID (Observação** O TSID é obrigatório em algumas áreas. Essas informações de identificação normalmente aparecem na área de cabeçalho de um fax que receber. Essas informações ajudam a identificar a máquina de fax na qual o fax se origina. Essas informações normalmente incluem o número de fax do remetente e o nome comercial**);**
8. Clique em **Avançar;**
9. Digite o CSID (identificação do assinante chamado) que deseja na caixa **CSID (Observação** O CSID digitado é exibido na máquina de fax na qual o fax se origina. Esse número ajuda a confirmar se você está enviando o fax ao destinatário correto**);**
10. Clique em **Avançar;**
11. Marque a caixa de seleção **Imprimir em** se quiser que cada um dos faxes recebidos seja impresso automaticamente. Ao marcar essa caixa de seleção, é possível selecionar uma impressora especifica onde é possível imprimir o fax recebido;
12. Marque a caixa de seleção **Armazenar uma cópia na pasta** se quiser criar uma cópia arquivada de cada fax. Ao marcar essa caixa de seleção, é possível especificar o local de armazenamento para a cópia do fax;
13. Clique em **Avançar;**
14. Confirme as definições da configuração na lista **Resumo da Configuração** e clique em **Concluir.**

O Assistente para configuração de fax fecha e a janela do Console de fax abre. O computador está configurado agora para enviar ou receber fax.

10 COMPETÊNCIA 4 – INTEGRAÇÃO SOC E SOS

Agora chegou o momento final, de vermos como integrar todos os recursos aprendidos das estações de trabalho com o servidor de rede. Vamos praticar como deixar as estações de trabalho acessando o que há de melhor dos servidores criados, e em seguida, fecharemos esta disciplina com os conhecimentos de como proceder para manter o sistema operacional sempre atualizado.

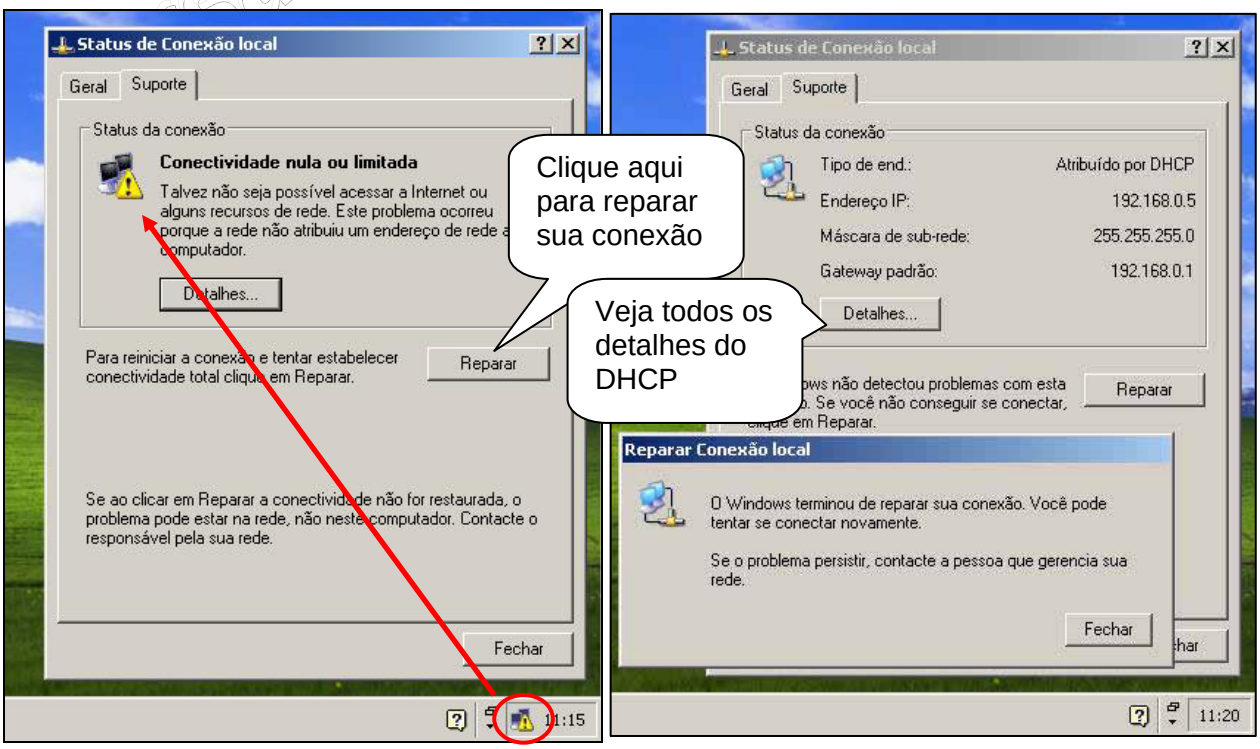
10.1 CONFIGURAÇÃO DOS SERVIÇOS DE ACESSO A REDE

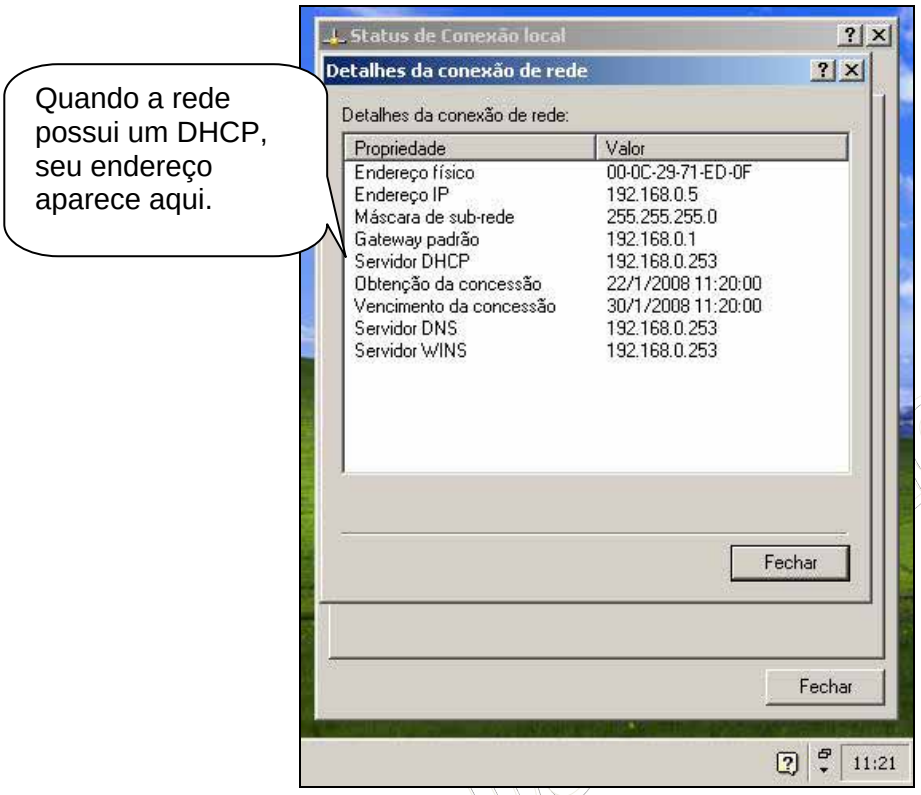
A integração do sistema operacional cliente de rede com seu respectivo servidor de rede é realizada através dos vários serviços que configuramos até aqui, são eles:

- O DHCP, que irá fornecer endereços de rede automáticos para as estações de trabalho;
- Inserir a estação de trabalho no domínio da empresa;
- Acessar o domínio da empresa e seus respectivos serviços de intranet;
- Compartilhar áreas de trabalhos remotas fornecidas na rede;
- Manusear de forma segura os arquivos em rede;
- Trabalhar com perfis móveis
- Acessar uma conta de e-mail corporativa;

O DHCP

A primeira ação que realizamos em rede é ligar a estação de trabalho ao mesmo switch onde está o servidor. Quando não temos um servidor DHCP na rede, ou não estamos conectados no mesmo barramento de rede que o servidor DHCP, então o sistema apresenta uma mensagem de "Conectividade nula ou limitada", porém, quando estivermos ao alcance do servidor DHCP, teremos uma séria de informações sobre a rede preenchidas de forma automática.

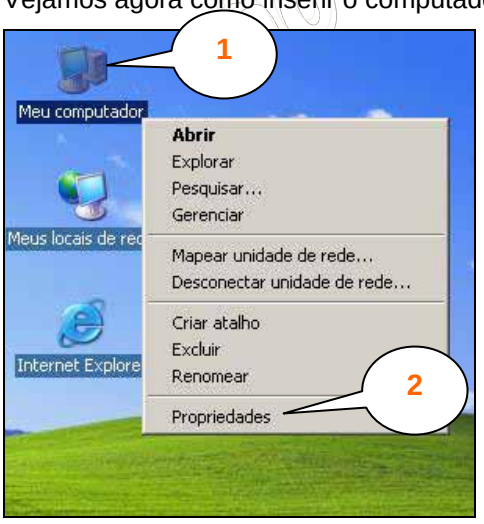


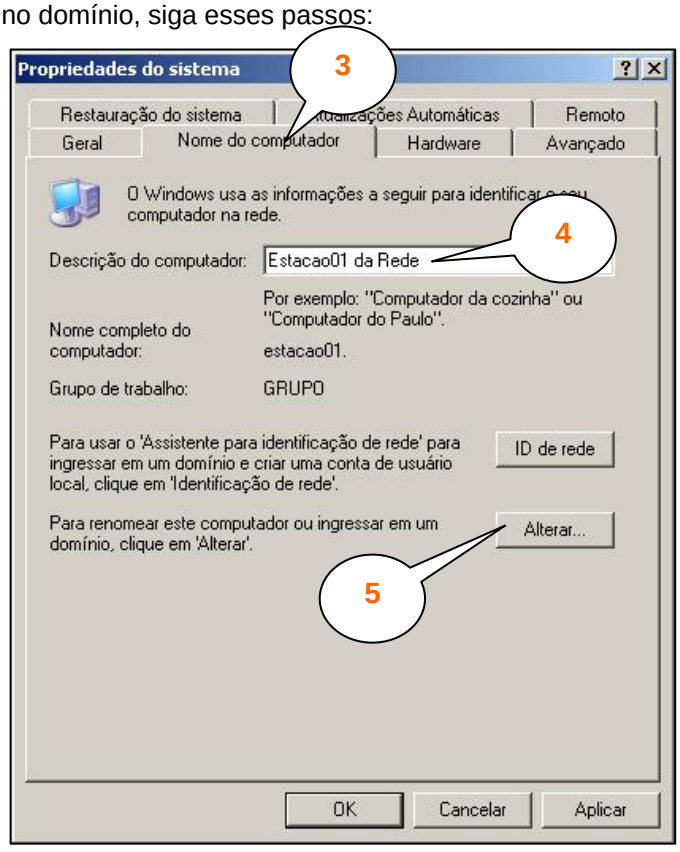


Agora que estamos em rede, vejamos como inserir a estação de trabalho no domínio da empresa:

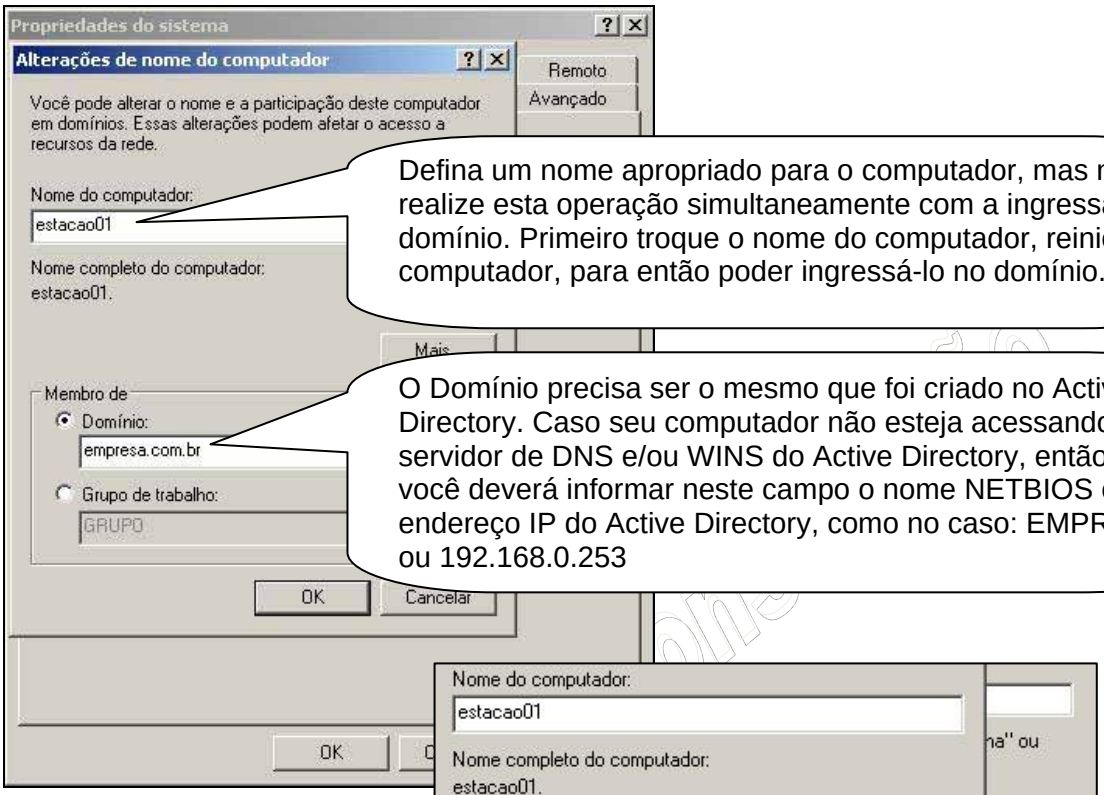
Logon em Domínios do Active Directory

Vejamos agora como inserir o computador no domínio, siga esses passos:





Defina uma descrição para sua estação de trabalho, e em seguida clique em “Alterar” para ingressar o computador no domínio:



Defina um nome apropriado para o computador, mas não realize esta operação simultaneamente com a ingressão no domínio. Primeiro troque o nome do computador, reinicie o computador, para então poder ingressá-lo no domínio.

O Domínio precisa ser o mesmo que foi criado no Active Directory. Caso seu computador não esteja acessando o servidor de DNS e/ou WINS do Active Directory, então você deverá informar neste campo o nome NETBIOS ou o endereço IP do Active Directory, como no caso: EMPRESA ou 192.168.0.253

Ao clicar em OK, obtendo sucesso na ingressão ao domínio, será apresentado uma tela de boas vindas ao domínio. Reinicie o computador.

Após o computador ser reiniciado, você será apresentado a seguinte tela de Logon:

Pressione simultaneamente as teclas Ctrl+Alt+Del para que seja exibida a tela de usuário e senha:

Se quiser acessar o computador com sua senha local, escolha o nome do seu computador. Se quiser acessar o computador e ter acesso aos recursos da rede, selecione o domínio "EMPRESA".

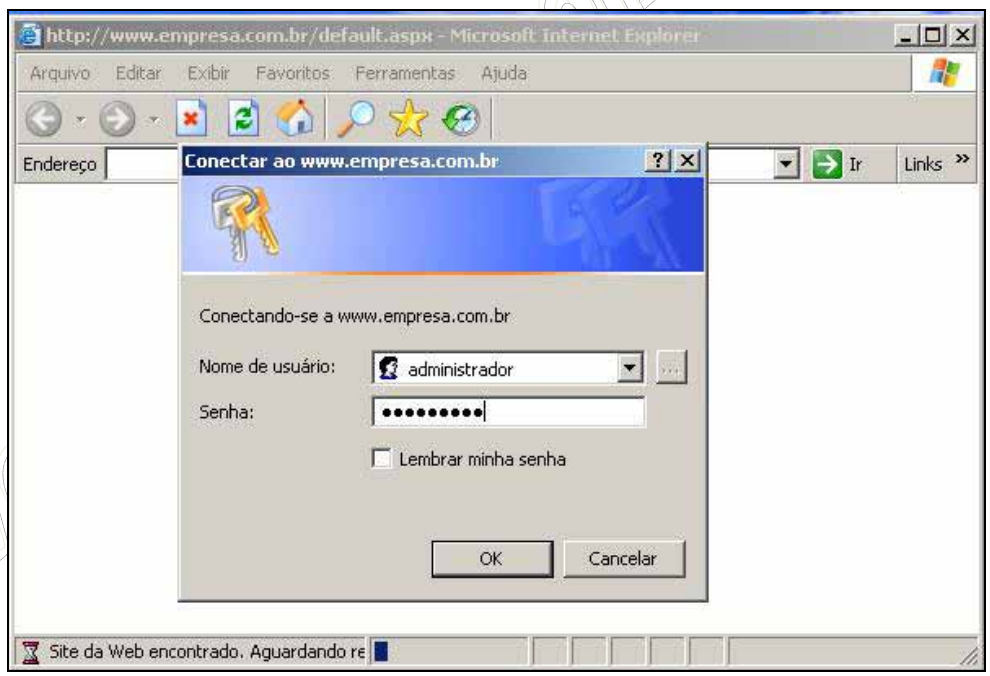
Para instalar um novo hardware, definir regras e permissões para a máquina local, é necessário acessar o computador com a senha de Administrador Local. Para manipular pastas, arquivos e impressoras compartilhadas em rede é necessário acessar com a senha de Administrador da Rede.

Dessa forma observa-se que existe uma discreta diferença entre as contas de Administrador Local e de Rede, da mesma forma que existirão entre as contas de usuário local e as contas de usuário em rede.

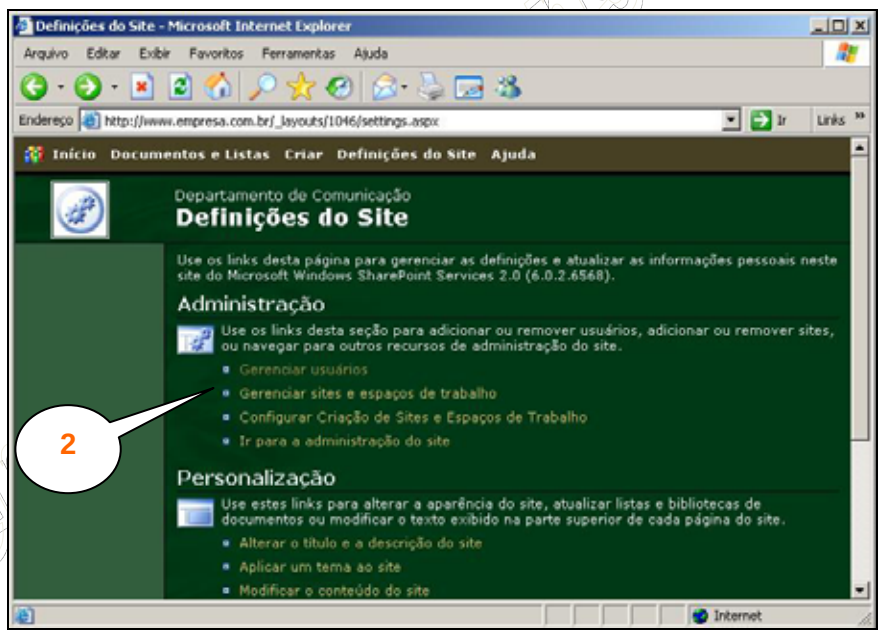
As contas de usuários locais não estarão submetidas as políticas de grupo da rede, bem como não poderão acessar os recursos da rede. Para acessar os recursos da rede, o usuário local precisará informar ao servidor um usuário e senha válidos da rede, toda a vez que for acessar determinado recurso da rede. As contas de rede poderão acessar as estações de trabalhos que estiverem inseridas no domínio, e estarão submetidas tanto as políticas de grupo da rede, quanto as diretrizes de segurança local da estação, definidas pelo Administrador local.

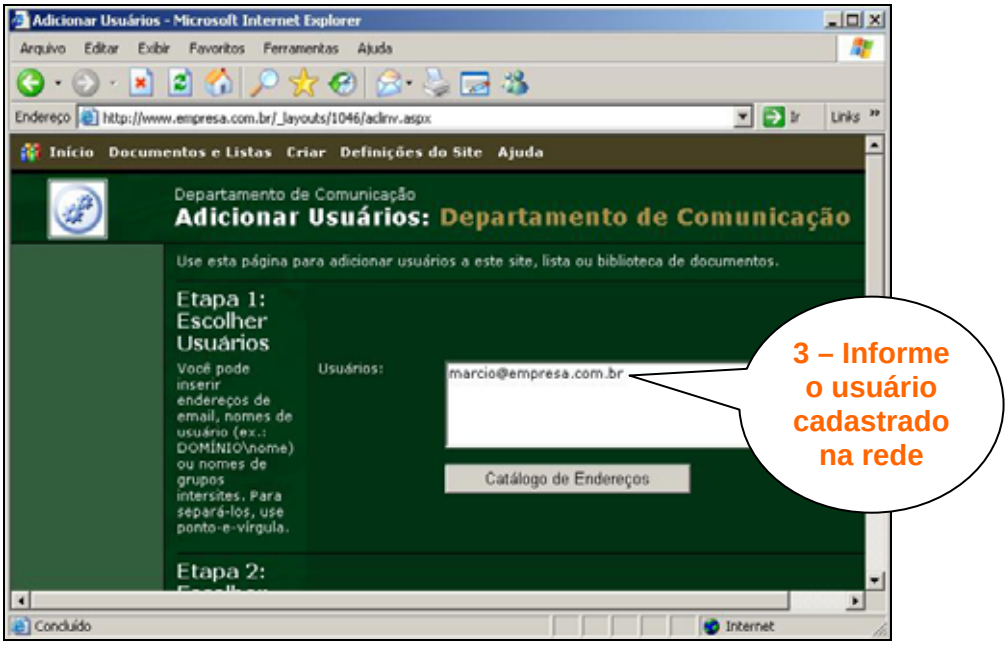
Serviços de Intranet

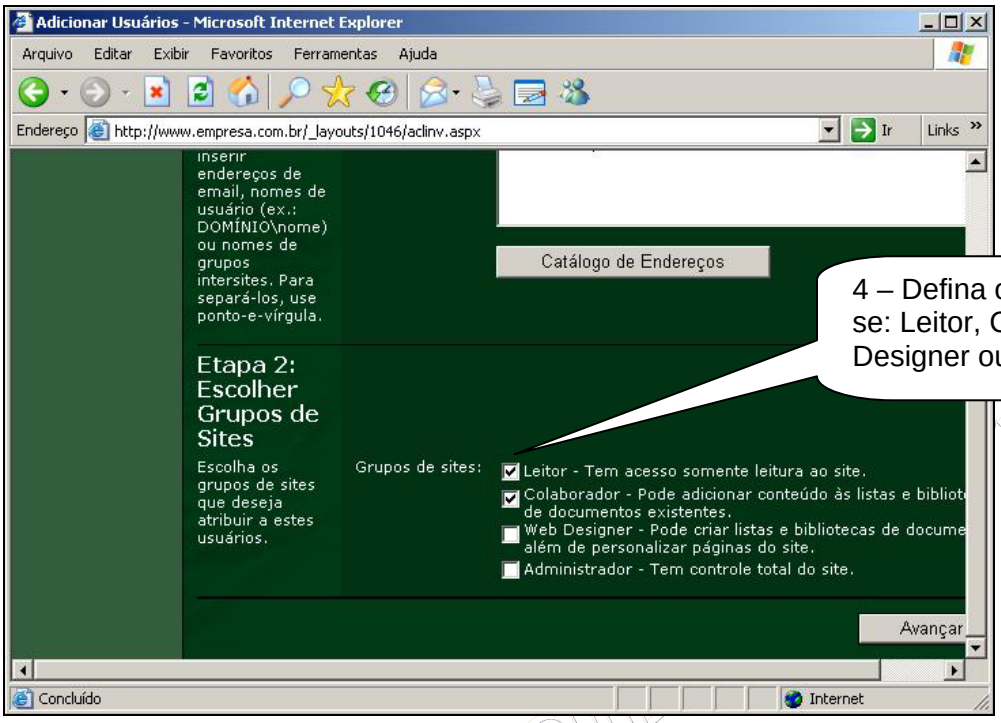
Agora que estamos acessando a rede e o domínio, vamos apreender a como utilizar os recursos da intranet. Para isso, antes de mais nada, precisaremos criar o nosso usuário no sistema da Intranet, vejamos como:



Acesse o site da intranet (se você configurou bem o IIS então este mesmo site poderá ser o site da Internet também): www.empresa.com.br . Como ainda não temos um usuário cadastrado na intranet, então precisaremos efetuar o logon como Administrador e em seguida acessar a aba para adicionar novos usuários:







Na etapa 02, na escolha dos grupos de sites, você poderá atribuir as permissões de acesso a cada usuários, são elas:

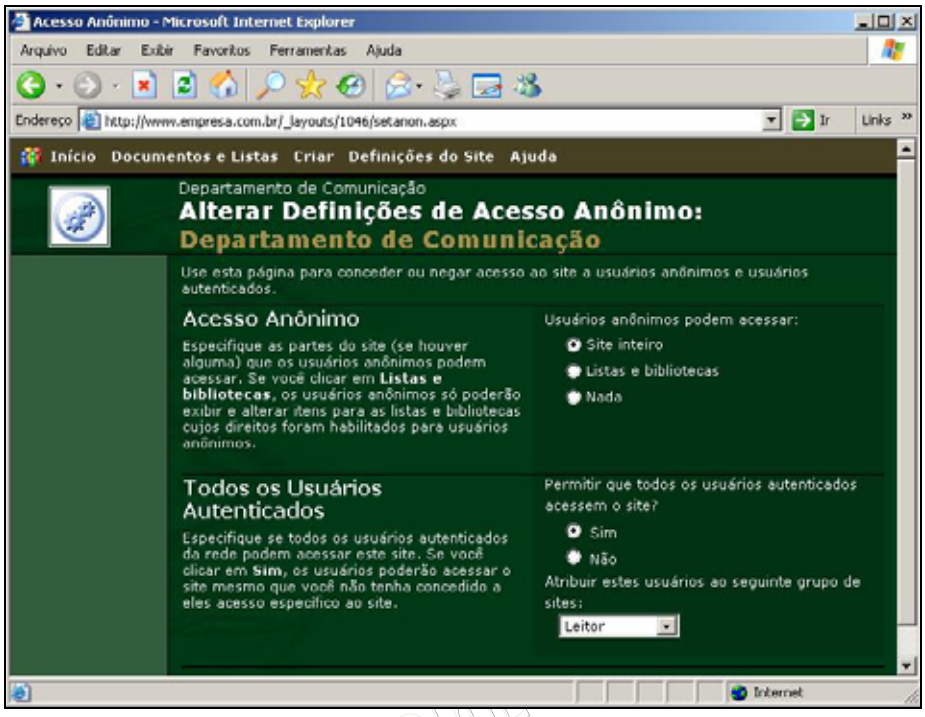
- Leitor – Tem acesso somente leitura ao site;
- Colaborador – Pode adicionar conteúdo às listas e biblioteca de documentos existentes.
- Web Designer – Pode criar listas e bibliotecas de documentos além de personalizar páginas do site;
- Administrador – Tem controle total do site.

Na etapa 03 confirme os dados do usuário e insira um nome amigável para o mesmo;

Na etapa 04 envie um e-mail de confirmação para o usuário, e pronto. O usuário está finalmente cadastrado na intranet.

Alguns administradores de rede vão preferir que toda e qualquer pessoa da intranet, logada ou não, possam acessar o site de comunicações (quadro de avisos eletrônicos) da empresa. Para isso, siga o procedimento abaixo:

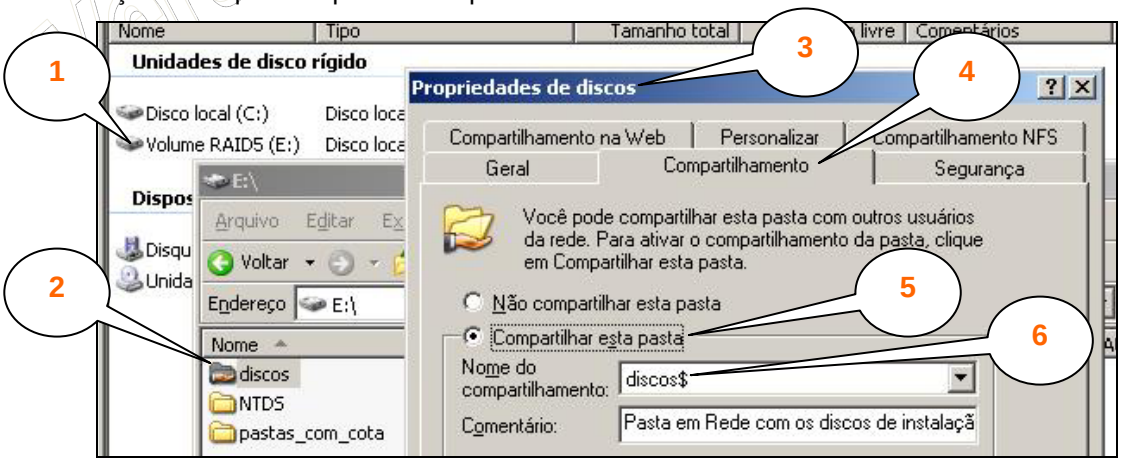
Clique em “Definições do Site” -> “Alterar Definições de Acesso Anônimo”. Selecione a opção onde usuários anônimos podem acessar todo o site:



Muitas outras opções estão disponíveis no serviço SharePoint, vimos apenas o necessário para iniciarmos a operação do mesmo. Vejamos agora como utilizar o principal recurso de uma rede: os arquivos e pastas compartilhadas.

Compartilhamento de arquivos

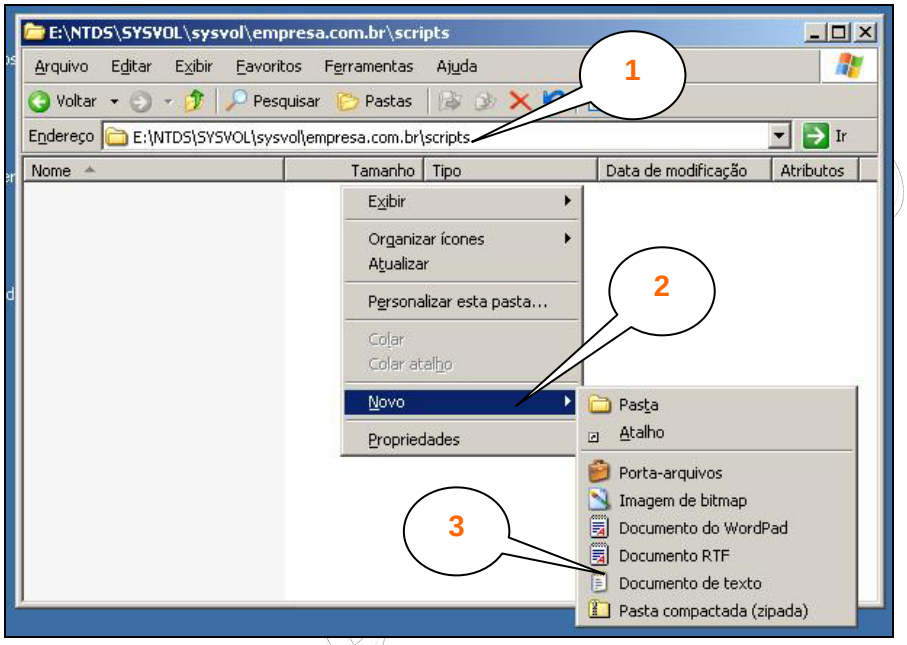
A primeira ação que iremos desenvolver é criar um compartilhamento de arquivos no servidor de arquivos. Esses arquivos estão em um volume RAID-5 no servidor, para garantir a segurança física desses dados. Iremos criar o compartilhamento “discos$”, lembrando que o símbolo de “$” ao final do nome de compartilhamento indica que este compartilhamento está oculto para os sistemas de visualização de arquivos e pastas compartilhadas:



O endereço completo desde compartilhamento na rede, ou padrão universal UNC, será: \\servidor\discos$, este compartilhamento servirá apenas como um repositório dos principais discos de instalação dos computadores, sistemas e drivers de hardwares, logo deverá ser do tipo: apenas leitura para todos, e permissão total para os membros da Informática.

Muitos usuários de estações de trabalho em rede não estão capacitados para operarem compartilhamentos e demais recursos da rede, logo, é necessário facilitar as atividades para esse tipo de usuário. Uma forma prática de publicar para toda a rede um recurso compartilhado é através da manipulação dos scripts de logon. Um script de logon é um conjunto de procedimentos que sempre serão realizados no momento em que o usuário efetuar o logon na estação de trabalho.

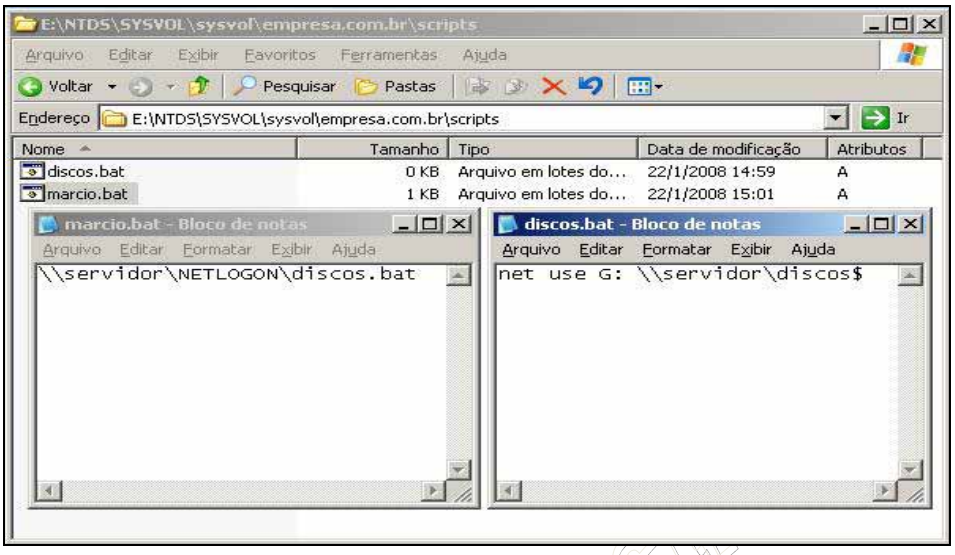
Os scripts de logon podem ser criados para um único usuário ou para grupos de usuários. Através desses scripts é possível realizar um mapeamento automático de pastas e impressoras de rede, por exemplo. Para continuar nosso exemplo prático, vamos criar um script de logon genérico para todos os usuários da rede, de forma a mapear o compartilhamento de "discos$", e um script específico para cada usuário, vejamos:



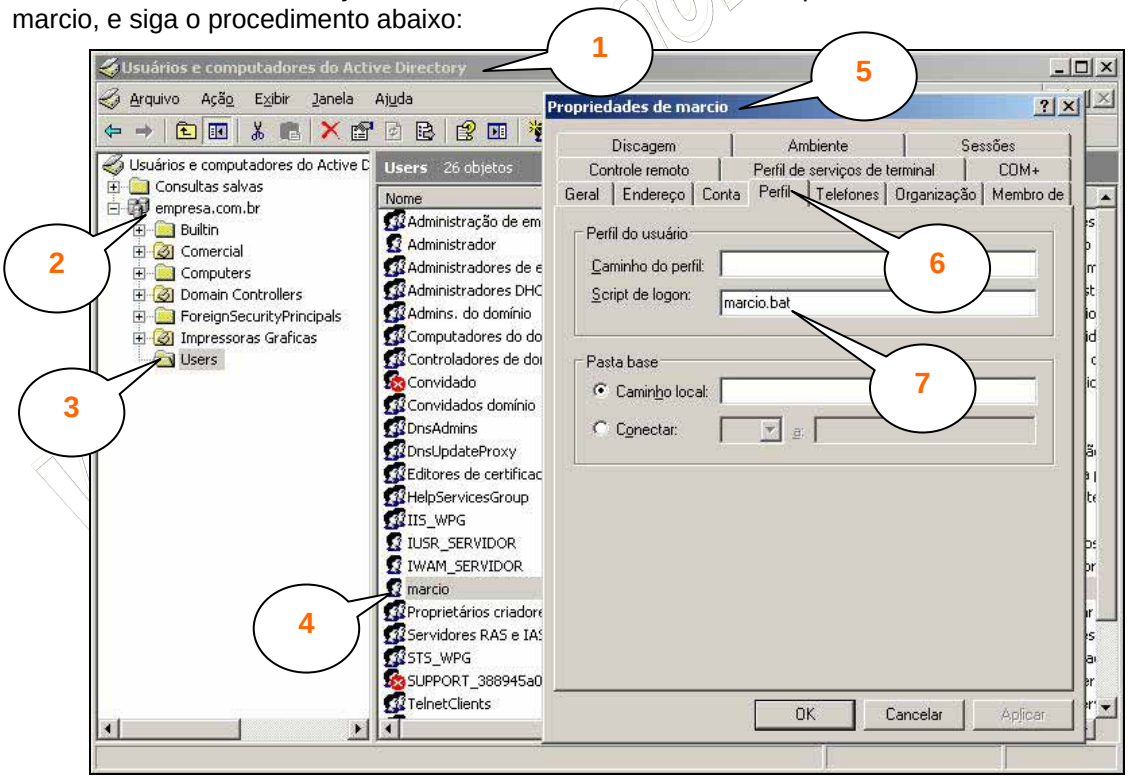
A pasta onde residem os scripts de logon sempre estarão em %\NTDS\SYSVOL\sysvol\<domínio>\scritps. Onde o símbolo de "%" deve ser substituído pelo caminho escolhido por você no momento da instalação do Active Directory. O diretório SYSVOL é especial para o AD. É nele que irão residir os principais controle da rede, como os scripts, as políticas de grupos e os perfis dos usuários.

Uma vez na pasta "scripts" você deve criar um arquivo texto com a extensão ".bat" (outras extensões também são possíveis, como .vbs e .wsh, a depender da linguagem de programação que você queira adotar como Visual Basic Script ou Windows Shell Host). Os arquivos ".bat" trabalham com os comandos que podem ser executados via Prompt do DOS, ou seja, diretamente em linha de comando. É importante saber que toda e qualquer operação realizada via uma interface gráfica do Windows Server 2003 possui seu respectivo comando via linha de comando, isso é de extrema importância pois assim temos uma noção do limite de aperfeiçoamento que podemos chegar através dos scripts de logon.

Continuando nosso exemplo, iremos criar dois arquivos textos de extensão .bat, são eles: discos.bat, onde serão informados os comandos para mapear o recurso "discos$" da rede, e marcio.bat, um script específico para a conta do usuário Márcio e que por sua vez irá executar o script genérico discos.bat:



Uma vez criados os scripts chegou a hora de informarmos ao sistema que o script marcio.bat deverá estar associado ao usuário Márcio. Dessa forma, execute o "Gerenciar o computador", siga até a aba do Active Directory, e acesse "Gerenciar Usuários e computadores". Edite o usuário marcio, e siga o procedimento abaixo:



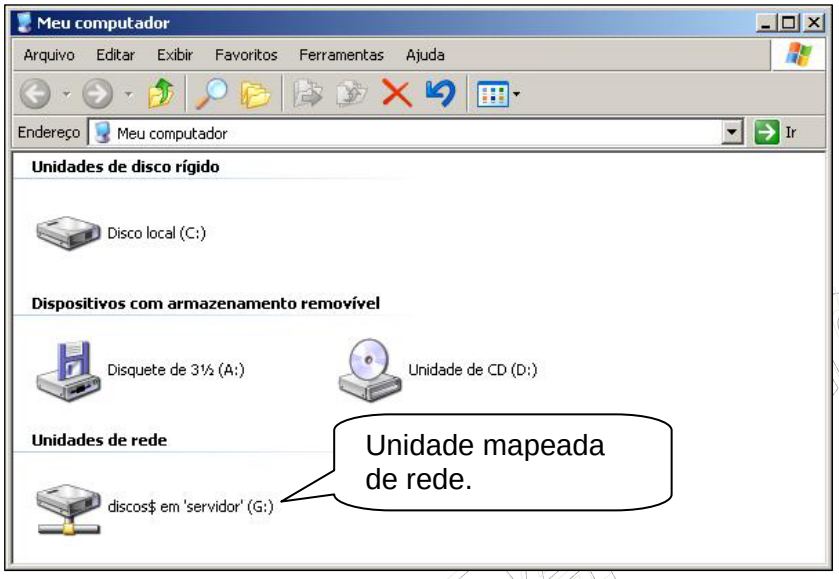
No campo "Script de logon", informe o nome do script que você criou para o usuário márcio e que está na pasta scripts.

Manusear arquivos compartilhados em rede

Agora que estamos equipados com uma área compartilhada em rede, essa área sendo automaticamente mapeada para nosso usuário no mesmo instante do logon, vejamos agora como lidar com as questões de permissões, acesso e disponibilidade da informação.

O primeiro passo é realizar o logon na estação de trabalho, nesse momento será observada uma nova janela, minimizada, e que rapidamente aparece e some. Esta janela é o script de logon que definimos na sessão anterior. Como definimos um script do tipo .bat, ou seja, que executa comandos de linha de comando em Prompt DOS, nada mais esperado do que uma janela DOS:

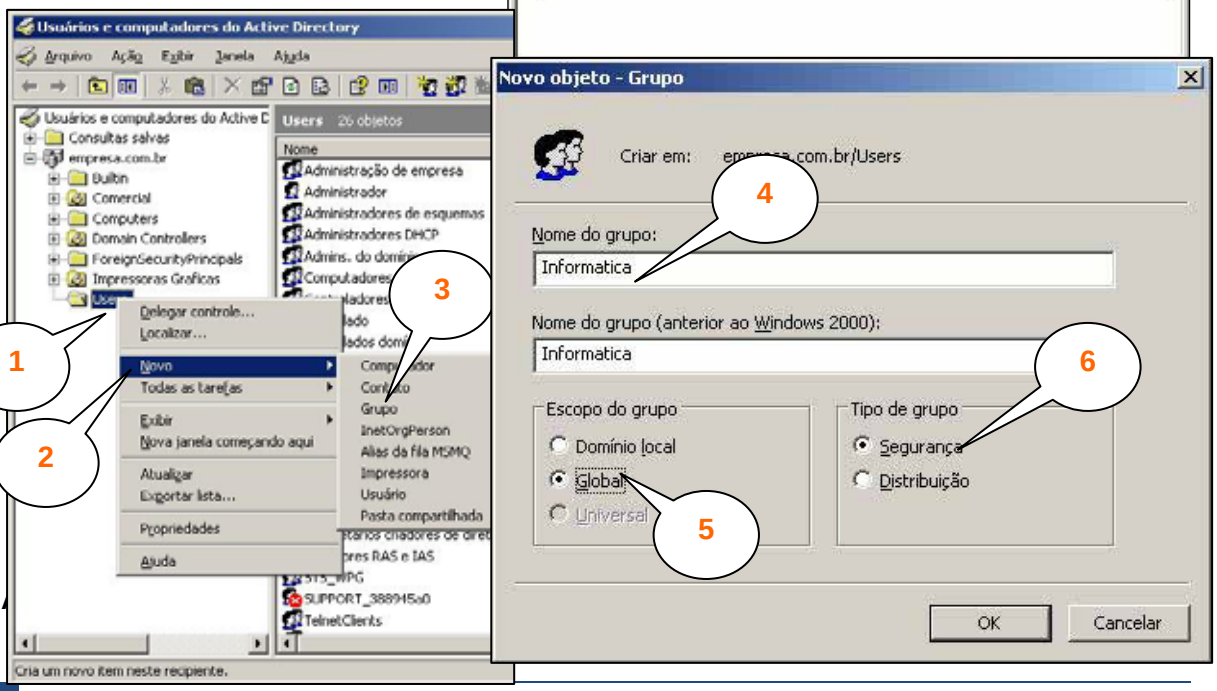
Uma vez que script de logon tenha sido executado com sucesso, você deverá acessar o “Meu Computador” para visualizar a nova unidade de rede disponibilizada. Essa nova unidade é muito semelhante a uma unidade de cd-rom, porém, os dados que estão ali disponíveis, estão na verdade em \\servidor\discos$:



Conforme definimos anteriormente, apenas a equipa de informática deverá ter acesso irrestrito a este compartilhamento. Abaixo vemos uma mensagem de acesso negado ao usuário marcio, no momento em que o mesmo tenta salvar ou modificar qualquer arquivo do G:. Veremos agora como adicionar o usuário marcio ao grupo da informática de forma que o mesmo possa salvar ou modificar arquivos nesta pasta compartilhada:

Para facilitar a administração das contas, iremos criar um grupo para os técnicos da informática, denominado, informática, as contas que pertencerem a este grupo terão permissões de controle total sobre a área compartilhada “discos$”.

Acesse o “Gerenciar o computador”, em seguida localize a aba do “Active Directory”, abra o “Usuários e computadores do domínio” e crie um novo grupo, conforme os passos abaixo:



Os grupos são usados para reunir contas de usuário, contas de computador e outras contas de grupo em unidades gerenciáveis. Trabalhar com grupos em lugar de usuários individuais ajuda a simplificar a manutenção e a administração da rede.
Há dois tipos de grupo no Active Directory: grupos de distribuição e grupos de segurança. Você pode usar grupos de distribuição para criar listas de distribuição de email e grupos de segurança para atribuir permissões para recursos compartilhados:

- Distribuição: podem ser usados somente com aplicativos de email (como o Exchange) para enviar mensagens para grupos de usuários. Os grupos de distribuição não são habilitados para segurança, o que significa que não podem ser listados em listas de controle de acesso discricional (DACLs). Se você precisa de um grupo para controlar o acesso a recursos compartilhados, crie um grupo de segurança;
- Segurança: Quando usados com cuidado, os grupos de segurança são uma forma eficaz de atribuir acesso a recursos na rede. Com grupos de segurança, você pode:
    1. Atribuir direitos de usuário a grupos de segurança no Active Directory. Os direitos de usuário são atribuídos a grupos de segurança para determinar o que os membros do grupo podem fazer no escopo de um domínio (ou floresta). Os direitos de usuário são atribuídos automaticamente a alguns grupos de segurança na instalação do Active Directory, para ajudar os administradores a definir a função administrativa de um usuário no domínio. Por exemplo, um usuário adicionado ao grupo Operadores de cópia no Active Directory tem o direito de fazer backup e restaurar arquivos e diretórios localizados em todos os controladores de domínio no domínio.
    Isso é possível porque, por padrão, os direitos de usuário Fazer backup de arquivos e diretórios e Restaurar arquivos e pastas são atribuídos automaticamente ao grupo Operadores de Backup. Portanto, os membros deste grupo herdam os direitos de usuário atribuídos ao grupo. Você pode atribuir direitos de usuário a grupos de segurança, usando Diretivas de Grupo, para ajudar a delegar tarefas específicas. Seja criterioso ao atribuir tarefas delegadas, porque um usuário sem treinamento que tenha direitos demais em um grupo de segurança tem potencial para causar danos significativos à rede;

    2. Atribuir permissões a grupos de segurança para recursos. As permissões não devem ser confundidas com direitos de usuário. As permissões são atribuídas ao grupo de segurança no recurso compartilhado. As permissões determinam quem pode acessar o recurso e o nível de acesso, como Controle Total.
    Algumas permissões definidas em objetos de domínio são atribuídas automaticamente para permitir vários níveis de acesso a grupos de segurança padrão, como Operadores de contas ou Admins. do domínio.
    Os grupos de segurança são listados em DACLs que definem permissões para recursos e objetos. Ao atribuir permissões para recursos (compartilhamentos de arquivos, impressoras e assim por diante), os administradores devem atribuir essas permissões a um grupo de segurança em vez de a usuários individuais. As permissões são atribuídas uma vez ao grupo, em vez de várias vezes a cada usuário. Cada conta adicionada a um grupo recebe os direitos atribuídos ao

grupo no Active Directory e as permissões definidas para aquele grupo no recurso.

Como os grupos de distribuição, os grupos de segurança também podem ser usados como uma entidade de email. Quando você envia um email para o grupo, ele é enviado para todos os participantes do grupo.

Os grupos, não importam se são um grupo de segurança ou um grupo de distribuição, são caracterizados por um escopo que identifica a extensão em que o grupo é aplicado à árvore do domínio ou floresta. Existem três escopos de grupo: universal, global e domínio local:

- Domínio local: podem incluir outros grupos e contas de domínios Windows Server 2003, Windows 2000 ou Windows NT e podem ter permissões somente em um domínio;
- Global: é o inverso do domínio local, podem incluir outros grupos e contas somente do domínio no qual o grupo está definido e podem ter permissões para qualquer domínio na floresta;
- Universal: podem incluir outros grupos e contas de qualquer domínio na árvore de domínio ou floresta e podem ter permissões para qualquer domínio na árvore de domínio ou floresta.

QUANDO USAR GRUPOS COM ESCOPO DE DOMÍNIO LOCAL

Os grupos com escopo de domínio local ajudam a definir e gerenciar o acesso a recursos em um único domínio. Esses grupos podem ter como membros:

- Grupos com escopo global
- Grupos com escopo universal
- Contas
- Outros grupos com escopo de domínio local
- Uma combinação de quaisquer itens acima

Por exemplo, para fornecer aos usuários acesso a uma determinada impressora, você pode adicionar todas as cinco contas de usuário à lista de permissões da impressora. Se, no entanto, mais tarde desejar fornecer aos cinco usuários acesso a uma nova impressora, terá de especificar novamente todas as cinco contas na lista de permissões da nova impressora.

Com um pouco de planejamento, você pode simplificar essa tarefa administrativa rotineira criando um grupo com escopo de domínio local e atribuindo-lhe permissão para acessar a impressora. Inclua as cinco contas de usuário em um grupo com escopo global e adicione esse grupo àquele que tem o escopo de domínio local. Quando você desejar fornecer aos cinco usuários acesso a uma nova impressora, atribua ao grupo com o escopo de domínio local permissão para acessar a nova impressora. Todos os membros do grupo com escopo global automaticamente recebem acesso à nova impressora.

QUANDO USAR GRUPOS COM ESCOPO GLOBAL

Use grupos com escopo global para gerenciar objetos de diretório que exijam manutenção diária, como contas de usuário e de computador. Como os grupos com escopo global não são replicados fora de seu próprio domínio, as contas em um grupo que tem escopo global podem ser alteradas freqüentemente sem que isso gere tráfego de replicação para o catálogo global.

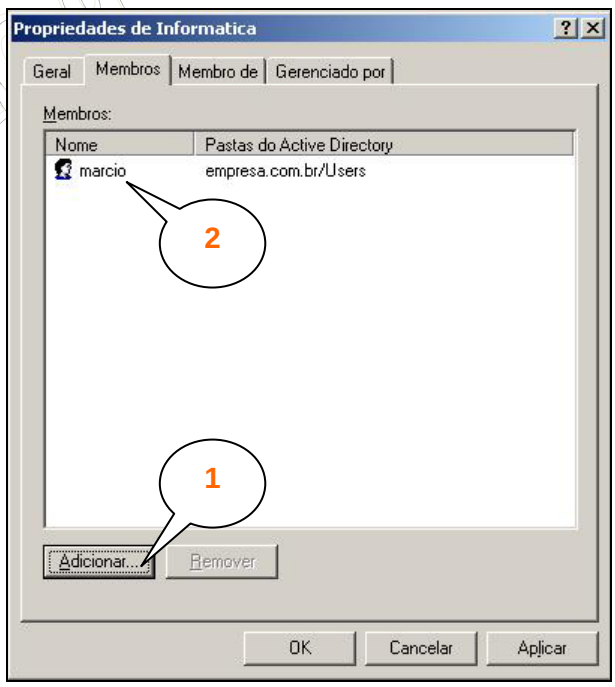
Embora as atribuições de direitos e permissões sejam válidas somente no domínio no qual são atribuídas, ao aplicar grupos com escopo global de forma uniforme nos domínios apropriados, você pode consolidar referências a contas com finalidades semelhantes. Isso simplificará e racionalizará o gerenciamento de grupos em domínios. Por exemplo, em uma rede com dois domínios, Europa e

EstadosUnidos, se houver um grupo com escopo global chamado ContabilidadeGL no domínio EstadosUnidos, também deverá haver um grupo chamado ContabilidadeGL no domínio Europa (a menos que a função de contabilidade não exista no domínio Europa)
É recomendável usar grupos globais ou grupos universais em vez de grupos de domínio local ao especificar permissões para objetos de diretório de domínio replicados para o catálogo global.

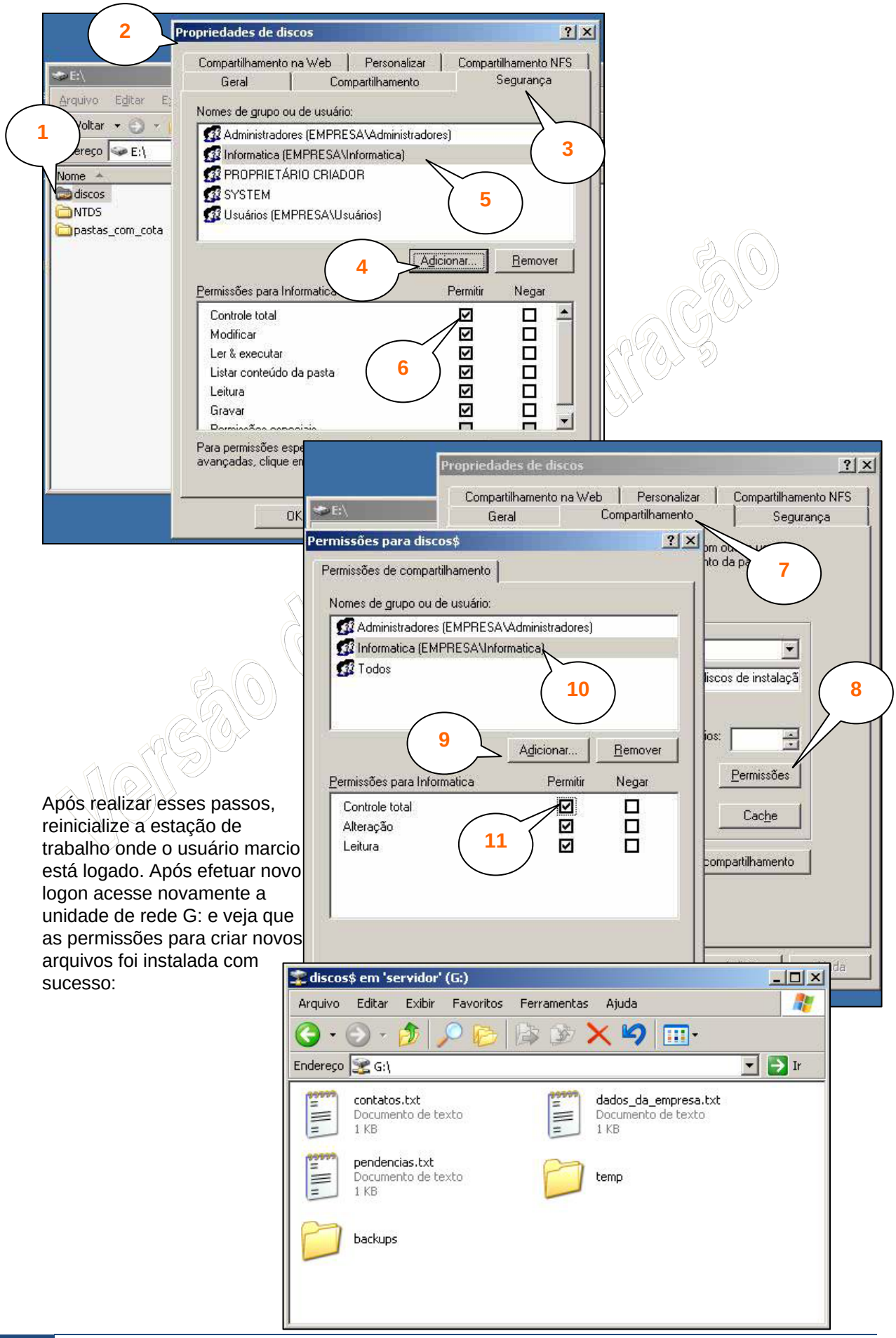
QUANDO USAR GRUPOS COM ESCOPO UNIVERSAL

Use grupos com escopo universal para consolidar os grupos que estendam domínios. Para fazer isso, adicione as contas a grupos com escopo global e aninhe esses grupos em grupos que tenham escopo universal. Com essa estratégia, todas as alterações de participação nos grupos com escopo global não afetarão os grupos com escopo universal.
Por exemplo, em uma rede com dois domínios, Europa e EstadosUnidos, e um grupo que tenha escopo global chamado ContabilidadeGL em cada domínio, crie um grupo com escopo universal chamado ContabilidadeU para ter como seus membros os dois grupos ContabilidadeGL: ContabilidadeEstadosUnidos\GL e ContabilidadeEuropa\GL. O grupo ContabilidadeU pode ser usado em qualquer parte da empresa. Todas as alterações na participação dos grupos individuais ContabilidadeGL não causarão a replicação do grupo ContabilidadeU.
A participação de um grupo com escopo universal não deve ser alterada com freqüência, pois todas as alterações feitas nessas participações de grupo podem fazer com que toda a participação do grupo seja replicada em cada catálogo global na floresta.

Voltando ao nosso exemplo, termine de adicionar o grupo Informática e adicione o membro márcio:



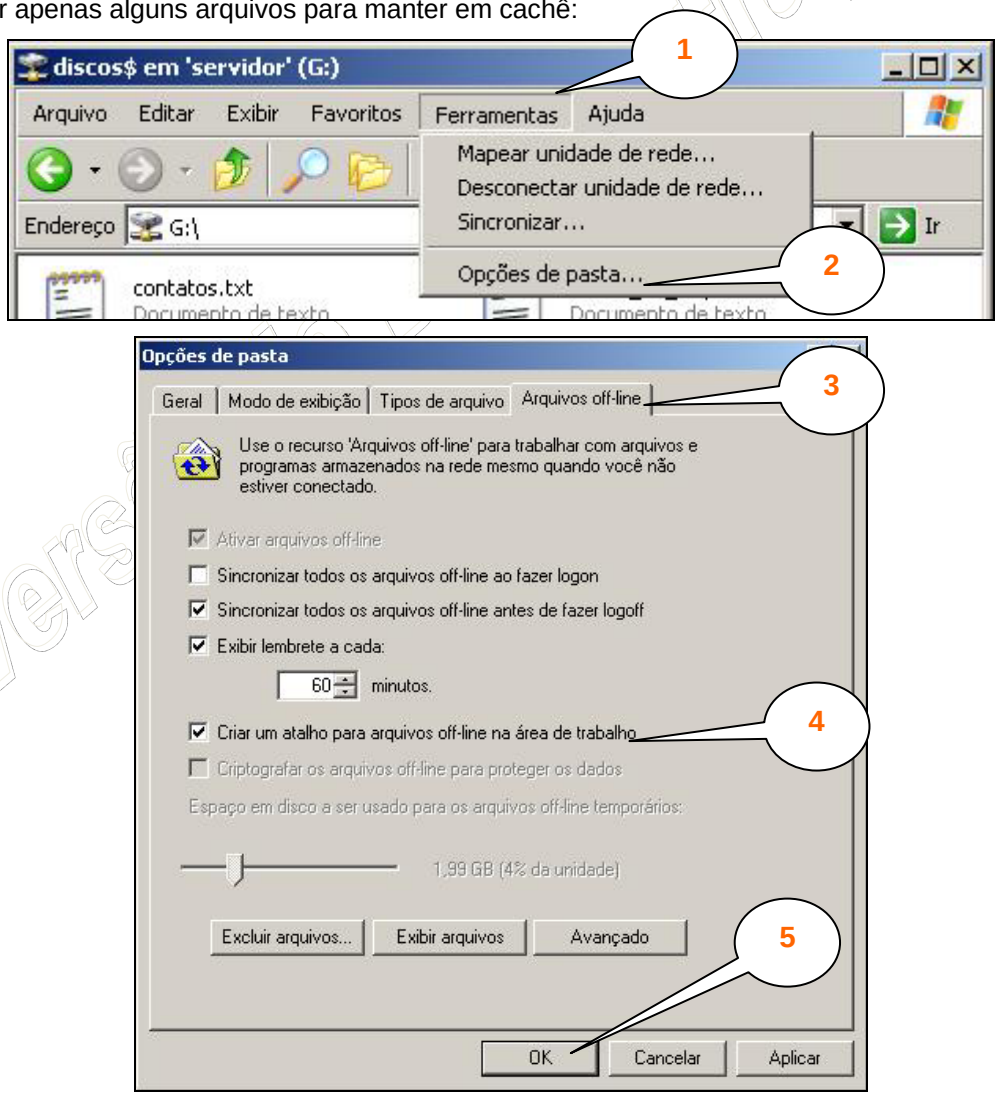
Agora estamos preparados para adicionar à pasta e:\discos, ao qual é acessada através da rede pelo UNC \\servidor\discos$, as permissões de acesso para o grupo Informática. Conforme vimos no estudo do sistema de arquivos NTFS, o sistema operacional Windows Server 2003, atua em dois níveis de proteção: atributos NTFS e permissões de acesso remoto. Ou seja, para liberarmos o acesso ao compartilhamento “discos$” ao grupo informática, teremos que realizar duas operações: 1. Atribuir permissões NTFS; 2. Atribuir permissões de compartilhamento, vejamos:



Após realizar esses passos, reinicialize a estação de trabalho onde o usuário marcio está logado. Após efetuar novo logon acesse novamente a unidade de rede G: e veja que as permissões para criar novos arquivos foi instalada com sucesso:

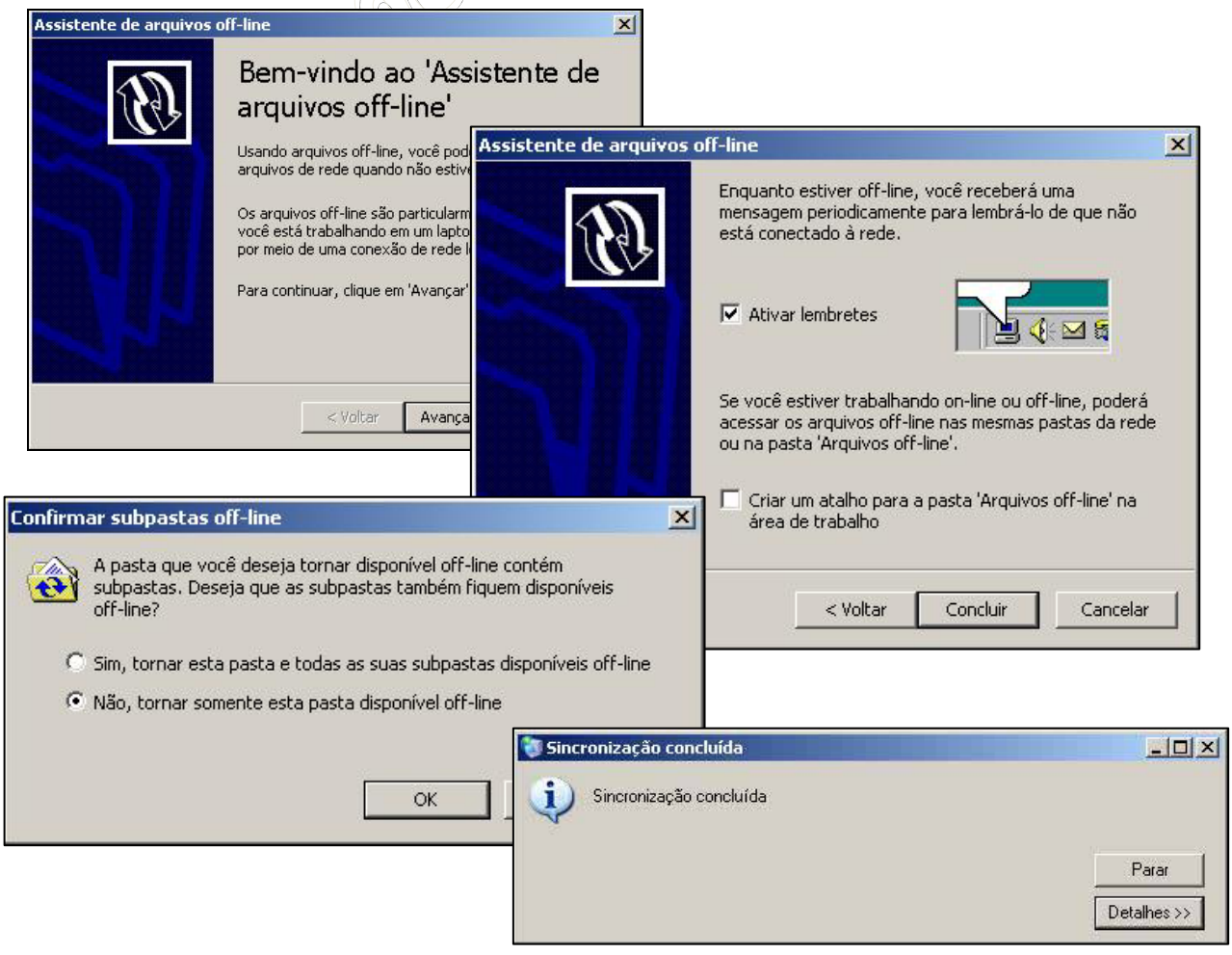
Agora vamos supor que o usuário “marcio” precise muito manter o arquivo “contatos.txt” em rede. Esse arquivo contém os dados dos principais clientes de Márcio. E precisa estar 100% do tempo disponível para consulta e inclusão de dados. O que ocorre se por um motivo qualquer, a rede torne-se indisponível? Significa que “marcio” não poderá acessar a unidade de rede G: e por conseqüência não poderá acessar o arquivo “contatos.txt”? Para muitos essa resposta é simplesmente sim, mas para nós, que estamos estudando o sistema operacional de rede Windows Server 2003, vamos apreender agora como a resposta é não:

Estamos falando do recurso “Arquivos Off-line”. Através deste recurso é criada uma área de armazenamento temporária em seu computador (também conhecida como Cache), para os arquivos mais críticos da rede, de forma que são gravados em seu computador e posteriormente sincronizado com os da rede. Enquanto estivermos online, conectados ao servidor através da unidade G: iremos trabalhar com os arquivos da rede, uma vez que a comunicação tenha sido interrompida iremos acessar o atalha da área de trabalho denominado “Arquivos Off-line”. Nesta pasta estarão as cópias dos arquivos que escolhermos para serem “sincronizados”, vejamos agora como habilitar esse recurso em nosso computador, configurar a unidade de rede para sincronizar e escolher apenas alguns arquivos para manter em cachê:

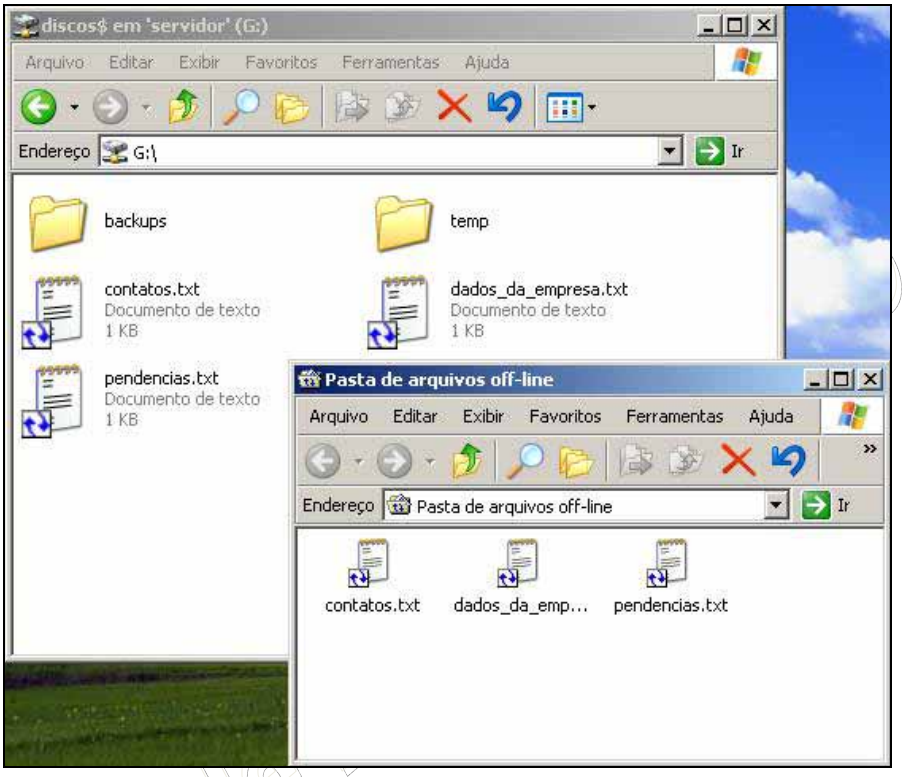


Os passos acima mostram como habilitar os Arquivos Off-line na estação de trabalho, vejamos agora como configurar uma unidade de rede para responder através deste recurso:

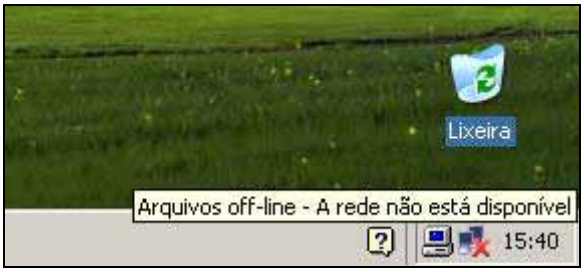
Ao clicar em “Tornar disponível off-line” um assistente o ajudará nas devidas escolhas a serem feitas:



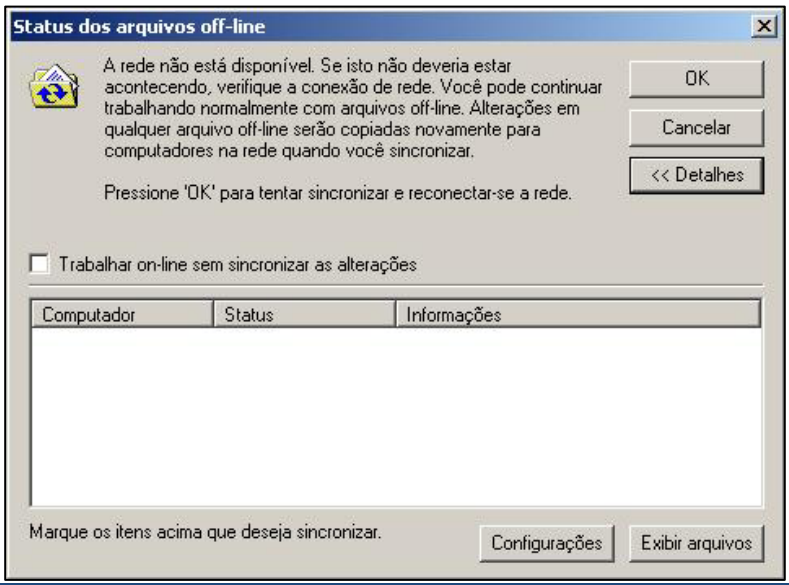
Uma vez habilitado o recurso de “Arquivos Off-line”, os ícones dos arquivos e da própria pasta, mudarão, para indicar que o recurso está sendo gerenciado pelos Arquivos Off-line:



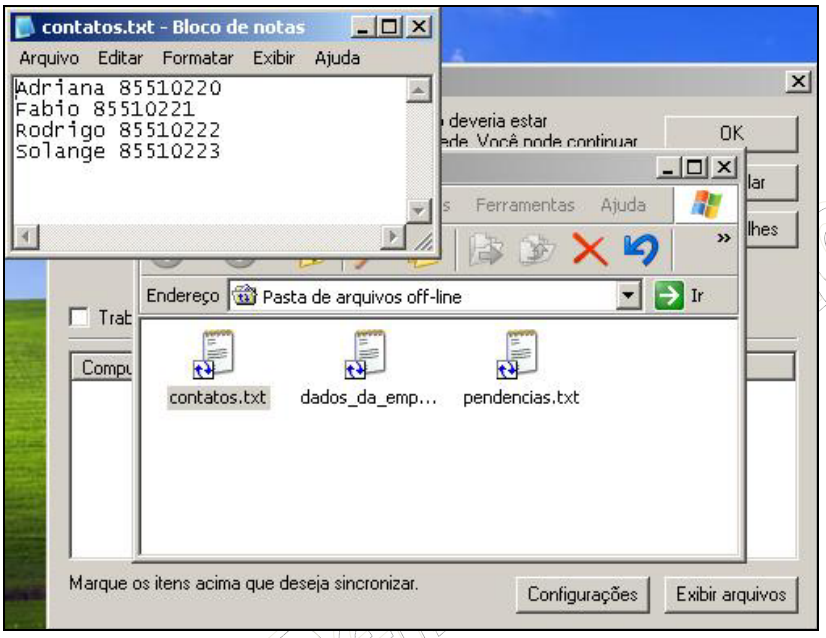
Vamos simular agora uma interrupção na rede, de forma a vermos como atua o Arquivos Off-line, acompanhe abaixo que o cabo de rede foi desligado e que o assistente de Arquivos Off-line identifica o ocorrido:



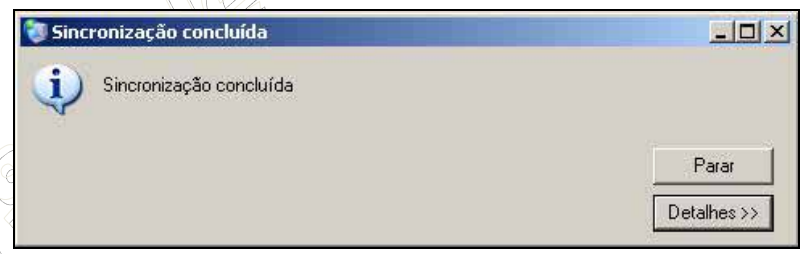
Clique sobre o assistente e verifique as recomendações:



Caso a rede permaneça off-line você pode clicar no botão “Exibir arquivos” para acessar os arquivos Off-line, ou opcionalmente clicar sobre o ícone da área de trabalho “Arquivos Off-line”, ambos o direcionarão para a mesma pasta. Vemos como os arquivos aparecem quando off-line:



Quando a conexão de rede for restabelecida acesse novamente este assistente, através do mesmo ícone da área de trabalho, e clique no botão de “OK” para os arquivos que foram modificados sejam enviados para a rede. Uma mensagem de sucesso será exibida caso não haja problemas:



Caso algum arquivo tenha sido modificado tanto no computador quanto na rede, um alerta de “Conflito” é exibido para você escolher qual versão quer atualizar. Também é possível escolher um único arquivo da unidade de rede para ser mantido em “Arquivos Off-line” para isso basta clicar com o botão direito do mouse sobre o arquivo pretendido e escolher a opção “Tornar disponível Off-line”:

Perfil móvel de usuários

Vejamos agora um outro recurso muito interessante das redes Microsoft, o perfil móvel de usuários.

O Perfil Móvel é criado pelo administrador do sistema e armazenado em um Servidor. Esse perfil está disponível sempre que você faz logon em qualquer computador na rede. Qualquer alteração feita no Perfil Móvel será atualizada no Servidor. Se o usuário efetuar logon em outra máquina, todas as configurações e preferências do Desktop (Área de trabalho), como por exemplo, impressoras, papel de parede, configurações de vídeo, etc, estarão disponível para o usuário.

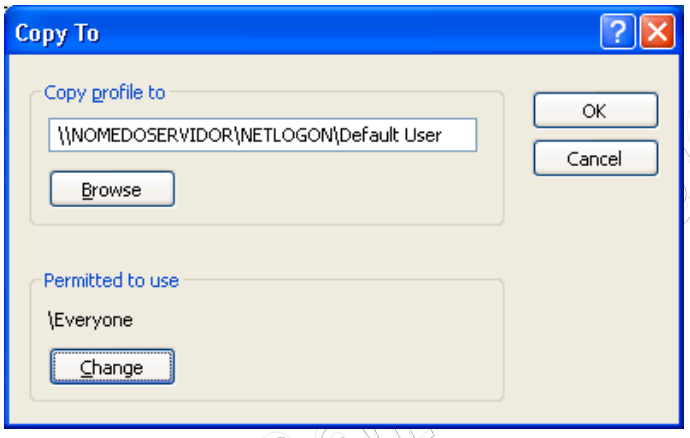
Para quem está querendo implementar um Perfil Móvel para todo o Domínio com um perfil modelo, veja abaixo as etapas de como criar essa configuração:

Observação:

Esse procedimento descrito abaixo funcionará somente para usuários que ainda não efetuaram logon na máquina cliente, caso o usuário já tenha efetuado logon você poderá excluir o perfil do usuário e solicitar que ele efetue logon para que o perfil personalizado que você irá criar com as etapas abaixo possa entrar em vigor. Antes de excluir o perfil do usuário salve em um local da rede para que você não perca nenhuma informação do usuário, como por exemplo, as Identidades do Outlook Express, Favoritos do Internet Explorer e o Meus Documentos.

1. Crie um usuário modelo no seu Domínio com o Active Directory Usuários e computadores.
2. Efetue logon em uma estação de trabalho Windows XP Professional com a conta do usuário modelo.
3. Crie todos os atalhos e configurações desejadas para servir como um perfil modelo para sua rede.
4. Efetue logoff da conta de usuário modelo, e efetue logon com a conta de administrador local da estação de trabalho.
5. No Painel de Controle acesse Sistema, clique na guia Avançado, e na seção Perfil de Usuário, clique no botão Configurações. Para ver a caixa de diálogo como mostra a figura 1.1.

6. Na caixa de diálogo Perfil de Usuário, selecione o perfil modelo, e clique no botão Copiar Para.
7. Na caixa de diálogo “Copiar Para”, no campo “Copiar Perfil Para” digite o caminho UNC, como por exemplo, \\SERVIDOR\NETLOGON\Default User.
8. Em “Uso Permitido”, clique no botão Alterar e defina o Grupo Todos, para que todos possam acessar o Perfil modelo, em seguida, clique no botão OK, para fechar a caixa de diálogo “Copiar Para”:



Observações:
Você está salvando o perfil modelo no compartilhamento NETLOGON com o nome Default User, porque quando um usuário efetua logon pela primeira fez em uma estação de trabalho o sistema operacional automaticamente irá procurar primeiro nesse compartilhamento por um perfil com o nome Default User, caso ele exista o perfil do usuário será copiado baseado neste perfil que está no compartilhamento NETLOGON e não no perfil Default User local da máquina cliente, e caso o perfil não exista ele irá usar o perfil Default User local da máquina do cliente.

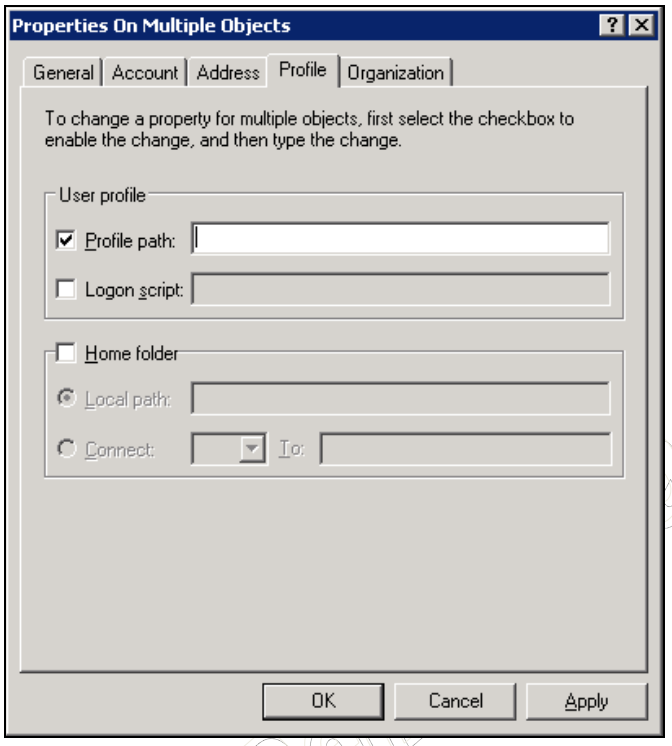
Um pequeno ajuste que você deverá fazer é acessar o compartilhamento NETLOGON\Default User e renomear a pasta "NomedoPefilModelo Documents" para “Meus Documentos”, para que os usuários não vejam o nome do perfil modelo junto com o nome de Documents.

Caso você queira salvar os perfis dos usuários em um local centralizado na rede, siga os passos abaixo:

1. Abra o Active Directory, Usuários e computadores, e selecione todos usuários dentro do mesmo container para que você possa adicionar de uma única vez o caminho do Profile (Perfil).
2. Na caixa de diálog Properties On Multiple Objects, clique na guia Profile, e selecione a opção Profile path, e digite o caminho para o perfil, como por exemplo...

\\NOMEDOSERVIDOR\NOMEDOCOMPARTILHAMENTO\%USERNAME%

...e em seguida clique no botão OK:



Pronto! Agora além do usuário ter um perfil de partida todo personalizado por você os perfis de todos os usuários do seu Domínio serão salvos em um compartilhamento da rede e você poderá fazer os backups para guardar os perfil dos usuários, caso você necessite de formatar a máquina do cliente você poderá voltar todas as suas configurações através do backup do perfil.

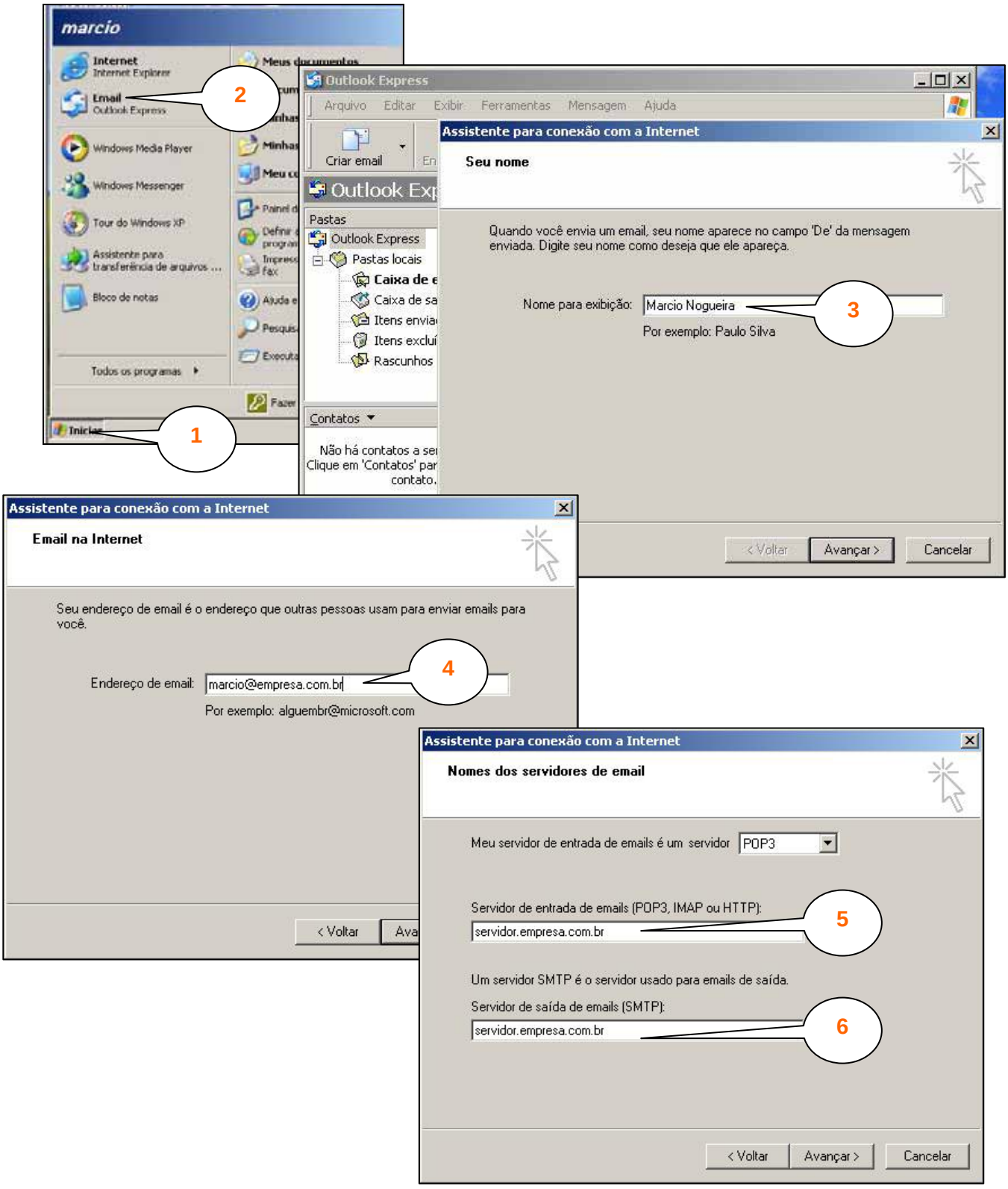
Para finalizar, não confunda Perfil Móvel com Perfil Obrigatório. O usuário com o Perfil Móvel poderá efetuar logon em qualquer máquina da rede, podendo salvar as alterações feitas no perfil. O usuário com o Perfil Obrigatório poderá efetuar logon em qualquer máquina da rede, mas não poderá salvar as alterações feitas no perfil. Geralmente esse tipo de perfil é usado para computadores que ficam expostos ao público ou para o Call Center.

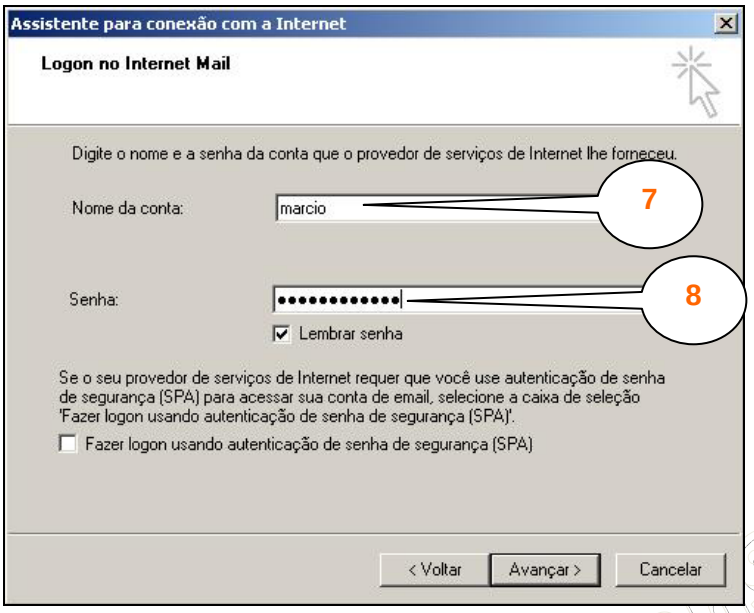
E-mail corporativo

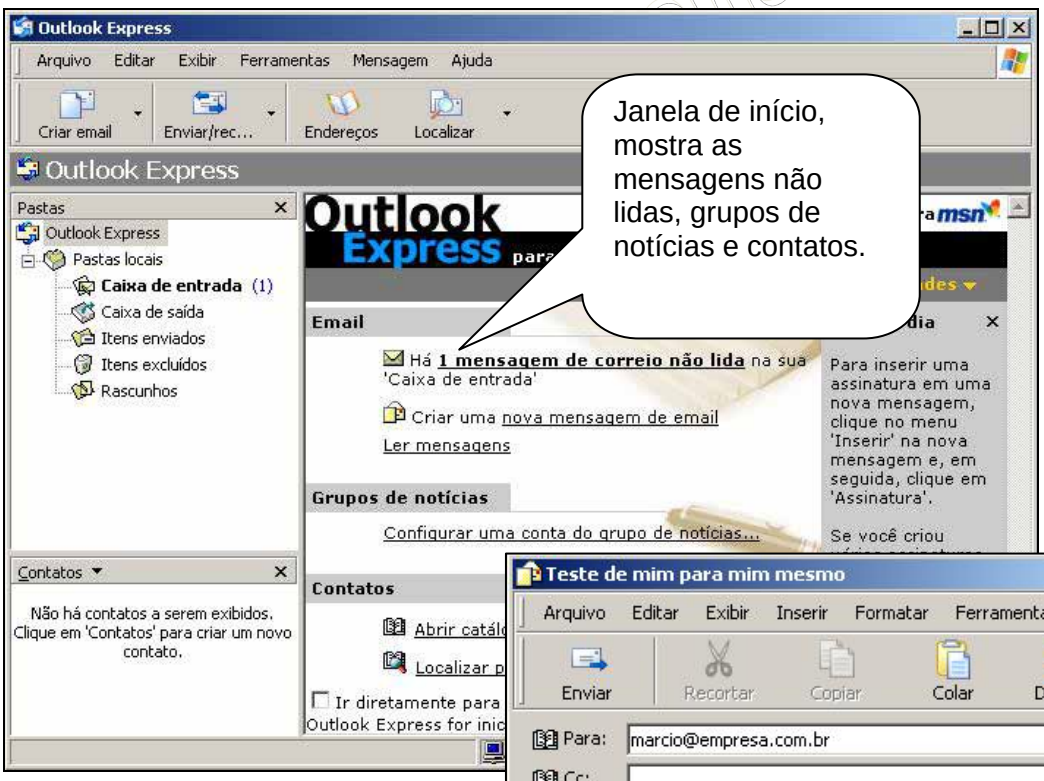
Veremos agora como acessar o e-mail corporativo, aquele criado pelos servidores POP3 e SMTP do Windows Server 2003.

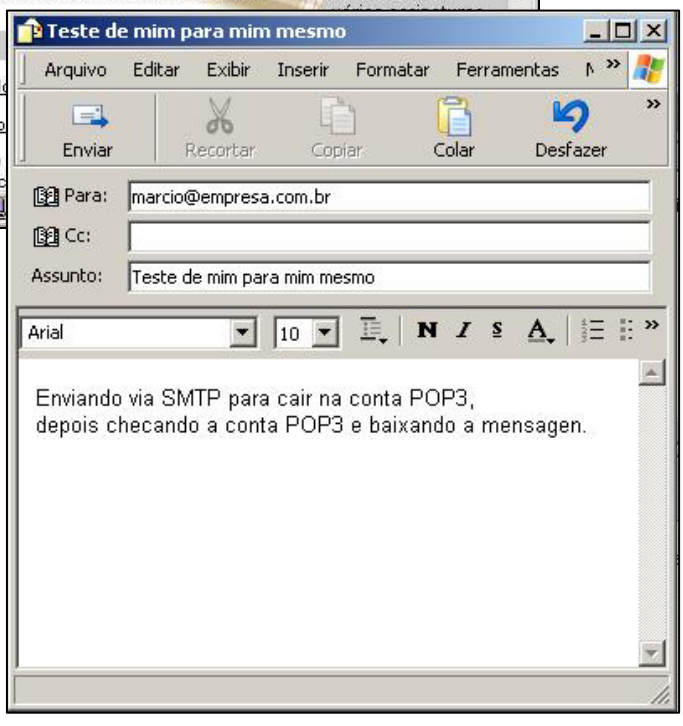
Na estação de trabalho acesso o aplicativo Outlook Express. O Outlook Express é um cliente de e-mail dos mais simples existentes, ideal para operar com nossos serviços básicos de POP3 e SMTP. Caso você esteja querendo uma solução mais completa, que inclua entre outras coisas: lista de e-mails, controles de acesso, filtros anti-spam, gerenciamento de filas e desempenho, procure pela alternativa Microsoft Exchange, como servidor, e Microsoft Outlook, como cliente de e-mail. O Microsoft Outlook está disponível junto com o pacote Microsoft Office.

Vejamos agora como acessar e configurar o Outlook Express:



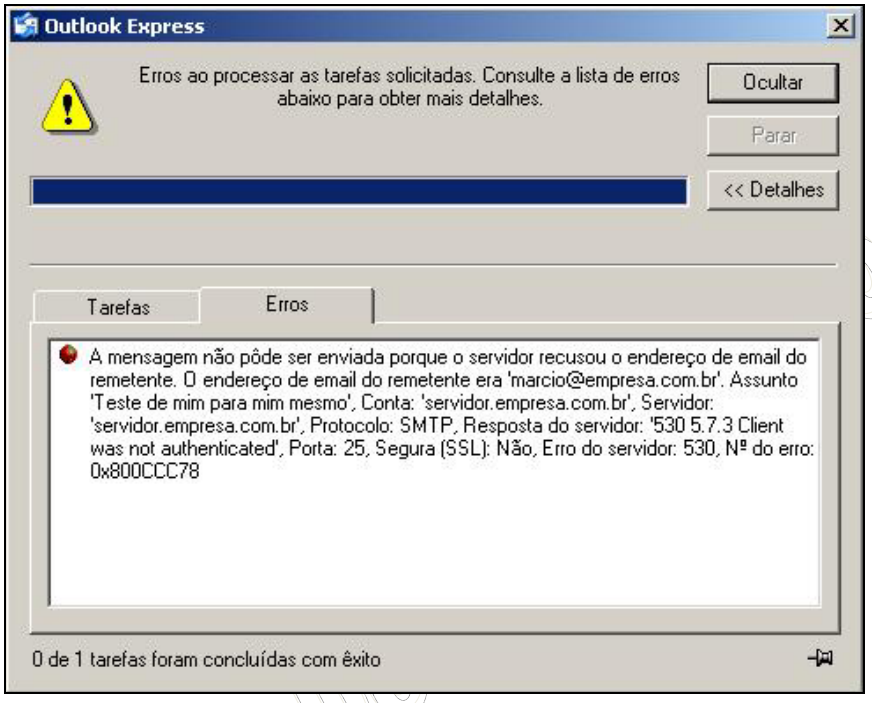




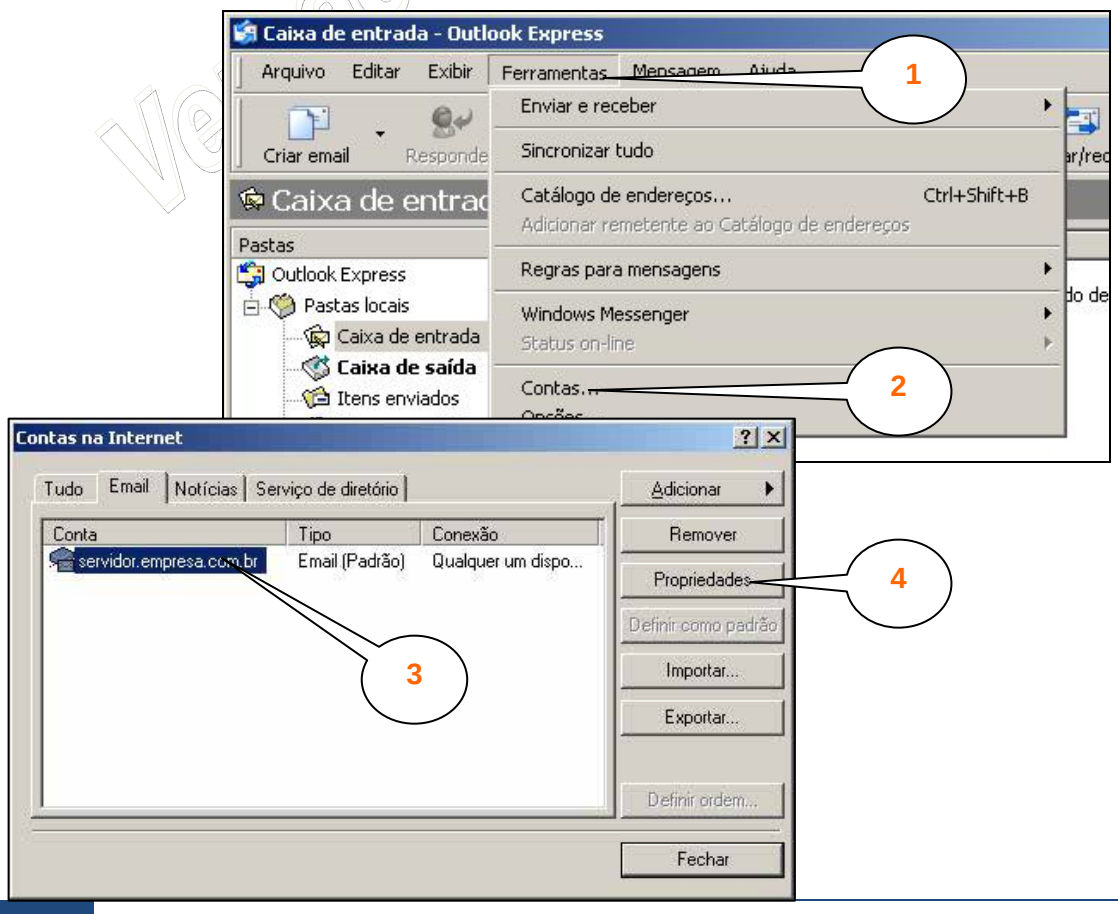


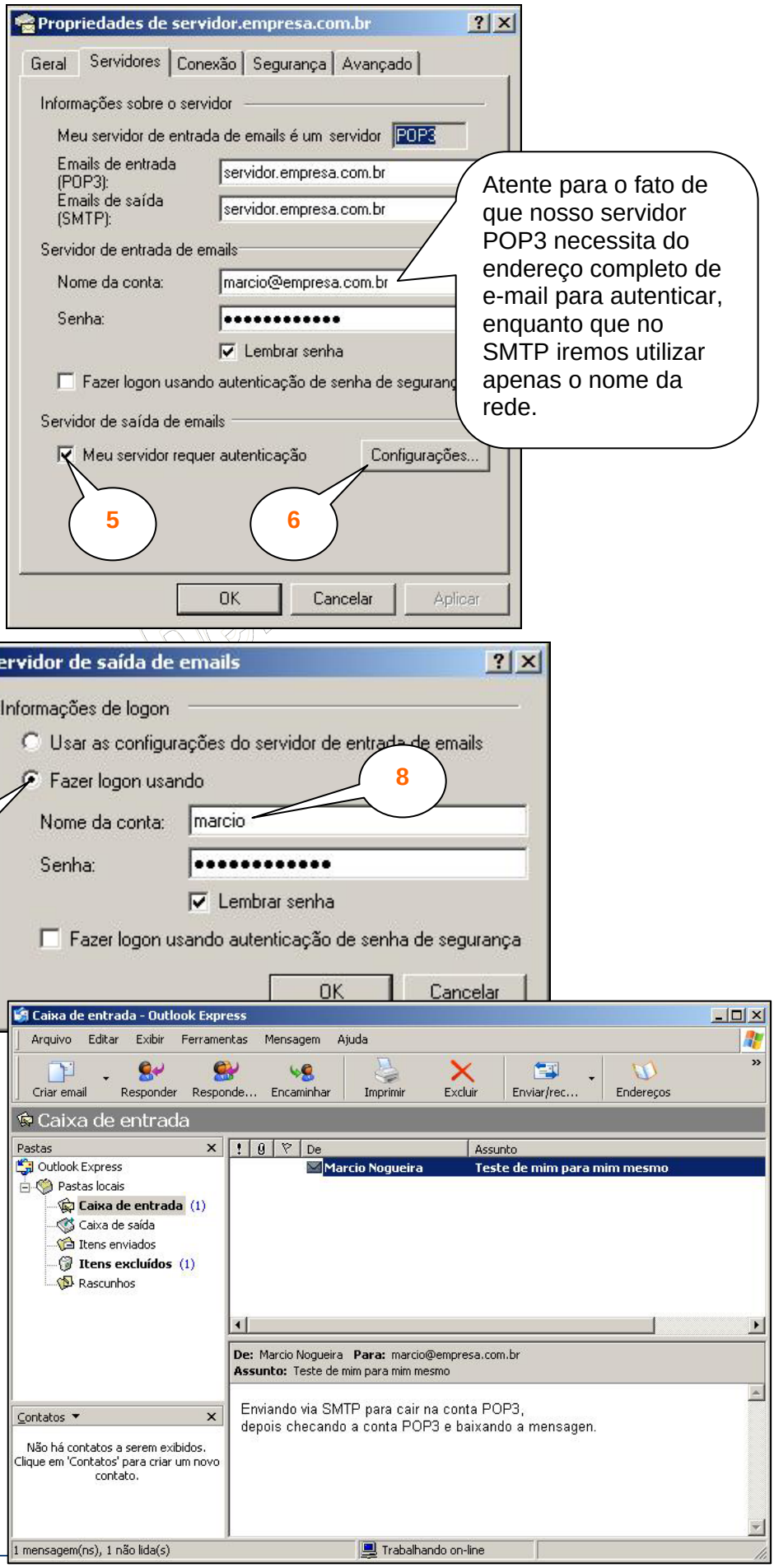
Façamos o primeiro teste, tente enviar uma mensagem de você para você mesmo. Isso pode parecer sem significado, mas possui uma grande importância. Como os serviços de envio e recebimento de mensagens são separados, através do SMTP (envio) e POP3 (recebimento), significa que estaremos utilizando o SMTP para enviar uma mensagem e uma conta POP3 para verificar se a mensagem ocorreu com sucesso.

Para ilustrar as configurações avançados do cliente de e-mail, vamos trabalhar sobre o seguinte erro:



Observe que a mensagem de erro foi: “Client was not authenticated”, que significa: O cliente não foi autenticado. Isso realmente procede, se você recordar as configurações que realizamos no serviço SMTP observará que protegemos o servidor contra envios adulterados por parte dos hackers, dessa forma habilitamos a autenticação do SMTP, ou seja, apenas usuários logados no SMTP poderão enviar mensagens. Vejamos agora como configurar o Outlook Express para autenticar no SMTP antes de enviar novas mensagens:



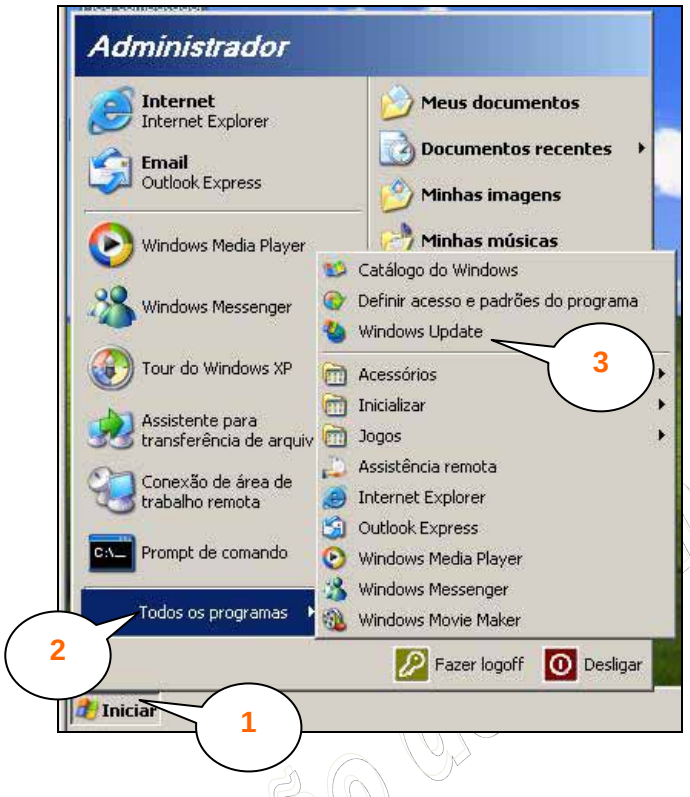


Finalmente após essa configuração poderemos observar que a mensagem que estava preza na caixa de saída consegue ser enviada e que posteriormente a mensagem é baixado do servidor POP3:

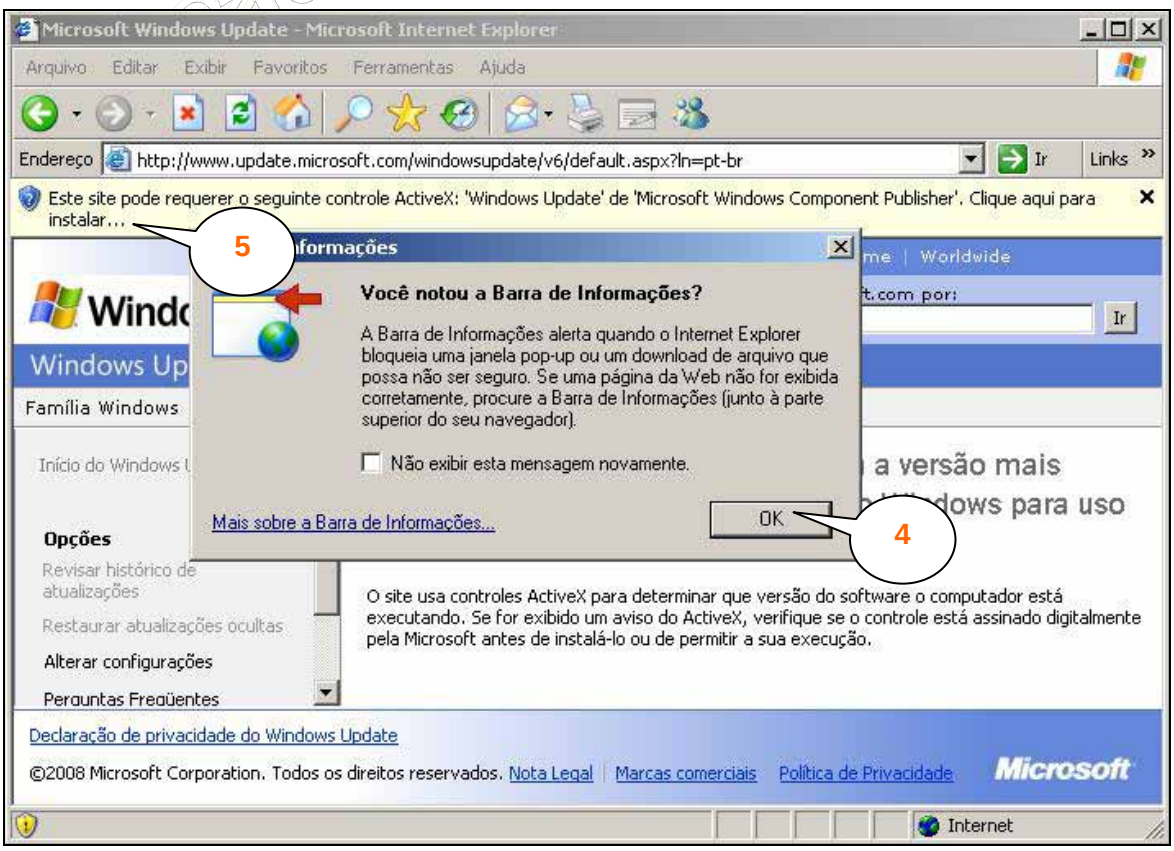
10.2 ATUALIZAÇÃO DO SISTEMA OPERACIONAL

Por fim, precisamos saber como atualizar nossos sistemas operacionais, veja a seguir como proceder para manter o Windows sempre atualizado:

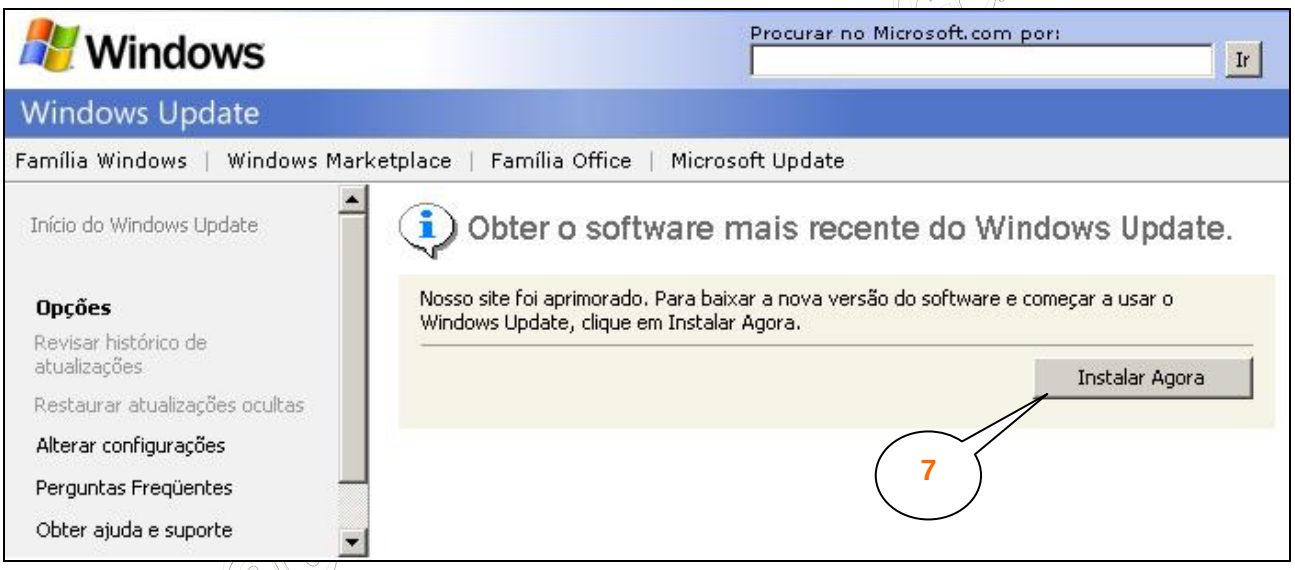
Para iniciar vá em: Iniciar -> Todos os Programas -> Windows Update



Instale o controlador Active-X solicitado pelo site:

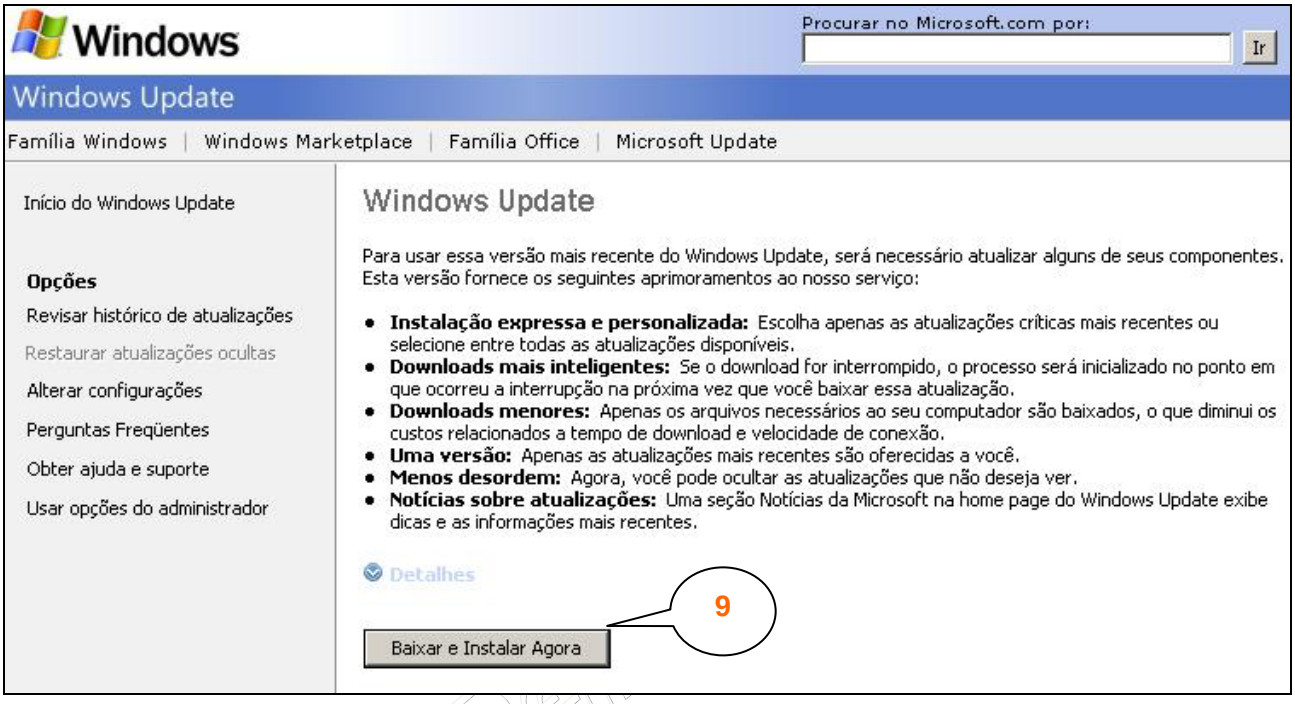


Instale a versão mais recente do software de atualização quando solicitado:

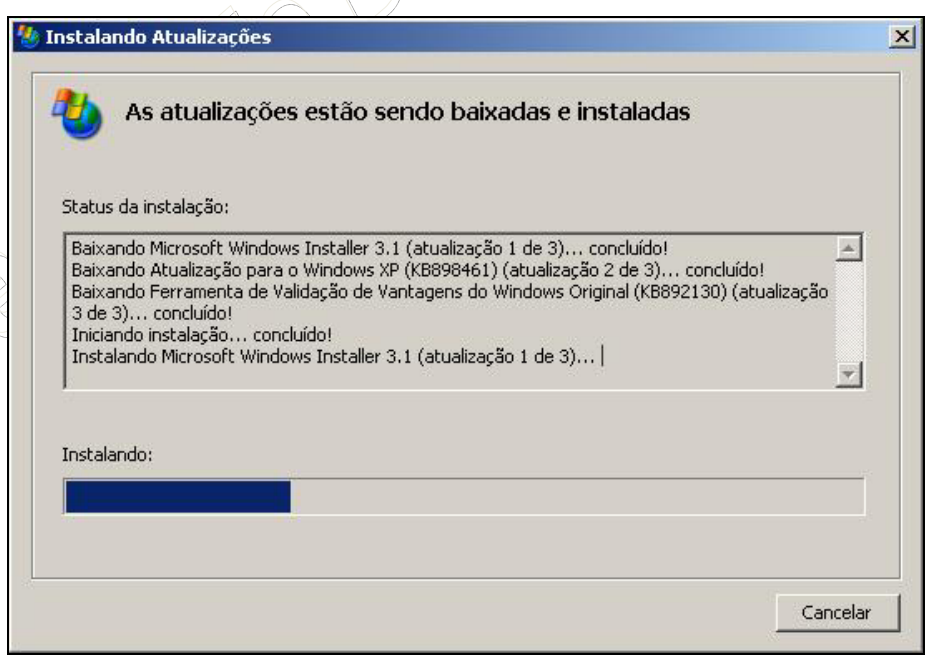


Faça uma atualização expressa, de forma que a baixar as principais atualizações de segurança e recomendadas:

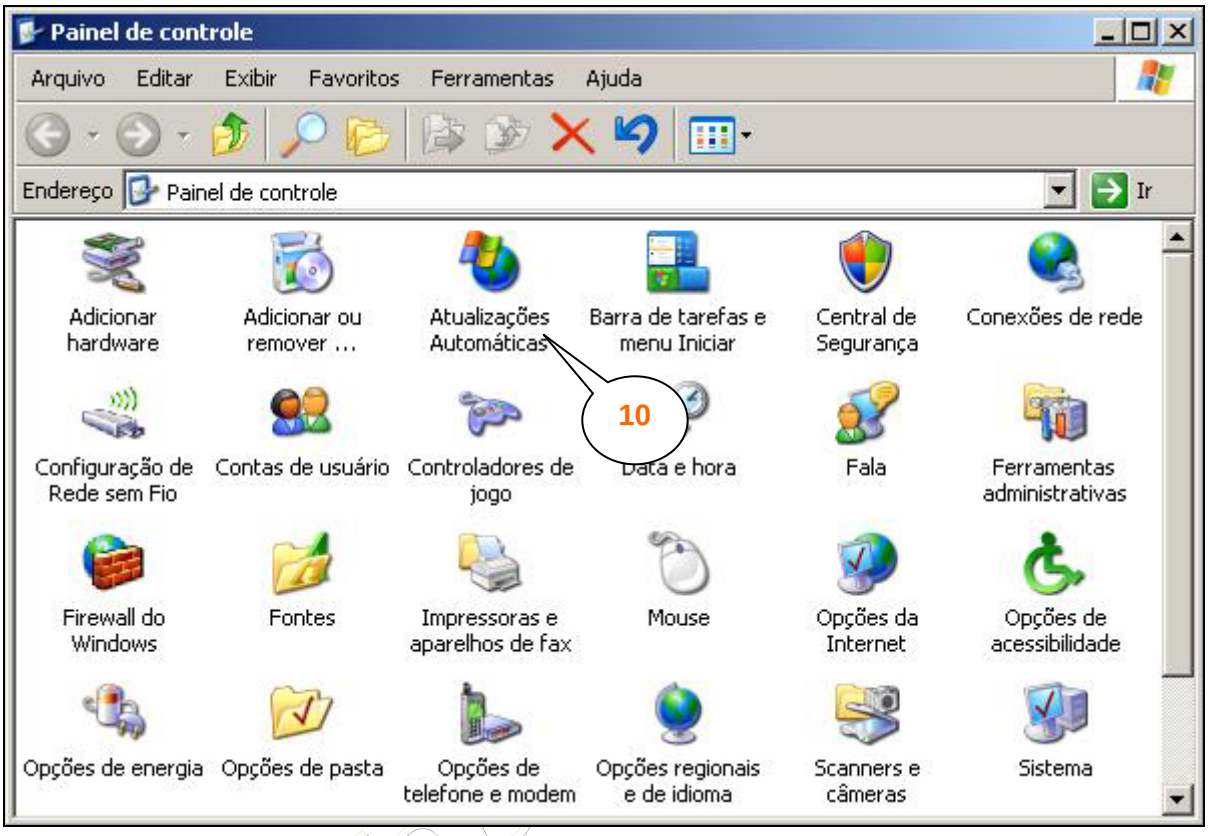
Verifique abaixo os itens que serão atualizados com a escolha da opção “Expressa”:

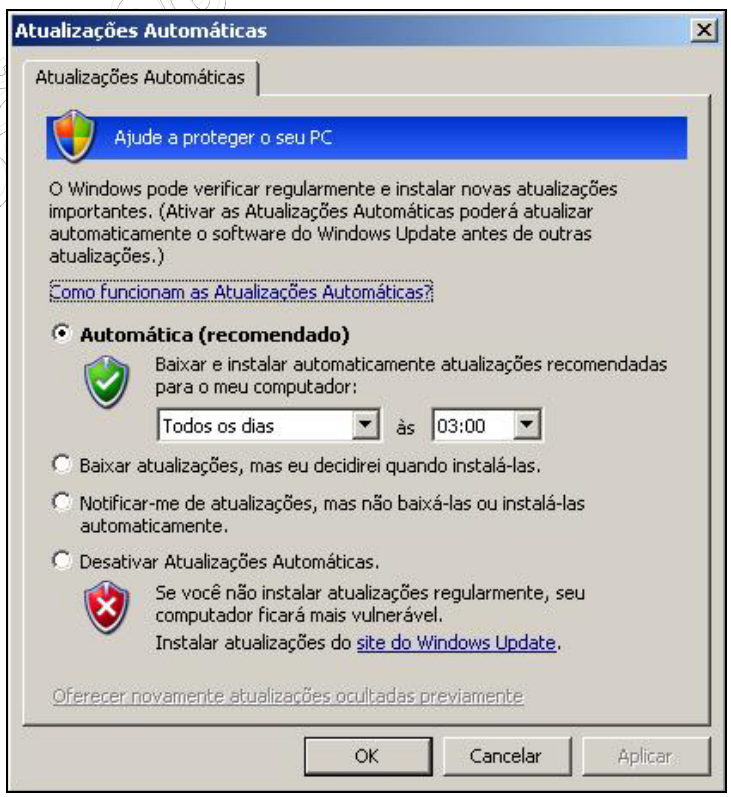


Aguar até que todas as atualizações sejam baixadas e instaladas, ao término do processo será solicitado para você reiniciar o computador:



Uma vez realizada a atualização do sistema para comunicação com o Windows Update você agora pode optar por automatizar as atualizações do Windows. Para isso, acesso o Painel de controle e siga as orientações abaixo:





Encerramos aqui nossa apostila, espero que você tenha praticado e estudado com atenção todas as telas aqui demonstradas, elas são úteis para aprender os conceitos e memorizar os passos, além de servir como uma excelente referência para sua vida profissional. Conte comigo para tirar suas dúvidas e sugerir melhorias para nossa disciplina de Sistemas Operacionais de Rede. Prof. Márcio Nogueira – marcio.nogueira@terra.com.br